

SQquadra

(Rev. 7a Agosto 2020)

Sommario

1 Principali Funzionalità di SQquadra231	6
1.1 Organizzazione della presente parte del manuale	6
1.1.1 Aree coperte da SQquadra	6
1.1.2 Sicurezza del canale di comunicazione.....	6
1.2 D.Lgs. 231/01 – Responsabilità amministrativa degli enti.....	7
1.2.1 Versione Base 231	7
1.2.2 Terminologia utilizzata all'interno di Squadra 231	7
1.2.3 Manutenzioni	8
1.2.4 Attività per la gestione del MOG e dell'Organismo di Vigilanza [MOG]	17
1.3 Sistemi informativi e Privacy	55
1.3.1 Analisi del Sistema	55
1.3.2 Trattamenti ed Eventi indesiderati (Violazioni).....	65
1.3.3 Documenti	75
1.3.4 Comunicazioni.....	81
1.3.5 Sistema Informativo	82
1.4 Sistema di Gestione	91
1.4.1 ANALISI	91
1.4.2 PIANIFICAZIONE	98
1.4.3 SUPPORTO.....	103
1.4.4 OPERATIVO	111
1.4.5 VALUTAZIONE	113
1.4.6 MIGLIORAMENTO	116
1.4.7 PREVENZIONE DELLA CORRUZIONE	118
1.4.8 GESTIONE DEL SISTEMA	125
1.4.9 VARIE	125
1.5 Altre Funzioni	128
1.5.1 Documentazione di supporto	128
1.5.2 Amministrazione del Sistema	128
1.5.3 Consulenti.....	130
1.5.4 Rapporti con la Pubblica Amministrazione	130
1.5.5 Oneri per la Sicurezza.....	130
1.5.6 Documentazione per la Sicurezza nei Cantieri [SicLa].....	130
2 Caratteristiche generali di SQUADRA231.....	132
2.1 Ingresso.....	132
2.2 Menù generale	132
2.3 Identificativo della maschera.....	133
2.4 Elaborazioni.....	133
2.5 Manutenzioni.....	133
2.5.1 Manutenzioni - Modalità GRIGLIA	134
2.5.2 Manutenzioni - Modalità DETTAGLI	135
2.5.3 Manutenzioni – Griglie di dettaglio.....	137
2.6 Cruscotti di presentazione dei dati	138
2.6.1 Personalizzazione dei Cruscotti	146
3 APPENDICE: Informativa sul Trattamento dei dati dei Clienti.....	147
3.1 Informativa sul trattamento dei dati personali per i Clienti de IL TIGLIO SRL	147
3.2 Accordo in merito al Trattamento di dati personali gestiti dall'Applicazione web SQquadra disponibile via Internet.	150
4 APPENDICE: Informativa sul trattamento dei dati inseriti dagli Utenti.....	153
4.1 Premessa	153
4.2 Informazioni generali.....	153
4.2.1 Origine dei dati e responsabilità	153
4.2.2 Dati personali.....	153
4.2.3 Caratteristiche dei trattamenti	154
5 APPENDICE: SGSI de IL TIGLIO SRL	158
5.1 Introduzione	158
5.1.1 Utilizzo di SQquadra	158
5.2 Politica (Rev. 1.a)	159
5.3 Servizi Cloud	163
5.4 Server di Produzione	167

5.5	Livello di Servizio	172
5.5.1	Sicurezza Fisica	172
5.5.2	Funzionalità operativa	173
5.5.3	Rilevamento guasti e/o anomalie	173
5.5.4	Statistiche	174
6	APPENDICE: Aggiornamenti del Modello.....	175
6.1	Aggiunta di nuovi Reati.....	175
7	APPENDICE: Aggiornamento Codice di Comportamento ANCE 2020	176
7.1	Premessa	176
7.2	Analisi dei Nuovi Punti di Controllo	176
7.3	Nuove correlazioni	176
7.4	Aggiornamento dei Punti di Controllo	176
7.5	Verifica dei Punti di Controllo aziendali	177
7.6	Adeguamento della Parte Generale	177
8	APPENDICE: CoSO Report	178
8.1	La gestione dei rischi aziendali (ERM)	178
8.1.1	Versione del Giugno 2017	178
8.1.2	Gestione del Rischio e Performance (Profilo di rischio).....	183
8.1.3	Le principali modifiche della versione 2017 rispetto a quella del 2004.....	184
8.1.4	La gestione del rischio: qualche malinteso	186
8.1.5	Benefici connessi alla gestione del rischio aziendale.....	186
8.1.6	Il ruolo del rischio nella scelta della strategia	187
8.1.7	Possibili risposte al Rischio	188
8.1.8	I Rischi connessi ai cambiamenti.....	189
8.1.9	Uno sguardo rivolto al futuro.....	190
9	APPENDICE: Analisi dei Rischi 231	191
9.1	Introduzione	191
9.2	Analisi degli Illeciti e dei Reati presupposto.....	193
9.3	Progettazione del Modello	196
9.3.1	Livello di Rischio	196
9.3.2	La Regolazione	200
9.3.3	Pericoli.....	205
9.3.4	Correlazione	205
9.3.5	Rischio Residuo Teorico.....	205
9.3.6	Il calcolo del Rischio Residuo Atteso	206
9.3.7	Gap Analysis	207
9.4	Adequatezza del Modello	207
10	APPENDICE: Rischio Residuo Rilevato	208
10.1	Introduzione	208
10.2	Conformità alle procedure	208
10.3	Valutazione in assenza di audit / informative	209
10.4	Decadimento delle valutazioni nel tempo	209
10.5	Funzioni aziendali multiple	210
10.6	Controlli di secondo livello	210
10.7	Correlazione.....	210
10.8	Governance	211
10.9	Valutazione riepilogativa per Reato	212
10.10	Metodo Lineare	212
10.11	Metodo Non Lineare	213
11	APPENDICE: Asseverazione	214
11.1	Introduzione	214
11.2	SQuadra231 per l'Asseverazione	214
12	APPENDICE: Oneri aziendali per la sicurezza	218
12.1	Introduzione	218
12.2	Oneri Aziendali	218
12.3	Gare	219
13	APPENDICE: Analisi del Contesto.....	221
13.1	Introduzione	221
13.2	Metodologia	221
13.3	Modalità operative	229
14	APPENDICE: Analisi del Rischio per Processi	232
14.1	Introduzione	232
14.2	Processi	235
14.3	Analisi	236

15 APPENDICE: Valutazione Fornitori	237
15.1 Introduzione	237
15.2 Criteri per la Valutazione	237
15.3 Modalità operative	240
15.4 Registro	242
16 APPENDICE: Comunicazioni.....	243
16.1.1 Elementi da Comunicare.....	243
17 APPENDICE: Conformità legislativa e ad altre prescrizioni	248
17.1 Introduzione	248
17.2 Modalità operative	250
18 APPENDICE: Idoneità Tecnico Professionale	254
18.1 Premessa	254
18.2 Archivio documenti aziendali	254
18.3 Archivio aziendale dei Soggetti Fornitori	256
18.3.1 Documenti del Soggetto	256
19 APPENDICE: Regolamento Europeo protezione dei dati personali (GDPR)	257
19.1 Premessa	257
19.2 Criteri per determinare la necessità di effettuare una Valutazione Impatto Privacy (PIA)	259
19.3 Glossario predisposto da Confindustria per il Registro delle attività di Trattamento	261
19.3.1 Organigramma	261
19.3.2 Descrizione del trattamento	261
19.3.3 Misure di sicurezza: alcuni esempi	263
20 APPENDICE: Sistema di Gestione per la Sicurezza delle Informazioni	265
20.1 Norma ISO 27001.....	265
20.2 Rischi	265
20.3 Eventi indesiderati	267
20.3.1 Definizioni.....	267
20.3.2 Gestione degli eventi imprevisti	269
21 APPENDICE: Controlli sui Sistemi Informativi	270
21.1 Norma ISO 27001.....	270
21.2 Agenzia per l'Italia Digitale.....	270
21.2.1 La scelta delle Classi	270
21.3 Framework Nazionale per la Cyber Security”	271
21.3.1 Premessa	271
21.3.2 La cyber security	271
21.3.3 Organizzazione del Framework	273
21.3.4 Contestualizzazione del Framework	275
21.3.5 Contestualizzazione per le PMI	275
21.3.6 Controlli essenziali 2016	276
22 APPENDICE: Linee Guida ENISA sulla sicurezza dei dati personali.....	277
22.1 Introduzione	277
22.1.1 La Sicurezza delle informazioni	277
22.1.2 Gestione del Rischio	277
22.1.3 Obblighi di sicurezza nel GDPR.....	278
22.2 Valutazione dei Rischi per la sicurezza dei dati personali	279
22.2.1 Definizione dell'operazione di trattamento e del suo contesto	279
22.2.2 Comprensione e valutazione dell'impatto	279
22.2.3 Valutazione dell'impatto	280
22.2.4 Definizione delle minacce	280
22.2.5 Valutazione del rischio	281
23 REVISIONI	282

Organizzazione del presente Manuale

Il presente Manuale contiene una presentazione delle funzionalità del software SQuadra231 (versione 2016) [software presentato anche nella Terza Parte (sezione D) del Codice di Comportamento di ANCE 2013] nella sua versione ESTESA.

Nella prima parte vengono illustrate le **funzionalità di SQuadra231**.

Nella seconda parte vengono presentate le **modalità operative** comuni a tutte le funzioni di SQuadra231. *Per quanto possibile SQuadra231 utilizza modalità operative intuitive o comunque standard per chi opera comunemente con applicativi web, è tuttavia necessaria la lettura di questa sezione prima dell'uso di SQuadra231 per conoscere le convenzioni utilizzate.*

L'APPENDICE 3 fornisce indicazioni sul **Trattamento dei dati**.

L'APPENDICE 4 contiene la **Informativa sul trattamento dei dati**.

Nell'APPENDICE 5 vengono riportate le caratteristiche principali del Sistema per la Gestione della Sicurezza delle Informazioni **SGSI de IL TIGLIO SRL** compresi i livelli del Servizio di SQuadra231.

L'APPENDICE 6 descrive le operazioni da compiere per aggiornare il Modello in caso di introduzione di **nuovi reati**.

Nell'APPENDICE 7 vengono indicate le modalità per l'utilizzo dell'Aggiornamento del **Codice di Comportamento ANCE 2018**. Ovviamente questa Appendice interessa solo gli utenti che utilizzavano il Codice di Comportamento ANCE antecedente.

L'APPENDICE 8 contiene una descrizione dei documenti predisposto dal comitato internazionale **COSO** espressamente citati nelle Linee Guida di Confindustria.

L'APPENDICE 9 fornisce un metodo per l'**Analisi dei Rischi 231** ed è rivolta agli enti che non possono definire la propria complessità "standard" secondo quanto previsto dal Codice di Comportamento ANCE 2013 (Cfr. Analisi dei rischi, pag. 182-183) e che quindi non possono utilizzare direttamente l'analisi dei rischi effettuata da ANCE (identificazione dei reati applicabili e dei processi critici).

L'APPENDICE 10 illustra le modalità utilizzate da SQuadra231 per il calcolo del **Rischio Residuo Rilevato** a seguito dell'applicazione del Modello ed alle attività di Vigilanza svolte dall'OdV.

Nell'Appendice 11 vengono analizzate le modalità di **Asseverazione** di un ente.

Nell'APPENDICE 12 viene illustrato un semplice strumento per il calcolo degli **oneri della sicurezza aziendali** da indicare negli appalti pubblici sulla base del metodo messo a punto nel documento ANCE-ITACA.

L'APPENDICE 13 descrive le modalità per effettuare una **Analisi del Contesto** e può essere direttamente utilizzata come istruzione per il Sistema di Gestione aziendale.

L'APPENDICE 14 descrive le modalità per effettuare una **Analisi dei Processi** e può essere direttamente utilizzata come istruzione per il Sistema di Gestione aziendale.

L'APPENDICE 15 descrive le modalità con le quali viene effettuata la **Valutazione dei Fornitori** e può essere direttamente utilizzata come istruzione per il Sistema di Gestione aziendale.

L'APPENDICE 16 descrive le modalità con le quali è possibile trasmettere della **Comunicazioni** via mail ed ottenere delle risposte automatizzate.

L'APPENDICE 17 descrive le modalità con le quali viene effettuata assicurata la **Conformità legislativa ed in genere alle Prescrizioni aziendali** e può essere direttamente utilizzata come istruzione per il Sistema di Gestione aziendale.

L'APPENDICE 18 descrive le funzionalità per la gestione dei Documenti necessari per l'**Idoneità Tecnico Professionale**.

Nell'APPENDICE 19 vengono illustrate le caratteristiche di SQuadra in relazione al **Regolamento Europeo** per la protezione dei dati personali.

L'APPENDICE 20 illustra le caratteristiche principali di un **Sistema per la Gestione della Sicurezza delle Informazioni**.

L'APPENDICE 21 riporta alcuni sistemi di riferimento per i **Controlli sul Sistema Informativo**.

Nell'APPENDICE 22 vengono illustrati i documenti predisposti da **ENISA** per la protezione dei dati personali.

L'ultima parte riporta le principali modifiche apportate in corrispondenza con le varie **Revisioni** del presente manuale ed è dedicata unicamente agli utenti che hanno già letto una versione precedente del Manuale per individuare con facilità le novità dell'ultima versione¹.

¹ SQuadra231 è in continua evoluzione in funzione delle richieste provenienti dagli utenti. Ad ogni modifica del programma viene aggiornato anche il Manuale d'uso. Il Manuale è caratterizzato dall'indice della Versione che è composto da un numero che viene modificato in occasioni di revisioni significative e da una lettera che viene modificata ad ogni revisione anche se di piccola entità. È opportuno controllare la versione attuale con quella disponibile e, soprattutto in caso di cambio di numerazione, si consiglia di leggere le novità della nuova versione.

1 Principali Funzionalità di SQuadra231

1.1 Organizzazione della presente parte del manuale

Di seguito viene riportata una presentazione delle funzionalità di SQuadra231 ESTESO.

I comandi e le modalità operative la cui conoscenza è necessaria per poter utilizzare SQuadra231 sono riportati nella Sezione successiva di cui si consiglia la lettura per poter utilizzare al massimo le potenzialità del prodotto.

1.1.1 Aree coperte da SQuadra

SQuadra copre varie aree fra loro parzialmente integrate. Per semplicità possiamo definire le seguenti Aree:

- D.Lgs. 231/01 (Manutenzione Modello e attività OdV).
- Privacy.
- Sistemi di Gestione.
- Funzionalità Varie.

È possibile iniziare ad utilizzare SQuadra partendo da una qualunque delle Aree coperte.

Il presente Manuale rispecchia la suddivisione per Aree ed è possibile iniziare la lettura delle funzionalità partendo dall'Area di maggiore interesse.

1.1.2 Sicurezza del canale di comunicazione

SQuadra opera tramite un protocollo (HTTPS²) che garantisce la sicurezza della comunicazione.

La possibilità di accedere a SQuadra tramite una connessione internet richiede particolare accortezza nella qualità e nella riservatezza delle password (per la modifica e il recupero della password si veda avanti all'inizio della presentazione delle Modalità Operative).

1.1.2.1 Controlli di SQuadra sulla Sicurezza

SQuadra segnala con una mail all'utente la rilevazione di più di 5 tentativi di accesso con password errata. Qualora l'utente non riconosca come suoi i tentativi e sospetti quindi un attacco dall'esterno ai dati memorizzati si consiglia di modificare la propria password aumentandone la "robustezza" (lunghezza, uso di caratteri speciali, ecc.).

SQuadra permette all'utente di controllare tutti i LOG di accesso (si veda avanti in Altre Funzioni / Amministratore del Sistema). Qualora si rilevi la presenza di accessi non riconosciuti come propri sarà necessario modificare immediatamente la propria password.

SQuadra non impone la modifica periodica della Password, necessaria come misura di sicurezza solo se vengono inseriti all'interno del programma dati personali, ma segnala, con una mail all'utente qualora non abbia provveduto a modificare la prima password assegnata entro 3 mesi e qualora non abbia modificato la propria password da più di 12 mesi.

² Un protocollo HTTPS fornisce l'autenticazione del sito web e del server web associato, proteggendo la comunicazione dagli attacchi noti tramite la tecnica del man in the middle. Inoltre, HTTPS fornisce una cifratura bidirezionale delle comunicazioni tra un client e un server, che protegge la stessa contro le possibili operazioni di ascolto segreto della conversazione privata tra le parti senza il loro consenso e di manomissione o alterazione della comunicazione falsificandone i contenuti. In pratica, tale meccanismo fornisce una garanzia soddisfacente del fatto che si stia comunicando esattamente con il sito web voluto, oltre a garantire che i contenuti delle comunicazioni tra l'utente e il sito web non possano essere intercettate o alterate da terzi.

1.2 D.Lgs. 231/01 – Responsabilità amministrativa degli enti

1.2.1 Versione Base 231

Per l'avvio di un Sistema 231 è previsto un modulo Base (semplificato) che fornisce anche un supporto per la prima compilazione.

Per utilizzare il Modulo Base (per l'uso della quale si rimanda allo specifico manuale) è necessario selezionare "VERSIONE BASE" nel menu all'estrema destra in alto (sotto il nome dell'Utente).

Verranno nuovamente richieste le credenziali e si entrerà nella gestione documenti.

Per avere un supporto alla prima compilazione è necessario scorrere le varie maschere con i bottoni in alto a destra andando alle FUNZIONI AZIENDALI, ai DATI ANAGRAFICI ed infine al QUESTIONARIO.

1.2.2 Terminologia utilizzata all'interno di Squadra 231

Processi	Sono i Processi tipici di qualunque Ente. Non sono modificabili.
Attività	Ogni Processo viene suddiviso in varie Attività. Possono essere modificate.
Punti di Controllo	All'interno di ogni Attività vengono definiti dal Progettista 231 una serie di Punti di Controllo che, nel loro insieme, permettono di prevenire la commissione dei vari Reati previsti dalla 231.
	I Punti di Controllo possono prendere spunto dalle indicazioni delle varie Linee Guida (in particolare quella di ANCE che, a sua volta, fa riferimento a quelle di Confindustria).
Procedure	Sono le modalità concrete di applicazione del Punto di Controllo all'interno dell'ente. <i>ATTENZIONE: Per valutare la correttezza formale di una Procedura si suggerisce di verificare che sia possibile per l'Organismo di Vigilanza applicare una sanzione disciplinare ad una specifica persona a frante della non applicazione della stessa.</i> <i>In pratica una Procedura è ben definita se è possibile, per che deve effettuarne il controllo, rilevare delle evidenze oggettive che ne dimostrino la corretta applicazione (presenza di un documento, di una firma, di una registrazione, ecc.).</i> <i>In caso di rilevazione di una Non Conformità nell'applicazione della Procedura deve essere possibile identificare il responsabile della carenza. In pratica lo stesso compito non può essere affidato a più di una persona in modo indistinto. È possibile affidare lo stesso compito a più persone solo indicando l'area di competenza di ognuno (es. il Cantiere di competenza); altrimenti è necessario indicare un solo Responsabile che potrà delegare ad altri mantenendo comunque la responsabilità del controllo sulle attività delegate ed assumendosi la responsabilità finale nei confronti dell'Organismo di Vigilanza.</i>

1.2.3 Manutenzioni

1.2.3.1 Personalizza

Questo gruppo di opzioni permettono di predisporre e modificare il Modello di Organizzazione e Gestione.

Dati Aziendali

Vengono qui inserite le informazioni aziendali fondamentali (Ragione Sociale, Partita Iva, ecc.).

Sono inoltre mantenibili alcune informazioni che verranno utilizzate per automatizzare alcune funzioni rivolte all'OdV:

- Sede presso la quale si riunisce prevalentemente l'OdV.
- Nominativi dei Membri dell'OdV (sono previsti fino ad un massimo di 5 membri).
- Data di prima nomina dell'OdV.
- Data prevista per la prossima riunione dell'OdV (la data verrà aggiornata automaticamente, in base alla pianificazione effettuata al momento della registrazione dell'ultimo Verbale).
- Data prevista per la prossima Relazione periodica dell'OdV (la data verrà aggiornata automaticamente, in base alla pianificazione effettuata al momento della registrazione dell'ultima Relazione – si ipotizza che la Relazione debba essere prodotta entro il mese successivo alla fine del periodo in esame).

Vengono inoltre presentati (questi dati non possono essere modificati dall'utente):

- Data dell'aggiornamento dei Punti di controllo Aziendali alle LINEE GUIDA (il dato, *significativo solo per Aziende che basano il loro Modello sul Codice di Comportamento ANCE*, viene modificato dal programma al momento della prima elaborazione del questionario e ogni volta che l'utente richiede l'aggiornamento come descritto avanti nel Capitolo relativo alle Versioni).

Funzioni Aziendali

Per ogni Funzione Aziendale prevista dalle Procedure predisposte per rispondere ai vari Punti di Controllo è necessario definire i nominativi dei responsabili.

Nella visualizzazione in griglia viene indicato il numero di Procedure assegnate alla Funzione ed è possibile ordinare le Funzioni Aziendali in base al responsabile o selezionare solo quelle assegnate ad un Responsabile.

Dai dettagli è possibile visualizzare (ed eventualmente modificare) le Procedure assegnate alla Funzione. È inoltre possibile richiederne una stampa.

[Nuovo](#)

Se nell'Azienda sono presenti altre Funzioni queste potranno essere generate liberamente dall'utente. Dovranno quindi essere definite le Procedure nelle quali è coinvolta la nuova Funzione.

Funzioni Multiple

Alcune Funzioni sono "multiple" cioè ricoperte da un numero di persone variabili e non definibili al momento dell'approvazione del MOG (es. Capocommissa). In questo caso è possibile indicare Responsabili "generici" quali, ad esempio, "Capocommissa per le Commesse di competenza". Sarà quindi necessario inserire nelle lettere di incarico / procure che già vengono predisposte all'apertura di ogni nuova Commessa le eventuali responsabilità aggiuntive previste dal Modello.

Sarà responsabilità dell'Organismo di Vigilanza svolgere un numero significativo di audit fra le persone che ricoprono la stessa Funzione "multipla".

Duplica

Se nell'Azienda, a prescindere dalle figure tipicamente "multiple", alcune Figure sono sdoppiate (ad esempio è possibile che in una Azienda vi siano due Responsabili Commerciali per lo studio delle Gare uno per quelle Pubbliche ed uno per quelle Private o due Responsabili Acquisti uno per i Materiali ed uno per i Macchinari) è possibile DUPLICARE una funzione. In questo caso, a differenza di quanto avviene con il Pulsante "Nuovo", alla nuova funzione verranno assegnate le stesse procedure previste per quella di partenza. Sarà necessario specificare l'area di competenza delle 2 figure (es. Pubblico e Privato / Materiali e Macchinari) e i rispettivi nominativi.

Le Procedure duplicate automaticamente dal Programma potranno poi essere modificate per rispecchiare le effettive modalità operative in uso nelle due aree di competenza.

Elimina

Non sarà possibile eliminare una Figura Aziendale a meno che prima non si siano riassegnate tutte le Procedura ad essa assegnate in precedenza ad altra Figura Aziendale (vedi avanti Modifica Procedure).

In generale si sconsiglia di eliminare le Funzioni Aziendali proposte. Si ricorda, infatti, che è possibile assegnare più Funzioni Aziendali allo stesso nominativo. Questo permette, in caso di crescita dell'azienda o di modifiche organizzative di modificare semplicemente il nome associato alla Funzione Aziendale senza dover modificare tutte le Procedure relative.

Punti di controllo

Per ogni Punto di controllo previsto in fase di progettazione è possibile definire se attualmente NON SIGNIFICATIVO ed in caso indicarne le motivazioni.

Per evitare modifiche indesiderate da questa funzione non è possibile modificare il Punto di Controllo (per la modifica si veda avanti "Punti di controllo Aziendali" nel Capitolo "MOG").

È quindi possibile definire/modificare le Procedure previste per rispondere al Punto di controllo indicando, per ognuna, il Responsabile, come effettuare la Registrazione e con quale Tempistica (la definizione di COME, CHI, DOVE e QUANDO costituisce una procedura formalizzata).

Ogni Procedura è caratterizzata dai campi:

- Codice
- Responsabile (da scegliere fra quelli definiti fra le Funzioni Aziendali)
- Tipo Procedure (Protocollo, Modalità di gestione delle risorse finanziarie, Informativa per l'OdV, Divieto, ecc.).
- Cosa (dettagli dell'attività prevista)
- Registrazione (indicazione di come si ha evidenza dell'attività svolta)
- Quando (indica la tempistica entro la quale l'attività deve essere svolta)
- Note (se necessarie)

Le “micro-procedure” predisposte per rispondere allo specifico Punto di Controllo potranno fare riferimento alle procedure aziendali già presenti ad esempio per il Sistema Qualità quando queste già coprono gli aspetti analizzati dal Punto di controllo.

Funzione addetta al controllo dell'applicazione della Procedura

Nota: La corretta applicazione di ogni Procedura del Modello deve essere controllata per verificare la corretta attuazione del Modello stesso. Non tutte le Procedure debbono però essere controllata direttamente dall'OdV che, in molti casi, può limitarsi ad effettuare un controllo di secondo livello rispetto ai controlli effettuati sulla Procedura ad esempio dal Responsabile Qualità o dal RSPP.

Per ogni procedura è possibile definire, ove presente, la Funzione preposta al controllo.

È opportuno, in questi casi, definire il tipo di controllo previsto (Audit documentale, Visita in Cantiere, Ispezione non programmata, ecc.), la periodicità prevista (espressa in mesi) e il campione di evidenze ritenuto adeguato (es. “1 Contratto di fornitura, 1 Contratto di Consulenza e almeno 2 Contratti con subappaltatori”, “Il 10% delle gare alle quali si è partecipato nel periodo”, ecc.).

Scostamento rispetto alla situazione attuale

Nota: Le varie Procedure previste nel Modello, per quanto possibile, utilizzano già quelle adottate per i Sistemi di Gestione (Qualità, Sicurezza, Ambiente, ecc.).

Per avere una indicazione sulla situazione attuale è possibile definire le caratteristiche di ogni Procedura:

- Nuova Procedura
- Prassi aziendale
- Prassi consolidata
- Procedura già formalizzata
- Procedura del Sistema di Gestione
- Procedura consolidata del Sistema

Per ogni procedura è possibile definire lo scostamento rispetto alla situazione ottimale: Procedura già consolidata e parte integrante di un Sistema di Gestione.

Dettaglio delle prassi adottate ed Allegati

Nota: Come indicato a pag. 63 del Codice di Comportamento ANCE (nella versione ritenuta idonea “al raggiungimento dello scopo fissato all’art. 6 comma 3 del D.Lgs. 231/01” – esimente - dal Ministero della Giustizia nel dicembre 2013) “L’individuazione per la specifica realtà organizzativa dei parametri CHI [il responsabile dell’attuazione per lo specifico protocollo] / COSA [la regola da seguire per applicare il protocollo] / COME [le modalità di registrazione del controllo effettuato] / QUANDO [la fase temporale del controllo] costituisce la procedura (istruzione operativa) per l’attuazione di quanto previsto dallo specifico protocollo”.

Le Aziende che lo desiderano possono comunque dettagliare meglio la singola Procedura.

Per ogni Procedura è possibile aggiungere la descrizione di dettaglio della prassi aziendale ed eventuali Allegati (es. Modelli utilizzati, Istruzioni specifiche, ecc.).

Fra gli Allegati è possibile inserire una descrizione in Word della prassi aziendale che potrà essere stampata – vedi stampe personalizzate – di seguito alle procedure sintetiche (CHI, COME, DOVE e QUANDO).

Altre Procedure

È possibile richiedere che vengono proposte, oltre alle Procedure previste per l'Azienda, anche altre Procedure previste per lo specifico Punto di controllo da SQuadra231 o eventuali Procedure definite in precedenza dall'Azienda.

Possono essere modificate solo le Procedure Aziendali attuali.

Le precedenti Procedure definite dall'Azienda o le altre Procedure previste da SQuadra231 possono diventare Procedure Aziendali attuali utilizzando il bottone “Duplica”.

Correlazioni

Nota: Ogni Punto di controllo nasce per limitare la possibilità di commettere determinati Reati.

Nel Codice di Comportamento ANCE viene riportata una valutazione, sempre per una impresa di costruzioni standard, della correlazione dei vari Punti di controllo con i Reati e con gli aspetti legati alla Governance aziendale ed il relativo Livello: Normale o Critico.

Per gli altri Punti di Controllo vengono definite le correlazioni con i vari Reati.

Per le Procedure proposte da SQuadra231 o nuove viene duplicata, in automatico, la stessa correlazione prevista per il Punto di controllo.

Ogni impresa può modificare la valutazione della correlazione in funzione delle proprie specifiche caratteristiche anche in relazione all'eventuale variazione del Livello di Rischio definito per i vari Reati.

Ad esempio un Punto di controllo può essere soddisfatto da due o più Procedure ognuna delle quali può essere correlata solo ad alcuni dei Reati/Governance ai quali è correlato il Punto di controllo.

Sotto ogni Punto di Controllo vengono presentati i Reati correlati. Per evitare modifiche indesiderate queste correlazioni non possono essere modificate da questa funzione (per la modifica delle correlazioni si veda avanti “Punti di controllo Aziendali”).

Il bottone “Visualizza Correlazioni” mostra graficamente una sintesi della Correlazione prevista dalle Linee Guida e quella assegnata alle varie Procedure previste aziendalmente per assicurare che l’insieme delle Procedure previste per un Punto di controllo sia correttamente correlato ai Reati.

Entrando in ogni Procedura sarà possibile modificare le Correlazioni relative (che vengono presentate sotto la singola Procedura).

Procedure

In questa maschera vengono presentate direttamente tutte le Procedure della versione attuale dell’Azienda. In questo caso non verranno quindi visualizzati i Punti di controllo per i quali non è prevista nessuna Procedura.

Nei dettagli viene indicato il Punto di controllo (ovviamente non modificabile) al quale si riferiscono.

Nella visualizzazione in Griglia è possibile ordinare e selezionare per Funzione Aziendale o per Responsabile.

1.2.3.2 Documenti

MOG-Parte Speciale

La Parte Speciale del MOG viene prodotta in formato WORD ma è opportuno non apportare le modifiche sui files così ottenuti ma apportare le modifiche sul Programma per ottenere che queste siano riportate in automatico in tutti i documenti correlati.

Oltre alla stampa della Parte Speciale ufficiale del Modello è possibile ottenere stampe correlate quali, ad esempio:

- Stampe alternative della Parte Speciale secondo diversi ordinamenti (per Reato, per Responsabile, ecc.).
- Le Nomine dei vari Responsabili.
- Stampe per la rilevazione degli Audit.
- Richieste di Informative.
- Organigramma (Responsabili con numero Procedure).
- Analisi dei Rischi (Reati con numero Procedure).
- Procedure complementari per la sicurezza.

Il Programma propone alcuni esempi di stampe che l'utente può liberamente utilizzare ma anche modificare o duplicare per apportare alcune personalizzazioni.

ATTENZIONE: non tutte le combinazioni possibili producono stampe significative. È opportuno utilizzare le stampe predefinite per i documenti ufficiali o, in caso contrario controllare attentamente il Documento prodotto dal programma.

Esiste la possibilità di ottenere, oltre ai tipi di stampe predefinite, molti formati di stampa.

È possibile definire:

- Un Codice e la Descrizione
- L'intestazione della stampa.
- L'organizzazione (Per Processo, per Reato, per Responsabile e per Responsabile Controlli).
- Quali Punti di controllo o Procedure presentare (Tutti, Solo i significativi, Solo quelli non significativi, Solo le Procedure identificate come Informative, Solo le Procedure identificate come Divieti, Solo le Procedure identificate come Protocolli e Modalità di gestione delle risorse finanziarie significativi, Solo i Punti correlati alla Sicurezza, Solo i Punti collegati alla sicurezza fuori dal Processo specifico per la Sicurezza, Solo i Punti del Processo Sicurezza).
- Il tipo di presentazione per i Reati correlati (è possibile escluderli dalla stampa o presentarli in base alla correlazione con il Punto di controllo e/o con le singole Procedure – si veda avanti in MOG). Verranno presentate solo le correlazioni con i Reati significativi per l'Ente (Livello di Rischio aziendale non nullo). Per le aziende che hanno realizzato il MOG partendo dalle interviste è possibile ottenere anche la stampa dei Pericoli a fronte dei quali è stato predisposto il Punto di Controllo.
- È possibile decidere se stampare solo le Procedure, solo i Punti di controllo o tutti e due.
- Per gli utenti che utilizzano SQuadra231 per gestire anche i Sistemi di Gestione è possibile scegliere di tenere separati i due sistemi (solo 231 o solo Sistemi di Gestione) o integrare i due sistemi con la stampa, in contemporanea, di entrambi. Per chi utilizza SQuadra231 anche per gestire i punti di controllo previsti da ANAC è possibile scegliere se stampare solo i Punti ANAC o tutti.
- Se stampare le Note interne (in genere non vengono inserite nei documenti ufficiali).
- È possibile richiedere la stampa di elementi aggiuntivi:
 - La Check-list per gli Audit o per l'autovalutazione sul rispetto del Modello che verranno proposte sotto ogni Procedura.
 - Gli Obblighi 231 che verranno proposti alla fine delle Nomine (la stampa verrà, in questo caso, comunque organizzata per Responsabile o per Controllore). Nelle Nomine è possibile evidenziare quali sono i Punti Critici (richiamati dal Sistema Disciplinare). In genere vengono stampati, in fondo ad ogni nomina, gli obblighi di comunicazione di criticità nei rapporti con la PA. Se questo aspetto è correttamente gestito nel Modello con appositi Punti di Controllo questa parte è inutile e può non essere stampata.
 - Note per vari tipi di informative. I documenti sono predisposti per essere forniti in formato cartaceo (con gli spazi per la compilazione) o per essere modificati direttamente in formato digitale tramite Word.
 - L'Organigramma indica, per ogni Responsabile, quali Funzioni aziendali ricopre, in quali Processi è coinvolto e per quante procedure suddivise per tipo.
 - L'Analisi dei Rischi mostra, per ogni Processo, le Attività previste e gli Illeciti231 correlati.
- Se presentare il nominativo del Responsabile accanto alla Funzione Aziendale (più chiaro per le piccole organizzazioni ma inopportuno per organizzazioni con grosso turnover).
- Può essere richiesta la stampa dell'eventuale Organismo di Controllo definito per ogni Procedura.
- Se presentare o meno le firme finali (da inserire per i Documenti ufficiali).

- Se si desidera avere, all'inizio della stampa della Parte Speciale, una LEGENDA che illustra le informazioni presenti nella stampa.
- Normalmente accanto al titolo dei vari Punti viene indicata l'origine (ANCE, Confindustria, Aziendale, ecc.) ma è possibile evitarne la stampa.
- Se, oltre agli elementi essenziali delle procedure (CHI, COSA, DOVE e QUANDO), sono state inserite alcune descrizioni dettagliate in formato Word delle prassi aziendali, è possibile richiederne la stampa di seguito alle procedure relative.
- È possibile richiedere una stampa estesa nella quale vengono esplicitati i Reati correlati e, per stampe per Responsabili nei quali è stata richiesta la Legenda, vengono fornite le indicazioni che esplicitano, per ogni Procedura, il significato dei vari campi.
- È possibile "filtrare" le Procedure di interesse in base al contenuto dei vari campi (Cosa, Registrazione, Quanto e Controllo). In questo modo è possibile, ad esempio, ottenere una stampa delle sole procedure che prevedono la Registrazione in un dato documento.

MOG-Altri Documenti

È possibile ottenere delle stampe di documenti d'esempio (MOG Parte Generale e Codice Etico) ed Altre stampa (Questionario [solo per gli associati ANCE]).

Codice Etico "dinamico": Testi

Il Codice Etico è un documento orientato a tutti gli stakeholder dell'azienda.

Esso indica il comportamento al quale devono attenersi i Dipendenti ed i Collaboratori dell'Ente (d'ora in poi "PERSONALE") ma anche tutti coloro che operano per conto dell'Ente (d'ora in poi "FORNITORI").

Può essere utile anche per far sapere a tutti gli stakeholder (quindi ancora una volta il PERSONALE e i FORNITORI ma anche i Clienti, la Pubblica Amministrazione e più in generale tutta la Collettività) cosa attendersi nei loro rapporti con l'Ente.

Vengono forniti dei testi, modificabili, per la costruzione di un Codice Etico "dinamico" che consente vari tipi di stampe orientate ai vari interessati.

Nei Testi deve essere rispettata la codifica ed in particolare è necessario utilizzare i seguenti primi caratteri per i Codici:

- "1": Per tutte le descrizioni delle Mappe di Lettura.
- "2": Per tutte le descrizioni del Questionario.
- "G": Per i Principi Generali.

Ogni Testo è caratterizzato da:

- Un Codice.
- Descrizione.
- Il testo che verrà stampato. Nel testo è possibile inserire i seguenti testi "speciali":
 - "[azienda)": Verrà sostituito con il nome dell'azienda.
 - "[Tab)": Verrà sostituito con il simbolo della tabulazione.
- Il numero del colore con il quale apparirà nella griglia.
- Lo stile con il quale verrà stampato nel documento. Uno stile particolare è "InizioSezione" che permette, appunto, di inserire una separazione di sezione.
- La tipologia per i testi particolari. Sono previste le seguenti tipologie:
 - Capitolo: per i testi sotto ai quali si desidera la presentazione della Legenda. Vengono differenziati i Capitoli che si desidera appaiano come elementi del Questionario. È possibile definire il "Capitolo introduttivo generico" e quello specifico per i fornitori.
 - Dettaglio: per i testi che verranno stampati solo quando vengono chiesti anche i Dettagli.

- Illustrazione Legenda: per i testi che descrivono la Legenda (verranno presentati solo se è richiesta la stampa della Legenda).
- Elementi del Questionario: il testo verrà sostituito dal programma con la tabella contenente tutti i Capitoli identificati come elementi del Questionario (vedi sopra).
- Inserimento Questionario: Il testo verrà sostituito con il Questionario.
- Modalità di lettura: Illustrano le modalità di lettura (verranno presentate solo quando sono presenti stampe "Suddivise")
- Mappe: per i testi che presentano i vari tipi di mappe.

Per i testi "Capitolo" è necessario indicare chi sono gli interessati:

- Il PERSONALE per sapere come comportarsi.
 - Quando il comportamento non è rivolto a tutto il personale è necessario indicare la funzione specifica.
- Il PERSONALE per sapere cosa attendersi dall'Ente.
- Il personale dei FORNITORI per sapere come devono comportarsi.
 - Quando il comportamento non è rivolto a tutto il personale è necessario indicare la funzione specifica.
- Il FORNITORE per sapere cosa attendersi dall'Ente.
- I CLIENTI per sapere cosa attendersi dall'Ente.
- La Pubblica Amministrazione per sapere cosa attendersi dall'Ente.
- La Collettività per sapere cosa attendersi dall'Ente.

I testi "Capitolo" senza nessuna indicazione specifica verranno presentati sempre.

Il Codice serve per collegare al Testo "padre", per il quale sono definiti gli interessati, tutti i Testi "figli" caratterizzati da un codice che inizia come il codice del "padre" (es. "C01" = Padre; "C01a", "C01b", ... = Figli).

Nella griglia vengono indicati i testi Modificati (Testo attuale diverso da quello proposto originariamente) e quelli non aggiornati (Testo proposto originariamente diverso da quello che verrebbe proposto attualmente).

Nei dettagli è possibile verificare il testo proposto in origine e quello che verrebbe fornito attualmente.

Codice Etico "dinamico": Stampe

Vengono proposte alcune possibili stampe.

L'utente può modificarle o aggiungerne di nuove, eventualmente partendo dalla duplicazione di una di quelle proposte.

Ogni stampa è caratterizzata da:

- Un Codice ed una Descrizione.
- L'intestazione che apparirà nella stampa.
- Il tipo di presentazione:
 - Presentazione di Base: (in genere per il Codice Etico Ufficiale) con tutti gli elementi a prescindere dall'interessato.
 - Suddiviso per Destinatario: produce tanti documenti, uno per ogni Interessato.

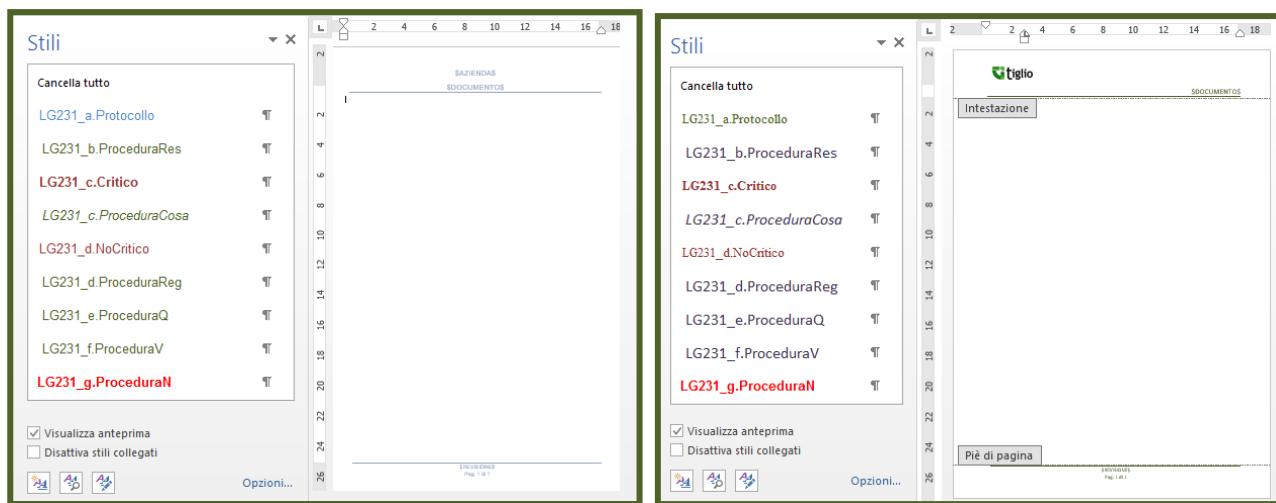
- Base + Suddiviso: dopo il documento di base vengono presentati i vari documenti per i vari interessati (permette una presentazione in cui ognuno può scegliere la modalità di lettura).
- Prescrizioni per i Fornitori: Presenta l'estratto con gli obblighi per i fornitori e richiede l'adesione.
- Se si desidera la stampa della legenda.
- Se si desidera la stampa dei Dettagli.
- Se si desidera la stampa dei Codici (per stampe interne finalizzate alla modifica del documento).

Modelli Aziendali

Tutti i Documenti vengono prodotti in formato WORD utilizzando degli stili predefiniti.

Ogni Azienda può sostituire i Files usati per i formati di base da SQuadra231 con Files che contengano i propri formati di base.

È possibile modificare l'intestazione e il fine pagina e tutti gli stili (font, colore, dimensione, paragrafo, ecc.) per adattarsi allo standard dell'Azienda.



MOG Parte Speciale (Nominativo con Reati)**P.01-Governance**

I protocolli relativi al processo di governance sono in realtà principi generali di buona organizzazione derivati dai "compliance programs" utilizzati negli Stati Uniti e richiamati dalla relazione di accompagnamento del DLgs 231/2001.

In quanto principi generali, questi protocolli non si trasformano direttamente in procedure, ma sono l'origine di più specifici protocolli orientati alla prevenzione dei reati e proposti all'interno dei rimanenti processi aziendali; l'insieme delle procedure emesse a fronte di questi ultimi protocolli costituisce evidenza anche del rispetto dei protocolli/principi generali relativi al processo di governance.

P.02-Processo di approvvigionamento**Attività - P02.A01-Valutazione e qualificazione dei fornitori****Cod: P02.01 - Sistema di qualificazione dei fornitori [ANCE]**

Il vertice aziendale decide le modalità per la valutazione e qualificazione dei fornitori, che può essere effettuata predisponendo uno specifico Albo Fornitori Qualificati, ovvero effettuata di volta in volta al momento della richiesta di offerta al fornitore, e comunque prima della stipula di ciascun ordine/contratto di fornitura

01.01-Mansioni e responsabilità
01.03-Procedure

Responsabile: 02.01-a: Resp.: XXX (Amministratore Unico) Funz.: Amministratore Unico
Decidere con attenzione le modalità per la valutazione e qualificazione dei fornitori, che può essere effettuata predisponendo uno specifico Albo Fornitori Qualificati, ovvero effettuata di volta in volta al momento della richiesta di offerta al fornitore, e comunque prima della stipula di ciascun ordine/contratto di fornitura.

Registrazione: Procedura di qualifica dei fornitori

Quando: Revisione annuale della procedura

Cod: P02.02 - Dichiarazione di operare secondo comportamenti etici [ANCE]

La funzione proposta alla valutazione e qualificazione dei fornitori decide l'inserimento del fornitore nell'Albo Fornitori Qualificati, ovvero il suo utilizzo, accertando che lo stesso dichiari di operare nel rispetto di tutte le leggi e norme applicabili e secondo comportamenti etici.

La funzione proposta alla valutazione e qualificazione dei fornitori in ogni caso non qualifica soggetti imprenditoriali la cui reputazione in termini di legalità è dubbia sulla base di informazioni disponibili all'impresa.

CRITICO 01.04-Codice etico
CRITICO Art. 24-03-Criminalità organizzata

Responsabile: 02.02-a: Resp.: XXX (Resp. Acquisti) Funz.: Resp. Acquisti

Valutare le informazioni fornite dal fornitore di operare secondo principi etici.

Registrazione: Sigla sulla Richiesta d'Offerta.

Quando: Prima dell'Invio della Richiesta d'Offerta.

0.a: Prima versione preliminare
Pag. 1 di 67

MOG Parte Speciale (Nominativo con Reati)**P.01-Governance**

I protocolli relativi al processo di governance sono in realtà principi generali di buona organizzazione derivati dai "compliance programs" utilizzati negli Stati Uniti e richiamati dalla relazione di accompagnamento del DLgs 231/2001.

In quanto principi generali, questi protocolli non si trasformano direttamente in procedure, ma sono l'origine di più specifici protocolli orientati alla prevenzione dei reati e proposti all'interno dei rimanenti processi aziendali; l'insieme delle procedure emesse a fronte di questi ultimi protocolli costituisce evidenza anche del rispetto dei protocolli/principi generali relativi al processo di governance.

P.02-Processo di approvvigionamento**Attività - P02.A01-Valutazione e qualificazione dei fornitori****Cod: P02.01 - Sistema di qualificazione dei fornitori [ANCE]**

Il vertice aziendale decide le modalità per la valutazione e qualificazione dei fornitori, che può essere effettuata predisponendo uno specifico Albo Fornitori Qualificati, ovvero effettuata di volta in volta al momento della richiesta di offerta al fornitore, e comunque prima della stipula di ciascun ordine/contratto di fornitura

01.01-Mansioni e responsabilità
01.03-Procedure

Responsabile: 02.01-a: Resp.: XXX (Amministratore Unico) Funz.: Amministratore Unico
Decidere con attenzione le modalità per la valutazione e qualificazione dei fornitori, che può essere effettuata predisponendo uno specifico Albo Fornitori Qualificati, ovvero effettuata di volta in volta al momento della richiesta di offerta al fornitore, e comunque prima della stipula di ciascun ordine/contratto di fornitura.

Registrazione: Procedura di qualifica dei fornitori

Quando: Revisione annuale della procedura

Cod: P02.02 - Dichiarazione di operare secondo comportamenti etici [ANCE]

La funzione proposta alla valutazione e qualificazione dei fornitori decide l'inserimento del fornitore nell'Albo Fornitori Qualificati, ovvero il suo utilizzo, accertando che lo stesso dichiari di operare nel rispetto di tutte le leggi e norme applicabili e secondo comportamenti etici.

La funzione proposta alla valutazione e qualificazione dei fornitori in ogni caso non qualifica soggetti imprenditoriali la cui reputazione in termini di legalità è dubbia sulla base di informazioni disponibili all'impresa.

CRITICO 01.04-Codice etico

CRITICO Art. 24-03-Criminalità organizzata

Responsabile: 02.02-a: Resp.: XXX (Resp. Acquisti) Funz.: Resp. Acquisti

Valutare le informazioni fornite dal fornitore di operare secondo principi etici.

Registrazione: Sigla sulla Richiesta d'Offerta.

0.a: Prima versione preliminare
Pag. 1 di 75

Le nuove stampe utilizzeranno i formati aziendali.

Oltre agli Stili è possibile personalizzare l'Intestazione e la Terminazione di Pagina utilizzando le normali funzionalità di Word ad esempio inserendo i loghi aziendali.

ATTENZIONE: Il programma utilizza alcuni segnalibri di word che, se presenti, verranno compilati da SQuadra231. È opportuno controllare i segnalibri presenti nel File di base proposto (con le funzionalità di Word: Inserisci/Collegamenti/Segnalibri) e quindi verificare i Segnalibri sul documento modificato. In particolare, se si inserisce il Logo aziendale è opportuno eliminare il Segnalibro "Azienda".

Sono presenti varie tipologie di documenti che avranno effetto sulle varie stampe. Per ogni tipologia è possibile richiedere il Modello Base, modificarlo in locale e quindi memorizzarlo su SQuadra231.

ATTENZIONE: a seguito di nuove funzionalità del programma potrebbero essere introdotti nuovi stili nei documenti di base. In questo caso le stampe che utilizzano i nuovi stili, non trovando questi nei documenti personalizzati e salvati in precedente, segnaleranno un errore.

In questo caso è necessario aggiungere manualmente i nuovi stili (il cui nome è segnalato nell'errore) al modello personalizzato (eventualmente prendendo spunto dalla nuova versione del Modello Base).

1.2.4 Attività per la gestione del MOG e dell'Organismo di Vigilanza [MOG]

1.2.4.1 Gestione del MOG in modifica

L'utilizzo di questo insieme di funzioni è rivolto alla miglior definizione della Parte Speciale del Modello di Organizzazione e Gestione della Azienda.

Adeguatezza del Modello in modifica

Mentre molte Linee Guida, come ad esempio quelle di Confindustria, sono organizzate per Reato, il MOG proposto da ANCE è organizzato per Processi per renderne facile l'integrazione con gli altri Sistemi di Gestione (Qualità, Sicurezza, Ambiente, Privacy, ecc.) e l'applicazione da parte dei vari Responsabili.

Questa organizzazione, ripresa anche da SQuadra231, rende meno immediata l'attività di controllo della adeguatezza del Modello rispetto alla funzione di prevenire la commissione dei singoli Reati che deve essere effettuata attraverso l'analisi della correlazione fra Procedure Aziendali e Reati.

Grazie alla definizione della Correlazione fra Procedure e Reati è però possibile analizzare il Modello "per Reato".

Nota: Nel modulo per la gestione dei Verbali dell'OdV (vedi avanti) viene presentata una bozza di analisi dell'adeguatezza del Modello.

Correlazione Procedure - Reati

È possibile modificare la correlazione relativa ad ogni Procedura (vedi nella sezione Personalizza). Con questa funzione è possibile modificare le correlazioni di tutte le Procedure (ad esempio analizzare tutte le correlazioni definite con un determinato Reato).

Prospetto Correlazioni

Un prospetto riepilogativo indica, per ogni aspetto della Governance, la correlazione prevista da ANCE per i Punti di controllo ritenuti significativi e la correlazione prevista dall'azienda per le Procedure predisposte. Per tutti gli aspetti legati alla Governance viene indicata la variazione percentuale media.

Sempre nello stesso prospetto viene indicato, per ogni Reato, un valore numerico in relazione alla Gravità prevista dal Legislatore, il Rischio Lordo previsto da ANCE per una azienda standard e quello definito dall'Azienda in base alla propria valutazione.

Sempre per ogni Reato viene quindi indicata, come per i vari aspetti della Governance, la correlazione prevista da ANCE per i Punti di controllo ritenuti significativi e la correlazione prevista dall'azienda per le Procedure predisposte. Viene quindi indicata l'aumento in percentuale.

Viene quindi indicato per tutti i Reati la percentuale media e l'incremento della correlazione "pesata" rispetto al Rischio Lordo aziendale (è infatti importante aumentare la correlazione soprattutto per i reati con Rischio Lordo maggiore).

Errori

Nel Prospetto è presente un foglio dove vengono riportati eventuali errori:

- Procedure senza Correlazione con nessun Reato o elemento di Governance.
- Procedure in cui è ripetuta la Correlazione con lo stesso Reato.

Correlazione Punti di Controllo e Procedure

Un ultimo foglio del Prospetto riporta eventuali reati correlati al Punto ma non alla Procedura. Se per il Punto di Controllo sono state previste più Procedure non è necessario che tutte "coprano" tutti i Reati ma è necessario che li "coprano" nel loro insieme.

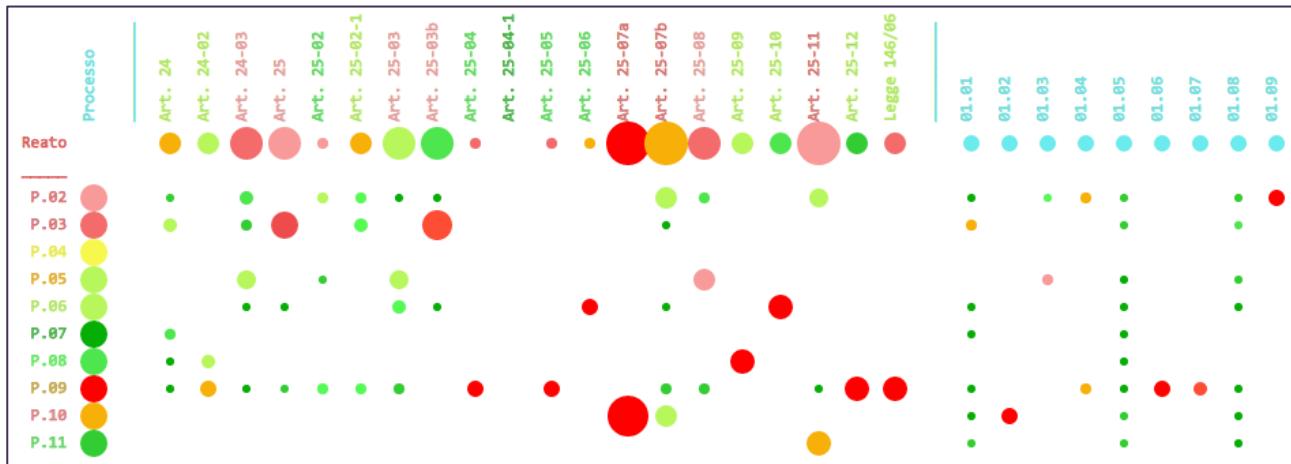
Variazioni delle Correlazioni

Un prospetto evidenzia le variazioni di Correlazioni fra il Modello attualmente approvato (se esistente) e la versione in modifica.

Questo foglio consente una verifica delle modifiche prima dell'approvazione di una nuova versione.

Analisi Correlazioni

Vista la quantità di elementi da analizzare sono state predisposte delle rappresentazioni grafiche che hanno lo scopo di fornire una visione d'insieme.



Una prima rappresentazione permette di visualizzare la correlazione fra i Reati e gli aspetti di Governance con i vari Processi.

Nella prima riga vengono riportate informazioni relative ai Reati. La dimensione dei cerchi indica il Livello di Rischio aziendale mentre il colore indica la Gravità per il Legislatore (Verde = bassa, Rosso = alta). Ad esempio il comma 1 dell'articolo 25-07 relativo alla sicurezza ha pene molto superiori rispetto ai commi 2 e 3 dello stesso articolo ma il Livello di Rischio aziendale è comunque Alto in relazione alla diversa probabilità di accadimento.

Vengono poi presentati gli aspetti della Governance aziendale.

Nelle altre righe vengono presentati i vari Processi.

Nella prima colonna viene riportato il ruolo complessivo assegnato dal Modello al Processo (Verde=Basso, Rosso=Alto e Giallo = Non previsto).

Gli altri elementi indicano la correlazione fra Reato e Processo. Il raggio indica il Livello di Rischio mentre il colore indica la distribuzione percentuale (la somma per reato sarà sempre 100%) nel contrasto allo specifico reato (verde = bassa, rosso = alta).

Portando il mouse su ogni elemento il sistema indica le informazioni di dettaglio relative.

In particolare viene riportata la percentuale di controllo del reato e la Quota di Rischio (Livello di Rischio per percentuale).

Ordinamento

Oltre al primo ordinamento nel quale i Reati ed i Processi sono ordinati per codice è possibile richiedere altre presentazioni nelle quali sia i Processi che i Reati possono essere ordinati in base al Livello di Rischio (dal più significativo al meno significativo).

Nelle rappresentazioni di sintesi, premendo con il mouse su ogni elemento viene prodotto un documento di excel con i dati di dettaglio che hanno portato ai valori di sintesi.

Altre rappresentazioni

È possibile ottenere rappresentazioni analoghe, di sempre maggior dettaglio, per Reato/Attività e per Reato/Procedura.

È possibile anche ottenere una rappresentazione analoga che mostra la correlazione fra i Reati e i vari Responsabili (anche in questo caso è possibile ottenere un foglio di excel con i dati di dettaglio).

Nota: In generale è auspicabile che la funzione di controllo del Modello per ogni Reato coinvolga il maggior numero di Processi/Attività aziendali e non sia concentrata su uno o pochi Processi/Attività.

Flussi dei controlli

Per visualizzare come vengono tenuti sotto controllo i vari Reati è stata predisposta una rappresentazione nella quale a sinistra vengono mostrati i vari Reati, al centro i Processi coinvolti e a destra i Responsabili delle varie Procedure (l'altezza del prospetto può essere modificata nella definizione dei dati aziendali relativi al metodo nell'analisi del modello approvato).

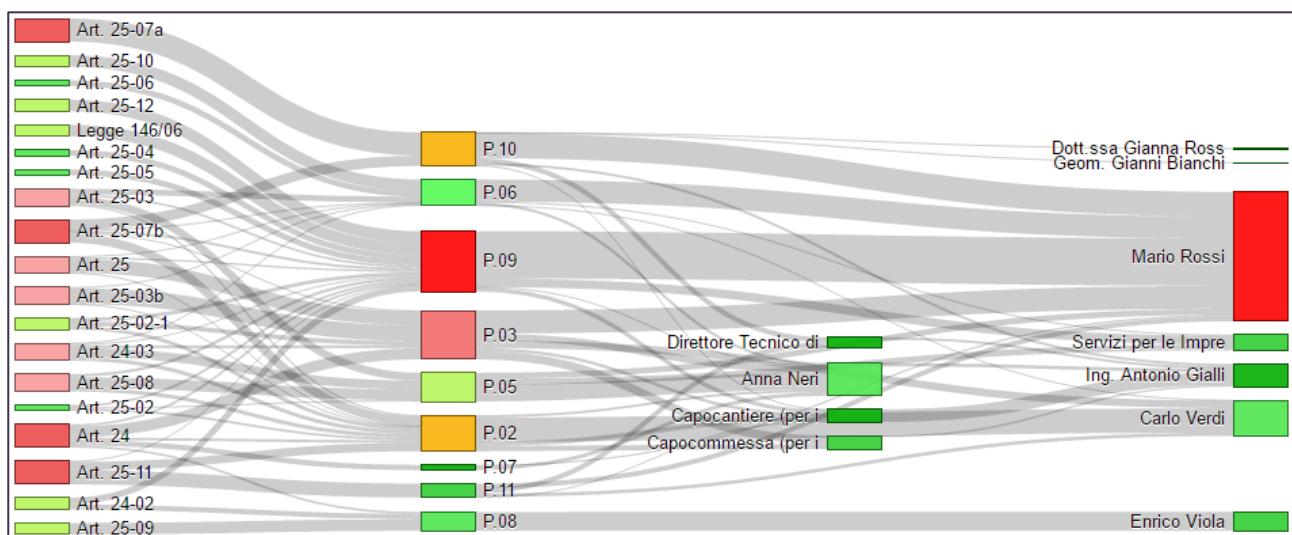
Portando il mouse su ogni elemento e sui flussi il sistema indica le informazioni di dettaglio relative. È anche possibile "spostare" gli elementi per evidenziare meglio i flussi relativi.

Per i Reati i Colori indicano il Livello di Rischio aziendale (Verde = Non Significativo / Rosso = Reato Pregresso).

Per i Processi e le Persone i Colori danno indicazioni sulla quantità di Livelli di Rischio controllato attraverso i Punti di Controllo di competenza (Rosso=Massimo / Verde=Minimo).

Sono disponibili anche analisi di maggior dettaglio in cui al posto dei Processi vengono presentate le Attività o le singole Procedure.

È possibile scegliere se vedere tutti i Reati o solo quelli che hanno un Livello di Rischio superiore al valore scelto come "Da controllare" per concentrare l'attenzione solo su quelli più significativi.



Nella Figura riportata a titolo d'esempio è possibile notare che il Reato relativo al primo comma dell'articolo sulla Sicurezza (Art. 25-07a), che riguarda gli obblighi del Datore di Lavoro, è totalmente coperto da Punti di Controllo previsti all'intero al Processo relativo alla Sicurezza (P.10).

Gli altri aspetti legati alla sicurezza (Art. 25-07b) sono coperti da Punti di Controllo che ricadono solo in parte nel Processo relativo alla Sicurezza (P.10) mentre altri sono legati al Processo relativo all'Approvvigionamento (P.02) ed alle Risorse Umane (P.09).

Gran parte di questi Processi ricadono sotto la responsabilità di Mario Rossi che, nell'esempio, ricopre, fra l'altro, il ruolo di Datore di Lavoro e di Responsabile del Personale.

Una parte di responsabilità ricadono sull'Ing. Antonio Gialli che ricopre il ruolo di RSPP ed ha anche il compito di effettuare controlli di primo livello sui Capicommissari, sui Direttori Tecnici e sui Capocantieri. Per alcuni aspetti l'RSPP controllerà anche le attività del Responsabile Amministrativo (Anna Neri).

Cerchi dei Rischi

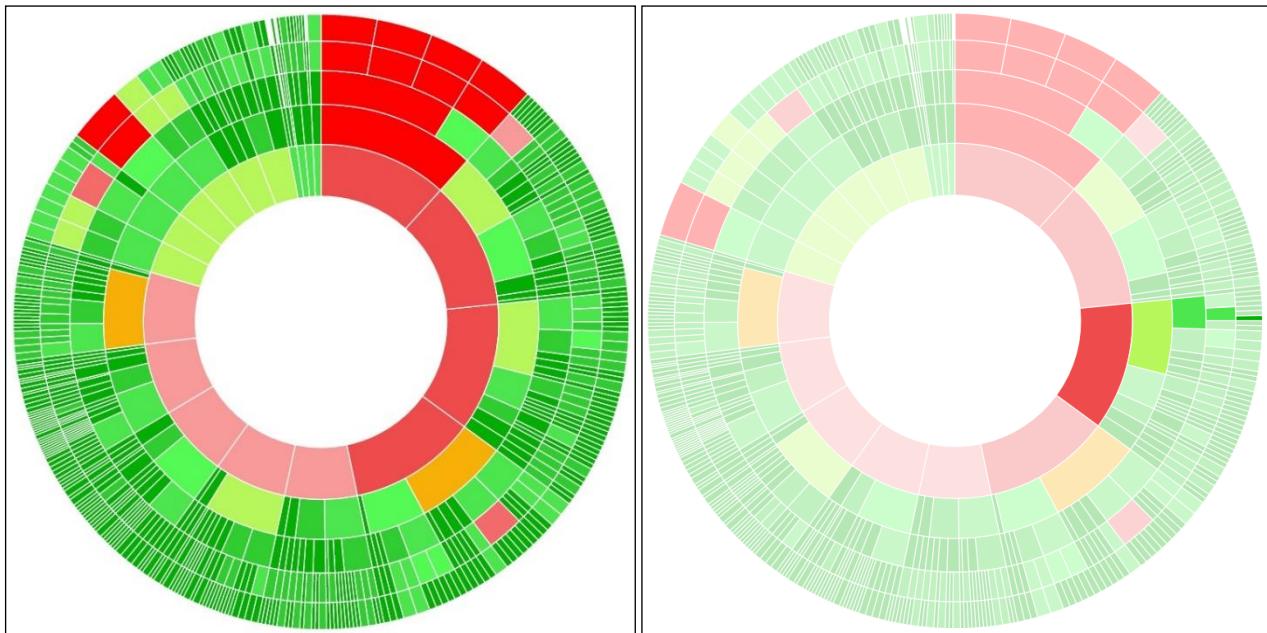
Un'ultima rappresentazione grafica permette di avere una visione di insieme sulla distribuzione delle Procedura predisposte per rispondere ai vari Punti di Controllo in relazione ai vari Reati.

In una prima rappresentazione vengono mostrati i vari Processi, le Attività, i Punti di Controllo, le Procedure e, infine, per ogni Procedura i Reati che dovrebbe prevenire.

Una seconda rappresentazione mostra i vari Reati e, per ogni Reato, i Processi, le Attività, i Punti di Controllo e, infine, le Procedure correlate al Reato stesso. Questa rappresentazione [d'ora in poi

“Per Reati”] permette anche un confronto con l’ultima versione approvata e quindi attualmente in uso.

Portando il mouse su ogni elemento il sistema indica le informazioni di dettaglio relative ed evidenzia gli “archi” sottesi.



È possibile scegliere la modalità di presentazione:

- Proporzionale al Livello di Rischio sotteso ai Punto di Controllo.
- Proporzionale al Livello di Rischio sotteso ai Punto di Controllo moltiplicato per il Livello di Rischio del Reato (per concentrare l’attenzione sui Reati più significativi).
- Proporzionale alla criticità associata ai Punti di Controllo (1=Normale, 2=Critica).
- Proporzionale alla criticità associata ai Punti di Controllo nell’ultima Versione approvata [questa funzionalità è presente solo per la rappresentazione “Per Reati”]

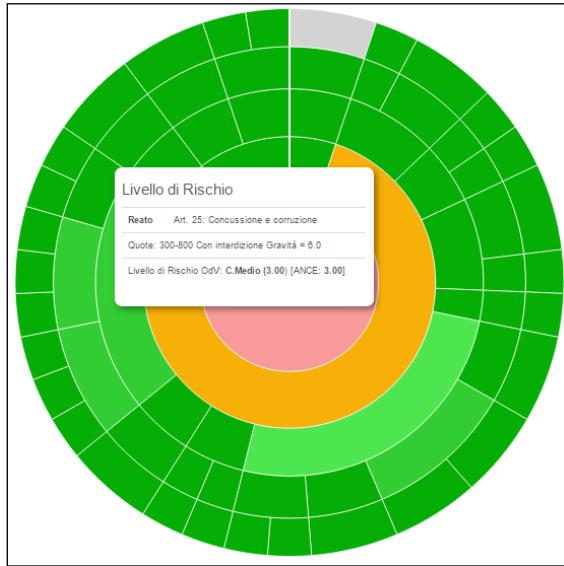
Per i Reati i Colori indicano il Livello di Rischio aziendale (Verde = Non Significativo / Rosso = Reato Pregresso).

Per gli altri elementi i Colori danno indicazioni sulla quantità di Livelli di Rischio controllato attraverso i Punti di Controllo di competenza (Rosso=Massimo / Verde=Minimo).

Nella rappresentazione “Per Reati” viene utilizzato il colore Giallo per indicare i punti in cui la correlazione è diminuita rispetto alla versione attuale ed il Grigia per indicare un aumento.

ZOOM

Facendo clik con il mouse su un qualunque elemento verrà presentato il dettaglio a partire da quell’elemento.



Sarà possibile “tornare indietro” premendo al centro del grafico.

Nota: Per quanto possibile sarebbe auspicabile che tutte le Procedure abbiano la stessa funzione di controllo rispetto a tutti i Reati (uniformità dei settori del penultimo cerchio esterno nella rappresentazione per Processo). È infatti da evitare che alcune Procedure racchiudano in se una funzione di controllo troppo elevata perché, nel qual caso, la rilevazione di una semplice non conformità potrebbe porre in discussione l’efficacia dell’attuazione del MOG. Per i Punti di Controllo più significativi è quindi opportuno, dove possibile, prevedere più di una Procedura per "suddividere" la funzione di controllo.

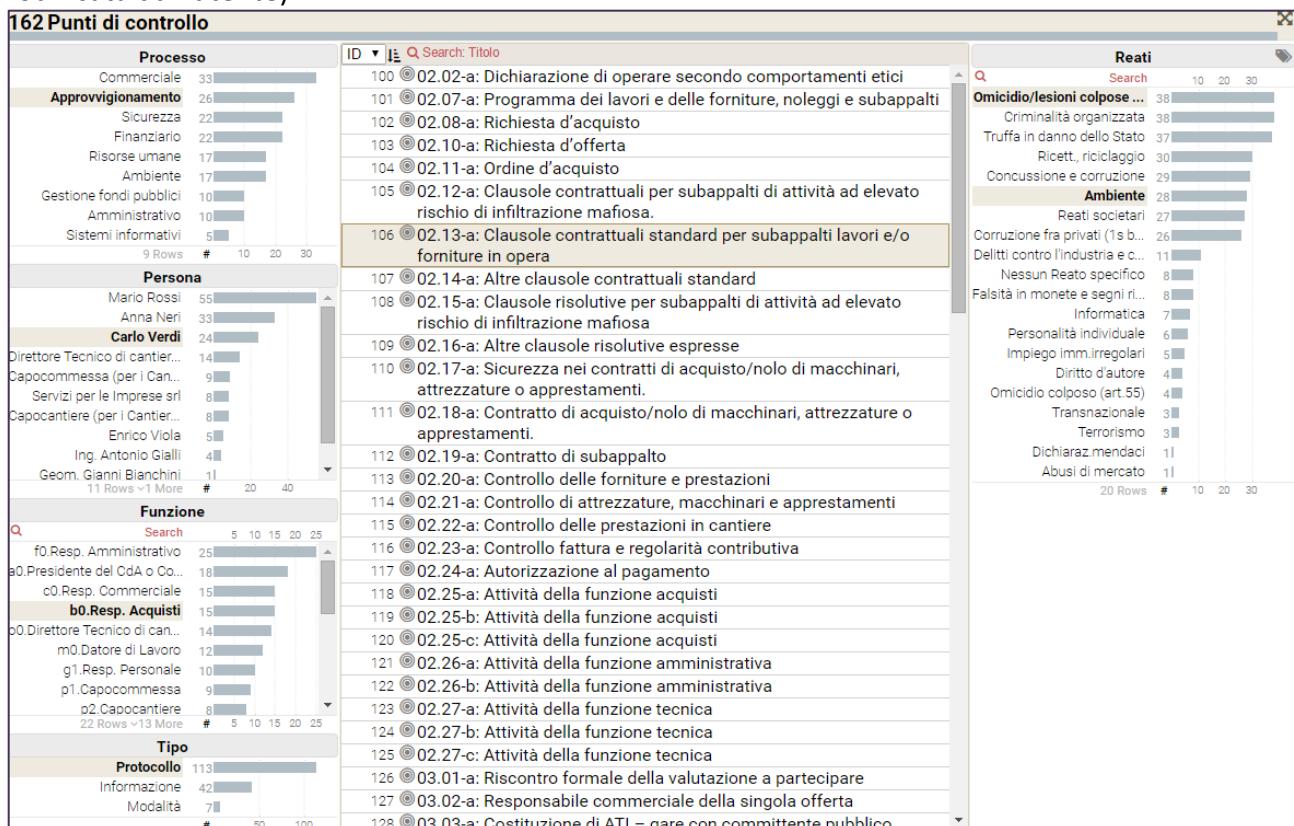
Nella presentazione per Reato è auspicabile l’omogeneità dei settori dell’ultimo cerchio esterno, per quanto possibile. Questi rappresentano, infatti, la funzione di controllo rispetto ai singoli Reati. Un livello di controllo troppo alto concentrato su una sola Procedura mette a rischio la funzione di controllo di quel Reato in caso di rilevazione di una Non Conformità nell’applicazione della Procedura.

Punti e Procedure

Cruscotto delle Correlazioni

Per avere una visione completa delle Correlazioni è stato predisposto un Cruscotto multidimensionale nel quale è possibile analizzare gli aspetti principali relativi ad ogni Procedura.

È possibile operare sul Cruscotto nel quale sono presentate al centro le singole Procedure o sul Cruscotto di sintesi (nel quale vengono presentati solo i grafici di riepilogo) che rappresenta una fotografia della situazione e che può essere facilmente copiabile come immagine per, eventualmente, inserirlo in verbali o relazioni (gli elementi presentati e la loro posizione può essere modificata dall'utente).



Per il funzionamento dei Cruscotti si rimanda alle indicazioni presenti nel capitolo relativo all'interno della Sezione "Caratteristiche generali di SQuadra".

Definizione del GAP per le singole Procedure

Per ogni Procedura è possibile definire il GAP rispetto alla situazione preesistente prima dell'introduzione della nuova versione del Modello.

Per facilitare l'operazione di definizione è stata prevista questa funzione per una più rapida assegnazione delle valutazioni.

Mappatura dei Reati

Azioni a Rischio

Il Legislatore richiede (cfr. Art.6 comma 2 lettera a) di "individuare le attività nel cui ambito possono essere commessi reati".

I dati di seguito descritti possono essere originati dalle interviste (vedi la successiva sezione: "Analisi dei Rischi / Mappatura delle attività a Rischio").

SQuadra231 permette di definire le Azioni (Attività elementari) a Rischio indicando le Famiglie di Reati potenzialmente interessate.

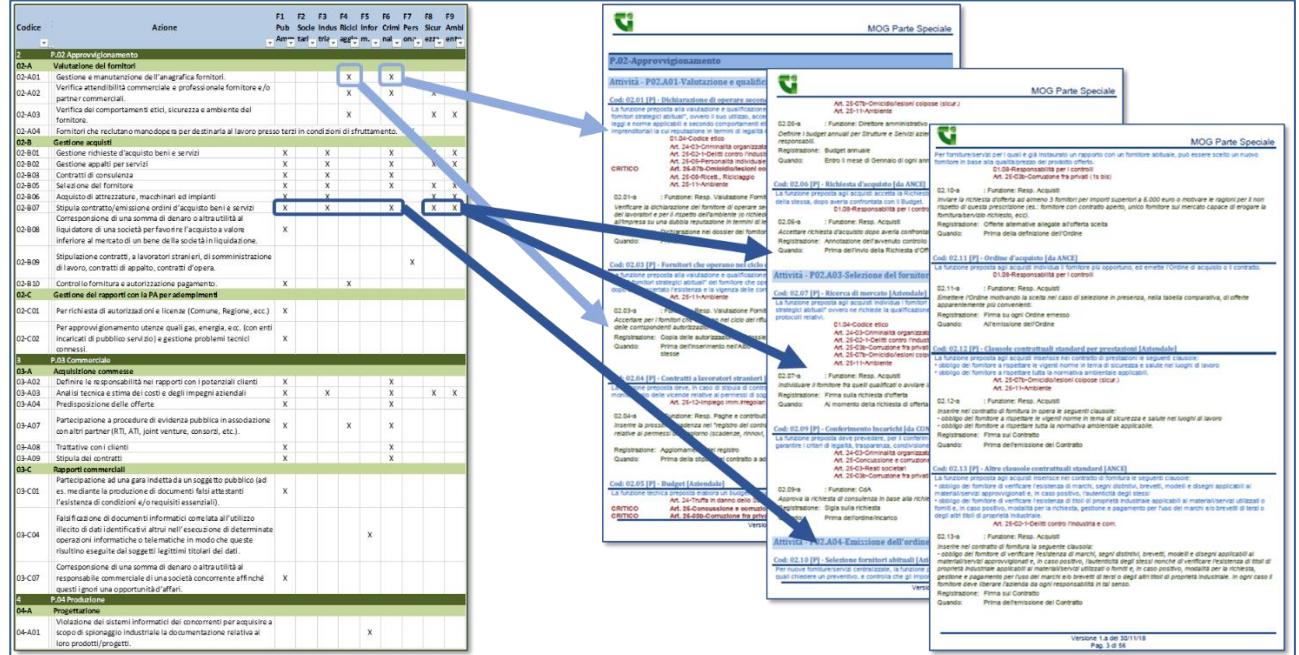
Singole Interviste										
Codice	Azione	F1	F2	F3	F4	F5	F6	F7	F8	F9
		Pub	Socie	Indus	Ricid	Infor	Crimi	Pers	Sicur	Ambi
02-A	Codice									
02-A01	Codice									
02-A02	Codice									
02-A03	Codice									
02-B	B.02 Approvvigionamento									
02-B01	Valutazione dei fornitori									
02-B02	Gestione e manutenzione dell'anagrafica fornitori.									
02-B03	Verifica dei comportamenti etici, sicurezza e ambiente del fornitore.									
02-B04	Fornitori che reduttano manodopera per destinarla al lavoro presso terzi in condizioni di sfruttamento.	X								
02-B10	Gestione acquisti									
02-C	C. Gestione dei rapporti con la PA per adempimenti									
02-C01	Per richiesta di autorizzazioni e licenze (Comune, Regione, ecc.)	X								
02-C02	D.02 Commerciale									
02-C03	Acquisizione commesse									
02-C04	Definire le responsabilità nei rapporti con i potenziali clienti	X								
02-C05	Partecipazione a procedure di evidenza pubblica in associazione con altri partner (RTI, ATI, joint venture, consorzi, etc.).	X								
02-C06	Trattative con i clienti	X								
02-C07	Stipula dei contratti	X								
02-C08	Rapporti commerciali									
02-D	Per richiesta di autorizzazioni e licenze (Comune, Regione, ecc.)	X								
02-E	E.02 Produzione									
02-E01	Progettazione									
02-E02	Violazione dei sistemi informatici dei concorrenti per acquisire a scopo di spionaggio industriale la documentazione relativa ai loro prodotti/progetti.									

Codice	Azione	F1	F2	F3	F4	F5	F6	F7	F8	F9
		Pub	Socie	Indus	Ricid	Infor	Crimi	Pers	Sicur	Ambi
02-F	P.02 Approvvigionamento									
02-F01	Valutazione dei fornitori									
02-F02	Gestione e manutenzione dell'anagrafica fornitori.									
02-F03	Verifica attendibilità commerciale e professionale fornitore e/o partner commerciali.									
02-F04	Verifica dei comportamenti etici, sicurezza e ambiente del fornitore.									
02-F05	Fornitori che reduttano manodopera per destinarla al lavoro presso terzi in condizioni di sfruttamento.									
02-G	Gestione acquisti									
02-G01	Gestione richiesta d'acquisto beni e servizi	X								
02-G02	Gestione appalti per servizi	X								
02-G03	Contratti di consulenza	X								
02-G04	Selezione del fornitore	X								
02-G05	Acquisto di attrezzature, macchinari ed impianti	X								
02-G06	Stipula contratti, accordi e impegni fra le parti	X								
02-G07	Corrispondenza di una somma di denaro o altra utilità al liquido direttore di una società per favorire l'acquisto a valore inferiore al mercato di un bene della società in liquidazione.	X								
02-G08	Stipulazione contratti, a lavoratori stranieri, di somministrazione di lavoro, contratti di appalto, contratti d'opera.									
02-G09	Controllo forniture e autorizzazione pagamento.	X								
02-H	C. Gestione dei rapporti con la PA per adempimenti									
02-H01	Per richiesta di autorizzazioni e licenze (Comune, Regione, ecc.)	X								
02-I	P.03 Commerciale									
02-I01	Acquisizione commesse									
02-I02	Definire le responsabilità nei rapporti con i potenziali clienti	X								
02-I03	Partecipazione a procedure di evidenza pubblica in associazione con altri partner (RTI, ATI, joint venture, consorzi, etc.).	X								
02-I04	Trattative con i clienti	X								
02-I05	Stipula dei contratti	X								
02-I06	Rapporti commerciali									
02-J	Per richiesta di autorizzazioni e licenze (Comune, Regione, ecc.)	X								
02-K	E.02 Produzione									
02-K01	Progettazione									
02-K02	Violazione dei sistemi informatici dei concorrenti per acquisire a scopo di spionaggio industriale la documentazione relativa ai loro prodotti/progetti.									



Azioni a Rischio / Punti di controllo

È possibile, quindi, definire quali Punti di Controllo sono stati previsti per prevenire la commissione dei reati legati alla specifica Azione.



Selezione di Azioni / Famiglie di Reato / Punti di controllo

Per facilitare la definizione dei Punti di Controllo previsti per prevenire la commissione dei Reati potenzialmente collegati ad una determinata Azione è possibile operare per selezione.

Vengono presentate tutte le Azioni a Rischio ed ogni Azione è ripetuta per le Famiglie di Reato potenzialmente interessate. Vengono evidenziate, in rosso, le Azioni/Famiglie non collegate a nessun Punto di Controllo.

Scegliendo una Azione/Famiglia vengono presentati tutti i Punti di Controllo le cui Procedure sono correlate ai Reati previsti dalla Famiglia di Reati in esame. Fra questi vengono evidenziati, in verde, quelli già collegati.

È possibile selezionare uno o più elementi per Collegarli (se non ancora collegati) o Scollegarli (qualora precedentemente collegati).

Stampe Azioni

Squadra231 presenta la correlazione Punti/Azioni per verificare che tutte le Azioni abbiano almeno un Punto di Controllo per la prevenzione delle varie Famiglie di Reati.

È possibile ottenere:

- Per ogni Azione a Rischio l'elenco di tutti i Punti di Controllo collegati.
- Per ogni Punti di Controllo l'indicazione delle Azioni a Rischio che può concorrere a controllare.

Presentazione

Vengono fornite le stesse informazioni presenti nelle stampe sotto forma di presentazione interattiva.

Grafico

Scegliendo un Reato viene presentata, per ogni Azione a Rischio, quali Punti di Controllo sono previsti per la Famiglia di Reati alla quale appartiene il Reato scelto.

I codici dei Punti di controllo vengono presentati in verde se correlati proprio al Reato scelto e non solo alla Famiglia. Sotto il Codice del Punto vengono indicati con cerchi Rossi i Punti non collegati a nessuna Azione a Rischio.

Per le Azioni a Rischio non collegate a nessun Punto di Controllo vengono indicati, in azzurro, tutti i Punti di controllo potenziali.

Punti di controllo Aziendali

NOTA: Per una impresa “standard” il numero e la tipologia dei Punti di controllo proposti nel Codice di Comportamento ANCE sono tali da ricondurre, per ciascun reato, il livello di rischio residuo a un valore da considerare accettabile. Qualora l’impresa modifichi la valutazione del Rischio Lordo o comunque in caso di caratteristiche specifiche è necessario aggiungere ai Punti di controllo ANCE ulteriori Punti di controllo specifici per l’impresa che la stessa si pone l’obiettivo di garantire.

SQuadra231 permette di aggiungere ai Punti di controllo di base ulteriori Punti di controllo specifici per l’impresa. Ovviamente per questi nuovi Punti di controllo sarà necessario indicare anche a fronte di quali Reati sono stati predisposti.

Attività Specifiche

Qualora l’impresa lo ritenga può inserire i nuovi Punti di controllo su Attività non previste dal Codice di Comportamento ANCE che dovrà inserire appositamente.

Punti di controllo ANCE

Vengono presentati i Punti di controllo presenti nel Codice di Comportamento ANCE utilizzati nel Modello. Questi punti essendo stati definiti puntualmente ed in questa forma, nel loro insieme, valutati come idonei dal Ministero non possono essere modificati dall’utente.

Se l’utente ha la necessità di modificarli dovrà creare nuovi Punti di controllo Aziendali e ritenere quelli ANCE di partenza come Non Significativi.

1.2.4.2 Gestione del MOG Approvato

L'utilizzo di questo insieme di funzioni è rivolto alla gestione della Parte Speciale del Modello di Organizzazione e Gestione della Azienda.

Versioni della Parte Speciale del MOG

Squadra231 è orientato alla predisposizione del Modello di Organizzazione ed al suo costante aggiornamento.

Quando l'Organismo dirigente decide di emettere una nuova versione è opportuno memorizzare come allegati copie dei documenti approvati e firmati³.

Il Programma provvede a salvare una copia delle Procedure della Parte Speciale del MOG. La copia, non modificabile dall'utente, verrà utilizzata per eseguire gli Audit e per lo svolgimento delle altre attività dell'OdV (controllo della validità delle Nomine, controllo del flusso informativo previsto dalle Procedure, ecc.) sulla base del modello ufficialmente emesso anche se nel frattempo si stanno apportando delle modifiche al MOG (utilizzando le scelte di Squadra sotto MANUTENZIONI) che però non sono ancora approvate e quindi non operative.

Stato delle Versioni

Le Versioni possono trovarsi nei seguenti stati:

- In modifica (l'unica versione sulla quale è possibile apportare modifiche).
- Attuale (l'ultima versione approvata dall'Organo dirigente e quindi sulla quale opera l'OdV)
- Precedente (viene utilizzata per ricavare le versioni delle singole Procedure – si veda avanti).
- Superata (archiviate solo per mantenere la storia dell'evoluzione del Modello).

È possibile apportare modifiche ed emettere solo una versione "In modifica". È anche possibile riemettere la versione "Attuale" per apportare piccole modifiche formali (ad esempio per correggere errori sintattici o refusi).

Sarà possibile riemettere la versione "Attuale" solo se non vengono apportate modifiche a Procedure già sottoposte ad Audit.

SUGGERIMENTO: Come detto il programma consente di riemettere la versione "Attuale" quando si evidenziano solo piccole modifiche formali. In generale è consigliabile emettere sempre una nuova versione quando si apportano modifiche alla Parte Speciale del Modello dopo che questa sia stata ufficialmente distribuita per evitare che siano presenti documenti differenti con lo stesso indice di Versione.

È possibile utilizzare una codifica delle Versioni su 2 livelli (es. "3.b", "3.c", "3.d", "4.a", "4.b", ecc.) in cui il primo livello (in genere un numero) indica le Revisioni significative approvate ufficialmente dall'Organo Dirigente della Società mentre il secondo livello (che, nell'esempio sopra riportato, è rappresentato da una lettera) può essere utilizzato per identificare in modo univoco Versioni emesse in autonomia dall'OdV per correggere solo errori formali o comunque riscrittura di Procedure solo per una più chiara comprensione del Modello stesso senza modifiche sostanziali.

Solo le nuove Revisioni (nell'esempio identificate con la lettera "a") richiedono di svolgere specifica attività formativa per tutto il personale mentre le modifiche apportate nelle varie Versioni all'interno della stessa Revisione ("b", "c", ecc.) saranno, dove necessario, presentate ai soli Responsabili coinvolti.

Quando si emette una versione "In modifica" il programma provvede a:

- L'eventuale versione "Precedente" viene posta nello stato di "Superata";
- L'eventuale versione "Attuale" viene posta nello stato di "Precedente";
- La versione "In modifica" viene posta nello stato "Attuale";
- Viene creata, in automatico, una nuova versione "In modifica".

³ L'Ente deve poter assicurare l'adempimento di tutti gli obblighi previsti dall'Art.80 del D.Lgs 81/08, come richiesto dai Punti di Controllo nel Processo Sicurezza, è quindi opportuno allegare anche il Manuale per la Sicurezza definito dall'Ente che descriva le specifiche modalità operative.

Dati salvati con la Versione

Vengono salvati con la Versione le seguenti informazioni:

- Le Funzioni Aziendali con Riferimento alle Persone coinvolte nel sistema.
- I Punti di Controllo.
- Le Procedure.
- La Correlazione fra i Punti di Controllo ed i vari Reati (solo per i Reati significativi cioè con Livello di Rischio Aziendale non nullo).
- La Correlazione fra le Procedure e i vari Reati (solo per i Reati significativi).
- I Livelli di Rischio individuati per i vari Reati.

Controlli da effettuare dopo l'emissione di una nuova Versione

Una volta emessa la nuova Versione è opportuno effettuare un controllo sulle modifiche rispetto alla versione precedente (vedi avanti “Controllo sull’evoluzione”) ed identificare come analoghe le Procedure che hanno subito modifiche solo formali (vedi avanti “Versioni Procedure”).

Stampe di una Versione

È possibile richiedere le stampe di Versioni già emesse.

Aggiornamento dei Punti di controllo previsti dalle Linee Guida ANCE

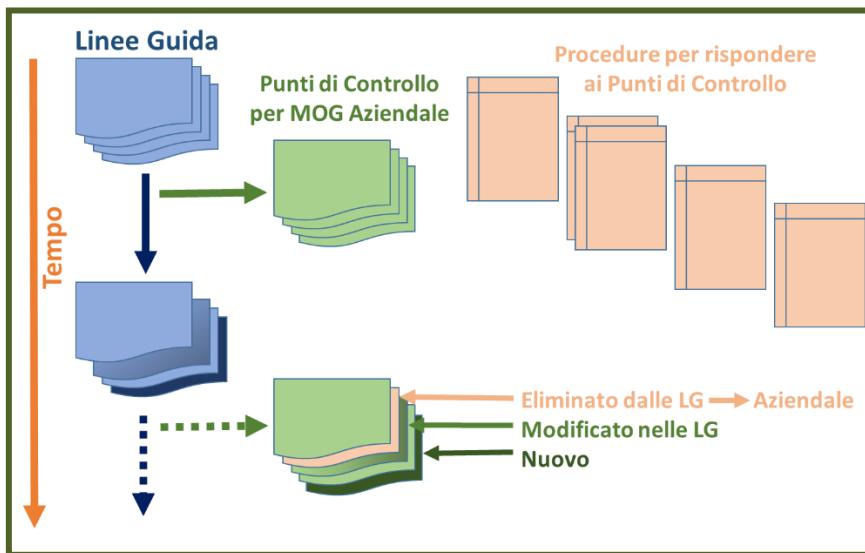
Nota: Questo paragrafo è riservato agli Enti che basano il proprio Modello sul Codice di Comportamento ANCE

“In presenza di singole novazioni legislative o giurisprudenziali, ANCE renderà tempestivamente disponibili agli enti aderenti sul proprio sito suggerimenti per un congruente adeguamento del Modello organizzativo (nuovi Punti di controllo e/o adeguamento degli esistenti), fermo restando che tali suggerimenti saranno periodicamente fatti confluire in una nuova revisione del Codice di Comportamento e sottoposti al Ministero della Giustizia per le valutazioni di competenza.”⁴

In genere è opportuno che il Modello aziendale si basi sempre sui Punti di controllo proposti dalle Linee Guida nella versione più aggiornata.

In ogni momento è possibile, sempre dalla scelta di Menù “MOG/Versioni”, ottenere un documento di Excel con l’indicazione dei Punti di controllo modificati e, eventualmente, aggiornare i Punti di controllo in base alle nuove proposte provenienti dall’aggiornamento delle Linee Guida.

⁴ Cfr. Codice di Comportamento per le Imprese di Costruzione 2013, Parte Prima pag. 18.



NOTA: Nel tempo le Linee Guida vengono aggiornate (eliminando alcuni Punti di controllo, modificandone altri ed aggiungendone di nuovi).

L'azienda, in un determinato momento, ha deciso di utilizzare, per il proprio Modello Aziendale, i Punti di controllo proposti, in quel momento, dalle Linee Guida. L'azienda predispone una o più Procedure per ognuno di questi Punti di controllo.

In ogni momento è possibile controllare le variazioni fra i modelli attualmente proposti dalle Linee Guida e quelli utilizzati aziendalmente e, se si desidera, procedere all'aggiornamento di questi ultimi.

L'operazione di aggiornamento dei Punti di controllo viene effettuata solo su esplicita indicazione dell'utente che ne deve avere consapevolezza anche perché, a seguito della modifica dei Punti di controllo sarà opportuno rivedere le Procedure predisposte per rispondere alla versione precedente dei Punti di controllo modificati ed aggiungere Procedure per rispondere ai Punti di controllo nuovi.

Eventuali Punti di controllo non più presenti nell'ultima versione delle Linee Guida non verranno cancellati (per non perdere le Procedure aziendali per loro predisposte) ma verranno considerati come Punti di controllo Aziendali (l'azienda potrà comunque eliminare questi Punti di controllo se non li ritiene più necessari).

In assenza di nuovi aggiornamenti i Punti di controllo utilizzati saranno quelli proposti dalle Linee Guida al momento della elaborazione del Questionario.

Analisi dell'evoluzione

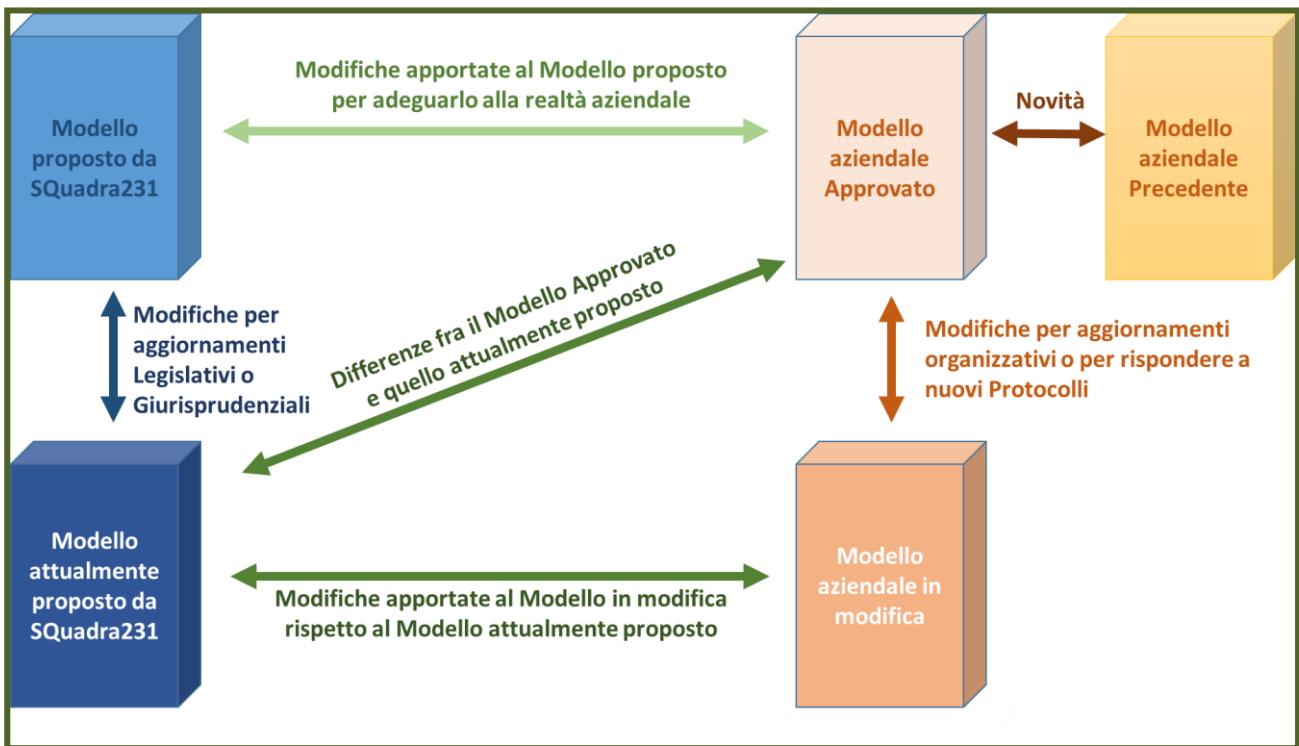
In ogni momento SQuadra231 permette ottenere vari documenti di Word contenenti tutte le informazioni (Rischi Lordi, Organigramma, Punti di controllo, Procedure e relativa correlazione con i Reati) relativi a diverse situazioni:

- Versione in Modifica (non ancora approvata).
- Versione Approvata (quella attualmente in uso nell'Ente).
- Ultima Versione Approvata precedente all'attuale.

Per gli Enti che basano il proprio Modello sul Codice di Comportamento ANCE è inoltre interessante ottenere:

- Versione proposta da SQuadra231 in base al Codice ANCE al momento della prima stesura del Modello Aziendale.
- Versione attualmente proposta da SQuadra231 in base al Codice ANCE.

Confrontando i vari documenti fra di loro sarà quindi possibile evidenziare le variazioni con la funzionalità di Word: Revisione/Confronta.



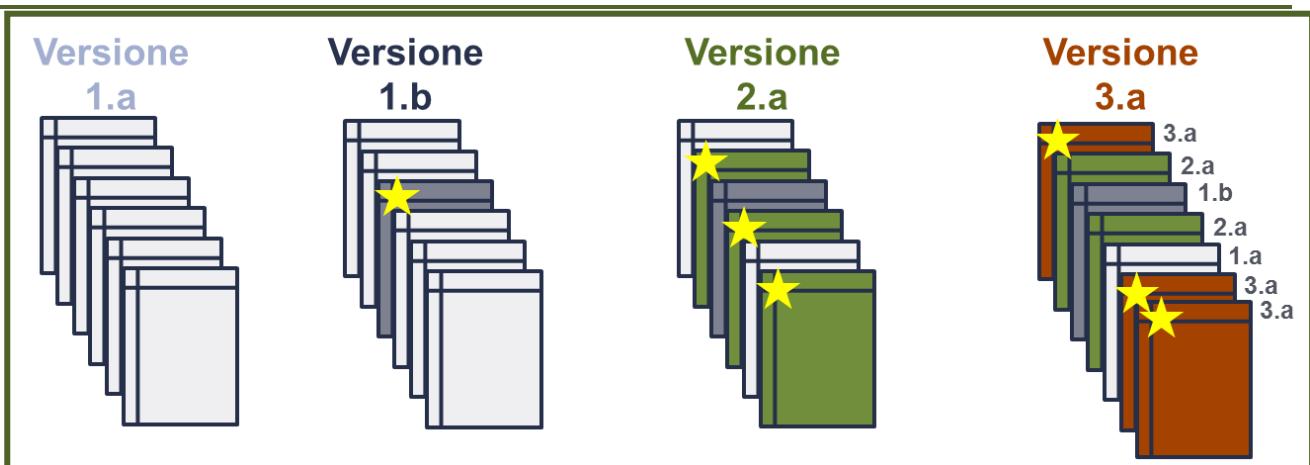
SUGGERIMENTO: Da un confronto fra questi documenti (ottenibile anche utilizzando le funzionalità di WORD: Revisione/Confronta) è possibile:

- Evidenziare le modifiche della Versione in modifica rispetto alla Versione Attuale per analizzare le novità in caso di emissione ufficiale della versione in modifica.
- Evidenziare le novità dell'ultima Versione emessa rispetto alla precedente.

Per le Aziende che utilizzano le Linee Guida ANCE:

- Individuare le variazioni nelle Linee Guida proposte da ANCE rispetto alla versione utilizzata come riferimento per l'emissione dell'ultima Versione e quindi delle quali tener conto per una eventuale modifica del Modello.
- Analizzare le personalizzazioni apportate per il Modello Aziendale nella Versione attualmente emessa rispetto alle Linee Guida attuali.
- Analizzare le personalizzazioni risultanti fra il Modello Aziendale nella Versione attualmente emessa e le Linee Guida attuali.
- Effettuare gli ultimi 2 raffronti con la Versione attualmente "in modifica" che quindi potrebbe essere emessa se approvata dall'Organo dirigente della Società.

Versioni Procedure



NOTA: Per semplicità e completezza l'Organo Dirigente della Società è chiamato ad emettere nuove Versioni dell'intera Parte Speciale del Modello la cui validità alla prevenzione dei reati è da considerare nella sua interezza.

In realtà la Parte Speciale del MOG è composta dalle varie Procedure e, in genere, l'emissione di una nuova Versione della Parte Speciale corrisponde alla modifica solo di un certo numero di Procedure; le altre rimangono immutate rispetto alla Versione precedente.

È quindi opportuno che ogni singola procedura sia caratterizzata dalla versione di prima emissione.

Alla emissione di una nuova Versione non è quindi necessario effettuare nuovamente tutte le NOMINE o non considerare più validi tutti gli AUDIT svolti in base ad una Versione precedente ma bisogna controllare solo le Procedure "di nuova emissione".

Il programma confronta in automatico le Procedure con quelle precedenti e riporta la versione di prima emissione per quelle identiche.

L'OdV può scegliere di ritenere analoghe anche procedure le cui modifiche sono unicamente formali (anticipando in questo modo la versione di prima emissione). Potrà eventualmente indicarne le motivazioni nelle note.

Documenti approvati

Possono essere stampati i documenti relativi all'ultima versione approvata e quindi quelli validi all'interno dell'azienda e gli unici utilizzabili dall'OdV nella sua funzione di vigilanza.

Analisi del Modello Approvato

Metodi e Intervalli di Rischio

Ogni impresa può decidere le modalità per la valutazione dei Livelli di Rischio e per l'elaborazione dei Rischi Residui Rilevati.

Ogni impresa può definire i Livelli (in un intervallo da 0 a 10) di rischio da utilizzare per identificare:

- Rischi Trascurabili
- Rischi sotto controllo
- Rischi da tenere sotto controllo
- Rischi NON ACCETTABILI

Viene richiesto di fornire i valori per il calcolo della Gravità dei vari Gruppi di Reati presupposto (per il significato dei Gruppi di Reato si veda l'Appendice "Analisi dei rischi 231"). In particolare, viene richiesto di fornire il peso relativo fra Quote minime (Pm) e Quote Massime (PM) ed il Peso dell'interdizione (PI).

Il calcolo della gravità sarà:

PI (solo se prevista l'interdizione)+(10-PI)(Pm x Quote_min + PM * Quote_MAX)/(Pm+PM)/100.*

Vengono quindi richiesti i pesi per determinare la Probabilità in base ai 4 parametri (Effettività, Benefici, Soggetti e Frequenza). La somma dei Pesi deve fare 100

Il calcolo della probabilità sarà:

Somma dei Parametri moltiplicati per il Peso / 100.

Livelli di Rischio

NOTA: Questa funzionalità viene abilitata in base alle indicazioni riportate nei "Metodi e Intervalli".

Nel Codice di Comportamento ANCE viene riportata una valutazione, per una impresa di costruzioni standard, del livello di rischio lordo (inteso come combinazione di gravità e probabilità del reato in assenza di un modello di prevenzione reati) connesso a ciascuna fattispecie di reato.

Ogni impresa può modificare la valutazione del Rischio Lordo in funzione delle proprie specifiche caratteristiche. In caso di diminuzione dei valori proposti da ANCE è opportuno descriverne le motivazioni.

Qualora nell'azienda vi sono stati reati pregressi (ovvero reati commessi nei tre anni precedenti alla valutazione in oggetto) sarà necessario utilizzare lo specifico livello a meno che non siano state apportate significative modifiche alle procedure o all'organizzazione aziendale tali da prevenire il ripetersi della commissione del reato che dovranno essere dettagliatamente illustrate.

Livelli di rischio⁵

- Non significativo..... 0
- Trascurabile..... 1
- Basso 2
- Medio 3
- Alto 4
- Reato pregresso⁶ 5

Livelli di Rischio dalle Interviste

Qualora l'impresa decida di analizzare il proprio Livelli di Rischio tramite le Interviste è possibile modificare i Livelli di Rischio in base al risultato delle Interviste (Vedi avanti).

Presentazioni sul Modello approvato analoghe a quelle sul Modello in fase di modifica

È possibile effettuare tutte le analisi presentate per il Modello in modifica sull'ultima versione Modello approvata e quindi attualmente valida e sulla quale deve operare l'OdV.

Per una illustrazione si rimanda ai precedenti paragrafi sulla Adeguatezza del Modello in modifica.

Responsabili coinvolti nel sistema 231

Con l'emissione vengono memorizzate le varie Funzioni Aziendali.

Vengono anche proposti i nominativi assegnati alle varie Funzioni Aziendali individuali.

Ad ogni nominativo è possibile aggiungere l'indirizzo mail per permettere al programma la predisposizione di comunicazioni automatiche.

È possibile inserire la data prevista per il Prossimo Audit che verrà utilizzata per la Pianificazione degli Audit. La Data verrà aggiornata dal programma al momento della registrazione dell'ultimo Audit svolto in funzione della Stabilità del processo analizzato.

È possibile inserire anche la data prevista per la Prossima Informativa che verrà utilizzata per il controllo da parte dell'OdV delle Informative ricevute. La Data verrà aggiornata dal programma al momento della registrazione dell'ultima Informativa ricevuta in funzione della Stabilità del processo analizzato.

Per comodità il programma mostra il numero di Procedure e di Informative assegnate al Responsabile dall'ultimo MOG approvato.

Una eventuale modifica al nominativo verrà considerato come una correzione ortografica e verrà riportata automaticamente anche nei nominativi delle Funzioni Aziendali previste per il MOG attualmente in modifica.

⁵ Se si considera il primo Comma dell'Art. 25-07 (che avrà Gravità sicuramente =10) si ipotizza una Probabilità del 40%; per il secondo e terzo comma (dove sono previste al massimo 500 quote) la Gravità sarà circa la metà (in funzione del valore attribuito all'interdizione) e quindi la Probabilità pari a circa l'80%

⁶ Ovviamente l'ultimo livello non viene utilizzato nelle stime ANCE.

Andranno inseriti anche i nominativi delle altre persone coinvolte nella gestione del Modello (ad esempio quelle che ricoprono le Funzioni Aziendali “multiple”, che non vengono dettagliatamente indicate nel MOG) al fine di gestire correttamente le attività dell’OdV anche per questi responsabili.

Procedure

Per ogni persona vengono presentate le Procedure collegate.

Allegati

Per ogni persona è possibile aggiungere vari allegati.

Formazione

È necessario inserire la formazione effettuata per ogni persona relativamente al D.LgsL 231/01.

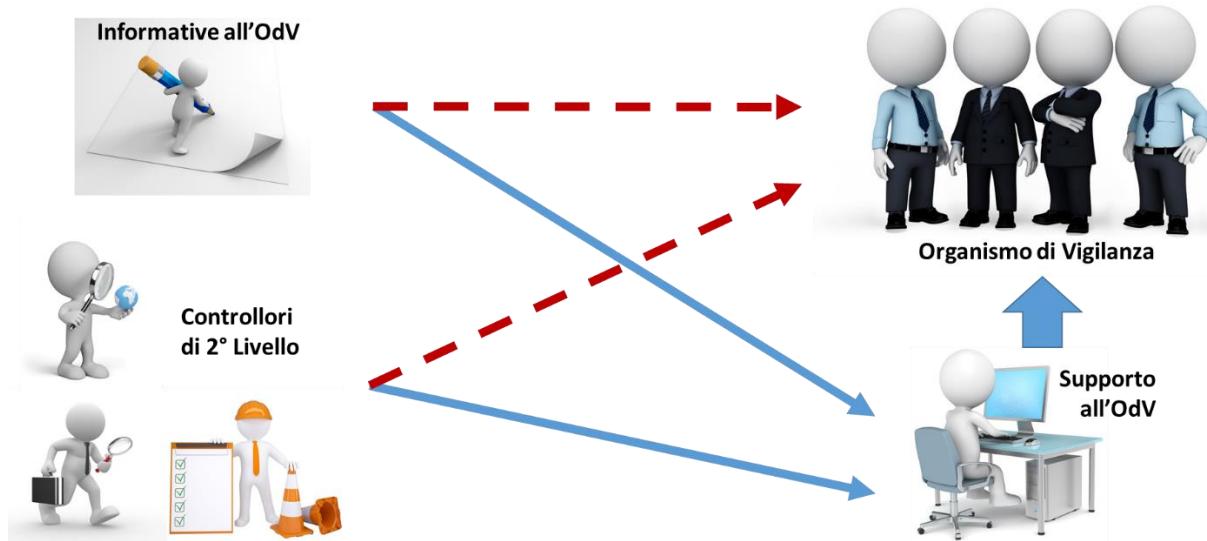
Fra i vari eventi formativi verranno evidenziati quelli relativi alla Formazione generica sul Decreto e/o alla Formazione specifica sul Modello di Organizzazione e Gestione con particolare riferimento alle responsabilità assegnate con conseguente firma della Nomina.

Funzioni Multiple

Per le Funzioni Multiple è necessario effettuare l'associazione con le varie Persone già definite (vedi punto precedente) indicando i Cantieri di competenza.

1.2.4.3 Attività di Supporto all’OdV

All'interno dell'azienda può essere individuato un referente che supporti l'OdV raccogliendo e trasmettendo gli Audit svolti dai Controllori (secondo quanto previsto dalle varie Procedure) e le Informative per l'OdV.



Il referente di supporto potrà anche raccogliere le varie informative.

Rimane la possibilità dei controllori di 2° livello di inviare direttamente all’OdV le risultanze delle proprie attività di controllo. Analogamente i singoli responsabili potranno inviare le proprie informative direttamente all’OdV.

Sulle informazioni ricevute dal referente di supporto l’OdV non potrà apportare modifiche.

Audit effettuati dai Controllori

Audit da Trasmettere

In questa funzione è possibile inserire gli Audit effettuati dai vari Controllori indicando:

- Codice e Descrizione.
- Data di riferimento.
- Data di annullamento (dalla data di annullamento le valutazioni presenti nei dettagli dell’audit non verranno più utilizzate per il calcolo del Rischio Residuo Rilevato).

- Note.

È possibile definire un file di excel da utilizzare per l'importazione dei dettagli (vedi avanti per come ottenere il file da compilare ed utilizzare per l'importazione).

Dettagli dell'Audit

Ogni Audit è costituito da un insieme di controlli effettuati sulle varie Procedure di interesse.

Ogni Dettaglio è caratterizzato da:

DATI DELL'AUDIT:

- Procedura.
- Data svolgimento audit.
- Nome del Controllore.
- Persona sottoposta ad audit.
- Livello di Conformità rilevato.
- Numero di mesi dopo i quali si ritiene opportuno svolgere un nuovo audit.
- Evidenze rilevate.
- Note interne.
- Osservazioni elevate dal Controllore alla Persona sottoposta ad Audit.

RILIEVI (dove presenti):

- Descrizione del Rilievo.
- Trattamento concordato.
- Data prevista per la conclusione del Trattamento.
- Data effettiva di conclusione del Trattamento.
- Data di chiusura del Rilievo.
- Note sulla chiusura.
- Conformità rilevata a valle della chiusura del Rilievo.

RAPPORTI CON ODV:

- Note per l'OdV.
- Se presenti verranno presentate le Risposte fornite dall'OdV.

Allegati

Ad ogni Audit è possibile collegare vari allegati.

In particolare, sarà opportuno trasmettere il Rapporto di Audit (stampabile come sottoindicato) firmato dalla persona sottoposta ad Audit e da chi ha effettuato i controlli.

Rapporto di Audit

È possibile richiedere il documento di word del Rapporto di Audit con le evidenze e le valutazioni relative a tutti i dettagli.

Trasmissione degli Audit all'OdV

In ogni momento è possibile “trasmettere” all'OdV l'Audit con tutti gli Allegati ed i Dettagli. Da quel momento non sarà più possibile visualizzarlo o modificarlo.

I dettagli degli Audit trasmessi saranno visibili nella funzione illustrata di seguito.

Al momento della trasmissione il programma provvede ad inviare una mail al Controllore in modo da renderlo consapevole che da quel momento i suoi dati saranno utilizzati dall'OdV per valutare l'adeguatezza del Modello.

Verrà anche inviata una mail all'OdV per segnalare la disponibilità di nuove informazioni.

Eliminazione dei dettagli.

La funzione permette una cancellazione “massiva” di tutti gli elementi di dettaglio, ad esempio per effettuare una nuova rilevazione.

Viene predisposto un file di excel per la nuova rilevazione contenente i dati precedentemente inseriti.

Importa Audit

Questa funzione permette l'inserimento automatico dei dettagli dell'Audit delle informazioni raccolte sul foglio di excel appositamente predisposto (vedi avanti).

Gestione dei Rilievi

Vengono presentati tutti gli Audit (sia già trasmessi che da trasmettere) contenenti Rilievi ancora aperti (per i quali non è ancora stata definita la data di chiusura) per permetterne la registrazione della data effettiva di conclusione del Trattamento e quella di Chiusura.

Una volta inserita la data di chiusura i rilievi non saranno più visibili.

Solo l'OdV potrà visualizzarli e, in caso, annullare la chiusura rendendoli nuovamente visibili e modificabili.

Predisposizione dei documenti per lo svolgimento degli Audit

Questa funzione fornisce un documento di Word utilizzabile per lo svolgimento degli Audit con la possibilità di restringere le procedure di interesse.

Viene fornito anche un Foglio di Excel per raccogliere le informazioni in modo da inserirle direttamente all'interno di SQuadra (con l'apposita funzione illustrata precedentemente) invece di doverle inserire manualmente nei “Dettagli dell'Audit” come visto in precedenza.

Informative per l'OdV

In questa funzione è possibile inserire le Informative per l'OdV indicando:

- Codice e Descrizione.
- Data di riferimento.
- Data di annullamento (dalla data di annullamento le valutazioni presenti nei dettagli dell'audit non verranno più utilizzate per il calcolo del Rischio Residuo Rilevato).
- Note.

È possibile definire un file di excel da utilizzare per l'importazione dei dettagli (vedi avanti per come ottenere il file da compilare ed utilizzare per l'importazione).

Informative da Trasmettere

In questa funzione è possibile inserire le Informative per l'OdV dei vari Responsabili indicando:

- Procedura.
- Data compilazione dell'Informativa.

- Periodo di interesse.
- Persona che ha predisposto l'informativa.
- Informazioni per l'OdV.
- Note interne.

Allegati

Ad ogni Informativa è possibile collegare vari allegati.

In particolare, sarà opportuno trasmettere l'Informativa (stampabile come sotto indicato) firmato dal responsabile della compilazione.

Rapporto dell'Informativa

È possibile richiedere il documento di word dell'informativa con tutti i dettagli.

Trasmissione dell'Informativa all'OdV

In ogni momento è possibile "trasmettere" all'OdV l'Informativa con tutti gli Allegati ed i Dettagli. Da quel momento non sarà più possibile visualizzarla o modificarla.

I dettagli delle Informative trasmesse saranno visibili nella funzione illustrata di seguito.

Al momento della trasmissione il programma provvede ad inviare una mail all'OdV per segnalare la disponibilità di nuove informazioni.

Eliminazione dei dettagli.

La funzione permette una cancellazione "massiva" di tutti gli elementi di dettaglio, ad esempio per effettuare una nuova informativa.

Viene predisposto un file di excel per la nuova rilevazione contenente i dati precedentemente inseriti.

Importa Informative di dettaglio

Questa funzione permette l'inserimento automatico dei dettagli dell'Informativa dalle informazioni raccolte sul foglio di excel appositamente predisposto (vedi avanti).

Predisposizione foglio di excel per la rilevazione delle Informative sulle varie Procedure

Questa funzione fornisce un documento di Excel per raccogliere le informative in modo da poterle inserire direttamente all'interno di SQuadra (con l'apposita funzione illustrata di seguito) invece di doverle inserire manualmente in "Informative da Trasmettere" come visto in precedenza.

Assegnazione delle responsabilità di controllo nel MOG in Modifica

Assegnazione dei controllori alle Procedure

Come illustrato nella gestione delle Procedure è possibile definire la persona addetta al controllo.

Questa funzione permette di assegnare ad un Controllore più procedure.

Per prima cosa è possibile individuare le Procedure di interesse (in base all'assenza del Controllore, del Processo o delle Funzione Responsabile). Fra le Procedure presentate è possibile selezionare quelle di interesse e quindi, con l'apposito bottone, assegnare il Controllore.

Controllo assegnazione Controllori

Viene fornito un file di Excel nel quale sono evidenziati eventuali errori nell'assegnazione dei Controllori (Controllore = Controllato) e le Procedure con e senza Controllori.

Vengono distinte le Informative ed i Divieti che, in genere, non prevedono un controllore ma direttamente informative da inviare all'OdV.

1.2.4.4 Attività dell'Organismo di Vigilanza

L'utilizzo di questo insieme di funzioni è rivolto principalmente ai membri degli OdV. Per l'utilizzo di queste funzioni è indispensabile che si siano gestite correttamente le Versioni del MOG come illustrato precedentemente.

Controllo delle attività di Supporto all'OdV

Con queste funzioni l'OdV può effettuare i controlli sulle attività di supporto e fornire informazioni. L'OdV può rinviare alla funzione di supporto elementi già trasmessi se ritiene non siano correttamente gestiti (valutazioni di conformità non adeguatamente supportate dalle evidenze, rilievi chiusi senza adeguata verifica del trattamento, ecc.) ma non può modificare le valutazioni ricevute.

Audit trasmessi dai Controllori

Controllo Audit

È possibile controllare tutti gli Audit trasmessi.

L'OdV può annullare la data di invio ritrasmettendo l'intero Audit a chi fornisce il supporto all'OdV, ad esempio, per chiedere maggiori informazioni sulle evidenze o sulle osservazioni.

Per ogni Audit è possibile verificare i dettagli ed eventualmente rispondere alle Note registrate dai Controllori o inserire note interne.

È, inoltre, possibile annullare la data di chiusura dei Rilievi qualora le modalità di chiusura non soddisfino l'OdV.

Gestione dei Rilievi

Vengono presentati tutti gli Audit (sia già trasmessi che da trasmettere) contenenti Rilievi per permetterne il controllo.

Si ricorda che i Rilievi con inserita la data di chiusura sono visibili solo all'OdV.

Se l'OdV desidera renderli nuovamente visibili e modificabili dalla funzione di supporto dovrà annullare la data di chiusura.

Informative trasmesse all'OdV

Analogamente a quanto visto per gli Audit è possibile controllare le informative ricevute (ed eventualmente, annullando la data di trasmissione, chiederne una revisione), le ultime informative di dettaglio e lo storico.

Analisi della Conformità delle varie Procedure

Il "cruscotto" mostra le varie Procedure con le informazioni relative alle informazioni a disposizione dell'OdV.

Attività periodiche dell'OdV

Verbali OdV

È possibile definire i dati essenziali di ogni riunione dell'OdV.

A conclusione di ogni riunione dell'OdV è necessario dare una indicazione sulla periodicità in base alla quale prevedere la data per la prossima Riunione.

Allegati

È possibile memorizzare come allegati il verbale della riunione dell'OdV ed eventuali altri documenti analizzati.

Rilievi

Ad ogni verbale possono essere associati dei Rilievi / Azioni da intraprendere.

Testo base per il Verbale in Word

Il programma consente di produrre un documento di Word con un testo di riferimento per la stesura del Verbale (sia per OdV Monosoggettivi che Collegiali) che dovrà poi essere rivisto per ottenere la stesura finale.

Vengono presentate una serie di "frasi" predefinite fra le quali dovranno essere scelte quelle di interesse.

Alcune di queste frasi sono da utilizzare prevalentemente solo nella fase iniziale (Nomina, Regolamento, ecc.) e vengono evidenziati in colore verde. Fra queste "frasi" sono presenti anche alcune illustrate nel paragrafo successivo.

Alcune "frasi" (evidenziate in giallo) prevedono anche delle elaborazioni da parte del Programma che provvederà a produrre testi specifici come ad esempio:

- L'analisi degli aggiornamenti normativi successivi al Dicembre 2013 (data di rilascio dell'idoneità del Codice di Comportamento ANCE).
- Se sono state svolte delle Interviste per l'Analisi dei Rischi è possibile ottenere una descrizione di sintesi dei risultati (è previsto anche il caso di aziende standard ANCE).
- La valutazione dell'Adeguatezza del Modello (è possibile valutare sia il MOG attualmente in fase di modifica in vista della sua approvazione da parte dell'Organo Dirigente sia il MOG nell'ultima versione approvata e quindi attualmente in uso).
- La predisposizione di una bozza di Regolamento di Funzionamento dell'OdV (che definisce le modalità operative stabilite autonomamente fra i Membri dell'OdV per organizzare la propria attività all'interno delle regole stabilite dall'Organo dirigente della società all'interno della Parte Generale del MOG).
- Elenco delle Nomine accettate dai vari Responsabili e di quelle mancanti o da aggiornare.
- Elenco dei Responsabili che hanno svolto la Formazione sui temi del D.Lgs. 231/01 e di quelli che la devono ancora svolgere.
- Il testo di una comunicazione di sollecito per il Responsabile del Personale affinché provveda alla raccolta delle accettazioni delle Nomine mancanti ed alle attività di Formazioni non ancora effettuate.
- Elenco degli Audit svolti e Pianificazione dei prossimi Audit all'interno del Verbale e una comunicazione per ogni Responsabile sulla pianificazione degli Audit (con riportate le Procedure di competenza che saranno sottoposte a verifica).
- Elenco delle Informative ricevute e di quelle previste ma non ancora prevenute all'OdV. Una comunicazione, per ogni Responsabile che non ha ancora inviato all'OdV la propria Informativa con l'elenco delle informazioni minime da comunicare all'OdV in base alle Procedure.
- L'Elenco dei Rilievi chiusi nel periodo e di quelli ancora aperti. Per i Rilievi ancora aperti viene predisposta una Comunicazione ai Responsabili del Trattamento.
- Analisi delle Segnalazioni ricevute dall'OdV tramite l'apposito canale di comunicazione.
- Elenco dei Provvedimenti disciplinari proposti dall'OdV all'Organo dirigente.
- Relazione sul Rischio Rilevato a seguito degli Audit svolti.

Quando SQuadra231 predispone, nel testo di Word, le comunicazioni da inviare ai vari Responsabili provvede anche a predisporre delle bozze di comunicazioni che possono essere inviate, in alternativa all'invio della comunicazione cartacea, via MAIL (si veda il punto successivo).

NOTA: Il primo elemento selezionabile ("Testo base automatico") racchiude i tipici richiami per un verbale standard (Audit, Informative, Rilievi, ecc.).

Relazioni periodiche dell'OdV

È possibile memorizzare le informazioni principali delle Relazioni che periodicamente l'OdV predisponde per gli organi Dirigenti e di Controllo della Società.

Valutazioni sui Rischi per i vari Reati

È possibile definire una valutazione riepilogativa dei Rischi residui rilevati nel periodo per i vari Reati. La valutazione può partire dall'Analisi dei Rischi Rilevati (si veda il capitolo successivo del presente Manuale).

Allegati

È possibile memorizzare come allegati le Relazioni stesse ed eventuali altri documenti allegati.

Analisi dei Rischi residui per i vari Reati

È possibile definire, per ogni Relazione, una valutazione per ogni famiglia di Reati previsti dal D.Lgs. 231/01.

Qualora si utilizzi l'Analisi dei Rischi (presentata nel capitolo successivo) verranno riportati i risultati della valutazione dei Rischi Residui. Sarà cura dell'OdV confermare le valutazioni ottenute in automatico o fornire valutazioni differenti eventualmente indicandone le motivazioni.

Testo base per la Relazione in Word

Il programma consente di produrre un documento di Word con un testo di riferimento che dovrà poi essere rivisto per ottenere la stesura finale.

Nel Documento vengono riportate in automatico informazioni relative a:

- Nuove emissioni della Parte Speciale del MOG avvenute nel Periodo di Riferimento.
- Stato delle attività di formazione.
- Elenco delle riunioni svolte dall'OdV nel Periodo.
- Elenco delle Informative ricevute dall'OdV nel Periodo.
- Analisi delle Segnalazioni ricevute dall'OdV.
- Elenco degli Audit svolti e la Pianificazione dei prossimi.
- L'elenco dei Rilievi, Non Conformità ed Osservazioni rilevate con l'evidenziazione di quelle ancora aperte.
- L'eventuale elenco dei Provvedimenti disciplinari proposti dall'OdV.
- Un giudizio sintetico sull'applicazione del Modello.
- Gli obiettivi per i Periodi successivi.

Informative

È possibile memorizzare informazioni di sintesi sulle varie Informative ricevute dall'OdV. È opportuno allegare la copia digitale dei documenti ricevuti.

Anche per le Informative è necessario dare una indicazione sulla stabilità del sistema per poter prevedere la data prevista per la prossima Informativa.

È possibile considerare non valida una Informativa o definire una data dalla quale deve essere esclusa ai fini del calcolo dei Rischi Residui.

Per le Informative periodiche è possibile chiedere al programma di creare tutte le procedure che dovrebbero essere oggetto dell'Informativa (in base a quanto previsto dal Modello per lo specifico Responsabile). Dove necessario possono essere aperti dei Rilievi o delle Osservazioni a seguito della Informativa ricevuta.

Il programma provvede a modificare per la Persona la data prevista per la prossima Informativa in base alla periodicità (ad esclusione, ovviamente, di quelle occasionali).

Audit

È possibile memorizzare le verifiche ispettive svolte. Ogni Audit viene svolto ad una Persona ed è caratterizzato dalla data di svolgimento e da note di carattere generale. Vengono quindi analizzate tutte le Procedure di competenza della Persona sottoposta ad Audit escluse quelle controllate da altre Funzioni Aziendali.

È possibile considerare non valido un Audit o definire una data dalla quale deve essere escluso ai fini del calcolo dei Rischi Residui.

Per ogni procedura è possibile la registrazione delle evidenze (anche attraverso l'archiviazione digitale dei documenti raccolti) e dei Rilievi o Osservazioni (per comodità il programma riporta le evidenze rilevate nell'eventuale precedente audit).

È opportuno allegare all'Audit il verbale delle attività svolte con la firma anche della persona coinvolta. Alla fine dell'Audit è necessario dare una indicazione sulla stabilità del sistema per poter ripianificare l'audit stesso.

Il Programma permette di stampare una scheda riepilogativa dell'Audit (con l'indicazione dei documenti allegati e dei Rilievi rilevati) oltre alla stampa di tutti gli Allegati connessi.

Il programma provvede a modificare per la Persona la data prevista per il prossimo Audit in base alla periodicità (ad esclusione, ovviamente, di quelli occasionali).

Via via che vengono trattati i Rilievi è possibile inserire una nuova valutazione con la relativa data di valutazione. Questi nuovi valori verranno considerati per l'analisi del Rischio Rilevato.

Rilievi e Non Conformità

Tutti i Rilievi e Non Conformità rilevati in relazione ad una Informativa o ad un Audit vengono presentati in una maschera di riepilogo.

È inoltre possibile inserire direttamente nuovi Rilievi.

Ai vari Rilievi è possibile aggiungere degli Allegati.

Attività di verifica archiviate direttamente dall'OdV

Qualora l'azienda non sia in grado di fornire all'OdV una funzione che si occupi di raccogliere gli Audit effettuati dai controllori e le informative (vedi capitolo "Attività di Supporto all'OdV") l'OdV può svolgere in prima persona queste attività "fondendole" con le attività di "Controllo delle attività di supporto" presentate precedentemente.

In questo caso l'OdV avrà accesso diretto a tutti i dati e quindi non sono previste le specifiche funzionalità di trasmissione e blocco viste nel caso della presenza della funzione di supporto.

Analisi Procedure

Storico delle attività di vigilanza

È possibile visualizzare tutti i dettagli relativi alla vigilanza effettuata sulle singole procedure.

Analisi dell'attività di vigilanza

Il cruscotto presenta tutte le procedure evidenziando l'ultima vigilanza effettuata.

Provvedimenti disciplinari

Questa funzione permette all'OdV di registrare i Provvedimenti disciplinari che richiede all'Organismo dirigente di applicare a Dipendenti, Dirigenti e Collaboratori.

Viene quindi registrato anche l'esito delle richieste.

Pianificazione

SQuadra231 fornisce l'elenco delle scadenze per l'OdV ed in particolare:

-  Riunioni dell'OdV ripianificate.
-  Relazioni periodiche da predisporre (si prevede di effettuare la relazione nel mese successivo al periodo di riferimento).
-  Nomine ancora da effettuare o non aggiornate.
-  Formazione non ancora effettuata.
-  Audit da effettuare o ripianificati.
-  Informative da ricevere.
-  Scadenze per il trattamento dei Rilievi ancora aperti.

SQuadra231 permette di ottenere un elenco delle informazioni in formato Excel (per un controllo di dettaglio) o di averne una visualizzazione in formato Calendario (per un più immediato impatto visivo).

Nella Pianificazione, ovviamente, non vengono considerate solo le Persone indicate come "Validi".

Controllo ed invio e-mail

Come illustrato in precedenza SQuadra231 è in grado di produrre delle bozze di e-mail da inviare alle varie Persone.

È possibile controllare le e-mail proposte per modificare il testo e per cancellare quelle non di interesse (in genere perché si è provveduto alla comunicazione via cartacea della quale l'OdV terrà traccia autonomamente).

È infine possibile selezionare ed inviare le e-mail di interesse. SQuadra231 provvede ad inviare una copia di ogni e-mail inviata all'indirizzo dell'OdV al fine di documentare l'attività di vigilanza.

Le e-mail per le quali non è definito l'indirizzo di destinazione vengono segnalate in rosso; quelle inviate vengono segnalate in verde.

Archivio Documenti

È possibile memorizzare liberamente altri Documenti ritenuti importanti per dimostrare l'idoneità e l'applicazione del Modello.

Ogni Documento sarà caratterizzato da:

- Periodo di riferimento (in genere l'anno)
- Data
- Tipo (per poter raggruppare famiglie di documenti analoghi)
- Note di dettaglio
- Uno o più allegati in formato digitale.

1.2.4.5 Segnalazioni all’OdV

SQuadra231 permette di creare un canale di comunicazione fra l’Organismo di Vigilanza (OdV) e tutti i portatori di interesse (dipendenti, collaboratori, fornitori, clienti, ecc.) che desiderano:

- Segnalare, in buona fede o sulla base di una ragionevole convinzione, atti di violazione della legge tentati, presunti ed effettivi, oppure qualsiasi violazione o carenza concernente il sistema di gestione per la prevenzione dei reati.
- Richiedere consulenza su cosa fare quando ci si trova dinanzi a un sospetto o a una situazione che possa comprendere atti di violazione del Codice Etico.
- Richiedere chiarimenti o spiegazioni da parte dell’OdV sul Codice Etico, Modello aziendale.

SQuadra231 separa, come previsto da ANAC, i dati identificativi del segnalante dal contenuto della segnalazione, prevedendo l’adozione di codici sostitutivi dei dati identificativi, in modo che la segnalazione possa essere processata in modalità anonima e rendere possibile la successiva ricostruzione dell’identità del segnalante nei soli casi consentiti.

SQuadra231 prevede tre attori principali:

- Il Segnalante (“Whistleblower”): segnala l’illecito all’Ente / Amministrazione.
- L’Istruttore (OdV): prende in carico la segnalazione e gestisce l’istruttoria.
- L’Amministratore e Custode di chiavi (IL TIGLIO SRL): gestisce la piattaforma e autorizza le richieste di accesso degli istruttori alle identità dei segnalanti.

Appena un membro dell’Organismo di Vigilanza ha accesso alla gestione delle Segnalazioni è opportuno pubblicizzare a tutti gli Stakeholder, in genere tramite il Sito Aziendale, le modalità con le quali tutti possono comunicare, anche in forma anonima, con l’OdV.

Fra i “Documenti di Supporto” (sotto il menu VARIE) sono presenti delle Note sulle Segnalazioni (in formato Word) che possono essere utilizzate per predisporre la documentazione per comunicare a tutti gli stakeholder la politica nei confronti delle segnalazioni dei sospetti e le modalità operative messe a disposizione per la creazione di un canale di comunicazione con l’Organismo di Vigilanza.

Nello stesso documento è riportata una bozza per la predisposizione dell’apposita sezione nel regolamento dell’OdV.

Configurazione del Canale di Comunicazione

Per prima cosa è opportuno personalizzare il proprio canale inserendo:

- Uno specifico Logo (è possibile richiedere una immagine d’esempio).
- Un testo che si desidera appaia all’apertura del canale (ad esempio: CANALE ALTERNATIVO PER LE SEGNALAZIONI *Le Segnalazioni all’Organismo di Vigilanza possono essere inoltrate anche mediante canali alternativi alla presente piattaforma: per iscritto mediante lettera indirizzata all’Organismo di Vigilanza Via XXX o consegnata brevi manu allo stesso. Qualora le Segnalazioni riguardino direttamente un componente dell’Organismo di Vigilanza le stesse dovranno essere indirizzate direttamente al Presidente del Collegio Sindacale al seguente indirizzo e-mail: Presidente@collegiosindacale.it.*)
- La mail alla quale verrà inviata una comunicazione ad ogni nuova segnalazione.
- Il numero di mesi dalla chiusura della segnalazione dopo cui verranno oscurate tutte le comunicazioni contenenti dati personali (in genere 6 mesi).
- Il numero di mesi dalla chiusura dell’ultima segnalazione dopo di cui verrà disabilitato il segnalante e verranno resi anonimi i dati personali forniti (in genere 12 mesi).

È inoltre opportuno definire le Zone e gli Argomenti che verranno utilizzate per catalogare ogni Segnalazione.

Contenuto di ogni Segnalazione

Ogni Segnalazione è caratterizzata da alcuni dati di carattere generale:

- Dati inseriti dal Segnalante e modificabili dall'OdV:
 - Titolo.
 - Argomento (selezionato fra quelli predisposti dall'OdV).
 - Zona (selezionato fra quelli predisposti dall'OdV).
- Dati gestiti dall'OdV:
 - Processo coinvolto.
 - Criticità.
 - Stato della Segnalazione (una Segnalazione viene considerata chiusa se lo stato è Chiusa o Non Considerata).
 - Note dell'OdV.

Per ogni Segnalazione sono presenti quindi le Comunicazioni relative provenienti dal Segnalante e le risposte o richieste di chiarimenti da parte dell'OdV al Segnalante.

È possibile ottenere una stampa della Segnalazione con le relative Comunicazioni e la stampa di tutti gli allegati collegati alla Segnalazione.

Se il segnalante desidera rimanere "riservato" il suo nominativo non verrà presentato all'OdV che però potrà accedervi qualora fosse strettamente necessario alla gestione della segnalazione. Il sistema terrà traccia dell'eventuale comunicazione del nominativo all'OdV.

L'OdV dovrà consultare periodicamente le Comunicazioni ricevute e, per ogni Segnalazione analizzarla e, dove necessario, richiedere chiarimenti e quindi fornire informazioni sulle attività svolte.

Per prima cosa l'OdV dovrà catalogare la Segnalazione definendo, fra l'altro, se vengono trattati dati personali (in questo caso il sistema provvederà in automatico ad oscurare tutte le comunicazioni selle Segnalazioni chiuse dopo il numero di mesi dall'ultima Comunicazione definiti dall'OdV).

Sarà cura dell'OdV, per quanto possibile, anonimizzare le informazioni relative alla Segnalazione fin da quando possibile senza inficiare la Segnalazione stessa. L'eliminazione di ogni riferimento a dati personali andrà comunque effettuato prima della chiusura.

Accedendo ad una specifica Segnalazione sarà possibile vedere tutte le Comunicazioni intervenute fra Segnalante e OdV.

Le Comunicazioni dei Segnalatori sono evidenziate in verde ed è possibile, premendo il bottone RISPOSTA predisporre la base per la risposta contenente i principali riferimenti alla comunicazione del Segnalante.

Nell'apposito folder relativo alle Risposte dell'OdV viene presentata, se presente, l'ultima risposta dell'OdV che potrà essere modificata fino all'eventuale risposta da parte del Segnalante.

Report sulle segnalazioni

È possibile avere informazioni riepilogative su tutte le segnalazioni ricevute (eventualmente in un determinato periodo temporale). In particolare, è possibile ottenere:

- Un documento di word con una sintesi delle Segnalazioni.
- Un documento di Excel con un foglio relativo ai Segnalatori ed uno relativo alle Segnalazioni.
- Una presentazione d'insieme in cui vengono presentate le Segnalazioni.

1.2.4.6 Rischi

L'utilizzo di questo insieme di funzioni è rivolto principalmente al progettista del sistema e ai membri degli OdV. Per l'utilizzo di queste funzioni è indispensabile che si siano gestite correttamente le Versioni del MOG e siano stati registrati gli Audit e i Rilievi come illustrato precedentemente.

Analisi dei Rischi

Per imprese che valutano la propria complessità "standard" secondo quanto previsto dal Codice di Comportamento ANCE 2013 (Cfr. Analisi dei rischi, pag. 182-183) l'analisi dei rischi effettuata da ANCE (identificazione dei reati applicabili e dei processi critici) è applicabile direttamente e i protocolli di prevenzione proposti sono da ritenere già adeguati alla gravità e probabilità del sottostante reato che si intende prevenire.

Analisi dei rischi aziendali

Azioni a Rischio

Il Decreto richiede di "individuare le attività nel cui ambito possono essere commessi reati". È possibile definire tutte le "azioni a rischio" per l'Ente.

Le Azioni a Rischio sono caratterizzate da un codice di 6 caratteri con il seguente formato PP.Ann dove:

- PP: è il numero del Processo (01 = Governance / 11=Ambientale).
- A: permette di scomporre il Processo in varie Attività.
- nn: è il numero dell'Attività a rischio all'interno dell'Attività.

SQuadra offre un elenco di possibili "azioni a rischio" di riferimento (circa 100); ogni azienda può escluderne alcune o aggiungerne altre in funzione delle caratteristiche specifiche.

Per facilitare l'inserimento di nuove "azioni a rischio" la codifica delle azioni proposta da SQuadra non è contigua in modo da lasciare varie posizioni libere.

Gruppi di Reati

IL TIGLIO SRL mantiene sempre aggiornato l'elenco degli Illeciti (Articoli del D.lgs. 231/01) e dei relativi Reati presupposto (Articoli del c.p. o del c.c. richiamati dal Decreto).

I Reati presupposto sono stati raggruppati in Gruppi omogenei dal punto di vista dei Punti di controllo per prevenire la commissione dei reati.

ATTENZIONE: IL TIGLIO SRL cercherà di mantenere aggiornati gli Illeciti ed i Reati presupposto ma non garantisce la correttezza delle informazioni a fronte dei continui cambiamenti apportati dal Legislatore.

OGNI UTENTE È TENUTO A VERIFICARE LA CORRETTEZZA DEI DATI RIPORTATI.

Ogni utente che lo desidera potrà indicare a IL TIGLIO SRL (posta@iltigliosrl.it) ogni errore o mancanza rilevata.

Ogni Ente deve definire la probabilità della commissione di uno dei Reati presupposto per ogni Gruppo di Reati (si rimanda alla descrizione presente nell'Appendice "Analisi dei Rischi 231" nel capitolo "Progettazione del Modello").

Pericoli

È necessario indicare, per ogni Gruppo di Reati "significativo" (con probabilità di commissione non nulla per l'Ente), in quali fra le "Azioni a rischio" sopra definite è possibile commetterli e qual è l'effettivo "pericolo" (es. per i Reati relativi alla "illecita intermediazione", nell'attività di "Stipula di contratti per prestazioni" un pericolo può essere: "L'assenza delle clausole contrattuali di garanzia relativamente al rispetto dei diritti dei lavoratori").

Punti di Controllo

È possibile definire, per ogni Punti di Controllo, i Pericoli che il PdC può contribuire a prevenire.

Esportazioni su Excel

Per analisi di sintesi sono predisposte delle esportazioni su Excel. In particolare, sono previste le seguenti esportazioni:

Illeciti, Gruppi di Reati e Reati (Livello di Rischio).

- Per ogni Illecito vengono riportati:
 - Data di entrata in vigore.
 - Data dell'ultima modifica.
 - Quote minime e massime previste.
 - Eventuale previsione dell'applicazione dell'interdizione.
 - Gravità calcolate (per il calcolo della gravità si rimanda all'appendice "Analisi dei Rischi 231").
 - Livello di Rischio (anche in questo caso si rimanda all'appendice sopra citata).
- Per ogni Gruppo di Reati vengono riportati:
 - Effettività.
 - Benefici.
 - Soggetti coinvolti.
 - Frequenza.
 - Gravità.
 - Livello di Rischio
- Per ogni Reato presupposto viene riportato:
 - Illecito nel quale è richiamato con i relativi dati.
 - Gruppo di Reati nel quale è stato accorpato con i relativi dati.
 - Reato presupposto (con anche un campo per l'ordinamento dei reati es "02" al posto di "bis").
 - Data di inserimento come reato presupposto.
 - Data di eventuale ultima modifica successiva.
 - Quote minime e massime previste.
 - Mesi minimi e massimi previsti per l'interdizione.
 - Gravità.
- In un ultimo foglio viene presentato, per ogni Illecito i Gruppi di Reati coinvolti con:
 - Gravità.
 - Livello di Rischio.

Azioni a Rischio, Pericoli e Punti di Controllo.

- Per le Azioni a Rischio viene riportato:
 - Processo.
 - Attività
 - Azione a Rischio
 - Numero di Pericoli connessi all'Azione.
 - Numero di Punti di Controllo connessi all'Azione.
- Nel foglio "Pericoli" vengono riportati:
 - Processo, Attività e Azione e Rischio.
 - Gruppo di Reati.
 - Pericoli previsti.

- Nel foglio “Punti di Controllo” vengono riportati:
 - Processo, Attività e Azione e Rischio.
 - Processo, Attività e Punto di Controllo collegati all’Azione a Rischio.
- Nel foglio “Correla” vengono riportati:
 - Processo, Attività e Azione e Rischio.
 - Gruppo di Reati e Pericolo.
 - Processo, Attività e Punto di Controllo collegati al pericolo.
- Nel foglio “Correla_Modifica” vengono presentati:
 - Per ogni Processo, Attività e Azione e Rischio.
 - Gruppo di Reati e Pericolo.
 - Tutti i Punti di Controllo collegati all’Azione a Rischio.
 - L’indicazione di quali è effettivamente collegato [in base ai valori di Probabilità definiti per ogni Gruppo di Reati] (con una “X”). L’utente può sostituire la “X” con una “T” se desidera togliere la correlazione o inserire della “A” se vuole aggiungere una nuova correlazione. Il file così modificato potrà essere importato attraverso la funzione descritte di seguito.

Stampe dei Reati

È possibile ottenere la stampa dei Reati secondo molti formati in base ad una serie di impostazioni. Vengono già fornite alcune tipologie di Stampe ma ogni utente può crearne altre.

Ogni tipo di stampa è caratterizzata da:

- Un codice ed una descrizione.
- L’intestazione che apparirà come titolo della stampa.
- È possibile scegliere alcune stampe speciali (alcuni dei parametri successivi non saranno significativi).
- 4 Livelli dove è possibile indicare la priorità fra i vari elementi.
- È possibile richiedere una illustrazione di alcuni dei Reati presupposto.
- È possibile indicare se e come si desidera vengano presentati i Processi.
- Per gli Illeciti 231 è possibile richiedere la stampa del testo dell’Articolo, delle Caratteristiche (Data di introduzione nel Decreto, Quote minime e massime previste, eventuale presenza dell’interdizione e data dell’eventuale ultima modifica) e dei Sotto Illeciti (raggruppamento dei Reati presupposto per sanzioni previste).
- Per i Reati presupposto è possibile richiedere la stampa del testo dell’Articolo e di alcune Caratteristiche (Data di inserimento nel Decreto, Ultima modifica, Quote minime e massime previste, Durata dell’interdizione espressa in mesi minimi e massimi. Vengono, inoltre, inserite ulteriori indicazioni relative al Reato).

NOTA: Si suggerisce di salvare la stampa descrittiva degli Illeciti e dei Reati presupposto al momento di ogni aggiornamento del Modello.

In ogni momento sarà possibile richiedere lo stesso tipo di stampa ed effettuare (utilizzando le normali funzionalità di word) un “confronto” fra i documenti per verificare le modifiche apportate dal legislatore.

Stampe dei Punti di Controllo

È possibile ottenere la stampa dei Punti di Controllo secondo molti formati in base ad una serie di impostazioni.

Vengono già fornite alcune tipologie di Stampe ma ogni utente può crearne altre.

Ogni tipo di stampa è caratterizzata da:

- Un codice ed una descrizione.
- L'intestazione che apparirà come titolo della stampa.
- È possibile definire la specificità della stampa (ordine di presentazione delle varie informazioni).
- È possibile richiedere la descrizione del Punto di Controllo (oltre al Codice ed al Titolo).
- È possibile richiedere di esplicitare gli Illeciti che il Punto di Controllo può prevenire.

Rappresentazioni grafiche

È possibile ottenere una rappresentazione grafica delle relazioni fra Illeciti, Reati, Azioni a Rischio secondo molti formati in base ad una serie di impostazioni.

Vengono già fornite alcune tipologie di rappresentazioni ma ogni utente può crearne altre.

Ogni tipo di rappresentazione è caratterizzata da:

- Un codice ed una descrizione.
- È possibile indicare se si desidera rappresentare unicamente un elemento (uno specifico Illecito, uno specifico Gruppo di Reati o un singolo Processo).
- È possibile indicare quali dei 7 elementi visualizzare.
- La rappresentazione può presentare l'altezza dei vari Illeciti proporzionale alla Gravità (data dalle pene massime e minime previste dal Legislatore) o proporzionale al Livello di Rischio (Gravità per Probabilità); nel secondo caso non verranno presentati gli Illeciti non ritenuti significativi.
- È possibile definire l'Altezza e la Larghezza del grafico (da personalizzare in funzione del numero di informazioni richieste).

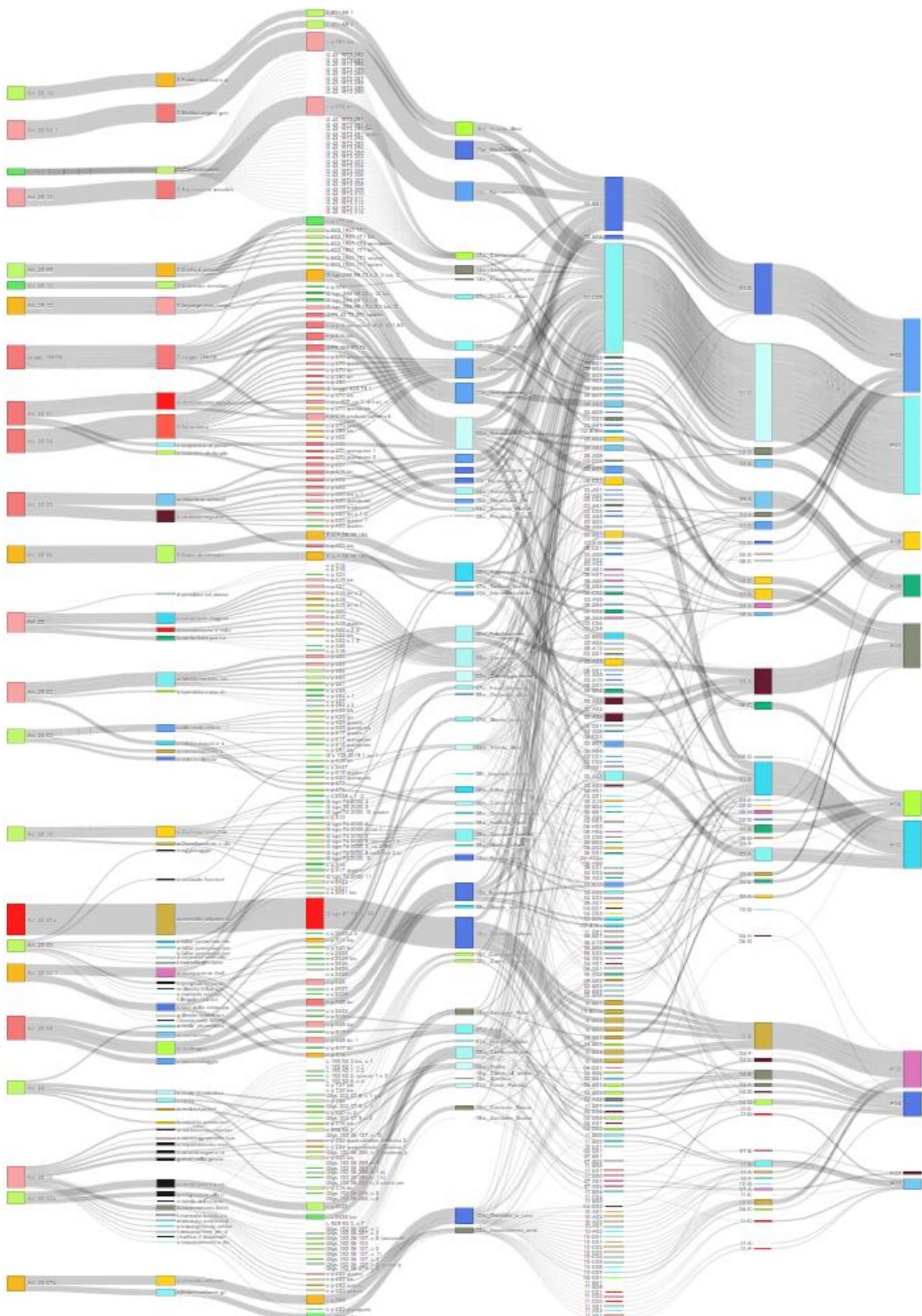
Nella figura riportata nella pagina seguente sono riportati, partendo da sinistra, nelle colonne le seguenti informazioni:

- Illecito 231.
- Sotto Illeciti (raggruppati per le sanzioni previste dal Legislatore).
- Reati presupposto.
- Gruppi omogenei di Reati.
- Azioni a Rischio.
- Attività.
- Processi.

L'altezza dei vari elementi corrisponde a:

- Per gli Illeciti è proporzionale alla Gravità.
- Per i singoli Reati presupposto è proporzionale alla Gravità di ogni Reato e assicurando che la somma delle altezze coincida con l'altezza dell'Illecito.
- Per i vari Gruppi di Reati corrisponde alla somma delle altezze dei Reati relativi.
- Per le varie Azioni a Rischio corrisponde alla somma delle suddivisioni dell'altezza dei Gruppi di Reati in parti uguali.
- Per le Attività ed i Processi alla somma delle altezze delle Azioni a Rischio.

I flussi fra i vari elementi indicano le varie relazioni.



Analisi aziendale

Viene prodotto un documento che riassume i principali controlli e segnala le principali criticità potenziali.

Aggiornamento correlazione

Come descritto precedentemente è possibile collegare ogni PdC a vari Pericoli (che a loro volta sono collegati agli Illeciti). È possibile richiedere l'aggiornamento, in funzione di questi collegamenti, delle Correlazioni dei vari PdC con gli Illeciti e del Livello (Normale o Critico in base al Livello dei Pericoli e del valore di soglia definito in MOG / MOG Approvato / Analisi Modello Approvato: Metodo e Intervalli).

È consigliabile prima verificare l'ipotesi e solo dopo chiedere l'Aggiornamento effettivo.

Aggiornamento Livello di Rischio Calcolato

Come descritto precedentemente è possibile definire, ogni Gruppo di Reati gli elementi che permettono di determinare il Livello di Rischio.

È possibile richiedere che il Livello di Rischio Calcolato per ogni Illecito (MOG / MOG Approvato / Analisi Modello Approvato: Livelli di Rischio) venga aggiornato con il massimo Livello di Rischio fra i Gruppi di Reati racchiusi per ogni Illecito.

È consigliabile prima verificare l'ipotesi e solo dopo chiedere l'Aggiornamento effettivo.

Creazione degli elementi standard

Per facilitare l'avvio del sistema è possibile richiedere la creazione di elementi standard.

Verranno create:

- Azioni a rischio.
- Valutazioni “generiche” sui Gruppi di Reati.
- Pericoli “generici”.

È necessario che l'Ente personalizzi gli elementi importati.

Creazione degli elementi standard

In caso di modifica degli Illeciti o dei Reati presupposto da parte del Legislatore è opportuno provvedere all'Aggiornamento dei Gruppi di Reati.

Importazione Pericoli

È possibile richiedere anche l'importazione dei Pericoli ritenuti significativi per l'Ente.

Come già descritto, nell'esportazione “Azioni a Rischio, Pericoli e Punti di Controllo” vengono proposti dei Pericoli di riferimento nel foglio “Correla_Modifica”.

L'utente può sostituire le “X” con “T” se desidera togliere la correlazione o inserire della “A” se vuole aggiungere una nuova correlazione. Il file così modificato potrà essere importato.

Interviste

Per le imprese che devono effettuare una Analisi dei Rischi questa può basarsi su delle interviste che dovranno coinvolgere tutti i principali responsabili di settore ed eventuali titolari di deleghe o procure specifiche e non solo le figure apicali (ai sensi del DLgs. 231/01).



Le interviste potranno essere svolte sulla base di vari questionari compilabili via WEB (esempi di Questionari sono presenti sotto VARIE / DOCUMENTI DI SUPPORTO) che permettono di svolgere una indagine di dettaglio con lo scopo di raccogliere e documentare l'attuale livello organizzativo dell'Ente sia nel suo complesso che per i singoli Processi e di ottenere una valutazione sui rischi legati alla commissione dei vari reati previsti dal DLgs. 231/01.

Permetteranno, quindi, di fornire elementi oggettivi sui quali basare la successiva costruzione del Modello.

Tutti i dati raccolti nelle interviste potranno essere inseriti su SQuadra231 per essere elaborati e fornire una prima Analisi dei Rischi sulla base delle indicazioni riportate nella successiva APPENDICE: Analisi dei Rischi.

Importazione Questionari

Per ogni intervista è possibile riempire il Testo Base in formato excel fornito dal programma (“Base per Questionari”).

Nel file andranno riportate, nel foglio “Questionari”, le valutazioni su:

- Organizzazione dell’ENTE: Requisiti organizzativi aziendali.
- Analisi per Processo: Regolazione, per le funzioni svolte nei vari Processi. Verrà indicata anche il coinvolgimento nelle attività del Processo.
- Analisi per Gruppi di Reati: Valutazione dell’Effettività, dei Benefici, dei Soggetti coinvolti e della Frequenza delle operazioni per i vari Gruppi di Reati.

Il file andrà salvato su SQuadra e quindi è possibile richiedere l’importazione delle informazioni inserite nei Questionari.

Importazione Pericoli

Una volta importati i dati dei Questionari è possibile richiedere una ipotesi di Pericoli relativi ai Processi di interesse e per i Reati ritenuti significativi per l’ENTE (“Base per Pericoli”).

NOTA: Si ricorda che è opportuno valutare le Azioni a Rischio significative per l’Ente. Ovviamente verranno proposti solo i Pericoli relativi alle Azioni a Rischio significative.

Nel file sono riportati i dati ricavati dai Questionari e una ipotesi di Pericoli potenziali.

È possibile eliminare Pericoli non ritenuti significativi e aggiungerne di nuovi associandoli alle Azioni previste (riportate nel foglio Azioni) ed ai Gruppi di Reati.

È anche possibile variare il Livello del Pericolo (un numero fra 1 e 10).

Una volta salvato il file i Pericoli possono essere importati.

Manutenzione manuale

I dati possono anche essere inseriti direttamente o modificati nelle apposite maschere correlate alla intervista.

Stampa della singola intervista

I dati così definiti possono essere stampati per farli firmare dall'intervistato ed è opportuno che la scannerizzazione venga memorizzata nel campo File PDF.

Analisi di tutte le interviste

I dati registrati per le varie interviste permettono di ottenere un riepilogo a livello di Ente.

Per una descrizione dei vari Fogli si rimanda all'Appendice: "Analisi dei Rischi 231".

Una volta controllato il documento di analisi è possibile richiedere di aggiornare i dati dell'Ente.

Verranno aggiornate le valutazioni sulla probabilità per i vari Gruppi di Reati e i Livelli di Rischio per ogni Illecito 231 .

Analisi del Rischio Residuo Rilevato

Una corretta applicazione del Modello garantisce la riduzione del Livello di Rischio ad un livello di Rischio Residuo accettabile. Si rimanda all'apposita Appendice per una analisi di dettaglio del Rischio Residuo Rilevato.

SQquadra231 permette di valutare la percentuale di conformità per ogni Reato in base alla correlazione con le varie Procedure e il risultato degli Audit o delle Informative ricevute dalle Funzioni Aziendali responsabili dei Controlli di primo livello.

Verranno, ovviamente, considerati solo gli ultimi Audit / Informative considerati "Validi".

La valutazione può servire come base alle valutazioni che l'OdV deve effettuare all'interno delle Relazioni che periodicamente predisporre per gli Organi di direzione e di controllo della Società.

È necessario indicare la data rispetto alla quale viene effettuato il calcolo (si ricorda che le valutazioni di conformità "decadono" con il passare del tempo).

Se si desidera i risultati del calcolo possono essere riportati nella valutazione dei rischi legati ad una specifica relazione dell'OdV (ovviamente è prima necessario definire la Relazione di interesse).

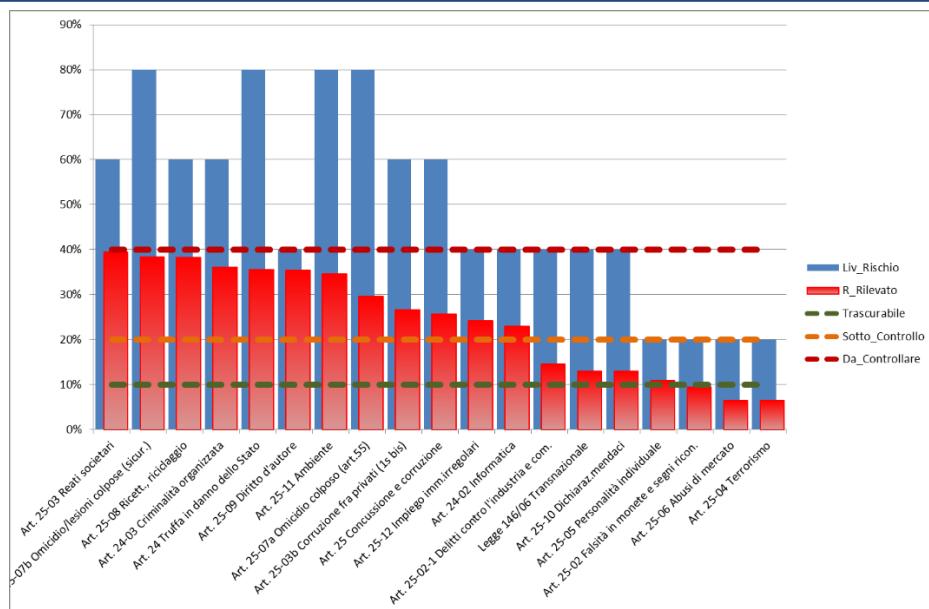
Calcoli

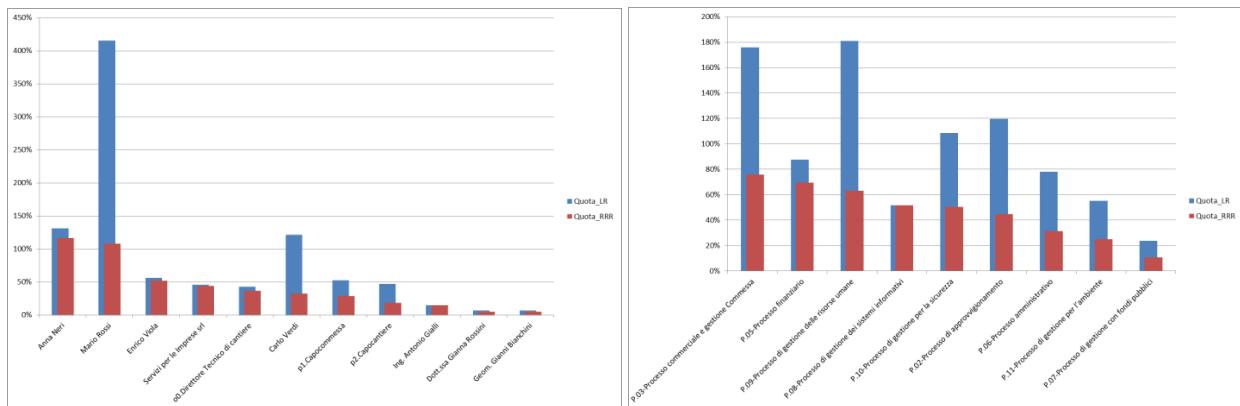
Il Documento contiene vari fogli:

- **Parametri:** nel quale vengono riportati i dati essenziali
- **Responsabili:** nel quale sono indicati tutte le Persone che ricoprono Funzioni Aziendali sia Singole che Multiple. Per ogni Persona viene indicato lo stato rispetto alla Formazione ("Effettuata" o "Da effettuare") ed alle Nomine ("Corretta", "Da aggiornare" o "Da effettuare").
- **Audit Multipli:** in questo foglio vengono presentati i risultati di tutti gli Audit effettuati alle Funzioni Aziendali definite come multiple e, per ogni Procedura, vengono calcolati i valori medi. (Si ricorda che sarà compito dell'OdV valutare il giusto campionamento e considerare non più validi Audit troppo "vecchi" sostituiti da nuovi Audit ad altre persone con le stesse Funzioni).

- **Procedure:** vengono presentati, per ogni Procedura, i risultati dell'ultimo Audit; per le Procedure assegnate a Funzioni "multiple" vengono presentati i valori medi.
- **Governance:** vengono presentati i vari elementi che contribuiscono a formare una valutazione sulla Governance aziendale.
- **Correlazione:** in questo foglio viene presentata, per ogni Procedura, il livello di correlazione con i vari Reati o elementi di Governance. Vengono inoltre riportati, per permettere di effettuare elaborazioni aggiuntive, il Rischio Lordo di riferimento, la Quota di Correlazione, la Quota di Conformità rilevata in base agli Audit, la Quota di Rischio legata alla specifica Procedura e, infine, la Quota di Non Conformità.
- **Corr_Resp:** è un foglio che contiene calcoli intermedi.
- **Reati:** in questo foglio viene riportato il risultato finale dell'analisi dei Rischi così come rilevati in base agli audit ed al controllo della Formazione e della Nomine. Vengono anche riportati, per controllo, i dati numerici ottenuti in maniera alternativa dagli elementi di dettaglio.
- **Funzioni:** i dati relativi al Rischio Rilevato di cui al foglio precedente vengono presentati suddivisi per Responsabile o, per le funzioni multiple, per Funzione. Queste informazioni possono servire ad orientare le attività dell'OdV.
- **Processi:** i dati relativi al Rischio Rilevato – per la sola parte correlata con gli Audit - vengono presentati suddivisi per Processo. Queste informazioni possono servire ad individuare i Processi da tenere maggiormente sotto controllo.
- **G_Reati:** Rappresentazione grafica dei Rischi Rilevati.
- **G_Funzioni:** Rappresentazione grafica del livello di Non Conformità a carico di ogni Funzione.
- **G_Processi:** Rappresentazione grafica del livello di Non Conformità per ogni Processo.

Reato	Punti	Audit_Reati	Governan	Conf_Tot	Liv_Risch	R_Rilevato	Valutazione
Art. 24 Truffa in danno dello Stato	22,0	58,693%	46,044%	55,531%	80%	35,575%	C.Da tenere sotto controllo
Art. 24-02 Informatica	4,5	41,667%	46,044%	42,761%	40%	22,896%	C.Da tenere sotto controllo
Art. 24-03 Criminalità organizzata	27,0	37,870%	46,044%	39,914%	60%	36,052%	C.Da tenere sotto controllo
Art. 25 Concussione e corruzione	18,5	60,878%	46,044%	57,170%	60%	25,698%	C.Da tenere sotto controllo
Art. 25-02 Falsità in monete e segni ricon.	5,0	55,000%	46,044%	52,761%	20%	9,448%	A.Trascrabile
Art. 25-02-1 Delitti contro l'industria e com.	6,5	69,423%	46,044%	63,578%	40%	14,569%	B.Sotto controllo
Art. 25-03 Reati societari	16,5	30,303%	46,044%	34,238%	60%	39,457%	C.Da tenere sotto controllo
Art. 25-03b Corruzione fra privati (1s bis)	17,0	58,897%	46,044%	55,684%	60%	26,590%	C.Da tenere sotto controllo
Art. 25-04 Terrorismo	2,0	75,000%	46,044%	67,761%	20%	6,448%	A.Trascrabile
Art. 25-05 Personalità individuale	5,0	45,000%	46,044%	45,261%	20%	10,948%	B.Sotto controllo
Art. 25-06 Abusi di mercato	1,0	75,000%	46,044%	67,761%	20%	6,448%	A.Trascrabile
Art. 25-07a Omicidio colposo (art.55)	4,0	68,750%	46,044%	63,074%	80%	29,541%	C.Da tenere sotto controllo
Art. 25-07b Omicidio/lesioni colpose (sicur.)	23,5	54,043%	46,044%	52,043%	80%	38,366%	C.Da tenere sotto controllo
Art. 25-08 Ricett., riciclaggio	18,5	33,108%	46,044%	36,342%	60%	38,195%	C.Da tenere sotto controllo
Art. 25-09 Diritto d'autore	2,0	0,000%	46,044%	11,511%	40%	35,396%	C.Da tenere sotto controllo
Art. 25-10 Dichiaraz.mendaci	1,0	75,000%	46,044%	67,761%	40%	12,896%	B.Sotto controllo
Art. 25-11 Ambiente	16,5	60,303%	46,044%	56,738%	80%	34,609%	C.Da tenere sotto controllo
Art. 25-12 Impiego imm.irregolari	4,0	37,500%	46,044%	39,636%	40%	24,146%	C.Da tenere sotto controllo
Legge 146/06 Transnazionale	2,0	75,000%	46,044%	67,761%	40%	12,896%	B.Sotto controllo





Visualizzazione Rischio Residuo Rilevato

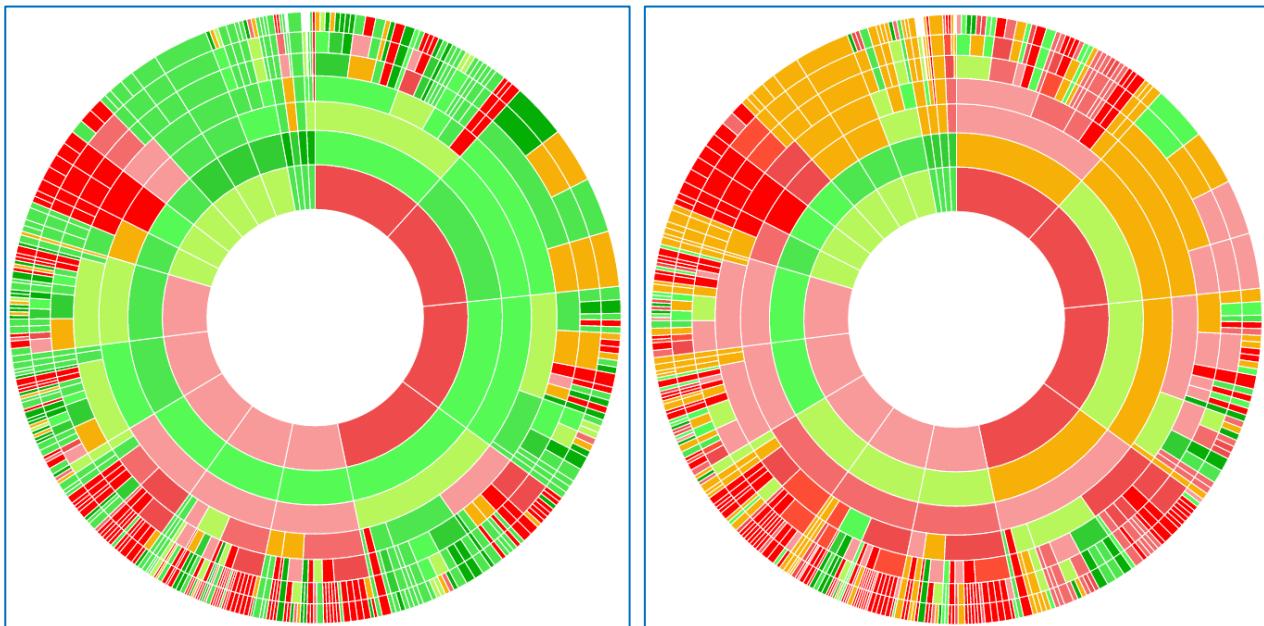
Anche per il Rischio Rilevato è possibile richiedere una visualizzazione per Reati e Processi.

Cerchio dei Rischi Residui Rilevati

Come già visto per le correlazioni anche per il Rischio Residuo Rilevato è possibile richiedere una rappresentazione “circolare”.

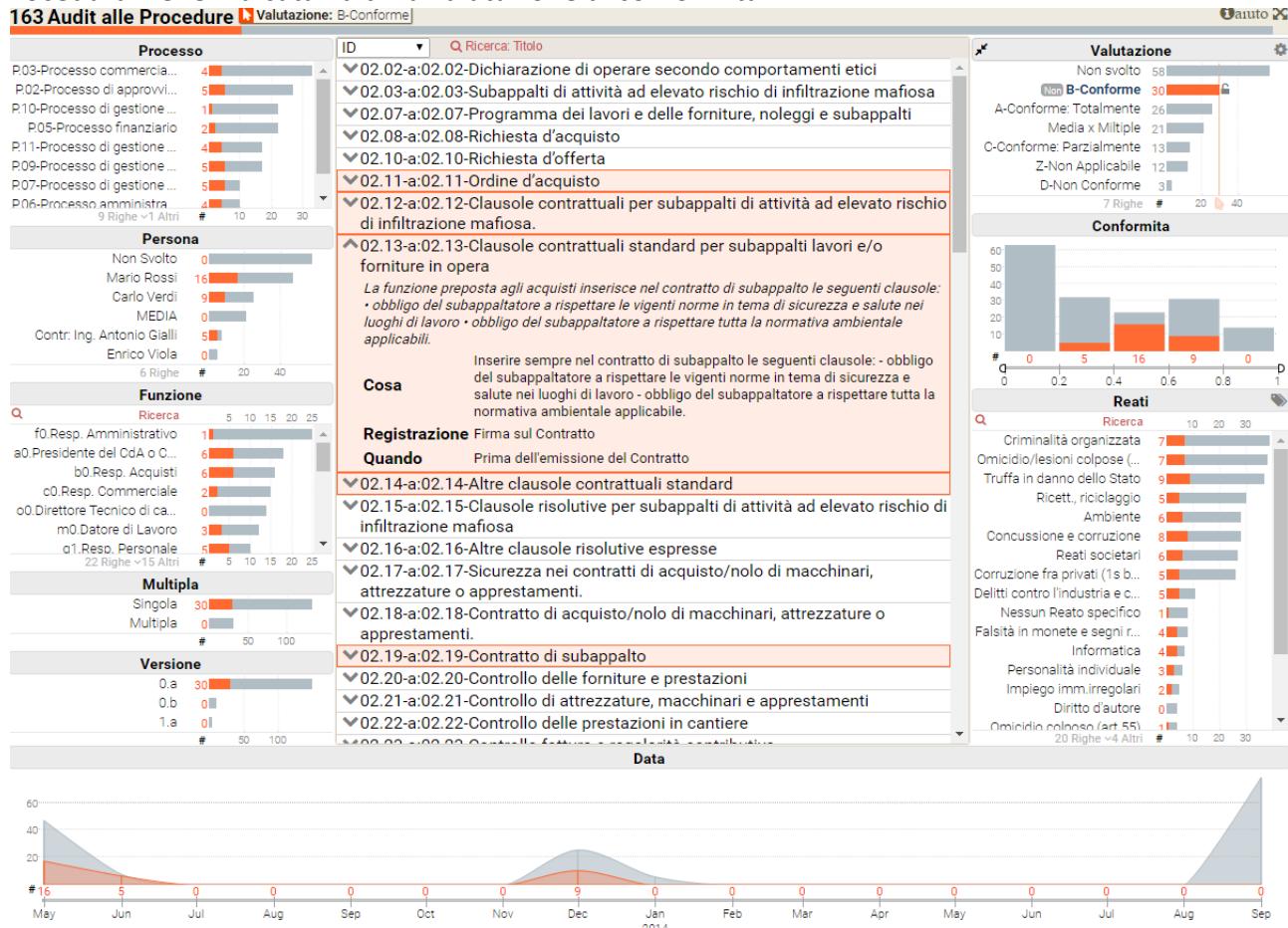
Anche in questo caso si è scelta una rappresentazione dei rischi “quadratica” per evidenziare maggiormente i rischi maggiori.

Nella figura sono riportati i valori relativi ad un anno nel quale sono stati svolti regolari audit e il risultato che si avrebbe considerando il decadimento legato al tempo qualora non venissero più effettuati audit nell'anno successivo.



Presentazione del Rischio Residuo Rilevato

È possibile ottenere un Cruscotto per la presentazione del Rischio Rilevato nella quale, per ogni Procedura viene indicata l'ultima valutazione di conformità.



Per il funzionamento dei Cruscotti si rimanda alle indicazioni presenti nel capitolo relativo all'interno della Sezione "Caratteristiche generali di SQuadra".

Andamento del Rischio Residuo Rilevato nel tempo

SQuadra231 fornisce una sintesi sull'andamento storico del Rischio Rilevato evidenziando tutti gli eventi (Audit, Informativa, attività di formazione, ecc.) che portano le variazioni "discrete" al valore del Rischio Rilevato (si ricorda che il tempo porta variazioni "continue" del Rischio Rilevato in funzione del "decadimento" della Conformità rilevata).

Evento	Totale	Art. 24 Tr	Art. 24-02	Art. 24-03	Art. 25 Cx	Art. 25-02	Art. 25-02	Art. 25-03	Art. 25-04	Art. 25-05	Art. 25-06	Art. 25-07	Art. 25-08	Art. 25-09	Art. 25-10	Art. 25-11	Art. 25-12	Legge 14
01/01/13-A-Versione Prima Versione	47,00	4,00	2,00	3,00	3,00	1,00	2,00	3,00	1,00	1,00	1,00	4,00	4,00	3,00	2,00	2,00	2,00	
05/02/13-B-Formazione e Nomine: Anna Neri, Carlo V...	46,15	3,93	1,96	2,95	2,95	0,98	1,96	2,95	2,95	0,98	0,98	3,93	3,93	2,95	1,96	1,96	1,96	
06/03/13-B-Formazione e Nomine: Geom. Gianni Bia...	45,97	3,91	1,96	2,93	2,93	0,98	1,96	2,93	2,93	0,98	0,98	3,91	3,91	2,93	1,96	1,96	1,96	
06/04/13-B-Formazione e Nomine: Dott.ssa Gianna F...	45,87	3,90	1,95	2,93	2,93	0,98	1,95	2,93	2,93	0,98	0,98	3,90	3,90	2,93	1,95	1,95	1,95	
07/05/13-C-Audit: Mario Rossi.	29,81	2,70	1,19	2,13	1,65	0,68	1,47	2,21	1,75	0,35	0,68	0,35	1,57	3,09	2,25	1,82	0,69	3,00
19/06/13-C-Audit: Carlo Verdi.	24,74	2,47	1,15	1,68	1,40	0,38	0,76	1,96	1,44	0,32	0,66	0,32	1,49	2,29	1,93	1,77	0,65	1,93
20/06/13-D-Informativa con Controlli: Ing. Antonio Gia...	22,07	1,97	1,12	1,61	1,27	0,37	0,74	1,87	1,30	0,31	0,54	0,31	1,44	1,58	1,85	1,75	0,62	1,61
01/07/13-A-Versione Revisione Prima Versione	23,62	2,02	1,15	1,92	1,43	0,38	0,77	1,91	1,52	0,33	0,55	0,33	1,49	1,89	1,98	1,78	0,65	1,66
19/07/13-C-Audit: Ing. Enrico Milano.	22,05	1,65	1,14	1,84	1,26	0,37	0,55	1,89	1,33	0,32	0,54	0,32	1,46	1,73	1,96	1,76	0,64	1,45
25/07/13-C-Audit: Ing.Cira Napoli.	22,43	1,73	1,14	1,84	1,29	0,38	0,62	1,90	1,36	0,32	0,54	0,32	1,47	1,79	1,96	1,76	0,64	1,53
20/12/13-C-Audit: Carlo Verdi.	22,73	1,77	1,14	1,79	1,28	0,47	0,72	1,96	1,32	0,32	0,54	0,32	1,46	1,78	1,90	1,76	0,64	1,72
01/01/14-A-Versione 1.a - Versione rivista per modifica...	23,53	1,86	1,15	1,80	1,43	0,47	0,74	1,99	1,49	0,32	0,57	0,32	1,48	1,89	1,92	1,77	0,65	1,78
15/01/14-C-Audit: Enrico Viola.	21,28	1,61	0,56	1,79	1,42	0,47	0,73	1,98	1,48	0,32	0,56	0,32	1,48	1,88	1,92	0,46	0,64	1,25
22/09/14-Z-Ultima rilevazione	26,77	2,27	0,76	2,00	1,80	0,55	0,93	2,20	1,84	0,49	0,69	0,49	2,08	2,42	2,12	0,50	0,97	2,20

1.3 Sistemi informativi e Privacy

Si consiglia la consultazione dell'Appendice relativa al Regolamento Europeo per la protezione dei dati personali.

1.3.1 Analisi del Sistema

GDPR: Art. 24 comma 1: "Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario."

Questa sezione di SQuadra consente alla società di analizzare il contesto e predisporre misure di carattere generale che andranno periodicamente riesaminate.

1.3.1.1 Conformità

È possibile effettuare una analisi della conformità del proprio Sistema relativamente alla gestione dei dati personali.

Vengono proposti una serie di Argomenti ma è possibile aggiungerne di specifici.

Ogni Argomento è caratterizzato da:

- Tipologia.
- Codice e Argomento.
- Sede/Oggetto (da utilizzare quando lo stesso Argomento deve essere ripetuto più volte ad esempio in caso di differenti sedi o insieme di dati).
- Significatività (per dare un peso relativo ai vari Argomenti).
- Conformità valutata.
- Misure attualmente poste in atto.
- Note interne.

È possibile descrivere le eventuali Misure Aggiuntive:

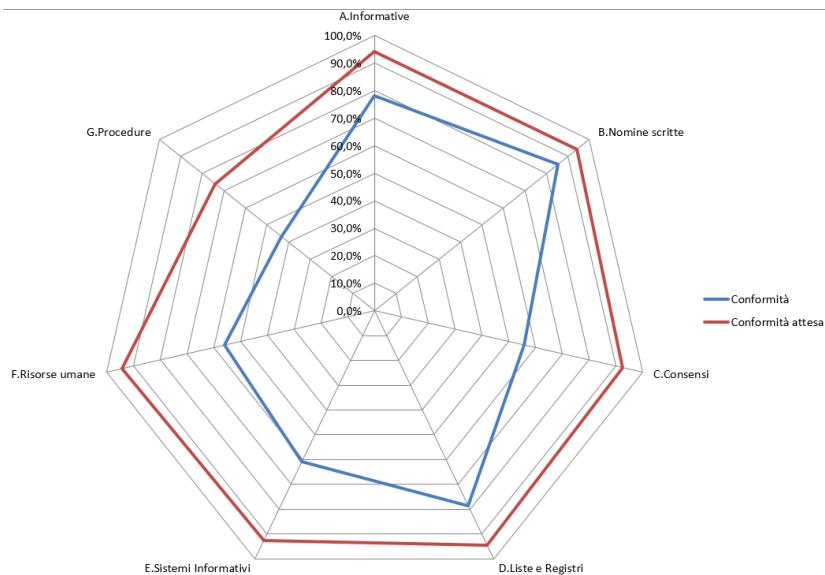
- Misure aggiuntive previste per migliorare la conformità.
- Responsabile delle Misure Aggiuntive.
- Risorse messe a disposizione per l'attuazione delle Misure Aggiuntive.
- Tempi entro i quali devono essere attuate le Misure Aggiuntive.
- Criteri per la Valutazione della corretta attuazione delle Misure Aggiuntive.
- Conformità attesa in funzione della corretta applicazione delle Misure Aggiuntive.

Report di Conformità

Per ottenere il Report è necessario definire i dati di interesse e quindi premere Salva.

Apparirà il bottone “Report di Conformità” che produrrà un documento di Word.

NOTA: Da “Sistema Informatico” (vedi avanti) è possibile ottenere il Report SGSI complessivo all'interno del quale sono riportati i dati relativi alla Conformità attuale ed attesa.



NOTA: È possibile ottenere il riepilogo delle attività previste per i vari Responsabili in “Sistema Informatico”.

1.3.1.2 Minacce

SQuadra permette di analizzare le Minacce al Sistema Informativo e di descrivere le misure adottate per mitigare. Vengono proposte quelle di default che potranno essere liberamente modificate.

L'analisi delle Minacce è descritta su SQuadra a cura del Responsabile del Sistema Informatico.

Per ogni minaccia viene definito:

- Un Codice.
- La Tipologia (Eventi Naturali, Fisici Intenzionali, Problemi tecnici, ecc.).
- La Descrizione della minaccia.
- Oggetto di riferimento (in caso di più sedi o divisioni).
- Probabilità e Gravità (dalle quali viene calcolato il livello di Rischio) – Si veda l'appendice sul SGSI.
- Misure attuali.
- Impatto della minaccia su: Riservatezza, Integrità e Disponibilità.
- Note interne (ad esempio: gli impatti attesi ove la minaccia si concretizzi, gli effetti visibili della minaccia, il comportamento suggerito all'utente che scopre il danno, il comportamento suggerito al responsabile per il primo intervento, ecc.).
- Riferimento alle Minacce Generiche previste nell'Appendice del documento “Metodologia per la gestione del rischio sulla privacy” prodotto da CNIL (Commissione francese per la privacy).

Per la valutazione delle probabilità di accadimento delle minacce si consiglia di adottare una stima di tipo qualitativo, prodotta dalla interpretazione soggettiva del fenomeno effettuata dal referente (cioè dalla persona o dal gruppo di persone che in azienda ha più esperienza sull'argomento, e/o ne detiene la responsabilità).

Il termine “soggettivo” non deve essere inteso come arbitrario; la valutazione dei rischi con approccio soggettivo è da considerarsi in questo contesto come “valutazione da esperto”, legata cioè alla professionalità derivante dall'esperienza e dalla conoscenza dei molteplici fattori in gioco.

In tal senso l'approccio qualitativo, se ben supportato da una adeguata metodologia di impiego, viene considerato teoricamente corretto, e può beneficiare di alcuni vantaggi rispetto all'approccio quantitativo, come la possibilità di tener conto anche di fattori non quantificabili, di essere collegato alla situazione reale vissuta quotidianamente dall'azienda e di permettere un riesame senza attendere la registrazione degli eventi; ovviamente occorre, nel tempo, utilizzare l'analisi della registrazione storica degli eventi legati alla classificazione dei rischi come strumento di verifica e controllo della stima qualitativa.

Nello stimare la probabilità di accadimento di un evento dannoso il referente valuta, sulla base della sua esperienza:

- La frequenza e la intensità con cui la minaccia si può presentare.

- La presenza di vulnerabilità utilizzabili dalla minaccia, non coperte dai controlli in essere ovvero l'esistenza e l'adeguatezza dei controlli di sicurezza esistenti.
- L'effettiva attuazione dei controlli di sicurezza in essere, coerentemente a quanto previsto dalle policy e dalle procedure di sicurezza.

Se il Rischio supera il livello basso è opportuno attuare misure aggiuntive tali da portare il rischio, una volta correttamente attuate, ad un livello accettabile.

Le contromisure consistono nella esecuzione di attività o adozione di comportamenti che possono portare a:

- *Eliminazione del rischio (ad esempio eliminazione della causa).*
- *Riduzione della probabilità di accadimento.*
- *Riduzione dell'impatto.*
- *Trasferimento o sterilizzazione del rischio (es. assicurazione o condizioni contrattuali concordate con il cliente).*

Ogni azione correttiva o preventiva intrapresa per contrastare il rischio residuo comporta un investimento direttamente proporzionale alla complessità generale della soluzione adottata, che deve essere commisurato al valore del bene da proteggere.

In questo caso andranno quindi definiti:

- Misure Aggiuntive.
- Responsabile dell'attuazione.
- Risorse messe a disposizione.
- Tempi previsti.
- Criteri per la valutazione dei risultati.
- Probabilità e Gravità attese in caso di corretta attuazione delle Misure Aggiuntive.

La valutazione delle minacce deve essere ripetuta in occasione dei riesami della sicurezza delle informazioni e in caso di cambiamenti significativi.

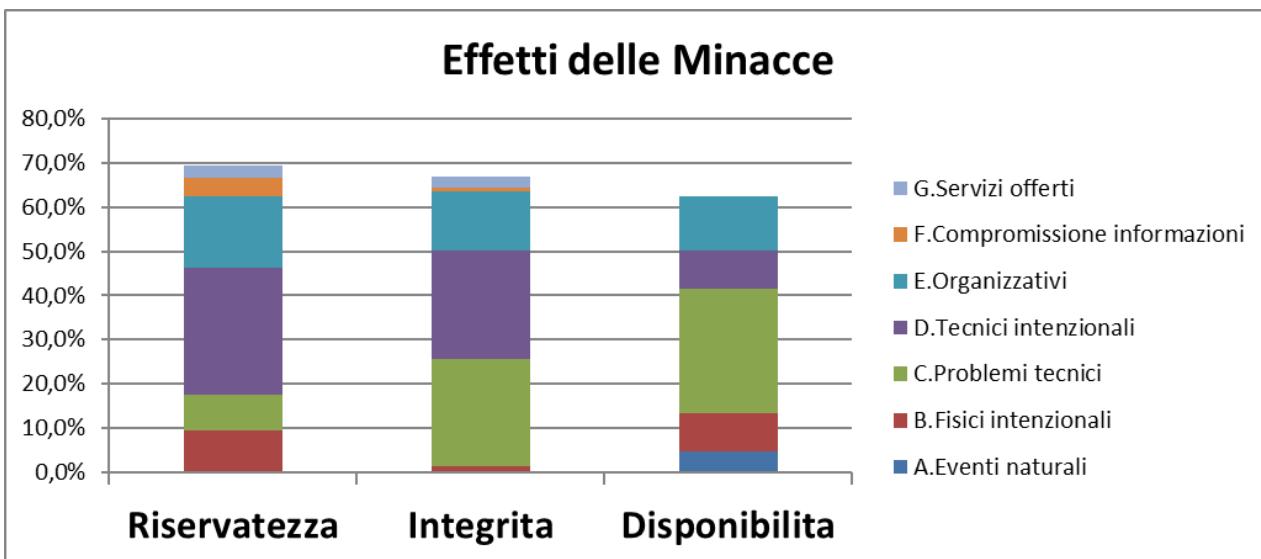
Il Report sul SGSI riporta una valutazione numerica sullo stato delle Minacce consentendo a chi esegue l'analisi la possibilità di iterare sulla fase di adozione contromisure fino a quando il rischio residuo risulta accettabile, lasciando evidenza della situazione in essere al momento dell'analisi, delle contromisure adottate e delle stime di riduzione fornite, del livello residuo del rischio.

I valori di probabilità e impatto ottenuti, per ogni minaccia, mediante l'adozione delle opportune contromisure costituiranno l'input per l'analisi che sarà svolta successivamente (ad una diversa data, e quindi su uno Report diverso).

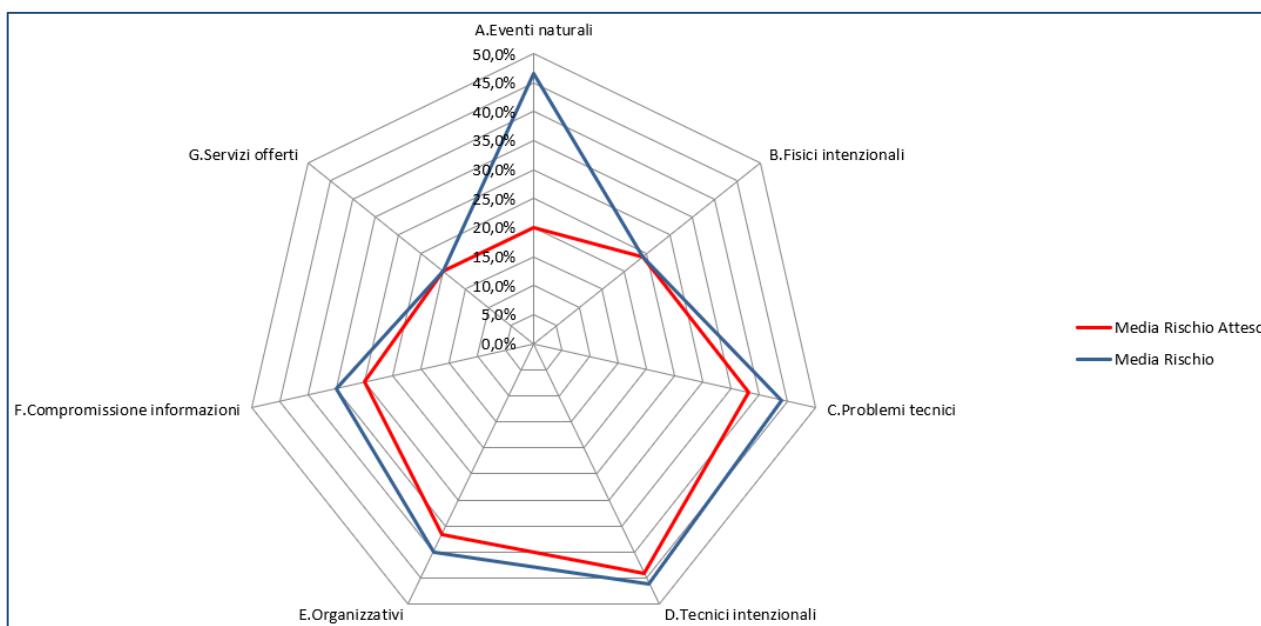
Report delle Minacce

È possibile ottenere un documento di Word con il report delle Minacce.

NOTA: Da "Sistema Informatico" (vedi avanti) è possibile ottenere il Report SGSI complessivo all'interno del quale sono riportati i dati relativi alle Minacce.



NOTA: Da “Sistema Informatico” (vedi avanti) è possibile ottenere il Report SGSI complessivo all’interno del quale sono riportati i dati relativi alla media dei Rischi attuali ed attesi delle Minacce per le varie tipologie.



NOTA: È possibile ottenere il riepilogo delle attività previste per i vari Responsabili in “Sistema Informatico”.

1.3.1.3 Controlli

Squadra permette di descrivere i Controlli effettuati sul Sistema informativo.

È possibile riferirsi a diversi standard illustrati nell’apposita Appendice.

Norma ISO 27001

Nell’Appendice A “Obiettivi di controllo e controlli di riferimento” della Norma ISO 27001 vengono proposti una serie di Controlli che vengono proposti e che potranno essere liberamente modificati.

Ogni Controllo è caratterizzato da:

- Area.
- Obiettivo.
- Codice e Descrizione.
- Controllo richiesto.

- Misure adottate.
- Note sull'applicazione.
- Riferimenti alle modalità di verifica. In fase di stampa è possibile raggruppare i Controlli per Riferimento⁷.
- Significatività del controllo.
- Valutazione sull'applicazione⁸.
- È inoltre possibile inserire un valore numerico (da 0 a 10) per indicare il Livello di Conformità.

Qualora le misure non sono ritenute idonee è opportuno prevedere misure aggiuntive indicando:

- Misure Aggiuntive.
- Responsabile dell'attuazione.
- Risorse messe a disposizione.
- Tempi previsti.
- Criteri per la valutazione dei risultati.
- Valutazione e Livello di Conformità attesi a seguito della corretta adozione delle Misure Aggiuntive.

Per ogni Controllo è possibile avere dei Suggerimenti.

Obiettivi dei Controlli

Vengono riportati gli Obiettivi per le varie Aree previste.

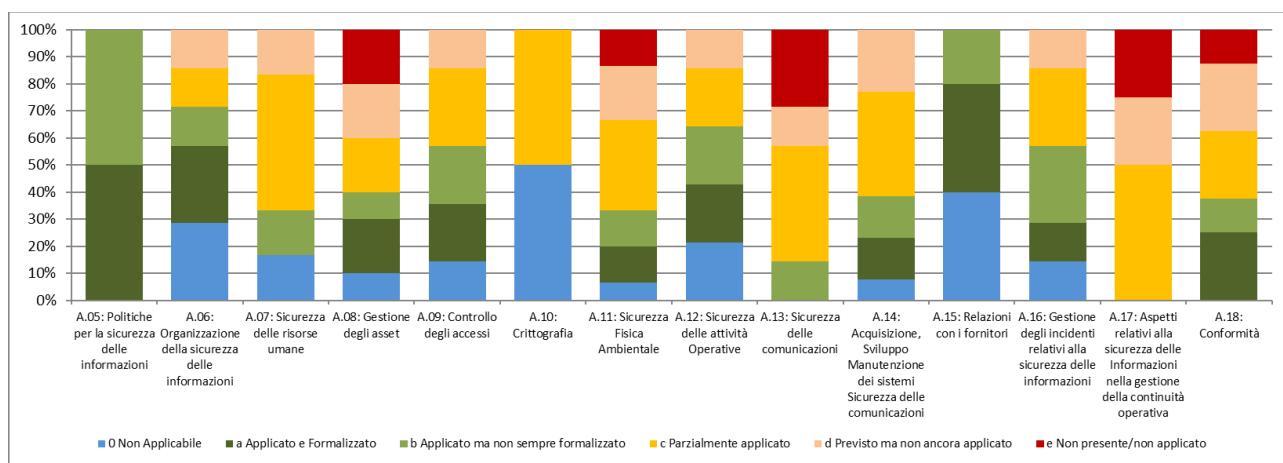
Ogni azienda può aggiungere nuovi Obiettivi.

Stampa dei Controlli

Per ottenere il Report è necessario definire i dati di interesse e quindi premere Salva.

Apparirà il bottone “Stampa Controlli” che produrrà un documento di Word.

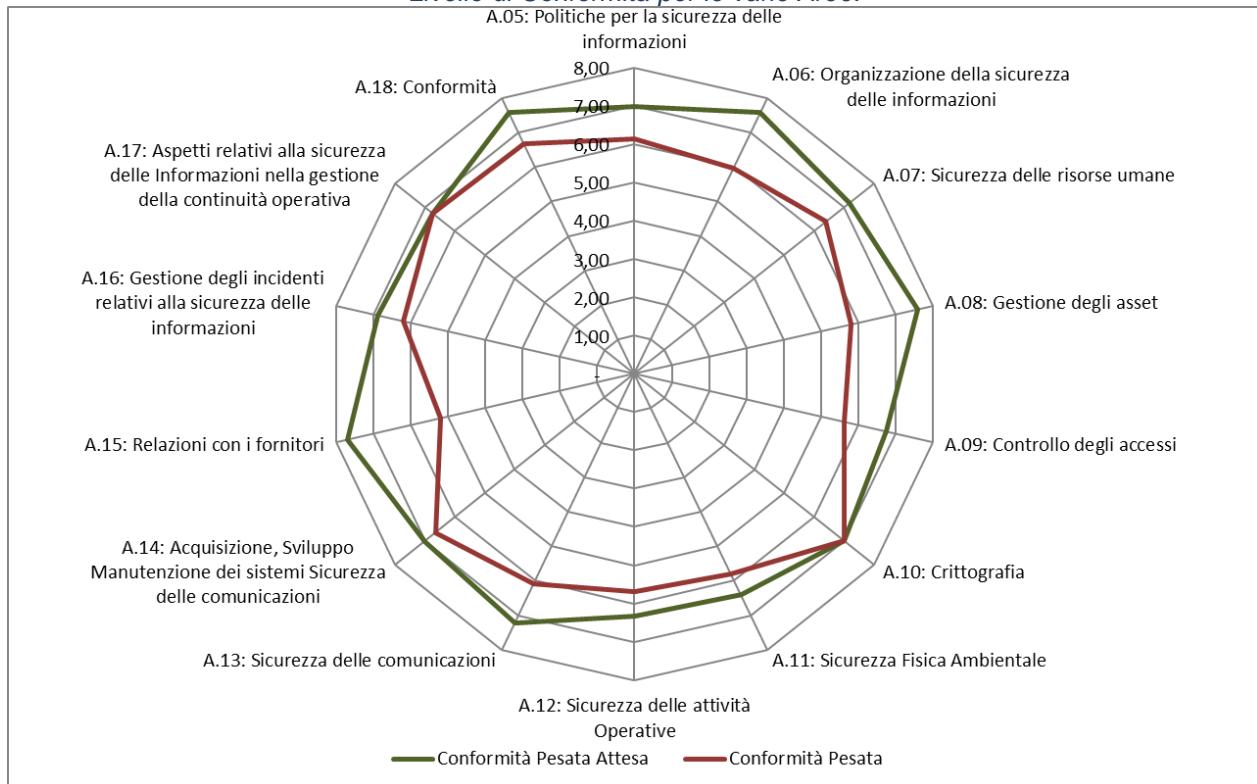
NOTA: Da “Sistema Informatico” (vedi avanti) è possibile ottenere il Report GDPR complessivo all'interno del quale sono riportati i dati relativi ai Controlli.



⁷ Se viene utilizzato il Modulo di SQuadra per il Riesame della Direzione i Riferimenti possono essere utilizzati anche per la preparazione del Riesame come indicato nella sezione del Manuale relativa al Riesame.

⁸ Per i criteri di valutazione sono state utilizzate le indicazioni riportate nella GAP Analysis ISO / IEC 27001 di CSQA Certificazioni Srl.

Livello di Conformità per le varie Aree.

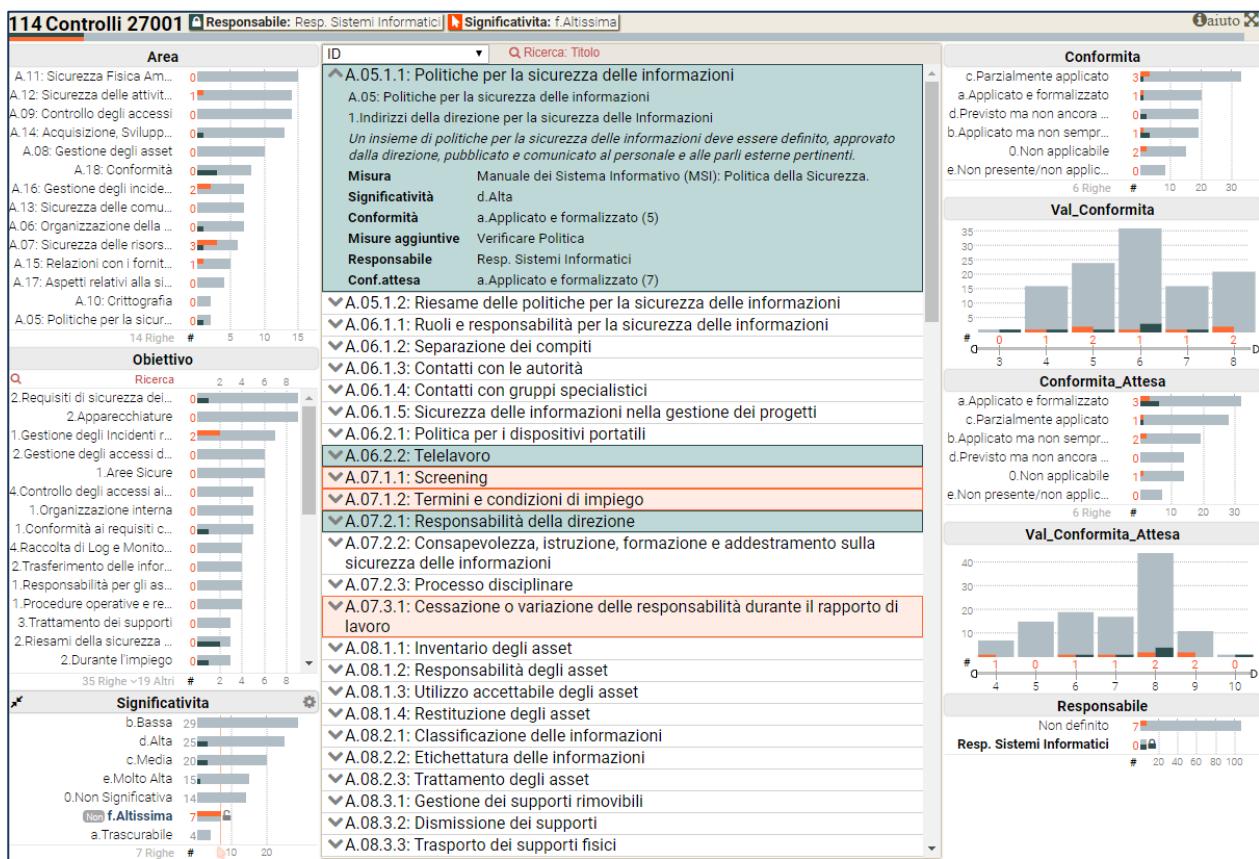


Raffronto fra Conformità rilevata e Conformità attesa in caso di corretta attuazione delle Misure Aggiuntive.

NOTA: È possibile ottenere il riepilogo delle attività previste per i vari Responsabili in “Sistema Informatico”.

Presentazione

È possibile avere una presentazione d'insieme relativa a tutti i Controlli.



Per il funzionamento dei Cruscotti si rimanda alle indicazioni presenti nel capitolo relativo all'interno della Sezione "Caratteristiche generali di SQuadra".

Storia

È possibile periodicamente, ad esempio in occasione dei Riesami, salvare le valutazioni riportate per poter analizzare l'andamento nel tempo della Conformità rispetto ai vari Controlli.

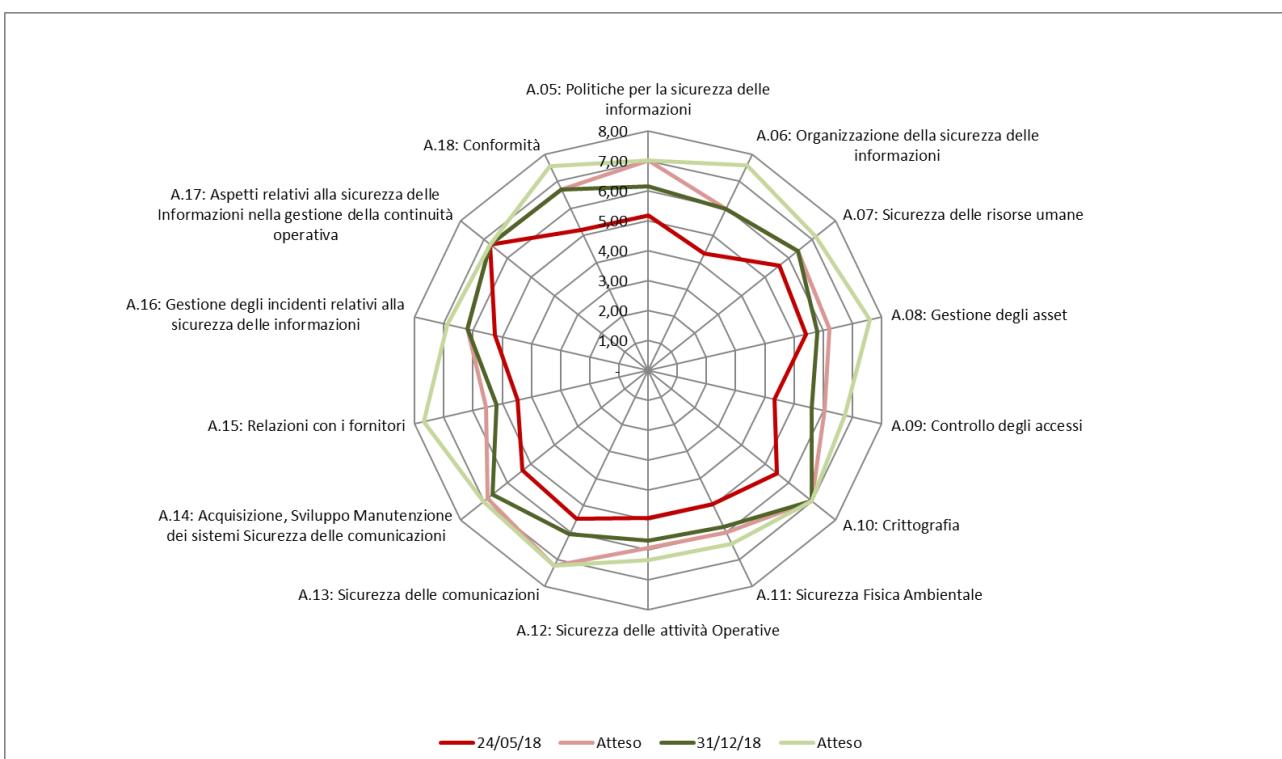
I valori storizzati vengono presentati sotto ogni Controllo. È possibile rilevare quanto i nuovi valori di Conformità coincidano con i valori Attesi ed eventualmente illustrare i problemi quali:

- Non è stato possibile la completa applicazione delle misure aggiuntive previste.
- Le misure aggiuntive sono state applicate ma non si è raggiunto il livello di conformità atteso.
- Sono sopravvenuti elementi imprevisti che hanno modificato la conformità a prescindere dalle misure aggiuntive applicate.

È inoltre possibile ottenere un foglio di Excel con una visualizzazione dell'andamento della Conformità nel tempo.

Area	Atteso	31/12/18	Atteso	24/05/18	Atteso	01/01/18
A.05: Politiche per la sicurezza delle informazioni	7,00	6,13	7,00	5,17	7,00	4,27
A.06: Organizzazione della sicurezza delle informazioni	7,59	5,97	5,97	4,32	4,32	2,43
A.07: Sicurezza delle risorse umane	7,17	6,39	6,39	5,61	5,61	3,66
A.08: Gestione degli asset	7,60	5,80	6,20	5,40	6,20	2,80
A.09: Controllo degli accessi	6,75	5,61	6,05	4,33	5,69	3,44
A.10: Crittografia	7,00	7,00	7,00	5,50	5,50	4,50
A.11: Sicurezza Fisica Ambientale	6,41	5,81	6,01	4,96	5,72	3,32
A.12: Sicurezza delle attività Operative	6,34	5,69	5,92	4,94	5,22	3,62
A.13: Sicurezza delle comunicazioni	7,23	6,08	7,23	5,50	5,50	3,25
A.14: Acquisizione, Sviluppo Manutenzione dei sistemi Sicurezza delle comunicazioni	7,02	6,66	6,86	5,36	5,63	4,14
A.15: Relazioni con i fornitori	7,69	5,21	5,55	4,48	4,48	3,77
A.16: Gestione degli incidenti relativi alla sicurezza delle informazioni	6,89	6,19	6,19	5,26	6,12	2,85
A.17: Aspetti relativi alla sicurezza delle Informazioni nella gestione dell'operatività	6,74	6,74	6,74	6,74	6,74	4,19
A.18: Conformità	7,58	6,68	6,68	5,19	5,74	3,27

Vengono presentate le ultime 5 rilevazioni, se presenti, con Valori rilevati e valori Attesi.



Vengono presentate graficamente le ultime 2 rilevazioni con Valori rilevati e valori Attesi.

NOTA: Le valutazioni “nel tempo” vengono rapportate sempre alla Significatività attuale.
La Conformità rilevata o attesa complessiva di un periodo precedente può variare quindi nel tempo in relazione all’attuale significatività.

Ad esempio, se il Sistema dovesse iniziare a gestire categorie particolari di dati personali che richiedono specifiche misure di sicurezza o se si modifica l’organizzazione aziendale, come un utilizzo significativo del telelavoro, verranno variate le Significatività di vari Controlli e il sistema fornisce la conformità complessiva attesa rispetto a questi cambiamenti evidenziando eventuali carenze che richiedono Misure Aggiuntive.

Agenzia per l’Italia Digitale

L’Agenzia per l’Italia Digitale ha predisposto delle Misure minime di sicurezza ICT, rivolte alle Pubbliche Amministrazione, che possono comunque essere utilizzate come riferimento per tutte le organizzazioni.

Ogni Misura è caratterizzata da:

- Codice, Titolo, Controllo Misura (ovviamente non modificabili).

- Livello (viene proposto quello previsto dalla AgID).
- Modalità di implementazione.
- Note interne.
- Valutazione sull'applicazione (si veda quanto indicato per le valutazioni dei Controlli ISO 27001).

Qualora le misure non sono ritenute idonee è opportuno prevedere misure aggiuntive come illustrato per i Controlli ISO 27001.

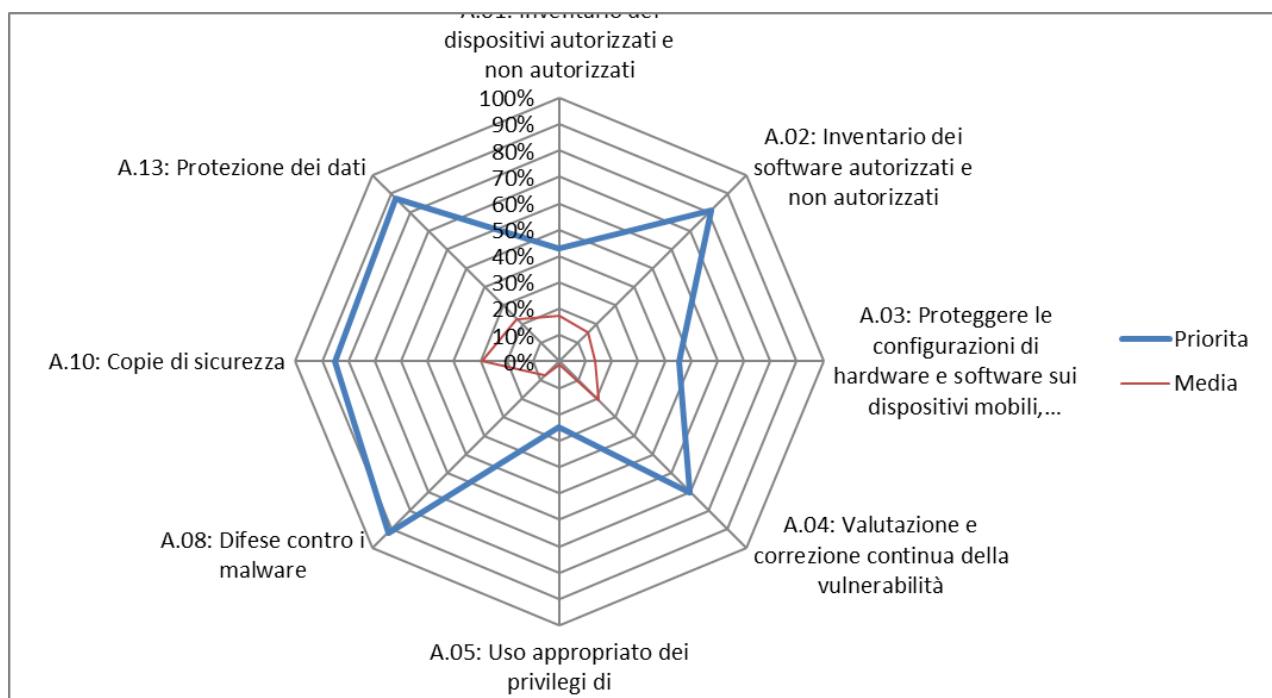
Per ogni Misura vengono riportati i Riferimento che l'AgID ha previsto rispetto al "Framework Nazionale per la Cyber Security" predisposto dalla Università "La Sapienza".

Stampa dei Controlli

Per ottenere il Report è necessario definire i dati di interesse e quindi premere Salva.

Apparirà il bottone "Stampa Controlli" che produrrà un documento di Word.

NOTA: Da "Sistema Informatico" (vedi avanti) è possibile ottenere il Report SGSI complessivo all'interno del quale sono riportati i dati relativi ai Controlli.



NOTA: È possibile ottenere il riepilogo delle attività previste per i vari Responsabili in "Sistema Informatico".

Framework Nazionale per la Cyber Security.

Il "Framework Nazionale per la Cyber Security" predisposto dalla Università "La Sapienza" individua 5 Funzioni che racchiudono 21 categorie suddivise in 98 Sottocategorie.

Ogni Sottocategoria è caratterizzata da:

- Codice, Funzione, Categoria e Sottocategoria (ovviamente non modificabili).
- Livello di Priorità (viene proposto quello per le PMI).
- Livelli di Maturità (vengono riportati quelli previsti per le PMI).

- Modalità di implementazione.
- Note interne.
- Valutazione sull'applicazione (si veda quanto indicato per le valutazioni dei Controlli ISO 27001).

Qualora le misure non sono ritenute idonee è opportuno prevedere misure aggiuntive come illustrato per i Controlli ISO 27001.

Stampa dei Controlli

Per ottenere il Report è necessario definire i dati di interesse e quindi premere Salva.

Apparirà il bottone “Stampa Controlli” che produrrà un documento di Word.

NOTA: Da “Sistema Informatico” (vedi avanti) è possibile ottenere il Report SGSI complessivo all'interno del quale sono riportati i dati relativi ai Controlli.

NOTA: È possibile ottenere il riepilogo delle attività previste per i vari Responsabili in “Sistema Informatico”.

Profili del Framework Nazionale per la Cyber Security

Squadra consente di utilizzare anche le versioni semplificate proposte dal Laboratorio Nazionale CINI di Cybersecurity ed in particolare:

- 2015 – PMI.
- 2016 – Controlli essenziali.

Una volta scelto il Profilo di interesse è necessario definire, per ogni Controllo:

- Modalità di implementazione.
- Note interne.
- Valutazione sull'applicazione (si veda quanto indicato per le valutazioni dei Controlli ISO 27001).
- Livello di Priorità.

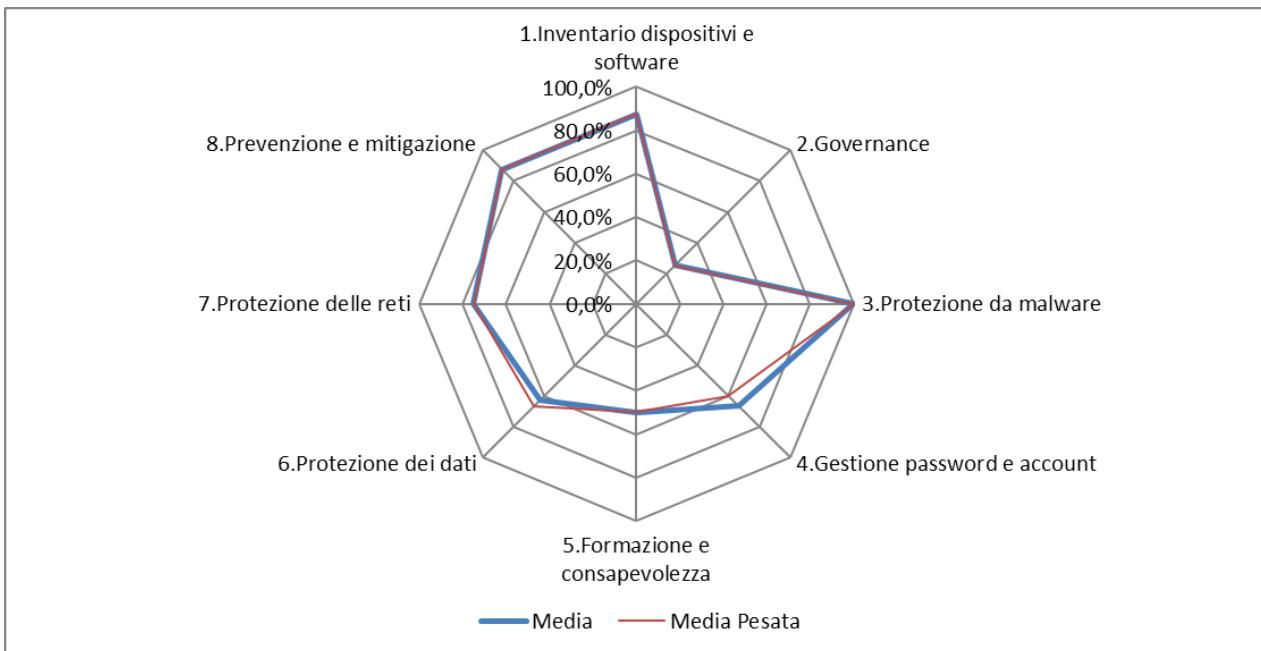
Qualora le misure non sono ritenute idonee è opportuno prevedere misure aggiuntive come illustrato per i Controlli ISO 27001.

Stampa dei Controlli

Per ottenere il Report è necessario definire i dati di interesse e quindi premere Salva.

Apparirà il bottone “Stampa Controlli” che produrrà un documento di Word.

NOTA: Da “Sistema Informatico” (vedi avanti) è possibile ottenere il Report SGSI complessivo all'interno del quale sono riportati i dati relativi ai Controlli.



NOTA: È possibile ottenere il riepilogo delle attività previste per i vari Responsabili in “Sistema Informatico”.

1.3.2 Trattamenti ed Eventi indesiderati (Violazioni)

1.3.2.1 Registro dei Trattamenti

È necessario definire i Trattamenti previsti.

NOTA: Il Garante per la Privacy ha fornito, il 8 ottobre 2018, delle istruzioni per la gestione del Registro.

Sarà cura del Referente Privacy responsabile del Trattamento curarne l’aggiornamento in occasione di modifiche organizzative e comunque verificarne periodicamente i contenuti.

NOTA: Viene utilizzato il termine Referente Privacy al posto di Responsabile perché il GDPR attribuisce le responsabilità interne all’azienda al Titolare o, dove nominato, al DPO mentre per Responsabile si intende la figura esterna all’azienda legata da un contratto (Art. 28 GDPR).

NOTA: Il registro dei Trattamenti può essere utilizzato sia per i trattamenti di cui l’azienda è Titolare sia per quelli per cui l’Azienda ha un contratto in qualità di Responsabile Esterno rispondendo ai commi 1 e 2 dell’Art. 30 del GDPR.

Si vedano anche le indicazioni di Confindustria riportate in Appendice GDPR.

*NOTA: SQuadra fornisce alcuni Trattamenti d’esempio. È **NECESSARIO** che l’utente analizzi nel dettaglio e personalizzi tutte le informazioni.*

Sulla base delle indicazioni fornite dal Garante per la Privacy, il 8 ottobre 2018, le PMI possono utilizzare un “registro semplificato” (si veda l’apposito capitolo successivo).

Ogni Trattamento è caratterizzato da:

- L’Area di riferimento (Gestione del Personale, Gestione Clienti, Gestione Fornitori, Dati Amministrativi, ecc.).
- Un Codice e il Dettaglio delle attività.
- Data di Inizio del trattamento ed eventuale data di conclusione.
- L’importanza del trattamento.
- La classificazione dei Dati:
 - **CONFIDENZIALE** - Il Livello di classificazione “Confidenziale” si applica alle informazioni la cui diffusione potrebbe causare serio danno all’Azienda, comportando conseguenze

economiche e legali significative e danneggiando seriamente la reputazione dell’azienda, delle società ad essa collegate o delle partecipate, con notevoli impatti su beni e asset aziendali. In genere solo un ristretto numero di persone, debitamente autorizzate, può accedere a queste informazioni.

- **RISERVATA** - Il Livello di classificazione “Riservata” si applica alle informazioni il cui utilizzo è limitato a un gruppo di persone, come ad esempio un Ufficio. In genere le informazioni classificate Riservate sono considerate importanti ai fini della sicurezza aziendale, da un punto di vista gestionale, finanziario ed organizzativo, o per l’elevato contenuto tecnologico. La perdita, anche accidentale, di tali informazioni può causare un danno grave all’Azienda. La conoscenza di tali informazioni può costituire rilevante valore per la concorrenza. Le informazioni soggette a norme di sicurezza di programmi / progetti specifici o a normative di legge nazionali/internazionali (come ad esempio le informazioni soggette al Decreto Legislativo n. 196 del 2003: Codice in materia di protezione dei dati personali) rientrano nella classificazione “Riservata”.
 - **INTERNA** - Il Livello di classificazione “Interna” si applica alle informazioni il cui utilizzo è limitato ai dipendenti della Società e al personale di società esterne che svolgono lavori in appalto o in outsourcing o attività di consulenza per l’Azienda. Questo livello di classifica si applica a quelle informazioni la cui compromissione potrebbe causare un danno lieve per la Società. In genere tali informazioni sono accessibili anche ai partner commerciali o industriali.
 - **PUBBLICA** - Il Livello di classificazione “Pubblica” si applica alle informazioni il cui utilizzo non può causare alcun danno all’Azienda. Tali informazioni possono essere considerate di pubblico dominio, essendo generalmente accessibili o disponibili al pubblico. Le informazioni che potrebbero essere pubblicate sul sito internet della Società, ad esempio, rientrano all’interno di tale categoria.
- Catalogazione dei dati personali e degli eventuali dati particolari o giudiziari.
 - Data di creazione e dell’ultimo Aggiornamento o verifica di adeguatezza.
 - Formato dei dati (Digitale e/o Cartaceo).

CRITICITÀ

- Una valutazione codificata ed eventualmente una descrizione degli impatti che ci sarebbero sui soggetti interessati qualora si concretizzasse la perdita di Riservatezza, Integrità e Disponibilità dei dati trattati.
- Tempo massimo di interruzione (MTPD: *Maximum tolerable period of disruption*), ossia il tempo massimo per cui il processo può non essere operativo
- Massima perdita di dati (MTDL: *Maximum Tollerance Data Loss*), intesa come tempo trascorso dall’ultimo salvataggio e, quindi, corrispondente ai dati da ricostruire una volta persi.
- La Vulnerabilità dei dati sia nel caso di attacchi deliberati che da azioni accidentali.

RESPONSABILITÀ

- Preposto o Referente Privacy (colui che sovrintende al trattamento in oggetto) - Ufficio.
- L’indicazione se il trattamento è svolto in qualità di Titolare (altrimenti il trattamento viene svolto solo in qualità di Responsabile Esterno).
- Incaricati.
- Supporto sui quali sono memorizzati.
- Prodotto utilizzato per il trattamento, Produttore, Documentazione relativa ed aggiornamento.
- Eventuali test previsti sui dati.

- Abilitazioni al trattamento.

DATI ESPRESSAMENTE RICHIESTI DALL'ART. 30 DEL REGOLAMENTO EUROPEO

- Licità del trattamento (consenso, esecuzione di un contratto, ecc.).

In relazione ai punti dell'Art. 6 del GDPR si ricorda che:

a) Il consenso che deve essere libero, informato, specifico e inequivocabile e revocabile. Il fatto che una persona non si sia opposta a un trattamento non va confuso con il consenso.

b) Il semplice fatto che il trattamento dei dati sia connesso al contratto, o previsto in qualche punto delle condizioni contrattuali, non significa automaticamente che sia possibile considerarlo necessario all'esecuzione del contratto.

c) È possibile trattare dei dati in quanto necessari per adempiere ad un contratto solo in caso di chiari e specifici obblighi legali ai sensi delle normative dell'UE o di uno Stato membro; in caso di orientamenti non vincolanti (ad esempio di agenzie di regolamentazione) o di un obbligo legale straniero è opportuno valutare il legittimo interesse.

f) Il legittimo interesse richiede di eseguire un test di bilanciamento rispetto agli interessi e diritti degli interessati.

- Nel caso di trattamento per “legittimo interesse” è necessario che questo sia specificato.
- Finalità del trattamento, compreso, dove applicabile, l’interesse legittimo perseguito dal titolare del trattamento e una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità stesse (descrizione catalogata di sintesi o estesa).
- Descrizione delle categorie di interessati e delle categorie di dati personali (descrizione catalogata di sintesi o estesa).
- Categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali (descrizione catalogata di sintesi o estesa).
- Ove applicabile, i trasferimenti di dati personali verso un paese terzo o un’organizzazione internazionale, compresa l’identificazione del paese terzo o dell’organizzazione internazionale e, dove necessario, la documentazione delle garanzie adeguate.
- Ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati e le modalità operative per garantire tale diritto.
- Una valutazione sintetica dei rischi per i diritti e le libertà degli interessati e, ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative previste per affrontare i rischi inclusi i meccanismi per garantire la protezione dei dati personali.

CONTROLLI PER PROTEGGERE I DIRITTI PERSONALI DEGLI INTERESSATI

- Come sono informati del trattamento gli interessati?
- Se necessario, come viene ottenuto il consenso?
- Come gli interessati esercitano i diritti (accesso, rettifica, cancellazione, restrizione, ecc.)?
- Gli obblighi dell’eventuale Responsabile sono chiaramente definiti in un contratto?

ELEMENTI DEL TEST DI BILANCIAMENTO PER TRATTAMENTI BASATI SUL LEGITTIMO INTERESSE⁹

- Valutazione dell’interesse legittimo da parte del Titolare.

Nota: Dovrà inoltre essere abbastanza specifico e articolato in maniera sufficientemente chiara da consentire di eseguire il test comparativo valutando l’interesse legittimo del Titolare rispetto agli interessi e ai diritti fondamentali dell’interessato. Dovrà altresì rappresentare un interesse concreto ed effettivo, ossia non essere teorico. Andrà valutato se esistono altri mezzi meno invasivi per conseguire lo scopo specifico.

- Impatto sugli interessi ed i diritti degli interessati.

Nota: Tenere conto della natura dei dati, lo status dell’interessato (es. minore, lavoratore dipendente), la modalità del trattamento (su vasta scala, comunicazione ad un ampio numero di persone, ecc.).

⁹ Qualora la base giuridica per un trattamento sia il Legittimo interesse del Titolare

Individuare gli interessi ed i diritti dell'interessato su cui potrebbe incidere il trattamento. Considerare le ragionevoli aspettative degli interessati.

- Bilanciamento provvisorio (in assenza di garanzie supplementari).
- Eventuali garanzie supplementari rispetto agli obblighi previsti dal GDPR (da applicare qualora il bilanciamento provvisorio sia dubbio e non è chiaro se prevale il legittimo interesse del Titolare).

Nota: Minimizzazione dei dati raccolti e loro immediata cancellazione dopo l'utilizzo. Misure tecniche ed organizzative volte a garantire che i dati non possano essere utilizzati per intraprendere azioni riguardo alle persone. Diritto incondizionato di opposizione. Diritto di accesso ai propri dati.

Minacce ENISA

NOTA: Si rimanda alla lettura della specifica Appendice.

Vengono proposte, a titolo d'esempio, alcune applicazioni tratte dal "Manuale sulla sicurezza di Trattamento dei dati personali" che devono, ovviamente, essere personalizzate.

Viene richiesta una valutazione della probabilità che si verifichino minacce per le aree previste dalle "Linee Guida sulla sicurezza del trattamento dei dati personali".

Per ogni Area vengono proposti gli elementi suggeriti da ENISA e viene calcolato il valore della probabilità ma questo deve essere confermato o modificato dall'utente in base alle considerazioni descritte nelle note.

A livello di Trattamento viene indicato il livello di Rischio in funzione della Probabilità delle Minacce e dell'Impatto massimo previsto (fra Riservatezza, Disponibilità ed Integrità) secondo la tabella riportata in appendice.

Responsabili esterni del Trattamento

Ove una parte del trattamento è affidata ad un Responsabile esterno sarà necessario indicare:

- Responsabile esterno.
- Parte del Trattamento gestito esternamente.
- Quota del Trattamento gestito esternamente.
- Data del contratto con il Responsabile esterno.
- Responsabile della verifica della corretta gestione dei dati personali da parte del Responsabile esterno.
- Data dell'ultima verifica.
- Periodicità della verifica (espressa in mesi).
- Eventuali note interne.

Dettaglio dei Rischi e delle Misure connessi ad ogni Trattamento

È possibile sostituire alla valutazione sintetica dei Rischi una esplicitazione dei singoli Rischi connessi al Trattamento indicando:

- Descrizione del Rischio.
- Dettaglio del Rischio (se necessario per illustrare nel dettaglio il rischio potenziale).
- Probabilità e Gravità (dalle quali viene calcolato il livello di Rischio) – Si veda l'appendice.
- Misure Aggiuntive (se previste).
- Responsabile dell'adozione delle misure aggiuntive.
- Risorse previste per l'adozione delle Misure aggiuntive.
- Tempi per la realizzazione delle eventuali Misure Aggiuntive.
- Criteri per la valutazione dei risultati a valle dell'adozione delle Misure aggiuntive.

Titolari del Trattamento

Ove il trattamento è eseguito, in qualità di Responsabili, per conto di un Titolare sarà necessario indicare:

- Titolare ed eventuale Contitolare.
- Se noto, il trattamento originale all'interno del quale si inserisce l'attività svolta in qualità di Responsabile.
- Data del contratto con il Titolare del trattamento in oggetto.
- Qualora il Titolare abbia contrattualmente richiesto di essere periodicamente relazionato sulla gestione del trattamento e sulle eventuali criticità: Data dell'ultima Relazione e Periodicità delle relazioni (espressa in mesi).
- Eventuali note interne.

NOTA: Un Trattamento può essere eseguito sia in qualità di Titolare che in qualità di Responsabile per conto di altri Titolari. Si pensi alla gestione delle paghe eseguita da una sola società di un gruppo. Il trattamento sarà svolto in qualità di Titolare per i propri dipendenti e di Responsabile (in base a specifici contratti) per i dipendenti delle altre società del gruppo.

Organigramma del Trattamento

È possibile inserire tutte le figure coinvolte nel trattamento con i relativi riferimenti:

- Titolare del trattamento
- Rappresentante del Titolare del trattamento
- Responsabile della protezione dei dati (DPO)
- Responsabile del trattamento
- Sub-responsabile del trattamento
- Delegato dal Titolare del trattamento – Referente privacy

Analisi della necessità di effettuare una Valutazione Impatto Privacy (PIA)

NOTA: La realizzazione di una valutazione d'impatto sulla protezione dei dati è obbligatoria soltanto qualora il trattamento "possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche". Essa è particolarmente importante quando viene introdotta una nuova tecnologia di trattamento dei dati. Secondo le buone prassi, una valutazione d'impatto sulla protezione dei dati va riesaminata continuamente e rivalutata con regolarità.

È possibile registrare, per ogni trattamento, le analisi effettuate sulla necessità di effettuare una PIA. È anche possibile registrare il risultato dell'eventuale PIA effettuata.

Se si ritiene che possa essere opportuno ripetere la valutazione sull'impatto è possibile indicare fra quanti mesi è opportune prevederla.

Criteri per determinare la necessità di effettuare una Valutazione Impatto Privacy (PIA)

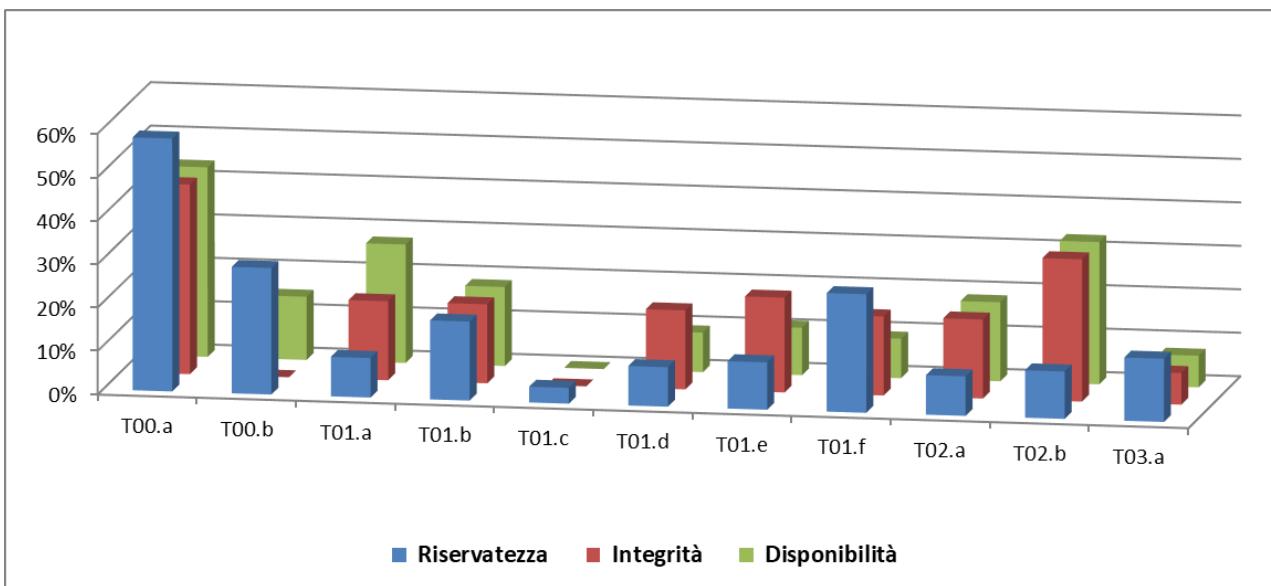
Vengono presentati gli elementi sulla base dei quali è possibile determinare la necessità di effettuare la PIA come previsto dalle Linee Guida dei Garanti europei (vedi Appendice relativa).

1.3.2.2 Stampa del Registro dei Trattamenti

Per ottenere il Registro dei Trattamenti è necessario definire i dati di interesse e quindi premere Salva.

Apparirà il bottone "Registro" che produrrà un documento di Word.

NOTA: Da "Sistema Informatico" (vedi avanti) è possibile ottenere il Report SGSI complessivo all'interno del quale sono riportati i dati relativi ai Trattamenti.



NOTA: È possibile ottenere il riepilogo delle attività previste per i vari Responsabili in “Sistema Informatico”.

1.3.2.3 Registro dei Trattamenti (Semplificato)

Sulla base delle indicazioni fornite dal Garante per la Privacy, il 8 ottobre 2018, le PMI possono utilizzare un “registro semplificato”.

Ogni Trattamento è caratterizzato da:

- Un Codice (che verrà utilizzato anche per l’ordine di presentazione dei vari trattamenti)
- L’Area di riferimento (Gestione del Personale, Gestione Clienti, Gestione Fornitori, Dati Amministrativi, ecc.).
- Il Dettaglio delle attività.
- Una valutazione sulla significatività del trattamento.
- Finalità del trattamento.
- Descrizione delle categorie di interessati
- Categorie di dati personali trattati.
- Categorie particolari di dati personali trattati (ex “sensibili”).
- Punti del comma 1 dell’Art. 6 che rendono lecito il trattamento.

In relazione ai punti dell’Art. 6 comma 1 del GDPR si ricorda che il trattamento è lecito unicamente se:

- a) *l’interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità; (C42, C43)*
 - b) *il trattamento è necessario all’esecuzione di un contratto di cui l’interessato è parte o all’esecuzione di misure precontrattuali adottate su richiesta dello stesso; (C44)*
 - c) *il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento; (C45)*
 - d) *il trattamento è necessario per la salvaguardia degli interessi vitali dell’interessato o di un’altra persona fisica; (C46)*
 - e) *il trattamento è necessario per l’esecuzione di un compito di interesse pubblico o connesso all’esercizio di pubblici poteri di cui è investito il titolare del trattamento; (C45, C46)*
 - f) *il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell’interessato che richiedono la protezione dei dati personali, in particolare se l’interessato è un minore. (C47-C50)*
- Punti del comma 2 dell’Art. 9 che rendono lecito il trattamento per categorie particolari di dati.

In relazione ai punti dell’Art. 9 comma 2 del GDPR si ricorda che il trattamento è lecito unicamente se:

- a) l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1;
- b) il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato;
- c) il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
- d) il trattamento è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato;
- e) il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;
- f) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;
- g) il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato; (C55, C56)
- h) il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità, fatte salve le condizioni e le garanzie di cui al paragrafo 3; (C53)
- i) il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale; (C54)
- j) il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.
- Formato dei dati trattati (Cartaceo o Digitale).
 - Incaricati del trattamento.
 - Eventuali Responsabili Esterne che partecipano al trattamento.
 - Destinatari esterni.
 - Eventuale trasferimento dati verso paesi terzi o organizzazioni internazionali.
 - Termini ultimi di cancellazione previsti.
 - Misure di sicurezza tecniche e organizzative.
 - Modalità utilizzate per la trasmissione dell'Informativa.
 - Modalità utilizzate per raccogliere il consenso quando necessario.
 - Catalogazione dei dati personali e degli eventuali dati particolari o giudiziari.
 - Formato dei dati (Digitale e/o Cartaceo).

INTERNI

NOTE: Vengono gestiti dati non richiesti per la compilazione del Registro dei Trattamenti semplificato ma che possono essere utili per la corretta gestione.

- Preposto o Referente Privacy (colui che sovrintende al trattamento in oggetto) - Ufficio.
- Note interne.
- Data di Inizio del trattamento ed eventuale data di conclusione.
- Data di creazione e dell'ultimo Aggiornamento o verifica di adeguatezza.

- Tempo massimo di interruzione (MTPD: *Maximum tolerable period of disruption*), ossia il tempo massimo per cui il processo può non essere operativo
- Massima perdita di dati (MTDL: *Maximum Tollerance Data Loss*), intesa come tempo trascorso dall'ultimo salvataggio e, quindi, corrispondente ai dati da ricostruire una volta persi.

ELEMENTI DEL TEST DI BILANCIAMENTO PER TRATTAMENTI BASATI SUL LEGITTIMO INTERESSE¹⁰

- Valutazione dell'interesse legittimo da parte del Titolare.

Nota: Dovrà inoltre essere abbastanza specifico e articolato in maniera sufficientemente chiara da consentire di eseguire il test comparativo valutando l'interesse legittimo del Titolare rispetto agli interessi e ai diritti fondamentali dell'interessato. Dovrà altresì rappresentare un interesse concreto ed effettivo, ossia non essere teorico. Andrà valutato se esistono altri mezzi meno invasivi per conseguire lo scopo specifico.

- Impatto sugli interessi ed i diritti degli interessati.

Nota: Tenere conto della natura dei dati, lo status dell'interessato (es. minore, lavoratore dipendente), la modalità del trattamento (su vasta scala, comunicazione ad un ampio numero di persone, ecc.). Individuare gli interessi ed i diritti dell'interessato su cui potrebbe incidere il trattamento. Considerare le ragionevoli aspettative degli interessati.

- Bilanciamento provvisorio (in assenza di garanzie supplementari).
- Eventuali garanzie supplementari rispetto agli obblighi previsti dal GDPR (da applicare qualora il bilanciamento provvisorio sia dubbio e non è chiaro se prevale il legittimo interesse del Titolare).

Nota: Minimizzazione dei dati raccolti e loro immediata cancellazione dopo l'utilizzo. Misure tecniche ed organizzative volte a garantire che i dati non possano essere utilizzati per intraprendere azioni riguardo alle persone. Diritto incondizionato di opposizione. Diritto di accesso ai propri dati.

Titolari del Trattamento

Ove il trattamento è eseguito, in qualità di Responsabili, per conto di un Titolare sarà necessario indicare:

- Titolare ed eventuale Contitolare.
- Se noto, il trattamento originale all'interno del quale si inserisce l'attività svolta in qualità di Responsabile.
- Data del contratto con il Titolare del trattamento in oggetto.
- Qualora il Titolare abbia contrattualmente richiesto di essere periodicamente relazionato sulla gestione del trattamento e sulle eventuali criticità: Data dell'ultima Relazione e Periodicità delle relazioni (espressa in mesi).
- Eventuali note interne.

NOTA: Un Trattamento può essere eseguito sia in qualità di Titolare che in qualità di Responsabile per conto di altri Titolari. Si pensi alla gestione delle paghe eseguita da una sola società di un gruppo. Il trattamento sarà svolto in qualità di Titolare per i propri dipendenti e di Responsabile (in base a specifici contratti) per i dipendenti delle altre società del gruppo.

1.3.2.4 Registro dei Trattamenti intermedio

L'Autorité de Protection des Données (Belgio) ha proposto un Registro estremamente completo e dettagliato. Anche l'Autorità francese (CNIL) ha predisposto una sua proposta.

¹⁰ Qualora la base giuridica per un trattamento sia il Legittimo interesse del Titolare

Sulla base di queste proposte è possibile gestire un Registro dei Trattamenti di complessità intermedia fra quello completo e quello semplificato.

Anche in questo caso è possibile gestire i Titolari del Trattamento e, ovviamente, ottenerne l'esportazione su excel.

1.3.2.5 Eventi Indesiderati (Violazioni e Incidenti)

In caso di violazione dei dati personali (vedi Artt. 33 e 34 del GDPR), il titolare del trattamento notifica la violazione all'autorità di controllo competente senza ingiustificato ritardo a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo. Tutti i titolari di trattamento dovranno in ogni caso documentare le violazioni di dati personali subite, anche se non notificate all'autorità di controllo e non comunicate agli interessati, nonché le relative circostanze e conseguenze e i provvedimenti adottati

Squadra consente di memorizzare, per ogni evento imprevisto (cfr. Appendice SGSL: Vulnerabilità, incidenti, violazioni), i seguenti dati:

- RILEVAZIONE
 - Codice e descrizione dell'evento.
 - Data ed Ora di conoscenza dell'evento.
 - Data dell'evento anomalo.
 - Data presunta della eventuale violazione.
 - Natura dell'evento.
 - Fonte della segnalazione.
 - Sistema coinvolto (Computer, Rete, Dispositivo mobile, Supporto di memorizzazione mobile, Strumento di backup, Documenti cartacei, ecc.).
 - Luogo dell'evento (ad esempio luogo di smarrimento in caso di dispositivi trasportabili).
 - Possibili conseguenze previste.
- VALUTAZIONE
 - Ove possibile, il numero approssimativo di interessati in questione e il numero approssimativo di registrazioni dei dati personali in questione.
 - Categorie di interessati / registrazioni coinvolte.
 - Natura dei dati coinvolti.
 - Classificazione della violazione.
 - Valutazione sulla violazione.
 - Descrizione del rischio per gli interessati.
 - Il livello di rischio stimato (in base al quale valutare la necessità di comunicazione all'Autorità ed agli Interessati).
 - Nome ed e-mail del contatto o del responsabile della protezione dei dati presso cui ottenere più informazioni.
 - Identificazione dell'incidente come Violazione (Data Breach).
 - Evento segnalato come indesiderato erroneamente: Falso positivo.
 - Ipotesi di azioni legali (con conseguente raccolta delle prove).
 - Eventuale data di comunicazione del Responsabile al Titolare (se si opera come Responsabile).
 - Eventuale data di comunicazione al Garante.
 - Provvisorietà della comunicazione al Garante qualora si opti per una comunicazione per fasi (al fine di essere tempestivi e possibilmente rispettare il limite delle 72 ore in caso di incidenti la cui analisi risulta complessa).
 - Eventuale data di comunicazione agli Interessati.
 - Minaccia collegata all'evento.

- Necessità di escalation ed eventuali risorse coinvolte.
- MISURE
 - Misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.
 - Data prevista per l'attuazione delle misure.
 - Data effettiva dell'attuazione delle misure.
 - Data di verifica e note di chiusura delle misure.
- MOTIVI PER L'EVENTUALE NON COMUNICAZIONE AL GARANTE
 - Misure tecniche e organizzative adeguate di protezione e tali misure che erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura.
 - Misure atte a scongiurare il sopravvenire di un rischio elevato per i diritti e le libertà degli interessati messe in atto successivamente alla violazione.
 - Sforzi necessari per l'eventuale comunicazione agli interessati.

Compilazione della comunicazione della Violazione

Fra i Documenti forniti da SQuadra GDPR (vedi capitolo successivo) è presente una ipotesi di Procedura per la gestione delle Violazioni alla quale si rimanda.

È possibile richiedere la stampa della comunicazione per gli interessati, sempre sulla base dei Documenti forniti da SQuadra GDPR nella quale verranno riportate le seguenti informazioni:

Etichetta	Contenuto tratto dalla Violazione in esame
[V_DATA_CONOSCENZA]	Data nella quale si è avuto conoscenza della Violazione.
[V_ORE]	È l'ora alla quale si è avuto conoscenza.
[V_DATA_VIOLAZIONE]	È la data, anche presunta, della Violazione.
[V_NATURA]	Natura della Violazione.
[V_CLASSIFICAZIONE]	Classificazione.
[V_VALUTAZIONE]	Valutazione.
[V_RISCHIO]	Rischio.
[V_LIV_RISCHIO]	Livello di Rischio stimato.
[V_MISURE]	Sito internet ufficiale dell'azienda.
[V_CONTATTO]	Nome della persona da contattare.
[V_MAIL_CONTATTO]	Indirizzo mail da utilizzare per il contatto.

Ovviamente sarà possibile richiedere la comunicazione solo se l'incidente è stato identificato come Violazione dei dati personali.

Emissione della Comunicazione

Per le Violazioni è possibile ottenere una bozza di Comunicazione automatica per gli interessati (Vedi Capitolo Comunicazioni).

1.3.3 Documenti

1.3.3.1 Documenti forniti da SQuadra GDPR

NOTA: È possibile gestire i documenti aziendali creando liberamente documenti ma, all'inizio dell'uso del programma, si consiglia di importare i documenti forniti da SQuadra GDPR come indicato di seguito.

Informazioni Aziendali

È necessario inserire una serie di informazioni che permetteranno la personalizzazione dei documenti. Nei testi dei documenti potrà essere inserita una delle etichette riportate nel successivo capitolo sui Documenti Aziendali che SQuadra provvederà a “tradurre” nel contenuto inserito fra le informazioni aziendali.

Fra le informazioni è presente “Indirizzo di spedizione” per il cui significato si rimanda alla lettura del paragrafo sulle Comunicazioni.

Viene inoltre richiesto:

- Le caratteristiche attuali dell'infrastruttura informatica dell'azienda.
- Le caratteristiche degli eventuali controlli effettuati sui Lavoratori (Goelocalizzazione e Videosorveglianza).
- I rapporti con i Consulenti IT (per i sistemi informatici).
- Attività connesse allo sviluppo del software.
- Come vengono gestite le Segnalazioni.
- Se vengono utilizzate connessione WiFi.

- Se viene utilizzato il nome personale negli indirizzi mail al posto della funzione aziendale (amministrazione@ditta.it, commerciale@ditta.it, ecc.).
- Se vengono utilizzati strumenti per l'analisi dei dati delle navigazioni su internet.
- Se viene utilizzato un Antispam remoto. Questi sistemi prevedono che tutte le mail vengano inviate su appositi server per effettuare le opportune valutazioni e quindi solo le mail che superano i controlli verranno inviate all'effettivo destinatario.
- Se è previsto che i vari PC siano dotati di piccoli gruppi di continuità.
- Se il cambio della password è lasciato all'incaricato o imposto dal sistema.
- Se le password vengono consegnate e conservate in busta chiusa o se le password non vengono consegnate a nessuno perché l'amministratore del sistema è in grado di resettarle in caso di necessità.
- Se l'azienda utilizza il telelavoro.
- Se si aderisce alle Linee Guida Privacy per l'Edilizia predisposte da ISTEKO.

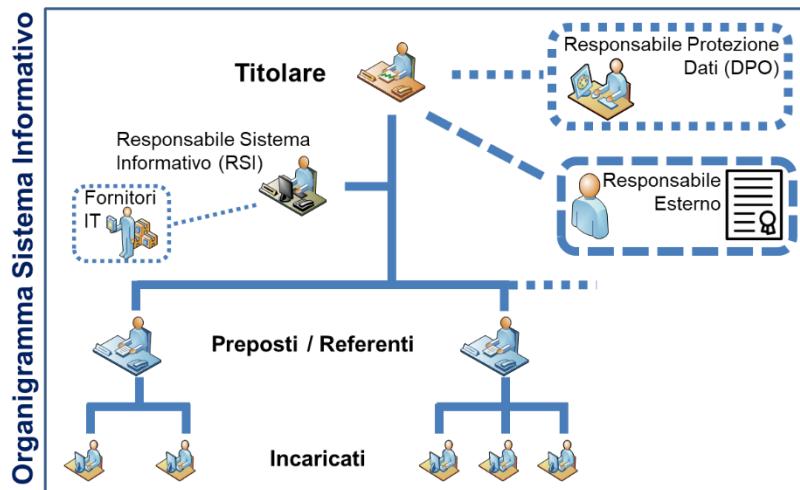
Aggiornamento dei documenti Aziendali

SQuadra GDPR fornisce una serie di Documenti.

NOTA: I Documenti forniti da SQuadra GDPR sono in continuo aggiornamento. I progettisti di SQuadra monitorano infatti l'evolversi della tematica sia in funzione di eventuali interventi del Legislatore europeo o del Garante italiano che delle richieste provenienti dagli utenti.

I Documenti devono essere presi in considerazione con le dovute cautele, come indicazione di massima ed a titolo di esempio, necessitano di preventiva e specifica valutazione da parte del Titolare del trattamento prima della definitiva adozione.

Prima di richiederli è necessario compilare le Informazioni Aziendali illustrate precedentemente che permettono una prima personalizzazione di questi Documenti.



La documentazione predisposta da SQuadra prevede una organizzazione aziendale quale quella indicata in figura. Il **Titolare** è affiancato dal **Responsabile del sistema informativo** (RSI) che coordina tutte le attività aziendali nel settore IT con il supporto di fornitori/consulenti IT.

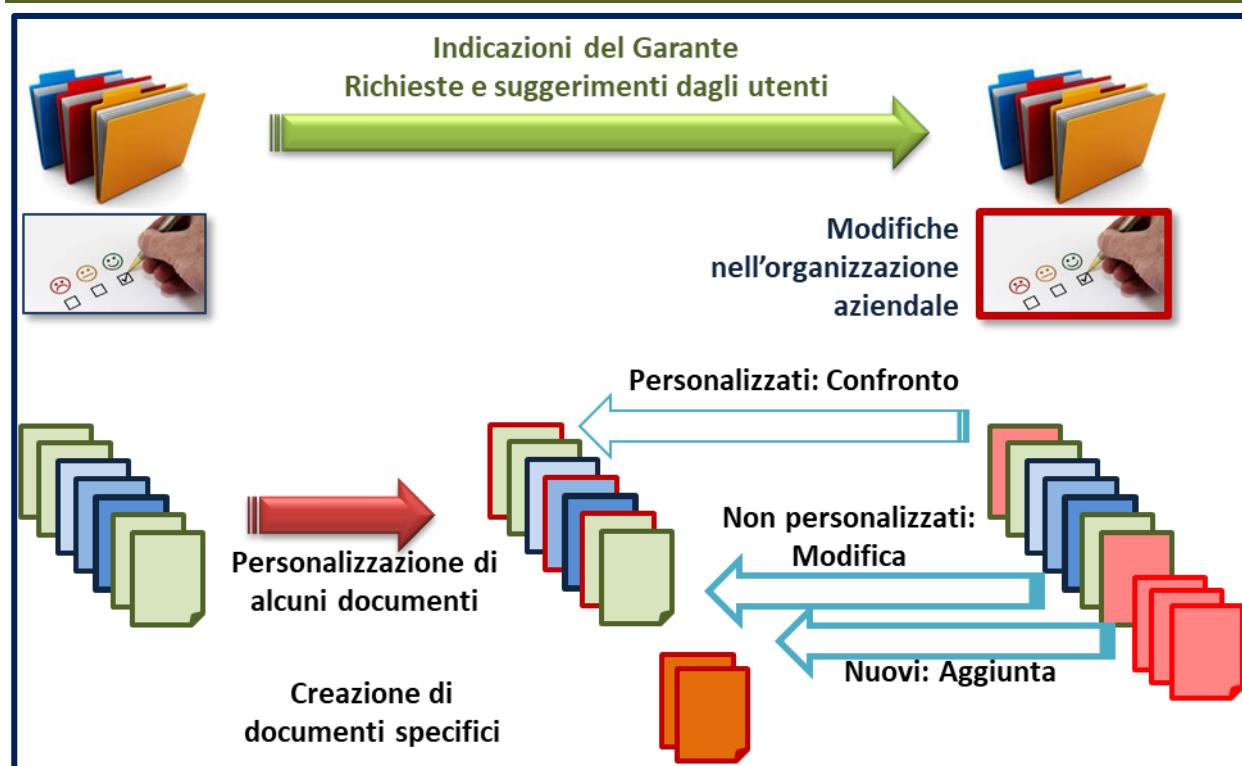
I vari uffici sono sotto la responsabilità di **Preposti/Referenti** del Titolare che coordinano e controllano le attività degli **incaricati autorizzati**.

In casi particolari il Titolare può valutare di nominare un **Responsabile della protezione dei dati** o DPO (Art. 37 del GDPR).

Il Titolare può assegnare, tramite appositi contratti, parti del trattamento a **Responsabili esterni** (Art. 28 del GDPR).

Ogni volta che si richiede l'aggiornamento dei documenti verrà copiata l'ultima versione dei Documenti di SQuadra che sono in continuo aggiornamento ed ampliamento.

Aggiornamento selettivo



Una volta importati i documenti forniti da SQuadra GDPR ogni azienda provvederà a personalizzarli. Potrà anche creare nuovi documenti per la specifica realtà aziendale.

I documenti di SQuadra GDPR sono, d'altra parte, continuamente aggiornati in funzione delle indicazioni fornite dal Garante o di suggerimenti provenienti dall'applicazione concreta da parte dei vari utenti. Possono anche cambiare alcune delle indicazioni fornite nelle Informazioni Aziendali.

In ogni momento i documenti forniti da SQuadra potrebbero, quindi, essere differenti da quelli forniti l'ultima volta sulla quale si è operato per le personalizzazioni.

Il programma presenta i documenti nuovi o modificati e, per quest'ultimi, viene indicato quali sono quelli sui quali sono state effettuate delle personalizzazioni dall'azienda.

NOTA: Mentre è consigliabile Aggiungere i nuovi e Modificare quelli modificati da SQuadra GDPR ma non personalizzati dall'Azienda per quelli Personalizzati è necessario analizzare le Personalizzazioni eventualmente per riprodurle dopo l'aggiornamento.

È possibile richiedere i dettagli di un documento per analizzare le singole frasi modificate.

Controllo su Excel dei nuovi documenti disponibili.

È possibile ottenere un documento di Excel nel quale vengono presentate le differenze fra i Documenti che verrebbero forniti attualmente da SQuadra, in base alle ultime informazioni, e quelli Aziendali.

Nel foglio “Documenti” vengono presentati tutti i Documenti Aziendali con:

- Eventuale Documento Base utilizzato per le Varianti.
- Data di Aggiornamento.
- Eventuali Modifiche rispetto ai Documenti attualmente forniti da SQuadra.
- Attuale Descrizione su SQuadra (solo se modificata).
- Attuale data d’Aggiornamento del Documento su SQuadra (solo se modificata).

Nel foglio “Testi” vengono presentati tutti i Testi dei Documenti aziendali con:

- Documento.
- Descrizione del Testo.
- Modifiche apportate (vengono considerate sia le modifiche apportate dall'Azienda rispetto ai Documenti originali [Personalizzazioni] sia le modifiche fra i Documenti originali e quelli attualmente forniti da SQuadra [Modifiche]).
- Testo e Testo formattato (se presente sostituisce il Testo) Aziendali.
- Testo e Testo formattato Originali [forniti da Squadra nell'ultimo aggiornamento]. Verranno presentati solo in caso di personalizzazioni aziendali.
- Testo e Testo formattato che verrebbero forniti attualmente da SQuadra. Verranno presentati solo se modificati rispetto agli Originali utilizzati nell'ultimo aggiornamento.

Documenti di WORD per confronti.

È possibile ottenere tre documenti di Word, con la stessa impostazione, riferiti rispettivamente ai documenti forniti da SQuadra Attualmente, ai Documenti Aziendali ed ai documenti forniti da SQuadra al momento dell'ultimo aggiornamento (quindi quelli utilizzati come origine per i documenti aziendali).

Utilizzando le normali funzionalità di Word (Revisione / Confronta) è possibile ottenere l'evidenziazione di tutte le differenze:

Nota: si consiglia di eliminare i commenti sulla formattazione dal menu Revisione di Word.

- Tra la Versione d'Origine e quella Aziendale: per vedere cosa è stato personalizzato.
- Tra la Versione Aziendale e l'Attuale proposta di SQuadra: per vedere le nuove proposte.
- Tra la Versione d'Origine e l'Attuale proposta da SQuadra: per vedere le novità.

Se le modifiche introdotte dal continuo aggiornamento della documentazione proposta da SQuadra, ricavabili dall'ultimo confronto, ritenute di interesse sono poche è possibile apportarle manualmente sui Documenti Aziendali utilizzando il primo confronto.

Se le modifiche di interesse sono molte rispetto alle modifiche apportate per adattare i documenti standard alla realtà aziendale, ricavabili dal secondo confronto, è conveniente ripetere l'importazione e riapplicare le eventuali personalizzazioni.

1.3.3.2 Documenti Aziendali

SQquadra Privacy permette di gestire una serie di Documenti (Informative, Nomine, Incarichi, Policy, ecc.) che possono essere definiti dall'utente liberamente o partendo da quelli forniti da SQquadra.

Ogni Documento è caratterizzato da un Codice ed una Descrizione.

Testi dei Documenti

Per ogni Documento vengono definiti tutti i testi che lo compongono.

Ogni testo è caratterizzato da:

- Codice e descrizione.
- Stile utilizzato nel Documento di Word.
- Testo vero e proprio.
- Eventuali note interne.
- Una valutazione sulla necessità di ulteriore personalizzazione.
- Nel Pannello TESTO FORMATTATO è possibile inserire un testo con alcune formattazioni. Se presente un testo verrà considerato al posto del testo nel Pannello BASE.

All'interno dei testi è possibile utilizzare delle "etichette" che SQquadra provvederà a "tradurre", in base alle informazioni aziendali, al momento della stampa.

Etichetta	Contenuto tratto dalle informazioni Aziendali
[TITOLARE]	È il Titolare del trattamento dei dati. In genere l'azienda, in persona del suo legale rappresentante pro-tempore.
[Mail_TITOLARE]	È l'indirizzo mail al quale è possibile contattare il Titolare.
[C.F.]	Codice Fiscale
[P.IVA]	Partita Iva
[RSI]	È il Responsabile dei Sistemi Informatici aziendali.
[Mail_RSI]	È l'indirizzo mail al quale è possibile contattare il Responsabile dei Sistemi Informatici aziendali.
[AMMINISTRATORI]	Il documento che contiene l'elenco degli Amministratori di Sistema.
[BACHECA]	È il luogo fisico o digitale dove vengono inserite le comunicazioni. Ad esempio "sull'area riservata del sito", "nella cartella 'comunicazioni' dell'intranet aziendale", "nella bacheca in sala mensa", ecc.
[SITO_AZIENDA]	Sito internet ufficiale dell'azienda.

Altre etichette che possono essere utilizzate nei documenti

[AZIENDA]	Verrà inserito il nominativo della Società.
[SOGLGETTO]	Funzione per la quale viene predisposto il Documento
[NOME_SOGLGETTO]	È il nome della persona o azienda incaricata della Funzione di cui sopra.

Etichette e caratteri speciali

Stile	Effetto
[tab]	Tabulazione
-	(segno meno) Permette, in una variante, di cancellare lo specifico testo base. <i>A titolo d'esempio si veda l'informativa per il Sito aziendale dove non ha senso inserire le firme finali.</i>
=	(segno uguale) Permette, in una variante, di cancellare tutti i testi base i cui Codici iniziano con il Codice di questo testo. <i>A titolo d'esempio si veda la Nomina a Responsabile Esterno per la gestione dei dati di SQquadra dove non si è ritenuto necessario inserire il questionario di valutazione.</i>

All'interno dei testi è possibile utilizzare degli Stili di Word particolari.

Stile	Effetto
Tz_Salto_Pagina	Salto pagina

Stile	Effetto
InizioSezione	Inizia una nuova sezione alla pagina successiva (ad esempio per fare ripartire la numerazione delle pagine).

Varianti

Un Documento può essere utilizzato come base per ottenerne delle “varianti”. Ad esempio, è possibile predisporre una Informativa di base e quindi predisporre tante informative (per i Dipendenti, per i Fornitori, per i Clienti, ecc.) che si differenziano dal documento base pur sfruttandone gli elementi principali.

Le “varianti”, al pari dei documenti di base, sono caratterizzate da un Codice ed una Descrizione.

Per le “varianti” devono essere definiti solo i testi che si desidera sostituire (utilizzando lo stesso codice) o aggiungere (utilizzando codici non presenti nel documento base).

I testi delle “varianti” sono caratterizzati dalle stesse informazioni dei testi “base”.

Vengono presentati i testi finali con l’indicazione dell’origine (Variante attuale o Base).

È possibile selezionare alcuni testi, in genere quelli per i quali è consigliata la personalizzazione, per copiarli come testi della variante. Sarà ovviamente necessario quindi procedere alle modifiche opportune partendo dal testo di base.

Stampe

È possibile richiedere la stampa del documento sia in formato WORD che in formato PDF.

Il documento di Word può essere prodotto anche con l’evidenziazione dei Codici dei vari testi. Saranno evidenziati i testi specifici.

È possibile richiedere la stampa con i Riferimenti ai Controlli che vengono gestiti dal Documento (in genere significativo per “Manuale” e “Policy”).

Emissione del Documento

È possibile richiedere l’emissione del Documento. Si rimanda al capitolo successivo relativo alle Comunicazioni.

Documenti Aziendali Base

È possibile richiedere documenti di Word relativi al Sistema di Gestione per la Sicurezza delle Informazioni:

- Manuale della Sicurezza delle Informazioni.
- Policy per gli incaricati.
- Procedure per i consulenti IT.
- Responsabilità del RSI.
- Politica per la Videosorveglianza.

I documenti sono personalizzati in funzione delle informazioni fornite ma dovranno essere ulteriormente personalizzati per rispondere alle specifiche caratteristiche aziendali.

Modelli base aziendali

Ogni azienda può personalizzare i moduli prodotti da SQuadra.

Per i documenti di Word è possibile modificare l'intestazione, eventualmente inserendo il logo aziendale, e tutti gli stili. Per i documenti di Excel è possibile modificare il formato dei vari fogli o modificare i dati di origine per i grafici.

Per ogni Modulo il programma propone il MODELLO BASE che può essere personalizzato e quindi salvato come FILE AZIENDALE.

Nella personalizzazione è necessario controllare i segnalibri di word (Inserisci / Collegamenti) che vengono utilizzati dal programma per l'intestazione e la terminazione delle pagine.

1.3.4 Comunicazioni

Le funzioni di SQuadra GDPR permettono di produrre ed aggiornare con facilità, ad esempio a seguito di specifiche istruzioni del Garante, i vari documenti.

Ogni azienda deve comunque “emettere” dei documenti (che possono essere prodotti utilizzando SQuadra GDPR ed eventualmente modificati o essere elaborati in modo autonomo) per comunicarli ai destinatari.

Per ogni documento “Emesso” è necessario indicare:

- Il Codice e la descrizione.
- L’indicazione degli interessati (coloro ai quali va consegnato il Documento).
- L’Origine del Documento:
 - Esterno (non prodotto utilizzando SQuadra GDPR).
 - Documento (uno dei documenti di base di SQuadra GDPR).
 - Variante (una delle varianti di un documento di base).
 - Variante per Responsabile (uno dei documenti specifici per Responsabilità).
- Documento di Origine (quando il Documento ha origine da SQuadra GDPR).
- Eventuali Note.

SQuadra fornisce alcune informazioni:

- Ultimo aggiornamento del Documento (ovviamente solo per i Documenti originati da SQuadra GDPR).

NOTA: Il sistema segnala come data di aggiornamento l’ultima fra tutti i documenti utilizzati per produrre il Documento di Origine. In caso di un Documento prodotto per un Responsabile (si veda avanti) sulla base di una Variante verrà indicata l’ultima fra le date del Documento base, della Variante e della Variante per Responsabile.

- Origine dell’aggiornamento (quale è il documento aggiornato più di recente).
- Ultima versione emessa.
- Stato delle Versioni (per segnalare l’eventuale necessità di emettere una nuova versione a seguito degli aggiornamenti dei documenti sui quali si basa).

Documenti Emessi: Versioni

Per ogni Documento Emesso possono esistere più versioni.

Ad esempio, in genere, esiste già una Informativa per i Dipendenti predisposta, precedentemente all’introduzione del GDPR, sulla base del Codice per la Protezione dei dati Personalni.

Per ogni Versione è possibile inviare delle Comunicazioni.

Per le modalità operative si rimanda all’apposita Appendice “Comunicazioni”.

1.3.5 Sistema Informativo

1.3.5.1 Inventario

È possibile definire:

- Apparati.
- Prodotti software.
- Data Base.
- Dispositivi Mobili (Aziendali e/o Personal).

Ad ogni elemento è possibile associare uno o più allegato (Contratti di assistenza, Nomine, ecc.).

Apparati

Per ogni Apparato è necessario definire:

- Codice e descrizione.
- Tipologia (Server, PC, ecc.).
- Sistema Operativo.
- Funzioni.
- Metodo di aggiornamento del Sistema Operativo.
- Criticità in caso di non funzionamento.
- Come è assicurata la continuità.
- Responsabile dell'Apparato.
- Data dell'ultima verifica.
- Periodicità della verifica espressa in mesi.
- Note interne.

NOTA: È possibile ottenere il riepilogo delle attività previste per i vari Responsabili in “Sistema Informatico”.

Prodotti software

Ogni Prodotto è caratterizzato da:

- Codice e descrizione.
- Tipologia.
- Funzioni.
- Metodo di aggiornamento.
- Responsabile del Prodotto.
- Data dell'ultima verifica.
- Periodicità della verifica espressa in mesi.
- Note interne.

NOTA: È possibile ottenere il riepilogo delle attività previste per i vari Responsabili in “Sistema Informatico”.

Data Base

Nota: Per Data Base si intende la situazione prevista dall'art. 4 Paragrafo 6 del GDPR, ovvero: “qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico”. In considerazione della maggiore “pericolosità” degli archivi rispetto ai dati personali sciolti, è opportuno che il titolare mantenga aggiornato, un elenco degli archivi di dati personali dallo stesso gestito. Per ciascun archivio dovrebbe essere individuato e nominato un responsabile, devono essere individuati coloro che accedono agli archivi e definiti gli specifici profili di autorizzazione. Il titolare dovrebbe definire, attuare e monitorare appropriati livelli di protezione per gli archivi, tenuto conto: della natura dei dati in essi presenti, del numero di dati personali in essi presenti, di coloro che hanno diritto ad accedervi.

Ogni Data Base è caratterizzato da:

- Codice e descrizione.
- Funzioni.
- Tipologia.
- Utenti Abilitati.
- Necessità di aggiornamento.
- Responsabile del Prodotto.
- Data dell'ultima verifica.
- Periodicità della verifica espressa in mesi.
- Note interne.

NOTA: È possibile ottenere il riepilogo delle attività previste per i vari Responsabili in “Sistema Informatico”.

Dispositivi Mobili

Ogni Dispositivo Mobile è caratterizzato da:

- Codice e descrizione.
- Assegnatario.
- Identificazione dei Dispositivi aziendali.
- Applicazioni installate.
- Responsabile del Dispositivo.
- Data dell'ultima verifica.
- Periodicità della verifica espressa in mesi.
- Note interne.

NOTA: È possibile ottenere il riepilogo delle attività previste per i vari Responsabili in “Sistema Informatico”.

1.3.5.2 Responsabilità

Per ogni Responsabilità possono essere definiti:

- Codice e descrizione.
- Tipo di responsabilità.
- Denominazione, Indirizzo, Telefono e e-mail (se significativo).
- Funzioni.
- Metodo di verifica dell'espletamento della Responsabilità.
- Nome del Responsabile delle Verifica.
- Data dell'ultima verifica.
- Periodicità della verifica espressa in mesi.
- Note interne.

NOTA: È possibile ottenere il riepilogo delle attività previste per i vari Responsabili in “Sistema Informatico”.

Ruoli e documento “Responsabilità per i Sistemi Informativi”

Per ogni Responsabile è possibile definire uno o più Ruoli al fine di ottenere il Documento “Responsabilità per i sistemi informativi”.

Documenti

Per ogni Responsabile è possibile creare specifici Documenti.

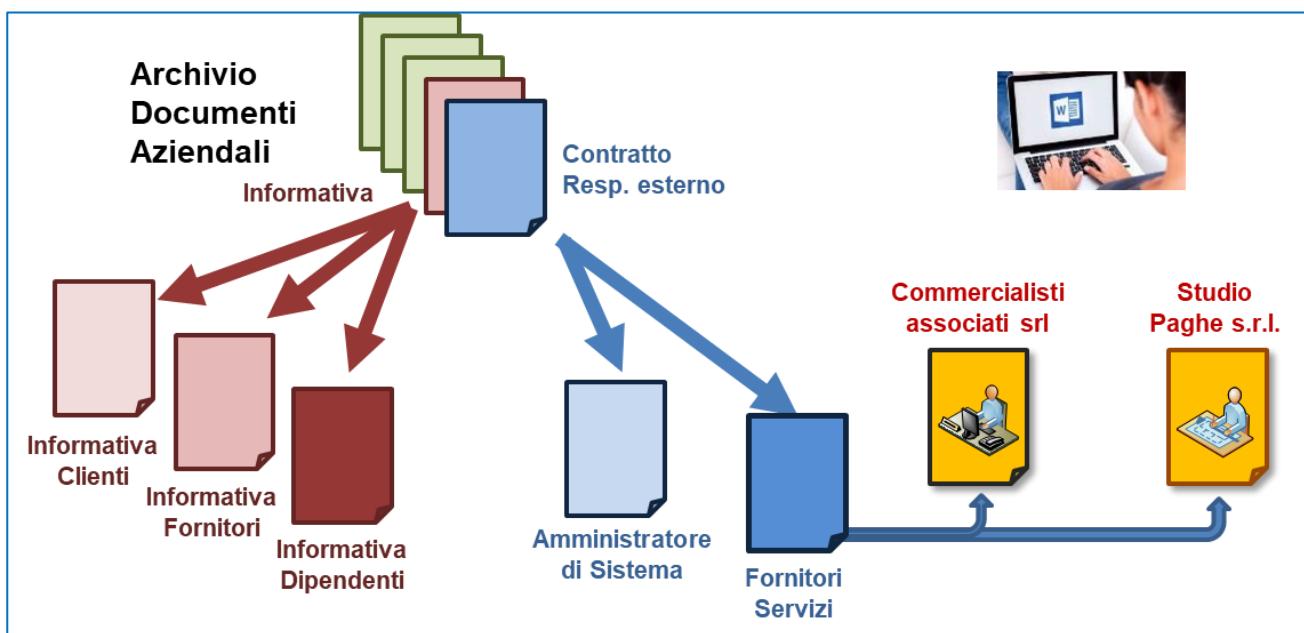
È possibile creare specifici documenti inserendo i vari testi ma, In genere si utilizzano i Documenti di Base o “Varianti” sui quali eventualmente (come già illustrato in precedenza) è possibile effettuare delle personalizzazioni aggiungendo testi specifici (se si utilizzano Codici dei testi non utilizzati) o sostituendo i testi (utilizzando per i nuovi testi gli stessi Codici).

Vengono presentati i testi finali con l'indicazione dell'origine:

- Specifico.
- Variante.
- Base

È necessario che tutti i testi valutati come “da personalizzare” siano stati personalizzati (o in una “variante” o nello specifico documento per il Responsabile).

È possibile richiedere la stampa del documento sia in formato WORD che in formato PDF.



Come abbiamo visto esiste un archivio dei documenti di base. Da ogni Documento è possibile produrre più varianti. Ogni Documento o Variante può essere ulteriormente personalizzato per il singolo Responsabile. Il documento finale è comunque prodotto in formato Word e quindi può essere ancora modificato come si desidera prima di renderlo ufficiale.

1.3.5.3 SGSI

Formazione

È possibile memorizzare i corsi di formazione. Ogni corso è caratterizzato, fra l'altro, dal Responsabile che dovrà gestire l'eventuale aggiornamento.

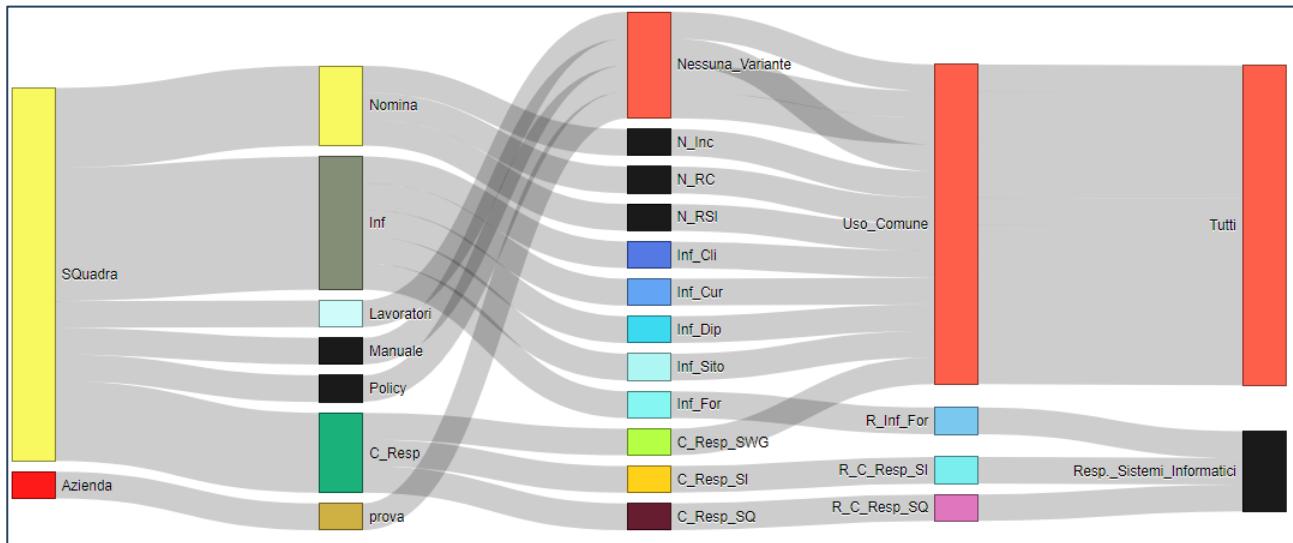
Per ogni corso è necessario definire i partecipanti. Se necessario, per ogni partecipante, è possibile effettuare la verifica delle competenze acquisite.

Scadenze per Responsabile

È possibile ottenere un elenco di tutte le scadenze relative ai vari Responsabili.

Presentazioni

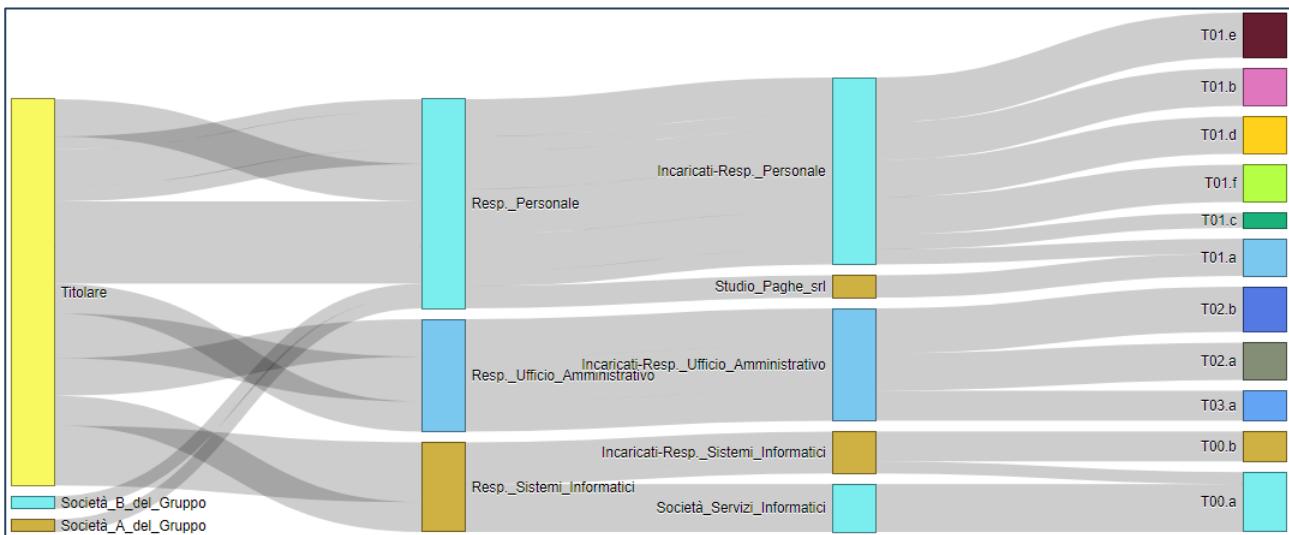
Vengono fornite alcune presentazioni grafiche al fine di fornire informazioni di sintesi sul sistema relativo alla gestione della Privacy.



È possibile visualizzare il sistema documentale con i Documenti base, le varianti e i documenti specifici per ogni responsabile.



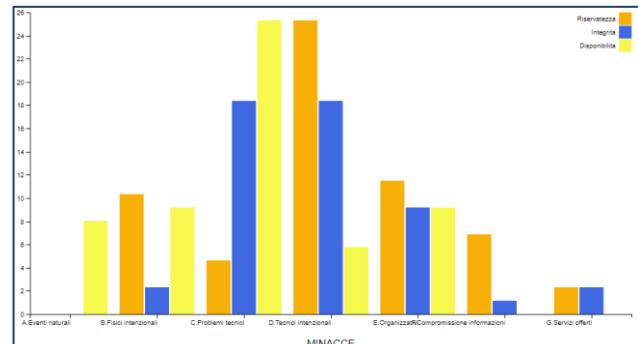
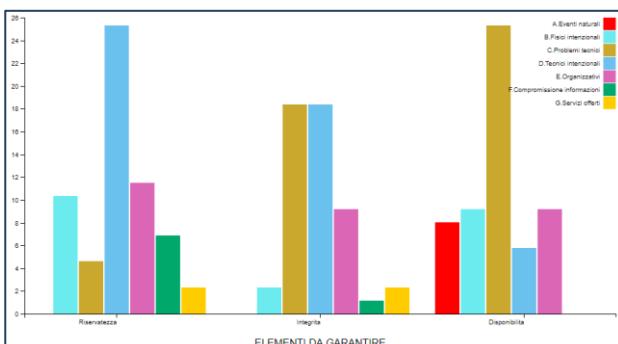
Possono essere visualizzati i rischi legati ai trattamenti analizzandoli secondo vari aspetti.



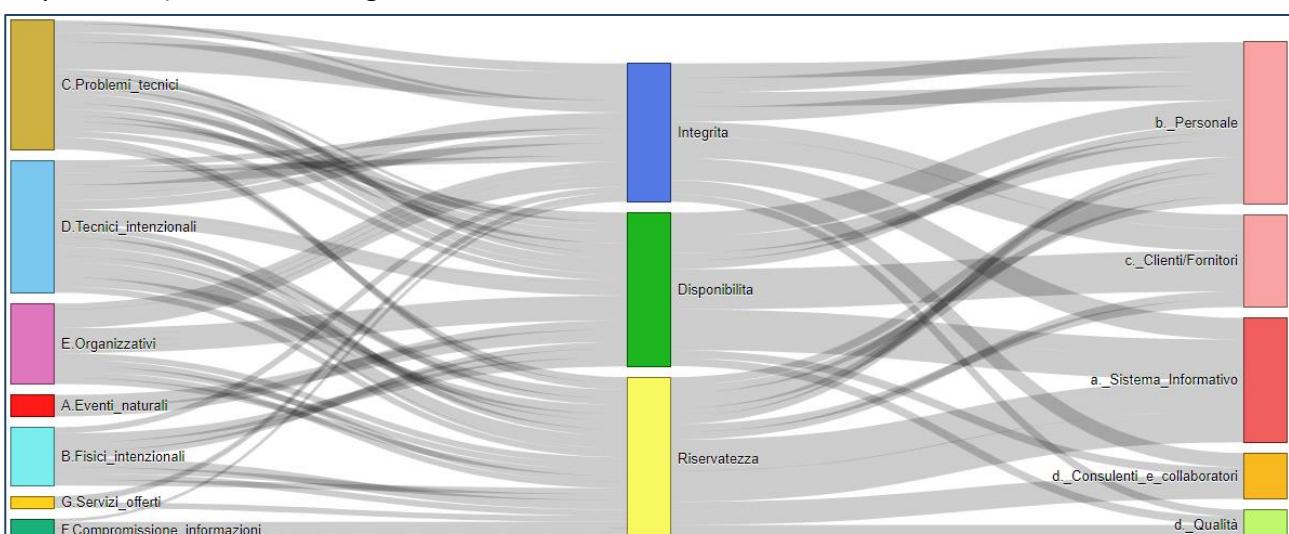
Possono essere analizzati i flussi delle responsabilità nei trattamenti.

Nella figura vengono presentati:

- Il Titolare e i Titolari di altre società per i quali si trattano i dati in qualità di Responsabile.
- I Preposti / Referenti che coordinano gli incaricati per conto del Titolare.
- Incaricati del trattamento e Responsabili esterni ai quali sono assegnate parti del trattamento.
- I vari Trattamenti.



È possibile analizzare la correlazione fra gli elementi da controllare (Riservatezza, Integrità e Disponibilità) e le varie famiglie di minacce.



È possibile analizzare la correlazione fra famiglie di minacce, elementi da controllare e aree di trattamento.

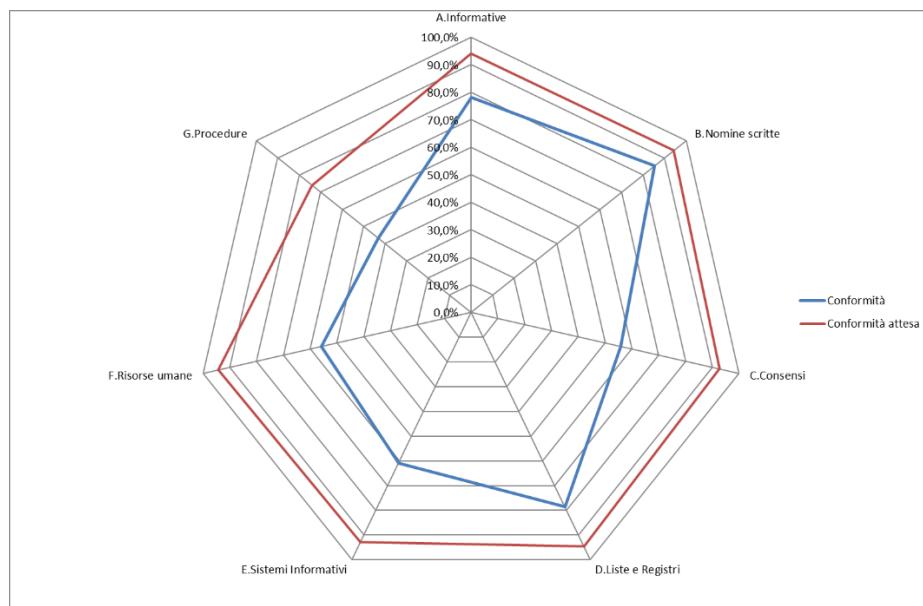
Report generale SGSI

È possibile ottenere un documento di Excel che racchiude nei vari Fogli tutte le attività svolte per il GDPR. È opportuno che questo documento venga stampato almeno annualmente, in occasione del riesame del sistema, ed archiviato per mostrare l'evoluzione del sistema stesso.

Conformità

Vengono riportate le informazioni relative alla Conformità.

Per ogni Argomento viene calcolata la conformità media e viene prodotto anche un grafico.



Conformità attuale ed attesa a fronte della corretta attuazione delle Misure Aggiuntive.

Trattamenti

Per ogni trattamento vengono riportate tutte le informazioni e, in funzione dell'importanza definita, viene calcolata l'incidenza (totale=100%).

Sempre per ogni trattamento viene calcolata l'incidenza pesata rispetto alle tre dimensioni (Riservatezza, Integrità e Disponibilità), utilizzando la scala: 0 se Non Significativa o Trascurabile; 1 per Bassa, 2 per Media, 3 per Alta e 4 per Critica.

Viene quindi calcolato (e riportato alla riga 2) il valore totale che indica l'importanza percentuale per l'azienda delle tre dimensioni (totale=100%).

Viene fornita anche una rappresentazione grafica della Rilevanza dei trattamenti.

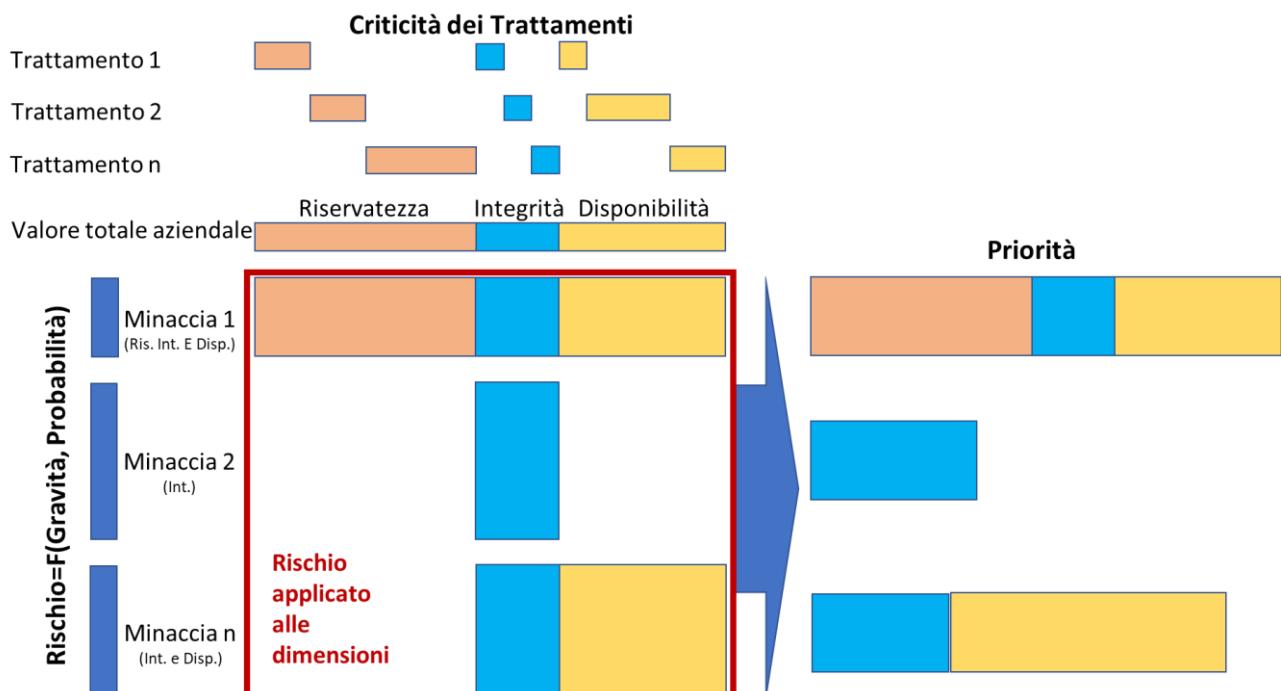
Vengono descritti tutti i Rischi, i Responsabili e i Titolari.

Minacce

Per ogni Minaccia viene presentato il Rischio (in funzione della Probabilità e della Gravità – vedi nell'appendice SGSI il capitolo relativo ai Rischi) e il valore percentuale corrispondente.

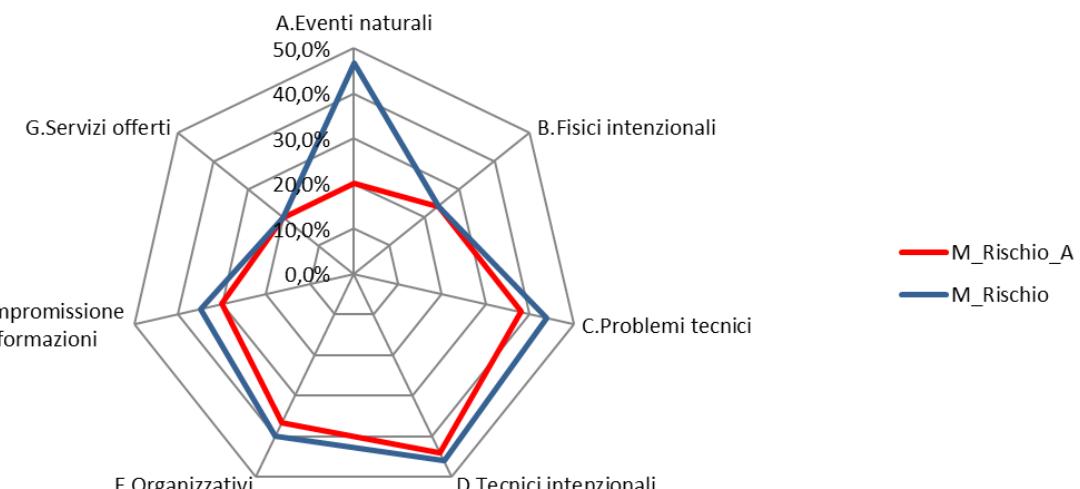
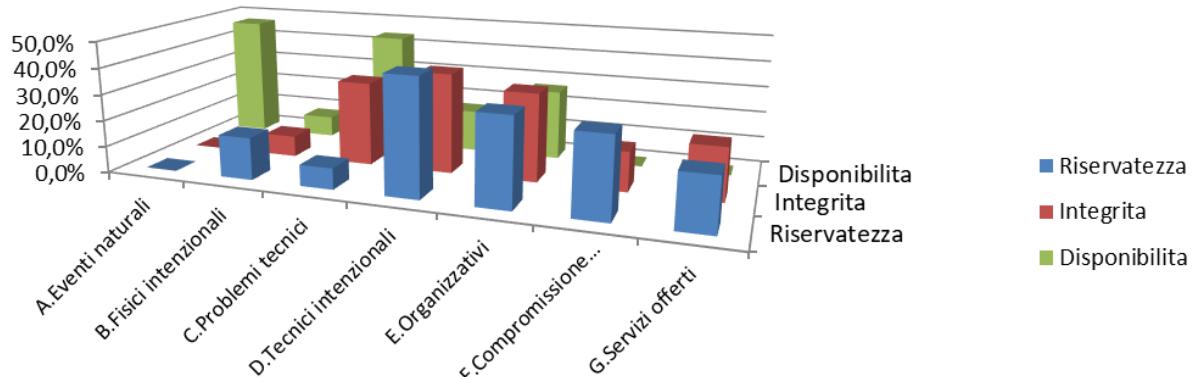
Viene quindi calcolato il Valore pesato come prodotto del rischio per l'effetto sulle tre dimensioni in base all'importanza aziendale di queste in base a quanto definito per i Trattamenti (vedi Foglio "Trattamenti" celle AU2:AW2).

Viene quindi determinata la Priorità di intervento per le varie Minacce. A seconda della criticità dei trattamenti rispetto a Riservatezza, Integrità e Disponibilità non è infatti detto che la priorità di intervento debba essere data alla Minaccia che presenta un maggiore Rischio come illustrato nella figura seguente.



Le Minacce vengono riunite per Tipologia per analizzare la correlazione con le tre Dimensioni.

Effetti delle Minacce



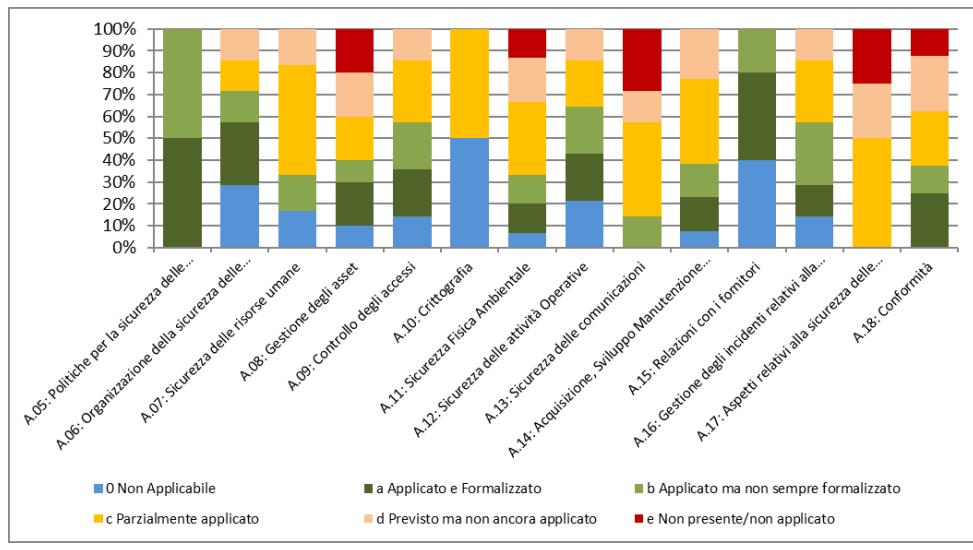
Media dei Rischii attuale ed attesi a fronte della corretta attuazione delle Misure Aggiuntive.

Controlli

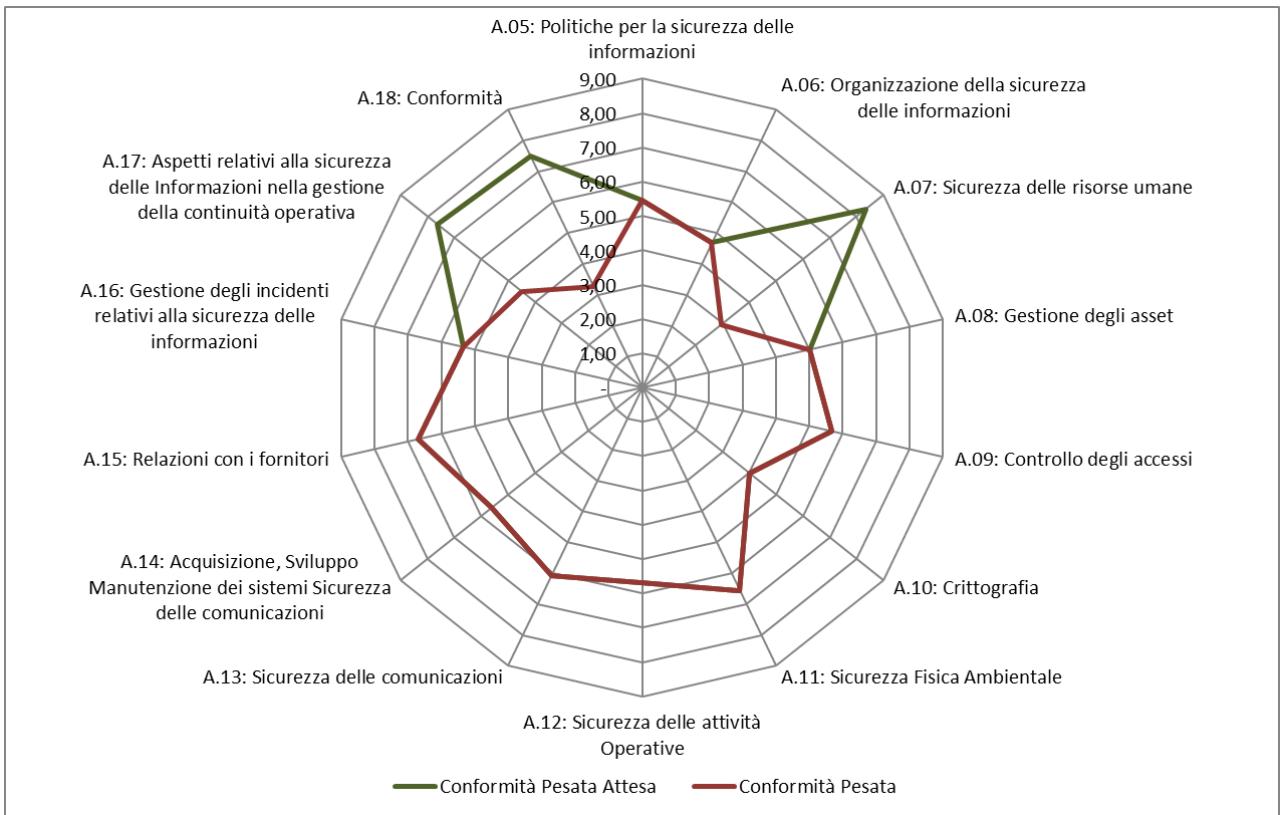
Vengono presentati tutti i Controlli previsti, ovviamente varranno compilati solo i fogli ritenuti significativi dall'azienda.

Per i controlli 27001 viene fornito un riepilogo per Aree.

Vengono anche forniti grafici per evidenziare i valori di Conformità indicati e la Conformità Pesata (in funzione della significatività) sia attuale che prevista a seguito della corretta attuazione delle Misure Aggiuntive previste.



Conformità dei Controlli 27001 per Area.



Conformità Pesata attuale ed attesa a fronte della corretta attuazione delle Misure Aggiuntive.

Apparati e Prodotti

Vengono presentati gli inventari aziendali con le informazioni sulle scadenze.

Responsabilità

Vengono riportati tutti i Responsabili con le informazioni sui tempi della verifica.

Formazione

Vengono riportate tutte le attività di formazione effettuate.

1.3.5.4 Importazioni

SQuadra GDPR permette di importare alcuni elementi.

Per ogni tipologia di importazione è necessario richiedere il File di Excel d'esempio nel quale andranno riempite le colonne di interesse.

Poiché il file d'esempio riporta i dati attuali si consiglia di inserire manualmente un elemento per comprendere meglio il significato delle varie colonne.

In ogni caso il file d'importazione deve contenere tutti gli elementi di interesse dato che i precedenti dati inseriti verranno cancellati prima di eseguire l'importazione.

Una volta compilato il file dovrà essere salvato e quindi selezionato per essere importato da SQuadra.

ATTENZIONE: è necessario che le colonne relative alle date ed ai valori numerici, se contengono un valore, questo deve essere appropriato altrimenti il programma segnalerà errore di conversione al momento dell'importazione.

1.4 Sistema di Gestione

Questa sezione offre un supporto per i sistemi di gestione per la Sicurezza (così come richiesti dall'Art. 30 del DLgs 81/08). Ovviamente è possibile utilizzare le funzionalità per un qualunque Sistema di Gestione (Qualità, Sicurezza e Ambiente).

1.4.1 ANALISI

1.4.1.1 Riesami della Direzione

È possibile archiviare tutti i Riesami della Direzione.

Ogni Riesame è caratterizzato dalla data di inizio della riunione e da altre informazioni fra le quali il numero dei mesi fra cui è previsto il prossimo Riesame (se l'attuale Riesame è un Riesame occasionale è possibile non prevederne una nuova pianificazione indicando 0 mesi).

INFORMAZIONI COLLEGATE

Analisi del Contesto

Per ogni Riesame è possibile effettuare una Analisi del Contesto come descritto nell'apposita Appendice.

Analisi per Processi

Per ogni Riesame è possibile analizzare gli Obiettivi per i vari Processi come descritto nell'apposita Appendice.

Informazioni documentate previste dalla ISO EN UNI 9001:2015.

Per ogni riesame è opportuno definire come vengono gestite, se significative, le varie informazioni documentate.

Determinazioni previste dalla ISO EN UNI 9001:2015.

La norma ISO 9001:2015, in diversi punti, usa la locuzione "deve determinare". Il verbo "determinare" implica un processo di scoperta che risulta in una conoscenza."

Dove è usato "determinare", anche se non c'è un requisito esplicito di "documentazione", l'organizzazione dovrebbe almeno essere in grado di dimostrare e dare confidenza di completezza e controllo di tali attività / processi.

Per ogni elemento previsto, se significativo, è opportuno definire come vengono determinati.

Sezioni del Riesame

Nota: Si veda, più avanti, "Oggetti del Riesame".

Per ogni Sezione del Riesame è possibile inserire, oltre alle informazioni di base:

Elementi di controllo

- *Lo stato delle azioni derivanti da precedenti riesami di direzione.*
- *Le modifiche di aspetti esterni e interni che sono pertinenti al sistema di gestione per la prevenzione della corruzione.*
- *Le informazioni sulla prestazione del sistema di gestione per la prevenzione della corruzione, includendo le tendenze relative: alle non conformità e alle azioni correttive; ai risultati del monitoraggio e della misurazione; ai risultati di audit; ai rapporti relativi alla corruzione; alle investigazioni; alla natura e all'entità dei rischi di corruzione affrontati dall'organizzazione.*
- *L'efficacia delle azioni intraprese per affrontare i rischi di corruzione.*

Obiettivi

- *Le opportunità per il miglioramento continuo del sistema di gestione per la prevenzione della corruzione.*
- Per ogni obiettivo viene indicato il Responsabile, le Risorse pianificate per il raggiungimento degli obiettivi ed i tempi previsti.

Ad ogni Sezione è possibile associare un allegato.

Documenti per il Riesame

Nota: Si veda, più avanti, "Oggetti del Riesame".

È possibile definire tutti i documenti che devono essere predisposti in preparazione del Riesame e che verranno analizzati nel corso dello stesso.

I documenti possono essere allegati.

Funzioni informatizzate utilizzate per il Riesame

Nota: Si veda, più avanti, "Oggetti del Riesame".

È possibile definire quali funzioni informatizzate, fra quelle che SQuadra mette a disposizione o fornite da altri programmi, vengono utilizzate.

Il corretto aggiornamento di queste funzioni sarà elemento di valutazione del Riesame.

Anche in questo caso è possibile aggiungere allegati quali, ad esempio alcune delle stampe prodotte per evidenziare lo stato di applicazione del sistema.

Informazioni Documentate

Nota: Si veda, più avanti, "Oggetti del Riesame".

Nel corso del Riesame è possibile voler verificare la corretta gestione di alcune informazioni documentate.

FUNZIONALITÀ PER I RIESAMI

Analisi del Contesto

È possibile ottenere un documento di Excel e due di Word (uno riepilogativo ed uno per Linea di Business) con la descrizione dell'analisi del Contesto.

Nel documento di Excel, nel foglio “Fattori”, qualora siano stati definiti, vengono riportati fra i Fattori Esterni anche i Rischi e le Opportunità definite per i vari Processi (vedi sotto). Verranno inseriti fra i 4 livelli in funzione del “Rischio Residuo / Opportunità da cogliere”.

È inoltre possibile copiare l'analisi del Contesto dal precedente Riesame per avere una base di partenza sulla quale fare le opportune modifiche.

Rischi ed Opportunità per i vari Processi

Viene fornito un documento di Excel ed uno di Word con l'analisi dei Rischi ed Opportunità per i vari Processi.

È possibile anche ottenere 2 rappresentazioni grafiche della situazione attuale.

È inoltre possibile copiare l'analisi dei Processi con relativi Rischi ed Opportunità dal precedente Riesame per avere una base di partenza sulla quale fare le opportune modifiche.

Stampa del Riesame.

Verrà prodotta la stampa del Riesame in base alle informazioni inserite nell'apposita “cartella”.

Ad esempio, è possibile ottenere, sotto ogni elemento di interesse, le procedure collegate per avere evidenza degli elementi significativi per il Riesame.

È possibile richiedere che, per ogni Sezione del Riesame, vengano definiti gli Elementi (Fattori Interni ed Esterni e Rischi ed Opportunità collegati ai vari Processi) di supporto per le attività, gli Elementi influenzati dalle attività e le aspettative delle Parti Interessate. Di questi elementi è possibile anche avere 2 rappresentazioni grafiche dei flussi.

Se definite è possibile stampare le modalità di gestione delle Informazioni documentate e gli elementi determinati.

È possibile ottenere la stampa di tutti gli allegati collegati al Riesame.

Importazione elementi per il Riesame

È possibile chiedere al programma l'importazione dalle Procedure (in base a quanto indicato come "Oggetti del Riesame" vedi avanti nel presente Manuale) delle Sezioni, dei Documenti utili per il Riesame, delle Informazioni Documentate previste dal Sistema e delle Funzioni gestite da specifici software.

1.4.1.2 Oggetti del Riesame

Come abbiamo visto, per ogni Riesame è possibile definire:

- Le Sezioni del Riesame stesso.
- I Documenti preparatori.
- La gestione delle Informazioni Documentate.
- Le funzioni del sistema gestite da specifici strumenti software.

Collegamento con le Procedure per i Punti della Norma

Queste informazioni possono essere ricavate in automatico in funzione di quanto descritto nelle Procedure predisposte per rispondere ai vari punti della Norma.

Questa funzione permette di definire come verranno individuati gli elementi di interesse per il Riesame dalle Procedure.

È necessario indicare quale frase precede l'informazione di interesse e se ricercarla nel campo Registrazione o nel campo Note.

Collegamento con i Controlli 27001

Le informazioni possono essere ricavate anche da quanto inserito come Riferimento nei Controlli 27001.

Anche in questo caso è necessario indicare quale frase precede l'informazione di interesse.

1.4.1.3 Criteri della Direzione

La direzione deve definire il Livello di Rischio Residuo) a seguito delle Misure Attuali previste a fronte di ogni Rischio/Opportunità per i vari Processi) oltre il quale devono essere previste Misure Aggiuntive.

1.4.1.4 Obiettivi

NOTA: Nelle recenti versioni delle Norme Internazionali che adottano la nuova Struttura di alto livello definita da ISO individuano la necessità di analizzare il "Contesto dell'organizzazione" per determinare i rischi e le opportunità al fine di prevenire, o ridurre, gli effetti indesiderati e accrescere gli effetti desiderati. Andranno quindi pianificate le azioni per affrontare questi rischi e opportunità.

Periodi di Analisi

Ogni Ente può effettuare periodiche analisi della realtà aziendale nella quale andranno definiti gli Obiettivi.

Ogni Periodo è caratterizzato dalla Data di Approvazione e, in genere, corrisponde ai Riesami della Direzione (anche se è possibile anche porsi degli Obiettivi pluriennali).

Obiettivi

Per ogni Obiettivo è necessario definire l'Importanza Strategica (relativa rispetto agli altri Obiettivi):

- Altissima.
- Molto Alta.
- Alta.
- Media.
- Bassa.
- Molto Bassa.
- Trascurabile.

Per ogni Obiettivo possono essere inseriti:

- Responsabile del raggiungimento dell'Obiettivo.
- Tempi previsti per l'attuazione.
- Frequenza prevista per il monitoraggio.
- Elementi che verranno utilizzati per la valutazione del raggiungimento dell'Obiettivo.

Per ogni Obiettivo devono essere analizzati Rischi ed Opportunità.

Rischi / Opportunità

Per ogni Rischio/Opportunità deve essere indicata l'Importanza relativa rispetto all'Obiettivo.

Per ogni Rischio/Opportunità deve essere valutata l'Efficacia delle Azioni in atto (eventualmente già presenti al momento dell'approvazione) e deve essere indicato quale Efficacia si prevede possa essere raggiunta una volta completate tutte le Azioni previste.

Per ogni Rischio/Opportunità devono essere definite le Azioni necessarie.

Azioni

Per ogni Azione ("cosa sarà fatto"¹¹) deve essere indicata l'importanza relativa dell'Azione rispetto al Rischio/Opportunità.

Per ogni Azione può essere definito:

- Area interessata.
- Processo coinvolto.
- Risorse previste ("quali risorse saranno richieste").
- Responsabile ("chi ne sarà responsabile")
- Tempi previsti ("quando saranno conseguiti gli obiettivi").
- Modalità di Valutazione ("come saranno valutati e riferiti i risultati").

¹¹ Si veda in particolare il punto 6.2 della 37001 punto 6.2 - Obiettivi per la prevenzione della corruzione e pianificazione per il loro raggiungimento nel quale, per le attività per raggiungere gli obiettivi, si riprendono gli elementi presenti nella 9001 e nella 14001 aggiungendo un punto sul controllo ed applicazioni di sanzioni e penalità.

- Controllore (“chi comminerà sanzioni e penalità” [solo per la 37001]).
- Frequenza previste per le Valutazioni.

Per ogni Azione è necessario definire la Valutazione Iniziale.

Valutazioni

Periodicamente sarà necessario effettuare delle Valutazioni sull'avanzamento delle Azioni e l'efficacia raggiunta per la gestione dei Rischi e delle Opportunità.

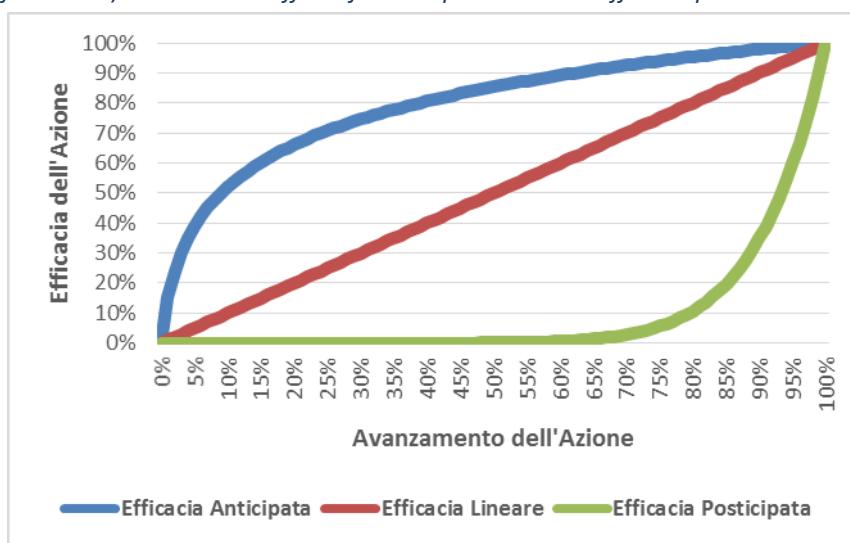
Fra le Valutazioni una può essere scelta come Attuale.

Le valutazioni effettuate sull'Efficacia delle Azioni in atto per i Rischi/Opportunità e sulla Percentuale di avanzamento delle varie Azioni permettono di controllare le attività svolte per raggiungere gli Obiettivi.

NOTA: vengono richieste 2 valutazioni separate sull'Efficacia delle Azioni e sul loro Avanzamento.

I due valori infatti sono correlati in modo differente da caso a caso. Solo in casi particolari vi è una corrispondenza lineare fra Avanzamento dell'Azione e Efficacia. In alcuni casi solo il completamento di una Azione ha Efficacia.

Ad esempio nella predisposizione di un Sito aziendale l'avanzamento dell'Azione (la preparazione dei testi, l'impostazione grafica e la verifica fuori linea) non ha alcun effetto fino alla pubblicazione effettiva pari al 100% dell'Azione stessa.



ANALISI DEL PERIODO

Stampa

È possibile ottenere un documento di Word con tutte le informazioni relative agli Obiettivi, Rischi/Opportunità, Azioni ed alle valutazioni effettuate.

Avanzamento

Un documento di Excel riunisce tutte le elaborazioni e fornisce l'evidenza dello stato d'avanzamento delle azioni.

Priorità Base

È evidente che sarà necessario assegnare la massima Priorità agli Obiettivi che hanno una Importanza MOLTO ALTA ed una valutazione sull'Efficacia delle Azioni per il Rischio/Opportunità MOLTO BASSA. Avranno ovviamente Priorità nulla gli Obiettivi per i quali l'Efficacia delle Azioni è già MOLTO ALTA.

Per tutte le altre combinazioni è necessario definire una relazione. È possibile utilizzare varie formule. SQuadra utilizza una scala Lineare per la valutazione dell'Efficacia, una scala quadratica per l'Importanza dagli Obiettivi e di ottenere la Priorità come prodotto fra questi valori.

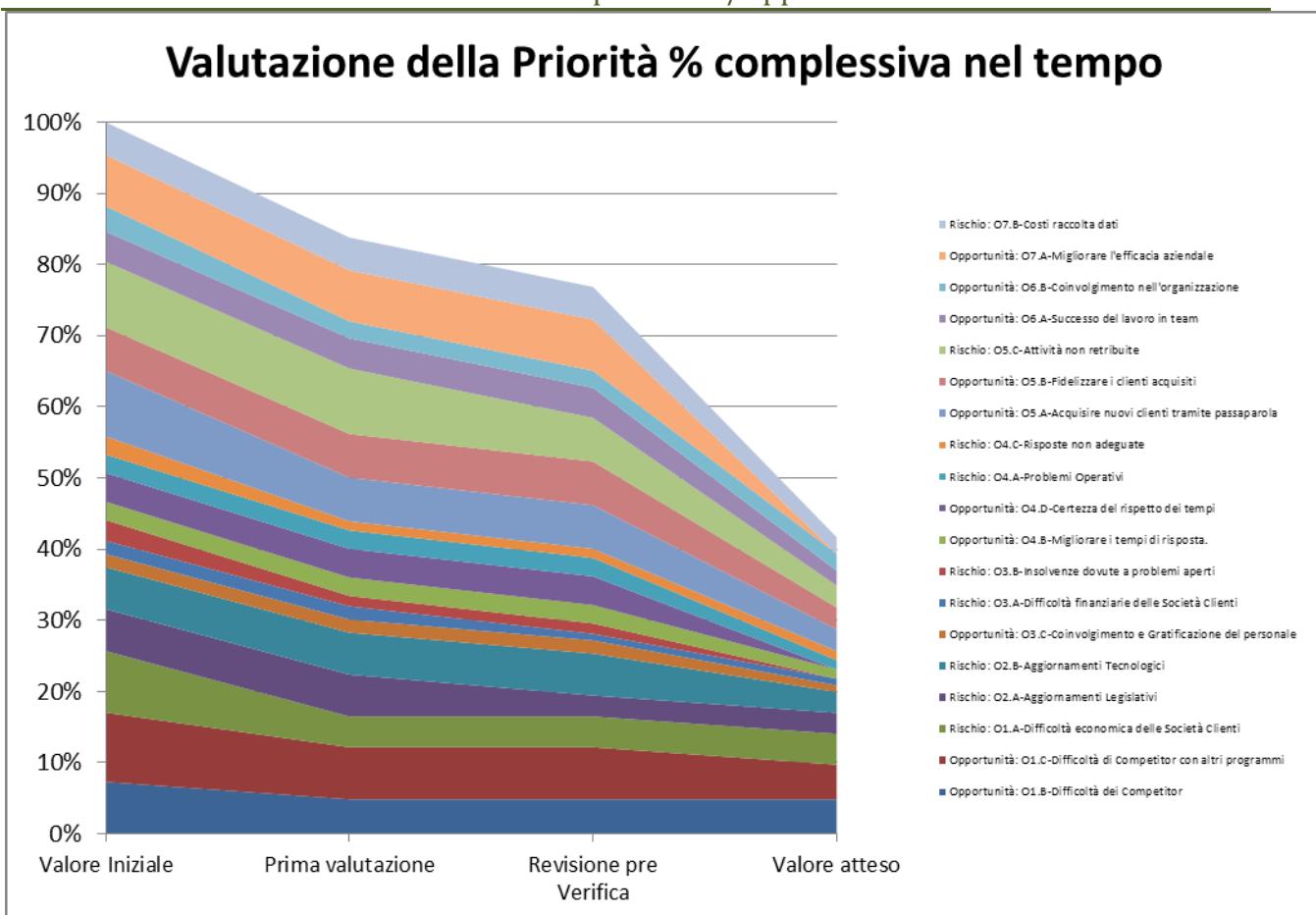
Efficacia Trascurabile	Obiettivo 6
	0

Molto Bassa	5	1
Bassa	4	4
Media	3	9
Alta	2	16
Molto Alta	1	25
Altissima	0	36

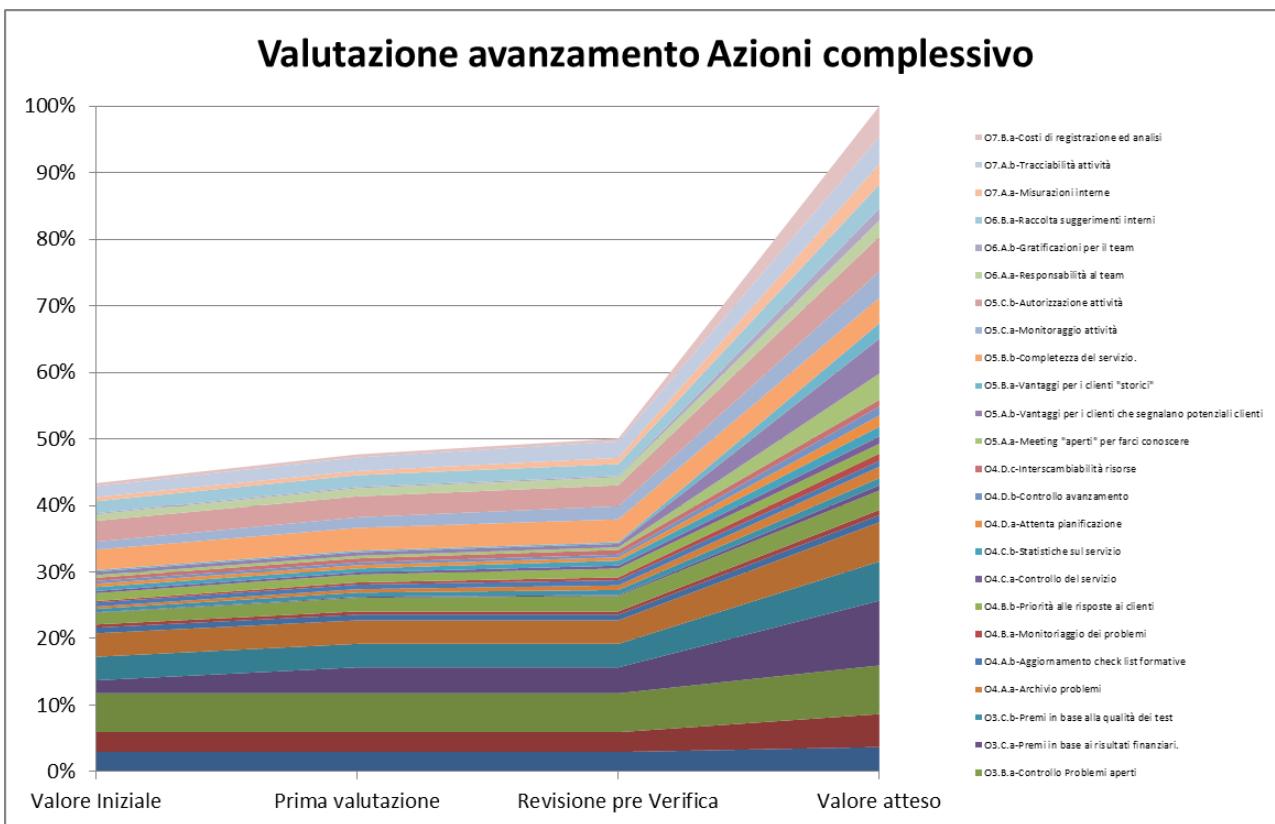
		Efficacia della azioni per Rischio/Opportunità						
		Trascurabile	Molto Bassa	Bassa	Media	Alta	Molto Alta	Altissima
Importanza obiettivi	Trascuribile	0	0	0	0	0	0	0
	Molto Bassa	6	5	4	3	2	1	0
	Bassa	24	20	16	12	8	4	0
	Media	54	45	36	27	18	9	0
	Alta	96	80	64	48	32	16	0
	Molto Alta	150	125	100	75	50	25	0
	Altissima	216	180	144	108	72	36	0

Gli stessi concetti si utilizzano per i vari Rischi/Opportunità nei quali si scomponete un Obiettivo.

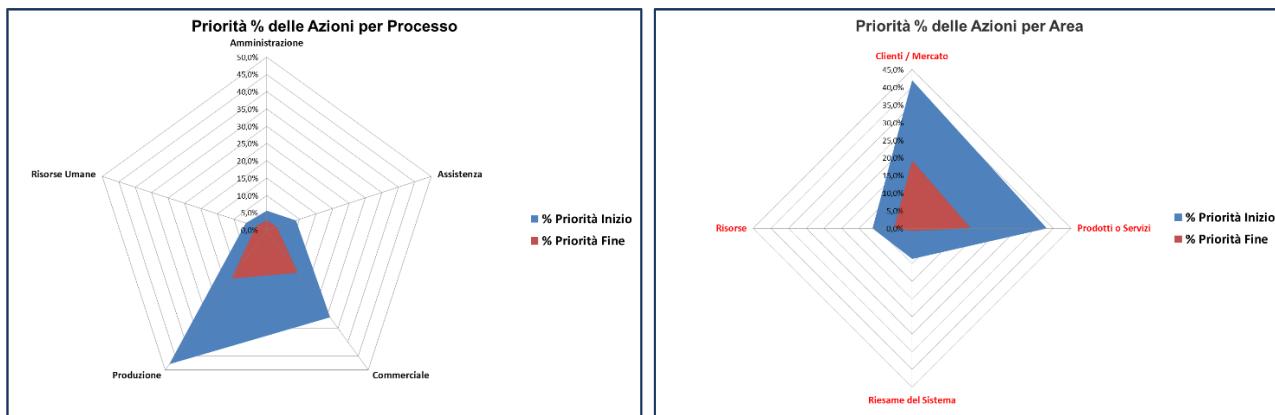
Valutazione dell'Avanzamento dell'efficacia per Rischi/Opportunità



Il valore della valutazione iniziale viene “normalizzato” ad un valore complessivo pari a 100% e tutte le altre valutazioni attese ed intermedie vengono riportate rispetto a questo valore.



Analogamente è possibile analizzare le valutazioni sull'avanzamento delle varie Azioni. In questo caso viene “normalizzato” la conclusione di ogni Azione ad un totale pari al 100%.



È infine possibile analizzare la situazione Iniziale e Finale per Processo e per Area.

SQquadra fornisce anche le stime delle date previste per la conclusione delle operazioni in base ad una ipotesi di completamento lineare rispetto all'efficacia o all'avanzamento. Queste stime servono solo a dare una indicazione di massima sul rapporto fra il tempo effettivamente trascorso e il raggiungimento degli obiettivi.

DUPLICAZIONE DEL PERIODO DI ANALISI

Tutte le informazioni del Periodo di Analisi possono essere duplicate per creare un nuovo Periodo laddove la Direzione desideri modificare Obiettivi / Rischi e Opportunità / Azioni.

1.4.2 PIANIFICAZIONE

1.4.2.1 Prescrizioni

Si rimanda all'apposita Appendice "Conformità legislativa e ad altre prescrizioni" che può essere utilizzata direttamente come Istruzione del Sistema di Gestione Aziendale.

1.4.2.2 Asseverazione

Check-list Documentazione e Applicazione

Vengono riportate le check-list di controllo previste dalla Prassi di riferimento UNI (si veda l'APPENDICE relativa all'Asseverazione).

È possibile per ogni elemento ritenuto significativo descrivere:

- Le indicazioni specifiche previste dal sistema di Gestione della Sicurezza dei Lavoratori (SGSL).
- La significatività per l'azienda.
- Il Responsabile.
- La periodicità con la quale controllare l'elemento.
- La data dell'ultimo Aggiornamento o Verifica.
- Il Nominativo di chi ha effettuato la Verifica.
- L'oggetto della Verifica (La Sede, un Cantiere, ecc.).
- Una Valutazione su 7 livelli predefiniti.
- Una descrizione della Verifica effettuata.

È possibile aggiungere degli Allegati ad ogni Elementi.

Nella stampa è possibile richiedere anche i suggerimenti previsti dal Manuale CNCPT.

È possibile ottenere la stampa per Responsabile in modo da assegnare le parti di competenza alle varie persone coinvolte.

SGSL: Scheda per l'Analisi Iniziale

È possibile inserire i dati essenziali per:

- Descrizione dell'organizzazione e del sito:
 - Dati societari (sede legale, ragione sociale, Iscrizione registro Imprese, codice fiscale, partita IVA ecc.).
 - Definizione dell'Organizzazione oggetto del Sistema (Struttura sociale, persone, ecc.).
 - Organigramma (collegamenti tra le funzioni aziendali e quelle della sicurezza [RSPP, ASPP, MC, RLS ecc.]).
 - Procedure operative di sicurezza e salute del lavoro (ove esistenti).
- Collocazione / Descrizione dell'Azienda:
 - Collocazione geografica e ubicazione (Indirizzo, contesto (urbano/extr), raggiungibilità ecc.).
 - Presenza di elementi significativi di interferenza circostanti (Presenza di aziende a rischio incidente rilevante, scuole, ospedali ecc. se ciò può essere significativo a seguito dei processi gestiti).
 - Descrizione luoghi di lavoro (la struttura: superfici, piani edificio, destinazioni d'uso, numero di scale, vie d'uscita ecc.).

- Presenza di attività lavorative interferenti (imprese in appalto, lavoratori autonomi, terziarizzazione di parte delle lavorazioni, ecc.) – Bisognerà valutare se vi sono e di che tipo attività lavorative svolte da terzi che interferiscono nella attività aziendali.
- Andamento:
 - Incidenti (eventi correlati al lavoro, non previsti, potenzialmente pericolosi ma che non determinano danni alle persone. Analisi dell'evento, causa, persone/cose coinvolte, eventuali ripercussioni ecc. N° eventi, ripetibilità, confronto nei periodi lunghi/brevi, ecc.).
 - Infortuni (evento correlati al lavoro, non previsti e che hanno causato danni alle persone. Analisi dell'evento, causa, persone/mansioni coinvolte, eventuali ripercussioni ecc. N° eventi, ripetibilità, confronto nei periodi lunghi/brevi, ecc.).
 - Malattie professionali (malattie causate dalla attività lavorativa (patologie, esposizione, rischi collegati, periodo di esposizione ecc.). N° malattie, periodo di interesse, mansioni coinvolte, processo coinvolto, ecc.).
 - Emergenze (eventi inaspettati e imprevedibili che determinano condizioni di pericolo grave ed immediato (ad esempio incendi, eventi sismici, fughe di sostanze pericolose, ecc.). Analisi dell'accaduto, cause, danni, persone/cose coinvolte, tempi, ripristino condizioni regolarità ecc. N° eventi, ripetibilità, tempi, ripristino, mancanza di procedure, procedure non corrette ecc.).
- Note:
 - Note generali.
 - Data dell'ultimo aggiornamento.
 - Responsabile dell'analisi.

SGSL: Politica, Obiettivi e Azioni

Squadra permette di definire i vari elementi della Politica definendo l'importanza relativa.

Per ogni elemento è possibile definire vari Obiettivi, anch'essi caratterizzati dall'importanza relativa).

Per ogni Obiettivo verranno definite le Azioni:

- I relativi Indicatori.
- La Priorità relativa.
- Il Responsabile.
- Costi e Tempi previsti.
- Note interne.

SGSL: Monitoraggio di Primo e Secondo Livello

DALLE LINEE GUIDA UNI-INAIL PER UN SISTEMA DI GESTIONE DELLA SALUTE E SICUREZZA SUL LAVORO

Al fine di verificare la gestione degli aspetti aziendali relativi alla SSL, le modalità di realizzazione di tale gestione ed il rispetto dell'obiettivo di miglioramento continuo in questo ambito l'azienda prevede due livelli di monitoraggio.

1 Monitoraggio di primo livello

Questo livello di monitoraggio prevede le verifiche del raggiungimento degli obiettivi relativi all'adozione delle misure di prevenzione e protezione e i progressi nell'attuazione di tali attività.

Tali monitoraggi, svolti in autocontrollo da parte dell'operatore adeguatamente formato sui contenuti della presente procedura, o da parte del preposto o del dirigente, o da altri soggetti interni od esterni per aspetti specialistici, sono di competenza delle risorse indicate nel documento "Organigramma aziendale della sicurezza" scegliendo tra coloro che hanno avuto un ruolo partecipativo nella valutazione dei rischi.

La pianificazione dei monitoraggi di primo livello è definita dal datore di lavoro che ne stabilisce la periodicità in collaborazione con il responsabile del sistema ed i dirigenti

La documentazione relativa ai monitoraggi di primo livello consiste nel siglare le misure preventive e correttive attuate sul piano di attuazione degli interventi del documento di valutazione dei rischi. Detto piano conterrà tutti gli interventi previsti a seguito di

diversi livelli e specificità della valutazione che possono essere oggetto di integrazioni ed aggiornamenti della stessa (aggiornamento generale del DVR, valutazione rischi chimico, incendio, esplosione, rumore, ecc.).

2 Monitoraggio di secondo livello

Il sistema di monitoraggio interno, strutturato dall'azienda, viene eseguito da soggetti competenti (dirigenti, rappresentanti della sicurezza o dipendenti) che hanno ricevuto una formazione adeguata, indipendenti dall'area/reparto preso in esame, con lo scopo di:

- a) Fornire informazioni sulla validità e affidabilità del sistema ed evidenziare le capacità dell'impresa di sviluppare le politiche in materia di sicurezza e di migliorare il controllo dei rischi.*
- b) Far intraprendere le opportune azioni preventive e correttive evidenziate dalle attività oggetto del monitoraggio e garantire che i progressi di attuazione di tali azioni correttive siano seguiti in base ai piani previsti.*
- c) Valutare l'efficacia complessiva dell'attuazione delle politiche di SSL all'interno dell'impresa.*

SQuadra consente di pianificare i monitoraggi (sia di Primo che di Secondo Livello) e di archiviare i risultati tenendo sotto controllo la chiusura delle eventuali Non Conformità rilevate.

Per i controlli di Primo Livello si può fare riferimento alle schede di controllo disponibili in VARIE / DOCUMENTI DI SUPPORTO.

Per i controlli di Secondo Livello si può fare riferimento alle Liste di controllo:

- Sugli aspetti Operativi previste dalla "PRASSI DI RIFERIMENTO - UNI/PdR 2:2013" Indirizzi operativi per l'asseverazione nel settore delle costruzioni edili e di ingegneria civile.
- Sui POS.
- Sui PRIMUS.

SGSL: Audit

SQuadra permette di memorizzare gli Audit effettuati.

Per ogni Audit è possibile definire:

- Un Codice.
- La data prevista.
- La data di effettivo svolgimento dell'Audit.
- Il Responsabile dello svolgimento dell'Audit.
- Obiettivi (Verifica del sistema aziendale per l'adempimento degli obblighi giuridici in materia di SSL, verifica della conformità nell'applicazione di disposizioni interne in materia di SSL, verifica della rispondenza ai requisiti del SGSL, ecc.).
- Estensione (L'audit si sviluppa su tutti i luoghi e per tutte le attività dell'unità produttiva, ivi comprese quelle affidate a Dritte esterne, che ricadono sotto l'area di responsabilità dell'organizzazione stessa oppure si svilupperà su una parte dei luoghi di lavoro).
- Persone Coinvolte (Datore di lavoro, RSPP, RLS/RLST, Medico Competente, Dirigenti, Preposti).
- Documenti di riferimento (NORME DI LEGGE vigenti in materia di SSL, SGSL, ISO 45001, Linee Guida SGSL — UNI 2001).
- Area (Area del Sistema, Unità Produttiva Attività controllate).
- Note interne.

SGSL: Rilievi e Non conformità

Ove necessario è possibile registrare eventuali Rilievi e Non Conformità.

Ogni Rilievo o Non conformità è caratterizzato da:

- Codice.
- Livello (da semplice Rilievo ad effettiva Non Conformità).
- Stato (da Registrata a Trattamento verificato).
- Evidenza origine del Rilievo e Non Conformità.

- Trattamento.
- Responsabile del Trattamento.
- Data Previste ed effettiva del Trattamento.
- Note relative alla Chiusura.
- Verificatore.
- Data di chiusura.

NOTA: È possibile rivedere tutti i Rilievo / Non Conformità relativi a tutti gli Audit ma è possibile aggiungerli o cancellarli solo dall'Audit.

SGSL: Archivio Documenti

È possibile archiviare:

- Procure.
- Incarichi.
- nomine.
- Autorizzazioni.

Per ogni elemento è possibile inserire una data di scadenza ed il Responsabile.

SGSL: Riesami

È possibile definire i vari Riesami.

Ogni Riesame è caratterizzato da:

- Un Codice.
- La data di svolgimento.
- Le persone presenti al Riesame.
- Valutazione sulla validità della Politica con l'indicazione della conferma o delle modifiche da apportare.
- Eventuali decisioni di carattere generale intraprese.
- Eventuali documenti di Output (Programma di Miglioramento, Programma di Formazione, ecc.).

Vengono poi presentati i vari elementi (Risultato monitoraggio interno, Esiti azioni intraprese, ecc.) per ognuno dei quali andranno definiti:

- Esiti.
- Documenti.
- Decisioni.

Check-list per un SGSL basato sulle procedure semplificate per piccole e medie imprese

Viene riportata la check-list di dettaglio, proposta dal FSC di Torino, per un corretto svolgimento delle verifiche documentali e tecniche relative al SGSL realizzati in conformità con le "Procedure semplificate per l'adozione dei modelli di organizzazione e gestione nelle piccole e medie imprese (PMI)" approvate con D.M. 13/02/2014.

Check-list per la verifica del DVR

Viene riportata la check-list, proposta dal FSC di Torino, relativa al documento di valutazione dei rischi aziendali (DVR). La check-list tiene conto di quanto previsto dagli artt. 28 e 29 del D.Lgs.

81/2008: le voci da 1 a 8 riguardano i contenuti del DVR e le voci da 9 a 14 riguardano le modalità di valutazione dei rischi.

Check-list per l'analisi dei Rischi specifici all'interno del DVR

Viene riportata la check-list, proposta dal FSC di Torino, per i rischi specifici.

Per ogni elemento è riportato il riferimento che, se uguale a 28/3 (Art. 20 comma 3) indica rischi per i quali il D.Lgs. 81/08 prevede specifici "Titoli" e/o "Capi" nei quali stabilisce ulteriori indicazioni sulla valutazione dei rischi.

È possibile fornire indicazioni generali e quindi specifiche per:

- Misure tecniche organizzative.
- Sorveglianza sanitaria.
- Informazione, formazione e Addestramento.
- DPI.
- Procedure d'emergenza.
- Segnaletica sicurezza.
- Altro.

Check-list per il Monitoraggio POS e PiMUS

Sono riportate le check-list, proposte dal FSC di Torino, relative ai POS e ai PiMUS che possono essere utilizzate per i Monitoraggi di Secondo Livello.

Check-list per la verifica dell'Organismo di Vigilanza e del Sistema Disciplinare

Viene riportata la check-list, proposta dal FSC di Torino, relativa all'OdV ed al Sistema Disciplinare.

Il MOG deve prevedere un sistema di controllo sull'attuazione del medesimo modello e sul rispetto nel tempo delle condizioni di idoneità delle misure adottate, come previsto dall'art. 30 comma 4 del D.Lgs 81/2008; tale sistema di controllo è costituito dal cosiddetto Organismo di Vigilanza (OdV). In particolare la vigilanza è effettuata in merito alla conformità del MOG, al raggiungimento degli obiettivi, alla sua corretta applicazione (compresa l'adeguatezza delle verifiche sull'applicazione delle procedure) e al mantenimento nel tempo dei suoi requisiti

Il sistema disciplinare-sanzionario è un requisito indispensabile di un MOG, è previsto dall'art. 30 comma 3 del D.Lgs 81/2008 e deve essere idoneo a sanzionare il mancato rispetto delle misure e procedure individuate dal modello stesso.

Stampe Check-list

È possibile ottenere le varie stampe.

1.4.2.3 Documentazione aziendale relativa alla sicurezza sul lavoro

Il modulo Documentazione per la Sicurezza è stato realizzato sulla base della check list predisposta dagli SPISAL della provincia di Treviso (<http://www9.ulss.ti.it/Minisiti/spisal/trasparenza.html>) Check List di Autovalutazione: Scheda 1 – Versione 15 del 02/01/2017) allo scopo di dare un'interpretazione uniforme alla normativa e di garantire alle imprese la chiara individuazione e l'agevole reperimento delle informazioni sui principali obblighi e sui relativi adempimenti imposti.

Vengono elencati i principali documenti relativi alla sicurezza sul lavoro di cui l'azienda deve essere in possesso.

Documentazione di dettaglio

In alcuni casi, per facilitare il riferimento alle norme, gli adempimenti vengono indicati separatamente e in modo analitico; è tuttavia possibile che un **unico documento** abbia i contenuti necessari e i requisiti per adempiere a più di uno degli obblighi riportati nelle tabelle successive. In questo caso è possibile dichiarare il Documento di dettaglio come “Non Significativo” indicando, nelle Note, il Documento all’interno del quale è racchiuso (ad esempio il DVR può contenere, al proprio interno, il “Calcolo o misura del livello di esposizione a campi elettromagnetici” se ritenuto significativo).

Informazioni su Obbligatorietà e Conservazione

Alcuni documenti sono **obbligatori** per tutte le aziende e in tutti i settori di attività. L’obbligatorietà degli altri documenti, non proposti come tali dal programma, dipende dall’effettiva presenza di una condizione particolare specificata nelle note dei vari documenti.

Alcuni documenti devono OBBLIGATORIAMENTE essere **conservati nella sede dell’unità locale a cui si riferisce il documento, o in cantiere**, a disposizione del personale che effettua la vigilanza. L’indisponibilità degli stessi presso l’unità produttiva è sanzionata a prescindere dalla loro esistenza in altra sede aziendale o presso i consulenti.

Significatività

In una prima analisi è opportuno segnalare come NON SIGNIFICATIVI tutti i Documenti non di interesse o, come detto precedentemente, racchiusi in altri documenti.

È opportuno indicare nelle NOTE le motivazioni per cui non sono stati ritenuti significativi per l’azienda o il Documento nel quale sono racchiusi.

Unità locale / Cantiere

È possibile duplicare il singolo documento per ogni Cantiere o Unità Locale di interesse. In questo caso è opportuno aggiungere una lettera al codice per identificare in modo univoco i vari documenti.

Nel campo Cantiere dovrà essere indicata l’Unità Locale o il Cantiere di riferimento.

Luogo

È opportuno indicare, per ogni Documento, il luogo di conservazione.

Date

Per ogni Documento è necessario indicare la data dell’ultimo aggiornamento.

Per i documenti che hanno una scadenza è opportuno indicare la data entro la quale iniziare le attività di revisione (anticipando l’effettiva data di scadenza del tempo necessario per l’aggiornamento).

Allegato

È opportuno archiviare digitalmente tutti i documenti per averne la disponibilità immediata in qualunque luogo dotato di connessione internet.

1.4.3 SUPPORTO

1.4.3.1 Lavoratori

Il programma permette di memorizzare una serie di informazioni relative ai Lavoratori (Dipendenti o Collaboratori) e quindi di produrre alcuni dei modelli previsti nel Sistema di Gestione Aziendale (Visite mediche, Formazione, Gestione DPI, ecc.).

I Lavoratori, in genere, non coincidono con i Responsabili 231. Nel caso in cui coincidono è qui possibile inserire altre informazioni tipiche del Lavoratore.

Fra le altre informazioni viene richiesto il “Fiduciario” che è, dove definito, la persona che preferibilmente accederà con le credenziali del Lavoratore negli archivi dello stesso in caso di assenza prolungata.

Per i Lavoratori è possibile ottenere una stampa dei Registri con tutte le informative relative al Lavoratore ed alle informazioni ad essi associate: Formazione, Visite Mediche e DPI (vedi paragrafi successivi).

È possibile inserire anche l'anagrafica di altre persone, comunque coinvolte nella gestione del sistema, che non siano lavoratori dell'azienda.

NOTA: Il Regolamento europeo sul trattamento dei dati personali (GDPR) prevede per l'interessato il diritto all'accesso ai propri dati (Art. 15). SQuadra consente di fornire ai vari lavoratori le indicazioni per visualizzare direttamente i dati personali trattati da SQuadra. Il Lavoratore avrà il diritto a chiederne la rettifica (Art. 16), la cancellazione (Art. 17) e alla limitazione (Art. 18) nei casi previsti.

Il Diritto alla portabilità (Art. 20) si realizza tramite la consegna del "Registro" del singolo Lavoratore che riporta tutti i dati in formato excel.

1.4.3.2 Lavoratori - Ruoli

I Ruoli permettono di descrivere le caratteristiche di ogni Lavoratore ed assegnare alcune attività:

- Specifica formazione.
- Specifiche visite mediche.
- Specifici DPI.

Ruoli di base

Per prima cosa è necessario definire i Ruoli di base. Per ogni ruolo è possibile definire le competenze previste.

È possibile richiedere l'importazione di alcuni elementi standard ma ogni azienda può aggiungerne di nuovi.

Attività per ogni Ruolo

È quindi necessario definire, per ogni Ruolo, le attività ad esso collegate. Anche in questo caso è possibile importare quelli di base proposti dal programma.

È possibile definire:

- Attività previste per il Ruolo (con l'indicazione dell'incidenza percentuale).
- I rischi connessi al ruolo.
- La formazione prevista.
- La sorveglianza sanitaria prevista.
- I DPI da consegnare.

Selezione dai Gruppi Omogenei (CPT – Torino)

Il CPT di Torino ha predisposto un elenco dei Gruppi Omogenei per le Costruzioni.

È possibile selezionare quelli di interesse per avere una definizione in automatico dei Ruoli aziendali.

Stampa dei Ruoli Aziendali

SQuadra fornisce una stampa nella quale sono riportati tutti i Ruoli aziendali con l'indicazione della Persone associate e delle caratteristiche (Attività previste, Rischi, ecc.).

Ruoli dei Lavoratori

Per ogni Lavoratore è possibile definire quali Ruoli ricopre. Ovviamente un Lavoratore può ricoprire più Ruoli e lo stesso Ruolo può essere ricoperto da più Lavoratori.

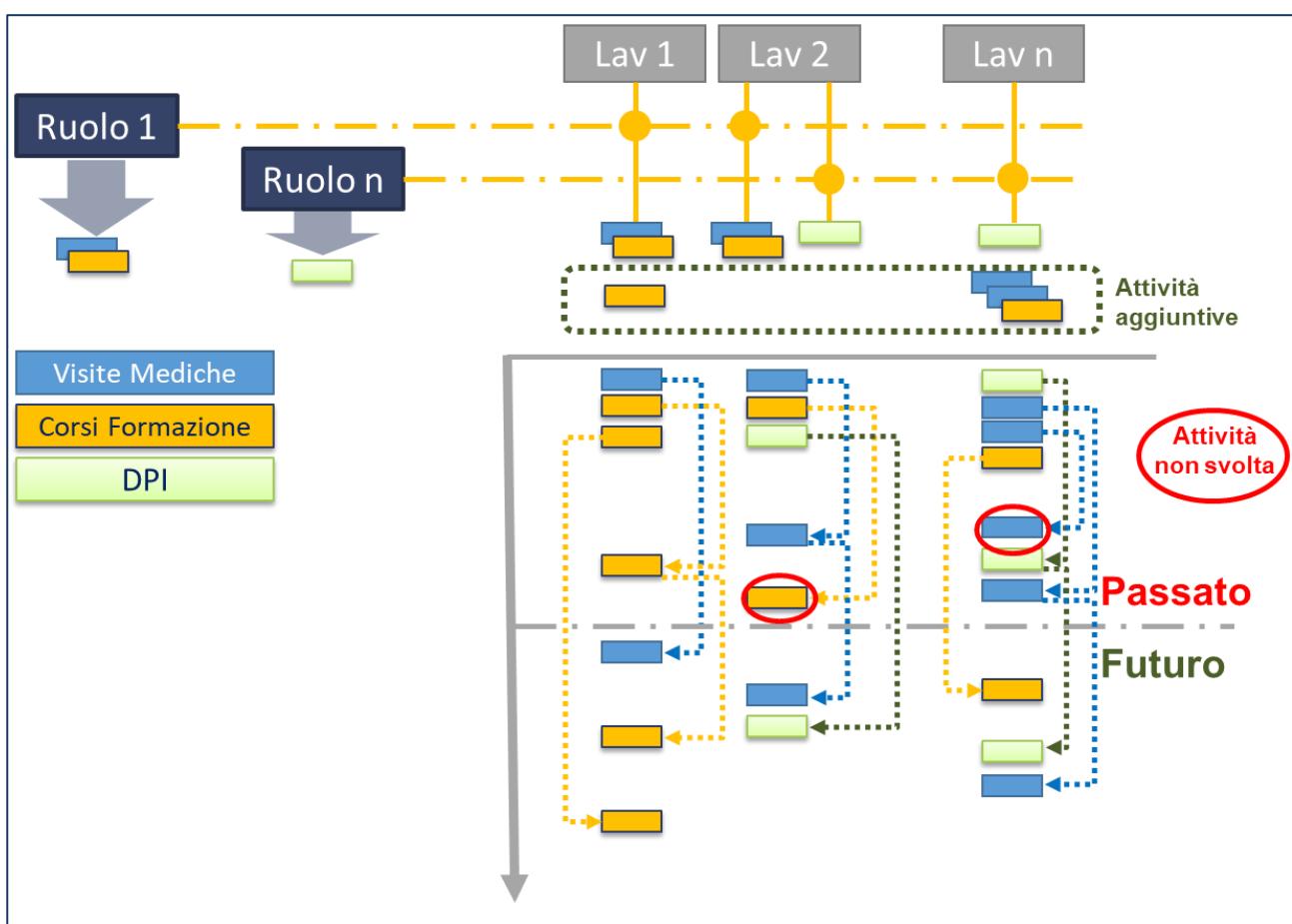
È possibile definire anche la data in cui un Lavoratore cessa di ricoprire un determinato Ruolo.

Per ogni ruolo possono essere definite le competenze necessarie. Le competenze vengono "ereditate" dalle competenze definite per i vari ruoli ma è possibile definire specifiche competenze per i vari utenti.

Creazione delle Attività

Ad ogni variazione (di attività previste per un Ruolo o di Ruoli assegnati ai Lavoratori) è possibile richiedere la creazione delle nuove attività.

Le attività verranno pianificate alla data odierna e poi verranno gestite normalmente come illustrato nei capitoli seguenti.



1.4.3.3 Lavoratori - Visite mediche

Fra le informazioni relative alla Visita medica è possibile registrare alcune date ed in particolare:

- Data in cui il Medico Competente consegna l'Idoneità all'azienda (quando non contestuale).
- Data in cui l'Azienda comunica al dipendente l'esito delle idoneità (se non comunicate direttamente dal Medico Competente).

ATTENZIONE: È proibito inserire in queste maschere dati personali “sensibili” quali, ad esempio, particolari prescrizioni per il lavoratore. Questi dati devono essere inseriti utilizzando le apposite funzionalità (vedi avanti nel presente Manuale) specificatamente sviluppate per la protezione dei dati personali (come richiesto dal Regolamento Europeo 679/2016).

1.4.3.4 Lavoratori - Addestramento

È possibile registrare, per ogni Lavoratore, l’addestramento effettuato.

È necessario indicare per quale attività viene svolto l’addestramento, il nominativo dell’Addestratore e la data di conclusione dell’addestramento a seguito di verifica che assicura che il lavoratore sia competente a svolgere l’attività.

L’addestramento può riferirsi a:

- DPI.
- Attrezzature.
- Strumenti.
- Impianti.
- Sostanze.
- Macchine.
- Operazioni.
- Altro.

Per ogni elemento è necessario indicare la Tipologia e il Tempo dedicato.

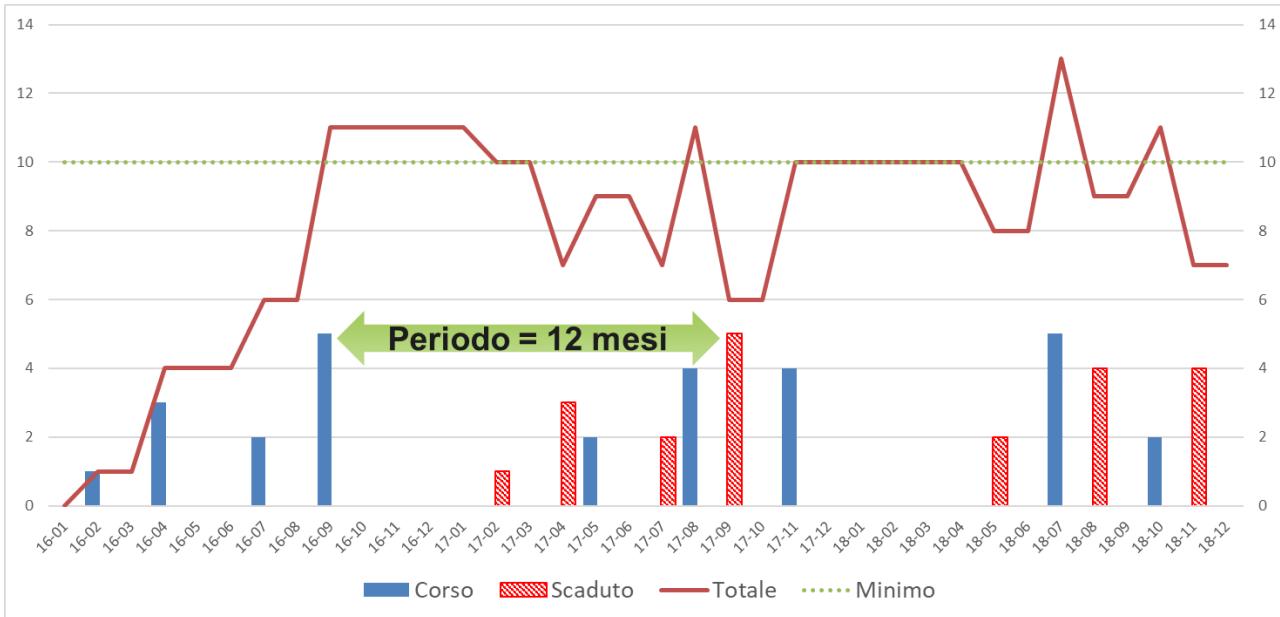
1.4.3.5 Lavoratori - Formazione

Per ogni Lavoratore è possibile definire la formazione effettuata o prevista.

Per ogni attività formativa è possibile definire:

- L’Argomento e gli Obiettivi.
- Il Formatore ed il Luogo della formazione.
- Metodo utilizzato e Tipo di formazione.
- L’eventuale necessità di Verifica e, nel caso, entro quanti mesi è prevista.
- Il numero di mesi trascorsi i quali è necessario ripianificare la formazione (dove necessario).
- I giorni di anticipo necessari per organizzare la formazione (tenendo conto della frequenza con la quale vengono organizzati i corsi, del rischio di indisponibilità, ecc.).
- Ore di formazione minima prevista nel periodo indicato al punto precedente (se previste – vedi grafico e nota successiva).
- Tipi particolari di formazione che permettono a SQuadra altri controlli:
 - Formazione sul D.Lgs 231/01.
 - Formazione sulle responsabilità specifiche assegnate dal Modello al singolo lavoratore come descritte dalla Nomina accettata.
 - Formazione specifica sul sistema di prevenzione della corruzione.
 - La Formazione può essere registrata per il singolo lavoratore o registrata come Corsi, in genere rivolti a più lavoratori.
- Per le formazioni di base che prevedono aggiornamenti è necessario indicare il nome degli aggiornamenti, le ore previste ed il Periodo espresso in mesi (es. La “Formazione XXX”, una volta effettuata, prevede che, nel periodo di X mesi, siano effettuate almeno XX ore di “Aggiornamento XXX”).
- Esito della Formazione.

- Metodo utilizzato e Data della Verifica (quando necessaria).



Nella figura viene riportato il caso di un tipo di formazione che richiede 10 ore all'anno.

Se la formazione effettuata negli ultimi 12 mesi non raggiunge le 10 ore è necessario effettuare immediatamente un corso per le ore mancanti. Nel caso la formazione nell'ultimo anno superi le ore previste (nell'esempio 10) è necessario pianificare la formazione per la data in cui scadrà la validità del corso più vecchio ancora significativo.

NOTA: Viene utilizzata unicamente nel caso in cui la formazione viene svolta con attestati multipli. Nel caso in cui la formazione preveda un unico attestato dovrà essere registrata solo l'attività di formazione nella quale viene rilasciato l'attestato finale.

Pianificazione

È possibile inserire nuove attività formative indicando la data prevista per ottenere una prima pianificazione delle attività da svolgere.

Una volta svolto un tipo di formazione la successiva pianificazione si otterrà semplicemente tenendo conto del numero dei mesi trascorsi i quali deve essere effettuata nuovamente.

Corsi

In caso di Corsi ai quali partecipano più lavoratori è possibile effettuare un inserimento specifico.

Le informazioni relative alla Formazione effettuata attraverso corsi possono essere modificate solo dall'apposita funzione mentre la formazione per il singolo lavoratore può essere registrata anche direttamente dalla manutenzione del Lavoratore.

Quando viene definito un nuovo Corso è possibile richiedere con il bottone “Importa Partecipanti” di aggiungere al Corso, in automatico, tutti i Partecipanti per i quali è pianificata una formazione sullo stesso argomento.

Per i Corsi è possibile ottenere il Registro ed allegare dei Documenti (ad esempio il Registro stesso con le relative firme).

Analisi

Nei Registri vengono riportate tutte le attività di Formazione con l'indicazione dell'ultima Formazione valida.

1.4.3.6 Lavoratori - Dispositivi di Protezione Individuale

Per ogni Lavoratore è possibile definire i DPI forniti. Anche in questo caso è possibile definire una pianificazione.

1.4.3.7 Lavoratori – Committenti che hanno ricevuto i dati personali del lavoratore

Alcuni Committenti/Appaltatori possono ricevere i dati personali del lavoratore, nell'ambito di contatti di Appalto/Subappalto (ad esempio per assolvere agli oneri derivanti dalla gestione della sicurezza nei cantieri D.Lgs. 81/2008 e/o dalla responsabilità solidale ex art. 29 del D.Lgs. n. 276/2003).

I dati personali sono forniti in esecuzione di un obbligo contrattuale e il Committente/Appaltatore diviene Titolare per i trattamenti che effettuerà sui dati forniti (visto che determinerà in autonomia le finalità e i mezzi del trattamento) dovrà quindi fornire a tutti gli interessati, ai sensi del GDPR apposita informativa (qualora non desideri utilizzare la "Informativa per i Lavoratori di altre imprese impegnate nei Cantieri Edili").

È possibile memorizzare tutti i committenti ai quali sono stati consegnati i dati personali.

Per ogni committente è possibile indicare (eventualmente selezionandoli fra tutti i lavoratori) l'elenco dei lavoratori indicando la data di consegna.

Uso di SQuadra nella “filiera” delle costruzioni.

L'utilizzatore di SQuadra al livello più alto deve inserire i dati del Committente.

SQuadra fornisce un codice che può essere comunicato ai vari fornitori di servizi.

Ogni fornitore di servizi dovrà registrare il Committente ma, inserendo il codice fornito, troverà in automatico i dati del Committente e i dati del Titolare per il trattamento dei dati al quale fornisce i dati dei suoi dipendenti. Anche in questo caso SQuadra fornisce un codice.

Ad ogni “livello” il sub fornitore di servizi, inserendo il codice comunicato dal suo cliente al quale ha fornito dati personali dei suoi dipendenti, avrà la visibilità di tutta la catena dei Titolari che trattano detti dati.

Le stesse informazioni sono visibili al Lavoratore che chiede l'accesso ai propri dati (vedi Nota nel precedente capitolo Lavoratori).

1.4.3.8 Idoneità e Prescrizioni

Le eventuali prescrizioni fornite dal Medico Competente sono categorie particolari di dati personali (una volta definiti come "sensibili"). Il trattamento di questi dati è necessario per il referente del lavoratore per l'attività lavorativa ma non sono necessari, e quindi ne è proibita la conoscenza, da parte del resto dell'organizzazione.

SQuadra permette di definire in quali Reparti (Ufficio, Sede distaccata, Cantiere, ecc.) opera ogni Lavoratore. Permette quindi di individuare, per gli utenti di SQuadra, per quali Reparti è necessario che siano informati relativamente alle prescrizioni.

In base alle informazioni di cui sopra solo chi ha necessità di conoscere l'informazione "sensibile" ne potrà venire, legittimamente, a conoscenza.

SQuadra fornisce anche delle stampe di questi dati "sensibili" solo ad utenti "autorizzati" a conoscerli. Una volta che SQuadra ha prodotto il file o la stampa fisica questi supporti devono essere trattati con le dovute accortezza dagli utenti per evitare che vengano conosciuti da persone che non ne hanno necessità.

Responsabile Prescrizioni

L'amministratore di sistema (vedi apposito capitolo più avanti in questo Manuale) dovrà definire chi è abilitato all'inserimento delle prescrizioni facendo attenzione a limitare l'accesso a questa funzionalità ai soli Utenti che devono, e quindi possono, gestire le prescrizioni.

Il Responsabile della gestione delle Prescrizioni dovrà inoltre gestire anche i Reparti, l'associazione dei Lavoratori ai Reparti e l'associazione dei Responsabili degli stessi Reparti che devono (e quindi possono) essere informati sulle prescrizioni per i singoli lavoratori.

Reparti

È possibile definire i Reparti di interesse (Uffici, Sedi distaccate, Cantiere, ecc.) nei quali operano i lavoratori. Nel definire i Reparti è possibile indicare il Sito (vedi SG / Varie / Tabelle Varie).

Per ogni Reparto vengono indicati i Lavoratori che vi operano (un Lavoratore può operare su più Reparti).

Sempre per ogni Reparto deve essere indicato il o i Responsabili che possono/devono essere informati sulle prescrizioni di tutti i lavoratori che operano per ogni Reparto (una persona può essere Responsabile per più Reparti). È opportuno controllare l'indirizzo di mail inserito per i Responsabili per consentire il corretto invio delle nuove prescrizioni.

Prescrizioni

Ad ogni nuova comunicazione da parte del Medico Competente il Responsabile Prescrizioni dovrà inserire le prescrizioni complessive relativa al Lavoratore in oggetto (la nuova prescrizione sostituisce tutte le precedenti). Il sistema rileverà la data di inserimento.

MAIL Prescrizioni

In ogni momento vengono presentate le MAIL inviate ai vari Responsabili (in verde e con la data di invio) e quelle ancora da inviare.

Il Responsabile Prescrizioni può richiedere l'invio automatico di tutte le mail da inviare o selezionare solo quelle che desidera inviare.

1.4.3.9 Macchinari

Anagrafica Macchinario

Il programma permette di memorizzare una serie di informazioni relative ai Macchinari e alle Attrezzature utilizzati.

È possibile inserire l'uso medio giornaliero (vengono richiesti 2 valori per poter operare sia con Macchinari per i quali è significativo l'uso chilometrico sia per quelli per i quali è significativo il numero di ore di utilizzo). In base alle rilevazioni (vedi avanti) il programma propone i valori di

utilizzo medi (ovviamente a partire dalla seconda rilevazione significativa). I valori medi vengono calcolati come media fra la più vecchia rilevazione significativa e la più nuova. Sarà comunque cura dell'utente valutare se modificare la stima sui consumi in base ai dati medi.

Qualora si sia sostituito il contatore è necessario inserire i valori in Km o Ore da aggiungere a quelli rilevati per avere l'utilizzo totale.

Per ogni Macchinario è possibile definire un Responsabile, se rientra nell'Allegato VII del D.Lgs. 81/08 e lo stato di Conformità (Dichiarazione di Conformità e rispondenza ai requisiti minimi previsti dall'Allegato V).

Manutenzioni ed altre Attività

Per ogni Macchinario è possibile inserire le Manutenzioni (sia Ordinarie che Straordinarie) o altre scadenze (Bollo, Assicurazione, Revisione, ecc.) o semplici rilevazioni periodiche (è opportuno effettuare rilevazioni periodiche per verificare l'utilizzo effettivo dei vari macchinari).

Per ogni attività è necessario indicare il tipo di manutenzione ed il rilievo (Data e, dove significativi, Km e/o Ore). Se è stato sostituito un contatore e nella macchina sono stati inseriti i valori da aggiungere questi verranno copiati sulla singola attività.

In caso di sola Pianificazione è necessario indicare la data in cui si effettua la pianificazione e la data prevista per l'attività (nel campo: "Prossima attività").

Dove ritenuto necessario è possibile inserire il nominativo del Responsabile ed eventualmente dell'Esecutore.

Pianificazione

Per alcune attività è possibile definire una pianificazione temporale delle scadenze (Bolli, Assicurazione, Revisione, ecc.). In questi casi ogni volta che viene effettuata una attività dovrà essere inserita la nuova data di pianificazione.

Per le Manutenzioni, in generale, non è possibile indicare una pianificazione temporale ma bisogna indicare l'uso Km/Ore. In funzione delle rilevazioni periodiche e delle stime dell'uso il programma è in grado di fornire, in ogni momento, la migliore pianificazione delle attività in funzione del reale utilizzo delle stesse.

Se non viene indicata la data di Pianificazione è possibile indicare il numero di Mesi entro i quali effettuare la nuova attività.

NOTA: Per ogni nuovo Macchinario da gestire con SQuadra è necessario inserire i dati anagrafici e quindi definire le varie attività previste (Bolli, Assicurazioni, Manutenzioni periodiche, ecc.). Per ogni attività è necessario inserire, usando il tipo "solo pianificazione", una descrizione, la data di pianificazione e i criteri per la riprogrammazione (direttamente la data o i valori d'uso Km o Ore).

Registri

Squadra produce un documento di Excel sia per un singolo Macchinario che per tutti con i seguenti fogli:

- Macchine: dove vengono presentati tutti i macchinari con i dati anagrafici, la stima dell'uso (Km e Ore), la media dell'uso rilevata dalle rilevazioni e i relativi scarti.
- Manutenzioni: dove vengono presentate tutte le attività con i relativi rilievi sull'uso.
- Pianificazione: dove, per ogni macchinario/tipo di attività, viene presentata la data dell'ultima rilevazione con i relativi ultimi valori relativi all'uso (Km, ore), la data prevista per

il prossimo intervento (dove significativa), i Km/Ore ai quali dovrà essere effettuato il nuovo intervento e la data prevista in base all'ultimo valore rilevato di uso e alla stima giornaliera definita (dove significativo). Viene quindi indicata la minima fra le date stimate e lo stato in relazione alla data odierna.

Pianificazione attività

È possibile configurare SQuadra in modo che pianifichi le nuove attività.

La pianificazione delle attività non è un'attività statica perché la pianificazione di varie attività può essere modificata da ogni nuova rilevazione dei consumi effettivi o da una nuova valutazione dei consumi medi.

SQuadra provvede quindi, ad ogni accesso alla gestione dei macchinari, ad eliminare e ricalcolare tutte le "Pianificazioni automatiche".

1.4.3.10 Piano delle Comunicazioni

L'organizzazione deve determinare le comunicazioni interne ed esterne pertinenti al sistema di gestione per la qualità, includendo: cosa vuole comunicare; quando comunicare; con chi comunicare; come comunicare; chi comunica.

Il programma permette di memorizzare e stampare le informazioni essenziali per ogni tipo di comunicazione.

È possibile richiedere la generazione delle corrispondenti Prescrizioni (vedi il precedente capitolo all'interno della PIANIFICAZIONE) per poter effettuare tutti i controlli sull'effettivo svolgimento delle Attività correlate. In questo caso verranno utilizzati i campi:

- Cosa.
- Argomento.
- Frequenza (qualora non vengano presentati gli elementi entrare in SG/Pianificazione/Prescrizioni).
- Rilevanza.
- Giorni necessari per la preparazione.

1.4.4 OPERATIVO

1.4.4.1 Valutazione dei Fornitori

Si rimanda all'apposita Appendice che può essere utilizzata direttamente come Istruzione del Sistema di Gestione Aziendale.

1.4.4.2 Dichiarazioni dei Fornitori

In molti casi è opportune che l'azienda richieda al Fornitore, prima di instaurare un rapporto commerciale, alcune dichiarazioni relative al rispetto di principi etici, della sicurezza sul lavoro, sul rispetto per l'ambiente, ecc.

In questi casi è possibile inviare la richiesta via mail e raccogliere in automatico le risposte da parte dei Fornitori.

È possibile predisporre più tipologie di dichiarazioni (ad esempio differenziando fra:

- Fornitori di prodotti.
- Fornitori di servizi.
- Consulenti.

- Ecc.

Per le Modalità operative si rimanda all'Appendice relativa alle Comunicazioni.

Fra i documenti di supporto (sotto VARIE) è possibile trovare un esempio di comunicazione da utilizzare per predisporre il file PDF da inserire nella richiesta di dichiarazioni.

1.4.4.3 Controlli

È possibile definire i controlli che si desidera effettuare e registrare i controlli effettuati.

Tipi di Controlli

Devono essere definiti i tipi di controllo. Ogni tipo di Controllo è caratterizzato da:

- Un Codice ed una Descrizione.
- Il Metodo e/o gli strumenti utilizzati.
- I Criteri di valutazione e di accettabilità (Corrispondenza integrale, Tolleranza, ecc.).
- I Documenti e/o le Norme di riferimento.
- La modalità di registrazione prevista (Allegato alla registrazione, sigla su documenti esterni, ecc.).
- Eventuali Note.
- È possibile associare una Scheda da utilizzare per il controllo.

Controlli

Vengono quindi definiti i Controlli veri e propri. Per ogni controllo vengono indicati a livello di pianificazione:

- La Commessa o Divisione di riferimento.
- La Fase o Settore ed eventualmente una ulteriore suddivisione.
- Il tipo di controllo che si desidera applicare fra quelli precedentemente definiti.
- La Frequenza prevista (ad ogni operazione, ogni mese, ecc.).
- La data prevista.

Al momento dell'esecuzione è necessario indicare:

- Data effettiva del controllo.
- Esecutore.
- Mesi per il prossimo controllo (verrà indicato 0 per controlli occasionali).
- Dettagli relativi al controllo effettuato.
- Note sul Controllo.
- Esito (da "Totalmente Conforme" a "Con gravi non conformità").

Se al Tipo di Controllo è stata associata una Scheda per la rilevazione questa può essere richiesta e visualizzata.

Ad ogni Controllo è possibile associare più Documenti (Scheda di Controllo compilata, Foto, ecc.).

Tramite l'apposito bottone è possibile generare il prossimo Controllo (in funzione della data effettive e dei mesi previsti).

Esportazione

È possibile ottenere un file di Excel nel quale vengono presentati tutti i Tipi di Controllo e il Registro dei Controlli nel quale ogni controllo è caratterizzato da una Stato:

- Eseguito (se definita la data di esecuzione).
- Da Pianificare (se manca la data prevista).
- Futuro (se la data di pianificazione è futura).
- Scaduto (se la data di pianificazione è già passata).

Viene presentato un'analisi riepilogativa nella quale sono indicati, per ogni Categorie e SottoCategoria, il numero complessivo ed il numero degli esclusi. Vengono quindi indicati i fornitori che hanno avuto per la prima volta una valutazione nell'ultimo anno (Nuovi) ed il numero di fornitori valutati nell'Anno.

1.4.4.4 Idoneità Tecnico Professionale

Si rimanda all'apposita Appendice che può essere utilizzata direttamente come Istruzione del Sistema di Gestione Aziendale.

1.4.4.5 Schede di sicurezza per sostanza pericolose

Per le procedure tecniche di uso e stoccaggio delle sostanze e dei preparati pericolosi viene fatto ricorso alle schede di sicurezza fornite dai fabbricanti, che possono essere memorizzate e quindi rese disponibili sia in sede che nel sito di utilizzo.

Ogni Scheda è caratterizzata dal Produttore, Tipologia e Materiale.

Per ogni Scheda è necessario indicare la data di emissione (per permettere facilmente di evidenziare eventuali aggiornamenti), la data dell'ultima verifica effettuata circa l'aggiornamento della stessa e il numero dei mesi entro i quali si ritiene opportuno effettuare un nuovo controllo.

La Scheda del fornitore aggiornata deve essere allegata in formato PDF.

1.4.5 VALUTAZIONE

1.4.5.1 Audit di Sistema

È possibile memorizzare su SQuadra gli audit effettuati o previsti ed ottenere la stampa degli stessi.

Ad ogni Audit è possibile collegare vari Allegati.

1.4.5.2 Indicatori per le prestazioni

Ogni azienda può definire i propri indicatori (“cosa è necessario monitorare e misurare”).

Se si desidera è possibile importare gli indicatori proposti dalla Prassi di riferimento UN/PdR 83:2020 (*Modello semplificato di Organizzazione e Gestione della salute e sicurezza sul lavoro, di cui al D.lgs. 81/2008, per micro e piccole imprese*).

Per ogni indicatore è necessario definire, in corrispondenza a determinate date, i seguenti elementi:

- Unità di Misura della valutazione numerica dell'indicatore.
- Il Responsabile (“chi è responsabile del monitoraggio”).
- Il Destinatario (“a chi e come tali informazioni devono essere riferite”).
- Il Monitoraggio (“i metodi di monitoraggio, misurazione, analisi e valutazione, come applicabile, per assicurare risultati validi”) ed i Criteri di valutazione.

- I Mesi fra cui è prevista la prossima rilevazione (“*quando il monitoraggio e la misurazione devono essere eseguiti*”).
- La Frequenza (“*quando i risultati del monitoraggio e della misurazione devono essere analizzati e valutati*”).
- Il valore dell’obiettivo
- Il criterio di raffronto con i dati attesi:
 - Minore di
 - Uguale a
 - Maggiore di
- Il Valore rilevato.

Il programma riporta, per ogni Indicatore, l’ultimo valore rilevato con il relativo scarto.

Riporta inoltre tutte le rilevazioni.

1.4.5.3 Soddisfazione delle parti interessate (Stakeholder)

Valutazioni

Ogni azienda può definire gli elementi attraverso i quali valutare la soddisfazione dei propri Stakeholder (Clienti, Lavoratori, Fornitori, ecc.).

Tipologie

È necessario definire le varie tipologie di portatori di interessi (Clienti Pubblici, Clienti Privati, Impiegati, Operai, ecc.). Per ogni tipologia è necessario definire l’incidenza percentuale della valutazione al fine di ottenere una valutazione complessiva.

Viene quindi richiesto il criterio per valutare l’incidenza della valutazione (Il fatturato negli ultimi 5 anni, il numero di gare previste, ecc.).

Elementi di valutazione

Per ogni Tipologia è necessario definire gli elementi sui quali si ritiene opportuno ottenere la valutazione sul grado di soddisfazione (Qualità, Tempi, ecc.). Per ogni elemento di valutazione è opportuno indicare una Importanza relativa rispetto agli altri mediante l’attribuzione di un numero da zero a 10.

Valutazioni

Per ogni tipologia devono essere inserite le valutazioni relative di vari Enti nei vari Periodi.

Per ogni Valutazione deve essere inserita l’incidenza (in relazione a quanto indicato nelle varie Tipologie).

Giudizi

Per ogni nuova Valutazione verranno copiati, in automatico gli ultimi elementi di valutazione previsti per la Tipologia con la relativa Importanza. È necessario inserire un valore numerico rappresentante il giudizio e, dove presente, una sintesi dell’eventuale giudizio descrittivo.

Analisi della Soddisfazione

Vengono riportati tutti i Giudizi con le seguenti informazioni:

- Periodo
- Tipologia e relativa Percentuale.
- Ente con Incidenza definita e Incidenza percentuale (100% per Periodo/Tipologia).

- Elemento di valutazione con Importanza e Importanza percentuale (100% per Tipologia).
- Giudizio.
- Giudizio Totale [Giudizio x Incidenza percentuale x Importanza percentuale] (Somma = Media Giudizi pesati).

Vengono poi riportati su altre cartelle una sintesi dei risultati:

- Totali per Periodo [Somma del Giudizio Totale].
- Per ogni Elemento per i Periodi nei quali sono stati rilevati.
- Per ogni Tipologia per i Periodi nei quali sono state rilevate.

Aggiornamento dall'Analisi del Contesto

È possibile richiedere l'aggiornamento delle Tipologie e degli Elementi di Valutazione dalle informazioni inserite nell'ultimo Riesame.

1.4.6 MIGLIORAMENTO

1.4.6.1 Non Conformità

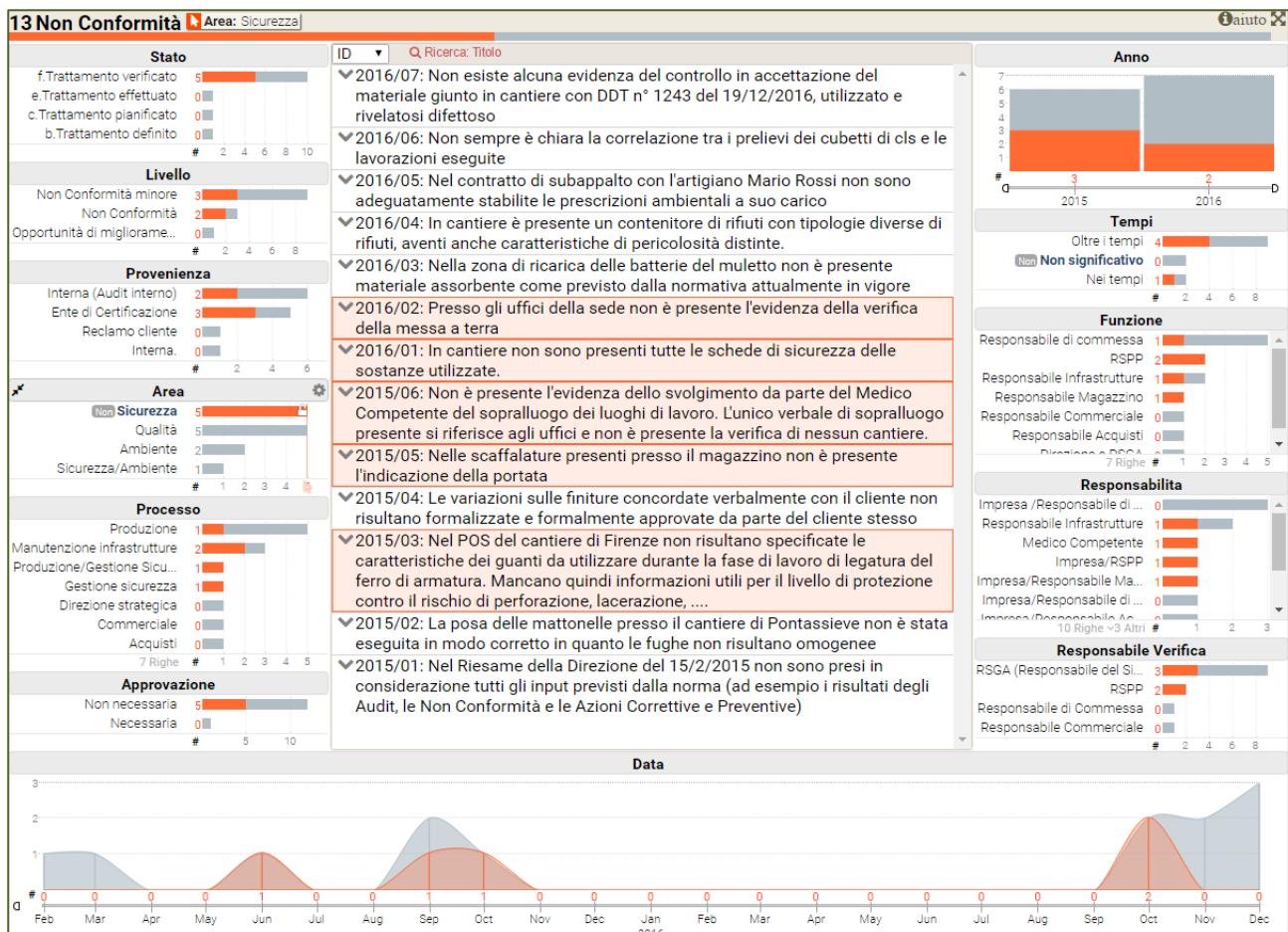
NOTA: I Rilievi specifici per la 231 sono gestiti fra le attività dell'OdV.

Per ogni Non Conformità possono essere memorizzate le informazioni relative alla RILEVAZIONE, al TRATTAMENTO ed alla VERIFICA.

In base alle informazioni inserite SQuadra determina lo stato della Non Conformità:

- **Registrata.**
- **Trattamento definito.**
- **Trattamento pianificato** (da quando è definita la data prevista per la conclusione del trattamento).
- **Trattamento approvato** (solo se per la Non Conformità è prevista l'approvazione da parte del Cliente).
- **Trattamento effettuato** (da quando viene inserita la data effettiva di conclusione del trattamento).
- **Trattamento verificato** (da quando viene inserita la data di verifica positiva del Trattamento).

Ad ogni Non Conformità possono essere associate una o più Azioni Correttive (vedi avanti).



Per il funzionamento dei Cruscotti si rimanda alle indicazioni presenti nel capitolo relativo all'interno della Sezione "Caratteristiche generali di SQuadra".

In ogni momento è possibile, oltre ad ottenere un Registro delle NC e le schede delle singole NC, analizzare le Non Conformità rilevate.

1.4.6.2 Azioni Correttive e Preventive/Miglioramento

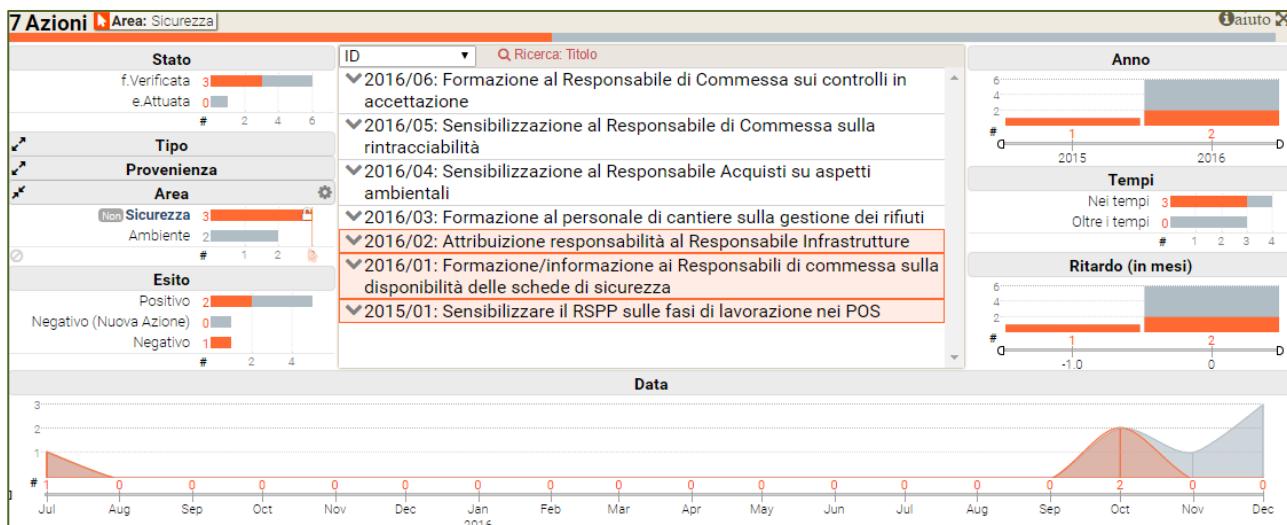
Per ogni Azione, sia Preventiva che Correttiva, possono essere memorizzate le informazioni relative alla DEFINIZIONE, all'APPROVAZIONE, all'ATTUAZIONE ed alla VERIFICA.

In base alle informazioni inserite SQuadra determina lo stato della Azione Correttiva o Preventiva:

- **Definita.**
- **Azione definita** (da quanto è stata definita l'Azione).
- **Azione pianificata** (da quanto viene inserita la data prevista per la conclusione dell'Azione).
- **Approvata** (da quando la Direzione approva l'Azione).
- **Attuata** (da quando il Responsabile definisce la data di conclusione).
- **Verificata** (da quando l'Azione viene verificata positivamente).

Ogni Azione Correttiva può essere associata a:

- Una Non Conformità
- Un Incidente (vedi avanti).



Per il funzionamento dei Cruscotti si rimanda alle indicazioni presenti nel capitolo relativo all'interno della Sezione "Caratteristiche generali di SQuadra".

Anche per le Azioni Correttive è possibile, in ogni momento, ottenere un Registro, le schede delle singole Azioni e una analisi di sintesi.

1.4.6.3 Incidenti

È possibile memorizzare tutti gli incidenti (a prescindere dal fatto che questi abbiano prodotto infortuni).

Per ogni Incidente è possibile rilevare:

- L'evento: Codice, Descrizione, Tipo, Segnalatore, Data, Evento, ecc.
- L'attuazione di misure atte a prevenirne il ripetersi (qualora non si decida di aprire una formale Non Conformità): Responsabile dell'attuazione e della verifica, Azioni previste, ecc.
- Infortunio (se verificatosi): Infortunato, Mansione, ecc.
- Analisi codificata delle cause: DPI, Formazione, Macchine, Valutazione dei Rischi, Fattori ambientali, ecc.

NOTA: è possibile registrare:

- *Infortuni: incidente che produce un danno all'integrità psico-fisica del lavoratore.*
- *Incidenti: evento inaspettato e indesiderato che può provocare un danno alle persone, alle cose, agli impianti, alle attrezzature e alle macchine.*

- *Situazioni pericolose: azione che può esporre i lavoratori a rischio di infortuni o a pericolo di incidenti.*

Per quanto concerne la rilevazione di infortuni, incidenti e comportamenti pericolosi devono essere responsabilizzati i singoli capi cantiere che si avvaranno anche delle segnalazioni dei capisquadra e dei singoli lavoratori.

Le informazioni dovranno essere inserite su SQuadra e saranno analizzate dal responsabile del SGSL che, eventualmente le completerà, specie con riferimento alle azioni preventive e correttive proposte.

Anche per gli incidenti è possibile effettuare una analisi attraverso lo specifico “cruscotto” che potrà anche essere utilizzata nel corso della riunione periodica.

Ad ogni Incidente posso essere associate una o più Azioni Correttive.

1.4.7 PREVENZIONE DELLA CORRUZIONE

1.4.7.1 Valutazioni

Elementi

È opportuno che ogni organizzazione determini “*gli elementi esterni e interni rilevanti per le sue finalità e che influenzano la propria capacità di raggiungere gli obiettivi del proprio sistema di gestione per la prevenzione della corruzione*”.

Al primo ingresso verranno proposti gli Elementi standard previsti dalla 37001:

- Dimensioni, struttura autorità decisionale delegata del dipartimento coinvolto.
- Modello commerciale del dipartimento coinvolto.
- Settore di riferimento per l'attività.
- Coinvolgimento di enti che controllano l'organizzazione.
- Coinvolgimento di enti su cui l'organizzazione esercita il controllo.
- Soci in affari coinvolti.
- Natura dell'attività.
- Entità e complessità dell'attività.
- Luogo in cui si svolge l'attività.
- Natura e entità delle interazioni con i pubblici ufficiali.
- Obblighi e adempimenti di legge, normativi, contrattuali e professionali applicabili.
- Personale coinvolto.

Per ogni Elemento è necessario definire l'importanza relativa standard per l'Ente.

Dettagli

Per alcuni elementi è possibile inserire dei Dettagli (ad esempio per la Natura dell'Attività vengono proposti gli elementi previsti dall'ANAC).

I Dettagli sono relativi alla Valutazione dell'Impatto ed a quella della Probabilità.

Per ogni dettaglio vengono indicate delle Note e dei Valori di Riferimento.

Azioni a rischio

È necessario definire ogni Azione specifica o i gruppi di azioni omogenee per “*effettuare valutazioni periodiche del rischio di corruzione*”.

Per ogni azione viene definita una data di inizio e la data di fine (assente per le Azioni ancora significative).

Ogni Azione può essere collegata ad un Ufficio e ad una Macro Azione.

In base ad un riepilogo calcolato delle valutazioni effettuate (vedi avanti) o, se presente, ad una esplicita valutazione di sintesi viene definito il Livello di Rischio e quindi la priorità di intervento.

Dettagli

Per ogni Azione può essere definito un Responsabile, una Descrizione di dettaglio, se è vincolata e come viene disciplinata (Procedure, Prassi, ecc.).

Possono, infine, essere descritti i Comportamenti a rischio.

Soci in affari

Per le Attività nelle quali sono coinvolti “*soci in affari che pongono un rischio di corruzione superiore al livello basso*” è opportuno indicare:

- Impegni specifici atti “*a prevenire atti di corruzione da parte del socio in affari, per suo conto o a suo vantaggio in relazione alla transazione, al progetto, all'attività o alla relazione pertinente*”.
- Clausole previste per garantire “*di cessare il rapporto con il socio in affari in caso di atti di corruzione commessi da parte del socio in affari, per suo conto o a suo vantaggio in relazione alla transazione, al progetto, all'attività o alla relazione pertinente*”.

Inadeguatezza

Se “*la due diligence condotta su una specifica transazione, progetto, attività o relazione con un socio in affari stabilisca che i rischi di corruzione non possono essere affrontati dai controlli per la prevenzione della corruzione esistenti*” è opportuno definire come gestire questa inadeguatezza.

Altrimenti è necessario:

- Interrompere (*In caso di una transazione, un progetto, un'attività o una relazione esistenti, adottare misure adeguate ai rischi di corruzione e alla natura della transazione, del progetto, dell'attività o della relazione per cessare, interrompere, sospendere o ritirarsi da ciò non appena possibile*).
- Bloccare (*in caso di una nuova proposta di transazione, progetto, attività o relazione, rimandarne o declinarne il prosieguo*).

Elementi di valutazione per l'Azione

Per ogni nuova Azione il sistema propone gli Elementi definiti come significativi a livello Aziendale. È possibile modificare l'importanza relativa per la specifica Azione delle Valutazioni. L'importanza non è assoluta nel senso che, nel “*valutare e mettere in ordine di priorità i rischi di corruzione identificati*”, tutte le Azioni verranno considerate comunque omogenee dal punto di vista dell'importanza complessiva¹². In pratica: abbassare l'importanza di un elemento rispetto al valore proposto a livello Aziendale significa alzare l'importanza “relativa” degli altri elementi.

Per ogni Elemento è necessario indicare l'Oggetto per poter recuperare l'ultima valutazione registrata.

In assenza di valutazione per lo specifico Elemento/Oggetto il sistema considera, cautelativamente, il rischio massimo.

Punti di Controllo

¹² Il Rischio complessivo = Somma(Voto x Importanza) / Somma(Importanza).

Dove la valutazione del rischio sia superiore al livello Basso è opportuno indicare quali dei Punti di Controllo definiti nel Modello dovrebbero tenere sotto controllo il rischio¹³.

Valutazioni

Per ogni Elemento è possibile effettuare varie valutazioni relativamente a vari Oggetti (ad esempio per un Socio in affari o per il Personale è necessario indicare il nominativo o la tipologia).

Via via che vengono effettuate le valutazioni queste devono essere registrate indicando:

- Data.
- Livello di valutazione.
- Valutazione descrittiva.
- Mesi entro i quali deve essere prevista una nuova valutazione.

Dettagli

Se per l'Elemento in esame erano stati previsti dei Dettagli questi vengono riproposti anche per la Valutazione.

Andranno quindi inserite delle valutazioni per ogni singolo Dettaglio.

Metodologia di calcolo

Dettagli

Il Programma provvede a calcolare per i Dettagli delle Valutazioni la media della Valutazione dell'Impatto e quella della Probabilità.

L'ANAC propone di ottenere la Valutazione complessiva del Rischio attraverso il semplice prodotto fra i due valori precedenti.

È comunque necessario definire come passare dal prodotto Probabilità per Impatto alla Gravità.

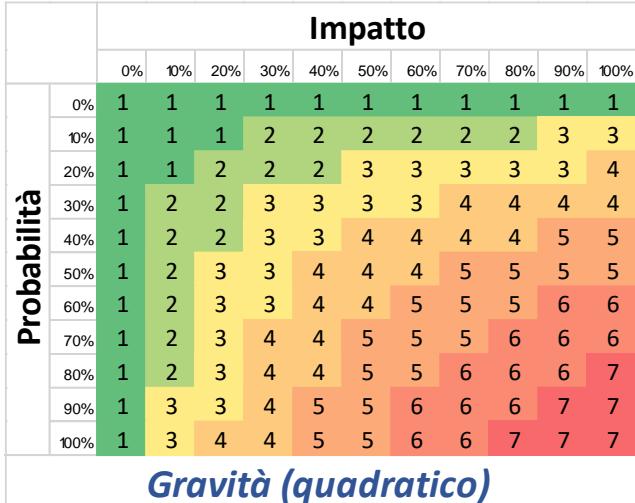
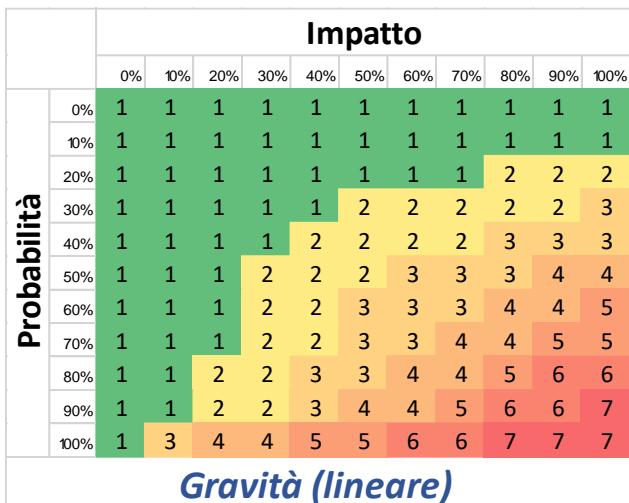
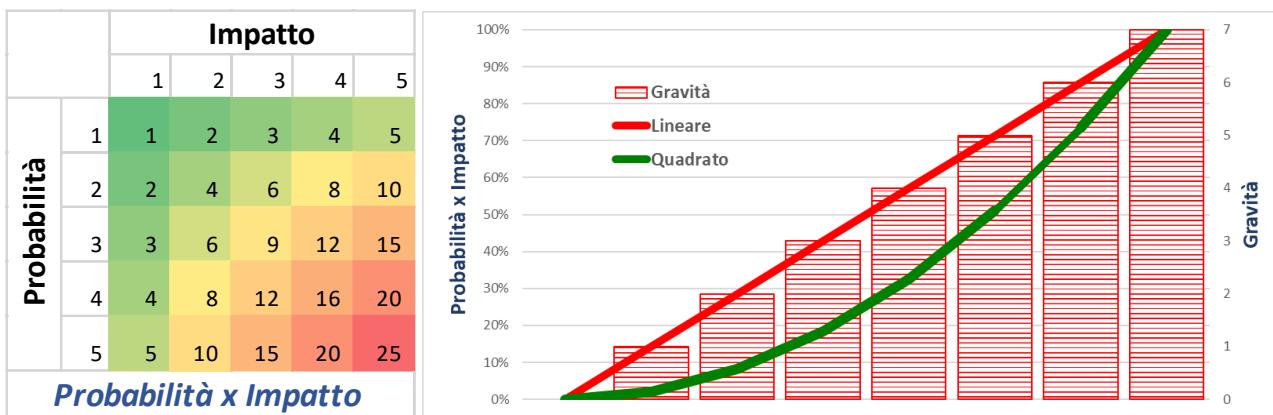
Ovviamente:

Prodotto minimo implicherà Gravità minima.

Prodotto massimo dovrà portare alla massima Gravità.

Per i valori intermedi un primo metodo da utilizzare è quello lineare ma è possibile utilizzare metodi più cautelativi che producano Gravità significative anche per valori del prodotto bassi. Il metodo utilizzato è quello quadratico.

¹³ Come indicato nella Circolare della Guardia di Finanza 19/03/12: “Non può essere richiesto che il modello **annulli completamente** il rischio di verifica dei reati ma che lo definisca e lo tenga sotto controllo mediante un’azione dispiegata con continuità. Il modello dovrà presentare quei requisiti di **efficienza, praticabilità e funzionalità**, in grado ragionevolmente di disinnescare le fonti di rischio”.



Per determinare i livelli di Gravità sono stati quindi utilizzati i seguenti valori del prodotto Probabilità x Impatto (formula cautelativa).

Il Livello di gravità calcolato deve essere confermato o modificato dalla valutazione per evitare una "applicazione meccanica" della metodologia.

Decadimento delle valutazioni nel tempo

In presenza di Valutazioni queste vengono considerate valide solo entro il limite dei mesi indicato. Superato questo periodo la valutazione "decade" (aumenta il rischio considerato) fino a coincidere con l'assenza di valutazione (rischio massimo) da quando sono trascorsi il doppio dei mesi previsti per effettuare una nuova valutazione¹⁴.

¹⁴ Posto TEMPO_MAX = Mesi previsti la successiva valutazione:

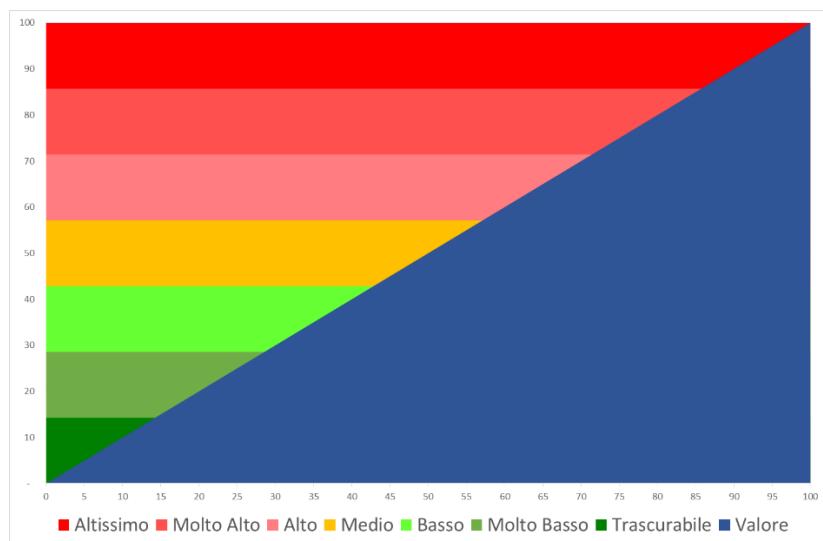
Per Tempo < TEMPO_MAX allora Valutazione_{Tempo} = Valutazione₀ altrimenti:

Valutazione_{Tempo} = Valutazione₀ + (1-TEMPO_MAX/Tempo) x (Massimo Rischio – Valutazione₀)

Valutazioni	Tempo trascorso / Tempo previsto per successiva valutazione														
	0,2	0,4	0,6	0,8	1,0	1,2	1,4	1,6	1,8	2,0	2,2	2,4	2,6	2,8	3,0
-	-	-	-	-	-	17	29	38	44	50	55	58	62	64	67
16,7	17	17	17	17	17	31	40	48	54	58	62	65	68	70	72
33,3	33	33	33	33	33	44	52	58	63	67	70	72	74	76	78
50,0	50	50	50	50	50	58	64	69	72	75	77	79	81	82	83
66,7	67	67	67	67	67	72	76	79	81	83	85	86	87	88	89
83,3	83	83	83	83	83	86	88	90	91	92	92	93	94	94	94
100,0	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100

Valutazione complessiva

La Valutazione complessiva calcolata per l’Azione è la media pesata delle Valutazioni sui vari Elementi (che tengono già conto del tempo trascorso) rispetto all’Importanza relativa assegnata all’Elemento per la specifica Azione¹⁵.



La valutazione complessiva viene riportata nella scala a 7 valori linearmente.

1.4.7.2 Personale

Persone

Per ogni persona coinvolta nel sistema è possibile inserire una serie di informazioni.

BASE

- Il Nominativo (deve precedentemente essere definito fra i Lavoratori vedi il successivo apposito capitolo del Manuale).
- Il tipo (Persone esposte a Rischio, membro dell’Alta Direzione, ecc.).
- Data d’inizio e fine collaborazione nella funzione.
- Nella normale formazione, vedi punto successivo, è possibile indicare se la formazione conteneva elementi specifici per la prevenzione alla corruzione. Il programma indica l’ultima formazione effettuata.

¹⁵ Valutazione Totale = Somma (Valutazione _{Tempo Elemento} X Importanza _{Elemento}) / Somma (Importanza _{Elemento})

Valutazioni

“In relazione a tutte le posizioni che sono esposte a un rischio di corruzione superiore al livello basso, e alla funzione di conformità per la prevenzione della corruzione, l’organizzazione deve” indicare i riferimenti relativamente a:

- La “due diligence sulle persone prima che siano assunte e sul personale prima che sia trasferito o promosso da parte dell’organizzazione, per determinare, per quanto ragionevole, che sia appropriato assumere o riposizionare tali persone e che sia ragionevole credere che osserveranno la politica di prevenzione della corruzione e i requisiti del sistema di gestione per la prevenzione della corruzione”.
- I “bonus sulla prestazione, gli obiettivi della prestazione e altri elementi incentivanti della remunerazione siano periodicamente sottoposti a riesame per verificare che siano messe in campo salvaguardie sufficienti per evitare che essi favoriscano la corruzione”.

Competenze

Per le “persone che lavorano sotto il controllo dell’organizzazione e che influiscono sulla sua prestazione di prevenzione della corruzione” è necessario:

- Determinare le competenze necessarie.
- Assicurare che queste persone siano competenti sulla base di istruzione, formazione o esperienza appropriate.
- Ove applicabile, intraprendere azioni per acquisire e mantenere le necessarie competenze e valutare l’efficacia delle azioni intraprese.

È possibile aggiungere alle persone (nel Modulo Lavoratori) degli allegati per “Conservare informazioni documentate appropriate a riprova della competenza”.

Dichiarazioni

È previsto che i membri del personale per i quali sono previste le valutazioni (vedi punto precedente) e “dell’alta direzione e dell’organo direttivo (se presente) depositino una dichiarazione a cadenze ragionevoli in proporzione al rischio di corruzione identificato, che confermino la loro osservanza della politica di prevenzione della corruzione.”

1.4.7.3 Trasparenza

Introduzione

Per gli Enti pubblici o per gli Enti di diritto privato in controllo pubblico o con partecipazione pubblica soggetti alla legge 190/2012 (“Disposizioni per la prevenzione e la repressione della corruzione e dell’illegalità nella pubblica amministrazione”) è possibile tenere sotto controllo la corretta pubblicazione delle informazioni previste nella Sezione Trasparenza.

Tipo di Ente

Per prima cosa è necessario definire in Manutenzioni / Personalizza / Dati Aziendali la tipologia dell’Ente al fine di ottenere tutti gli obblighi di pubblicazione relativi.

Pubblicazioni

Una volta definito il Tipo di ente, entrando in Pubblicazioni vengono presentati tutti gli elementi da pubblicare nella sezione Trasparenza del sito istituzionale con i relativi:

- Macrofamiglia.
- Riferimenti legislativi.
- Contenuti previsti.
- Estremi di validità.
- Eventuale non significatività per lo specifico ente.

- Gli estremi per l'aggiornamento.
- Le responsabilità.
- La periodicità prevista per il monitoraggio.

Monitoraggi

Periodicamente è necessario monitorare l'aggiornamento delle pubblicazioni.

Per ogni attività di monitoraggio è necessario definire la data ed il responsabile. Il programma indicherà il numero di elementi controllati ed il numero dei rilievi segnalati.

È possibile definire singolarmente le pubblicazioni controllate o chiedere la creazione dell'elenco delle pubblicazioni da controllare in funzione della periodicità dei controlli prevista.

Per ogni elemento è possibile evidenziare eventuali rilievi.

Duplicazione del Monitoraggio

Inserito il promo controllo è possibile duplicarlo per tutti i controlli da effettuare (quelli scaduti e quelli previsti entro 30 giorni). Sarà, ovviamente, necessario successivamente intervenire sui singoli monitoraggi per inserire eventuali particolarità o rilievi.

Prospetti

Vengono presentate tutte le informazioni da Pubblicare e tutti i Monitoraggi effettuati in 2 fogli di EXCEL.

Elenco

Vengono descritte tutte le informazioni ritenute significative di pubblicazione (in formato WORD) per allegarle o inserirle nel Piano Anticorruzione.

1.4.8 GESTIONE DEL SISTEMA

Per chi opera unicamente sul Sistema di Gestione è possibile richiedere da qui l'emissione delle Versioni e la stampa degli ultimi documenti approvati come già illustrato in precedenza per l'utilizzo totale del programma.

1.4.9 VARIE

1.4.9.1 Tabelle Varie

Siti

È possibile definire i Siti nei quali opera l'Azienda.

I Siti potranno essere utilizzati:

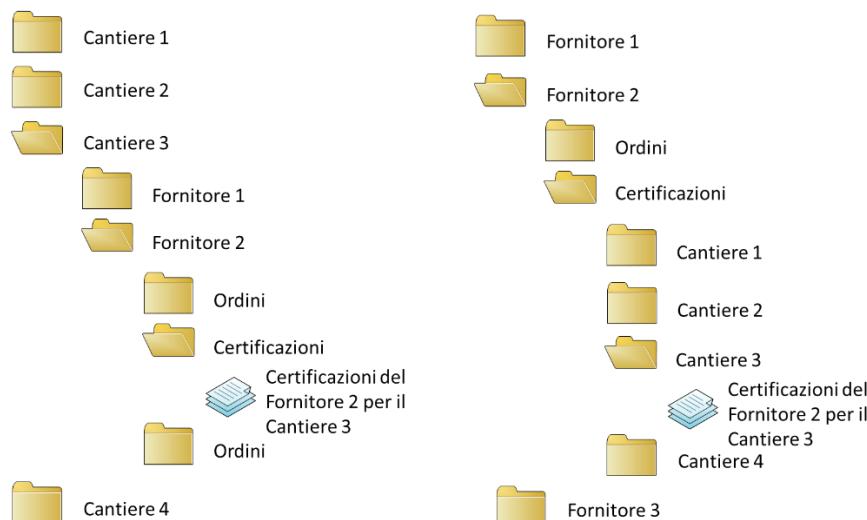
- Per specificare le Prescrizioni e le Attività per le Prescrizioni.
- Per specificare i Reparti utilizzati per la comunicazione delle Idoneità con Prescrizioni.

1.4.9.2 Documenti

Ogni azienda può catalogare ed archiviare documenti di varia natura.

Sono stati introdotti molti campi per catalogare i documenti permettendo ad ogni azienda di darsi una propria organizzazione per la documentazione.

I files vengono archiviati nel file system secondo una struttura “gerarchica” quindi è possibile ricercarli solamente secondo l'ordine gerarchico scelto (nell'esempio riportato nella figura successiva: Cantiere, Fornitori, Tipi Documenti o Fornitori, Tipi Documenti, Cantieri)



SQquadra permette l'archiviazione in una struttura “relazionale” in cui è possibile effettuare l'ordinamento e la ricerca secondo un qualunque criterio basandosi sulla classificazione effettuata per il Documento.

È possibile selezionare i documenti per predisporre un unico PDF riepilogativo.

Nota: Nei segnalibri di Acrobat, sotto Indice, vengono presentati i vari Documenti selezionati.

È possibile richiedere un elenco dei documenti su Excel.

1.4.9.3 Modelli base aziendali

Ogni azienda può personalizzare i moduli prodotti da SQquadra.

Per ogni Modulo il programma propone il MODELLO BASE che può essere salvato in locale, personalizzato e quindi salvato come FILE AZIENDALE.

Nota: per le modalità operative si rimanda a quanto descritto, nel presente Manuale, nella sezione: D.Lgs 231 / Manutenzioni / Documenti / Modelli Aziendali.

1.4.9.4 Scadenziario

È possibile visualizzare le scadenze su un calendario (specifiche icone rappresenteranno i vari tipi di scadenze) o su un foglio di Excel.

È inoltre possibile ottenere la stampa delle schede relative alle manutenzioni in scadenza per i vari macchinari al fine di facilitare la registrazione delle operazioni svolte.

1.4.9.5 MAIL: Definizione mail da inviare

SQuadra può inviare mail per segnalare le scadenze.

È necessario definire la tipologia della mail da inviare. In particolare, sarà necessario indicare:

- Il Tipo di scadenze che attivano l'invio di mail.
- Il Sistema di interesse (se presente verranno inviate le mail unicamente relative al sistema scelto).
- Con quanti giorni di anticipo rispetto alla scadenza dovrà essere inviata la mail.
- La periodicità dell'invio espressa in giorni (1=ogni giorno, 7=ogni settimana, ecc.).
- L'indirizzo del destinatario. È possibile indicare uno specifico indirizzo o scegliere fra tipologia di destinatario predefiniti.

ATTENZIONE: La ricezione delle mail non può essere assicurata (per falsi positivi degli anti-spam o per altri motivi) quindi non bisogna fare affidamento solo sulla ricezione delle mail per scadenze importanti.

Per indirizzi fissi è possibile richiedere la spedizione di una mail di prova. Qualora la mail venga escluso dall'anti-spam sarà necessario dichiarare il mittente come attendibile al fine di ricevere le successive.

1.4.9.6 MAIL: Mail Spedite

Verranno presentate tutte le mail inviate.

1.4.9.7 Importazioni

È possibile importare da appositi fogli di excel i dati relativi a:

- Persone.
- Visite Mediche.
- Formazione.
- Consegne DPI.
- Fornitori.
- Macchinari.
- Giudizi relativi alla soddisfazione delle parti interessate.

Per ogni tipologia di importazione è necessario richiedere il File di Excel d'esempio nel quale andranno riempite le colonne di interesse.

Poiché il file d'esempio riporta i dati attuali si consiglia di inserire manualmente un elemento per comprendere meglio il significato delle varie colonne.

In alcuni file compare la colonna ID; questa contiene informazioni di sistema per recuperare eventuali vecchi dati. Non deve essere compilata per elementi nuovi.

Una volta compilato il file dovrà essere salvato e quindi selezionato per essere importato da SQuadra.

ATTENZIONE: è necessario che le colonne relative alle date ed ai valori numerici, se contengono un valore, questo deve essere appropriato altrimenti il programma segnalerà errore di conversione al momento dell'importazione.

Persone e Macchinari

È possibile che i file di importazione vengano prodotti da appositi programmi esterni (es. programma per la gestione delle paghe).

Una volta importati i dati sarà possibile inserire gli eventuali campi aggiuntivi (ad esempio Note o Fiduciario).

Alla successiva generazione del file questo conterrà le vecchie informazioni più quelle relative al nuovo personale.

Per evitare di perdere le informazioni già inserite o corrette su SQuadra il programma importerà solo i nuovi Nomi trascurando le righe relative ai Nomi già presenti su SQuadra.

Se il file di importazione è invece generato partendo da SQuadra, ad esempio per aggiungere velocemente su excel un dato mancante (es. la mail), esso contiene già tutte le informazioni precedentemente presenti su SQuadra e quindi è corretto, prima dell'importazione, cancellare tutti i dati per assicurare l'importazione di tutti i Nomi.

Fornitori

L'importazione creerà tutte le Tipologie utilizzate qualora non già definite. Sarà necessario entrare nelle varie categorie e quindi inserire le informazioni opportune.

1.5 Altre Funzioni

1.5.1 Documentazione di supporto

SQuadra231 mette a disposizione alcuni documenti che possono essere di supporto per la gestione del Sistema.

In particolare, vengono qui riportati i documenti predisposti da ANCE per le imprese non certificate in base alla norma ISO 45001 al fine di rispondere alle richieste dell'Art. 30 del D.Lgs 81/08 quali:

- MANUALE SGSL: Il documento, conforme alle Linee Guida UNI INAIL, non è né una norma né una linea guida di riferimento, ma il manuale del SGSL, redatto in forma ritenuta adeguata a una impresa di costruzioni tipica, reso disponibile in formato WORD per essere ulteriormente personalizzato e solo successivamente adottato dalla singola impresa.
- CPT – Torino / INAIL - LA VALUTAZIONE DEI RISCHI NELLE COSTRUZIONI EDILI: modelli per la redazione del documento di valutazione dei rischi, piano operativo di sicurezza e piano di sicurezza sostitutivo.
- Elenco delle schede di sicurezza macchine, impianti, opere provvisionali, attrezzature ed utensili contenute nel Manuale operativo per la valutazione dei rischi nelle costruzioni edili edito dal CPT di Torino. La raccolta di tali schede, con riferimento ai mezzi in uso da parte dell'impresa deve essere integrata con l'ulteriore documentazione fornita dai fabbricanti.
- Liste di controllo semplificate, tratte dalla Guida per la valutazione del sistema sicurezza sul lavoro in edilizia edito dal CPT di Torino, Roma e Verona del 2002, (da adeguare ad eventuali successive prescrizioni normative) utilizzabili per il monitoraggio di cantiere a cura dei vari preposti e/o del capocantiere con riferimento alle diverse fasi lavorative.

Documenti per il contenimento della pandemia da COVID-19

- Sono riportati vari documenti che possono essere di supporto per le imprese.

Documenti specifici per il Decreto 231/01

- Sono riportati documenti legati alle Linee Guida ANCE e altri documenti di supporto.

Oltre ai Documenti di supporto sono presenti le funzionalità per l'aggiornamento della Parte Speciale del MOG per le imprese che utilizzano il Codice di Comportamento ANCE per le quali si rimanda all'apposita appendice.

1.5.2 Amministrazione del Sistema

Per permettere il corretto utilizzo di SQuadra anche da parte di altri utenti è necessario definirli assegnando ad ognuno le proprie abilitazioni.

Per ogni nuovo utente dovrà essere definita la Prima Password da comunicare al nuovo utente chiedendogli di modificarla al primo ingresso.

Per ogni nuovo utente creato devono essere indicate le Funzionalità che desideriamo assegnargli selezionando fra quelle previste. È inoltre possibile definire se, per la funzionalità in esame, l'utente abbia l'accesso completo o solo in visualizzazione (non potrà effettuare modifiche).

Per le Non Conformità e le Azioni Correttive è possibile definire il Sistema di interesse. Qualora non definito l'utente potrà operare con tutti gli elementi.

Qualora non si assegni nessuna Funzionalità specifica il nuovo utente avrà tutte le Funzionalità (esclusa quella di creare nuovi Utenti).

Abilitazione alla gestione delle Segnalazioni

L'abilitazione alla gestione delle Segnalazioni [si veda l'apposita Appendice] può essere definita per un solo utente alla volta (sarà l'unico che avrà la possibilità di vedere le segnalazioni e sarà responsabile della loro gestione).

Viene tenuta la cronologia delle abilitazioni a questa particolare abilitazione nel quale sarà possibile unicamente inserire delle note.

È importante non fornire agli stakeholder il codice azienda (impedendo quindi la possibilità di registrarsi come segnalante e quindi di inviare segnalazioni all'OdV) prima di aver abilitato un utente alla gestione delle Segnalazioni.

Configurazione

L'Amministratore può configurare alcune funzioni di SQuadra. In particolare, potrà:

- **Gestione dei Macchinari:** Potrà scegliere se richiedere la generazione automatica delle nuove scadenze.
- **Gestione Segnalazioni:** Potrà scegliere se permettere all'OdV di conoscere le identità dei segnalatori riservate.

LOG Aziendali

SQuadra è protetta da Password che sono memorizzate in modo criptato all'interno dei database. Nessuno, tranne l'utente, può conoscerla.

Dato che non tutti gli utenti memorizzano su SQuadra dati personali o dati riservati non sono stati imposti vincoli sulle caratteristiche delle password (lunghezza, presenza di caratteri speciali, scadenza, ecc.). **Deve essere cura del singolo utente in funzione della criticità dei dati gestiti gestire correttamente la propria password.**

Per offrire una maggiore sicurezza è stata realizzata una funzione dalla quale è possibile controllare i LOG degli accessi alle varie funzioni di SQuadra. **Qualora venga rilevato un accesso anomalo si consiglia di modificare immediatamente la propria password.**

1.5.2.1 Segnalazioni su SQuadra

Ogni utente può inviare, in qualsiasi momento, segnalazioni al team di sviluppo di SQuadra.

Potrà modificare o cancellare le segnalazioni fino a quando non saranno prese in carico dal team di sviluppo di SQuadra che potrà richiedere chiarimenti.

Quando una segnalazione è stata analizzata dal team sarà possibile vedere le risposte fornite alla segnalazione nell'apposita maschera.

Per inviare una segnalazione è necessario definire il Tipo e l'Area alla quale si riferisce oltre ai dati di contatto.

1.5.3 Consulenti

L'ANCE mette a disposizione delle Imprese un elenco di Consulenti qualificati per il corretto utilizzo di SQuadra231 con specifica esperienza per la messa a punto di un Modello di Gestione per la prevenzione dei Reati all'interno di imprese di costruzione.

Ogni azienda può visualizzare l'elenco dei Consulenti per i quali sono riportati delle note. È anche possibile richiedere la stampa dei Curricula relativi.

Nomina Consulenti

Ogni azienda può scegliere di essere affiancata da uno o più consulenti. I Consulenti selezionati avranno accesso a tutti i dati aziendali inseriti su SQuadra231.

L'azienda potrà decidere, in ogni momento, di sospendere l'accesso ai dati di SQuadra231 ai Consulenti precedentemente autorizzati.

1.5.4 Rapporti con la Pubblica Amministrazione

È possibile descrivere ed archiviare i rapporti che le varie funzioni aziendali hanno con la Pubblica Amministrazione.

Si possono archiviare diversi tipi di rapporto:

- Verifiche Ispettive.
- Documentazione da produrre.

È possibile indicare i giorni previsti per predisporre i documenti in modo da pianificare le scadenze. Qualora sia necessario è possibile evidenziare lo specifico rapporto all'OdV.

1.5.5 Oneri per la Sicurezza

SQuadra mette a disposizione un modulo sperimentale per il calcolo degli Oneri per la Sicurezza (si veda l'apposita appendice).

1.5.6 Documentazione per la Sicurezza nei Cantieri [SicLa]

L'ANCE mette a disposizione degli utenti di SQuadra tutta la modulistica e tutta la documentazione prevista dal Testo unico sicurezza (D.Lgs. 81/08) relativa alle varie casistiche (si veda l'apposita appendice).

1.5.6.1 Azienda

Vengono richieste una serie di informazioni relative all'Azienda che verranno utilizzate per la compilazione dei vari documenti.

1.5.6.2 Lavori

È necessario inserire le informazioni relative ai vari lavori.

Soggetti

Per ogni Lavoro è necessario definire i soggetti coinvolti.

Per ogni soggetto devono essere inserite le informazioni necessarie per la compilazione dei documenti fra cui le valutazioni sull'adeguatezza del POS.

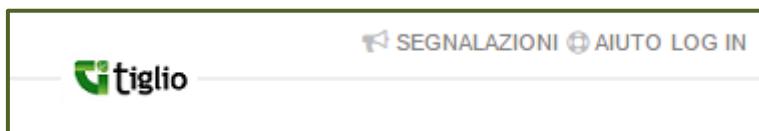
NOTA: è possibile, dal pannella RICERCA, copiare i dati anagrafici del soggetto se già inseriti in un altro lavoro.

Documenti

Una volta inseriti i vari Soggetti è possibile richiedere, attraverso l'apposito bottone, la Predisposizione dei Documenti necessari.

2 Caratteristiche generali di SQUADRA231

2.1 Ingresso



Dal link: <http://231.squadra.iltigliosrl.it/> è possibile accedere a:

- Segnalazioni (vedere apposita APPENDICE)
- Menù di Aiuto
- LOG IN / Menù Utente

NOTA: è possibile utilizzare SQuadra231 contemporaneamente su più schede del browser ma è necessario ripetere il LOG IN per ogni scheda. Non è ammesso di copiare semplicemente il link o duplicare la scheda.

Menù di aiuto

Dal Menù di aiuto è possibile inviare mail di richiesta al servizio assistenza di SQuadra231.

Sempre dal Menù di aiuto è possibile scaricare il programma per consentire, al servizio di assistenza, di collegarsi in caso di bisogno di supporto.

In alcuni casi sotto il Menù di aiuto è presente il link filmati illustrativi della funzionalità e delle modalità d'uso della maschera corrente del programma.

Dal Menù di aiuto è possibile scaricare la versione sempre aggiornata di questo manuale.

Menù Utente

Una volta inserite le Credenziali il bottone LOG IN si trasforma nel Menù utente che presenta il nome dell'utente e permette di:

- Cambiare la Password.
- Passare alla versione BASE di SQuadra231 (solo per le Aziende associate ad ANCE).
- Uscire dal Programma

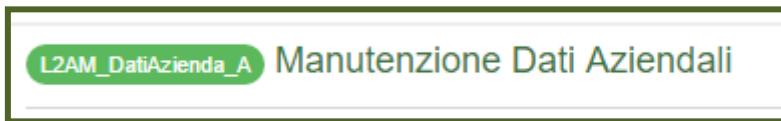
NOTA: È importante che l'utente modifichi la propria password al primo ingresso e periodicamente al fine di garantire la sicurezza. La password non deve essere comunicata a nessuno; in caso di smarrimento è sempre possibile richiedere al sistema (in basso nella maschera di Log in) di inviare alla mail dell'utente una nuova Password per l'accesso.

2.2 Menù generale

La parte superiore si presenta con le caratteristiche mostrate nell'immagine sottostante.

Nella parte in alto sono presenti il Menù di Aiuto e quello Utente e, sotto, vengono presentate le Sezioni del Menù all'interno delle quali si trovano le possibili Scelte e Sottoselezioni.

2.3 Identificativo della maschera



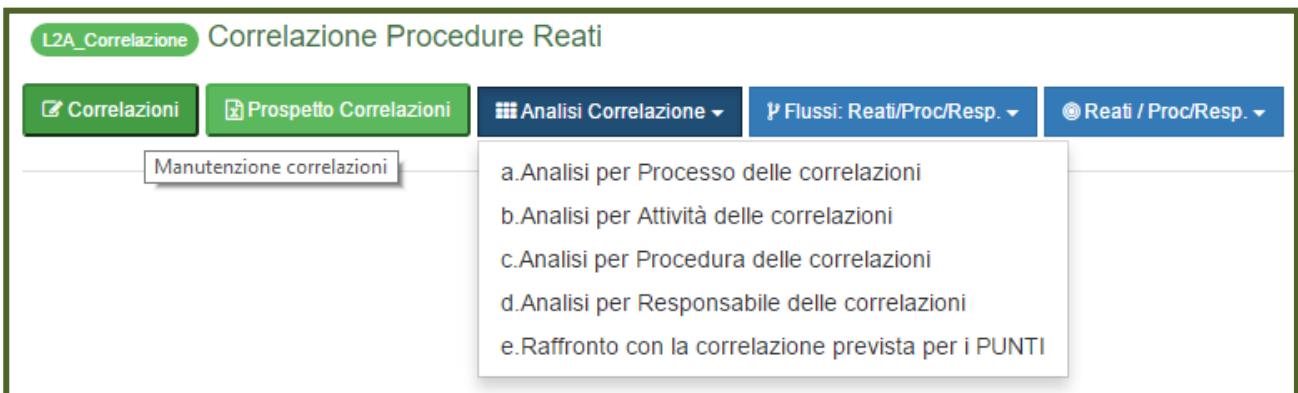
Ogni maschera presenta nella parte in alto a sinistra un Codice Identificativo (che deve essere citato nelle eventuali richieste di assistenza) ed una breve Descrizione.



Nel caso di elaborazioni di dettaglio, sotto il titolo della maschera appare la sequenza dei passaggi in base ai quali siamo arrivati alla maschera attuale. È possibile tornare indietro di un passo (il primo bottone del gruppo di destra in basso) o tornare al Menù premendo la prima icona in alto (casa).

2.4 Elaborazioni

Sotto alcune maschere appaiono una serie di Bottoni corrispondenti ad ulteriori scelte di funzionalità del programma non richiamabili direttamente dal Menu principale.



I Bottoni azzurri racchiudono ulteriori sotto scelte mentre i bottoni verdi permettono di accedere direttamente alla scelta (portando il mouse sopra un pulsante verde si ottengono ulteriori informazioni sull'operazione sottostante).

2.5 Manutenzioni

Tutte le Manutenzioni dei dati operano in maniera analoga.

Per prima cosa i dati già presenti vengono presentati in modalità GRIGLIA. L'utente può scegliere di andare nei DETTAGLI di ogni elemento fra quelli presenti nella GRIGLIA.

Se non è presente nessun Elemento o è presente un solo elemento il Programma, in alcuni casi, si predisporrà automaticamente per l'inserimento/modifica del primo elemento in modalità DETTAGLI.

2.5.1 Manutenzioni - Modalità GRIGLIA

		Nuovo	Esci	Manutenzione Funzioni: Azienda M srl			
Azione	Funzione	Area	Responsabile	Multipla	Nº Proc.		
	a0.Presidente del CdA o Consigliere Delegato	Per tutta l'azienda	Mario Rossi	<input type="checkbox"/>	18		
	b0.Resp. Acquisti	Per tutta l'azienda	Carlo Verdi	<input type="checkbox"/>	15		
	c0.Resp. Commerciale	Per tutta l'azienda	Mario Rossi	<input type="checkbox"/>	15		
	d0.Resp. Tecnico	Per tutta l'azienda	Carlo Verdi	<input type="checkbox"/>	1		
	f0.Resp. Amministrativo	Per tutta l'azienda	Anna Neri	<input type="checkbox"/>	25		
	f1.Servizi Amministrativi Esterni	Per tutta l'azienda	Servizi per le Imprese srl	<input type="checkbox"/>	5		
	g0.Gestione Paghe esterna	Per tutta l'azienda	Servizi per le Imprese srl	<input type="checkbox"/>	3		
	g1.Resp. Personale	Per tutta l'azienda	Mario Rossi	<input type="checkbox"/>	10		
	h0.Resp. Istruttoria per progetto con fondi p...	Per tutta l'azienda	Anna Neri	<input type="checkbox"/>	3		
	h1.Resp. Progetto con fondi pubblici	Per tutta l'azienda	Anna Neri	<input type="checkbox"/>	4		
	i0.Resp. Sistemi Informativi	Per tutta l'azienda	Enrico Viola	<input type="checkbox"/>	5		
	l0.Resp. Archivio	Per tutta l'azienda	Anna Neri	<input type="checkbox"/>	1		
	m0.Datore di Lavoro	Per tutta l'azienda	Mario Rossi	<input type="checkbox"/>	12		
	n0.RSPP	Per tutta l'azienda	Ing. Antonio Gialli	<input type="checkbox"/>	4		
	n1.Medico Competente	Per tutta l'azienda	Dott.ssa Gianna Rossini	<input type="checkbox"/>	1		
	n2.Rappresentante dei Lavoratori per la Sicu...	Per tutta l'azienda	Geom. Gianni Bianchini	<input type="checkbox"/>	1		
	o0.Direttore Tecnico di cantiere	Per tutta l'azienda	Direttore Tecnico di cantiere (per i Cantieri di co...)	<input checked="" type="checkbox"/>	14		
	p1.Capocommessa	Per tutta l'azienda	Capocommessa (per i Cantieri di competenza)	<input checked="" type="checkbox"/>	9		
	p2.Capocantiere	Per tutta l'azienda	Capocantiere (per i Cantieri di competenza)	<input checked="" type="checkbox"/>	8		
	q0.Resp. Ambientale	Per tutta l'azienda	Carlo Verdi	<input type="checkbox"/>	4		

<< << | Pagina 1 | di 2 | >> >> | 20 | ▾

Righe 1 - 20 di 22

Vengono presentate varie righe ognuna delle quali si riferisce ad uno degli elementi in esame.

In basso, al centro, viene indicata la pagina e viene data la possibilità di scorrere le varie Pagine. Accanto viene indicato quanti elementi si desidera presentare per ogni Pagina.

In basso, a destra, viene indicato il numero totale degli elementi.

Al centro vengono presentati gli Elementi di interesse.

Nella Parte alta della Griglia viene indicato il significato di ogni Colonna.

Dimensioni colonne

È possibile allargare o restringere la larghezza di una colonna, così da poter visualizzare nel modo più utile possibile le informazioni contenute all'interno della griglia.

Selezione dei dati

Sotto il Titolo di ogni colonna è presente uno spazio nel quale è possibile scrivere un insieme di caratteri. Alla conferma gli elementi verranno filtrati lasciando solo quelli che contengono l'insieme di caratteri definiti. Ovviamente, cancellando i caratteri inseriti verranno nuovamente presentati tutti gli elementi. È possibile inserire più filtri per le varie colonne.

Ordinamento dei dati

I dati possono essere ordinati in ordine crescente o decrescente per ogni colonna.

È possibile ottenere l'ordinamento in base ad una colonna e quindi, a parità di elementi di questa colonna, rispetto ad una successiva.

Facendo clik sul titolo di una colonna, accanto alla descrizione apparirà una freccia verso l'alto (ordinamento dal più piccolo al più grande); ad un nuovo clik la freccia sarà verso il basso (dal più grande al più piccolo).

Operazioni sui dati

Per ogni elemento, nella visualizzazione in GRIGLIA vengono mostrate alcune informazioni.

A sinistra vengono presentate le operazioni previste (le operazioni previste possono differire in funzione del tipo di informazione e dalle abilitazioni del singolo utente).

Le operazioni possibili sono:

	Modifica: permette di passare alla visualizzazione in DETTAGLIO nella quale sarà possibile apportare tutte le modifiche ai dati.
	Duplica: duplica l'elemento presentato nella riga e passa alla visualizzazione in DETTAGLIO per permetterne la modifica. Le informazioni verranno memorizzate dal Programma solo se verranno salvate dopo le opportune modifiche.
	Elimina: permette l'eliminazione dell'elemento. Il programma chiederà una conferma per evitare la perdita accidentale dei dati.
	Presentazione di dettaglio: in alcuni casi l'utente non è abilitato alla modifica delle informazioni presenti. Il pulsante permette di visualizzare in formato DETTAGLI i dati della riga selezionata.

Nuovo

Sopra la griglia è presente il pulsante che permette di inserire le nuove informazioni.

Esci

Sopra la griglia è presente il pulsante che permette di uscire dalla funzione attuale.

2.5.2 Manutenzioni - Modalità DETTAGLI

Dalla presentazione dei dati in Modalità GRIGLIA è possibile passare alla Modalità DETTAGLI nella quale è possibile inserire nuovi elementi o modificare quelli già presenti.

[L2AM_Registro_A] Manutenzione Procedure: Costruzioni edili H s.r.l.

Processo	P.02-Processo di approvvigionamento	Attività	P02.A01-Valutazione e qualificazione dei fornitori
Punto	02.01-Sistema di qualificazione dei fornitori	<p>Il vertice aziendale decide le modalità per la valutazione e qualificazione dei fornitori, che può essere effettuata predisponendo uno specifico Albo Fornitori Qualificati, ovvero effettuata di volta in volta al momento della richiesta di offerta al fornitore, e comunque prima della stipula di ciascun ordine/contratto di fornitura</p>	
Non Applicabile	<input type="checkbox"/>	Motivi non applicazione	<input type="text"/>
Codice	02.01-a	Responsabile	a0.Presidente del CdA o Consigliere Delegato: Carlo Bianchi
Cosa	Decidere le modalità per la valutazione e qualificazione dei fornitori, che può essere effettuata predisponendo uno specifico Albo Fornitori Qualificati, ovvero effettuata di volta in volta al momento della richiesta di offerta al fornitore, e comunque prima della stipula di ciascun ordine/contratto di fornitura.		
Registrazione	Procedura di qualifica dei fornitori	Quando	Revisione annuale della procedura
Note	<input type="text"/>		
<input type="button" value="Salva"/> <input type="button" value="Avanti >"/> <input type="button" value="Nuovo +"/> <input type="button" value="Reset"/>		<input type="button" value="+ Nuovo"/> <input type="button" value="Duplica"/> <input type="button" value="Elimina"/>	<input type="button" value="Esci"/> <input type="button" value="Lista"/> <input type="button" value="Prec."/> <input type="button" value="Succ. >"/>

In alto, a sinistra, viene indicato il codice identificativo della Maschera (dovrà essere indicato nelle eventuali segnalazioni di anomalie o richieste di chiarimento).

Di seguito vengono presentati i dati che caratterizzano l'elemento in esame. Alcuni campi (evidenziati in grigio) non sono modificabili dall'utente.

In basso vengono presentati i bottoni con le varie funzionalità.

A volte i dati vengono suddivisi in più cartelle che, ove opportuno, vengono presentate in alto.

Blocco di sinistra

Ogni modifica verrà memorizzata solo premendo il pulsante SALVA. Per comodità sono presenti anche i bottoni SALVA E SUCCESSIVO e SALVA E NUOVO che congiungono con la pressione di un solo Pulsante due funzioni e sono utili nel caso di inserimento di una serie di dati o nella modifica di un gruppo di elementi.

Il Pulsante RESET annulla tutte le modifiche effettuate dall'ultimo salvataggio.

Blocco di centro

Al centro si ritrovano gli stessi bottoni già illustrati per la modalità GRIGLIA: NUOVO, DUPLICA ed ELIMINA.

Blocco di destra

I bottoni a destra permettono di spostarsi all'elemento PRECEDENTE o SUCCESSIVO rispetto all'ordinamento della griglia.

Con il bottone LISTA si tornerà alla modalità Griglia.

È infine possibile uscire dalla FUNZIONE (Esci). Se siamo in un Dettaglio si tornerà al "passo" precedente.

Inserimento dati

Campi data

In tutti i punti del programma nei quali è richiesto di inserire una data vengono utilizzate le apposite funzionalità previste dal Browser in uso.

Campi di selezione fra elementi predefiniti

Alcuni campi testuali mostrano sulla destra una freccia in basso.

In questo caso nel campo è possibile inserire solo un valore predefinito fra quelli che appaiono premendo le frecce.

Per cancellare il valore inserito premere la "X" alla sinistra della freccia.

Per far sparire l'elenco degli elementi premere la Freccia in alto.

Campi di selezione "liberi"

Alcuni campi testuali mostrano sulla destra un bottone con tre barrette orizzontali.

In questo caso nel campo è possibile inserire uno dei valori già inseriti nello stesso campo che appaiono premendo il bottone.

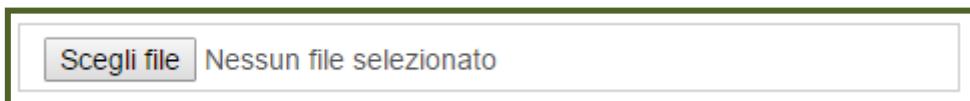
Scrivendo un qualunque testo vengono proposti (in basso) i testi già usati che lo contengono; con il mouse può essere uno degli elementi fra quelli proposti.

È comunque possibile inserire un qualunque altro testo (in questo caso è necessario premere ESC per passare al campo successivo) che si aggiungerà a quelli proposti per la prossima volta.

Per far sparire l'elenco degli elementi premere nuovamente il bottone con le tre barrette.

Campi File

Alcuni campi permettono di collegare ad un elemento un File presente nelle cartelle locali dell'Utente.



In questi casi l'utente dovrà selezionare il file sfogliando le proprie cartelle alla ricerca del file di interesse.

Alla richiesta di salvataggio verrà salvato il record con le altre informazioni ed inoltre verrà trasferito al server di SQuadra231 il File selezionato; l'operazione può quindi essere lenta in caso di file molto grossi in relazione alla banda a disposizione.



Quando si accede ad un record relativo ad un Allegato già salvato sul Server di SQuadra231 al posto di "Sfoglia" si troveranno i bottoni "Visualizza" (che permette di aprire in locale il file precedentemente archiviato) e "Annulla" (che elimina il file precedentemente archiviato permettendo l'inserimento di un nuovo file).

2.5.3 Manutenzioni – Griglie di dettaglio

In alcuni casi ad un elemento di dettaglio (es. un Punto di Controllo) sono collegati più elementi (es. Procedure e Reati collegati).

In questo caso, sotto le informazioni di dettaglio viene presentata una o più "linguette" con sotto, in modalità griglia, gli elementi.

2.6 Cruscotti di presentazione dei dati

In molte aree del programma viene utilizzata una particolare rappresentazione dei dati che chiameremo “Cruscotto” di presentazione alla quale è associata l’icona:

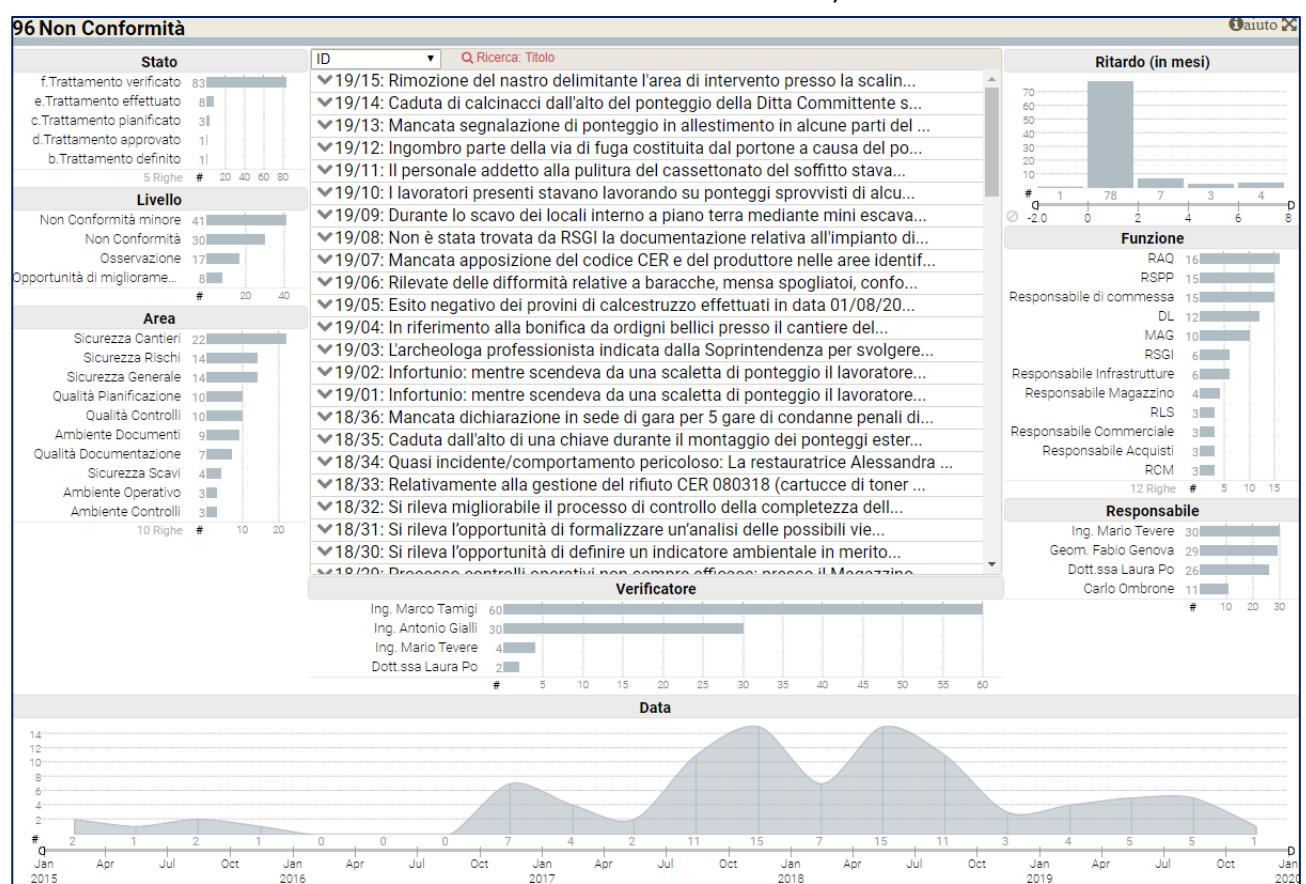


Di seguito riportiamo degli esempi relativi alla gestione di Non Conformità.

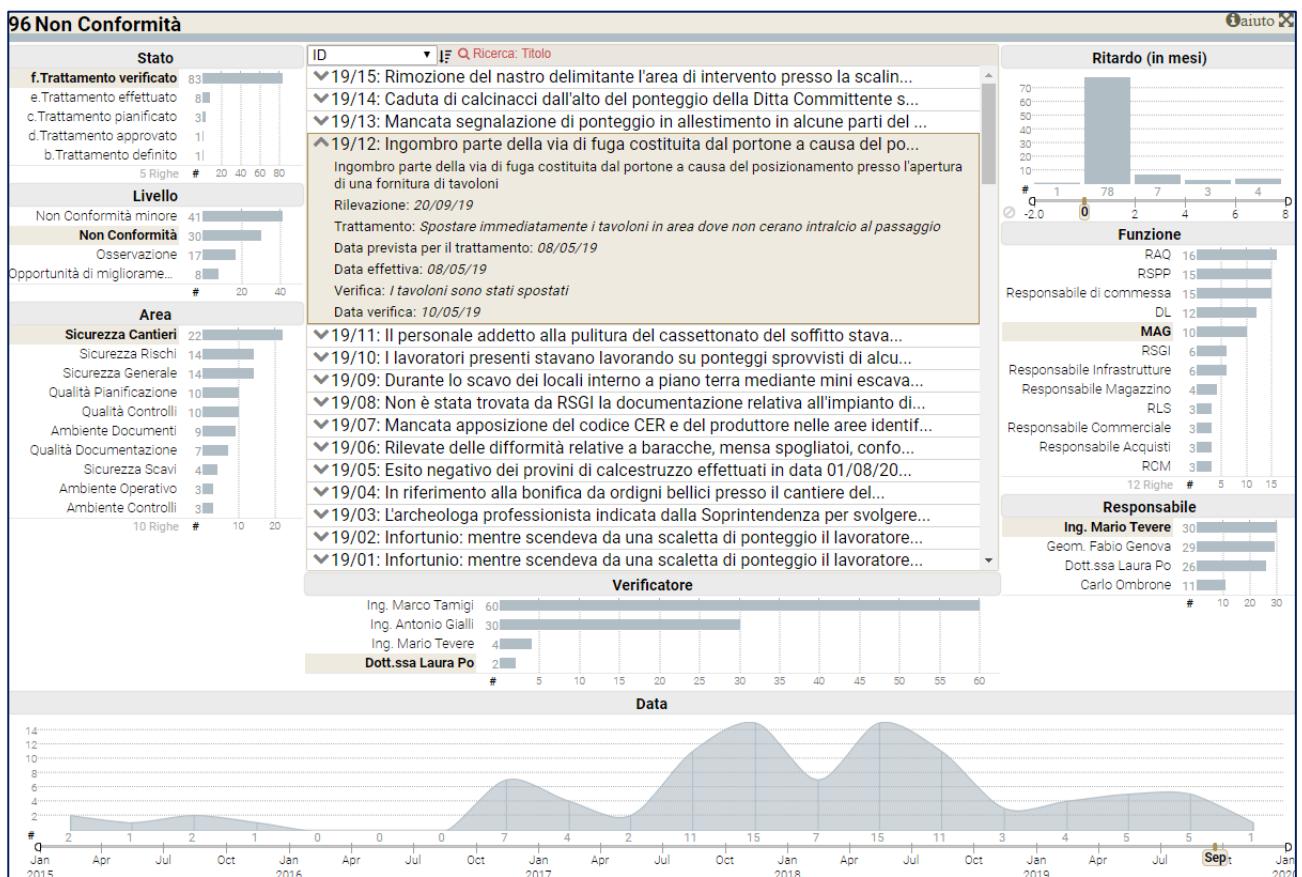
Entrando è possibile vedere, al centro, gli elementi di interesse (in questo caso le Non Conformità), a sinistra, a destra e in basso dei raggruppamenti di informazioni relative agli elementi di interesse (in questo caso: lo Stato, il Livello, l’Area, ecc.). Da notare che in basso viene presentata una scala temporale con l’indicazione del posizionamento nel tempo dei vari elementi.

In alto a sinistra viene indicato il numero degli elementi in analisi (in questo caso 96).

Nei vari raggruppamenti è indicata la numerosità per i vari oggetti (Nell’esempio: In 83 NC il trattamento è stato verificato mentre in 8 è stato solo effettuato ma non ancora verificato. Le NC Minori sono 41. Sono relativa alla Sicurezza Cantieri 22 NC. ecc.).



Nel cruscotto ogni Non conformità è identificata dal Codice (in questo caso Anno e Numero progressivo) e dei primi caratteri della Descrizione ma, premendo la freccia verso il basso, è possibile visualizzare tutti i suoi dettagli (vedi NC 19/12).



Quando ci si posiziona su una specifica Non Conformità vengono evidenziati tutti gli oggetti collegati.

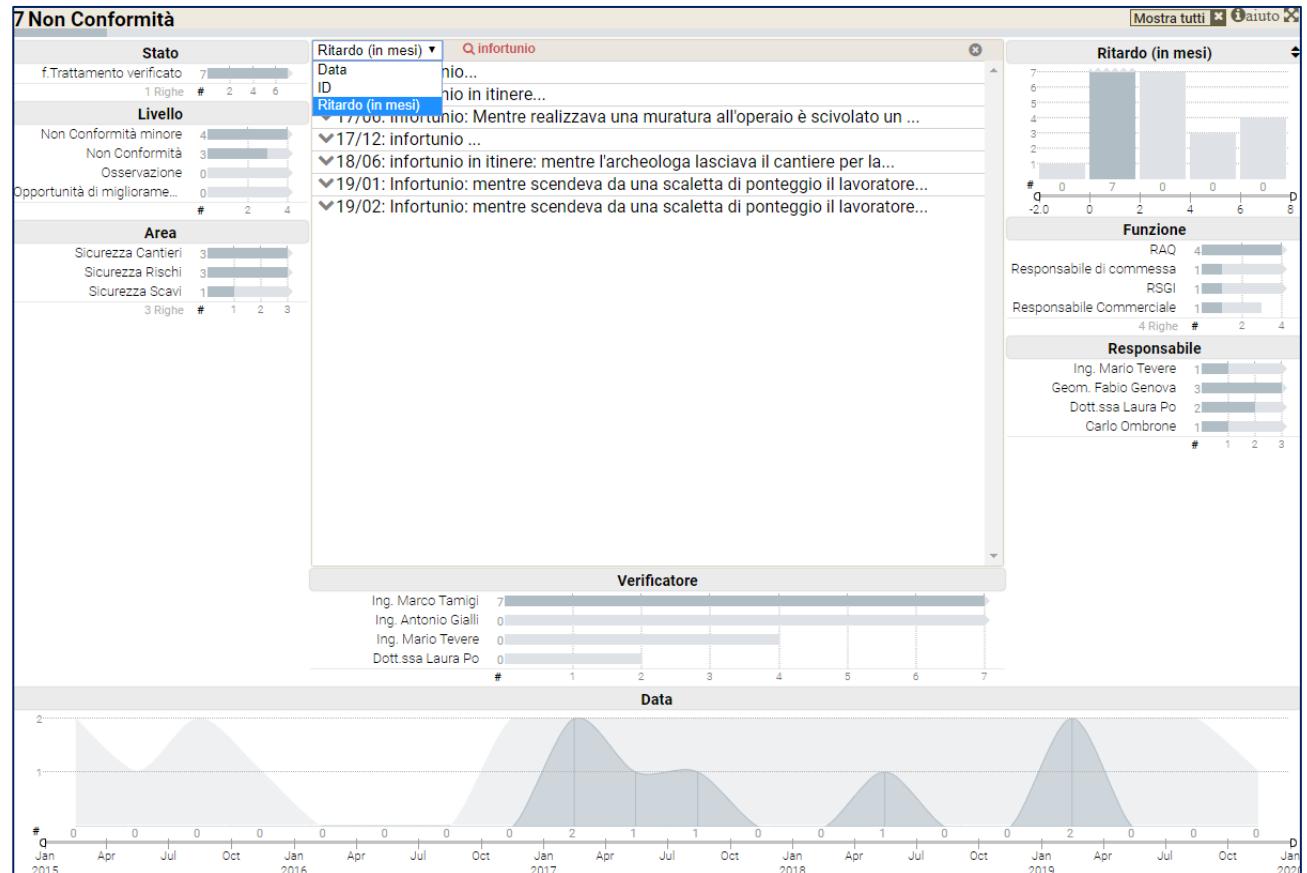
Nell'esempio posizionandosi sulla NC 19/12 è possibile vedere che:

- STATO: Trattamento verificato.
- LIVELLO: Non Conformità.
- AREA: Sicurezza Cantieri.
- RITARDO: 0 Mesi.
- FUNZIONE: MAG.
- RESPONSABILE: Ing. Mario Tevere.
- VERIFICATORE: Dott.ssa Laura Po.
- DATA: Settembre 2019.

I dati possono essere presentati secondo vari criteri di ordinamento oltre che in base all'identificativo (ordine nel quale appaiono all'apertura del "cruscotto").

È anche possibile "filtrare" gli elementi in base ad un qualunque testo.

Nell'esempio seguente vengono mostrate le 7 Non Conformità che soddisfano il filtro scelto ("Infortunio") ordinate in base al Ritardo (dal più alto al più basso).



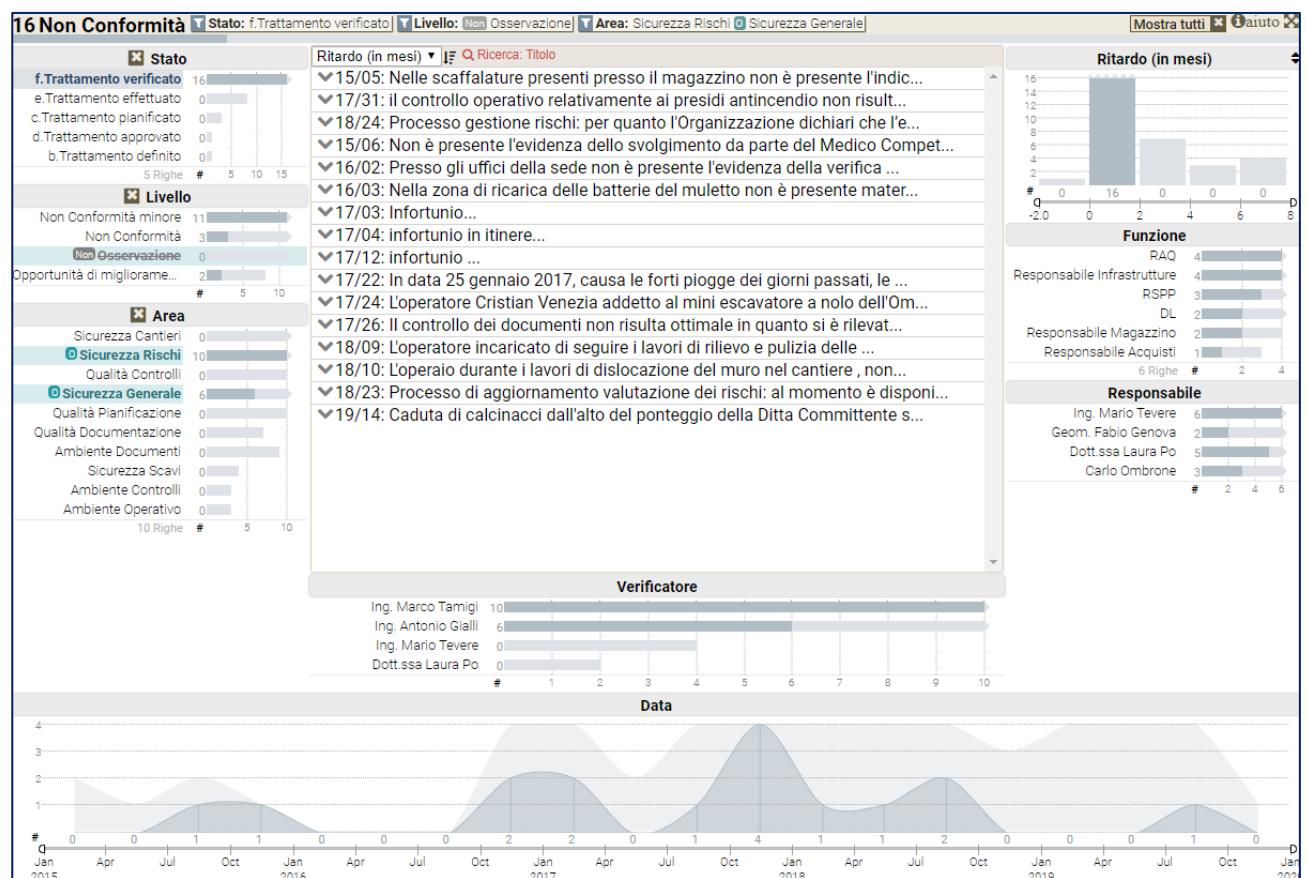
Tutte le informazioni di contorno si riferiscono ai soli elementi presentati in quel momento (nell'esempio alle sole 7 Non conformità di interesse).

Premendo il bottone "Mostra tutti" (in alto a destra) vengono ripresentati tutti gli elementi.

È possibile “filtrare” gli elementi anche in base ad una o più Caratteristiche semplicemente utilizzando il mouse per evidenziare l’elemento o l’area di interesse.

Nell’esempio seguente sono state individuate le 16 Non Conformità che:

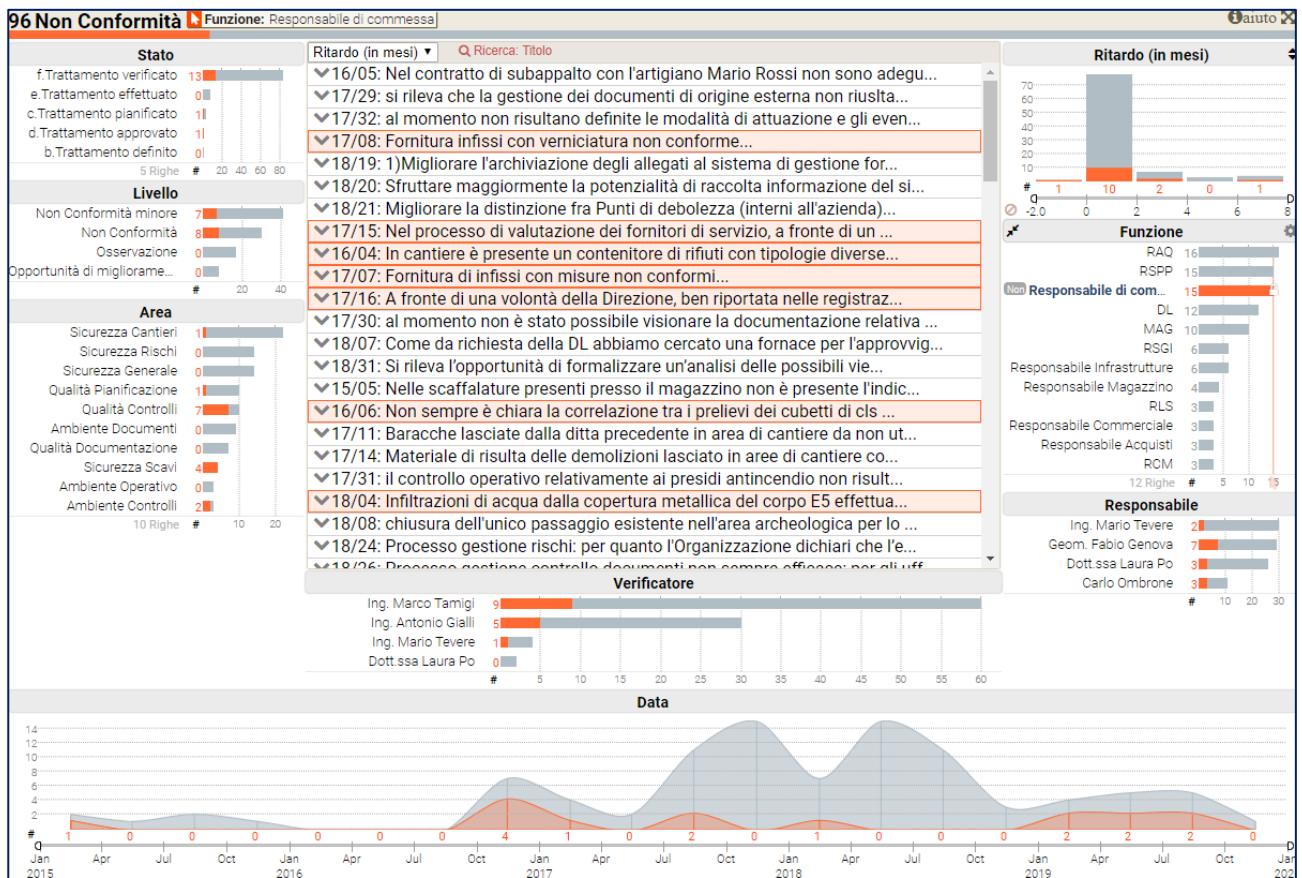
- Hanno lo Stato = “Trattamento verificato”.
- Non sono ritenute di Livello = “Osservazioni”.
- Sono relative all’Area: “Sicurezza Rischi” o “Sicurezza Generale”.



In alto, dopo l’indicazione del numero di elementi in esame, vengono riportati i criteri di filtro.

È possibile cancellare un singolo criterio di filtro o premere “Mostra tutti” per riavere la visione completa.

Portando semplicemente il mouse su un qualunque sottoinsieme di qualunque Elemento (ad esempio un particolare Stato o un particolare Livello o un intervallo di Date di rilevazione) vengono immediatamente evidenziate in rosso tutte le Non Conformità collegate ed evidenziate, sempre in rosso, le correlazioni con gli altri elementi (nell'esempio successivo l'attenzione è stata posta sulle 15 Non Conformità relative alla Funzione = "Responsabile di commessa").



Il cruscotto mostra che:

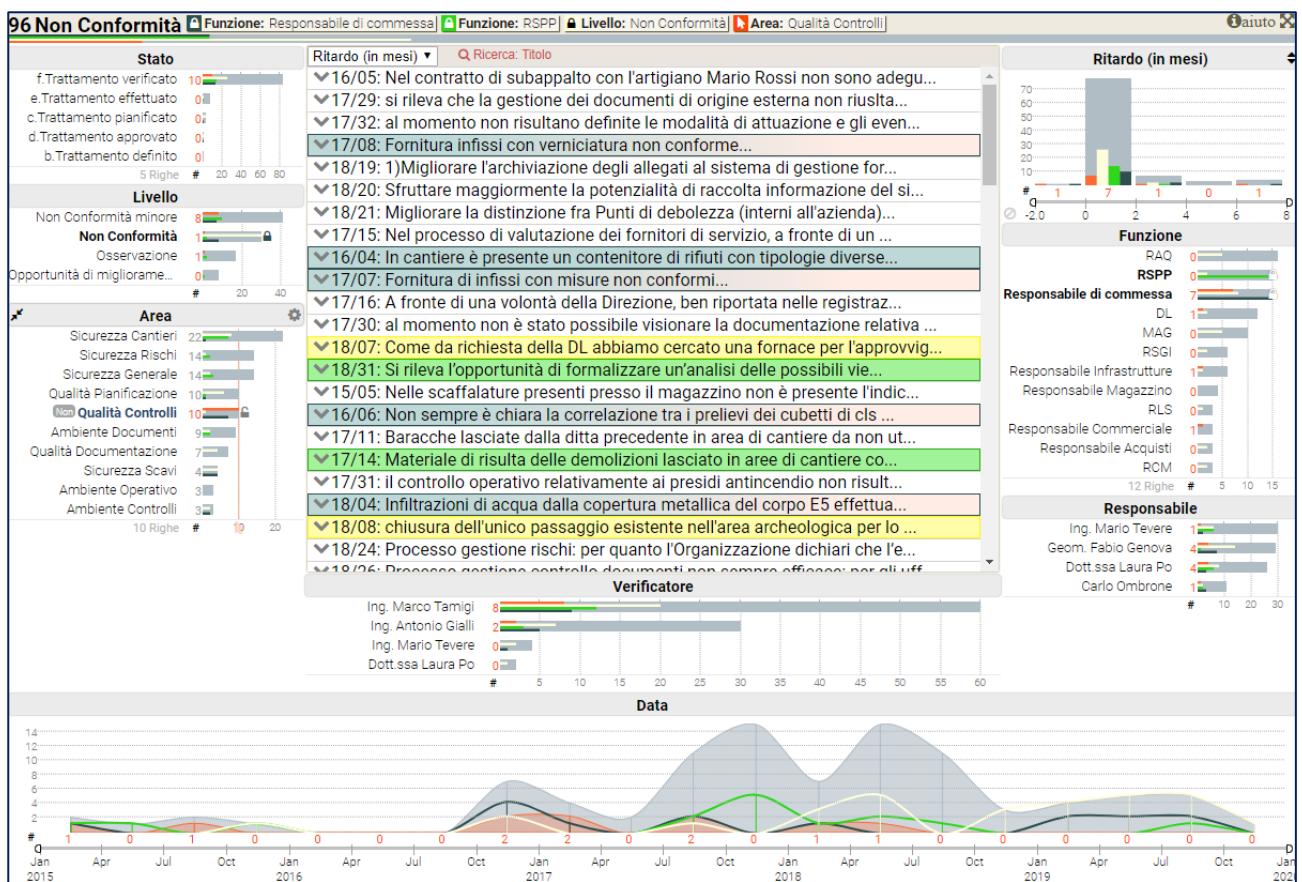
- 13 sono Verificate mentre per 1 il trattamento è pianificato e per 1 il trattamento è approvato.
- 7 sono “Non Conformità minori” mentre 8 sono “Non Conformità”.
- 1 è relativa alla “Sicurezza Cantieri”, 1 alla “Qualità Pianificazione” 7 alla “Qualità Controlli”, 4 alla “Sicurezza Scavi” e 2 a “Ambiente Controlli”.
- 1 ha un ritardo negativo mentre 1 ha un ritardo maggiore di 6 mesi.
- 7 sono assegnate al Geom. Fabio Genova, 3 ciascuna alla Dott.ssa Laura PO e a Carlo Ombrone, 2 all'Ing. Mario Tevere.
- I verificatori interessati sono: Ing. Marco Tamigi (9), Ing. Antonio Gialli (5) e Ing. Mario Tevere (1).

Premendo sul “lucchetto” che appare accanto alla selezione questa viene evidenziata con il colore nero. Analogamente una successiva selezione può essere evidenziata con il colore verde e quindi con il colore giallo. Esiste quindi la possibilità di analizzare in contemporanea fino a 4 criteri di selezione.

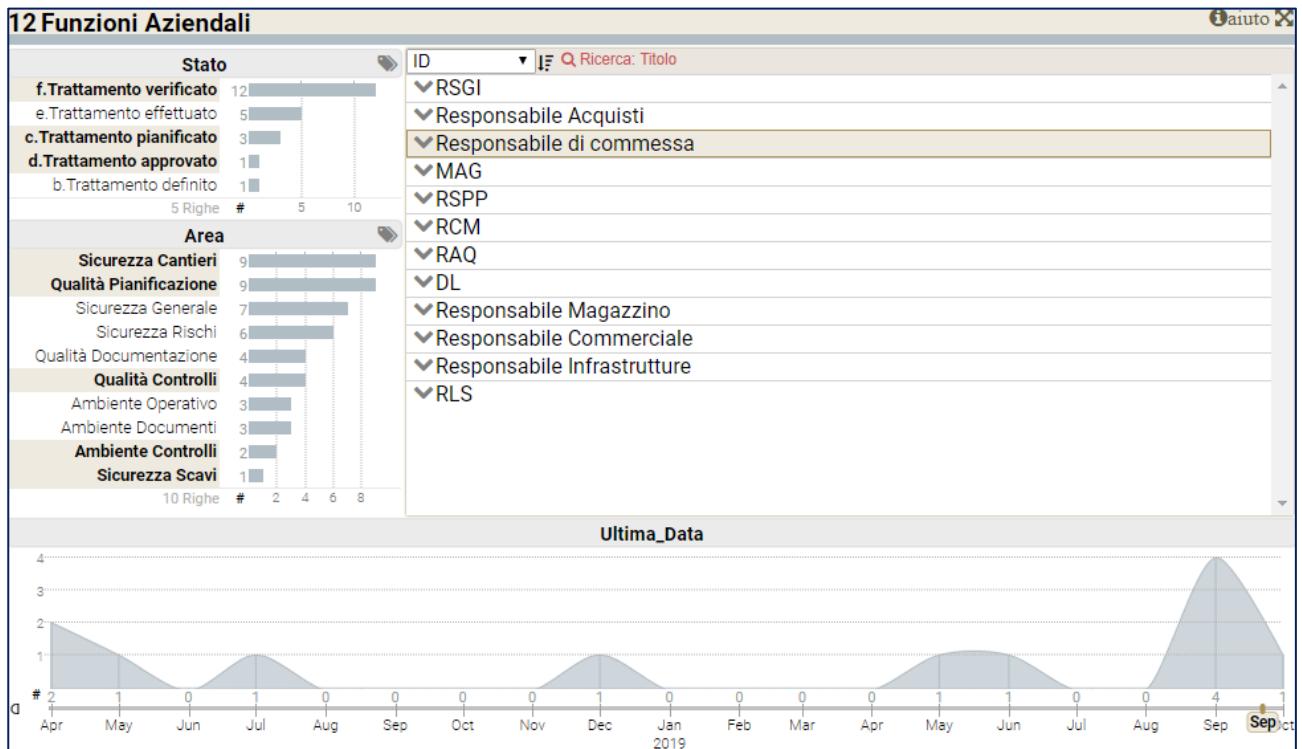
Nell'esempio riportato nella figura successiva vengono evidenziate contemporaneamente le seguenti con i rispettivi colori:

- NERO: NC della Funzione “Responsabile di commessa”.
- VERDE: NC della Funzione “RSPP”.
- GIALLO: Livello = “Non Conformità”.
- ROSSO: Area = “Qualità Controlli”.

Le Non Conformità, al centro, vengono evidenziate con il colore corrispondente o con più colori se rispondono a più caratteristiche (vedi, ad esempio, la 16/06).



Gli stessi elementi possono essere visti anche secondo differenti punti di vista. Nell'esempio riportato sotto le Non Conformità sono analizzate in base alla Funzione che le ha rilevate.

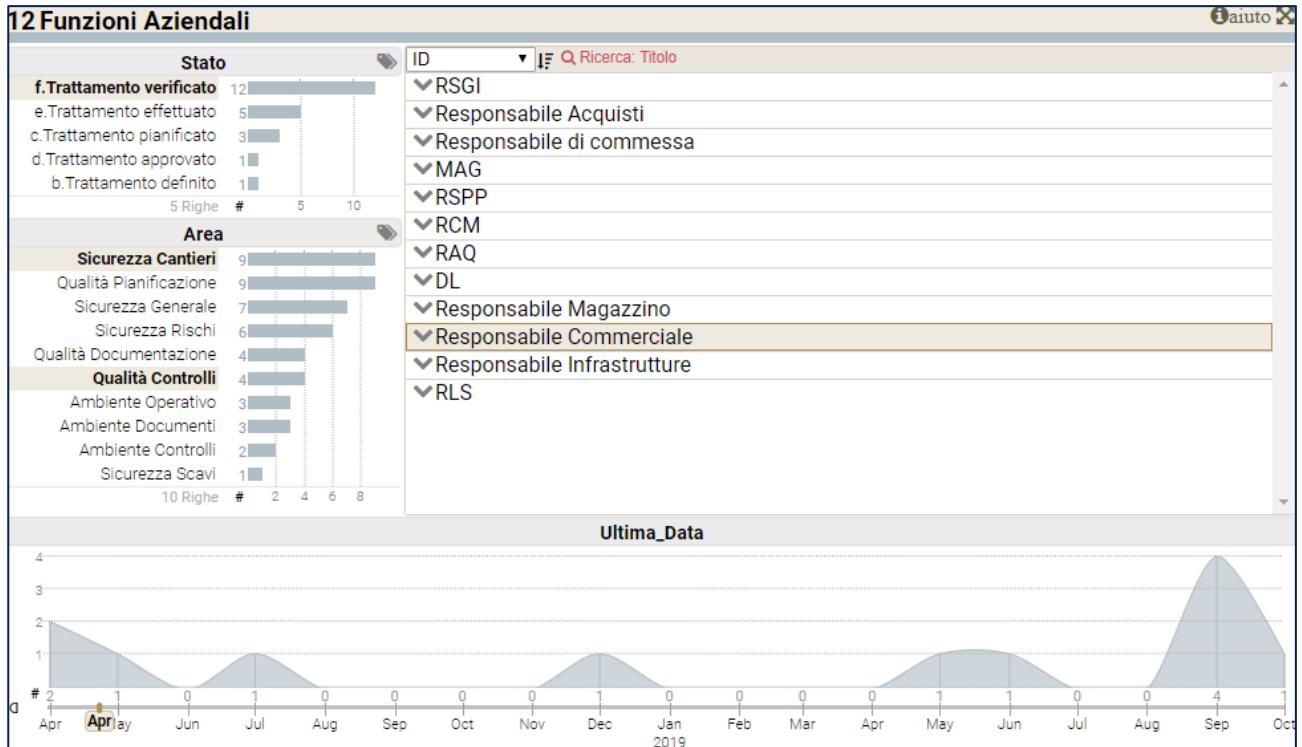


Sono presenti 12 Funzioni Aziendali.

Evidenziano una qualunque Funzione è possibile vedere in quali Stati si trovano le Non Conformità relative o a quali Aree appartengono.

Nell'esempio sopra riportato il "Responsabile di commessa" ha rilevato Non Conformità che si trovano negli Stati: "Trattamento verificato", "Trattamento pianificato" e "Trattamento approvato".

Le Aree interessate sono: "Sicurezza Cantieri", "Qualità Pianificazione", "Qualità Controlli", "Ambiente Controlli" e "Sicurezza Scavi". L'ultima Non Conformità è del settembre 2019.

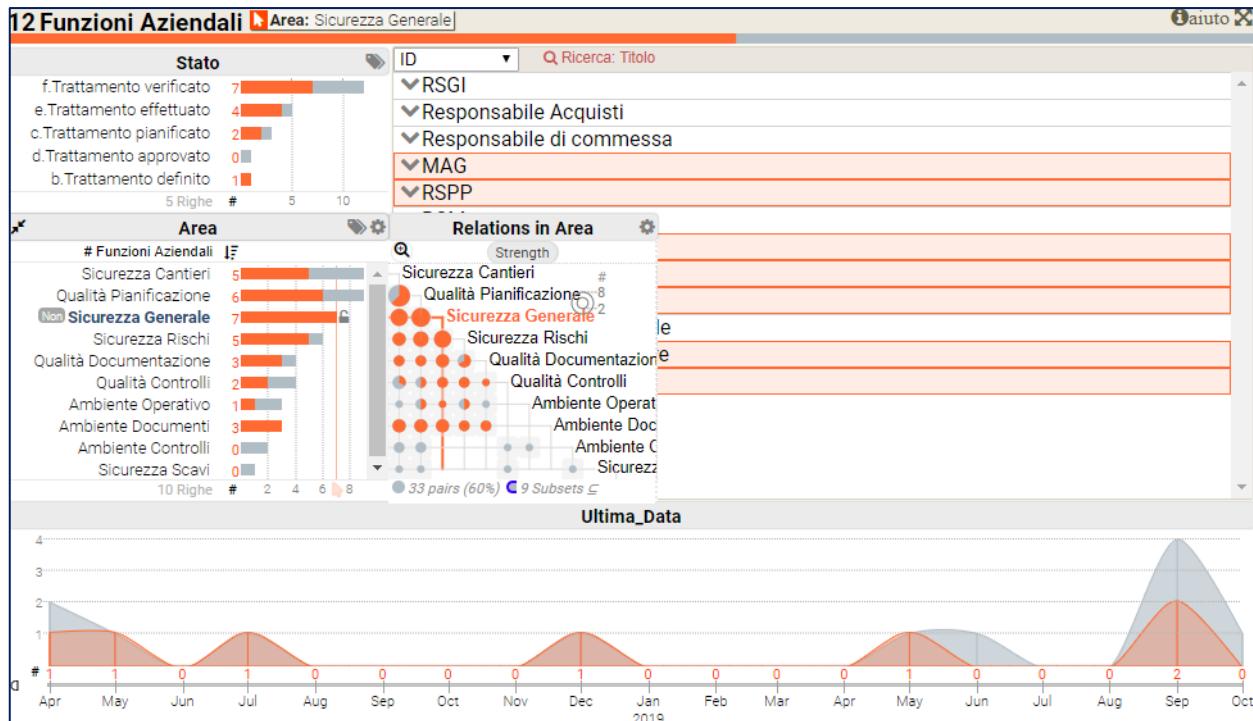


Tutte le Non Conformità del “Responsabile Commerciale” hanno Stato = “Trattamento verificato” e Area: “Sicurezza cantieri” o “Qualità Controlli”. L’ultima Non Conformità è dell’Aprile 2018.

È possibile ottenere una visualizzazione specifica che evidensi tutte le relazioni fra le varie Non Conformità.

Nell’esempio viene mostrato quali altre Aree hanno interessato le Non Conformità rilevate dalle Funzioni che hanno rilevato Non Conformità relative alla “Sicurezza Generale”.

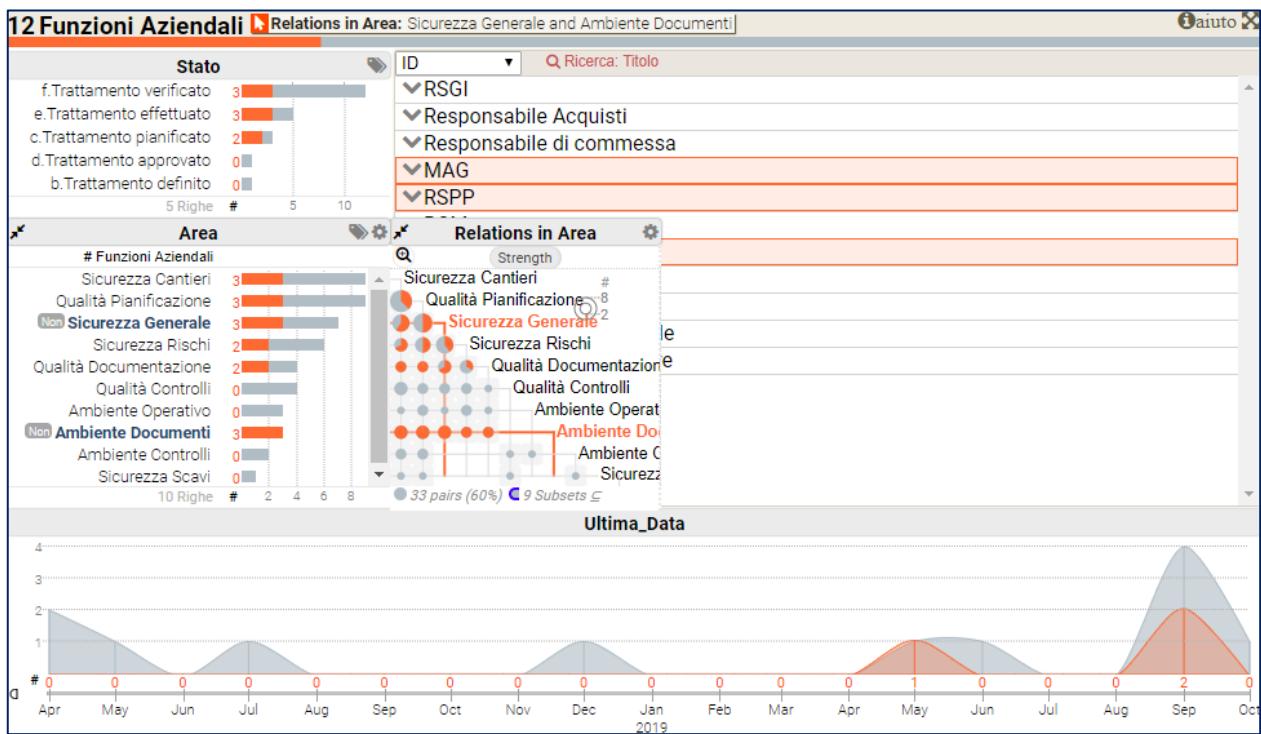
Seguendo la linea orizzontale e poi verticale viene mostrato quante delle 7 Funzioni hanno rilevato anche Non Conformità relative ad altre Aree e vedere, ad esempio, che non nessuna di queste ha rilevato Non Conformità relative a “Ambiente Controlli” e “Sicurezza Scavi”



Posizionando il mouse su un qualunque incrocio è possibile analizzare qualunque relazione.

Nell’esempio sotto riportato analizziamo le Funzioni che hanno rilevato Non Conformità sia per l’Area “Sicurezza Generare” che “Ambiente Documenti”.

Gli archi indicano le relazioni con le altre Aree. Le 3 Funzioni non hanno rilevato NC relative a “Qualità Controlli” e “Ambiente Operativo” (cerchi solo grigi).



2.6.1 Personalizzazione dei Cruscotti

La possibilità di visualizzare contemporaneamente molti oggetti che caratterizzano l’elemento analizzato è sicuramente comoda ma, a volte, soprattutto in relazione alla dimensione dello schermo utilizzato, può essere opportuno concentrare l’attenzione solo sugli elementi ritenuti essenziali.

In molti casi sono previste più possibili presentazioni dei dati nelle quali vengono scelti solo alcuni dei possibili oggetti da visualizzare. Vengono presentate alcune modalità di presentazione predefinite ma l’utente può liberamente cambiarle o crearne di nuove.

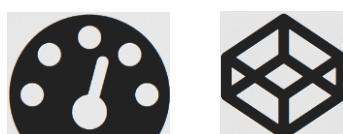
Ogni “Presentazione” è caratterizzata da un Codice ed un Descrizione. È quindi necessario indicare se si desidera visualizzare, al centro, gli elementi di dettaglio.

Per ogni “Presentazione”, in basso, sono visualizzate le impostazioni cioè i vari Oggetti di Riepilogo fra i quali è possibile scegliere per la specifica presentazione.

Ogni Oggetto può essere presentato (a Sinistra, al Centro, a Destra o in Basso) o meno.

Una volta scelta l’impostazione è possibile premere il bottone che richiama il cruscotto con le caratteristiche desiderate.

Le icone seguenti vengono utilizzate per indicare la possibilità di scegliere fra le varie presentazioni e per richiedere la presentazione del cruscotto con le impostazioni desiderate:



3 APPENDICE: Informativa sul Trattamento dei dati dei Clienti.

3.1 Informativa sul trattamento dei dati personali per i Clienti de IL TIGLIO SRL

Ai sensi dell'art. 13 del Regolamento UE N.2016/679 (Regolamento europeo in materia di protezione dei dati personali - GDPR) ed in relazione ai dati personali raccolti presso l'interessato che si intendono trattare, informiamo l'interessato di quanto segue:

Identità e dati di contatto del Titolare del trattamento.

Di seguito Le indichiamo quali sono i nostri riferimenti ai quali potrà rivolgersi per ogni chiarimento.

- Il Titolare del trattamento è: IL TIGLIO SRL, con sede in Viale della Repubblica 141, 59100 Prato, nella persona del suo rappresentante pro tempore Giuliano Marullo.
- Il Titolare può essere contattato tramite mail all'indirizzo: privacy@iltigliosrl.it.

Finalità del trattamento cui i dati sono destinati i dati personali e relativa base giuridica.

Di seguito Le indichiamo perché Le chiediamo i Suoi dati personali.

I dati forniti al momento dell'instaurazione del rapporto commerciale ovvero acquisiti in occasione dello sviluppo dello stesso, vengono raccolti allo scopo di provvedere agli adempimenti contabili, fiscali, commerciali, tecnici e per tutte le attività aziendali in genere inerenti al rapporto in essere.

In particolare, i dati personali saranno trattati:

senza il consenso degli interessati (articolo 6, lettere b, c, f, GDPR), per le seguenti finalità:

- Per provvedere in modo adeguato agli adempimenti connessi all'espletamento dell'attività economica della nostra società e in particolare per: esigenze preliminari alla stipulazione di un contratto; adempiere agli obblighi contrattuali nei confronti dell'interessato dando esecuzione ad un atto, pluralità d'atti od insieme di operazioni necessarie all'adempimento dei predetti obblighi; dare esecuzione presso ogni ente pubblico o privato agli adempimenti connessi o strumentali al contratto; dare esecuzione a adempimenti di obblighi di legge.

Il conferimento dei dati per le finalità sopra descritte è obbligatorio. La mancanza dei dati e/o l'eventuale espresso rifiuto al trattamento comporterà l'impossibilità per il Titolare di svolgere l'incarico conferito oppure la possibile violazione di richieste delle Autorità competenti.

Categorie di dati personali trattati.

Di seguito Le indichiamo quali tipologie di dati personali Le chiediamo.

Nell'ambito delle finalità dei trattamenti evidenziati al precedente paragrafo, saranno trattati unicamente dati personali che rientrano nella seguente categoria:

- COMUNI: dati anagrafici (quali, ad esempio: nome, cognome, indirizzo, data di nascita, cittadinanza), identificativi dei documenti d'identità (quali, ad esempio: numero patente/CI/passaporto), dati di contatto (quali, ad esempio: e-mail, contatti telefonici), coordinate bancarie.

Al fine di limitare l'uso di dati personali a quanto strettamente necessario (Art. 5 1/c del GDPR) sarà Vostra cura fornirci unicamente dati aziendali. Vi preghiamo quindi di fornirci, a titolo d'esempio, indirizzi mail aziendali quali "commerciale@azienda.it" e non contenenti riferimenti alle persone fisiche quali "m.rossi@azienda.it", numeri di telefono aziendali e non personali, ecc.

Qualora dobbiate necessariamente fornirci dati personali relativi a persone fisiche diverse da chi riceve la presente informativa (es. di Vostri titolari, soci, dipendenti o collaboratori) dovrete informare le persone fisiche titolari di detti dati che questi potranno essere trattati dalla nostra azienda e fornirgli le informazioni essenziali della presente informativa.

La presente informativa riguarda eventuali dati personali da Voi forniti ed è rivolta alle persone fisiche titolari di detti dati (interessati).

Categorie di destinatari dei dati personali.

Di seguito Le indichiamo chi potrà trattare i Suoi dati personali e a chi potranno essere comunicati.

Per le finalità di cui sopra i dati personali da Lei forniti potranno essere resi accessibili:

- A dipendenti e collaboratori del Titolare, nella loro qualità di addetti autorizzati al trattamento dei dati (o c.d. "incaricati al trattamento").
- A terzi soggetti che svolgono attività per conto del Titolare, nella loro qualità di Titolari autonomi, Contitolari del trattamento o Responsabili del trattamento, per lo svolgimento di attività economiche (commerciali, gestionali, gestione dei sistemi informativi, assicurative, intermediazione bancaria o non bancaria, factoring, gestione della spedizione, imbustamento e invio corrispondenza, gestione e tutela del credito) o per l'assolvimento di norme di legge (studi commercialisti, avvocati).
- Ad Autorità giudiziarie o di vigilanza, amministrazioni, enti ed organismi pubblici (nazionali ed esteri).
- Ad altre entità giuridiche di cui il Titolare fa parte.

È possibile richiedere l'elenco aggiornato dei soggetti destinatari dei dati all'indirizzo mail privacy@iltigiosrl.it.

Modalità del trattamento.

Di seguito Le indichiamo come saranno trattati i Suoi dati personali.

Il trattamento dei dati personali degli interessati è realizzato per mezzo delle operazioni (raccolta, registrazione, organizzazione, strutturazione, aggiornamento, conservazione, adattamento o modifica, estrazione ed analisi, consultazione, uso, comunicazione mediante trasmissione, raffronto, interconnessione, limitazione, cancellazione o distruzione) compiute sia in formato digitale (su server e cloud adeguatamente protetti e ubicati all'interno dell'Unione Europea di proprietà e/o nella disponibilità del Titolare e/o di società terze incaricate, debitamente nominate quali responsabili del trattamento) sia in forma cartacea (in contenitori non accessibili a terzi estranei).

In ogni caso, sarà garantita la sicurezza logica e fisica dei dati e, in generale, la riservatezza dei dati personali trattati, mettendo in atto tutte le necessarie misure tecniche e organizzative adeguate a garantire la loro sicurezza.

Principi generali.

Di seguito Le indichiamo gli aspetti generali che caratterizzano il trattamento dei Suoi dati personali.

I dati saranno trattati in modo lecito, corretto e trasparente nei confronti dell'interessato, raccolti per le finalità sopra indicate, limitati e conservati quanto necessario con adeguate misure di sicurezza.

Non è previsto il trasferimento all'estero dei dati nei paesi extra-UE.

I dati personali degli interessati non saranno oggetto di diffusione.

Non è previsto che i dati vengano trattati per processi decisionali automatizzati.

In caso di violazione dei dati personali suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare provvederà ad informare i Clienti senza ingiustificato ritardo. Sarà cura dei Clienti informare tutti gli interessati.

Periodo di conservazione dei dati personali.

Di seguito Le indichiamo per quanto tempo conserveremo i Suoi dati personali.

I dati personali raccolti per le finalità indicate al relativo paragrafo precedente saranno trattati e conservati per tutta la durata dell'eventuale rapporto instaurato. A decorrere dalla data di

cessazione di tale rapporto, per qualsivoglia ragione o causa, i dati saranno conservati per la durata dei termini prescrizionali applicabili ex lege o per il tempo necessario all'adempimento delle finalità di cui sopra.

Diritti esercitabili.

Di seguito Le indichiamo tutti i diritti che Le garantiamo sui Suoi dati personali.

In conformità a quanto previsto nel Capo III, Sezione I, GDPR, gli interessati potranno esercitare i diritti ivi indicati ed in particolare:

- **DIRITTO DI INFORMAZIONE:** Diritto di ricevere tutte le informazioni relative al trattamento in forma concisa, trasparente, intellegibile e facilmente accessibile (la presente informativa).
- **DIRITTO DI ACCESSO:** Ottenere conferma che sia o meno in corso un trattamento di dati personali che La riguardano e, in tal caso, ricevere informazioni relative, in particolare, a: finalità del trattamento, categorie di dati personali trattati e periodo di conservazione, destinatari cui questi possono essere comunicati (Art.15 GDPR),
- **DIRITTO DI RETTIFICA:** Ottenere la rettifica dei dati personali inesatti che La riguardano e l'integrazione dei dati personali incompleti (Art.16 GDPR) con relativo obbligo del titolare di comunicare tali modifiche.
- **DIRITTO ALLA CANCELLAZIONE (c.d. Oblio):** Diritto di richiedere la cancellazione dei propri dati quando è esaurita la finalità del trattamento, è stato revocato il consenso, è stata fatta opposizione al trattamento, i dati sono stati trattati in violazione di legge (Art.17 GDPR).
- **DIRITTO ALLA LIMITAZIONE:** Diritto di limitare il trattamento dei propri dati in caso di inesattezze, di contestazione o come misura alternativa alla cancellazione (Art. 18 GDPR).
- **DIRITTO ALLA PORTABILITÀ DEI DATI:** Ricevere i dati personali che La riguardano forniti al Titolare nonché trasferire i dati a un altro Titolare nei casi previsti dall'Art. 20 del GDPR.
- **DIRITTO DI OPPOSIZIONE:** Diritto di opporsi in qualsiasi momento al trattamento dei propri dati personali, salvo che sussistano motivi legittimi (Art. 21 GDPR).
- **DIRITTO DI PROPORRE RECLAMO ALL'AUTORITÀ DI CONTROLLO:** Garante per la protezione dei dati personali, Piazza di Montecitorio n. 121, 00186, Roma (RM).

Gli interessati potranno esercitare tali diritti (escluso l'ultimo) mediante il semplice invio di una richiesta via e-mail all'indirizzo del Titolare, sopra indicato.

3.2 Accordo in merito al Trattamento di dati personali gestiti dall'Applicazione web SQuadra disponibile via Internet.

(Ai sensi dell'art. 28 del Regolamento UE n. 679/2016)

TRA

_____ (P.IVA _____) Titolare del trattamento (d'ora in poi "TITOLARE") ai sensi del Regolamento europeo 679/2016 in materia di protezione delle persone fisiche con riguardo al trattamento dei dati personali (d'ora in poi "GDPR").

E

IL TIGLIO SRL (di seguito anche "RESPONSABILE").

PREMESSO CHE

- Il TITOLARE utilizza l'applicativo denominato SQuadra all'interno del quale può inserire dei dati personali. IL TIGLIO SRL offre l'Applicazione in modalità SaaS (Software as a Service – Software come servizio) come meglio specificato nell'Appendice "Informativa sul trattamento dei dati" del Manuale d'uso - di seguito, "Contratto di servizi").
- In virtù del Contratto di servizi il RESPONSABILE esegue operazioni di trattamento di dati personali di titolarità del TITOLARE, e riferiti unicamente ai dati necessari per l'erogazione dei servizi sopra indicati.
- Il RESPONSABILE dichiara e garantisce di possedere competenza e conoscenze tecniche in relazione alle finalità e modalità di trattamento, alle misure di sicurezza da adottare a garanzia della riservatezza, completezza ed integrità dei dati personali trattati, nonché in relazione alla normativa italiana ed europea in materia di protezione dei dati personali, e di possedere i requisiti di affidabilità idonei a garantire il rispetto delle disposizioni normative in materia.
- Sulla base delle referenze del RESPONSABILE, il TITOLARE ritiene l'idoneità e la qualificazione del RESPONSABILE atta a soddisfare, anche sotto il profilo della sicurezza del trattamento, i requisiti di cui alla normativa applicabile (artt. 28 e ss. del GDPR) e intende nominare lo stesso quale Responsabile del trattamento dei dati personali relativi al Contratto di servizi.

Tutto quanto sopra premesso le Parti convengono quanto segue:

1. Premesse

Le premesse costituiscono parte integrante ed essenziale del presente accordo.

2. Oggetto

Con la sottoscrizione del presente accordo il TITOLARE nomina IL TIGLIO SRL responsabile del trattamento in relazione alle operazioni di trattamento dati personali attuate ai soli fini dell'esecuzione del Contratto di servizi. Tale nomina non comporta il diritto ad alcuna remunerazione integrativa rispetto al corrispettivo pattuito contrattualmente.

I compiti assegnati al RESPONSABILE sono esclusivamente quelli resi necessari dalle attività connesse all'esecuzione del Contratto di servizi.

3. Trattamento dei dati personali previsto dal Contratto di servizi

Il RESPONSABILE, nello svolgimento delle attività necessarie alla conservazione dei dati ed al fine di permetterne il loro utilizzo (vedi "Contratto di servizi"), potrà venire a conoscenza, anche involontariamente, di alcuni dati personali.

4. Obblighi del Titolare del trattamento

Qualora, nell'ambito delle operazioni di trattamento dei dati personali, il TITOLARE ritenga necessario, al fine di adeguarsi alla normativa in materia di protezione dei dati, fornire istruzioni

aggiuntive in merito alle finalità, modalità e procedure per l'utilizzo e il trattamento dei dati personali le trasmetterà a IL TIGLIO SRL e dovrà concordare con esso le misure tecniche ed organizzative più idonee o valutare l'interruzione dell'utilizzo dell'Applicazione.

Il TITOLARE si obbliga a non inserire all'interno dell'Applicazione dati personali che, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, possono presentare un rischio elevato per i diritti e le libertà delle persone fisiche e quindi possano richiedere la valutazione di impatto sulla protezione dei dati (Art. 35 e 36 del GDPR).

Il TITOLARE assicurerà direttamente tutti i diritti degli interessati dei quali inserirà i dati personali sull'Applicazione (es.: obblighi di informativa, acquisizione del consenso e risposta alle richieste degli interessati in particolare: diritto all'accesso, rettifica, cancellazione, limitazione e portabilità).

5. Obblighi del Responsabile del trattamento

Ai fini di un corretto trattamento dei dati personali, il RESPONSABILE si impegna a:

Conformità

- Svolgere qualsiasi operazione di trattamento di dati personali in conformità ai principi e alla regolamentazione previsti dalla normativa vigente in materia di protezione dei dati personali.
- Trattare tutti i dati, direttamente o indirettamente, unicamente nei paesi UE o in quelli per i quali vige una decisione di adeguatezza.
- Eseguire fedelmente le eventuali istruzioni concordate con il TITOLARE, evitando attività di trattamento non conformi alle già menzionate istruzioni o volte a perseguire finalità diverse da quelle correlate all'esecuzione del Contratto di servizi.
- Adottare le misure di sicurezza previste dal successivo articolo del presente accordo.
- Garantire il pieno rispetto degli obblighi di cui il RESPONSABILE è tenuto in virtù della normativa vigente, ivi incluso a titolo esemplificativo, l'obbligo di tenuta del registro delle attività di trattamento svolte sotto la propria responsabilità ai sensi dell'art. 30 del GDPR.

Riservatezza

- Non effettuare copie dei Dati Personalni diverse da quelle strettamente necessarie alla corretta esecuzione del Contratto di servizi.
- Non divulgare o rendere noti a terzi i dati personali e adottare le misure organizzative e tecniche necessarie per assicurare la massima riservatezza dei dati personali acquisiti e utilizzati nello svolgimento delle attività oggetto della presente designazione.
- Mantenere il dovuto riserbo in ordine alle informazioni delle quali sia venuto a conoscenza nel corso dello svolgimento del Contratto di servizi anche dopo la conclusione dello stesso.

Autorizzati al trattamento

- Garantire che l'accesso ai dati personali da parte del personale (dipendenti e/o collaboratori) che opera sotto la responsabilità avvenga solo sulla base del principio di stretta necessità, provvedendo a individuare e designare, anche ai fini di cui all'art. 32 del GDPR, le persone fisiche autorizzate al trattamento dei dati personali per le suddette finalità, impegnando gli stessi con idonei vincoli di riservatezza.
- Formare adeguatamente il personale addetto all'esecuzione del Contratto di servizi rendendoli edotti delle disposizioni del GDPR, fornendo loro istruzioni precise e vigilando sulla loro osservanza.

Informazioni al TITOLARE

- Informare il TITOLARE, attraverso specifici AVVISI presentati al primo utilizzo di SQuadra, di qualsiasi violazione o rischio di violazione concernente i dati personali di cui il RESPONSABILE è venuto a conoscenza nello svolgimento dei Contratto di servizi, senza ingiustificato ritardo e comunque entro 48 ore dal momento in cui ne è venuto a conoscenza, e attuare qualsiasi

- misura che si renda strettamente necessaria al fine di porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.
- Tenere informato il TITOLARE, tramite la specifica Appendice del Manuale di SQuadra, riguardo alle operazioni di trattamento, con particolare riguardo, ma non esclusivamente, alle misure di sicurezza adottate, alla conformità con la normativa nonché riguardo a qualsiasi circostanza o criticità eventualmente riscontrata.

6. Sub Responsabili

Il RESPONSABILE potrà ricorrere a un altro responsabile del trattamento per l'esecuzione di specifiche attività di trattamento per conto del TITOLARE, su tale altro responsabile del trattamento saranno imposti, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, gli stessi obblighi in materia di protezione dei dati contenuti nel presente accordo, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del GDPR.

L'elenco degli eventuali altri responsabili che potranno avere accesso ai dati personali contenuti nell'Applicazione è disponibile nel Manuale Utente di SQuadra.

7. Durata

L'efficacia del presente accordo decorre dalla data di sottoscrizione dello stesso ad opera di entrambe le PARTI sino alla cessazione, per qualsiasi causa intervenuta, del Contratto di servizi.

All'atto della cessazione del Contratto di servizi il RESPONSABILE potrà procedere a cancellare tutti i dati inseriti dal TITOLARE in caso di esplicita richiesta del TITOLARE e a fronte di apposito contratto.

8. Misure di Sicurezza

Con riferimento alle operazioni di trattamento dei dati personali necessarie ai fini della esecuzione del Contratto di servizi, il RESPONSABILE dichiara e garantisce:

- Di mantenere, ogni e qualsiasi misura di sicurezza idonea a prevenire i rischi di distruzione, perdita, anche accidentale, dei dati personali nonché di accesso non autorizzato o trattamento illecito dei medesimi come previsto nel Contratto di servizi.
- Che tali misure tecniche ed organizzative siano tali da garantire un livello di sicurezza adeguato al rischio come previsto dall'art. 32 del GDPR, nonché ogni altro obbligo di legge.

Il RESPONSABILE si impegna a verificare regolarmente l'idoneità delle misure adottate ed a tenere informato il Titolare come indicato al precedente nell'ultimo capoverso degli "Obblighi del Responsabile del trattamento".

9. Responsabilità

In funzione dei dati trattati da SQuadra non si ritiene possano derivare danni per IL TITOLARE che dovrà interrompere l'utilizzo di SQuadra ed eventualmente cancellare i dati inseriti qualora valuti non adeguate le misure di sicurezza predisposte da IL TIGLIO SRL.

IL TIGLIO potrà essere chiamato a risarcire, in caso di inadempienza, al massimo l'importo incassato direttamente dal TITOLARE nell'ultimo anno.

Data: _____ Per il TITOLARE: _____

IL TIGLIO SRL, preso atto di quanto previsto nel presente accordo e della normativa vigente, dichiara di accettare la nomina a Responsabile esterno del trattamento.

Per IL TIGLIO SRL:

4 APPENDICE: Informativa sul trattamento dei dati inseriti dagli Utenti.

4.1 Premessa

Nell'esercizio della propria attività d'impresa IL TIGLIO SRL riserva massima attenzione alla protezione ed alla tutela dei dati personali di tutti coloro che con essa operano o interagiscono, adottando a tal fine ogni idonea, adeguata e necessaria procedura e sistema di sicurezza.

Credendo fermamente nei principi di trasparenza e correttezza, la presente informativa viene pertanto resa allo scopo di fornire a tutti i soggetti interessati una descrizione completa circa le modalità e le finalità del trattamento dei dati personali che viene effettuata da IL TIGLIO SRL nella erogazione dei servizi (di seguito "Servizi SQuadra"), e ciò anche in conformità a quanto previsto dal Regolamento (UE) n. 2016/679 in tema di protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (di seguito per brevità "GDPR").

La presente informativa privacy viene rilasciata a completa ed integrale sostituzione di ogni altra regolamentazione eventualmente prima d'oggi esistente in tema di protezione dei dati personali trattati da IL TIGLIO SRL per le medesime finalità qui contenute.

4.2 Informazioni generali

4.2.1 Origine dei dati e responsabilità

4.2.1.1 Fonte da cui hanno origine i dati personali

I dati personali oggetto della presente informativa riguardano i dati inseriti su SQuadra dagli utilizzatori del programma SQuadra (d'ora in poi "Utenti") e trattati da IL TIGLIO SRL per la gestione del rapporto le finalità contenute nella presente informativa quale Responsabile Esterno.

Ogni Utente può utilizzare SQuadra unicamente utilizzando le credenziali d'accesso fornite. L'Utente dovrà modificare la Prima Password fornita dal Sistema e non dovrà comunicarla ad altri.

È opportuno che le credenziali d'accesso siano personali. Gli Utenti amministratori possono generare credenziali da assegnare ad altri utenti o richiederle a IL TIGLIO SRL.

4.2.1.2 Esclusione della contitolarità del trattamento.

È espressamente esclusa l'instaurazione tra IL TIGLIO SRL e gli Utenti di un rapporto di contitolarità del trattamento dei dati ai sensi dell'articolo 26 del GDPR.

Le finalità ed i mezzi del trattamento dei dati personali oggetto della presente informativa non sono stati infatti determinati congiuntamente da IL TIGLIO SRL e dall'Utente agendo ciascuno di essi con ruoli (e quindi eseguendo attività) differenti tra loro.

4.2.1.3 Responsabile esterno del trattamento dei dati,

Responsabile Esterno del trattamento dei dati personali è IL TIGLIO SRL, con sede in Viale della Repubblica 141, 59100 Prato, nella persona del suo rappresentante pro tempore Giuliano Marullo contattabile all'indirizzo e-mail g.marullo@iltigliosrl.it.

4.2.2 Dati personali

4.2.2.1 Definizione

Per dati personali si intendono tutte le informazioni riguardanti una persona fisica, identificata oppure identificabile tramite riferimento ad elementi quali ad esempio il nome, gli estremi del documento d'identità, l'identità fisica, fisiologica, genetica, economica, culturale o sociale di tale persona, nonché tramite gli estremi identificativi sulla sua ubicazione.

I dati personali come sopra descritti vengono trattati da IL TIGLIO SRL unicamente quando l'Utente, nell'ambito di un Trattamento di cui lo stesso è Titolare o Responsabile, li inserisce all'interno di SQuadra.

4.2.2.2 Tipologia e categoria dei dati trattati

All'interno di SQuadra, vengono normalmente memorizzati solamente dati personali che riguardano informazioni di carattere identificativo come nome, cognome, data e luogo di nascita, luogo di residenza, codice fiscale, partita iva e sede, numero di telefono, indirizzo e-mail, username, password, sesso, ecc.

Non si ritiene che gli Utenti inseriscano all'interno di SQuadra categorie particolari di dati personali quali ad esempio i dati che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

Qualora un Utente intenda inserire su SQuadra categorie particolari di dati personali o dati aziendali particolarmente riservati, la cui natura richiede particolari misure di sicurezza, dovrà informare IL TIGLIO SRL ed eventualmente concordare, tramite specifico contratto, le misure di sicurezza aggiuntive da applicare.

4.2.3 Caratteristiche dei trattamenti

4.2.3.1 Finalità e modalità del trattamento dei dati

Il trattamento dei dati personali ad opera di IL TIGLIO SRL avviene solo ed esclusivamente per le seguenti finalità:

- Permettere il normale funzionamento di SQuadra.
- Garantire la disponibilità dei dati di SQuadra.
- Offrire assistenza sull'utilizzo di SQuadra.
- Rispondere ad una richiesta o ad un reclamo.
- Risolvere eventuali anomalie di SQuadra.
- Eseguire test.
- Migliorare le funzionalità di SQuadra.
- Eseguire controlli e applicare le politiche IL TIGLIO SRL per prevenire, rilevare, mitigare e/o accertare violazioni della sicurezza e/o attività anche solo potenzialmente vietate, illegali e/o illecite.

Non verranno effettuate attività di marketing tramite telefonate, e-mail, SMS o via posta cartacea.

I dati presenti su SQuadra verranno trattati solo in formato digitale.

4.2.3.2 Obblighi de IL TIGLIO SRL

Il TIGLIO SRL si impegna a:

- Trattare i dati personali soltanto seguendo le indicazioni presenti in questa Informativa.
- Garantire di aver redatto, predisposto ed attivato quanto necessario per essere conforme al GDPR.
- Assicurare che solo il personale debitamente autorizzato da IL TIGLIO SRL (e sotto la responsabilità di IL TIGLIO SRL) potrà accedere ai dati personali inseriti su SQuadra.

- Garantire che le persone autorizzate al trattamento dei dati personali (incaricati) si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza.
- Fornire, nel presente Manuale d'uso, indicazioni sulle misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato (in particolare: diritto all'accesso, rettifica, cancellazione, limitazione e portabilità).
- Informare gli Utenti, in caso di violazione dei dati personali che possa comportare rischi per i diritti e le libertà degli interessati, senza ingiustificato ritardo e comunque entro 24 ore dal momento in cui è venuto a conoscenza della violazione.

4.2.3.3 Base giuridica del trattamento dei dati

IL TIGLIO SRL tratta i dati personali per adempiere ad un obbligo relativo ad un contratto o una convenzione e, in misura strettamente necessaria e proporzionata, per garantire la sicurezza delle reti e dell'informazione per tale intendendosi la capacità di una rete o di un sistema d'informazione di resistere, a un dato livello di sicurezza, a eventi imprevisti o ad atti illeciti o dolosi che compromettano la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati personali conservati o trasmessi e la sicurezza dei relativi servizi offerti o resi accessibili tramite tali reti.

4.2.3.4 Dati personali di soggetti terzi forniti dall'Utente

Ogni qual volta l'Utente intenda inserire su SQuadra dati personali - ivi compresi quelli facenti parte delle categorie particolari di dati personali - diversi da quelli suoi propri e quindi dati personali di soggetti terzi (di seguito per brevità **“Terze Parti”**) con i quali IL TIGLIO SRL non ha rapporti contrattuali pendenti ed ai quali non potrà quindi rivolgersi, l'Utente dovrà preventivamente informare le Terze Parti sulla destinazione dei loro dati personali (di seguito per brevità **“Dati di Terze Parti”**) nonché sulle modalità tramite le quali IL TIGLIO SRL tratterà detti dati in conformità a quanto previsto nella presente informativa¹⁶.

IL TIGLIO SRL potrà trattare Dati di Terze parti qualora venga richiesto di erogare all'Utente servizi di assistenza, aggiornamento e manutenzione e questo potrebbero determinare (ancorché occasionalmente) l'accesso ai Dati di Terze Parti.

Nei suddetti casi IL TIGLIO SRL eseguirà il trattamento dei Dati di Terze Parti non in qualità di titolare ma come responsabile o sub-responsabile del trattamento ai sensi e per gli effetti dell'articolo 28 del GDPR.

Conformemente alla normativa vigente, non avendo IL TIGLIO SRL alcun rapporto e/o potere decisionale con le Terze Parti, rimarrà esclusivamente in capo all'Utente, l'obbligo di adempiere a tutte le prestazioni e/o in genere alle prescrizioni previste dalla medesima normativa nei riguardi delle Terze Parti, avendo altresì cura l'Utente di informare adeguatamente le Terze Parti di tutti gli elementi idonei affinché quest'ultimo possa sempre avere integrale e chiara consapevolezza dell'attività svolta da IL TIGLIO SRL in qualità di responsabile e/o sub-responsabile del trattamento dei Dati di Terze Parti.

Una volta fornite tali informazioni, l'Utente dovrà altresì ottenere dalle Terze Parti il consenso al trattamento e/o al trasferimento dei Dati di Terze Parti presso IL TIGLIO SRL se la liceità del trattamento si basa sul consenso.

¹⁶ Fra i Documenti di Supporto (sotto Varie) è presente un esempio di informativa.

4.2.3.5 Modalità di condivisione delle informazioni con terze parti

I dati personali inseriti su SQuadra potranno essere condivisi con soggetti terzi solamente nei casi che seguono:

- Trattamento da parte di entità esterne (es. fornitori di tecnologie informatiche) che opereranno sui dati secondo le istruzioni fornite da IL TIGLIO SRL medesima.
- Esigenze di giustizia, legali e/o in genere di tutela per le quali IL TIGLIO SRL potrebbe conservare o divulgare i dati personali laddove necessario per soddisfare esigenze di giustizia ad esempio perché richiesti da un'Autorità amministrativa, un'Autorità di controllo e/o vigilanza ovvero nell'ambito di un procedimento giudiziario o, comunque, in ottemperanza a disposizioni di legge, o comunque per l'esercizio di diritti legali o per la difesa contro denunce e/o azioni legali oppure per prevenire, individuare o indagare su attività illegali, frodi, abusi, violazioni delle posizioni giuridiche soggettive de IL TIGLIO SRL o laddove vi siano minacce anche solo potenziali alla sicurezza dei Servizi IL TIGLIO SRL o alla sicurezza fisica di qualsiasi persona.
- Uso di Data Center dove IL TIGLIO SRL tratterà e conserverà i dati personali raccolti nei server di cui dispone.

4.2.3.6 Principi generali

Non è previsto il trasferimento all'estero dei dati nei paesi extra-UE.

I dati personali degli interessati non saranno oggetto di diffusione da parte de IL TIGLIO SRL.

SQuadra non effettua processi decisionali automatizzati.

Ogni Utente deve cancellare i dati personali inseriti o renderli non riconducibili a persone fisiche quando vuole interrompere il trattamento.

I dati personali inseriti su SQuadra verranno conservati fino ad esplicita richiesta di cancellazione formulata dall'Utente a seguito della quale dovrà essere stipulato un contratto con IL TIGLIO SRL per la rimozione in modo sicuro dei dati personali.

Dal momento della disattivazione delle credenziali i dati della singola azienda non potranno più essere trattati (se non per copie di backup) e potranno essere cancellati da IL TIGLIO SRL.

Rimane altresì salvo il caso in cui la maggior (o minore) conservazione dei dati debba essere effettuata per soddisfare esigenze di giustizia ad esempio per ottemperare ad una richiesta dell'autorità amministrativa, autorità di controllo e/o di vigilanza ovvero per l'esercizio e/o per la tutela (in via giudiziale e/o stragiudiziale) dei propri diritti o per esercitare la difesa contro denunce e/o azioni legali.

4.2.3.7 I diritti dell'interessato

Ogni azienda ha il dovere di informare tutti gli interessati a cui sono riferibili i dati personali trattati da IL TIGLIO SRL del fatto che, in ogni momento potranno esercitare i propri diritti nei confronti del Titolare del trattamento dei dati aziendali.

In particolare, ad ogni interessato, conformemente e nei termini e modalità previsti dal GDPR, può esercitare i diritti di seguito descritti.

- Diritto di informazione, accesso, rettifica e cancellazione dei dati, limitazione ed opposizione all'uso dei dati e diritto di revoca del consenso. Questi diritti dovranno essere curati dagli Utenti tramite le normali funzionalità di SQuadra.
- Diritto alla portabilità. L'Utente potrà dare esecuzione a questo diritto tramite le esportazioni in formato excel o word presenti su SQuadra.
- Diritto di proporre reclamo. L'Interessato avrà sempre diritto di proporre reclamo alla competente Autorità di controllo laddove ravvisi problematiche afferenti all'utilizzo dei propri dati personali da parte dell'Utente.

- Processo decisionale automatizzato. SQuadra non utilizza tecnologie automatizzate per l'assunzione di decisioni o la profilazione.

Se l'Interessato avrà bisogno di assistenza in merito ai propri diritti, dovrà contattare l'Utente che ha inserito i suoi dati su SQuadra.

4.2.3.8 Misure di sicurezza

IL TIGLIO SRL garantisce la messa in atto ed il mantenimento di misure tecniche ed organizzative idonee per garantire un livello di sicurezza adeguato, effettuando altresì costantemente una serie di controlli tecnici, amministrativi e fisici per mantenere riservati e sicuri i dati personali dell'Interessato (si veda l'Appendice: SGSI de IL TIGLIO SRL).

5 APPENDICE: SGSI de IL TIGLIO SRL

5.1 Introduzione

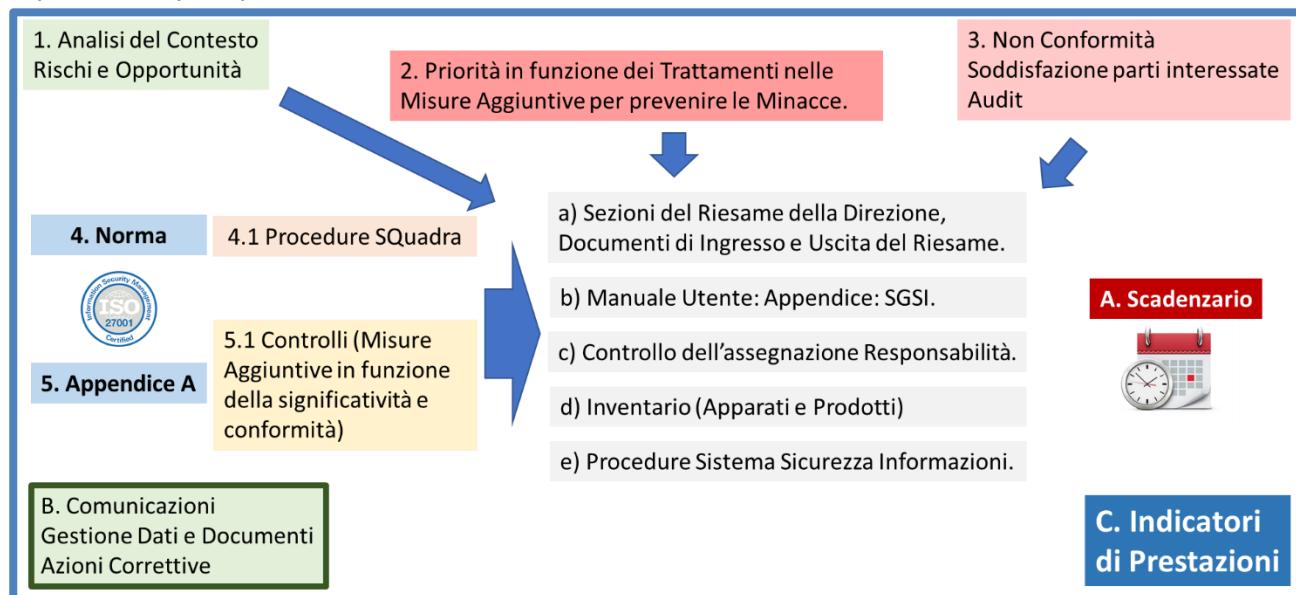


Obiettivo della presente Appendice è quello di informare tutti gli Utenti di SQuadra sull'organizzazione che IL TIGLIO SRL si è dato per garantire la sicurezza delle informazioni.

Per maggiore garanzia degli Utenti IL TIGLIO SRL ha richiesto ed ottenuto nel febbraio 2019 la Certificazione secondo la norma internazionale UNI CEI EN ISO/IEC 27001:2013 per "Fornitura del software applicativo 'SQuadra' in modalità SaaS¹⁷ (Software as a Service) e gestione delle relative informazioni".

5.1.1 Utilizzo di SQuadra

IL TIGLIO SRL ha scelto di utilizzare le varie funzionalità di SQuadra per la gestione del SGSI. Di seguito riportiamo le principali funzionalità utilizzate.



1. Il Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) è progettato e gestito partendo dalla **Analisi del Contesto** [SG / Analisi / Riesami] dal quale sono stati individuati **Rischi ed Opportunità**.

¹⁷ Software come servizio, è un modello di distribuzione del software applicativo dove un produttore di software sviluppa, opera (direttamente o tramite terze parti) e gestisce un'applicazione web che mette a disposizione dei propri clienti via Internet (cloud computing).

2. Sono quindi stati analizzati tutti i **Trattamenti** aziendali [Privacy / Trattamenti] per individuare la Criticità aziendale delle tre dimensioni (Riservatezza, Integrità e Disponibilità). Parallelamente sono state individuate tutte le **Minacce** [Privacy / Analisi del Sistema / Minacce] e valutato il Rischio in funzione della Gravità e della Probabilità [Privacy / Sistema Informativo / SGSI / Report SGSI]. È quindi possibile individuare la priorità per le varie Azioni Aggiuntive previste.

3. Vengono analizzate le **Non Conformità** [SG / Miglioramento / NC], la **Soddisfazione delle Parti Interessate** [SG / Valutazione / Soddisfazione parti interessate] ed i risultati degli **Audit Interni** [SG / Valutazioni / Audit].

4. È stata presa come base di riferimento la **Norma Internazionale 27001** per ogni punto della quale è stata definita una o più micro **Procedure** (CHI, COSA, DOVE e QUANDO) [Manutenzione / Personalizza / Procedure].

5. La Norma 27001 fornisce una **Appendice A** nella quale sono descritti 114 Controlli. Per ogni **Controllo** è stata individuata [Privacy / Analisi del Sistema / Controlli] la Significatività aziendale e la Conformità stimata. Sono quindi state previste delle Misure Aggiuntive.

Tutti questi elementi vengono analizzati per:

- a) Descrivere gli elementi da trattare nelle varie **Sezioni del Riesame della Direzione** [SG / Analisi / Riesami] e raccolti in **Documenti di Ingresso e Uscita**.
- b) Inserire le informazioni che possono interessare gli Stakeholder direttamente nel **Manuale Utente** di SQuadra nell'Appendice SGSI.
- c) Individuare e gestire [Privacy / Sistema Informativo / Responsabili] le **Responsabilità** da assegnare.
- d) Tenere sempre aggiornato l'**Inventario** [Privacy / Sistema Informativo / Inventario / Apparati e Prodotti].
- e) Definire le **Procedure del SGSI**.

A. In base a tutte le informazioni inserite è possibile tenere sempre sotto controllo lo **Scadenziario** [Privacy / Sistema Informativo / Sistema Informativo / Scadenze per Responsabile] in cui, per ogni Responsabile sono indicate le attività previste con le relative tempistiche.

B. Per la Gestione del SGSI vengono utilizzate le normali funzionalità (le modalità di **Comunicazioni** [SG / Supporto / Comunicazione], la **Gestione dei Dati e dei Documenti** [SG / Varie / Documenti], le **Azioni Correttive** [SG / Miglioramento / AC], ecc.).

C. Tutto il Sistema è controllato in base agli **Indicatori di Prestazioni** [SG / Valutazione / Indicatori di Prestazione].

5.2 Politica (Rev. 1.a)

IL TIGLIO SRL è consapevole che oggi viviamo in una società basata sulla conoscenza, in cui le informazioni sono un patrimonio prezioso. Le informazioni, sia relative a dati personali che ai dati aziendali, in qualsiasi forma devono essere protette adeguatamente da tutte le minacce e le vulnerabilità, siano esse interne o esterne, intenzionali o accidentali. In particolare, devono essere assicurate la riservatezza, l'integrità e la disponibilità delle informazioni, nella misura richiesta dall'attività aziendale.

Il Regolamento Europeo [2016/679] relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (d'ora in poi GDPR)

individua i principi applicabili al trattamento dei dati (Art. 5) e obbliga Il Tiglio srl a mettere in atto misure tecniche e organizzative adeguate a garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al regolamento (Art. 24).

IL TIGLIO SRL, in funzione dei servizi offerti, deve rispondere a legittime aspettative degli utilizzatori relativamente alla sicurezza delle informazioni.

IL TIGLIO SRL, consapevole che il proprio sistema informativo è un patrimonio aziendale, ha predisposto ed approvato la seguente Politica in merito alla Sicurezza delle Informazioni. L'attuazione di tale Politica prevede una adeguata valutazione dei rischi per individuare le minacce di eventi che impattano negativamente sulla sicurezza delle informazioni, la loro gravità e la probabilità di accadimento.

Tale Politica è stata divulgata a tutte le strutture organizzative interne ed esterne coinvolte nella gestione del Sistema Informativo.

La Politica si basa sull'analisi del contesto sulla base di fattori interni quali:

- Le strategie aziendali attuali e future e le relative priorità.
- Il livello di innovazione, attuale e prevista, per la Società.
- La struttura organizzativa per i sistemi informativi, inclusi i fornitori principali e i processi affidati all'esterno (in outsourcing o esternalizzati).
- Le caratteristiche delle sedi dei locali dove sono trattate le informazioni e dove sono collocati gli archivi e i sistemi informatici, inclusi quelli presso fornitori o altre parti esterne.
- Le tipologie delle informazioni trattate ed il relativo livello di protezione voluto.
- I rapporti con il personale interno ed esterno e le loro competenze informatiche.
- Le aspettative delle parti interne interessate (stakeholder), ossia del personale, degli azionisti e dei soci; tra queste aspettative vi è il rispetto dei contratti e degli accordi e la buona qualità dell'ambiente di lavoro.
- L'evoluzione della tecnologia.
- La normativa applicabile.
- I concorrenti ed i potenziali concorrenti.
- Le strategie di mercato, attuali e previste, dei fornitori e dei clienti attuali e potenziali.
- Le aspettative delle parti esterne interessate, tra cui i clienti ed i fornitori attuali e potenziali.

IL TIGLIO SRL, per questi motivi, ha definito i seguenti obiettivi:

- Istituire e condurre un Sistema di Gestione della Sicurezza delle Informazioni [SGSI] che sia:
 - Adeguato alle caratteristiche organizzative della Società ed alle necessità degli utenti.
 - Sostenibile dal punto di vista organizzativo e finanziario.
 - Conforme alle normative ed ai regolamenti vigenti.
 - In grado di assicurare la pianificazione ed il pieno controllo di tutte le attività.
- Individuare e adottare una metodologia per definire, classificare ed analizzare obiettivi, opportunità e rischi.
- Definire una struttura organizzativa che permetta di individuare responsabilità gestionali specifiche per la gestione della sicurezza delle informazioni.
- Divulgare in forma adeguata, accessibile e comprensibile ai collaboratori ed alle terze parti interessate, le direttive e le procedure di sicurezza.
- Assicurare il costante allineamento del sistema di gestione alla evoluzione tecnologica.

- Certificare e mantenere presso un Ente terzo la conformità e l'efficacia del Sistema di Gestione.
- Supporto organizzativo, finanziario e operativo da parte della Direzione per il raggiungimento degli obiettivi definiti e perseguire il miglioramento continuo del Sistema di gestione della sicurezza delle informazioni.

L'adozione di un SGSI dovrebbe garantire, con ragionevole sicurezza, gli obiettivi di sicurezza. In particolar modo i benefici che ci si aspetta di ottenere dall'implementazione del SGSI sono i seguenti:

- Prevenire incidenti relativi alla sicurezza delle informazioni.
- Rendere sistematica la gestione della sicurezza informatica.
- Individuare le cause di inefficacia dei processi di gestione.
- Determinare le conseguenze dei requisiti normativi e contrattuali.
- Comunicare ai clienti gli sforzi per l'aumento consapevole della sicurezza delle informazioni.
- Diffondere la cultura della sicurezza delle informazioni presso gli utilizzatori dei servizi.
- Gestire un sistema di registrazione di non conformità, reclami, incidenti e quasi incidenti e di monitoraggio degli stessi e dei costi connessi.
- Prevenire danni anche di immagine provenienti da incidenti sulla gestione della sicurezza delle informazioni.

IL TIGLIO SRL si impegna ad informare, con almeno 6 mesi di anticipo, tutti gli utenti in caso di cessazione del servizio per permettere di stampare tutti i dati fino ad allora inseriti tramite le normali stampe.

Politiche di dettaglio

La presente Politica è sostenuta da specifiche politiche di dettaglio.

Controllo degli accessi

Tutte le risorse informatiche devono essere protette dai rischi di accesso non autorizzato. A tal fine ogni utente deve essere dotato di adeguati e sicuri elementi identificativi univoci. I meccanismi di sicurezza per accessi devono essere proporzionati ai potenziali rischi connessi con i diritti dell'utente. Ogni utente deve avere unicamente i diritti necessari allo svolgimento delle attività di sua competenza.

I diritti di accesso devono essere riesaminati periodicamente ed eventuali credenziali rilasciate a personale che ha modificato i diritti (es. interruzione del rapporto di collaborazione) devono essere immediatamente disattivate.

Devono essere implementati opportuni controlli atti a garantire un accesso sicuro ai servizi internet.

I sistemi devono essere configurati in modo da prevedere la chiusura automatica della sessione lavorativa dopo un periodo predefinito di inattività.

Backup

Deve essere definito quali dati salvare, le varie metodologie utilizzate e il numero di versioni da mantenere. L'esito delle operazioni di backup deve essere monitorato. Devono essere descritte le metodologie per il ripristino dei dati.

Anti-malware

Misure di sicurezza per la prevenzione e la protezione da malware devono essere applicate a tutti i sistemi che costituiscono l'infrastruttura informatica aziendale. Tutto il software installato sui sistemi informativi deve essere conforme ai brevetti e/o ai termini delle licenze e costantemente

aggiornato a fronte della rilevazione di criticità. I firewall devono essere configurati per impedire traffico non autorizzato verso i sistemi aziendali.

Classificazione delle informazioni

In funzione delle caratteristiche dei dati gestiti tutte le informazioni vengono considerate ai massimi livelli per quanto riguarda disponibilità, integrità e riservatezza.

Privacy e protezione dei dati personali

Gli utenti sono sensibilizzati alla corretta gestione della Privacy relativamente ai dati da loro inseriti tramite l'apposita appendice del manuale utente.

Obiettivi rivolti ai clienti ed utenti

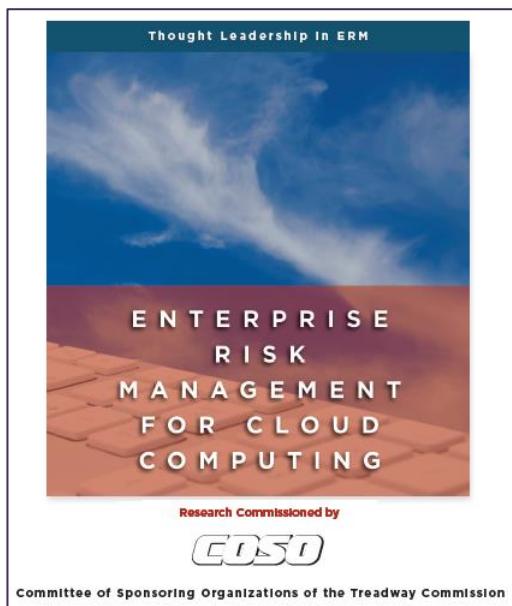
I principali obiettivi che IL TIGLIO SRL si pone nell'attuazione del proprio Sistema per la Gestione della Sicurezza delle Informazioni sono:

- Assicurare la continuità del servizio: Ore di non funzionamento [in orario lavorativo (9-13 e 15-19 dei giorni lavorativi) per interruzioni superiori ai 5 minuti] inferiori alle 8 ore/anno.
- Assicurare l'utilizzo di dati sempre aggiornati: Ore di inserimento da ripetere per recupero dei dati da Backup precedenti inferiori a 8 ore/anno.
- Assicurare la qualità di SQuadra: Numero di anomalie registrate nell'area Segnalazioni di SQuadra relative ad errori del programma inferiori a 3/anno.

Nella figura seguente viene evidenziato come gli obiettivi rivolti ai clienti ed utenti sono correlati con gli obiettivi interni (Rosso = Alta. Verde = Bassa).

	Utilizzo di Cloud certificati 27001	Immagini e Backup frequenti	Ambiente operativo stabile	Controllo sulle funzioni che accedono ai dati
Assicurare la continuità del servizio: <i>Ore di non funzionamento [in orario lavorativo (9-13 e 15-19 dei giorni lavorativi) per interruzioni superiori ai 5 minuti] inferiori alle 8 ore/anno.</i>				
Assicurare l'utilizzo di dati sempre aggiornati: <i>Ore di inserimento da ripetere per recupero dei dati da Backup precedenti inferiori a 8 ore/anno.</i>				
Assicurare la qualità di SQuadra: <i>Numero di anomalie registrate nell'area Segnalazioni di SQuadra relative ad errori del programma inferiori a 3/anno.</i>				

5.3 Servizi Cloud



"Enterprise Risk Management per il Cloud Computing" è una pubblicazione del Committee of Sponsoring Organization of the Treadway Commission¹⁸ (CoSO) che mira a sfruttare i principi dell'*Enterprise Risk Management - Integrated Framework* di CoSO al fine di fornire linee guida che identifichino sinteticamente i rischi e l'impatto che il cloud computing può avere su un'organizzazione.

In particolare, individua le opportunità ed i rischi connessi con l'utilizzo del cloud computing. Di seguito riportiamo, per ogni elemento, le valutazioni per IL TIGLIO SRL in quanto Cliente di Servizi Cloud e l'attenzione che IL TIGLIO SRL ha per gli Utenti (in quanto Fornitore di servizi Cloud).

Le Opportunità

Risparmio sui costi

I clienti cloud pagano solo le risorse informatiche che utilizzano piuttosto che acquistare o noleggiare apparecchiature che potrebbero non essere utilizzate completamente in ogni momento. Se il cloud computing viene utilizzato per soddisfare tutte le esigenze tecnologiche di un'organizzazione, non ci sono più requisiti di spazio fisico e costi dei servizi tradizionalmente associati al mantenimento di un data center dedicato. Un'organizzazione che ottiene tutte le sue risorse informatiche da un fornitore di servizi cloud può mettere direttamente a costo la spesa (con beneficio fiscale rispetto all'esecuzione di investimenti da ammortizzare).

IL TIGLIO SRL come cliente di servizi Cloud	IL TIGLIO SRL come fornitore di servizi Cloud
ILTIGLIO SRL si appoggia totalmente a servizi Cloud sfruttando al massimo l'opportunità offerta.	Gli Utenti possono sfruttare queste opportunità relativamente ai servizi gestiti con Squadra.

Velocità di implementazione, Scalabilità e aggiornamento

I fornitori di servizi cloud possono soddisfare l'esigenza di elaborazione e archiviazione dati quasi istantaneamente.

Un'organizzazione può scalare far crescere o diminuire la sua capacità da un server a centinaia di server senza spese in conto capitale. Questa capacità consente a un'organizzazione di ottenere grandi quantità di risorse informatiche per l'esecuzione di attività di calcolo ad alta intensità temporanea, quando necessario, senza investire in capacità di calcolo in eccesso per far fronte a periodi di domanda elevata e poco frequenti.

Possedere e gestire una funzione IT è costoso e richiede molto tempo. Il cloud computing consente a un'organizzazione di concentrarsi più tempo sullo scopo e gli obiettivi principali. La maggior parte delle offerte di servizi cloud si basano su una base tecnologica standardizzata e pre-costruita che

¹⁸ Vedi l'Appendice dedicata.

facilita un migliore supporto. Questa base facilita anche i aggiornamenti tecnologici più coerenti e l'adempimento rapido delle richieste di risorse IT.

IL TIGLIO SRL come cliente di servizi Cloud	IL TIGLIO SRL come fornitore di servizi Cloud
IL TIGLIO SRL monitora costantemente le prestazioni dei servizi offerti e modifica le richieste al proprio fornitore di servizi. IL TIGLIO SRL concentra la propria attenzione alla corretta configurazione ed alle misure per garantire la sicurezza delle informazioni.	Gli Utenti possono utilizzare le varie funzionalità di SQuadra dal momento che ottengono le credenziali senza la necessità di nessuna risorsa IT interna.

Benefici ambientali

Se ogni organizzazione dovesse sostituire il proprio data center privato con il cloud computing, il risultato sarebbe una significativa riduzione del consumo energetico complessivo, delle emissioni di carbonio e dell'uso fisico del territorio.

I Rischi

Forza dirompente

Facilitare l'innovazione (con maggiore velocità) e gli aspetti di risparmio sui costi del cloud computing possono essere considerati essi stessi come eventi a rischio per alcune organizzazioni. Abbassando le barriere di accesso per i nuovi concorrenti, il cloud computing potrebbe minacciare o perturbare alcuni modelli di business, rendendoli addirittura obsoleti in futuro.

I concorrenti esistenti che abbracciano completamente il cloud potrebbero essere in grado di portare più rapidamente nuove idee e innovazione nei loro mercati. Poiché le soluzioni di cloud computing consentono notevoli risparmi sui costi a breve termine grazie alla riduzione delle spese in conto capitale, un'organizzazione che adotta il cloud potrebbe essere in grado di ottenere margini migliori rispetto ai suoi concorrenti non cloud. Così, quando un'organizzazione di un settore adotta soluzioni cloud, altre organizzazioni del settore potrebbero essere costrette a seguire l'esempio e adottare il cloud computing.

IL TIGLIO SRL come cliente di servizi Cloud	IL TIGLIO SRL come fornitore di servizi Cloud
IL TIGLIO SRL offre ai propri clienti soluzioni Cloud dal 2008 avendo scelto di utilizzare a sua volta i servizi Cloud forniti dai principali fornitori nazionali ed internazionali.	Gli Utenti utilizzando SQuadra possono sfruttare le potenzialità del Cloud.

Responsabilità – Rischio di attacchi mirati

Quando un'organizzazione adotta soluzioni cloud gestite da terze parti, vengono create nuove relazioni di dipendenza con il fornitore per quanto riguarda la responsabilità legale, l'universo del rischio, l'escalation degli incidenti, la risposta agli incidenti e altre aree. Le azioni del fornitore dei servizi Cloud e degli altri utilizzatori del cloud possono avere un impatto sull'organizzazione in vari modi. Considerare quanto segue:

- Dal punto di vista legale, i fornitori di servizi cloud e le organizzazioni clienti sono imprese distinte. Tuttavia, se il fornitore di servizi Cloud trascurasse o fallisse nelle sue responsabilità, potrebbe avere implicazioni di responsabilità legale per le organizzazioni di clienti. Ma se un'organizzazione cliente fallisce nelle sue responsabilità, è meno probabile che vi siano implicazioni legali per il fornitore di servizi Cloud.
- I fornitori di servizi Cloud e le organizzazioni loro clienti avranno probabilmente programmi separati di gestione del rischio aziendale (ERM) per affrontare il rispettivo universo di rischi

percepiti. L'universo dei rischi di un'organizzazione che utilizza il cloud computing è una combinazione di rischi che la singola organizzazione deve affrontare insieme a un sottoinsieme dei rischi che il suo fornitore di servizi Cloud dovrebbe affrontare.

Il consolidamento di più organizzazioni che operano sull'infrastruttura di un CSP rappresenta un obiettivo più attraente di una singola organizzazione, aumentando così la probabilità di attacchi mirati. Di conseguenza, nella maggior parte dei casi i livelli di rischio intrinseco di una soluzione Cloud sono più elevati per quanto riguarda la riservatezza e l'integrità dei dati.

Un servizio Cloud nel quale molte organizzazioni utente condividono risorse presenta un rischio di perdita di dati che non esiste quando i server e le risorse dedicate sono utilizzate esclusivamente da un'organizzazione.

IL TIGLIO SRL come cliente di servizi Cloud	IL TIGLIO SRL come fornitore di servizi Cloud
IL TIGLIO SRL ha deciso di utilizzare unicamente fornitori di servizi Cloud certificati per la sicurezza delle informazioni secondo la Norma internazionale 27001.	IL TIGLIO SRL offre ai propri clienti la garanzia che le misure messe in atto per la sicurezza dei dati sono conformi alla Norma 27001 avendo scelto di certificare la fornitura dei servizi offerti.

Mancanza di trasparenza - Problemi di sicurezza e conformità

I clienti dei servizi cloud hanno poche informazioni sulle posizioni di archiviazione dei dati, sugli algoritmi utilizzati dal fornitore per fornire o allocare le risorse informatiche, sui controlli specifici utilizzati per proteggere i componenti dell'architettura di cloud computing o sul modo in cui i dati dei clienti sono segregati all'interno del cloud.

In alcuni casi possono sorgere problemi di sicurezza e conservazione in relazione alla conformità a normative e leggi e le varie normative sulla privacy e sulla protezione dei dati emanate in diversi paesi. Esempi di queste leggi sulla privacy e sulla protezione dei dati sono la *USA PATRIOT Act*, la direttiva UE sulla protezione dei dati, ecc. Nel cloud, i dati si trovano sull'hardware al di fuori del controllo diretto dell'organizzazione. Un'organizzazione potrebbe non essere in grado di ottenere e rivedere le operazioni di rete o i log degli incidenti di sicurezza perché in possesso del fornitore di servizi Cloud. Il fornitore di servizi Cloud potrebbe non essere obbligato a rivelare queste informazioni o potrebbe non essere in grado di farlo senza violare la riservatezza degli altri inquilini che condividono l'infrastruttura cloud.

IL TIGLIO SRL come cliente di servizi Cloud	IL TIGLIO SRL come fornitore di servizi Cloud
IL TIGLIO SRL utilizza solo fornitori di servizi Cloud che assicurano che i dati sono trattati solo all'interno della UE nel rispetto del GDPR.	I Dati degli utenti di SQuadra non vengono trattati al di fuori della UE.

Problemi di affidabilità e prestazioni

Il guasto di sistema è un evento che può verificarsi in qualsiasi ambiente informatico, ma che pone sfide uniche con il cloud computing. Sebbene gli accordi sui livelli di servizio possano essere strutturati per soddisfare requisiti particolari, le soluzioni offerte dal fornitore di servizi Cloud potrebbero a volte non essere in grado di soddisfare queste metriche di prestazioni se un locatario del cloud o un incidente pone una richiesta imprevista di risorse sull'infrastruttura cloud.

Alcuni fornitori di servizi cloud sono aziende relativamente giovani, o la linea di business del cloud computing è una nuova anche per un'azienda consolidata. Di conseguenza, la durata e la redditività dei servizi cloud sono sconosciuti. I clienti di servizi di cloud computing potrebbero trovarsi di fronte a interruzioni operative.

IL TIGLIO SRL come cliente di servizi Cloud	IL TIGLIO SRL come fornitore di servizi Cloud
---	---

IL TIGLIO SRL utilizza fornitori di servizi Cloud di grandi dimensioni che quindi dovrebbero essere in grado di assicurare le prestazioni concordate.

IL TIGLIO SRL monitora costantemente le prestazioni offerte ai propri clienti e in caso di necessità acquisisce maggiori risorse dal fornitore di servizi Cloud.

Mancanza di portabilità o interoperabilità delle applicazioni

Molti fornitori di servizi Cloud offrono strumenti di sviluppo di software applicativo con le loro soluzioni cloud. Quando questi strumenti sono proprietari, possono creare applicazioni che funzionano solo all'interno dell'architettura specifica della soluzione offerta dal fornitore. Di conseguenza, queste nuove applicazioni (create da questi strumenti proprietari) potrebbero non funzionare bene con sistemi che risiedono al di fuori della soluzione cloud. Inoltre, più applicazioni sviluppate con questi strumenti proprietari e più dati organizzativi memorizzati in una specifica soluzione cloud di CSP, più difficile è cambiare fornitore.

IL TIGLIO SRL come cliente di servizi Cloud	IL TIGLIO SRL come fornitore di servizi Cloud
IL TIGLIO SRL non utilizza nessuna prestazione proprietaria in modo da poter sempre migrare su altri fornitori di servizi Cloud.	Non significativo per gli utenti di SQuadra.

5.4 Server di Produzione

Servizi DNS

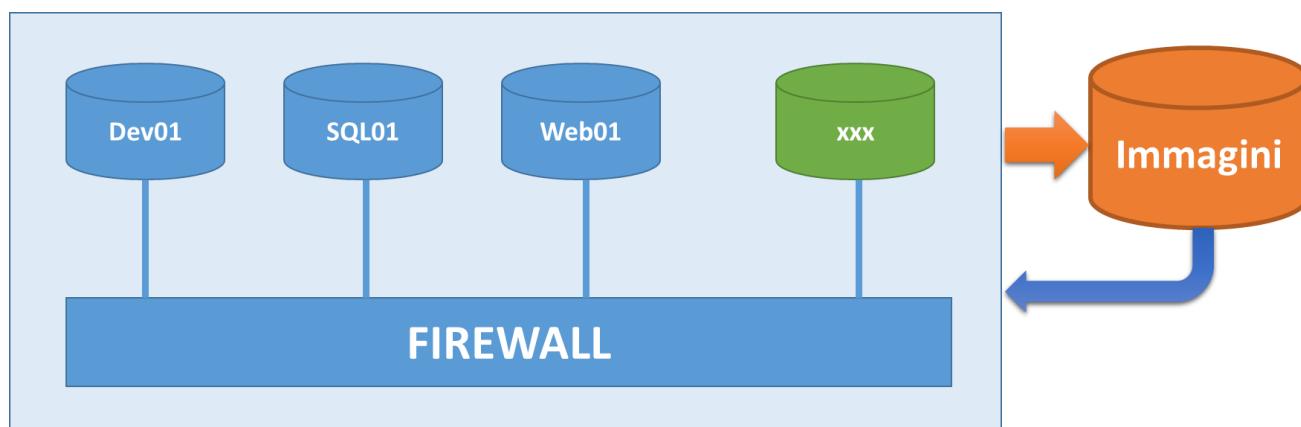
Il DNS (gestione della risoluzione dei nomi di dominio in indirizzi IP) de IL TIGLIO SRL è gestito tramite un pannello di controllo fornito dal fornitore del servizio al quale ha accesso unicamente il Responsabile della Sicurezza delle Informazioni (RSI) nella persona dell'Ing. Giuliano Marullo.

NOTA: IL TIGLIO SRL si impegna ad utilizzare come fornitore di servizi DNS uno dei leader di mercato a livello nazionale. IL TIGLIO SRL accetterà uno dei contratti standard predisposti dal fornitore di servizi DNS solo dopo aver valutato come adeguate le garanzie offerte dallo stesso. In caso di non rispondenza alle garanzie richieste o di sviluppi tecnologici IL TIGLIO SRL potrà con facilità migrare tutti i servizi verso altro fornitore (fra i numerosi presenti sul mercato) che offre maggiori garanzie o migliori funzionalità. Il fornitore di servizi DNS verrà comunque scelto fra quelli i cui servizi sono certificati in base alla ISO 27001 (Sistemi di gestione della sicurezza dell'informazione).

Servizi cloud

SQuadra opera su un Data Centre virtuale, offerta da un fornitore di servizi Cloud, all'interno della quale sono presenti un Firewall e i Server utilizzati da SQuadra. Nell'area virtuale sono presenti anche altri Server con i quali IL TIGLIO SRL fornisce altri servizi diversi da SQuadra (non oggetto della certificazione). Al pannello di controllo per la gestione del server può accedere unicamente il RSI.

NOTA: IL TIGLIO SRL si impegna ad utilizzare come fornitore di servizi Cloud uno dei leader di mercato a livello nazionale. IL TIGLIO SRL accetterà uno dei contratti standard predisposti dal fornitore di servizi Cloud solo dopo aver valutato come adeguate le garanzie offerte dallo stesso. In caso di non rispondenza alle garanzie richieste o di sviluppi tecnologici IL TIGLIO SRL potrà con facilità migrare tutti i servizi verso altro fornitore (fra i numerosi presenti sul mercato) che offre maggiori garanzie o migliori tecnologie. Il fornitore di servizi Cloud verrà comunque scelto fra quelli i cui servizi sono certificati in base alla ISO 27001 (Sistemi di gestione della sicurezza dell'informazione) ed i servizi utilizzati sono dichiarati conformi alla ISO 27017 (Sicurezza informatica del cloud computing), 27018 (Protezione dei dati personali nel cloud), 27035 (Risposta agli incidenti) e 22301 (Continuità operativa).



I Server utilizzati per SQuadra sono:

- Dev01: è il server di sviluppo.
- SQL01: contiene i Data Base.
- Web01: è l'unico server esposto su internet e contiene gli eseguibili.

I Server di SQuadra offrono potenza di calcolo, protezione fisica e logica, livelli di continuità e garanzie sui dati superiori a quelli adottati normalmente da ogni singola azienda per i propri dati.

In base alle caratteristiche di disponibilità offerta dai fornitori di servizi Cloud rispetto alla criticità dei dati gestiti da SQuadra non si ritiene di dover predisporre ulteriori livelli di ridondanza.

Server di Sviluppo (Dev01)

Le credenziali per l'accesso ai vari Server sono note unicamente al Responsabile della Sicurezza delle Informazioni (RSI) nella persona dell'Ing. Giuliano Marullo.

Le password utilizzate per l'accesso ai Server sono tutte differenti e devono rispettare criteri di qualità imposti dalla configurazione del Sistema Operativo. Ad ogni accesso viene riportata l'ora del precedente ultimo accesso e l'eventuale presenza di tentativi di accesso per permettere al RSI di verificare la presenza di attacchi al sistema.

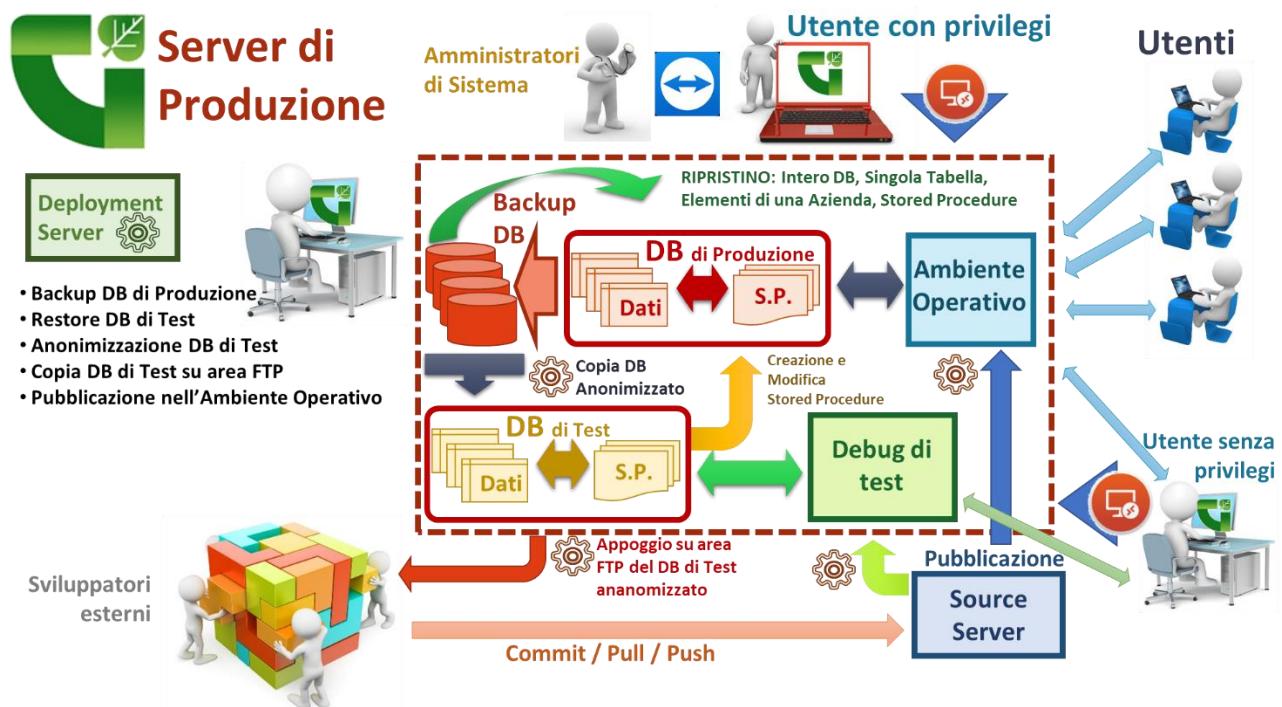
Il RSI accede ai Server tramite una connessione Terminal Server su una VPN sicura. Le apparecchiature utilizzate per l'accesso non vengono lasciate incustodite durante gli accessi e comunque sono dotate di Salva-Schermo protetto da password.

Tutti i Server sono protetti da un antivirus sempre aggiornato a cura dell'Amministratore di Sistema. La sicurezza fisica dei server è garantita dal fornitore dei servizi cloud.

Vista la tipologia di dati trattati da SQuadra e le misure di sicurezza attuate per i Server non si ritiene necessario applicare tecniche di crittografia.

Periodicamente, almeno 8 volte al giorno, vengono effettuate copie dell'immagine dei Server per il recupero in caso di disastro. Lo spazio riservato contiene oltre 120 immagini quindi è possibile recuperare le informazioni anche a distanza di circa 15 giorni.

Il recupero può essere effettuato in sostituzione su tutti i server o su un singolo server o su un nuovo server (per poter fare analisi o copie selettive). È anche possibile accedere al singolo file contenuto nelle immagini.



Il Responsabile della Sicurezza delle Informazioni (RSI) de Il TIGLIO SRL può accedere alla piattaforma di gestione del fornitore dei servizi Cloud (per spegnere o riaccendere l'intero server, per variare le risorse del server, ecc). RSI accederà con i privilegi di amministratore per svolgere o far svolgere dagli Amministratori di Sistema manutenzioni e configurazioni del Server di Produzione. Gli Amministratori di Sistema non accederanno direttamente al Server di Produzione ma si collegheranno, tramite Team Viewer, con il Portatile del RSI attraverso il quale potranno operare solo sotto il controllo diretto del RSI.

Gli Utenti si collegano al Server di Produzione tramite un Ambiente Operativo omogeneo per tutte le funzionalità. L'Ambiente Operativo accede alle Tabelle che contengono i Dati tramite delle Stored Procedure (anch'esse memorizzate all'interno del DB di Produzione).

Il RSI controlla le funzionalità del Deployment Server (DS) fra le quali il Backup automatico del DB di Produzione che viene effettuato una volta al giorno.

Una funzionalità del DS permette di partire dalle copie del DB per generare un DB di Test. Un'ulteriore funzionalità ne consente l'anonymizzazione.

Il RSI può, sempre utilizzando una funzionalità del DS, copiare il DB di Test (anonymizzato) nell'area FTP dalla quale potrà essere "prelevata" dagli eventuali sviluppatori esterni che provvedendo periodicamente ad aggiornare apposite "ramificazioni" dei sorgenti utilizzando il Source Server.

A fronte della disponibilità di nuovi sorgenti, sviluppati direttamente dal RSI o dagli sviluppatori esterni, RSI effettua tutte le prove sul DB di Test prima di lanciare la funzionalità che provvede alla pubblicazione dei sorgenti sull'Ambiente Operativo di produzione. La pubblicazione, tranne casi eccezionali, avviene al di fuori del normale orario di lavoro.

Il RSI utilizza normalmente le funzionalità dell'applicativo in produzione (in una configurazione a lui riservata che prevede, in aggiunta alle normali funzionalità, anche specifiche funzionalità per la gestione del Sistema (Creazione nuovi Utenti, Manutenzione di Tabelle di Sistema, ecc.) e, qualora rilevi (o gli venga segnalato) un qualunque malfunzionamento, è in grado di pubblicare una versione precedente dei sorgenti.

Il RSI sul DB di Test crea o modifica Stored Procedure e, sempre dopo adeguati test, le aggiorna sul DP di Produzione.

Livelli di accesso

Riepilogando i livelli di accesso sono i seguenti:

Tipo di Accesso	Funzionalità	Sicurezza
Gestore del Data Center Virtuale (*)	Può accedere al pannello di controllo messo a disposizione dal fornitore dei servizi cloud per accendere o spegnere il server e per modificarne la configurazione (CPU, Memoria, HD, ecc.).	Password con almeno 12 caratteri con: maiuscole, minuscole, numeri e segni.
Utente dei Server con privilegi di amministratore (*)	Può accedere al Server per gestire il Sistema Operativo (Creazione Utenti, apertura e chiusura porte, abilitazione di servizi, ecc.). Ha anche i massimi diritti sul DB e su Tutte le Cartelle.	Password con almeno 12 caratteri con: maiuscole, minuscole, numeri e segni.
Utente del Server Dev01 (*)	Può accedere al Server per operare sui sorgenti, sui DB (fisicamente su SQL01) e sui Files (fisicamente su WEB01).	Password con almeno 8 caratteri con: maiuscole, minuscole, numeri e segni.
Utente del Server SQL01 (*)	Accesso solo per attività di amministratore.	Password con almeno 8 caratteri con: maiuscole, minuscole, numeri e segni.
Utente del Server Web01 (*)	Accesso solo per attività di amministratore.	Password con almeno 8 caratteri con: maiuscole, minuscole, numeri e segni.

Utente di SQuadra privilegiato (*)	Ha accesso a funzionalità specifiche di SQuadra per la gestione del sistema (Creazione Utenti, Manutenzione Tabelle di Sistema, ecc.). Ha anche accesso alle normali funzionalità di SQuadra.	Password con almeno 8 caratteri con: maiuscole, minuscole, numeri e segni.
Utenti di SQuadra "particolari"	Sono particolari utenti di SQuadra che possono gestire più aziende (che li hanno espressamente nominati e che possono, in ogni momento disabilitarli).	Password.
Utente di SQuadra	È il normale utilizzatore di SQuadra. Può agire unicamente sulle funzionalità abilitate e sui dati della propria azienda.	Password.

(*) L'accesso è riservato al solo RSI.

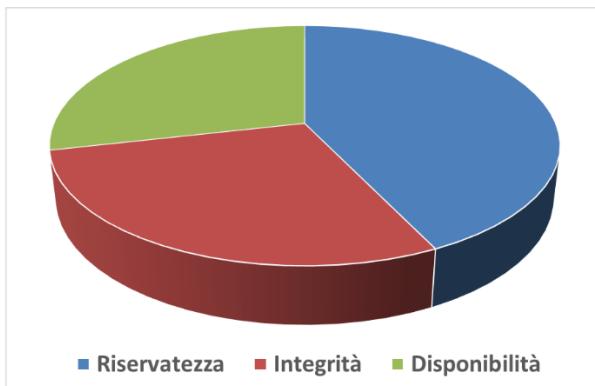
Classificazione delle Informazioni

Le informazioni gestite sono tutte contenute nelle tabelle del DB e nei Documenti Allegati.

Il DB è composto da numerose Tabelle contenenti le varie informazioni. Solo alcune tabelle possono contenere dati personali o riservati ma tutto il DB viene classificato al livello massimo quindi contenente dati personali o riservati.

Gli Allegati sono di varia natura (Certificati, Schede di Sicurezza, Evidenze di Audit, ecc.). Solo alcuni potranno contenere dati personali o riservati. Tutti gli Allegati vengono classificati al livello massimo quindi contenenti dati personali o riservati.

Dall'analisi dei Trattamenti si ritiene necessario garantire, sia per il DB che per gli Allegati, soprattutto la Riservatezza rispetto a Disponibilità ed Integrità.



DB di Produzione

Nei Server SQL01 sono presenti tutti i dati trattati da SQuadra sia all'interno del DB di Produzione.

Vista la tipologia dei dati trattati e la sicurezza fisica e logica assicurata al Server di Produzione non si ritiene di utilizzare controllo crittografici.

Al DB di Produzione ha accesso come amministratore unicamente RSI che è l'unico che può creare o modificare Tabelle e Stored Procedures.

RSI è in grado di recuperare massivamente tutto il DB di Produzione dalle immagini periodiche dalla copia gestita dal Deployment Server.

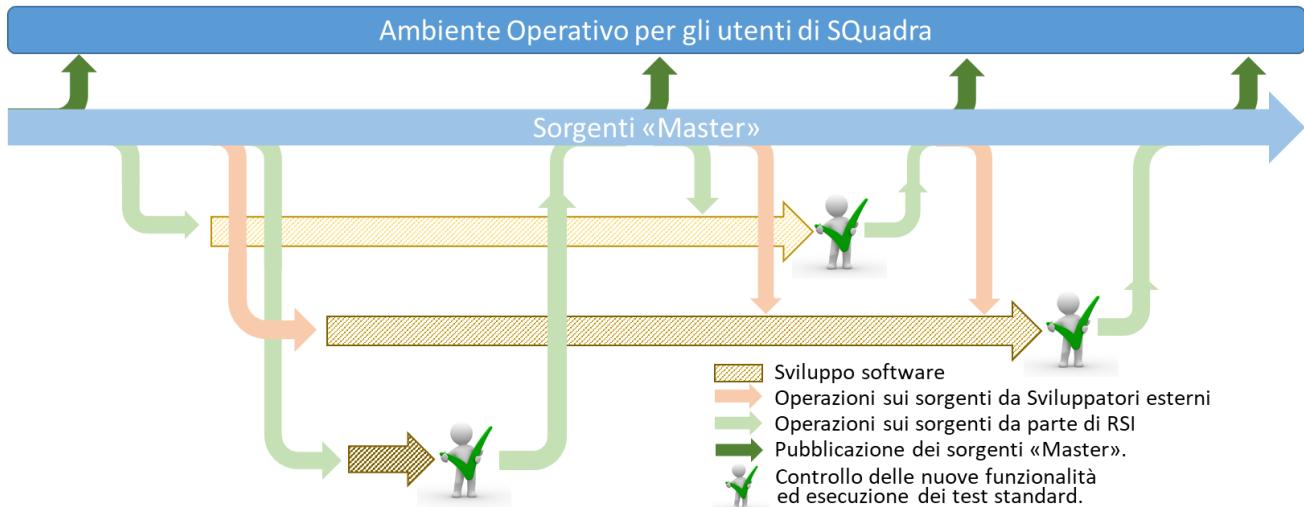
RSI può, inoltre, di recuperare dati parziali sempre partendo da copie di backup ma copiandole sul DB di Test.

Documenti allegati

I Documenti inseriti dagli Utenti come Allegati sono conservati sotto un'area di memorizzazione del Server WEB01. I Documenti sono raggruppati per azienda (per permetterne, in caso di richiesta, la cancellazione massiva) ma il nome dell'azienda è codificato. Anche il nome dei singoli files è codificato.

Sviluppo dell'applicativo

Dai sorgenti “Master” vengono costruiti, dal RSI stesso o dagli Sviluppatori esterni, dei rami per sviluppare specifiche funzionalità.



Lo sviluppo del ramo viene effettuato lavorando sul DB di Test anonimizzato o, per gli sviluppatori esterni, su una copia di questo.

Una volta concluso lo sviluppo del ramo vengono effettuate da parte del RSI, sempre sul DB di Test, le prove sulle nuove funzionalità e i test sulla non regressione rispetto alle funzionalità standard.

Solo il RSI può, in caso di esito positivo dei test, provvedere alla “fusione” del nuovo codice nel “Master” e quindi alla Pubblicazione sull’ambiente operativo che avviene possibilmente al di fuori del normale orario lavorativo.

Tutti i rami di sviluppo non ancora conclusi acquisiscono le modifiche apportate al “Master”.

Gestione dei Cambiamenti

I Test sulle funzionalità standard sono rivisti in caso di segnalazioni pertinenti da parte degli utenti. L’opportunità di aggiungere nuovi test a fronte delle nuove funzioni introdotte è valutata da RSI.

In genere le funzionalità di SQuadra permettono di inserire dati ma non modificano i dati inseriti quindi, eventuali errori, sono limitati al non salvataggio dei dati.

Quando vengono introdotte nuove funzionalità che modificano massivamente dati presenti sul DB, RSI valuta l’opportunità di effettuare una copia specifica delle Tabelle coinvolte prima di pubblicare le nuove funzionalità per permettere un rapido controllo degli effetti e per recuperare i dati precedenti in caso di rilevazione di anomalie in casi particolari non evidenziate nella fase di test.

L’utilizzo di nuove tecnologie per la sicurezza dei dati viene valutato dal RSI in relazione alle problematiche connesse alla sicurezza dei dati gestiti da SQuadra in relazione ad attacchi conosciuti.

Attività dell’Amministratore di Sistema

L’Amministratore di Sistema (nella persona di Mirko Meoni, legato a IL TIGLIO SRL da apposito contratto) accede al Server di Produzione unicamente tramite Team Viewer utilizzando il numero di controllo fornito, di volta in volta, da RSI che controlla le attività svolte tramite l’accesso con Terminal Server.

I LOG delle attività svolte dall'Amministratore sono conservati per almeno 6 mesi.

5.5 Livello di Servizio

Obiettivo della presente Appendice è quello di definire i Livelli di Servizio di riferimento per l'erogazione del servizio offerto da IL TIGLIO SRL e per il monitoraggio del livello di qualità effettivamente erogato.

IL TIGLIO SRL si riserva la facoltà di modificare i Livelli di Servizio di riferimento in qualsiasi momento. Le modifiche apportate alla presente appendice entrano in vigore dalla data della pubblicazione, a tempo indeterminato fino alla prossima modifica o sostituzione.

Limitazioni

I Livelli di Servizio di riferimento non sono validi in caso di problemi di erogazione o disponibilità:

- Dovuti a fattori al di fuori del ragionevole controllo de IL TIGLIO SRL (ad esempio, calamità naturali, atti di terrorismo oppure problemi di rete o guasti del dispositivo all'esterno dei data center utilizzati da IL TIGLIO SRL, sia sul sito della società o tra il sito della società e il data center utilizzato da IL TIGLIO SRL).
- Derivanti da interventi straordinari da effettuarsi con urgenza ad insindacabile giudizio de IL TIGLIO SRL per evitare pericoli alla sicurezza e/o stabilità e/o riservatezza e/o integrità dell'Infrastruttura virtuale sulla quale opera SQuadra e dei dati e/o informazioni in essa contenuti.
- Derivanti dall'utilizzo di servizi, hardware o software non forniti da IL TIGLIO SRL, inclusi, a titolo esemplificativo, i problemi causati da larghezza di banda inadeguata o correlati al software o ai servizi di terzi.
- Derivanti da cause che determinano l'inaccessibilità, totale o parziale, dell'Infrastruttura virtuale imputabili a guasti nella rete internet esterna al perimetro di competenza de IL TIGLIO SRL e comunque fuori dal suo controllo.
- Risultanti da tentativi della società di eseguire operazioni che superino le quote del normale utilizzo derivanti dalla limitazione imposta da IL TIGLIO SRL circa i comportamenti offensivi sospetti.

Garanzie e Compensazioni

IL TIGLIO SRL per dimostrare il proprio impegno concreto nel rispetto dei Livelli di Servizio di riferimento, a fronte di ogni violazione di questi rilevata da un'Azienda, riconoscerà, alla stessa, l'allungamento di un mese del contratto di utilizzo dei servizi offerti.

Per le Aziende che operano all'interno della convenzione con ANCE per ogni rilevazione di violazione dei Livelli di Servizio verrà offerto un intervento in collegamento telematico di assistenza sulle problematiche inerenti alla 231, alla Privacy, alla Gestione dei Sistemi, all'Asseverazione o sull'uso del programma.

5.5.1 Sicurezza Fisica

Il fornitore dei servizi Cloud utilizzato da IL TIGLIO SRL, relativamente ai sistemi di difesa e monitoraggio, assicura:

- VIGILANZA E CONTROLLO: Sensori anti-intrusione, videosorveglianza, controllo degli accessi con doppi meccanismi di autenticazione e sistemi tecnologici anti-tailgating.
- MONITORAGGIO H24/365: Network Operation Center (NOC) on-site, ridondato e presidiato 24 ore su 24, 365 giorni all'anno ed affidato esclusivamente a nostro personale.

- **SICUREZZA DEI DATI:** La gestione e la protezione dei dati in infrastrutture ad elevata sicurezza sono certificate ISO 27001.
- **IMPIANTI RIDONDANTI:** Power center e sistemi di raffreddamento totalmente ridondati ed equipaggiati con i più moderni apparati.
- **BACKUP ENERGETICO:** Efficienti aree backup, completamente ridondate, garantiscono la massima affidabilità dell'alimentazione e del raffreddamento.
- **PREVENZIONE INCENDI:** La separazione di tutti gli impianti e ambienti e i sistemi di rilevazione auto-spegnimento garantiscono la massima sicurezza contro il rischio di incendi.

5.5.2 Funzionalità operativa

Il TIGLIO SRL farà ogni ragionevole sforzo, direttamente o tramite i propri fornitori, per garantire la massima disponibilità dell'Infrastruttura virtuale utilizzata dagli utenti e, contestualmente, l'osservanza dei seguenti parametri di funzionalità operativa.

Risorse del Data Center attraverso il quale viene erogato il Servizio

- Tempo di funzionamento del 100% per alimentazione elettrica e/o climatizzazione ambientale.
- Tempo di funzionamento del 99,95% su base annuale, di accessibilità rete internet alla Infrastruttura virtuale utilizzata dagli utenti.
- Tempo di funzionamento del 99,9% su base annuale, per la disponibilità dei server che ospitano l'Infrastruttura virtuale su cui opera SQuadra.

Tempo di funzionamento

Sulla base delle caratteristiche offerte dal Data Center attraverso il quale viene erogato il Servizio IL TIGLIO SRL assicura un Tempo di funzionamento del 99% su base annuale che dovrebbe essere adeguato alle esigenze degli utenti in relazione al tipo di dati gestiti da SQuadra.

NOTA: Il tempo di manutenzione programmata non viene conteggiato ai fini del calcolo dei tempi di funzionamento. La manutenzione programmata riguarda le attività svolte regolarmente da IL TIGLIO SRL o dai suoi fornitori per mantenere la funzionalità delle risorse del Data Center attraverso il quale viene erogato il servizio. Per quanto possibile le attività di manutenzione verranno svolte al di fuori del normale orario lavorativo (9-13 e 15-19 per i giorni lavorativi) o con periodi di interruzione del servizio inferiori ai 5 minuti.

Servizio Backup

I dati di SQuadra vengono duplicati, per permetterne il ripristino in caso di problemi, almeno giornalmente.

- Periodo di inserimento dati perso per recupero di dati precedenti (RPO) minore di 8 ore su base annuale.

Nota: Ad esempio il sistema permette di inserire i dati fino alle 15:30 di un giorno ma, a causa di un problema, vengono quindi ripristinati i dati relativi al giorno precedente. In questo caso viene considerato perso il periodo di inserimento pari a 4,5 ore (9:00-13:00 più 15:00-15:30). Ovviamente risentiranno del problema solo le aziende che hanno inserito nuovi dati nel periodo "perso".

- Tempo necessario per il ripristino (RTO) in caso di segnalazione di problemi sui dati:
 - Inferiore a 1 ora in caso di problemi sull'intero DB (problemI derivanti da un malfunzionamento del sistema).
 - Entro 2 giorni lavorativi in caso di problemi legati ad una sola Azienda (problemI derivanti da un errore operativo del singolo utente).

5.5.3 Rilevamento guasti e/o anomalie

RSI utilizza per la sua attività professionale SQuadra accedendo almeno giornalmente all'applicazione e rilevando eventuali malfunzionamenti.

Si ricorda a tutti gli utenti che un'apposita funzionalità di SQuadra (VARIE / Amministrazione Sistema / Segnalazioni su SQuadra) consente di inviare richieste al team di SQuadra.

Fra le segnalazioni si invitano gli utenti ad indicare, a titolo d'esempio:

- Problemi di accesso a SQuadra.
- Problemi con i tempi di risposta di SQuadra (ovviamente non derivanti dalla banda disponibile per l'Utente).
- Sospetta perdita di dati per anomalie di SQuadra.
- Sospetta violazione della riservatezza dei dati inseriti su SQuadra.
- Problemi connessi all'introduzione di nuove funzionalità non chiaramente documentate nel presente Manuale.

È possibile utilizzare le Segnalazioni su SQuadra anche per formulare richieste di nuove funzionalità.

In caso di non funzionamento è comunque possibile segnalare le eventuali anomalie attraverso l'apposita scelta presente nel menù di destra o inviando direttamente una mail all'indirizzo: assistenza@iltigiosrl.it.

5.5.4 Statistiche

I servizi di Squadra vengono utilizzati dal novembre 2009 da centinaia di aziende su tutto il territorio nazionale e, in questi anni, non sono mai stati segnalati problemi sui server o sulla connettività o perdita di dati da parte degli utenti.

6 APPENDICE: Aggiornamenti del Modello

6.1 Aggiunta di nuovi Reati

Periodicamente il Legislatore incrementa i reati per i quali è prevista l'applicazione del D.Lgs 231/01.

Quando viene aggiunta una nuova famiglia di Reati (nuovi articoli 24.xxx o 25.yyy o l'aggiunta all'interno di un articolo già esistente di Reati che richiedono una analisi del rischio differenziata) è necessario definire il Livello di Rischio in: Rischi / Analisi del Modello approvato / Livelli di Rischio.

Se il Livello di Rischio non viene definito come "NON SIGNIFICATIVO" sarà necessario definire come il Modello agisce per limitare la possibilità di commettere il nuovo reato.

Questo sarà possibile:

- Correlando una o più Procedure già presenti al nuovo Reato (in Manutenzioni / Personalizza / Procedure).
- Creando nuove Procedure, in risposta a Punti di Controllo già presenti, e correlandole al nuovo Reato.
- Creando nuovi Punti di Controllo, con le relative Procedure che dovranno essere correlate al nuovo Reato.

Il Modello così modificato andrà, ovviamente, approvato dall'Organo Dirigente.

7 APPENDICE: Aggiornamento Codice di Comportamento ANCE 2020

7.1 Premessa

La revisione 2013 del Codice di Comportamento ANCE è stata valutata idonea ed adeguata dal Ministero della Giustizia in data 20 dicembre 2013.

Il quadro di riferimento complessivo della revisione generale effettuata nel 2013 conserva ancora piena validità. Le modifiche legislative apportate al DLgs 231/2001 dopo tale data sono state valutate per proporre le opportune modifiche.

Sono stati quindi predisposti, ad oggi, gli aggiornamenti 2018, 2019 e 2020 (l'ultimo, che racchiude anche gli altri, è scaricabile dal sito ANCE), da utilizzare insieme alla revisione 2013 del Codice di Comportamento a suo tempo valutata idonea ed adeguata dal Ministero della Giustizia.

La presente appendice indica le attività che dovranno compiere le Aziende che hanno già predisposto un Modello sulla base del Codice di Comportamento ANCE 2013.

7.2 Analisi dei Nuovi Punti di Controllo

Vengono presentati i nuovi Punti di Controllo e confrontati con quelli presenti in azienda.

I Punti di Controllo aziendali possono essere “Collegati” con i Punti base (se generati dal programma) o avere lo stesso Codice (se inseriti manualmente). Il programma confronta le descrizioni e segnala l’eventuale presenza di differenze.

7.3 Nuove correlazioni

In alcuni casi l’aggiornamento ANCE propone che alla maggiore gravità dei nuovi reati presupposto debba corrispondere la individuazione come CRITICI alcuni protocolli preesistenti.

In “Nuove Correlazioni” vengono presentate le Procedure sviluppate dall’azienda in risposta ai Punti di Controllo per i quali è variata la correlazione per il Punto di Controllo. L’utente dovrà valutare se le procedure individuate siano ancora adeguate e se ritiene opportuno portare la correlazione con i vari Reati a CRITICA.

7.4 Aggiornamento dei Punti di Controllo

NOTA: Prima di eseguire le operazioni seguenti si consiglia di eseguire una stampa completa del MOG in modifica per poter controllare successivamente le modifiche effettuate.

In “Manutenzione / Documenti / MOG Parte Speciale (Personalizzato)” selezionare una stampa completa (ad esempio la stampa ufficiale) nella quale come Reati correlati selezionare “Con Reati e Governance per Punti e Procedure”.

In “VARIE / Documenti di Supporto / Aggiornamento ANCE 2020” è presente la funzione “Aggiornamento Punti di Controllo e delle correlazioni” che aggiorna tutti i Punti di Controllo e le correlazioni previste per i Punti di Controllo sulla base dell’aggiornamento ANCE.

Prima di procedere all’aggiornamento EFFETTIVO si consiglia di procedere con l’ANALISI che produce un foglio di excel con l’elenco dei Punti di Controllo (modificati o nuovi con accanto ai Modificati il precedente contenuto) ed un foglio con l’elenco delle Correlazioni modificate o nuove.

NOTA: Dopo l’aggiornamento effettivo si consiglia di effettuare la stessa stampa effettuata in precedenza. Utilizzando le funzionalità di Word è possibile, confrontando i due documenti, verificare le modifiche effettuate in automatico del programma.

Per i nuovi Punti di Controllo vengono previste apposite Procedure che dovranno essere controllate dall’azienda.

Per quelli modificati dovranno essere analizzate le Procedure preesistenti per valutare la necessità di un aggiornamento a fronte della variazione del Punto di Controllo.

L'aggiornamento, qualora vengano introdotti nuovi Punti di Controllo, deve essere ripetuto per verificare le correlazioni proposte per i Punti di Controllo aggiunti.

7.5 Verifica dei Punti di Controllo aziendali

Una volta concluso l'allineamento all'Aggiornamento ANCE 2020 è consigliabile andare a controllare gli eventuali Punti di Controllo aziendali che erano stati introdotti autonomamente in funzione delle novità legislative introdotte dopo il 2013.

In particolare, è opportuno verificare che per ogni Punto di Controllo sia presente almeno una Procedura e che per ogni Procedura sia correttamente definito il Responsabile.

In "MOG / Punti di controllo aziendali / Punti di Controllo Specifici" è possibile trovare i Punti di Controllo non "compresi" nell'aggiornamento ANCE 2020. Sarà compito dell'azienda decidere se lasciarli o eliminarli.

7.6 Adeguamento della Parte Generale

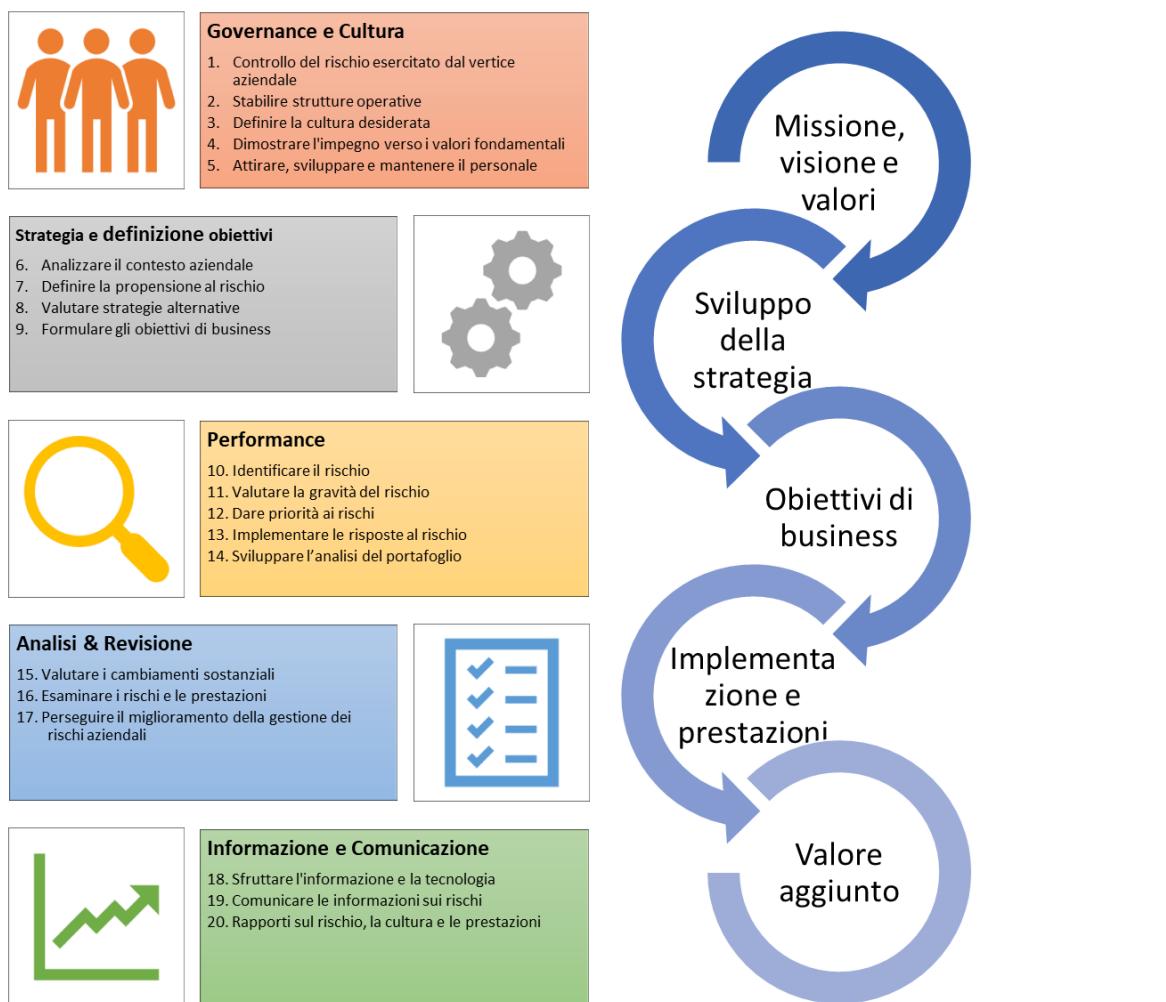
Fra i documenti di supporto è presente un testo di Word che può essere utilizzato per l'aggiornamento della Parte Generale relativamente alla gestione delle Segnalazioni.

8 APPENDICE: CoSO Report

8.1 La gestione dei rischi aziendali (ERM)

8.1.1 Versione del Giugno 2017

Lo strumento più comunemente adottato per i processi per la gestione dei rischi è quello sviluppato dal Committee of Sponsoring Organization of the Treadway Commission¹⁹ (CoSO). Nel 2017, CoSO ha pubblicato un framework aggiornato di “Enterprise Risk Management - Integrating with Strategy and Performance”, d'ora in poi: “Gestione del rischio aziendale - Integrazione con la strategia e le prestazioni”. Il quadro di riferimento è costituito da cinque componenti e 20 principi che affrontano l'evoluzione della gestione del rischio aziendale e la necessità per le organizzazioni di migliorare il loro approccio alla gestione del rischio per soddisfare le esigenze di un ambiente aziendale in evoluzione, per riflettere strategicamente su come gestire la crescente volatilità, complessità e ambiguità dell'ambiente di business - internamente ed esternamente.



¹⁹ Nata nel 1985, CoSO è un'organizzazione volontaria del settore privato dedicata a fornire una leadership di pensiero attraverso lo sviluppo di strutture complete e linee guida sul controllo interno, la gestione del rischio aziendale e la deterrenza antifrode. COSO è sponsorizzato congiuntamente dall'American Accounting Association (AAA), dall'American Institute of Certified Public Accountants (AICPA), Financial Executives International (FEI), dall'Institute of Management Accountants (IMA) e dall'Institute of Internal Auditors (IIA). Per maggiori informazioni, visitare il sito COSO.org.

“Gestione del rischio aziendale: integrazione con la strategia e le prestazioni” chiarisce l’importanza della gestione del rischio aziendale nella pianificazione strategica e l’integrazione in un’organizzazione - perché il rischio influenza e allinea la strategia e le prestazioni in tutti i reparti e le funzioni.

Come gli altri documenti CoSO, ERM è strutturato utilizzando componenti e principi. Le cinque componenti sono supportate da venti principi che coprono argomenti che spaziano dalla governance e cultura, alla definizione di strategie e obiettivi, alla performance, al riesame e revisione, all’informazione, alla comunicazione e al reporting. Ognuno dei principi rappresenta un concetto fondamentale associato ad un componente, sono universali nella loro applicazione e fanno parte della gestione del rischio aziendale.

Le cinque componenti interconnesse sono:

- **Governance e cultura:** La governance definisce il tono dell’organizzazione, rafforzando l’importanza della gestione del rischio aziendale e stabilendo responsabilità di supervisione. La cultura riguarda i valori etici, i comportamenti desiderati e la comprensione del rischio nell’entità.
- **Strategia e definizione degli obiettivi:** La gestione del rischio aziendale, la strategia e la definizione degli obiettivi lavorano insieme nel processo di pianificazione strategica. L’appetito per il rischio è stabilito e allineato con la strategia; gli obiettivi di business mettono in pratica la strategia e servono come base per identificare, valutare e rispondere al rischio.
- **Performance:** I rischi che possono influire sul raggiungimento degli obiettivi strategici e commerciali devono essere identificati e valutati. I rischi sono classificati in ordine di priorità in base alla gravità nel contesto della propensione al rischio. L’organizzazione seleziona quindi le risposte al rischio e adotta una visione di portafoglio dell’ammontare del rischio assunto. I risultati di questo processo sono comunicati ai principali stakeholder a rischio.
- **Analisi e revisione:** Esaminando le prestazioni dell’entità, un’organizzazione può considerare quanto bene le componenti di gestione del rischio aziendale funzionano nel tempo e alla luce di cambiamenti sostanziali, e quali revisioni sono necessarie.
- **Informazione, comunicazione e rendicontazione:** La gestione dei rischi aziendali richiede un processo continuo di acquisizione e condivisione delle informazioni necessarie, sia da fonti interne che esterne, che fluisce verso l’alto, verso il basso e attraverso l’organizzazione.

Le cinque componenti del quadro sono sostenute da 20 principi. Questi principi riguardano tutto, dalla governance al monitoraggio. Sono gestibili in termini di dimensioni e descrivono pratiche che possono essere applicate in modi diversi per diverse organizzazioni, indipendentemente dalle dimensioni, dal tipo o dal settore. L’adesione a questi principi può fornire al management e al consiglio di amministrazione una ragionevole aspettativa che l’organizzazione comprenda e si sforzi di gestire i rischi associati alla sua strategia e ai suoi obiettivi aziendali.

 Governance e cultura	<ol style="list-style-type: none">1. Controllo del rischio esercitato dal consiglio di amministrazione - Il consiglio di amministrazione fornisce la supervisione della strategia e svolge responsabilità di governance per supportare il management nel raggiungimento degli obiettivi strategici e di business.2. Stabilire le strutture operative - L’organizzazione stabilisce le strutture operative nel perseguitamento della strategia e degli obiettivi di business.3. Definire la cultura desiderata: l’organizzazione definisce i comportamenti desiderati che caratterizzano la cultura desiderata dell’entità.
---	--

	<p>4. Dimostrare dell'impegno verso i valori fondamentali: l'organizzazione dimostra un impegno verso i valori fondamentali dell'entità.</p> <p>5. Attirare, sviluppare e mantenere personale competente: l'organizzazione si impegna a costruire capitale umano in linea con la strategia e gli obiettivi di business.</p>
 Strategia e definizione degli obiettivi	<p>6. Analizzare il contesto aziendale: l'organizzazione considera i potenziali effetti del contesto aziendale sul profilo di rischio.</p> <p>7. Definire la propensione al rischio: l'organizzazione definisce l'appetito per il rischio nel contesto della creazione, conservazione e realizzazione di valore.</p> <p>8. Valutare strategie alternative: l'organizzazione valuta le strategie alternative e l'impatto potenziale sul profilo di rischio.</p> <p>9. Formulare gli obiettivi di business: l'organizzazione considera il rischio e stabilisce gli obiettivi di business a vari livelli che allineano e supportano la strategia.</p>
 Performance	<p>10. Identificare il rischio: l'organizzazione identifica il rischio che incide sulla performance della strategia e sugli obiettivi di business.</p> <p>11. Valutare la gravità del rischio: l'organizzazione valuta la gravità del rischio.</p> <p>12. Dare priorità ai rischi: l'organizzazione dà priorità ai rischi come base per la selezione delle risposte ai rischi.</p> <p>13. Implementare le risposte al rischio: l'organizzazione identifica e seleziona le risposte al rischio.</p> <p>14. Sviluppare l'analisi del portafoglio: l'organizzazione sviluppa e valuta una visione del rischio del portafoglio.</p>
 Analisi e revisione	<p>15. Valutare i cambiamenti sostanziali: l'organizzazione identifica e valuta i cambiamenti che possono influenzare sostanzialmente la strategia e gli obiettivi di business.</p> <p>16. Esaminare i rischi e le prestazioni: l'organizzazione esamina le prestazioni dell'entità e considera il rischio.</p> <p>17. Perseguire il miglioramento nella gestione dei rischi aziendali - L'organizzazione persegue il miglioramento della gestione del rischio di impresa.</p>
 Informazione, comunicazione e rendicontazione	<p>18. Sfruttare i sistemi informativi: l'organizzazione sfrutta i sistemi informativi e tecnologici dell'entità per supportare la gestione del rischio aziendale.</p> <p>19. Comunicare le informazioni sul rischio: l'organizzazione utilizza i canali di comunicazione per supportare la gestione del rischio aziendale.</p> <p>20. Rapporti su rischio, cultura e prestazioni: l'organizzazione riferisce su rischio, cultura e performance a più livelli e in tutta l'entità.</p>

Secondo CoSO, l'ERM (Enterprise Risk Management) fornisce a un'entità un percorso per creare, preservare e realizzare valore. Le sue fondamenta supportano gli obiettivi strategici e di business di un'organizzazione, pur mantenendo una governance efficace. I suoi processi aiutano a identificare, valutare, gestire, monitorare e comunicare meglio i rischi che le organizzazioni devono affrontare. Un ERM efficace aiuta un'organizzazione a identificare le sfide che si prospettano e a adattarvisi.

Destinatari

“Gestione del rischio aziendale: integrazione con la strategia e le prestazioni” è stato redatto per un pubblico eterogeneo a seconda dei ruoli e delle responsabilità di gestione del rischio aziendale con l'intento di sintetizzare l'importanza e i benefici della gestione del rischio aziendale. In particolare, evidenzia il ruolo di governance e di controllo del vertice aziendale per quanto riguarda la gestione dei rischi aziendali.

I principi di ERM si applicano a tutte le entità, inclusi gli enti senza scopo di lucro e governativi, indipendentemente dalle dimensioni. Anche se alcune piccole e medie imprese possono applicare i principi della gestione del rischio d'impresa in modo diverso rispetto alle grandi imprese, essi rimangono applicabili ad ogni tipo di impresa.

ERM e Controllo interno

I due documenti CoSO (Controllo interno del 2013 e l'ERM del 2017) si completano a vicenda, senza che nessuno dei due documenti si sostituisca all'altro. I documenti sono complementari ed entrambi i quadri utilizzano una struttura di componenti e principi, tuttavia questi ultimi sono adattati a ciascuno di essi. Per evitare ridondanza, alcuni aspetti del controllo interno comuni ad entrambi non vengono ripetuti nel documento ERM.

Il documento di ERM si concentra sulla gestione dei rischi aziendali che vanno oltre il controllo interno; tuttavia, il quadro integrato di controllo interno rimane un quadro valido e adeguato alla progettazione, l'attuazione, la conduzione e la valutazione dell'efficacia del controllo interno e per la rendicontazione.

Il ruolo della gestione dei rischi

Il documento sottolinea il ruolo della gestione del rischio aziendale nella creazione, conservazione e realizzazione del valore.

La gestione del rischio d'impresa non è più incentrata principalmente sulla prevenzione dell'erosione del valore e sulla minimizzazione del rischio ad un livello accettabile. Piuttosto, è vista come parte integrante delle scelte strategiche e dell'identificazione di opportunità per creare e mantenere il valore. Invece di concentrarsi semplicemente sulla riduzione di rischi specifici, la gestione del rischio aziendale diventa parte integrante e dinamica della gestione di un'entità lungo tutta la catena del valore.

In tutto l'aggiornamento del documento è evidenziata l'integrazione della gestione del rischio aziendale in tutti gli aspetti delle operazioni di un'organizzazione. A partire dall'integrazione della gestione del rischio d'impresa nel processo di definizione della strategia, di definizione degli obiettivi di business e di gestione del rischio in esecuzione, la considerazione del rischio non viene posizionata come attività aggiuntiva o separata. Piuttosto, l'importanza e il ruolo della gestione del rischio aziendale viene presentata come supporto alle operazioni di un'organizzazione, la gestione delle prestazioni e, in ultima analisi, la creazione, la realizzazione e la conservazione del valore.

Il ruolo della cultura

Il documento pone un particolare accento all'importanza dell'influenza della cultura sulle pratiche di gestione del rischio aziendale. L'importanza di comprendere e plasmare la cultura è esaminata nel contesto della governance del rischio e del controllo dell'entità e di come essa influisce su altre componenti del Quadro per il modo in cui le strategie sono scelte ed eseguite. In particolare, fornisce il contesto per l'identificazione e la valutazione dei rischi e l'assegnazione di risorse per far fronte a tali rischi.

La strategia

Il documento evidenzia il rischio di scegliere una strategia che non è in linea con la missione, la visione e i valori fondamentali di un'entità.

Il documento pone l'attenzione sui tre concetti seguenti:

- La possibilità che la strategia e gli obiettivi di business non siano in linea con la missione, la visione e i valori.
- Le implicazioni della strategia scelta.
- Il Rischio per l'esecuzione della strategia.

I concetti sono esaminati progressivamente in tutto il documento, esplorando le considerazioni per l'identificazione, la valutazione e la gestione del rischio e l'impatto sulla strategia per ciascuno di essi.

Prestazioni e la gestione del rischio aziendale

Come indicato dal nuovo titolo, il documento aggiornato rafforza il rapporto tra rischio e performance. Il rischio è parte integrante della definizione degli obiettivi aziendali e degli obiettivi di performance attraverso quanto segue:

- Come le pratiche di gestione del rischio aziendale supportano l'identificazione e la valutazione dei rischi che possono influire sulle prestazioni.
- Come viene definita la tolleranza accettabile, come i cambiamenti nelle prestazioni possono portare a cambiamenti nel profilo di rischio di un obiettivo aziendale e viceversa.
- Come la valutazione dei rischi e il reporting dei rischi non sono lunghe liste di rischi potenziali, ma piuttosto evidenziano come i rischi possono influire sul raggiungimento della strategia e degli obiettivi aziendali.

Per sottolineare l'importanza di questa relazione, il documento aggiornato introduce l'analisi del profilo di rischio (vedi capitolo successivo). I profili di rischio mostrano come il tipo e la gravità del rischio possono cambiare in risposta ai cambiamenti del livello di performance per una data strategia o obiettivo aziendale tenendo conto della propensione al rischio dell'entità permettendo di identificare dove un'organizzazione può assumere rischi eccessivi o essere in grado di perseguire ulteriori opportunità. Integrando i concetti di propensione al rischio, performance e rischio i profili di rischio offrono una visione dinamica e completa del rischio e consentono di prendere decisioni più consapevoli del rischio.

Gestione del rischio aziendale e processo decisionale

Il processo decisionale avviene in ogni fase della catena del valore. Mentre le entità cercano di creare, realizzare e preservare il valore, le decisioni sono prese intorno alla selezione della strategia, alla definizione di obiettivi di business e di performance e all'allocazione delle risorse. L'integrazione della gestione del rischio aziendale nel ciclo di vita di un'entità supporta il processo decisionale consapevole dei rischi.

Le informazioni sui rischi comprendono la comprensione della gravità e del tipo di rischio, l'influenza del contesto aziendale, la comprensione delle ipotesi alla base dell'identificazione e della valutazione del rischio, nonché la cultura del rischio e l'appetito dell'entità.

Propensione e tolleranza al rischio

La propensione al rischio è la quantità di rischio che un'entità è disposta ad accettare nel perseguitamento della sua strategia e dei suoi obiettivi aziendali.

È necessario determinare l'entità del rischio accettabile per un determinato livello di prestazione. Non vanno analizzate singolarmente né il rischio né le prestazioni, ma piuttosto la continua evoluzione e l'influenza reciproca.

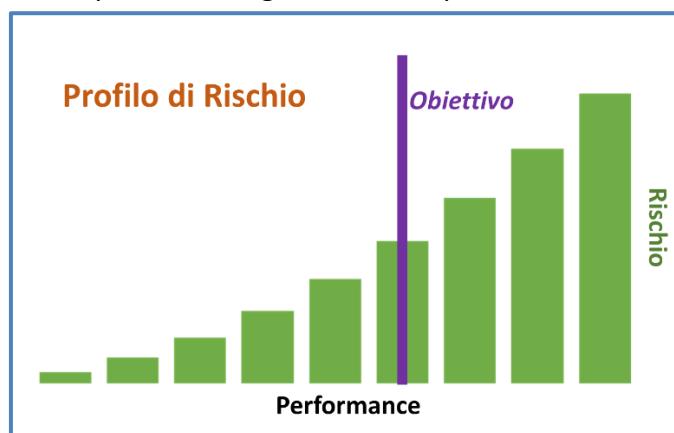
8.1.2 Gestione del Rischio e Performance (Profilo di rischio)

Il "profilo di rischio" di un'entità (rapporto tra rischio e performance) fornisce una visione composita del rischio a un particolare livello dell'entità (ad esempio, livello generale dell'entità, livello di unità aziendale, livello funzionale) o aspetto del modello aziendale (ad esempio, prodotto, servizio, geografia).

Questa visione composita consente al management di considerare il tipo, la gravità e le interdipendenze dei rischi e come questi possono influire sulle prestazioni. L'organizzazione dovrebbe inizialmente comprendere il profilo di rischio potenziale quando valuta strategie alternative. Una volta scelta la strategia, l'attenzione si sposta verso la comprensione del profilo di rischio attuale per la strategia scelta e i relativi obiettivi di business.

Il rapporto tra rischio e performance raramente è lineare. Le variazioni incrementali degli obiettivi di performance non sempre si traducono in corrispondenti variazioni del rischio (o viceversa). Di conseguenza è utile una rappresentazione grafica che illustra l'ammontare aggregato del rischio associato ai diversi livelli di performance. Tale rappresentazione considera il rischio come un continuum di risultati potenziali lungo il quale l'organizzazione deve bilanciare l'ammontare del rischio per l'entità e la performance desiderata.

La rappresentazione utilizzata mostra la relazione tra i vari aspetti della gestione del rischio aziendale. In questo modo si contribuisce a migliorare l'analisi del rischio, la propensione al rischio, la tolleranza e il rapporto complessivo con gli obiettivi di performance.



Nella figura, ogni barra rappresenta l'ammontare aggregato del rischio per uno specifico livello di performance per un obiettivo aziendale. La linea Obiettivo rappresenta il livello di performance scelto dall'organizzazione nell'ambito della definizione della strategia (ad esempio: Per una società di consulenza che cerca di offrire nuovi servizi, aumentano i rischi associati alla ricerca ed al mantenimento delle competenze e dell'esperienza delle risorse specialistiche).

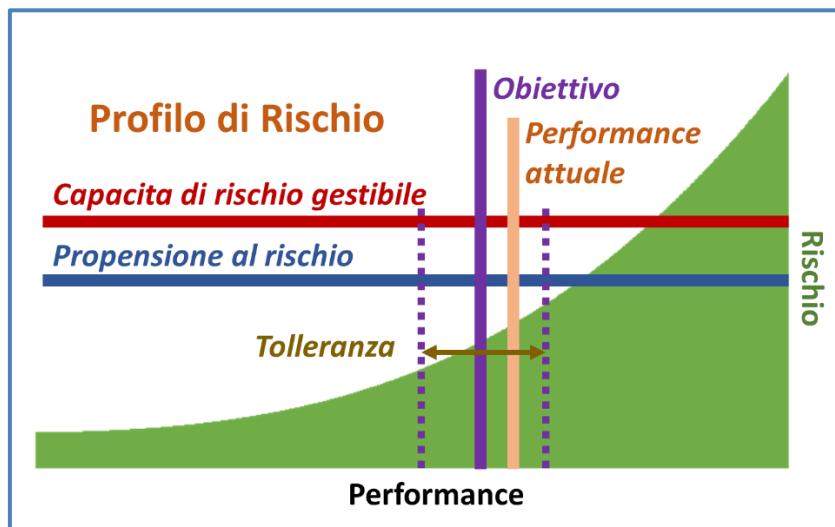
I profili di rischio aiutano il management a determinare quale sia la quantità di rischio accettabile e gestibile nel perseguitamento della strategia e degli obiettivi aziendali. I profili di rischio possono aiutare la gestione a:

- Comprendere il livello di performance nel contesto della propensione al rischio dell'entità (vedi Principio 7: Definire la propensione al rischio).
- Trovare il livello ottimale di performance data la capacità dell'organizzazione di gestire il rischio (vedi Principio 9: Formulare gli obiettivi di business).
- Determinare la tolleranza per la variazione delle prestazioni in relazione al target (vedi Principio 9: Formulare gli obiettivi di business).
- Valutare l'impatto potenziale del rischio su obiettivi prestabiliti (si veda il Principio 11: Valutare la gravità del rischio e il Principio 14: Sviluppare l'analisi del portafoglio).

Analizzare il contesto aziendale

Non esiste una propensione al rischio universale che si applica a tutte le entità.

Ogni organizzazione dovrebbe valutare la propria capacità di rischio, che è la quantità massima di rischio che è in grado di assorbire nel perseguitamento della strategia e degli obiettivi di business. La capacità di rischio deve essere presa in considerazione quando si stabilisce la propensione al rischio, in quanto generalmente un'organizzazione cerca di mantenere la propensione al rischio entro le proprie capacità.



L'organizzazione dovrebbe mantenere la propensione al rischio al di sotto della sua capacità di rischio.

La definizione della propensione al rischio dovrebbe permettere di individuare un equilibrio ottimale tra rischi e opportunità (crescita, rendimento) e dovrebbe riflettere la cultura dell'entità.

8.1.3 Le principali modifiche della versione 2017 rispetto a quella del 2004.

In linea con la sua missione generale, il CoSO Board ha commissionato e pubblicato nel 2004 “Enterprise Risk Management-Integrated Framework”. Nell'ultimo decennio, questa pubblicazione ha ottenuto un'ampia accettazione da parte delle organizzazioni nei loro sforzi per gestire il rischio. Tuttavia, anche in questo periodo, la complessità del rischio è cambiata, sono emersi nuovi rischi e sia i consigli di amministrazione che i dirigenti hanno aumentato la consapevolezza e il controllo della gestione del rischio aziendale, chiedendo al contempo una migliore comunicazione dei rischi. L'aggiornamento del 2017 affronta l'evoluzione della gestione del rischio aziendale e la necessità

per le organizzazioni di migliorare il loro approccio alla gestione del rischio per soddisfare le esigenze di un ambiente aziendale in evoluzione.

Il documento aggiornato, ora intitolato “Enterprise Risk Management - Integrating with Strategy and Performance”, evidenzia l’importanza di considerare il rischio sia nel processo di definizione della strategia che nella guida della performance.

Di seguito sono riportate alcune delle principali modifiche al quadro di riferimento²⁰:

- **Introduce una nuova struttura:** Con solo cinque componenti e venti principi allineati al ciclo di business, i principi chiave del Framework coprono processi che vanno dalla governance alle attività quotidiane. Sono gestibili in numero e applicabili a tutte le organizzazioni indipendentemente dalle dimensioni, dal tipo o dal settore e consentono una conversazione più completa sui rischi tra consiglio di amministrazione e direzione.
- **Esplora i diversi vantaggi dell'ERM:** il Framework presenta una chiara argomentazione a favore dell'integrazione delle pratiche di gestione del rischio aziendale con le pratiche di definizione delle strategie e di gestione delle prestazioni per contribuire a realizzare i benefici legati al valore. Concentrarsi su questi benefici migliora le conversazioni sul perché l'ERM è importante.
- **Si concentra sull'integrazione della gestione del rischio:** Il Framework offre una guida su come integrare meglio la gestione del rischio aziendale: collegando il rischio con la definizione della strategia e le attività quotidiane, integrandola nella cultura, nelle capacità e nelle pratiche di un'organizzazione e favorendo un migliore processo decisionale.
- **È scritto dal punto di vista degli affari:** Il linguaggio del Framework rende le conversazioni sul rischio rilevanti e universali, stabilendo definizioni, componenti e principi fondamentali per tutti i livelli di gestione coinvolti nella progettazione, implementazione e conduzione delle pratiche di ERM.
- **Dispone di una suite di nuova grafica:** Il Framework utilizza una nuova grafica concettuale. La grafica di base dà vita al rapporto tra la gestione del rischio e il modello di business. Altri grafici, come le curve di rischio, evidenziano le relazioni tra rischio, strategia e performance, integrando ulteriormente la gestione del rischio nelle conversazioni quotidiane.
- **Esplora la gestione del rischio a tutte le altitudini dell'organizzazione:** Dal livello di entità al livello di processo, il Framework esplora come l'identificazione, la valutazione e la gestione del rischio cambia dal transazionale a quello strategico.
- **Si immerge in discussioni più approfondite su argomenti impegnativi:** Il Framework esamina argomenti quali la propensione al rischio e la visione del rischio del portafoglio, e affronta alcune idee sbagliate che esistono oggi, fornendo una visione più approfondita.
- **Comprende una maggiore enfasi sulla cultura:** Il Framework esplora come le pratiche di gestione del rischio aziendale possono infondere maggiore trasparenza e consapevolezza del rischio nella cultura di un'organizzazione, aiutando le persone a prendere decisioni e comprendendo l'importanza della cultura nella formazione di tali decisioni.
- **Si rivolge all'evoluzione del ruolo della tecnologia dell'informazione:** Il Framework mette in luce come le tendenze di business, come la proliferazione di dati, l'intelligenza artificiale e l'automazione, influenzano la strategia di un'organizzazione, il contesto aziendale e la gestione del rischio.

²⁰ Tratte dalle note riportate sul sito PWC il 05 settembre 2017.

8.1.4 La gestione del rischio: qualche malinteso

Nel documento del 2017 sono stati evidenziati alcuni malintesi rilevati nell'utilizzo della versione 2004:

- **La gestione dei rischi aziendali non è una funzione o dipartimento.** È la cultura, le capacità e le pratiche che le organizzazioni integrano con la definizione della strategia e applicano quando attuano tale strategia, con lo scopo di gestire il rischio nella creazione, conservazione e realizzazione del valore.
- **La gestione del rischio d'impresa è più di un elenco dei rischi.** Richiede molto di più di un inventario di tutti i rischi all'interno dell'organizzazione. È più ampia e comprende le pratiche che il management mette in atto per gestire attivamente il rischio.
- **La gestione del rischio aziendale non si limita al controllo interno.** Essa affronta anche altri temi quali la definizione delle strategie, la governance, la comunicazione con le parti interessate e la misurazione delle prestazioni. I suoi principi si applicano a tutti i livelli dell'organizzazione e a tutte le funzioni.
- **La gestione dei rischi aziendali non è una lista di controllo.** È un insieme di principi sui quali i processi possono essere costruiti o integrati per una particolare organizzazione, ed è un sistema di monitoraggio, apprendimento e miglioramento delle prestazioni.
- **La gestione dei rischi aziendali può essere utilizzata da organizzazioni di qualsiasi dimensione.** Se un'organizzazione ha una missione, una strategia e obiettivi e la necessità di prendere decisioni che tengano pienamente conto del rischio, è possibile applicare la gestione del rischio aziendale. Può e deve essere utilizzato da tutti i tipi di organizzazioni, dalle piccole imprese alle imprese sociali a base comunitaria, dalle agenzie governative alle aziende Fortune 500.

8.1.5 Benefici connessi alla gestione del rischio aziendale

Tutte le organizzazioni devono definire la strategia e adeguarla periodicamente, rimanendo sempre consapevoli sia delle opportunità in continua evoluzione per la creazione di valore, sia delle sfide che si presenteranno nel perseguitamento di tale valore. A tal fine, hanno bisogno del miglior contesto possibile per ottimizzare la strategia e le prestazioni.

Le organizzazioni che integrano la gestione del rischio aziendale in tutta l'entità possono realizzare molti vantaggi, tra cui, ma non solo:

- **Aumentare la gamma di opportunità:** Considerando tutte le possibilità - sia gli aspetti positivi che negativi della gestione del rischio - la gestione del rischio può identificare nuove opportunità e sfide uniche associate alle opportunità attuali.
- **Identificazione e gestione del rischio a livello di impresa:** Ogni entità deve affrontare una miriade di rischi che possono influenzare molte parti dell'organizzazione. A volte un rischio può avere origine in una parte dell'entità ma avere un impatto su una parte diversa. Di conseguenza, il management identifica e gestisce questi rischi a livello di entità per sostenere e migliorare le prestazioni.
- **Aumentare i risultati positivi e i vantaggi e ridurre le sorprese negative:** La gestione del rischio d'impresa consente alle entità di migliorare la loro capacità di identificare i rischi e stabilire risposte adeguate, riducendo le sorprese e i relativi costi o perdite, traendo vantaggio da sviluppi vantaggiosi.
- **Ridurre la variabilità delle prestazioni:** Per alcuni, la sfida è meno con sorprese e perdite e più con la variabilità delle prestazioni. Esecuzione prima del previsto o al di là delle aspettative può causare tanta preoccupazione quanto l'esecuzione a corto di programmazione e le aspettative. La gestione dei rischi aziendali consente alle organizzazioni

di anticipare i rischi che incidono sulle prestazioni e di mettere in atto le azioni necessarie per ridurre al minimo le interruzioni e massimizzare le opportunità.

- **Miglioramento dell'impiego delle risorse:** Ogni rischio potrebbe essere considerato una richiesta di risorse. Ottenere solide informazioni sui rischi consente alla direzione, a fronte di risorse limitate, di valutare il fabbisogno complessivo di risorse, dare priorità all'impiego delle risorse e migliorare l'allocazione delle risorse.
- **Migliorare la resilienza delle imprese:** La redditività a medio e lungo termine di un'entità dipende dalla sua capacità di anticipare e rispondere ai cambiamenti, non solo per sopravvivere, ma anche per evolvere e prosperare. Ciò è in parte reso possibile da un'efficace gestione del rischio aziendale. Diventa sempre più importante man mano che il ritmo del cambiamento accelera e la complessità del business aumenta.

Questi benefici evidenziano il fatto che il rischio non deve essere considerato unicamente come un potenziale vincolo o una sfida alla definizione e all'attuazione di una strategia. Piuttosto, il cambiamento che è alla base del rischio e le risposte organizzative al rischio danno origine a opportunità strategiche e capacità di differenziazione chiave.

8.1.6 Il ruolo del rischio nella scelta della strategia

La scelta della strategia consiste nel fare scelte e accettare compromessi. Quindi ha senso applicare la gestione del rischio d'impresa alla strategia in quanto questo è l'approccio migliore per fare scelte ben informate.

Il rischio è spesso valutato principalmente in relazione al suo effetto potenziale su una strategia già definita. In altre parole, le discussioni si concentrano sui rischi per la strategia esistente ("Cosa potrebbe influire sulla pertinenza e la fattibilità della nostra strategia?").

Ma ci sono altre domande da porre sulla strategia, che le organizzazioni sempre più si pongono:

- Abbiamo modellato accuratamente la domanda dei clienti?
- La nostra catena di approvvigionamento consegnerà in tempo e nel rispetto del budget?
- Emergeranno nuovi concorrenti?
- La nostra infrastruttura tecnologica è all'altezza del compito?

Questo tipo di domande sono fondamentali per la realizzazione di una strategia.

Tuttavia, il rischio per la strategia scelta è solo uno degli aspetti da considerare. Ci sono due aspetti aggiuntivi alla gestione del rischio aziendale che possono avere un effetto molto maggiore sul valore di un'entità: la possibilità che la strategia non sia allineata con la missione aziendale e le implicazioni della strategia scelta.

Il primo di questi, **la possibilità che la strategia non sia in linea con la missione, la visione e i valori fondamentali di un'organizzazione**, è fondamentale per le decisioni che sono alla base della selezione della strategia. Ogni entità ha una missione, una visione e valori fondamentali che definiscono ciò che sta cercando di raggiungere e come vuole condurre gli affari. La missione, la visione e i valori fondamentali hanno dimostrato di essere importanti, e sono più importanti quando si tratta di gestire il rischio e di mantenere la capacità di resistenza durante i periodi di cambiamento.

Una strategia scelta deve sostenere la missione e la visione dell'organizzazione. Una strategia disallineata aumenta la possibilità che l'organizzazione non realizzi la sua missione e la sua visione, o possa compromettere i suoi valori, anche se una strategia viene portata a termine con successo. Pertanto, la gestione del rischio aziendale considera la possibilità che la strategia non sia in linea con la missione e la visione dell'organizzazione.

L'altro aspetto aggiuntivo sono **le implicazioni della strategia scelta**. Quando la direzione sviluppa una strategia e lavora attraverso alternative con il consiglio di amministrazione, prende decisioni sui compromessi inerenti alla strategia. Ogni strategia alternativa ha un proprio Profilo di Rischio. Il

vertice aziendale deve determinare se la strategia funziona in tandem con la propensione al rischio dell'organizzazione, e come aiuterà l'organizzazione a fissare gli obiettivi e, infine, ad allocare le risorse in modo efficiente.

La gestione del rischio aziendale, così come è stata tipicamente praticata, ha aiutato molte organizzazioni a identificare, valutare e gestire i rischi per la strategia. Ma le cause più significative di distruzione di valore sono radicate nella possibilità che la strategia non sostenga la missione e la visione dell'entità e le implicazioni della strategia.

La gestione del rischio d'impresa migliora la selezione delle strategie. La scelta di una strategia richiede un processo decisionale strutturato che analizza il rischio e allinea le risorse con la missione e la visione dell'organizzazione.

8.1.7 Possibili risposte al Rischio

Per tutti i rischi individuati, la direzione dovrà mettere in atto una risposta al rischio. Il management considera la gravità e l'ordine di priorità del rischio, nonché il contesto aziendale e i relativi obiettivi aziendali. Infine, la risposta al rischio tiene conto anche degli obiettivi di performance dell'organizzazione. Le risposte al rischio rientrano nelle seguenti categorie:

- *Accetta*: Non vengono intraprese ulteriori azioni per influire sulla gravità del rischio e il profilo di rischio rimane invariato. Questa risposta è appropriata quando la performance dell'entità e il rischio corrispondente sono al di sotto della soglia della propensione al rischio e all'interno delle linee che indicano una variazione accettabile della performance.
- *Evitare*: Vengono intraprese azioni per eliminare il rischio, che può significare la cessazione di una linea di prodotti, la diminuzione per espandersi in un nuovo mercato geografico o la vendita di una divisione. La scelta dell'evitamento suggerisce che l'organizzazione non è in grado di identificare una risposta che ridurrebbe l'impatto del rischio ad una gravità accettabile. La rimozione di un rischio tipicamente sposta la curva verso il basso e/o a sinistra con l'intento di avere la performance target a sinistra dell'intersezione della curva di rischio e della propensione al rischio.
- *Perseguire*: Si adotta un'azione che accetta un rischio maggiore per ottenere prestazioni migliori. Ciò può comportare l'adozione di strategie di crescita più aggressive, l'espansione delle operazioni o lo sviluppo di nuovi prodotti e servizi. Quando si sceglie di sfruttare il rischio, il management comprende la natura e l'entità delle modifiche necessarie per ottenere le prestazioni desiderate senza superare il rischio residuo target. In questo caso la curva di rischio può non cambiare, ma l'obiettivo può essere fissato ad un livello più alto, fissando quindi l'obiettivo in un punto diverso lungo la curva di rischio.
- *Ridurre*: Vengono intraprese azioni per ridurre la gravità del rischio. Ciò comporta una miriade di decisioni aziendali quotidiane che riducono il rischio residuo al profilo di rischio residuo e alla propensione al rischio dell'obiettivo. L'intento della risposta al rischio è quello di modificare l'altezza e la forma della curva, o sezioni applicabili della curva, per rimanere entro i limiti della propensione al rischio stabiliti per l'entità. In alternativa, per i rischi che rientrano già nella propensione al rischio, la risposta di riduzione può riguardare la riduzione della variabilità delle prestazioni attraverso l'impiego di risorse aggiuntive. L'effettiva riduzione di un rischio comporterebbe un appiattimento della curva di rischio per le sezioni interessate dalla risposta al rischio.
- *Condividi*: Si intraprendono azioni per ridurre la gravità di un rischio trasferendo o condividendo in altro modo una parte del rischio. Le tecniche comuni includono l'outsourcing a fornitori di servizi specializzati, l'acquisto di prodotti assicurativi e l'esecuzione di operazioni di copertura. Come per la risposta di riduzione, la condivisione del rischio riduce il rischio residuo in linea con la propensione al rischio. Una sezione della curva

di rischio può cambiare, anche se l'intera curva di rischio presenta somiglianze con una sezione in cui il rischio non è stato condiviso.

- *Rivedere l'obiettivo aziendale:* L'organizzazione sceglie di rivedere e potenzialmente rivedere l'obiettivo aziendale in considerazione della gravità dei rischi identificati e di variazioni accettabili delle prestazioni. Ciò può verificarsi quando le altre categorie di risposte al rischio non rappresentano le linee di azione desiderate per l'entità.
- *Rivedere la strategia:* L'organizzazione sceglie di rivedere e potenzialmente rivedere la strategia data la gravità dei rischi identificati e la propensione al rischio dell'entità. Analogamente alla revisione degli obiettivi aziendali, questo può verificarsi quando altre categorie di risposte al rischio non rappresentano le linee d'azione desiderate per l'entità. La revisione di una strategia, o l'adozione di una nuova strategia, richiedono anche lo sviluppo di un nuovo profilo di rischio.

Queste categorie di risposte al rischio richiedono che il rischio sia gestito nell'ambito del contesto aziendale, degli obiettivi aziendali, degli obiettivi di performance e della propensione al rischio dell'organizzazione. In alcuni casi, la direzione potrebbe dover prendere in considerazione un'altra linea d'azione, tra cui le seguenti:

- *Rivedere l'obiettivo aziendale:* L'organizzazione sceglie di rivedere e potenzialmente rivedere l'obiettivo aziendale in considerazione della gravità dei rischi identificati e della tolleranza. Ciò può verificarsi quando le altre categorie di risposte al rischio non rappresentano le linee di azione desiderate per l'entità.
- *Rivedere la strategia:* L'organizzazione sceglie di rivedere e potenzialmente rivedere la strategia data la gravità dei rischi identificati e la propensione al rischio dell'entità. Come nel caso di una revisione degli obiettivi aziendali, ciò può verificarsi quando altre categorie di risposte al rischio non rappresentano le linee d'azione desiderate per l'entità.

8.1.8 I Rischi connessi ai cambiamenti

Alcuni esempi di rischi legati ai cambiamenti dell'ambiente interno possono essere:

- *Crescita rapida:* Quando le operazioni si espandono rapidamente, le strutture esistenti, le attività aziendali, i sistemi informativi o le risorse possono essere interessati. I sistemi informativi potrebbero non essere in grado di soddisfare efficacemente le esigenze di informazione sui rischi a causa dell'aumento del volume delle transazioni. Potrebbe essere necessario ridefinire i ruoli e le responsabilità di controllo del rischio alla luce dei cambiamenti organizzativi e geografici dovuti a un'acquisizione. Le risorse possono essere tese fino al punto in cui le risposte al rischio e le azioni esistenti si rompono.
- *Innovazione:* Ogni volta che si introduce l'innovazione, sarà probabilmente necessario modificare le risposte ai rischi e le azioni di gestione. Ad esempio, l'introduzione di capacità di vendita attraverso dispositivi mobili può richiedere controlli di accesso specifici per tale tecnologia. Potrebbe essere necessaria una formazione per gli utenti. L'innovazione tecnologica può anche migliorare la gestione del rischio aziendale. Ad esempio, un nuovo sistema di utilizzo di dispositivi mobili che raccolga informazioni di vendita precedentemente non disponibili offre al management la possibilità di monitorare le prestazioni, prevedere le vendite potenziali e prendere decisioni in tempo reale sulle scorte.
- *Cambiamenti sostanziali nella leadership e nel personale:* Un cambiamento di gestione può influire sulla gestione del rischio aziendale. Un nuovo arrivato nel management può non comprendere la cultura dell'entità e può avere una filosofia diversa, o può concentrarsi esclusivamente sulle prestazioni, escludendo la propensione al rischio o la tolleranza.

8.1.9 Uno sguardo rivolto al futuro

Non c'è dubbio che le organizzazioni continueranno ad affrontare un futuro pieno di volatilità, complessità e ambiguità. La gestione del rischio d'impresa sarà una parte importante di come un'organizzazione gestisce e prospera in questi tempi. Indipendentemente dal tipo e dalle dimensioni di un'entità, le strategie devono rimanere fedeli alla loro missione. E tutte le entità devono mostrare caratteristiche che guidano una risposta efficace al cambiamento, tra cui l'agilità del processo decisionale, la capacità di rispondere in modo coeso e la capacità di adattamento per ruotare e riposizionarsi mantenendo elevati livelli di fiducia tra gli stakeholder.

Guardando al futuro, ci sono diverse tendenze che avranno un effetto sulla gestione del rischio aziendale. Solo quattro di queste sono:

- **Gestire la proliferazione dei dati:** Con l'aumentare del numero di dati disponibili e della velocità di analisi dei nuovi dati, la gestione del rischio aziendale dovrà adattarsi. I dati provengono sia dall'interno che dall'esterno dell'entità e saranno strutturati in modi nuovi. Gli strumenti avanzati di analisi e visualizzazione dei dati si evolveranno e saranno molto utili per comprendere il rischio e il suo impatto, sia positivo che negativo.
- **Sfruttare l'intelligenza artificiale e l'automazione:** Molti ritengono che siamo entrati nell'era dei processi automatizzati e dell'intelligenza artificiale. Indipendentemente dalle convinzioni individuali, è importante per le pratiche di gestione del rischio aziendale considerare l'impatto di queste e delle tecnologie future e sfruttarne le capacità. Relazioni, tendenze e modelli precedentemente irriconoscibili possono essere scoperti, fornendo una ricca fonte di informazioni critiche per la gestione del rischio.
- **Gestione del costo della gestione del rischio:** Una preoccupazione frequente espressa da molti dirigenti aziendali è il costo della gestione del rischio, dei processi di compliance e delle attività di controllo rispetto al valore guadagnato. Con l'evoluzione delle pratiche di gestione del rischio aziendale, diventerà importante che le attività che comprendono il rischio, la conformità, il controllo e persino la governance siano coordinate in modo efficiente per fornire il massimo beneficio all'organizzazione. Questo può rappresentare una delle migliori opportunità per la gestione del rischio aziendale per ridefinire la sua importanza per l'organizzazione.
- **Costruire organizzazioni più forti:** Man mano che le organizzazioni migliorano nell'integrare la gestione del rischio aziendale con la strategia e le prestazioni, si presenterà l'opportunità di rafforzare la resilienza. Conoscendo i rischi che avranno il maggiore impatto sull'entità, le organizzazioni possono utilizzare la gestione del rischio aziendale per aiutare a mettere in atto capacità che consentano loro di agire tempestivamente. Questo aprirà nuove opportunità.

In sintesi, la gestione del rischio aziendale dovrà cambiare e adattarsi al futuro per fornire in modo coerente i benefici delineati nel quadro di riferimento. Con la giusta attenzione, i benefici derivanti dalla gestione del rischio aziendale saranno di gran lunga superiori agli investimenti e daranno alle organizzazioni la fiducia nella loro capacità di gestire il futuro.

9 APPENDICE: Analisi dei Rischi 231

9.1 Introduzione

La presente Appendice è rivolta agli enti che non possono definire la propria complessità “standard” secondo quanto previsto dal Codice di Comportamento ANCE 2013 (Cfr. Analisi dei rischi, pag. 182-183) e che quindi non possono utilizzare direttamente l’analisi dei rischi effettuata da ANCE (identificazione dei reati applicabili e dei processi critici).

Finalità

Il sistema utilizzato per analizzare i rischi dell’Ente si fonda su un’analisi²¹ in grado di fornire obiettivi misurabili²² e quindi di attribuire un valore numerico al livello di rischio presente in azienda, e rendere l’insieme delle valutazioni il più oggettivo possibile ispirandosi a criteri prudenziali e all’adozione di parametri attendibili. I valori così determinati costituiscono la base su cui l’Organo Dirigente o l’OdV compie le proprie valutazioni sui rischi presenti in azienda e in generale sull’adeguatezza del sistema; i numeri identificati dal sistema quindi rappresentano un supporto ma non si sostituiscono ad un’attenta analisi da parte dell’Organo Dirigente o dell’OdV.

Principi per la gestione del rischio²³

Per far sì che la gestione del rischio sia efficace, un’organizzazione dovrebbe, a tutti i livelli, seguire i principi riportati qui di seguito.

La gestione del rischio crea e protegge il valore.

La gestione del rischio contribuisce in maniera dimostrabile al raggiungimento degli obiettivi ed al miglioramento della prestazione, per esempio in termini di salute e sicurezza delle persone, security²⁴, rispetto dei requisiti cogenti, consenso presso l’opinione pubblica, protezione dell’ambiente, qualità del prodotto gestione dei progetti, efficienza nelle operazioni, governance e reputazione.

La gestione del rischio è parte integrante di tutti i processi dell’organizzazione.

La gestione del rischio non è un’attività indipendente, separata dalle attività e dai processi principali dell’organizzazione. La gestione del rischio fa parte delle responsabilità della direzione ed è parte integrante di tutti i processi dell’organizzazione, inclusi la pianificazione strategica e tutti i processi di gestione dei progetti e del cambiamento.

La gestione del rischio è parte del processo decisionale.

La gestione del rischio aiuta i responsabili delle decisioni ad effettuare scelte consapevoli, determinare la scala di priorità delle azioni e distinguere tra linee di azione alternative.

La gestione del rischio tratta esplicitamente l’incertezza.

La gestione del rischio tiene conto esplicitamente dell’incertezza, della natura di tale incertezza e di come può essere affrontata.

La gestione del rischio è sistematica, strutturata e tempestiva.

Un approccio sistematico, tempestivo e strutturato alla gestione del rischio contribuisce all’efficienza ed a risultati coerenti, confrontabili ed affidabili.

²¹ Nel presente documento verrà utilizzata la terminologia riportata nella UNI ISO 31000 – Gestione del rischio.

²² Come previsto anche da ISO 9001, ISO 14001, OHSAS 18001.

²³ I seguenti principi, tratti dalla ISO 31000, sono citati nel Piano Nazionale Anticorruzione.

²⁴ Nota Nazionale: per “security” si intende la prevenzione e protezione per eventi in prevalenza di natura dolosa e/o colposa che possono danneggiare le risorse materiali, immateriali, organizzative e umane di cui un’organizzazione dispone o di cui necessità per garantirsi un’adeguata capacità operativa nel breve, nel medio e nel lungo termine.

La gestione del rischio si basa sulle migliori informazioni disponibili.

Gli elementi in ingresso al processo per gestire il rischio si basano su fonti di informazione quali dati storici, esperienza, informazioni di ritorno dai portatori d'interesse, osservazioni, previsioni e parere di specialisti. Tuttavia, i responsabili delle decisioni dovrebbero informarsi, e tenerne conto, di qualsiasi limitazione dei dati o del modello utilizzati o delle possibilità di divergenza di opinione tra gli specialisti.

La gestione del rischio è “su misura”.

La gestione del rischio è in linea con il contesto esterno ed interno e con il profilo di rischio dell'organizzazione.

La gestione del rischio tiene conto dei fattori umani e culturali.

Nell'ambito della gestione del rischio individua capacità, percezioni e aspettative delle persone esterne ed interne che possono facilitare o impedire il raggiungimento degli obiettivi dell'organizzazione.

La gestione del rischio è trasparente e inclusiva.

Il coinvolgimento appropriato e tempestivo dei portatori d'interesse e, in particolare, dei responsabili delle decisioni, a tutti i livelli dell'organizzazione, assicura che la gestione del rischio rimanga pertinente ed aggiornata. Il coinvolgimento, inoltre, permette che i portatori d'interesse siano opportunamente rappresentati e che i loro punti di vista siano presi in considerazione nel definire i criteri di rischio.

La gestione del rischio è dinamica.

La gestione del rischio è sensibile e risponde al cambiamento continuamente. Ogni qual volta accadono eventi esterni ed interni, cambiano il contesto e la conoscenza, si attuano il monitoraggio ed il riesame, emergono nuovi rischi, alcuni rischi si modificano e d altri scompaiono.

La gestione del rischio favorisce il miglioramento continuo dell'organizzazione.

Le organizzazioni dovrebbero sviluppare ed attuare strategie per migliorare la maturità della propria gestione del rischio insieme a tutti gli altri aspetti della propria organizzazione.

Definizione dei Rischi

Il sistema di valutazione del rischio parte dall'individuazione del Livello di Rischio [LR], ovvero il rischio in assenza di controllo, dal quale partire per arrivare a definire il Rischio Residuo [RR].

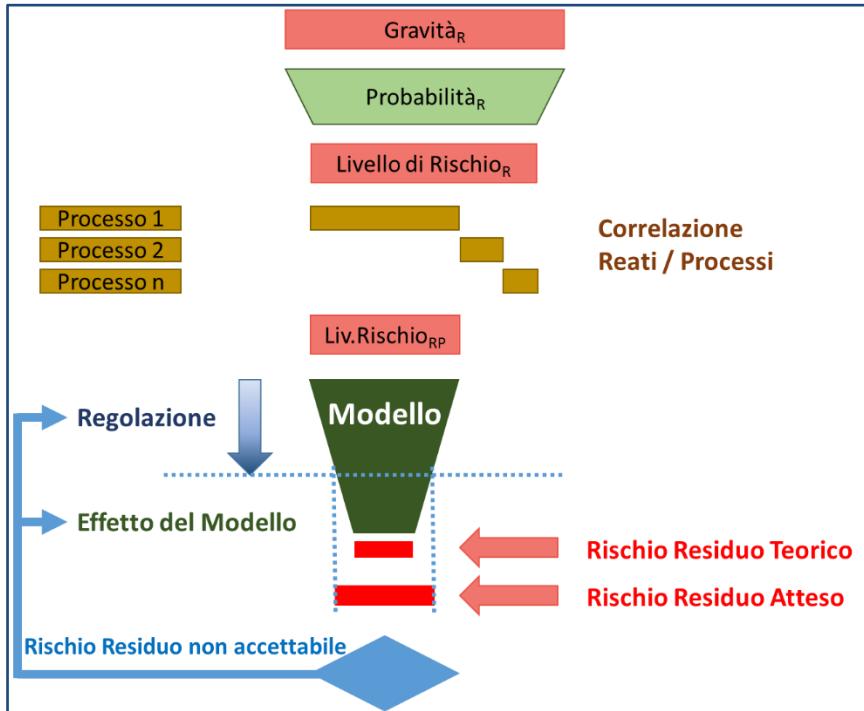
Il Livello di Rischio viene calcolato in relazione alla *gravità* del reato e alla *probabilità* che si verifichi lo specifico reato nell'Azienda (Livello di Rischio Aziendale). È quindi indipendente dal Modello applicato.

Viene quindi valutato il Rischio Residuo in funzione dell'applicazione del Modello di Organizzazione e Gestione.

Il Rischio Residuo si può distinguere in differenti valori. Un primo valore è il Rischio Residuo Teorico [RRT] che è il risultato della perfetta applicazione del Modello al Livello di Rischio.

Esiste poi il Rischio Residuo Atteso [RRA] in funzione della applicazione realistica del Modello in base al livello di Regolazione presente nell'Azienda ed in particolare nei vari Processi.

Il Modello deve infatti prevenire i reati nella sua probabile realistica applicazione e non solo nell'ipotetica applicazione perfetta del Modello.



Il Rischio Residuo Atteso dovrà essere ritenuto “accettabile” dall’Organo Dirigente dell’azienda. In caso contrario si dovrà agire per rendere più “stringente” il Modello (aggiungendo procedure di controllo – riducendo quindi il RRT) o dando maggiore Regolazione allo svolgimento delle Attività in oggetto (probabilità attesa di una applicazione conforme di tutte le procedure del Modello).

Il livello di conformità a quanto previsto nel Modello, osservato attraverso l’attività di audit effettuata dall’Organismo di Vigilanza, determinerà il Rischio Residuo Rilevato [RRR], ovvero il rischio che si stima essere presente. Se il livello di Conformità rilevato è minore del livello di Regolazione previsto il RRR sarà maggiore del RRT (e ritenuto accettabile).

Analisi delle Interviste

Nelle Note della presente Appendice viene fatto esplicito riferimento al Documento di Excel ottenibile da SQuadra231 da: Rischi / Analisi dei Rischi / Elabora Interviste.

9.2 Analisi degli Illeciti e dei Reati presupposto

Illeciti previsti dal D. Lgs 231/01

Il legislatore ha definito inizialmente gli illeciti negli articoli 24 e 25 del primo Decreto.

Successivamente ha aggiunto molti altri articoli ampliando il catalogo degli Illeciti 231 (oggi più di 20).

In genere ogni Articolo del Decreto può essere considerato un Illecito.

In due casi si è scelto di suddividere un Articolo del decreto in due Illeciti.

Illeciti relativi alla Sicurezza

I reati sulla sicurezza sono previsti dall’articolo 25-septies che risulta suddiviso in tre commi. Il primo prevede l’omicidio colposo in violazione dell’articolo 55 della legge 81/08 per cui sono previste 1000 quote, il secondo comma prevede l’omicidio colposo in violazione delle altre norme sulla sicurezza punito con un numero di quote variabile tra 250 e 500, infine l’ultimo comma punisce le lesioni colpose, sempre in violazione delle altre norme, con quote variabili tra le 100 e le 250.

Il primo comma avrà una correlazione diretta con il Processo della Sicurezza attraverso le Procedure che verificano la valutazione dei rischi e la nomina dell’RSPP da parte del Datore di Lavoro. Gli altri

due saranno correlati anche con le Procedure, presenti in altri Processi (ad esempio Approvvigionamento per la selezione dei fornitori o di Gestione delle Risorse Umane per la formazione del personale), che si occupano della sicurezza (a seconda della gravità dell'incidente si applicheranno le quote previste dal secondo o dal terzo comma ma le misure di prevenzione saranno sicuramente le stesse).

Illeciti relativi ai Reati Societari e Corruzione fra privati

È stato scelto di suddividere anche l'articolo 25-ter relativo ai reati societari in due Illeciti:

- Corruzione fra privati
- Altri reati societari

Sottoinsiemi di Illeciti

Per ogni Illecito il Legislatore ha richiamato vari gruppi di Reati per i quali ha previsto le differenti penne.

Per una facilità di lettura sono stati definite delle descrizioni per riunire gruppi di reati omogenei soprattutto dal punto di vista delle pene previste (oltre 60).

Reati presupposto

Ogni Illecito fa comunque esplicito riferimento a più Reati presupposto, in genere Articoli del Codice Penale (più di 200).

Per ogni Reato viene riportato il numero delle Quote (minime e massime) previste e, quando previsto, il numero di mesi (minimi e massimi) di interdizione.

In alcuni casi viene riportata anche una sintetica illustrazione del reato.

Gruppi di Reati omogenei dal punto di vista delle Azioni a rischio

Per la costruzione di un Modello di Organizzazione e Gestione non è tanto importante la suddivisione dei Reati presupposto per le pene previste ma per omogeneità rispetto alle possibili azioni a rischio.

Ad esempio, i commi 2 e 3 dell'articolo 25 septies prevedono pene differenti a seconda se, a seguito della “violazione delle norme sulla tutela della salute e sicurezza”, si verifica la morte o lesioni gravi per il lavoratore. In realtà le azioni a rischio e le misure per la prevenzione sono ovviamente le stesse.

L'Articolo 24 ter del D.Lgs. 231/01 (criminalità organizzata) e la legge 146/06 (reati transazionali) fano, spesso, riferimento agli stessi Reati presupposto.

Alcuni Reati previsti da differenti Illeciti possono essere affrontati con le stesse misure preventive; vedi, ad esempio il 640 ter c.p. (Frode informatica) richiamato dall'Art. 24 del Decreto che può trovare misure preventive analoghe a quelle previste per Reati presupposto richiamati dall'Art. 24 bis (Delitti informatici).

I vari Reati presupposto sono quindi stati riuniti in Gruppi omogenei rispetto alla Azioni a Rischio [d'ora in poi: “Gruppi di Reati”] (più di 50).

In genere non è possibile definire il Livello di Rischio per l'intero Illecito 231 ma è più corretto definirlo a livello dei Gruppi di Reati (si veda, ad esempio, l'Art. 25 undecies del Decreto (Reati ambientali) che sarà, in genere, applicabile per la “Gestione dei Rifiuti” ma solo raramente per “Danni all’ambiente provocati da Navi o Aeromobili”.

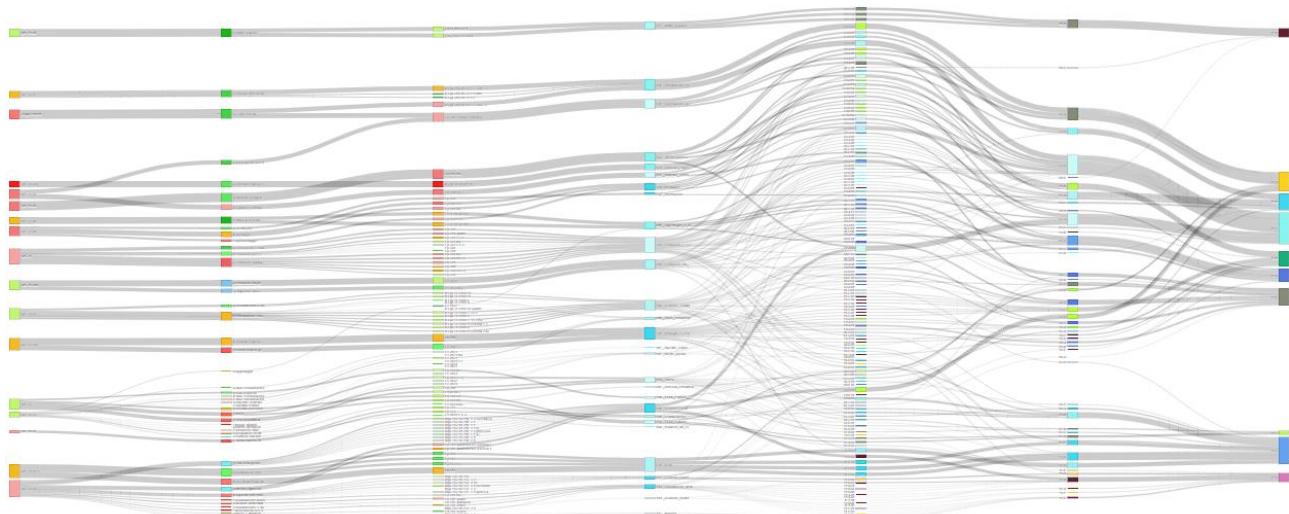
Famiglie di Reati

I vari Gruppi di Reato sono stati riuniti in 16 famiglie.

Azioni a rischio

Il Decreto richiede di “individuare le attività nel cui ambito possono essere commessi reati”. È possibile definire tutte le “azioni a rischio” per l’Ente.

Le Azioni a rischio sono riunite in Attività e Processi.



Da sinistra: Illeciti, Sotto illeciti (per sanzioni), Reati presupposto, Gruppi Reati omogenei, Azioni, Attività e Processi.

Governance

Ogni Modello, oltre a prevenire specifiche azioni a rischio di commissione di specifici reati, deve anche garantire una corretta Governance aziendale per la predisposizione di un efficace assetto organizzativo che adegui la struttura organizzativa dell’impresa ai fini del DLgs 231/01, riferito, in particolare alle attività/responsabilità macro-organizzative di stretta competenza del vertice aziendale coinvolgendo le attività specifiche degli amministratori (e in particolare di quelli dotati di deleghe), del direttore generale e degli eventuali institori con procure generali.

Le principali attività che costituiscono il processo di governance aziendale coincidono con la gestione dei sette strumenti organizzativi derivati dai “compliance programs” utilizzati negli Stati Uniti e richiamati dalla relazione di accompagnamento del DLgs 231/2001:

- Leadership e Governance
- Standard di comportamento
- Comunicazione
- Formazione
- Valutazione delle performance
- Controllo
- Reazione alle violazioni

Questi elementi sono analizzati, per uniformità, ricorrendo a Illeciti, Reati Presupposto e Gruppi omogenei di Reati “fittizi”.

Pericoli

Per ogni Gruppo Reati devono essere individuate le Attività a rischio ed indicate le possibili condotte negative che devono essere evitate dal modello (“Pericoli”).

Punti di Controllo

Per ogni “Pericolo” (come sopra descritto) devono essere individuati uno o più Punti di Controllo che costituiranno la base per il Modello di Organizzazione e Gestione.

9.3 Progettazione del Modello

9.3.1 Livello di Rischio

9.3.1.1 La Gravità

In ogni articolo del D.Lgs 231/01 (Illecito 231) che definisce i reati per i quali si applica la responsabilità amministrativa degli enti il legislatore ha differenziato le pene previste fra i vari commi dello stesso articolo che richiamano gli articoli del Codice Penale.

Il legislatore ha previsto pene che variano entro il range 100-1000 quote. Sempre il Legislatore ha previsto per quali commi dell’Illecito è possibile applicare l’interdizione. Nel valutare la Gravità di ogni gruppo di reati si è ritenuto corretto tenere in considerazione entrambi questi valori.

È opportuno considerare una media fra le quote massime e quelle le minime e considerare un valore fisso per i reati che prevedono la possibilità di interdizione²⁵.

Come è evidente il valore massimo è previsto per il primo Comma dell’Art.25.7 sulla Sicurezza che prevede, appunto quote minime e massime pari a 1.000 ed anche la possibilità dell’Interdizione [Gravità=10].

9.3.1.2 La Probabilità

Non è corretto valutare la probabilità che un Illecito (Articolo del Decreto) venga commesso all’interno dell’azienda visto che riunisce differenti tipologie di Reati presupposto. Come illustrato in precedenza sono stati predisposti dei Gruppi di Reati che riuniscono Reati presupposto “omogenei” dal punto di vista della commissione e per le misure opportune alla prevenzione.

Nello sforzo di garantire la maggior attendibilità possibile, nel questionario si chiede una valutazione, per ogni Gruppo di Reati, in merito a²⁶:

Effettività

L’eventuale presenza di eventi negativi nella storia dell’azienda con riferimento al Gruppo di Reati costituisce un effettivo fattore di rischio anche per il futuro.

²⁵ La formula utilizzata nel calcolo della gravità utilizza i PESI definiti dall’utente è la seguente (le Quote forniscono un valore massimo pari a 10 meno il valore che verrà aggiunto in caso di presenza dell’Interdizione):

$$\text{Gravità } [0 \div 10] = \text{Gravità_dalle_Quote} + \text{Gravità_Interdizione}$$

Dove Gravità_dalle_Quote è:

$$(\text{QuoteMax} * \text{PesoMax} + \text{QuoteMin} * \text{PesoMin}) / (\text{PesoMax} + \text{PesoMin}) / 1000 * (10 - \text{Gravità_Interdizione})$$

Vedi documento ANALISI: Foglio “Reati” colonna F.

²⁶ Probabilità = Funzione (Effettività, Possibilità, Fattori di Rischio)

Debbono essere considerati tutti gli eventi negativi (effettivi o potenziali) occorsi negli ultimi 5 anni, salvo il caso in cui agli stessi abbia fatto seguito un sostanziale riassetto organizzativo (cambio di management o miglioramento delle procedure). Nel valutare l'effettività "potenziale" è opportuno riferirsi anche a situazioni di pubblico dominio avvenute in aziende similari.

Per indicare una valutazione numerica omogenea relativamente alla effettività per i vari Gruppi di Reati è opportuno utilizzare come riferimento la seguente tabella:

0	<i>Nessun Precedente.</i>
3	<i>In presenza di potenziali precedenti che avrebbero potuto portare ad una pena lieve.</i>
7	<i>In presenza di potenziali precedenti che avrebbero potuto portare ad una pena significativa.</i>
10	<i>Precedenti effettivi.</i>

Possibilità

Potenziali benefici derivanti dall'illecito

La probabilità di un comportamento illecito è correlabile alla tipologia di organizzazione in funzione dell'attività che può dare origine al reato e al beneficio che può derivare dal comportamento illecito.

Per i Benefici che possono derivare dalla commissione dell'illecito utilizzare come riferimento la seguente tabella:

0	<i>Nessun Beneficio.</i>
3	<i>Potenziali benefici non molto significativi.</i>
7	<i>Potenziali benefici significativi sul piano economico o sul valore dell'azienda.</i>
10	<i>Potenziali benefici significativi sul piano economico e sul valore dell'azienda.</i>

Numero di Soggetti potenzialmente coinvolti

A parità del livello di controllo sul processo, una attività a rischio svolta frequentemente da molte persone diverse è più "pericolosa" della stessa attività svolta di rado da poche persone.

Per il Numero di Soggetti potenzialmente coinvolti nella commissione dell'illecito è possibile utilizzare la seguente tabella:

3	<i>Un solo ufficio (una sola persona per piccole imprese) nell'azienda può commettere l'illecito.</i>
7	<i>Pochi uffici (un numero ristretto e ben identificato di persone per piccole imprese) possono commettere l'illecito.</i>
10	<i>Tutto il personale ed i collaboratori possono commettere l'illecito.</i>

Frequenza delle operazioni a rischio.

Per indicare una valutazione numerica omogenea relativamente alla Frequenza delle operazioni a rischio di commissione dell'illecito è opportuno utilizzare come riferimento la seguente tabella:

1	<i>Operazioni con frequenza pluriennale.</i>
2	<i>Operazioni con frequenza annuale</i>
4	<i>Operazioni con frequenza semestrale.</i>
6	<i>Operazioni con frequenza trimestrale.</i>
8	<i>Operazioni con frequenza mensile.</i>
10	<i>Operazioni svolte quotidianamente</i>

Fattori di rischio aziendali

Un ultimo elemento che viene considerato per valutare la Probabilità sono i fattori di rischio a livello aziendale (Incentivi / pressioni, inclinazioni / giustificazioni, stato dei Sistemi Informativi, occasioni, mercato di riferimento, caratteristiche della Direzione, ecc.).

0%	<i>TRASCURABILI: Non esistono elementi di rischio aziendale.</i>
25%	<i>BASSI: Esistono pochi elementi di rischio aziendale solo in alcuni elementi.</i>
50%	<i>MEDI: Esistono pochi elementi di rischio ma su più elementi.</i>
75%	<i>ALTI: Esistono elementi significativi di rischio su alcuni elementi.</i>
100%	<i>MOLTO ALTI: Esistono elementi significativi di rischio su quasi tutti gli elementi.</i>

Calcolo della Probabilità

La media fra l'Effettività e la Possibilità ci fornisce una Probabilità BASE.

I Fattori di rischio fanno aumentare o diminuire la Probabilità complessiva. Non hanno effetto se uguali al 50%, migliorativi per valori più bassi e peggiorativi per valori più alti²⁷.

9.3.1.3 Il calcolo del Livello di Rischio

La gravità e la probabilità concorrono alla determinazione del Livello di Rischio per Gruppo di Reati.

Per quanto riguarda il valore della probabilità si è scelto di seguire una logica prudenziale.

Per valori di probabilità 0% (reati che non possono essere commessi all'interno dell'impresa) il rischio sarà 0, così come per probabilità 100% il rischio sarà massimo (uguale alla Gravità).

Per tutti i valori intermedi si è scelta la via più cautelativa per l'impresa (rappresentata dalla curva verde nella figura successiva) che prevede di considerare anche per bassi gradi di probabilità un Livello di Rischio relativamente rilevante²⁸. Come si può vedere con una Probabilità del 30% il Livello di Rischio sarà pari ad oltre il 50% della Gravità; con una Probabilità del 70% il Livello di Rischio sarà pari ad oltre il 90% della Gravità.

Gli Illeciti 231 racchiudono più Gruppi di Reati²⁹.

Per ogni Illecito viene considerato il Livello di Rischio massimo fra quelli calcolati per i Gruppi di Reati racchiusi.

Al di là delle valutazioni numeriche derivanti dall'analisi delle interviste l'Ente può determinare in modo soggettivo il Livello di Rischio per ogni Illecito³⁰.

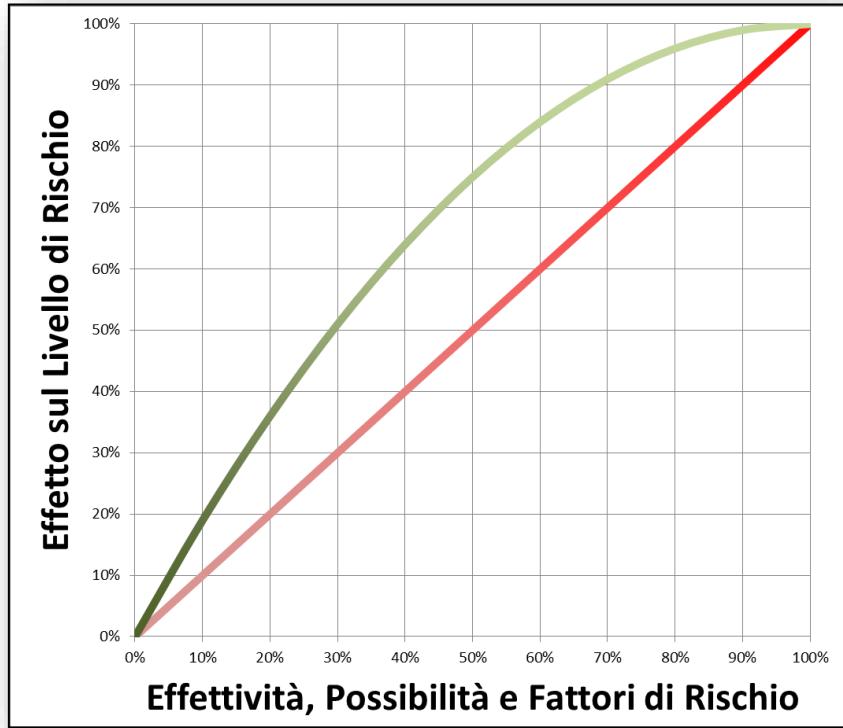
²⁷ Probabilità_{BASE} = (Effettività * Pe + Benefici * Pb + Soggetti * Ps + Frequenza * Pf)/(Pe+Pb+Ps+PF)
Probabilità = Probabilità_{BASE} x (1 + (Fattori Rischio – 50%)) [per valori > 100% si considera il 100%]
Vedi documento ANALISI: Foglio “GR_Reati” colonna K.

²⁸ Si è scelto di utilizzare il quadrato del valore residuo, ovvero la seguente formula:
Livello di Rischio(aziendale)=Gravità x (1-(1-Probabilità)²).

Vedi documento ANALISI: Foglio “GR_Reati” colonna L.

²⁹ Vedi documento ANALISI: Foglio “El_GR_Illeciti”.

³⁰ Vedi documento ANALISI: Foglio “Illeciti”.



La correlazione permette di distribuire il Livello di Rischio dei vari Gruppi di Reati tra i diversi Processi per ottenere il Livello di Rischio per Reato/Processo.

9.3.2 La Regolazione

La regolazione indica la stima della capacità di attuare correttamente il Modello.

La valutazione viene richiesta su una scala di dieci punti e sulla base di alcuni precisi parametri, affinché tutti gli intervistati si concentrino e si basino sugli stessi criteri, nel momento in cui sono chiamati ad esprimere un giudizio soggettivo. La valutazione sulla regolazione viene chiesta in riferimento sia all'intera organizzazione aziendale, sia in merito alle funzioni svolte dall'intervistato.

9.3.2.1 Requisiti Organizzativi aziendali

Le valutazioni sulla regolazione aziendale vengono raccolte per i 5 requisiti (nei quali sono suddivisi i 17 principi previsti dal COSO³¹ Internal Control – Integrated Framework - 2013) di seguito riassunti con anche l'indicazione di alcune situazioni di riferimento da utilizzare per assegnare una valutazione numerica omogenea ai vari punti (valori riportati in corsivo)³².

Principi del COSO Internal Control – Integrated Framework



COSO: Committee of Sponsoring Organizations of the Treadway Commission
Report – 2013

³¹ Committee of Sponsoring Organizations of the Treadway Commission (per maggiori informazioni visitare www.coso.org).

³² Nel mediare le valutazioni aziendali si tiene conto del ruolo aziendale (la direzione vale il doppio rispetto ad un Responsabile di Area e questa il doppio rispetto di un addetto).

Vedi documento ANALISI: Foglio “Interviste” riga 2 colonne da F a J. In K è riportata la media.

Ambiente di controllo

1. L'organizzazione dimostra il proprio impegno rispetto ai valori etici e all'integrità.
2. Il CdA è indipendente rispetto al Management ed esercita la propria supervisione sullo sviluppo e sull'implementazione del sistema del controllo interno.
3. Il Management definisce, sotto la supervisione del CdA, la struttura organizzativa, le linee di riporto, i livelli autorizzativi e le responsabilità funzionali al fine di perseguire gli obiettivi aziendali.
4. L'organizzazione dimostra il proprio impegno ad attrarre, sviluppare e trattenere risorse competenti, in linea con il conseguimento degli obiettivi aziendali.
5. L'organizzazione, nel raggiungimento degli obiettivi aziendali, ritiene i singoli individui responsabili per la parte di sistema di controllo interno di propria competenza.

Descrizione

Sensibilità dei vertici aziendali verso la definizione degli strumenti principali: formalizzazione di ruoli, compiti e responsabilità (poteri delegati, regolamenti interni, funzionigrammi, separatezza funzionale); sistema di comunicazione interna (scadenzatura delle informazioni necessarie e tempistiche di produzione di flussi e report, tempestività delle informazioni direttive, sensibilità e ricettività da parte delle strutture operative).

Valutazione periodica della adeguatezza dell'ambiente di controllo per la prevenzione dei reati.

Consapevolezza dell'importanza del controllo da parte di chi opera per l'organizzazione.

L'ambiente di controllo costituisce il fondamento di un efficace controllo interno definendone disciplina e organizzazione.

Elementi chiave

- Comunicazione e vigilanza su valori etici e integrità.
- Considerazione dell'importanza del controllo.
- Filosofia e stile operativo della direzione.
- Struttura organizzativa.
- Attribuzione di autorità e responsabilità.
- Politiche e procedure in tema di risorse umane.

6	<i>Esiste un sistema di deleghe tale da assicurare una puntuale determinazione di responsabilità e competenze nel processo aziendale di formazione ed attuazione delle decisioni.</i>
8	<i>Sono state individuate le attività nel cui ambito possono essere commessi reati e sono stati definiti specifici protocolli (correlati ad un preciso sistema di deleghe) diretti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire.</i>
9	<i>Oltre ad i protocolli di cui al punto precedente sono state definite anche le modalità di gestione delle risorse finanziarie e gli obblighi di informativa all'organismo di controllo.</i>
10	<i>È stato predisposto ed approvato dall'organo dirigente un modello di prevenzione dei reati coerente con le linee guida predisposte dall'associazione di categoria e ritenute idonee dal Ministero.</i>

Valutazione del rischio

6. L'organizzazione esplicita con sufficiente chiarezza i propri obiettivi, consentendo l'identificazione e la valutazione dei rischi ad essi legati.
7. L'organizzazione identifica i rischi connessi al conseguimento degli obiettivi aziendali e ne determina le modalità di gestione.
8. L'organizzazione prende in considerazione potenziali frodi nel valutare i rischi di conseguimento dei propri obiettivi aziendali.
9. L'organizzazione identifica e valuta i cambiamenti che potrebbero avere impatti significativi sul sistema di controllo interno.

Descrizione

La gestione dei rischi è un processo continuo di identificazione e analisi di quei fattori endogeni ed esogeni che possono coinvolgere l'organizzazione ad essere coinvolta nella commissione di reati, al fine di determinare come questi rischi possono essere gestiti (identificazione, misurazione e monitoraggio).

Elementi chiave

Capacità di rispondere a:

- Cambiamenti nell'ambiente operativo.
- Inserimento di nuovo personale.
- Sistemi informativi nuovi e aggiornati.
- Nuovi prodotti, nuove attività.
- Ristrutturazioni aziendali.

6	<i>È stato definito un Modello di Organizzazione e Gestione che descrive le modalità operative per la prevenzione dei reati.</i>
8	<i>È stato nominato un Organismo di Vigilanza per verificare la corretta applicazione del Modello.</i>
10	<i>È stato nominato un Organismo di Vigilanza dotato di ampi poteri e risorse.</i>

Attività di controllo

10. L'organizzazione definisce e implementa attività di controllo che contribuiscono a ridurre i rischi entro livelli accettabili.
11. L'organizzazione definisce e implementa attività di controllo sulla tecnologia, per supportare il raggiungimento degli obiettivi aziendali.
12. L'organizzazione declina le attività di controllo in politiche che definiscono i comportamenti attesi e in procedure che ne determinano le modalità operative di applicazione.

Descrizione

Modalità con cui vengono disegnati, strutturati ed effettivamente eseguiti i controlli ai diversi livelli organizzativi (di linea/operativi, gerarchico-funzionali, sulla gestione dei rischi e di revisione interna), necessari a garantire al vertice aziendale la corretta applicazione delle direttive impartite.

Le attività di controllo sono le direttive e le procedure che aiutano a garantire che le indicazioni della direzione siano eseguite.

Elementi chiave

- Esami della performance.
- Elaborazioni informatiche.
- Controlli fisici.
- Separazione delle funzioni.

6	<i>Vengono effettuati controlli occasionali sui processi principali.</i>
8	<i>Vengono effettuati controlli sistematici su tutti i processi.</i>
10	<i>Vengono effettuati controlli sistematici su tutti i processi da parte di personale qualificato, sia interno che esterno, per le attività di audit.</i>

Informazione e comunicazione

13. L'organizzazione ottiene o genera e utilizza informazioni rilevanti e di qualità a supporto del funzionamento del sistema di controllo interno.
14. L'organizzazione comunica internamente le informazioni, compresi gli obiettivi e le responsabilità di controllo interno, necessarie a supportare il funzionamento del sistema nel suo complesso.
15. L'organizzazione comunica con parti terze relativamente a questioni che interessano il funzionamento del sistema di controllo interno.

Descrizione

Valutazione della integrità e della completezza dei dati e delle informazioni, al fine di garantire la gestione e controllo di tutti i processi e attività aziendali.

La comunicazione permette di comprendere i ruoli e le responsabilità individuali pertinenti al controllo interno; può assumere diverse forme, quali manuali sulle procedure, e comunicazioni interne. La comunicazione può avvenire anche elettronicamente, verbalmente e attraverso le azioni della direzione.

Elementi chiave

Un sistema informativo comprende metodi e registrazioni che:

- Individuano e registrano tempestivamente tutte le operazioni significative.
- Descrivono le operazioni in modo sufficientemente dettagliato da permettere una corretta analisi delle informazioni.
- Presentano in modo corretto tutte le informazioni.

6	<i>Le informazioni principali vengono registrate in base a specifiche procedure o prassi consolidate.</i>
8	<i>Le informazioni relative alle attività più significative sono gestite tramite appositi strumenti informatici che mantengono evidenza delle operazioni svolte.</i>
10	<i>Le informazioni relative alle attività significative sono gestite tramite appositi strumenti informatici che mantengono evidenza delle operazioni svolte mantenendo traccia dei cambiamenti apportati.</i>

Attività di monitoraggio

16. L'organizzazione definisce, sviluppa ed esegue valutazioni continuative e ad hoc per accertare che le componenti del sistema di controllo interno siano presenti e funzionanti.
17. L'organizzazione valuta e comunica tempestivamente le carenze del sistema di controllo interno ai soggetti responsabili di intraprendere le necessarie azioni correttive, incluso il Senior Management e il CdA per quanto necessario e di competenza.

Descrizione

Capacità dei referenti aziendali di presidiare in modo continuativo il sistema di controllo interno, nonché di identificare e realizzare gli interventi migliorativi necessari a risolvere le criticità rilevate, assicurando mantenimento, aggiornamento e miglioramento del sistema di controllo.

Il monitoraggio dei controlli richiede di valutare se i controlli stiano operando come programmato e se siano stati modificati in modo appropriato al variare delle condizioni esterne ed interne.

Elementi chiave

Il monitoraggio dei controlli è realizzato attraverso attività di verifica continuative, valutazioni separate o una combinazione delle due.

6	<i>Esiste un piano di audit per i processi principali. Vengono registrate e gestite le eventuali non conformità rilevate.</i>
8	<i>Funzioni specifiche sono incaricate di svolgere con sistematicità audit su tutti i processi. Qualora l'organizzazione scopra una violazione al modello organizzativo viene condotta una indagine e vengono attuate misure correttive.</i>
10	<i>L'Organismo di Vigilanza controlla con continuità la corretta applicazione del Modello di Organizzazione e Gestione. Qualora l'organizzazione scopra una violazione al modello organizzativo viene condotta una rapida e completa indagine, di cui viene conservata adeguata documentazione, e vengono attuate misure correttive individuando la causa del problema ed eventualmente modificando i processi ed i controlli esistenti allo scopo di evitare che la violazione possa ripetersi in futuro.</i>

9.3.2.2 Regolazione per le funzioni svolte

Al fine di individuare il livello di regolazione in riferimento alle attività svolte dall'intervistato, si fa riferimento a parametri calibrati espressamente sulla necessità di valutazione del livello di organizzazione di una singola funzione aziendale, piuttosto che dell'intera organizzazione, come di seguito individuati.

Elementi di analisi di sintesi per le Funzioni

Procedurizzazione	
Esiste una procedura scritta che disciplina tutte le fasi dell'attività sia per gli aspetti tecnici o amministrativi che per gli aspetti deontologici e comportamentali.	
6	<i>Esiste una prassi consolidata alla quale si rifanno tutti gli operatori coinvolti nell'attività.</i>
8	<i>Esiste una procedura scritta che descrive nel dettaglio le modalità operative secondo le quali deve essere svolta l'attività.</i>
10	<i>La procedura che descrive l'attività viene periodicamente revisionata.</i>
Conoscenza	
Ogni operatore è in grado di spiegare con facilità le procedure di propria competenza. La conoscenza delle procedure rientra nei criteri di valutazione delle performance.	
6	<i>Gli operatori sono, in genere, in grado di spiegare le procedure di propria competenza.</i>
8	<i>Ogni operatore è in grado di spiegare con facilità le procedure di propria competenza.</i>
10	<i>La conoscenza delle procedure rientra nei criteri di valutazione delle performance.</i>
Applicazione	
La procedura è applicabile nella quasi totalità dei casi e sono comunque previste indicazioni per la gestione delle eccezioni.	
6	<i>La procedura è generalmente applicabile o le prassi coprono molte casistiche.</i>
8	<i>La procedura o le prassi aziendali sono applicabili nella quasi totalità dei casi.</i>
10	<i>Le procedure sono applicate nella totalità dei casi essendo previste indicazioni per la gestione delle eccezioni.</i>
Comunicazione	
La procedura viene comunicata in maniera autorevole al nuovo personale prima dell'inizio delle attività alle quali si riferisce e vengono comunicate immediatamente le variazioni. Le Procedure devono essere facilmente accessibili per gli interessati.	
6	<i>Le procedure devono essere facilmente accessibili per gli interessati o le prassi sono note a tutti.</i>
8	<i>Le procedure vengono comunicate al nuovo personale prima dell'inizio delle attività alle quali si riferiscono.</i>
10	<i>Le procedure vengono comunicate in maniera autorevole al nuovo personale prima dell'inizio delle attività alle quali si riferiscono e vengono comunicate immediatamente le variazioni.</i>
Aggiornamento	
La procedura deve essere aderente all'effettiva attività alla quale si rivolge. Devono essere previste le cause che ne richiedono un aggiornamento.	
6	<i>Le procedure sono aderenti all'effettiva attività alle quali si rivolgono.</i>
8	<i>Le procedure vengono periodicamente revisionate per garantire che siano aderenti all'effettiva attività alle quali si rivolgono.</i>
10	<i>Sono previste espressamente le cause che richiedono aggiornamenti delle procedure.</i>
Controllo	
Deve essere prevista una attività di ispezione e, in caso di non applicazione deve essere previsto un sistema disciplinare.	
6	<i>Sono previste visite ispettive sullo svolgimento delle attività.</i>
8	<i>Sono previste periodiche Verifiche Ispettive sul rispetto delle Procedure previste per l'attività.</i>
10	<i>Qualora nella periodica attività di ispezione si rilevino Non Conformità causate dal non rispetto delle Procedure è prevista l'applicazione di un sistema disciplinare.</i>

9.3.2.3 Regolazione complessiva

I dati così raccolti vengono elaborati al fine di ottenere la valutazione del livello di *regolazione* dei Processi aziendali, aggregando i valori relativi alle risposte sulla propria funzione³³.

Per utilizzare le due valutazioni (sull'intera organizzazione e sui singoli processi) si è scelto, in via cautelativa, di non effettuare la Media ma il Prodotto³⁴. Si suppone infatti una forte correlazione fra i due elementi e che:

- In una azienda totalmente priva di Requisiti Organizzativi a livello aziendale nessun Processo possa essere Regolato.
- Se un Processo è privo di Regolazione questa non può arrivare dai Requisiti Organizzativi generali.

9.3.3 Pericoli

Ogni Intervistato ha potuto valutare i Pericoli proposti ed aggiungerne di sua iniziativa³⁵.

In via cautelativa vengono considerati tutti i Pericoli presenti nelle varie interviste considerando il Livello massimo³⁶.

Vengono evidenziate situazioni anomale³⁷:

- Pericoli non “coperti” da nessun Punto di Controllo.
- Azioni a Rischio per le quali non è previsto nessun Pericolo.
- Gruppi di Reati ritenuti significativi ma per i quali non è previsto nessun Pericolo.

9.3.4 Correlazione

L'analisi dei Pericoli permette di individuare la correlazione fra gli Illeciti ed i Processi cioè la probabilità che, in caso di commissione di un particolare Illecito, la causa sia connessa ad un particolare Processo.

La correlazione permette quindi di scomporre il Livello di Rischio Aziendale nei Livelli di Rischio per vari Processi potenzialmente coinvolti³⁸.

9.3.5 Rischio Residuo Teorico

La definizione di un Modello ha lo scopo di portare il Livello di Rischio al Rischio Residuo Teorico.

In assenza di Punti di controllo specifici il Rischio Residuo sarà pari al Livello di Rischio.

³³ Nel mediare le valutazioni aziendali si tiene conto del coinvolgimento nel Processo dell'intervistato.

Vedi documento ANALISI: Foglio “Processi” colonne da E a J. Nella colonna K è riportata la media che viene utilizzata per i calcoli e riportata nel Foglio “Analisi” nella riga 3 nelle colonne da F a O.

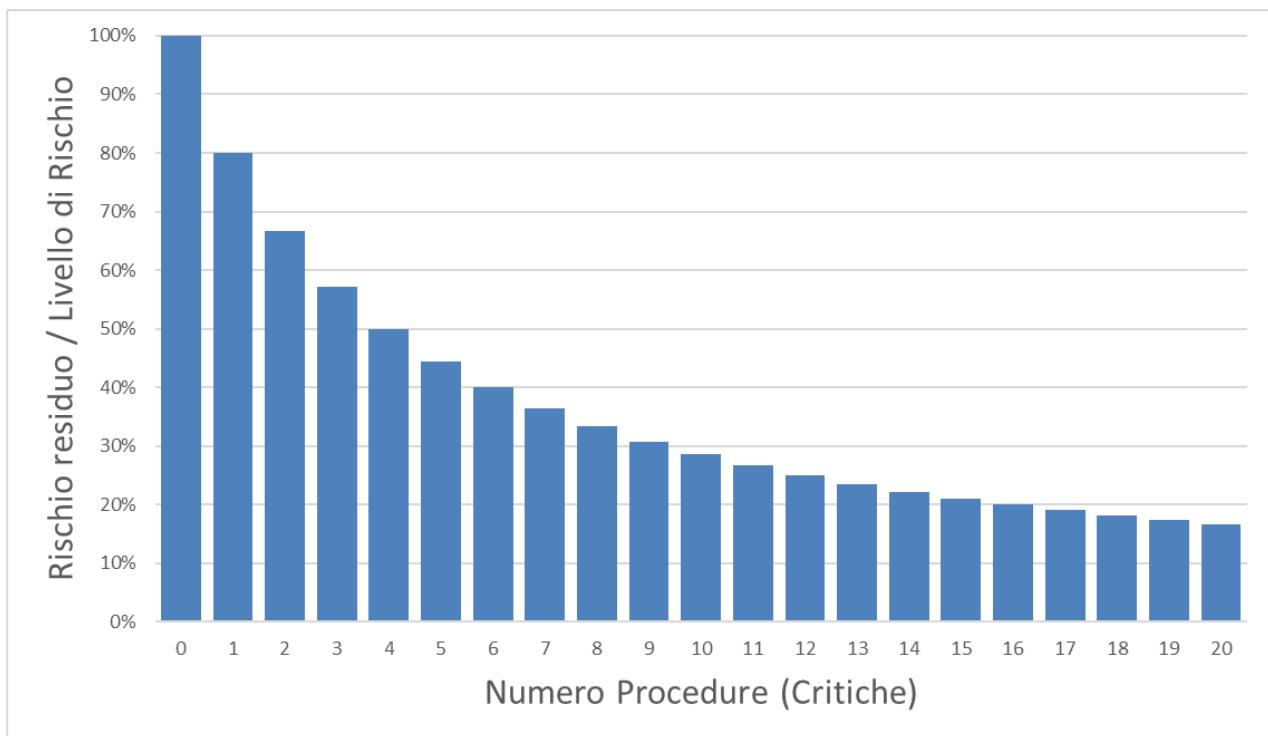
³⁴ Vedi documento ANALISI: Foglio “Analisi” nella riga 4 nelle colonne da F a O.

³⁵ Vedi documento ANALISI: Foglio “Pericoli_Int”.

³⁶ Vedi documento ANALISI: Foglio “Pericoli”.

³⁷ Vedi documento ANALISI: Foglio “Pericoli_NO”.

³⁸ Vedi documento ANALISI: Foglio “Analisi” nelle righe dei vari Reati nelle colonne da F a O.



Maggiore sarà il numero dei Punti di controllo previsti e delle relative Procedure maggiore sarà l'effetto di attenuazione del rischio connesso al Modello anche se il Rischio Residuo non si potrà mai annullare³⁹.

L'analisi viene effettuata a livello di Reato / Processo⁴⁰.

Ovviamente eventuali Punti di Controllo presenti in Processi dove non si ritiene possa essere commesso l'Illecito non hanno effetto sull'efficacia del Modello per lo specifico Illecito.

9.3.6 Il calcolo del Rischio Residuo Atteso

In presenza di una Regolazione completa il Rischio Residuo Atteso coinciderà con il Rischio Residuo Teorico.

In assenza di Regolazione l'effetto del Modello sarà nullo e quindi il Rischio Residuo Atteso sarà identico al Livello di Rischio.

È quindi corretto considerare che la Regolazione agisca sull'efficacia dei vari Punti di controllo (totalmente validi per Regolazione=100% e totalmente inutili per Regolazione=0%)⁴¹.

Nella figura seguente viene indicato il rapporto fra Rischio Residuo Atteso e Livello di Rischio.

³⁹ Si è scelta la formula: Rischio Residuo Teorico = Livello di Rischio / (1+ Numero Punti di controllo Critici/4)..

⁴⁰ Nel documento ANALISI, nel Foglio “Analisi” nelle colonne Q-Z vengono riportati i Punti di Controllo “Critici” (gli altri vengono considerati pari a 0,5). Nelle colonne AB-AK viene riportata la quota di Livello di Rischio per il Processo (colonna D per colonne F-O) diviso per (1+colonne Q-Z /4). Nella colonna AL viene riportato il Rischio Teorico.

⁴¹ Rischio Residuo Atteso = Livello di Rischio / (1 + Numero Punti di controllo x Regolazione/4).

Vedi documento ANALISI: Foglio “Analisi” colonne AM-AV riepilogate nella colonna AW.

I dati sono riportati nel Grafico “G_Analisi”.

		Numero Punti di controllo																				
		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Regolazione	100%	100%	80%	67%	57%	50%	44%	40%	36%	33%	31%	29%	27%	25%	24%	22%	21%	20%	19%	18%	17%	
	90%	100%	82%	69%	60%	53%	47%	43%	39%	36%	33%	31%	29%	27%	25%	24%	23%	22%	21%	20%	19%	18%
	80%	100%	83%	71%	63%	56%	50%	45%	42%	38%	36%	33%	31%	29%	28%	26%	25%	24%	23%	22%	21%	20%
	70%	100%	85%	74%	66%	59%	53%	49%	45%	42%	39%	36%	34%	32%	31%	29%	28%	26%	25%	24%	23%	22%
	60%	100%	87%	77%	69%	63%	57%	53%	49%	45%	43%	40%	38%	36%	34%	32%	31%	29%	28%	27%	26%	25%
	50%	100%	89%	80%	73%	67%	62%	57%	53%	50%	47%	44%	42%	40%	38%	36%	35%	33%	32%	31%	30%	29%
	40%	100%	91%	83%	77%	71%	67%	63%	59%	56%	53%	50%	48%	45%	43%	42%	40%	38%	37%	36%	34%	33%
	30%	100%	93%	87%	82%	77%	73%	69%	66%	63%	60%	57%	55%	53%	51%	49%	47%	45%	44%	43%	41%	40%
	20%	100%	95%	91%	87%	83%	80%	77%	74%	71%	69%	67%	65%	63%	61%	59%	57%	56%	54%	53%	51%	50%
	10%	100%	98%	95%	93%	91%	89%	87%	85%	83%	82%	80%	78%	77%	75%	74%	73%	71%	70%	69%	68%	67%
	0%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%

9.3.7 Gap Analysis

Se per ogni Procedura è stato definito lo “scarto” fra la situazione attuale e quella prevista dal Modello è possibile ottenere una analisi di riepilogo e quanto questo può influenzare sul raggiungimento del Livello di Rischio residuo atteso⁴².

9.4 Adeguatezza del Modello

Nel caso in cui il Rischio Residuo Atteso per alcuni Reati non venga ridotto ad un livello soddisfacente e dunque il sistema non risulti adeguato, è necessario intervenire incrementando il numero di procedure e/o la formazione e l’organizzazione del personale addetto alle attività in questione, ovvero agendo sui due elementi (Modello e Regolazione).

Una Procedura di controllo prevista in un ambiente con un’ottima regolazione può ridurre il rischio del 99%. Avremo quindi un Rischio Residuo pari all’1%.

Lo stesso risultato si può ottenere in un ambiente con regolazione media che può ridurre il rischio, ad esempio, del 90% se, invece di una Procedura, ne inseriamo 2 indipendenti. In questo caso la prima Procedura porta ad un Rischio Residuo al 10%. La seconda Procedura, applicato al Rischio Residuo risultante dall’applicazione della prima Procedura, porterà il Rischio Residuo complessivo di nuovo all’1% (10% del 10%).

In generale con una regolazione in cui sia “P” la probabilità di rispettare correttamente il Modello con “N” Procedure indipendenti avremo un Rischio Residuo pari a: $(1-P)^N$ e quindi un efficacia del Modello pari a: $1-(1-P)^N$.

Banalizzando: per ridurre il rischio di furto è analogo mettere una cassaforte o 2 porte blindate da aprire in successione.

⁴² Vedi documento “ANALISI”: Foglio “Gap_Analysis” e Grafico “G_GAP”

10 APPENDICE: Rischio Residuo Rilevato

10.1 Introduzione

La registrazione delle attività di formazione sul Modello 231 e sulle specifiche responsabilità in esso previste per i vari responsabili (con la relativa accettazione delle nomine) e la registrazione dei livelli di conformità rilevati negli audit svolti dall’OdV consentono di stimare il livello di conformità nell’applicazione del modello previsto, con il fine ultimo di valutare l’intero sistema e l’accettabilità del livello di Rischio Residuo eventualmente ancora presente.

I valori numerici che emergono da tale analisi supporteranno i giudizi espressi dall’OdV, fondati anche sull’esperienza di tipo ispettivo ed in campo consulenziale, che saranno il frutto di valutazioni sull’intero modello adottato da parte dell’Organo Dirigente.

Analisi dei Rischi

La presente Appendice può essere applicata sia ad imprese che valutano la propria complessità “standard” secondo quanto previsto dal Codice di Comportamento ANCE 2013 (Cfr. Analisi dei rischi, pag. 182-183 per le quali l’analisi dei rischi effettuata da ANCE è applicabile direttamente) sia per Enti che hanno realizzato una specifica Analisi dei Rischi secondo quanto indicato nell’APPENDICE precedente.

La tipologia di azienda relativamente all’Analisi dei Rischi è definita in: Rischi / Analisi Modello Approvato / Metodo e Intervalli / Base per il livello di Rischio”.

Nelle Note della presente Appendice viene fatto esplicito riferimento al Documento di Excel ottenibile da SQuadra231 da: Rischi / Rischio Rilavato / Calcoli.

10.2 Conformità alle procedure

La conformità alle procedure previste nello svolgimento delle attività viene individuata sulla base di 5 livelli, che vanno da “totalmente conforme” = 100% a “non conforme” = 0%.

Per le Procedure che rispondono a Punti di Controllo del tipo “*protocolli diretti a programmare la formazione e l’attuazione delle decisioni dell’ente in relazione ai reati da prevenire*” o “*modalità di gestione delle risorse finanziarie idonee ad impedire la commissione dei reati*”:

- **Totalmente conforme:** Sono rilevabili evidenze della corretta applicazione del punto in esame nel pieno rispetto di tutte le Procedure aziendali.
- **Conforme:** Sono rilevabili evidenze dell’applicazione del punto in esame anche se non esattamente in base alle Procedure previste
- **Parzialmente conforme:** Il punto in esame risulta sotto controllo anche se non sono rilevabili adeguate evidenze oggettive o se non sono state applicate le Procedure previste. Il Gruppo di Audit rilascerà delle Osservazioni.
- **Con Rilievi:** Il punto in esame non risulta completamente sotto controllo; non sono state applicate le Procedure previste. Verrà rilevato un Rilievo con la richiesta di trattamento entro una data prefissata.
- **Non conforme:** Il punto in esame non risulta sotto controllo. Viene rilevato un Rilievo ma si è in attesa della definizione del trattamento oppure il Rilievo non è stato trattato anche se è già stata superata la data prefissata.

Per le Procedure che, invece, rispondono a Punti di Controllo del tipo “*obblighi di informazione nei confronti dell’organismo deputato a vigilare sul funzionamento e l’osservanza dei modelli*”:

- **Totalmente conforme:** L’informatica è stata fornita dal Responsabile nei tempi previsti. Contiene una esaurente informazione sugli eventuali aspetti significativi afferenti alle attività

- di competenza del Responsabile avvenuti nel periodo in oggetto e non viene evidenziata nessuna anomalia o deroghe inerenti alle attività di competenza del Responsabile.
- **Conforme:** L'informativa è stata inviata dal Responsabile con un ritardo non significativo rispetto ai tempi previsti. Contiene una informazione sugli eventuali aspetti significativi afferenti alle attività di competenza del Responsabile avvenuti nel periodo in oggetto e non viene evidenziata nessuna anomalia significativa e solo poche deroghe, tutte autorizzate, inerenti alle attività di competenza del Responsabile.
 - **Parzialmente conforme:** L'informativa è stata inviata dal Responsabile solo dopo esplicito sollecito. Contiene una informazione sommaria sugli eventuali aspetti significativi afferenti alle attività di competenza del Responsabile avvenuti nel periodo in oggetto o vengono evidenziate alcune anomalie significative e/o deroghe inerenti alle attività di competenza del Responsabile. L'OdV rilascerà delle Osservazioni.
 - **Con Rilievi:** L'informativa è stata inviata dal Responsabile solo dopo vari solleciti. Non contiene informazioni su eventuali aspetti significativi afferenti alle attività di competenza del Responsabile avvenuti nel periodo in oggetto di cui l'OdV è venuto a conoscenza attraverso altri canali o vengono evidenziate anomalie significative e/o deroghe anche non autorizzare inerenti alle attività di competenza del Responsabile. L'OdV rilascerà delle Osservazioni. L'OdV provvederà ad effettuare dei Rilievi con la richiesta di trattamento entro una data prefissata.
 - **Non conforme:** Il punto in esame non risulta sotto controllo. L'informativa non è rilasciata neppure dopo esplicativi solleciti o un precedente Rilievo non è stato trattato anche se è già stata superata la data prefissata.

Come si vede il livello di conformità è influenzato, oltre che dal risultato degli audit, dal modo in cui vengono gestite le eventuali non conformità rilevate e dal tempo trascorso dall'ultima attività di controllo realizzata. In caso di non conformità individuata in fase di audit, deve essere concordato un trattamento ed una data prevista per la sua chiusura⁴³.

10.3 Valutazione in assenza di audit / informative

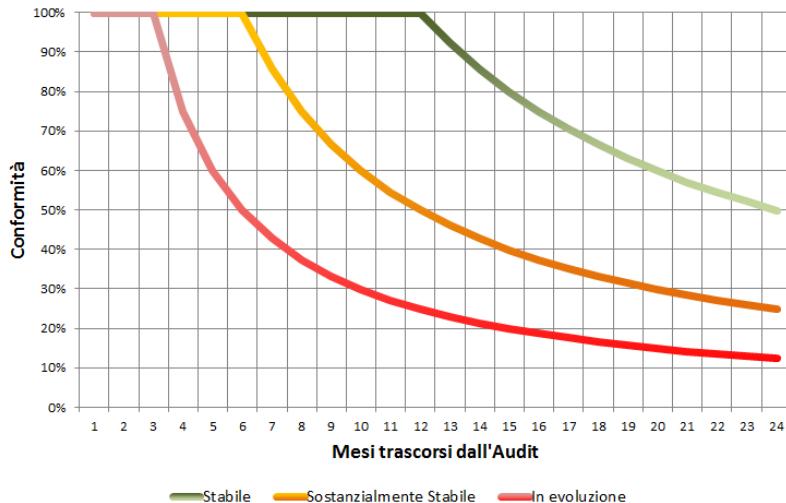
Il programma attribuisce un valore di conformità pari a 0 alle procedure che non sono mai state controllate ed alle informative non ancora ricevute, ovvero una totale non conformità, seguendo una logica cautelativa per l'impresa.

10.4 Decadimento delle valutazioni nel tempo

Le attività valutate conformi, manterranno tale conformità fino allo scadere della validità dell'audit effettuato, che viene stabilita dall'OdV stesso in base alla stabilità delle attività. L'OdV valuterà le attività: Stabili (audit valido 12 mesi), Sostanzialmente stabili (6 mesi), o In evoluzione (3 mesi). Una volta trascorso tale periodo, nell'eventualità che non si effettui un nuovo audit, e non potendo perciò più essere certi della validità della conformità rilevata, per attribuire comunque un valore alla conformità di quella attività è opportuno considerare un decadimento nella validità dei controlli. Nel far ciò si considera una perdita di validità più rapida per i processi in evoluzione e più lento per

⁴³ Vedi documento su RISCHI_RILEVATI: Foglio “Audit_Multipli” colonna P e Foglio “Procedure” colonna S.

gli altri. Ciò viene effettuato poiché si ritiene che un processo conforme per "N" mesi non possono considerarsi totalmente non conforme appena scaduto il suddetto periodo⁴⁴.



10.5 Funzioni aziendali multiple

Il programma considera, normalmente, soltanto l'ultima rilevazione effettuata per ogni procedura (distinguendo fra i Punti contenuti nelle Informative e gli altri rilevati da specifici Audit).

Nel caso delle funzioni aziendali multiple viene utilizzato un altro metodo. Si tratta, infatti, di funzioni ricoperte da più persone fisiche, ognuna per le proprie competenze, che non sono definibili una sola volta ma possono cambiare nel tempo (ad esempio la figura del direttore di cantiere) per cui l'analisi del solo ultimo audit non sarebbe rappresentativa. In questi casi è l'Organismo di Vigilanza il soggetto preposto all'identificazione di un campione di figure fisiche con una stessa funzione, in modo da raccogliere una quantità di audit significativa.

Il livello di conformità sarà dunque ottenuto mediando tra i valori risultanti dagli audit operati sul campione ritenuto significativo dall'OdV⁴⁵.

10.6 Controlli di secondo livello

Per ogni Procedura è possibile definire un Responsabile dei controlli di secondo livello.

Per le Procedure per le quali è stato definito un Responsabile dei controlli di secondo livello sarà quest'ultimo a fornire all'OdV l'informazione sulla Conformità rilevata⁴⁶.

10.7 Correlazione

Ogni Procedura è correlata sia ai vari Reati che agli aspetti legati alla Governance aziendale.

⁴⁴ Per audit "scaduti" (Mesi Trascorsi > Mesi di Stabilità) viene utilizzata la formula:

Conformità = Conformità Rilevata x Mesi di Stabilità / Mesi trascorsi

Vedi documento su RISCHI_RILEVATI: Foglio "Audit_Multipli" colonna R e Foglio "Procedure" colonna U.

⁴⁵ Vedi documento su RISCHI_RILEVATI: Foglio "Audit_Multipli".

⁴⁶ Vedi documento su RISCHI_RILEVATI: Foglio "Procedure". Nella colonna Persona verrà indicato il nome del Responsabile seguito da "[Contr. 2° liv.]".

La correlazione può essere considerata “normale” o “critica”⁴⁷. Le correlazioni relative allo stesso Reato vengono “normalizzare” per ottenere una correlazione totale pari al 100%. Tutte le correlazioni relative alla Governance vengono “normalizzate” complessivamente per ottenere il 100%⁴⁸.

La Quota di Conformità che ogni Punto di controllo apporta alla prevenzione di un reato sarà quindi data dalla Conformità rilevata per il Punto di controllo moltiplicata per la Quota di correlazione⁴⁹.

10.8 Governance

Le varie Procedure sono correlate ai vari Reati ma sono anche correlati agli aspetti di Governance aziendale:

- Precisa definizione delle mansioni ed attribuzione delle responsabilità.
- Puntuale assegnazione di deleghe e procure.
- Efficacia ed aggiornamento costante del sistema di Procedure aziendali.
- Completezza e diffusione del Codice Etico.
- Corretta comunicazione delle informazioni nell’azienda.
- Efficace formazione di tutto il personale compresi i neoassunti.
- Sostanziale attenzione al raggiungimento degli obiettivi per tutto il personale.
- Corretta assegnazione delle responsabilità dei controlli.
- Presenza ed applicazione di un sistema sanzionatorio.

Una cattiva Governance influenza negativamente l’aspettativa di conformità su tutte le Procedure.

Si ricorda, infatti, che la valutazione della conformità si basa su una analisi “a campione” e quindi solo in presenza di una buona Governance una rilevazione di aspetti conformi potrà dare una buona aspettativa sulla effettiva conformità di tutte le operazioni.

Dall’analisi degli Audit svolti è possibile rilevare la conformità rilevata sui vari aspetti della Governance e confrontarla con quella attesa in caso di totale conformità⁵⁰.

Ovviamente la Governance è condizionata anche dalla corretta formazione sul D.Lgs 231/01 e sulla formazione specifica sulle varie Procedure assegnate ai vari Responsabili e quindi sulla formalizzazione delle Nomine⁵¹.

La conformità media associata alla Governance si ottiene mediando i tre valori relativi alla conformità rilevata dagli audit e, in misura minore, allo stato della Formazione dei Responsabili e delle Nomine degli stessi⁵².

⁴⁷ Viene assegnato alle correlazioni “critiche” un valore doppio rispetto a quelle “normali”.

Vedi documento su RISCHI_RILEVATI: Foglio “Correlazioni” colonna K.

⁴⁸ Vedi documento su RISCHI_RILEVATI: Foglio “Correlazioni” colonna Q (per gli elementi di Governance viene utilizzato come Livello di Rischio la somma dei Livelli di Rischio previsti per tutti i Reati).

⁴⁹ Quota Conformità = Conformità x Quota Correlazione.

Vedi documento su RISCHI_RILEVATI: Foglio “Correlazioni” colonna R.

⁵⁰ Conformità per Governance dagli Audit = Somma Conformità / Somma Totale.

Vedi documento su RISCHI_RILEVATI: Foglio “Governance” riga 5.

⁵¹ Per la Formazione si assegna valore 1 se questa risulta effettuata e 0 se assente; per le Nomine si assegna valore 1 se questa risulta valida, 0,5 se non aggiornata rispetto all’ultima versione del MOG approvata e 0 se assente.

Vedi documento su RISCHI_RILEVATI: Foglio “Responsabili” colonne B, C e I per la Formazione e colonne D, E, F e I per le Nomine.

⁵² Governance = 75% x Conformità negli Audit + 25% x (Conformità Formazione + Conformità Nomine)/2

Vedi documento su RISCHI_RILEVATI: Foglio “Governance” riga 1.

10.9 Valutazione riepilogativa per Reato

Per ogni Reato viene riportata la conformità rilevata nel corso degli audit direttamente correlata allo specifico Reato⁵³ viene quindi riportata la conformità relativa alla Governance che è uguale per tutti i Reati⁵⁴.

La conformità Totale si ottiene mediando le due conformità precedenti dando un peso minore alla conformità relativa alla Governance (che però interviene su tutti i reati)⁵⁵.

Il Rischio Residuo Rilevato è funzione del Livello di Rischio dello specifico Reato e della conformità rilevata.

In funzione delle valutazioni sul grado di rischio accettabile viene indicata una valutazione sintetica in funzione del superamento dei vari intervalli (in base a quanto definito in Rischi / Analisi del Modello Approvato / Metodo e Intervalli).

Si noti che la somma dei Rischi Residui Rilevati corrispondono alla somma delle Non Conformità direttamente correlabili ai Reati e correlabili alla Governance rilevate nel corso degli Audit più le Non Conformità relative alle Nomine ed alla Formazione.

10.10 Metodo Lineare

Il metodo di calcolo applicato è definito in: Rischi / Analisi Modello Approvato / Metodo e Intervalli / “Tipo elaborazione per i Rischi Residui Rilevati”.

In questo caso si parte dalla considerazione che il Modello (insieme di Punti di Controllo adeguati in base alla loro correlazione con i vari reati alla prevenzione degli stessi) è stato valutato come idoneo dell’Organo Dirigente e quindi ci concentriamo sulla Conformità rilevata rispetto al Modello, a prescindere da come si è arrivati alla costruzione del Modello partendo da Linee Guida di categoria o in base ad il calcolo esposto nell’Appendice “Analisi dei Rischi 231”.

È quindi possibile calcolare il Rischio Residuo Rilevato applicando “linearmente” la conformità rilevata al Livello di Rischio per ogni Reato⁵⁶.

Per chiarire l’effetto delle varie parti del Modello sul Rischio Residuo Rilevato vengono riportati dei valori di dettaglio ed in particolare:

- Per ogni Punto di Controllo / Reato: la Quota di Livello di Rischio Totale⁵⁷ e di Rischio Residuo Rilevato⁵⁸.

⁵³ Vedi documento su RISCHI_RILEVATI: Foglio “Reati” colonna C corrispondente alla somma della colonna R del Foglio “Correlazione” filtrando le righe per lo specifico Reato (colonna L).

⁵⁴ Vedi documento su RISCHI_RILEVATI: Foglio “Reati” colonna D che corrisponde alla prima riga del foglio Governance.

⁵⁵ Conformità Totale = 75% x Conformità per il Reato + 25% x Conformità relativa alla Governance.

Vedi documento su RISCHI_RILEVATI: Foglio “Reati” colonna E.

⁵⁶ Rischio Residuo Rilevato = Livello di Rischio x (1 – Conformità Rilevata)

Vedi documento su RISCHI_RILEVATI: Foglio “Reati” colonna G (per Elaborazione Lineare).

⁵⁷ Quota Livello di Rischio = Livello di Rischio x 75% x Quota di Correlazione

Vedi documento su RISCHI_RILEVATI: Foglio “Correlazione” colonna S (per Elaborazione Lineare).

⁵⁸ Quota Rischio Residuo Rilevato = Quota Livello di Rischio x (1 – Conformità).

Vedi documento su RISCHI_RILEVATI: Foglio “Correlazione” colonna T (per Elaborazione Lineare).

- Per ogni Persona o Funzione Multipla / Reato: la Quota di Livello di Rischio e di Rischio Residuo Rilevato suddivisi per Origine (Audit correlati ai Reati, Audit correlati agli aspetti di Governance, alla Formazione ed alle Nomine)⁵⁹.
- Per ogni Reato: La Quota di Rischio Residuo Rilevato da addebitarsi alle Non Conformità rilevate negli Audit direttamente correlabili con i Reati ed a quelli correlabili alla Governance. Vengono inoltre presentati gli effetti delle Non Conformità nelle Nomine e nella Formazione⁶⁰.
- Per ogni Persona o Funzione Multipla: Gli stessi dati del punto precedente e viene anche indicata la Percentuale di Non Conformità complessiva per il singolo Responsabile⁶¹ (dato che può servire ad orientare le attività di Audit).
- Per ogni Processo: Il Livello di Rischio e il Rischio Residuo Rilevato⁶² (dato che potrà servire per individuare i Processi sui quali concentrare le attività di miglioramento).

Grazie a questi valori è possibile ottenere anche una rappresentazione grafica dello stato del sistema.

10.11 Metodo Non Lineare

Un secondo metodo è quello di analizzare l'effetto della Conformità sulla funzione di attenuazione del rischio da parte dei vari Punti di Controllo⁶³.

Questo metodo è, per sua natura, non Lineare dipendendo il Rischio Residuo Rilevato dall'insieme delle Non Conformità rilevate e dalla quantità di Punti di Controllo⁶⁴.

Non è quindi possibile effettuare un calcolo analogo a quello visto nel capitolo relativo al Metodo “Lineare” per “scomporre” il Rischio Residuo Rilevato.

È comunque possibile attribuire il Rischio Residuo Rilevato in proporzione ai valori di composizione del Rischio visti nel caso del Modello Lineare.

⁵⁹ Vedi documento su RISCHI_RILEVATI: Foglio “Corr_Resp”. I valori relativi agli Audit sui Reati sono ottenuti dal foglio “Correlazione” raggruppando le Funzioni Aziendali ricoperte dalla stessa Persona. I valori relativi agli Audit sulla Governance sono ottenuti “spalmando” il totale ottenuto nel foglio “Correlazione” in base al Livello di Rischio dei vari Reati. La stessa “spalmatura” viene effettuata anche per il Rischio Residuo legato alle Non Conformità su Formazione e Nomine.

Una sintesi viene riportata nel Foglio “Reati_Funzioni”.

⁶⁰ Vedi documento su RISCHI_RILEVATI: Foglio “Reati” colonne I, J, K e L. I dati sono una semplice sintesi dei dati presenti nel foglio “Corr_Resp”.

⁶¹ Vedi documento su RISCHI_RILEVATI: Foglio “Funzioni” colonne E, F, G e H per i dati ottenuti come sintesi dei dati presenti nel foglio “Corr_Resp”. Nella colonna D è riportata la Percentuale di Non Conformità rilevata sulle attività del singolo Responsabile come rapporto fra Livello di Rischio e Rischio Rilevato.

⁶² Vedi documento su RISCHI_RILEVATI: Foglio “Processi”. I dati si ottengono come sintesi dei dati presentati nel foglio “Correlazione”.

⁶³ Rischio Residuo Rilevato = Livello di Rischio / (1 + Punti di Controllo x Conformità Rilevata).

Essendo Rischio Residuo Teorico = Livello di Rischio / (1 + Punti di Controllo) il Rischio Residuo Rilevato potrà variare fra il Livello di Rischio (in caso di assenza totale di Conformità) e il Rischio Residuo Teorico (in caso di completa Conformità).

Vedi documento su RISCHI_RILEVATI: Foglio “Reati” colonna G (per Elaborazione Non Lineare).

⁶⁴ Si può notare che i due metodi danno lo stesso risultato solo quando il Numero dei Punti di Controllo corrisponde all'inverso della Non Conformità rilevata. Ad esempio se per un Reato sono previsti 5 Punti di controllo e la Conformità rilevata è pari all'80% con tutti e due i metodi il Rischio Residuo Rilevato corrisponde al 20% del Livello di Rischio.

11 APPENDICE: Asseverazione

11.1 Introduzione

UNI ha prodotto un documento che fornisce una indicazione operativa ai Comitati Paritetici Territoriali (CPT), in quanto organismi paritetici, per l'attività di asseverazione della corretta adozione e della efficace attuazione dei modelli di organizzazione e gestione della sicurezza di cui all'articolo 30, D.Lgs 81/08 e s.m.i., adottati dalle imprese edili e di ingegneria civile, e finalizzati a proteggere la salute e la sicurezza di tutti i lavoratori, considerando anche aspetti culturali, di comportamento e di *governance*.

All'interno del documento vengono riportate le seguenti definizioni:

- **Modello di organizzazione e gestione della sicurezza:** Modello organizzativo e gestionale per la definizione e l'attuazione di una politica aziendale per la salute e sicurezza, ai sensi dell'articolo 6, comma 1, lettera a), del decreto legislativo 8 giugno 2001, n. 231, idoneo a prevenire i reati di cui agli articoli 589 e 590, terzo comma, del codice penale, commessi con violazione delle norme antinfortunistiche e sulla tutela della salute sul lavoro.
- **Sistema di gestione della salute e sicurezza sul lavoro (SGSL):** Parte del sistema di gestione di un'organizzazione utilizzato per sviluppare ed implementare la propria politica e gestire i propri rischi per la sicurezza. Il sistema di gestione è un insieme di elementi tra loro correlati utilizzati per stabilire la politica e gli obiettivi e per conseguire questi ultimi. Comprende la struttura organizzativa e le attività di pianificazione (includendo, ad esempio, le responsabilità, le prassi, le procedure, i processi e le risorse).

11.2 SQuadra231 per l'Asseverazione

Modello di organizzazione e gestione

Il Modello di organizzazione e gestione (MOG) prodotto da SQuadra si basa sul Codice di Comportamento per le Imprese di Costruzione ritenuto dal Ministero della Giustizia idoneo al raggiungimento dello scopo fissato all'art. 6 comma 3 D.L.vo 231/2001 (base per la realizzazione dei MOG aziendali).

Il MOG si compone dalla Parte Generale (nella quale è descritto, fra l'altro, il Sistema Disciplinare e le modalità per la nomina dell'Organismo di Vigilanza) e dalla Parte Speciale nella quale sono riportati tutti i Punti di Controllo con le relative procedure aziendali per la loro attuazione.

Fra i Punti di Controllo previsti per contrastare i reati previsti dall'Art. 25 septies (Omicidio colposo o lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro) alcuni fanno riferimento al SGSL in sede, negli impianti fissi e nei cantieri (in particolare: 10.12 e 10.13).

Ovviamente sono presenti molti altri Punti di Controllo per la prevenzione dei reati previsti dall'Art. 25 septies (controllo degli oneri per la sicurezza sia in fase di Gara che in fase di stipula di contratti con subappalto, modalità per la selezione dei subappaltatori, contenuto dei contratti di subappalto, ecc.) normalmente non presenti in un SGSL.

Nel Modello sono poi previsti tutti gli altri Punti di Controllo per la prevenzione degli altri reati previsti dal D.Lgs. 231/01.

Sistema di gestione della salute e sicurezza sul lavoro (SGSL)

SQuadra fornisce un MANUALE DEL SGSL (Basato sulle Procedure semplificate per l'adozione dei modelli di organizzazione e gestione nelle piccole e medie imprese emanate con Decreto del

Ministero del Lavoro e delle Politiche Sociali del 13 febbraio 2014) che contiene al suo interno tutte le procedure necessarie e la modulistica per le registrazioni ed è redatto in forma ritenuta adeguata per una impresa di costruzioni tipica, reso disponibile in formato Word per essere ulteriormente personalizzato e solo successivamente adottato dalla singola impresa.

Ne consegue che:

- Con l'adozione del manuale, il Vertice Aziendale impegna l'azienda al puntuale rispetto dei suoi contenuti, che debbono ovviamente essere stati preliminarmente valutati come congruenti con le dimensioni e l'organizzazione e aziendali.
- Nel manuale vengono descritte le modalità di registrazione con utilizzo manuale dei Moduli allegati; un paragrafo specifico chiarisce che l'azienda intende progressivamente adottare SQuadra come strumento alternativo di registrazione informatica e individua, per ciascuna registrazione, la corrispondenza fra il singolo Modulo e la equivalente registrazione su SQuadra. Ovviamente l'azienda può sostituire i Modelli proposti con modelli aziendali equivalenti già in uso.
- Il manuale necessita in ogni caso di completamenti e/o personalizzazioni, fra i quali a titolo di esempio ricordiamo:
 - l'inserimento del nome, del logo e delle anagrafiche aziendali (copertina e premessa)
 - l'allineamento della politica per la sicurezza a quella eventualmente già adottata dall'azienda (Parte I § 1)
 - l'inserimento dei nominativi del personale che in azienda svolge un ruolo chiave in tema di sicurezza (Parte I § 3)
 - nel caso in cui il Datore di Lavoro non abbia conferito delega complessiva alla sicurezza ad un dirigente, il § 3.2 deve diventare "Compiti del Datore di Lavoro" (Parte I § 3)
 - il manuale non sostituisce in alcun modo il DVR, che si ipotizza già predisposto dall'azienda utilizzando le metodologie rese disponibili da Ance e dal CNCPT (Parte I § 7)
 - il manuale prevede la predisposizione di un Piano Sicurezza Preliminare – PSP non sempre già presente in azienda (Parte I § 8). Poiché per la redazione dello stesso si fa riferimento alle schede del Manuale operativo per la valutazione dei rischi nel settore delle costruzioni del CPT di Torino, l'azienda deve procurarsi tale documento, scaricabile anche attraverso il software SQuadra231 (SGSL: Allegato A)
 - qualora alcuni documenti obbligatori previsti dal manuale (ad esempio CPI sede) non fossero ritenuti applicabili, gli stessi debbono essere rimossi dall'elenco riportato nel manuale (Parte I § 10)
 - il manuale non sostituisce in alcun modo il POS del cantiere, che si ipotizza di volta in volta predisposto dall'azienda utilizzando le metodologie rese disponibili da Ance e dal CNCPT (Parte II § 1)
 - il manuale prevede un monitoraggio di primo livello (Parte II § 2) effettuato periodicamente dal capocantiere. Poiché per la redazione dello stesso si fa riferimento alle liste di controllo della Guida per la valutazione del sistema sicurezza sul lavoro in edilizia del CPT di Torino, Roma e Verona, l'azienda deve procurarsi tale documento, scaricabile anche attraverso il software SQuadra231 (SGSL: Allegato B)
 - la Check list di terzo livello (5.16) deve essere aggiornata in funzione delle procedure definite aziendalmente nella Parte Speciale del MOG

Ogni azienda deve valutare se, per alcune parti, invece di seguire le indicazioni riportate sul manuale, desidera continuare con la prassi già in uso. In questo caso dovrà sostituire le relative parti del Manuale.

SQuadra SGSL

I moduli proposti nel Manuale SGSL sono gestibili direttamente tramite le funzionalità di SQuadra231 come descritto dall'allegato 18.

Preverifica e Verifica Documentale

La Pressi di riferimento UNI prevede una preverifica che ha per oggetto la verifica degli: *obblighi documentali inerenti l'adozione del modello di organizzazione e gestione della salute e sicurezza. In particolare sono oggetto di analisi e verifica da parte di GDV:*

- *la documentazione inerente il modello organizzativo e di gestione: manuale, procedure, modulistica per le registrazioni, sistema disciplinare e sanzionatorio, sistema di controllo, articolazione delle funzioni con le relative idonee competenze tecniche;*
- *la documentazione inerente la sicurezza obbligatoria per legge, come indicato nell'Appendice C;*
- *l'applicazione della normativa pertinente (leggi, regolamenti e norme, protocolli e contrattazione collettiva);*
- *le informazioni sui processi produttivi e relative istruzioni operative, e gli schemi organizzativi.*

Come già indicato il Manuale SGSL contiene al suo interno “manuale, procedure, modulistica per le registrazioni” mentre nel MOG è contenuto il “sistema disciplinare e sanzionatorio” e le indicazioni sulla composizione dell’Organismo di Vigilanza.

L’elenco della Documentazione richiesta nell’Appendice C, che è anche oggetto anche della Verifica Documentale presso la sede dell’impresa, è riportata su SQuadra231 in SG / 06.Pianificazione / Asseverazione / Documenti. L’impresa può quindi tenere sempre sotto controllo questa documentazione.

NOTA: L’FSC Torino in collaborazione con CNCPT - ha predisposto il Manuale “Asseverazione dei modelli di organizzazione e gestione della sicurezza in edilizia” [d’ora in poi Manuale CPT]. L’opera costituisce un approfondimento delle regole presenti nella Prassi di Riferimento UNI/PdR 2:2013 ed è un supporto di carattere tecnico contenente indicazioni e strumenti operativi per la conduzione dell’attività asseverativa.

Nelle stampe è possibile ottenere i riferimenti e le indicazioni proposte nel Manuale CPT.

VERIFICA NEI CANTIERI E NEGLI ALTRI LUOGHI DI LAVORO DELL’IMPRESA (VERIFICA TECNICA)

La Pressi di riferimento UNI prevede quindi attività di verifica tecnica presso il/i cantiere/i e gli altri luoghi di lavoro dell’impresa richiedente che consistono:

- nello stabilire il grado della reale adozione del modello di organizzazione e di gestione della salute e sicurezza nelle sedi individuate nel corso della verifica documentale;
- nel raccogliere direttamente dati ed informazioni riguardo ai processi e alle attività rientranti nello scopo del modello di organizzazione e gestione della salute e sicurezza, considerando gli aspetti connessi con il rispetto di leggi e norme applicabili;
- nel verificare i documenti che non erano presenti al momento della verifica documentale presso la sede dell’impresa richiedente.

La verifica tecnica è finalizzata all'accertamento dei seguenti obblighi giuridici, così come previsto dall'art. 30, comma 1, lettere da a) ad h), e i commi 2, 3 e 4 del D.Lgs. 81/08 e s.m.i.

La Pressi di riferimento UNI fornisce nell’Appendice D la check-list di controllo operativo per la verifica tecnica.

La check-list è riportata nel Manuale SGSL fornito da SQuadra231 (Modello 5.13) e può essere gestita anche in forma informatizzata come descritto nella tabella precedente.

Anche in questo caso nelle stampe è possibile ottenere le indicazioni presenti nel Manuale CPT.

SGSL

Su SQuadra permette di registrare le informazioni richieste dalle Procedure Semplificate per la PMI:

- Scheda analisi Iniziale.
- Politica, Obiettivi e azioni.
- Audit.
- Rilievi e non conformità.
- Archivio delle Deleghe, Incarichi ed Autorizzazioni.
- Riesami del SGSL.

Su SQuadra sono state inoltre riportate alcune delle Check-list proposte dal Manuale CPT:

- Contenuti del MOG PMI.
- DVR
- DVR-Rischi.
- POS.
- PiMUS.
- OdV e Sistema Disciplinare.

All'interno dei Monitoraggi di Secondo Livello è possibile richiedere la stampa delle Check-list relative a:

- Controlli Operativi.
- POS.
- PiMus

12 APPENDICE: Oneri aziendali per la sicurezza

12.1 Introduzione

L'ANCE consiglia a tutte le imprese di indicare nelle offerte per appalti di lavori pubblici, in via cautelativa ed al fine di evitare esclusioni dalle gare, gli **oneri della sicurezza aziendali** anche nei casi in cui il bando di gara non lo richieda esplicitamente.

L'ANCE offre quindi alle aziende associate, all'interno di SQuadra231, un semplice strumento per il calcolo di questi oneri sulla base del metodo messo a punto nel documento ANCE-ITACA.

Definizioni

I costi della sicurezza derivano, in caso di lavori ex Titolo IV, dalla stima effettuata nel Piano di Sicurezza e Coordinamento (PSC) ai sensi dell'art. 100 del D.Lgs. 81/2008 s.m.i. o dall'analisi della Stazione appaltante anche per tramite del RUP quando il PSC non sia previsto – rif. punto 4.1.2. - secondo le indicazioni dell'allegato XV punto 4.

A tali costi l'impresa è vincolata contrattualmente (costi contrattuali) in quanto rappresentano "l'ingerenza" del committente nelle scelte esecutive della stessa; in essi si possono considerare, in relazione al punto 4.1.1. dell'allegato XV, esclusivamente le spese connesse al coordinamento delle attività nel cantiere, alla gestione delle interferenze o sovrapposizioni, nonché quelle degli apprestamenti, dei servizi e delle procedure necessarie per la sicurezza dello specifico cantiere secondo le scelte di discrezionalità tecnica del CSP / Stazione appaltante, valutate attraverso un computo metrico estimativo preciso.

Gli oneri aziendali della sicurezza afferenti all'esercizio dell'attività svolta da ciascun operatore economico (detti anche, in giurisprudenza piuttosto che in dottrina, costi ex lege, costi propri, costi da rischi specifici o costi aziendali necessari per la risoluzione dei rischi specifici propri dell'appaltatore), relativi sia alle misure per la gestione del rischio dell'operatore economico, sia alle misure operative per i rischi legati alle lavorazioni e alla loro contestualizzazione, aggiuntive rispetto a quanto già previsto nel PSC e comunque riconducibili alle spese generali. Detti oneri aziendali sono contenuti nella quota parte delle spese generali prevista dalla norma vigente (art. 32 del D.P.R. 207/2010 s.m.i.) e non sono riconducibili ai costi stimati per le misure previste al punto 4 dell'allegato XV del D.Lgs. 81/2008 s.m.i.

Gli oneri aziendali della sicurezza sono costituiti da due componenti: una gestionale ed una operativa.

- **La componente gestionale** è valutabile come quota parte degli oneri gestionali della sicurezza annui sostenuti dall'operatore economico in attuazione della normativa vigente in materia, a prescindere dai singoli e specifici contratti (ad esempio: quota parte delle spese sostenute per le visite mediche, formazione ed informazione di base dei Lavoratori ecc.).
- **La componente operativa** è riconducibile espressamente a oneri operativi rappresentativi di tutte le spese relative alle misure di prevenzione connesse allo specifico appalto (ad esempio: la formazione integrativa necessaria agli stessi lavoratori, alcuni DPI particolari ecc.).

12.2 Oneri Aziendali

Costi

Per la componente gestionale il programma permette di memorizzare via via le ultime rilevazioni disponibili con relativa documentazione in forma di allegato PDF.

Vengono presentati tutti gli elementi della Tabella ITACA relativi alle Misure per la gestione del rischio aziendale. L'utente può comunque aggiungere nuove attività qualora lo ritenesse utile.

Ogni attività è possibile definire le varie rilevazioni dei costi caratterizzate da:

- Data di rilevazione.
- Mesi del periodo sul quale “spalmare” il costo (es. 60 per un DPI che dura 5 anni, 12 per un costo annuale, ecc.).
- Costo unitario.
- Quantità (es. con riferimento al costo inserito: numero di persone, numero di ore, ecc.).
- Note.
- Allegato che giustifica il Costo unitario inserito (è opportuno inserire il contratto, la fattura, una busta paga, ecc.).

Fatturato

Per poter valutare l’incidenza dei costi è necessario inserire il fatturato con il quale si intendono confrontare.

È opportuno inserire via via gli aggiornamenti sul fatturato in base agli ultimi dati disponibili.

Per ogni rilevazione sono richieste le seguenti informazioni:

- Data di rilevazione.
- Mesi ai quali si riferisce il fatturato. È possibile utilizzare l’ultimo fatturato dal Bilancio aziendale o utilizzare un dato relativo ad un Biennio o un Triennio o, all’opposto, all’ultima Trimestrale. È opportuno che l’azienda scelga il valore che meglio rappresenta le previsioni future.
- Il valore del Fatturato per il periodo sopra definito.
- Note.
- Allegato che giustifica il valore del Fatturato.

Andamento nel tempo

Il programma produce un documento di Excel nel quale sono riportati i dati inseriti e mostra la variazione nel tempo dell’incidenza degli Oneri per la Sicurezza.

Il documento è caratterizzato dai seguenti fogli:

- **Dati.** Vengono qui riportati i dati inseriti nel tempo.
- **Dati_Uso.** In questo foglio vengono riportati, per ogni nuova data di rilevazione, tutti i dati utilizzati (gli ultimi disponibili alla data per ogni attività).
- **Grafico.** Viene riportato l’andamento dell’incidenza percentuale degli Oneri per la Sicurezza sul Fatturato.
- **G_Costi.** Viene riportato l’andamento dei costi nel tempo.

12.3 Gare

Informazioni sulla Gara

In questo modulo del programma è possibile inserire i dati relativi alle varie Gare ed in particolare:

- Un Codice.
- Una Descrizione.
- Delle Note sulla Gara.
- La data alla quale è stata effettuata l’elaborazione per il calcolo degli Oneri per la sicurezza (sicuramente antecedente alla data di consegna ma non coincidente).
- Importo offerto (utilizzato come base di calcolo per la valutazione dell’incidenza degli Oneri per la sicurezza).

- Eventuali Note specifiche sugli Oneri per la Sicurezza.

Oneri specifici

Per ogni gara è possibile definire degli Oneri specifici caratterizzati da:

- Un Codice.
- La Descrizione della Macro Attività (con riferimento alla Tabella ITACA).
- La Descrizione della Attività (sempre con riferimento alla Tabella ITACA).
- Il Costo Unitario.
- La Quantità da considerare.
- Delle Note
- Un eventuale Allegato a giustificazione del Costo Unitario indicato.

Stampa degli Oneri

Il programma utilizza tutti i costi aziendali noti alla data di elaborazione della Gara e tutti i costi specifici per calcolare il valore degli Oneri aziendali per la Sicurezza da dichiarare in sede di gara.

Predisponde quindi un documento di Word che può anche essere utilizzato come base per la giustificazione degli stessi.

Il Documento fa riferimento agli Allegati che vengono prodotti con l'apposita scelta del programma.

13 APPENDICE: Analisi del Contesto

13.1 Introduzione

Le nuove Norme internazionali richiedono all'Organizzazione di analizzare il proprio contesto.

SQquadra231 fornisce un supporto per facilitare questa analisi in occasione di ogni Riesame della Direzione.

Nella presente appendice viene presentato il metodo e quindi le modalità operative.

13.2 Metodologia

La Direzione Aziendale determina i fattori interni ed esterni rilevanti per le sue finalità ed indirizzi strategici periodicamente (almeno una volta all'anno ed in occasione di modifiche significative all'organizzazione) mediante un'analisi che utilizza vari strumenti teorici (illustrati di seguito) e ne valuta l'adeguatezza e l'eventuale necessità di aggiornamento.

13.2.1.1 Elementi di analisi

Vengono considerati 10 elementi di analisi⁶⁵. Per ogni elemento vengono analizzati gli aspetti generali e quelli specifici per linee di business.

A. Partnership chiave

Chi ci aiuta?

- Chi sono i nostri partner chiave?
- Chi sono i nostri fornitori chiave?
- Quali risorse chiave otteniamo dai partner?
- Quali attività chiave sono compiute dai partner?

Motivazioni per la partnership

- Ottimizzazione e risparmio.
- Riduzione del rischio e dell'incertezza.
- Acquisizione di particolari risorse o attività.

B. Attività chiave

Cosa facciamo (Produzione, Risoluzione dei problemi, ecc.)?

Quali attività chiave sono necessarie:

- Per il nostro valore offerto?
- Per i nostri canali distributivi?
- Per le relazioni con i clienti?
- Per i flussi di ricavi?

C. Risorse chiave

Chi siamo e cosa abbiamo (Risorse: fisiche, intellettuali, umane, finanziarie, ecc.)?

Quali risorse chiave sono necessarie:

- Per il nostro valore offerto?
- Per i nostri canali distributivi?
- Per le relazioni con i clienti?

⁶⁵ Gli elementi scelti si ispirano al Business Model Canvas.

- Per i flussi di ricavi?

Fattori Interni

Infrastrutture, Personale (Fidelizzazione, età, competenze specifiche, ecc.), Ambiente di lavoro.

Fattori esterni

Banche.

D. Valore offerto

Come ci rendiamo utili (quali benefici specifici ottengono i nostri clienti come risultato del nostro lavoro)?

- Quale valore trasferiamo al cliente?
- Quale problema del nostro cliente contribuiamo a risolvere?
- Quali necessità del cliente soddisfiamo?
- Quale bisogno soddisfi?
- Quale insieme di prodotti e servizi offriamo a ciascun segmento di clientela?

Fattori Interni

Prodotti e Servizi, Adattabilità, Sistema Qualità (Procedure, Controllo prestazioni, ecc.).

Fattori esterni

Concorrenza, Normative (Internazionali, Nazionali, Locali).

E. Relazioni con i clienti

Come interagiamo?

- Che tipo di relazione ciascun segmento della nostra clientela si aspetta di stabilire e mantenere con noi?
- Quali relazioni abbiamo stabilito?
- Quanto sono costose?
- Come si integrano con il resto del nostro modello di business?

F. Segmenti di clientela

A chi siamo utili?

- Per chi stiamo creando valore?
- Chi sono i clienti più importanti?
- Chi dipende da te per poter fare il suo lavoro?
- Chi sono i clienti dei tuoi clienti?

Fattori esterni

Andamento dei Mercati e dei Settori nei quali operiamo.

G. Canali

Come ci facciamo conoscere e come portiamo valore?

- Attraverso quali canali i segmenti di clientela vogliono essere raggiunti?
- In che modo sono raggiunti ora?
- Come sono integrati i diversi canali?
- Quali lavorano meglio?
- Quali sono i più convenienti?
- Come si integrano con le abitudini dei clienti?

Fasi di contatto

Nel considerare i Canali è opportuno tener presente le varie Fasi di contatto con i clienti:

- Consapevolezza: come aumentiamo la consapevolezza dei prodotti e servizi della nostra azienda?
- Presenza sul mercato: Come ti trovano i potenziali clienti?
- Valutazione: come facciamo ad aiutare i nostri clienti a valutare la proposta di valore della nostra azienda?
- Acquisto: come consentiamo ai nostri clienti di acquistare specifici prodotti o servizi?
- Consegna: come portiamo una proposta di valore ai clienti?
- Post Consegna: come forniamo assistenza post vendita?
- Post Consegna: come continuamo a supportare i clienti e ad assicurarci che siano soddisfatti?

Fattori Interni

Brand, Reputazione

H. Struttura dei costi.

Cosa diamo?

- Quali sono i costi più importanti nel nostro modello di business?
- Quali risorse chiave sono più costose?
- Quali attività chiave sono più costose?

Fattori Interni

Costi.

I. Flussi di ricavi

Cosa otteniamo (ricavi e benefici)?

- Per quale valore i nostri clienti sono veramente disposti a pagare?
- Per cosa pagano attualmente?
- Come pagano attualmente?
- Come preferirebbero pagare?
- Quanto contribuisce ogni singolo flusso di ricavi ai ricavi totali?

Fattori Interni

Prezzi, Redditività.

L. Altri Elementi

In quale ambito operiamo?

Abbiamo una collocazione territoriale per la fornitura dei nostri prodotti/servizi? è quella corretta?

Come operiamo?

A quali trasformazioni siamo soggetti?

Fattori Esterni

Tecnologia, Cultura, Ambiente, Territorio,

Società, Autorità, Politica, Opinione pubblica, Media.

13.2.1.2 Richieste della norma UNI EN ISO 9001:2015

La Norma richiede di identificare le linee di business, i processi, le attività e gli Asset chiave

A. PRODOTTI / SERVIZI

Quali sono gli elementi caratterizzanti il prodotto / servizio?

A1. Tipologia del prodotto/servizio

- Quali sono le caratteristiche salienti del prodotto servizio: commodities, prodotti a specifica cliente, prodotti a proprio marchio, conto terzi, conto lavoro?
- Che impatto ha la tipologia del prodotto/servizio sulle scelte di business?
(8.1, 7.1.6, 8.5.6)

A2. Requisiti Cogenti

- Esistono requisiti cogenti nazionali o internazionali che l'azienda deve rispettare?
- Quanto impatta sul prodotto / servizio il rispetto di tali requisiti?
- Qual è l'efficacia del sistema di gestione nell'assicurare che l'organizzazione abbia la capacità di soddisfare la normativa vigente applicabile e requisiti contrattuali?
(4.2, 6.1, 5.1.2, 7.1.6, 8.5.5, 8.5.6)

A3. Livelli prestazionali richiesti

- Quanto impatta sul business il ciclo di vita del prodotto / servizio?
- Esistono obblighi di garanzia, riparazione e assistenza per il prodotto, o esistono requisiti di uscita nell'erogazione dei servizi?
(8.5.5, 8.5.6)

B. MERCATO / CLIENTI

Quali sono gli elementi caratterizzanti del mercato?

B1. Tipologia dei clienti (Parco clienti e differenziazione)

- Qual è il risultato dell'analisi del parco clienti?
- Qual è la differenziazione sul fatturato di tale parco cliente?
- Quali sono le peculiarità dei mercati di destinazione geografici (Caratteristiche fisiche, politiche e sociali, valuta, requisiti cogenti, canali di vendita, logistica)?
- Qual è il risultato dell'analisi dei mercati di destinazione d'uso e canali di vendita?
- Quali aspettative sono identificate provenienti dai clienti circa la qualità, prezzo, disponibilità dei prodotti/servizi (prodotti standard, custom, ecc.)?
(4.1, 4.2, 6.1, 7.1.6)

B2. Tendenza di mercato e concorrenti

- Qual è il risultato dell'analisi del contesto competitivo, punti di forza e di debolezza propri e della concorrenza?
- Qual è l'impatto sul business dell'analisi della velocità di innovazione dei prodotti / servizi?
- Quali sono i punti di forza e di debolezza individuati in relazione alle prestazioni ambientali?
(4.1, 4.2, 6.1)

B3. Processo di gestione del cliente

- Qual è l'efficacia del processo di gestione del cliente e/o reclami delle parti interessate, comprese le azioni correttive applicate?
(4.1, 4.2, 6.1, 8.2)

C. PROPRIETA'

Quali sono gli elementi caratterizzanti la compagnia proprietaria?

C1. Visione

- Qual è la Visione strategica a medio e lungo termine?
- Come sono identificati gli obiettivi di business?
- È definita una politica dei sistemi di gestione?
- C'è adeguatezza e coerenza della politica dei sistemi di gestione (qualità / ambiente) con gli obiettivi di business?
- C'è adeguatezza e coerenza degli obiettivi (qualità / ambiente) con la politica del sistema di gestione?
- Qual è l'approccio all'innovazione e cambiamento, incluso l'aggiornamento della politica dei sistemi di gestione (qualità / ambiente)?
- Come viene gestita la continuità generazionale?

- Esistono possibilità di acquisizione o cessione societaria e quali sono i rischi collegati?
(4.2, 5.2, 6.1, 6.2)

C2. Responsabilità societaria

- Esistono rischi legati alla responsabilità civile e penale di prodotto / servizio?
- Esistono rischi legati a sanzioni e azioni legali?
- Esistono rischi reputazionali?
(6.1)

C3. Andamento economico finanziario

- Come viene gestita la soddisfazione delle aspettative di redditività a breve e medio termine?
- Come viene gestita la capacità di fare investimenti per il futuro (esiste una pianificazione degli investimenti)? Esistono difficoltà all'accesso al credito?
- Qual è l'approccio alla gestione del flusso di cassa?
- È attivo un presidio della solvibilità dei clienti o degli incassi?
- Sono messe a disposizione risorse per il raggiungimento degli obiettivi, investimenti legati al sistema di gestione qualità?
(5.1, 5.2, 6.2)

D. RISORSE DELL'ORGANIZZAZIONE

Quali sono gli elementi caratterizzanti le risorse dell'organizzazione?

D1. Struttura organizzativa

- Sono definiti i ruoli e le responsabilità decisionali?
- Sono noti all'interno dell'organizzazione?
- Sono definiti opportuni livelli autorizzativi?
(5.1, 8.5.6)

D2. Risorse umane

- Sono identificate le risorse chiave di cui l'azienda ha necessità ai fini della propria operatività?
- Quanto l'azienda basa il proprio funzionamento sulla capacità delle proprie risorse e quanto sulla strutturazione dei propri processi?
- È valutato il rischio relativo al reperimento di personale adeguato sul mercato in caso di necessità o al mantenimento delle figure chiave?
- Sono valutate le motivazioni di attaccamento all'azienda, il clima aziendale e di eventuali situazioni critiche di turnover/assenteismo?
- Come sono valutate in azienda le aspettative delle risorse interne?
- Sono valutate le competenze delle persone e la necessità di miglioramento o aggiornamento delle stesse?
- È pianificata formazione adeguata per colmare le carenze?
(4.1, 4.2, 5.1, 6.1, 7.2, 7.3, 7.1.6)

D3. Ambienti di lavoro

- Sono valutati metodi di lavoro creativi ed opportunità di maggiore coinvolgimento, regole per la sicurezza, fattori psicologici quali carico di lavoro e stress?
- Gli ambienti sono adeguati all'esecuzione del lavoro da parte del personale (spazi, movimentazione, ergonomia, accessibilità, sicurezza, salubrità)?
- Esistono requisiti aggiuntivi, legati ad esempio all'immagine nei confronti di clienti / utenti, a necessità di crescita degli spazi, ecc.?
(4.1, 4.2, 6.1)

D4. Risorse informatiche

- Sono state individuate le risorse informatiche fondamentali (software, fornitori)?
- Sono previste misure di protezione delle informazioni?
- Le informazioni sono disponibili dove servono?
- Le informazioni sono affidabili?
- Ne è prevista la gestione in caso di situazioni di emergenza?
(4.1, 6.1, 7.3, 7.1.6)

D5. Risorse tecnologiche

- L'organizzazione ha valutato l'adeguatezza degli impianti tecnologici rispetto a: prestazioni e capacità, costi di produzione, obsolescenza e tendenze emergenti, concorrenza, manutenibilità, adattabilità alle richieste dei clienti?
- In caso di cambiamento tecnologico, la stima dei rischi relativi?
(4.1, 6.1, 7.4, 7.1.6)

D6. Risorse naturali ed energetiche

- L'organizzazione dovrebbe considerare i rischi e le opportunità correlati alla disponibilità, alla variazione del costo ed all'utilizzo di energia e di risorse naturali nel breve e nel lungo periodo, sia nell'ambito della progettazione e dello sviluppo del prodotto, così come allo sviluppo dei propri processi. Come è gestito l'approccio all'utilizzo delle risorse naturali ed energetiche?
(4.1, 6.1, 7.1.6)

D7. Materie prime

- In caso di aziende dipendenti da materie prime questo elemento potrebbe rivelarsi fondamentale, ed i rischi relativi potrebbero essere legati a: costi delle materie prime e volatilità dei prezzi, provenienza delle materie prime da paesi a rischio, sostituibilità delle stesse, stabilità della qualità delle materie prime / semilavorati acquisite, deperibilità delle materie prime. Questi elementi vengono valutati?
- Qual è l'approccio all'approvvigionamento delle materie prime?
(4.1, 6.1, 7.1.6)

E. PROCESSI

Sono stati definiti i processi e come sono governati dall'organizzazione?

E1. Definizione del perimetro del sistema di gestione

- È definito il campo di applicazione del sistema di gestione?
- C'è coerenza dell'ambito dei sistemi di gestione rispetto a strategie e rischi identificati?
(4.3)

E2. Descrizione dei processi, input necessari e output previsti

- Esiste una mappatura dei processi che preveda l'identificazione e valutazione di input e output, ruoli e responsabilità, prassi operative consolidate, procedure e istruzioni?
- La documentazione del sistema di gestione è adeguata alle necessità aziendali e per dare confidenza che i processi siano gestiti come previsto?
- La documentazione di sistema è stata modificata per riflettere le modifiche apportate all'organizzazione?
- I processi/aspetti significativi operativi verificati sono stati valutati e giudicati conformi ai requisiti dello standard di riferimento?
- Sono definiti gli obiettivi del Sistema di gestione?
(4.4, 6.2, 7.5)

E3. Strumenti di controllo

- Come viene gestita la disponibilità di sistemi di monitoraggio dell'efficacia dei processi e della conformità dei prodotti e dei servizi?
- Come viene valutata la prestazione e l'efficacia dei sistemi di gestione (qualità / ambiente)?
- Come è valutata l'efficacia dei processi di Riesame della Direzione e degli audit interni?
- Quando necessario, come sono gestiti gli strumenti di monitoraggio?
- Le registrazioni disponibili sono sufficienti per il monitoraggio dei sistemi?
(7.1.5, 8.1, 9.1.1, 9.2, 9.3)

E4. Gestione dei cambiamenti e Preparazione della risposta alle emergenze

- Come viene gestita la pianificazione e analisi dei rischi legati ai cambiamenti di processo / prodotto?
- Come viene gestita la capacità di gestione delle modifiche non pianificate?
- Come viene gestita la capacità di gestione delle emergenze?
(6.1.1, 6.3, 7.1.6, 8.1, 8.5.6)

E5. Risultati e miglioramento delle prestazioni

- Come viene gestita la disponibilità dei risultati, l'analisi di coerenza con gli obiettivi e decisioni?
- Come vengono pianificate le azioni di miglioramento e messa a disposizione delle risorse?
- I progressi delle attività programmate e gli obiettivi sono monitorati dalla Direzione per garantire un miglioramento continuo?
- Come è valutata l'efficacia delle azioni correttive?
- Le registrazioni sono sufficienti per il monitoraggio del raggiungimento degli obiettivi?
- Come sono gestite le non conformità e le azioni correttive?
(8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 9.1, 9.3, 10.2)

E6. Comunicazione

- Quali sono i destinatari della comunicazione istituzionale aziendale?
- Sono definite le responsabilità della comunicazione?
- Come viene gestita la comunicazione aziendale?
- Sono definiti e controllati i canali di comunicazione all'esterno (WEB, social networks)?

- Uso corretto del marchio di certificazione e di altri riferimenti alla certificazione?
- Esistono dei piani di comunicazione di emergenza?
- Ruoli e responsabilità sono compresi e condivisi all'interno dell'organizzazione?
- La politica della qualità / ambientale è comunicata e compresa a tutti i livelli?
(7.4)

F. FORNITORI E PARTNERS

Quali sono le caratteristiche dei fornitori e dei partner dell'azienda?

F1. Analisi dei fornitori di prodotti e servizi

- L'organizzazione ha analizzato la qualità e stabilità del prodotto e servizio, la conformità alle leggi, la capacità produttiva, la flessibilità, la competenza, le tecnologie, la disponibilità al problem solving, e l'affidabilità dei fornitori, partner e outsourcer?
- L'organizzazione ha analizzato la diversificazione del parco fornitori? La capacità di trattativa commerciale? La capacità di pianificazione acquisti e gestione magazzino (valorizzazione finanziaria, deperibilità prodotti, tempi di consegna)?
- L'organizzazione ha valutato la disponibilità di fornitori di emergenza quando necessario?
(4.2)

F2. Outsourcing

- Sono stati definiti i criteri di controllo dei processi in outsourcing in funzione dell'impatto sulla conformità del prodotto/servizio?
- Sono disponibili registrazioni di tali controlli?
(4.2, 5.1.2, 5.2, 8.4)

G. ALTRE PARTI INTERESSATE

Quali sono i portatori di interesse e quali sono le loro aspettative tali da influenzare i risultati dell'organizzazione, (se non già inseriti in altri punti)?

G1. Altre parti interessate

- Sono identificate eventuali altre parti interessate che possono influenzare i risultati dell'organizzazione?
- Quali sono le parti interessate individuate (Es. famiglie dei dipendenti, fornitori, comunità locali, pubblica amministrazione, sindacati, soci, azionisti, investitori, consumatore/utente finale, ecc.)?
(4.2)

G2. Analisi delle aspettative delle altre parti interessate e gestione delle relazioni

- Sono state valutate le aspettative delle parti interessate che sono rilevanti per i risultati dell'organizzazione?
- Sono evidenziate eventuali criticità e contraddizioni rispetto alla politica e agli obiettivi dell'organizzazione?
- Sono definite le responsabilità per la comunicazione e mediazione con le parti interessate?
- Sono gestiti i rischi?
(4.2)

H. CONTESTO E GESTIONE DEI RISCHI

Qual è l'approccio dell'Organizzazione al contest, alle parti interessate, alla valutazione di rischi ed opportunità?

H1. Approccio al contesto e alle parti interessate

- I fattori interni ed esterni che influenzano la capacità di raggiungere i risultati attesi per il business sono stati identificati?
- Quale livello di formalità è necessario per avere il necessario coinvolgimento delle parti interessate interne ed esterne all'Organizzazione?
(4.1, 4.2)

H2. Analisi delle aspettative delle altre parti interessate e gestione delle relazioni

- Qual è l'approccio dell'Organizzazione alla gestione di rischi ed opportunità?

- Qual è l'approccio nella formalizzazione di metodologie e risultati relativi all'approccio al rischio?
- Qual è il coinvolgimento delle parti interessate?
(6.1, 6.2)

13.2.1.3 Integrazione fra i due criteri di analisi del contesto

		Richieste della Norma UNI EN ISO 9001:2015							
		Prodotti / Servizi	Mercato /Clienti	Proprietà	Risorse	Processi	Fornitori e partners	Altre parti interessate	Contesto e gestione rischi
Modello di analisi	A. Partnership chiave								
	B. Attività chiave								
	C. Risorse chiave								
	D. Valore offerto								
	E. Relazioni con i clienti								
	F. Canali								
	G. Segmenti di clientela								
	H. Struttura dei costi.								
	I. Flussi di ricavi								
	L. Altri Elementi								

13.2.1.4 Fattori Interni ed Esterini

Per ogni elemento individuato nel punto precedente è opportuno riconoscere i punti forti e deboli (fattori interni) dell'organizzazione e per esaminare le opportunità ed i rischi che si possono incontrare (condizioni esterne)⁶⁶.

Fattori Interni

PUNTI DI FORZA.

Risorse o capacità che l'organizzazione può impiegare per raggiungere gli obiettivi.

PUNTI DI DEBOLEZZA.

Sono limitazioni, difetti, limiti che, se non sono rimossi, possono impedire parzialmente o totalmente il raggiungimento degli obiettivi.

Fattori Esterini

OPPORTUNITÀ.

Condizione favorevole dell'ambiente in cui opera l'organizzazione.

MINACCE O RISCHI.

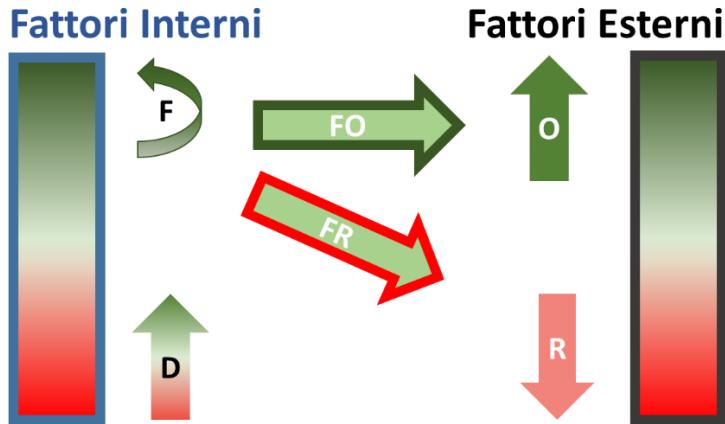
Situazioni sfavorevoli che possono potenzialmente compromettere le strategie ed il raggiungimento degli obiettivi.

Anche in questo caso è opportuno indicare sia informazioni valide per tutta l'organizzazione che informazioni specifiche per linea di business.

Strategie

⁶⁶ In analogia al metodo SWOT

La definizione di tutti i fattori interni ed esterni permetterà di definire ed attuare le seguenti strategie:



- F: Come mantenere e, se possibile, aumentare i punti di forza.
- D: Come superare i punti di debolezza per farli diventare, se possibile, punti di forza. Bisogna puntare a stemperare i fattori di debolezza (mitigando quindi gli eventuali impatti negativi) e, per quanto possibile, ricercare il modo di tramutarli in punti di forza (in grado di cogliere opportunità).
- O: Come sfruttare le opportunità.
- R: Come gestire i rischi. È necessario ricercare e definire le azioni da mettere in atto allo scopo di evitare che le minacce abbiano il sopravvento sui punti di debolezza insiti nel contesto.
- FO: Come utilizzare i punti di forza per sfruttare le opportunità. Vanno considerate tutte le possibili opportunità fornite dai punti di forza individuati e messi a punto gli interventi che ne possano amplificare l'impatto positivo.
- FR: Come utilizzare i punti di forza per contrastare le minacce ed i rischi. Bisogna fare leva sullo sfruttamento dei punti di forza al fine di ridurre gli impatti negativi conseguenti ad un eventuale materializzarsi degli eventi minacciosi.

13.2.1.5 Esigenze ed aspettative delle Parti Interessate

Per ogni elemento di analisi individuato in precedenza è opportuno, inoltre, individuare le Parti Interessate (stakeholder) al fine di definirne l'importanza delle loro esigenze ed aspettative.

Ancora una volta è opportuno indicare le esigenze ed aspettative valide per tutta l'organizzazione e quelle specifiche per ogni linea di business.

13.3 Modalità operative

13.3.1.1 Contesto

Alla definizione del primo Riesame vengono proposti i 10 elementi di analisi nel folder "Contesto".

Nei Riesami successivi potranno essere copiate tutte le informazioni dal Riesame precedente per effettuare le opportune modifiche.

Per ogni elemento dovranno essere inserite le caratteristiche generali valide per tutte le linee di business.

Sotto ogni elemento è possibile definire eventuali caratteristiche specifiche per le varie linee di business.

13.3.1.2 Fattori Interni ed Esterni

Sotto ogni elemento di analisi del contesto è possibile inserire i Fattori (interni ed esterni).

Per ogni Fattore viene richiesto il tipo per identificare e “graduare” il fattore:

- Fattori Interni:
 - Punto di Forza Significativo.
 - Punto di Forza.
 - Punto di Debolezza.
 - Punto di grave Debolezza.
- Fattori Esterni
 - Opportunità Importante.
 - Opportunità.
 - Minaccia o Rischio.
 - Rischio significativo.

È quindi possibile inserire la Linea di Business. Qualora non venga inserita il fattore verrà considerato valido per tutte le Linee di Business.

Ogni fattore è caratterizzato da un Codice (che deve essere univoco per il Riesame) e da una descrizione.

13.3.1.3 Esigenze ed Aspettative delle Parti Interessate

Sempre sotto ogni elemento di analisi del contesto è possibile inserire anche le esigenze e le aspettative delle Parti Interessate.

Anche per le Parti interessate è possibile inserire la Linea di Business. Qualora non venga inserita le informazioni verranno considerate valide per tutte le Linee di Business.

Viene quindi richiesta l’importanza (su 7 livelli).

Per ogni Esigenza ed Aspettativa è necessario inserire un Codice (univoco per il Riesame), la Tipologia e la Parte Interessata.

13.3.1.4 Stampe dell’Analisi del Contesto

Dal Riesame è possibile richiedere varie stampe dell’Analisi.

Analisi del Contesto (Excel)

Viene prodotto un documento Excel nel quale vengono presentati nelle varie cartelle:

- ELEMENTI: Tutti gli Elementi di Analisi (con l’indicazione di quelli specifici per una particolare Linea di Business).
- PARTI: Le Esigenze ed aspettative delle Parti Interessate.
- PUNTI: I vari Fattori Interni ed Esterni suddivisi per Elementi di Analisi.
- FATTORI: Il riepilogo di tutti i Fattori Interni ed Esterni, ordinati dai più positivi ai più negativi. Fra parentesi quadre vengono indicate le eventuali Linee di Business specifiche.

Analisi del Contesto (Word)

Viene prodotto un documento Word nel quale vengono riportati tutti gli Elementi di Analisi con, dove inseriti:

- Informazioni degli Elementi relative a specifiche Linee di Business.
- Elementi per l’Analisi dei Fattori Interni ed Esterni (fra parentesi quadre vengono indicate le eventuali Linee di Business specifiche).
- Esigenze ed aspettative delle Parti Interessate (fra parentesi quadre vengono indicate le eventuali Linee di Business specifiche).

Analisi del Contesto per Linee di Business (Word)

Viene prodotto un documento Word nel quale vengono riportati tutte le informazioni relative ad ogni Linea di Business (considerando anche le informazioni valide per tutte le Linee):

- Elementi di Analisi.
- Elementi per l'Analisi dei Fattori Interni ed Esterni.
- Esigenze ed aspettative delle Parti Interessate.

14 APPENDICE: Analisi del Rischio per Processi

14.1 Introduzione

Definizione di Rischio

Il rischio può essere definito con varie modalità. Una delle definizioni generali condivisibili è la seguente:

“la minaccia o la possibilità che un’azione o un evento produca effetti favorevoli o avversi in un’organizzazione permettendo o meno il raggiungimento degli obiettivi”.

La norma ISO 31.000 lo definisce invece come **“effetto dell’incertezza sugli obiettivi”** ed è sostanzialmente correlato ai fattori che determinano l’incertezza di raggiungere un determinato obiettivo.

Cos’è il Rischio?

Il rischio è una deviazione dal risultato atteso: tale deviazione può essere positiva o negativa

Il rischio è spesso caratterizzato per il riferimento a “eventi potenziali” e alle loro “conseguenze” o alla combinazione di essi.

L’incertezza è lo stato, anche parziale, della mancanza di informazioni relative a comprensione o conoscenza di un evento, delle sue conseguenze o aspettative.

Cos’è il Risk Management?

Definizione generale:

“sistematica applicazione di politiche, prassi e procedure di gestione nelle fasi di analisi, valutazione, trattamento, misurazione e registrazione del rischio”.

La norma ISO 31.000 lo definisce invece come **“attività coordinate per guidare e tenere sotto controllo una organizzazione con riferimento al rischio”**.

Gli 11 principi di gestione del Rischio

La gestione del rischio:

- Crea e protegge il valore.
- È parte integrante di tutti i processi dell’organizzazione.
- È parte del processo decisionale.
- Tratta esplicitamente l’incertezza.
- È sistematica, strutturata e tempestiva.
- Si basa sulle migliori informazioni disponibili.
- È “su misura”.
- Tiene conto dei fattori umani e culturali.
- È trasparente e inclusiva.
- È dinamica, iterativa e reattiva al cambiamento.
- Favorisce il miglioramento continuo dell’organizzazione.

Le fasi di una corretta gestione del Rischio

Le fasi principali di una corretta gestione del rischio sono le seguenti:

- Identificazione del rischio.
- Analisi del rischio.
- Ponderazione del rischio.

- Trattamento del rischio.
- Monitoraggio e riesame del rischio.

Identificazione del Rischio

L'obiettivo di questa fase è quello di individuare un elenco esaustivo dei rischi.

L'identificazione di tutti i possibili rischi è critica in quanto un rischio (che come abbiamo visto può avere effetti positivi o negativi) non identificato non viene considerato ed analizzato in modo adeguato.

La Direzione Aziendale applica strumenti e tecniche di identificazione dei rischi adatte ai propri obiettivi e capacità ed ai rischi che deve fronteggiare. Nell'identificazione dei rischi sono necessarie informazioni pertinenti ed aggiornate (per quanto possibile anche derivanti da conoscenze ed esperienze pregresse). Nell'identificazione dei rischi sono coinvolte le funzioni aziendali interessate.

I rischi associati al raggiungimento degli obiettivi sono opportunamente individuati all'interno di SQuadra in SQ / ANALISI / RIESAMI / ANALISI PROCESSI (sia per i processi principali sia per i processi di supporto).

Analisi del Rischio

L'analisi del rischio viene effettuata in modo soggettivo dalla Direzione Aziendale con in coinvolgimento eventuale delle funzioni aziendali interessate.

I possibili livelli di rischio sono determinati dall'indice di Rischio Iniziale (IR) e sono i seguenti:

Per Rischi con effetti negativi:

	Altissimo	È un livello che rischia di pregiudicare il proseguimento dell'attività aziendale e quindi di mette a repentaglio la vita stessa dell'impresa.
	Molto alto	È un livello che, a medio/lungo tempo, rischia di pregiudicare il proseguimento dell'attività aziendale. Mette a repentaglio la continuità dell'impresa.
	Alto	È un livello di rischio che non mette a repentaglio la vita dell'impresa ma che può comportare la perdita di importanti quote di mercato, può incidere molto negativamente sull'immagine aziendale, può pregiudicare in modo significativo la soddisfazione del cliente.
	Medio	È un livello di rischio che se sottovalutato e non correttamente gestito può portare a perdite anche significative per l'impresa.
	Basso	È un livello di rischio accettabile che può portare perdite poco significative per l'impresa e/o che può incidere in modo poco significativo sui livelli di soddisfazione del cliente.
	Molto basso	È un livello di rischio perfettamente adeguato.
	Trascurabile	È un livello di rischio non rilevabile.

Per Rischi con effetti positivi:

	Altissimo	È un livello che può pregiudicare una opportunità di rapida crescita o un significativo consolidamento dell'impresa che raramente potrebbe ripresentarsi.
	Molto alto	È un livello di opportunità che potrebbe non ripresentarsi che, a medio/lungo tempo, rischia di pregiudicare una crescita o un consolidamento dell'impresa.

	Alto	È un livello di rischio che, se non si coglie, può comportare la perdita dell'opportunità di aumentare importanti quote di mercato, di incidere molto positivamente sull'immagine aziendale, può accrescere in modo significativo la soddisfazione del cliente.
	Medio	È un livello di rischio che se sottovalutato e non correttamente gestito può portare alla perdita di opportunità significative per l'impresa.
	Basso	È un livello di rischio accettabile che può portare alla perdita di opportunità poco significative per l'impresa e/o che possono incidere in modo poco significativo sui livelli di soddisfazione del cliente.
	Molto basso	È un livello di rischio che, in genere, non richiede di cogliere le opportunità.
	Trascurabile	È un livello di rischio in cui le opportunità non sono rilevabili.

Ponderazione del Rischio

La ponderazione del rischio consiste sostanzialmente in due processi. Il primo è l'individuazione delle misure in atto per la gestione dei rischi. Tali misure consentono generalmente una riduzione del livello di rischio (prevenendo gli aspetti negativi e cogliendo le opportunità) tra quello iniziale e quello residuo.

Il secondo processo è quello di consentire di individuare una priorità di intervento in base al livello dei valori del Rischio residuo.

Il Rischio residuo è il livello di rischio presente e valutato in seguito all'adozione delle misure eventualmente in atto per la gestione del rischio.

I tempi di intervento sono correlati ai seguenti livelli di Rischio:

	Altissimo	Richiede interventi immediati.
	Molto alto	Richiede l'immediata pianificazione degli interventi.
	Alto	Richiede interventi rapidi e tempestivi (generalmente entro un mese).
	Medio	Richiede interventi tempestivi (generalmente entro tre mesi).
	Basso	L'azienda deve decidere se prevedere specifici interventi.
	Molto basso	In genere non sono obbligatori interventi specifici.
	Trascurabile	Non sono previsti interventi specifici.

Trattamento del Rischio

I possibili trattamenti del rischio sono i seguenti:

- Evitare il rischio se negativo.
- Conseguire un'opportunità.
- Rimuovere la fonte di rischio se negativo.
- Stimolare le Opportunità.
- Modificare la probabilità.
- Modificare le conseguenze.
- Condividere il rischio.
- Mantenere sotto controllo il rischio.

La Direzione Aziendale deve definire il rischio residuo accettabile (vedi SG / ANALISI / CRITERI DELLA DIREZIONE). Oltre tale livello dovranno essere previste ulteriori misure rispetto a quelle già in atto.

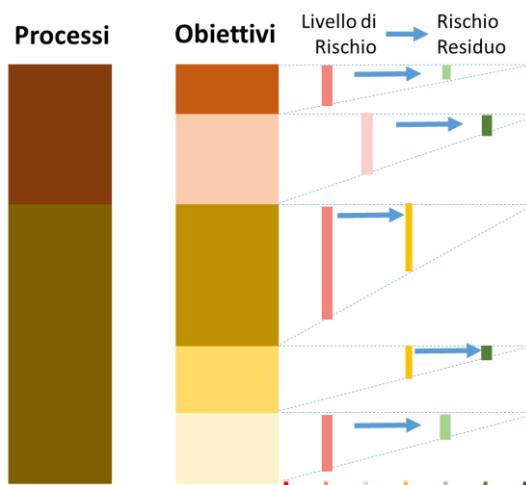
Le azioni da svolgere per livelli di rischio residuo uguale o superiore al rischio definito come accettabile sono individuate in specifici obiettivi o piani di miglioramento su SQuadra in SQ / ANALISI / RIESAMI / ANALISI PROCESSI e/o riportati nel Riesame della Direzione.

Monitoraggio e riesame del Rischio

In seguito all'attuazione del piano di miglioramento e di gestione e trattamento del rischio con le azioni tempificate, la Direzione Aziendale effettua, con la collaborazione dei vari responsabili, un monitoraggio ed una rivalutazione del rischio.

Il monitoraggio e la rivalutazione fanno parte del processo di gestione del rischio.

14.2 Processi



Per ogni Processo vengono definiti i vari Obiettivi con Rischi ed Opportunità. Per ogni Obiettivo viene definito il Livello di Rischio e il Rischio Residuo a seguito delle Misure Adottate.

In funzione dell'Importanza relativa dei vari Processi ed a quella dei vari Obiettivi di ogni Processo è possibile sommare il peso delle valutazioni.

Importanza dei Processi

Viene richiesto di descrivere i principali Processi ed i Processi di Supporto indicando:

- Responsabile.
- Risorse.
- Input e Output.
- Metodi (compresi il monitoraggio, le misurazioni e gli indicatori di prestazione) necessari ad assicurare l'efficace funzionamento.
- I principali documenti.

Per ogni Processo (Principale o di Supporto) viene richiesta l'importanza (su 7 livelli). In base alle varie importanze definite viene assegnata una percentuale di importanza ai vari Processi.

Rischi ed Opportunità per i vari Obiettivi

Per ogni Processo vengono definiti i vari Rischi/Opportunità legati ai vari Obiettivi.

È necessario definire un'importanza del Rischio/Obiettivo (su 7 livelli) in base alla quale viene definita l'incidenza percentuale rispetto al Processo.

Viene quindi definito il Livello di Rischio ed il Rischio Residuo a seguito delle Misure Attuali.

È possibile indicare il Criterio per determinare Misure Aggiuntive per il miglioramento (in genere quando il Rischio Residuo supera il livello Medio).

14.3 Analisi

Prospetto Rischi/Opportunità per Processo (Excel)

Per ogni Processo

Una prima analisi viene effettuata su un documento di Excel nel quale nella cartella RISCHI vengono presentati, per ogni Processo:

- L'importanza percentuale del Processo (vedi cartella Processi).
- L'importanza per ogni Rischio/Opportunità (100% per il singolo Processo in funzione dell'Importanza relativa definita) e sul Totale (100% su tutti i Processi).
- Il Valore del Livello di Rischio (in base alla valutazione), l'effetto sul singolo Processo (Livello di Rischio per importanza relativa del Rischio/Opportunità per il Processo) ed il valore pesato su tutti i Processi (Livello di Rischio per l'importanza relativa del Rischio/Opportunità sul totale dei Processi).
- Il Valore del Rischio Residuo ed il suo impatto sul Processo e su tutti i Processi.

Nella cartella PROCESSI viene riportata, per ogni Processo:

- L'Importanza percentuale (100% su tutti i Processi in funzione dell'importanza definita).
- Il Livello di Rischio (somma delle valutazioni per Processo riportati nella cartella RISCHI [colonna M]) e il Peso Aziendale (somma colonna N della cartella RISCHI).
- Il Rischio Residuo (somma colonna P cartella RISCHI) e il Peso Aziendale (somma colonna Q cartella RISCHI).

La somma dei Pesi Aziendali fornisce una indicazione complessiva di quanto le Misure adottate riducono il Livello di Rischio.

Prospetto Rischi/Opportunità per Processo (Word)

Il programma produce un documento di Word contenente tutte le informazioni inserite.

Nel documento di Word verranno segnalati i Rischi/Opportunità per i quali, pur essendo il Rischio Residuo superiore al livello previsto dalla Direzione (ed inserito il SG / Analisi / Criteri della Direzione), non sono indicate Misure Aggiuntive.

15 APPENDICE: Valutazione Fornitori

15.1 Introduzione

SQuadra231 fornisce un supporto per una valutazione articolata dei vari fornitori differenziata per tipologia e pesando le rilevazioni rispetto al tempo.

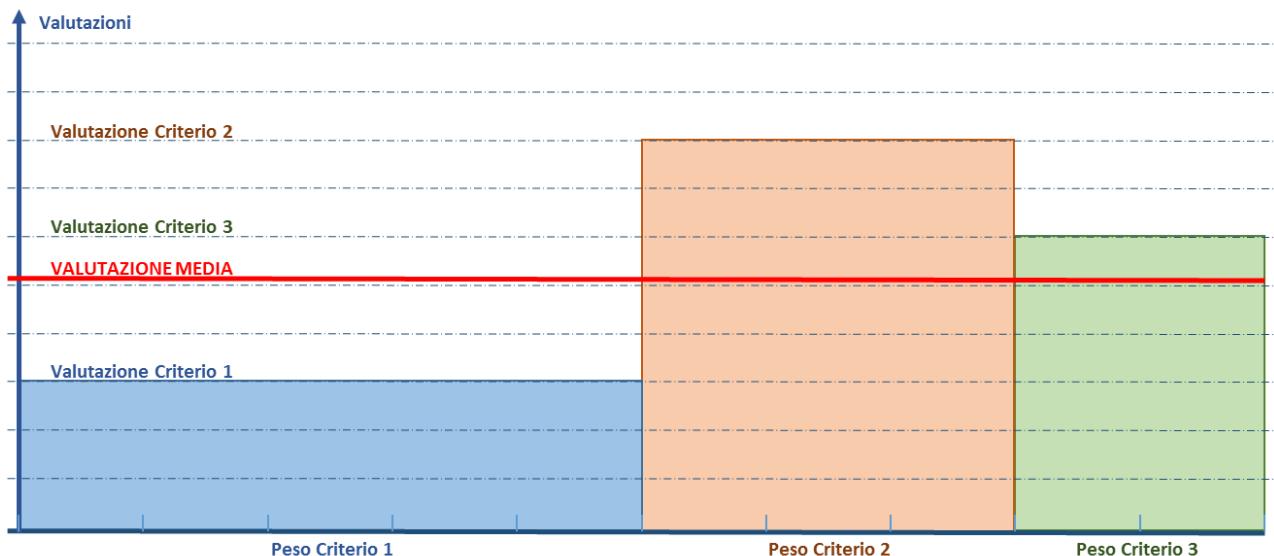
Nella presente appendice vengono presentati per primi gli aspetti teorici e quindi le modalità operative.

15.2 Criteri per la Valutazione

15.2.1.1 Valore riepilogativo per ogni rilevazione

Per ogni Rilevazione è opportuno valutare vari elementi (Qualità della fornitura, Rispetto dei Tempi, Disponibilità, ecc.).

Per ottenere una Valutazione riepilogativa non è opportuno effettuare una banale media aritmetica (che considera tutti gli elementi ugualmente significativi) ma differenziare l'importanza da assegnare ai vari elementi.



Per ogni rilevazione le valutazioni sui singoli criteri di analisi verranno pesate al fine di ottenere una valutazione di sintesi (che ovviamente terrà maggiormente in conto le valutazioni sui criteri con maggiore peso)⁶⁷.

Significato della valutazione

Come indicato le valutazioni possono riferirsi a vari elementi. Per tutte le valutazioni si utilizza una scala da 1 a 10.

Al fine di rendere la valutazione più omogenea possibile fra i vari valutatori verrà utilizzata la seguente tabella di riferimento (che andrà ovviamente adattata alle specificità dell'elemento in valutazione).

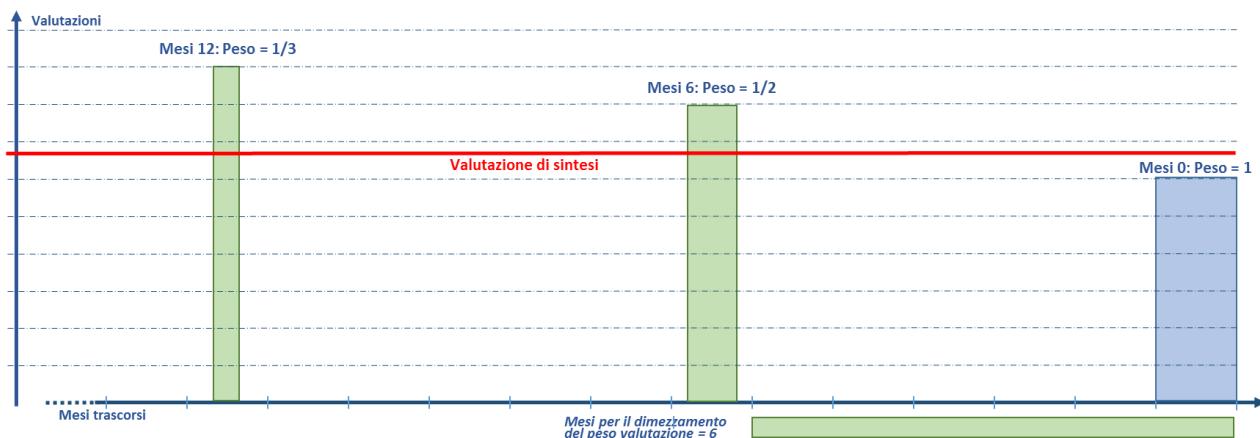
⁶⁷ Valutazione Media = Somma (Valutazione del Criterio_i x Peso percentuale del Criterio_i)

Valore	Significato
2	Per l'elemento non sono stati rispettati gli impegni esplicativi e, neppure a seguito di sollecitazioni, è stato possibile ottenerne il rispetto.
4	Per l'elemento non sono stati rispettati gli impegni esplicativi e, solo a seguito di sollecitazioni è stato possibile ottenerne il rispetto.
6	Per l'elemento sono stati rispettati gli impegni esplicativi.
8	Per l'elemento sono stati rispettati sia gli impegni esplicativi che quelli impliciti e le aspettative.
10	Per l'elemento sono stati rispettati tutti gli impegni superando le aspettative.

15.2.1.2 Valore riepilogativo fra più rilevazioni

Le valutazioni medie relative alle rilevazioni periodiche (ognuna ottenuta come indicato precedentemente) verranno “mediate”, fra di loro, tenendo in maggior conto le ultime rilevazioni rispetto a quelle precedenti.

In questo caso il “peso” della singola rilevazione è inversamente proporzionale al tempo trascorso e dipende dal Tempo di Dimezzamento espresso in mesi⁶⁸.



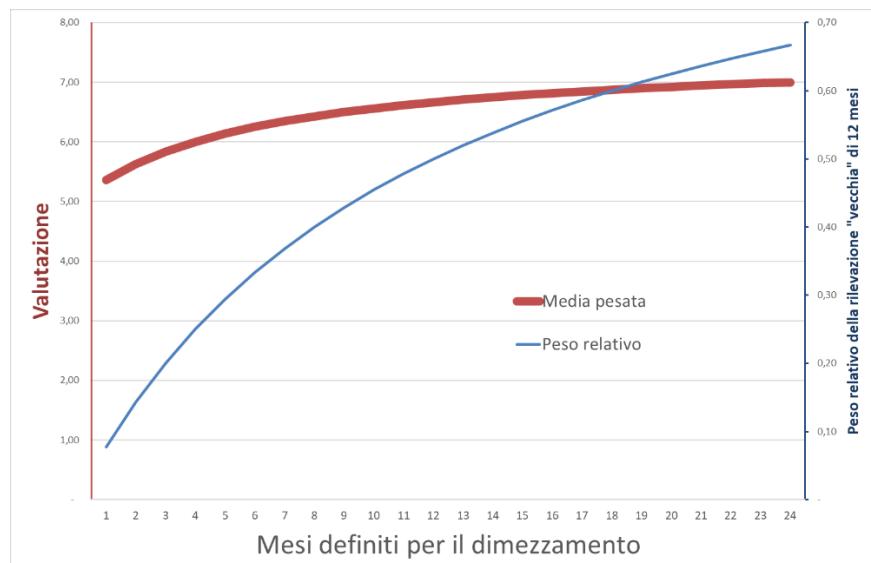
Supponiamo che il tempo di dimezzamento sia uguale a 6 mesi. Rispetto ad una valutazione attuale una valutazione di 6 mesi fa avrà un peso pari a 0,5 mentre una di 12 mesi fa avrà un peso pari a 0,333. Il valore di sintesi fra 3 rilevazioni (nell'esempio: attuale=6, a 6 mesi=8 e a 12 mesi=9) darà un valore (6,72) influenzato soprattutto dagli ultimi valori.

Supponiamo di rilevare una valutazione pari a 4. Otterremo una valutazione media per il fornitore pari a 5 se nello stesso mese è stata rilevata una valutazione pari a 6 qualunque sia il tempo di dimezzamento scelto.

Se consideriamo il tempo di dimezzamento pari a 12 mesi sempre per ottenere una media pari a 5 utilizzando una rilevazione vecchia di un anno sarà necessario che la valutazione sia pari a 7 per compensare la minor significatività della valutazione. Più aumentano i mesi trascorsi dalla precedente valutazione e più alto dovrà essere la valutazione precedente per poter ottenere la stessa media.

Considerando un tempo di dimezzamento pari a 6 mesi avremo un maggior “decadimento” e, sempre a titolo d'esempio, sarà necessaria una valutazione pari ad 8 vecchia di un anno o una valutazione pari a 7 rilevata a 6 mesi.

⁶⁸ Valutazione Media = Somma (Valutazione_i / (Mesi_i / MesiDimezz.+1)) / Somma (1/(Mesi_i / MesiDimezz.+1))



Nell'esempio riportato nella figura precedente viene considerata una valutazione attuale pari a 5 ed una valutazione rilevata 12 mesi fa pari a 10. Ovviamente la valutazione complessiva sarà un valore compreso fra 5 (nel caso si voglia trascurare la vecchia valutazione: mesi di dimezzamento = 0) e 7,5 (media aritmetica che assegna lo stesso peso alle 2 valutazioni: mesi di dimezzamento = infiniti).

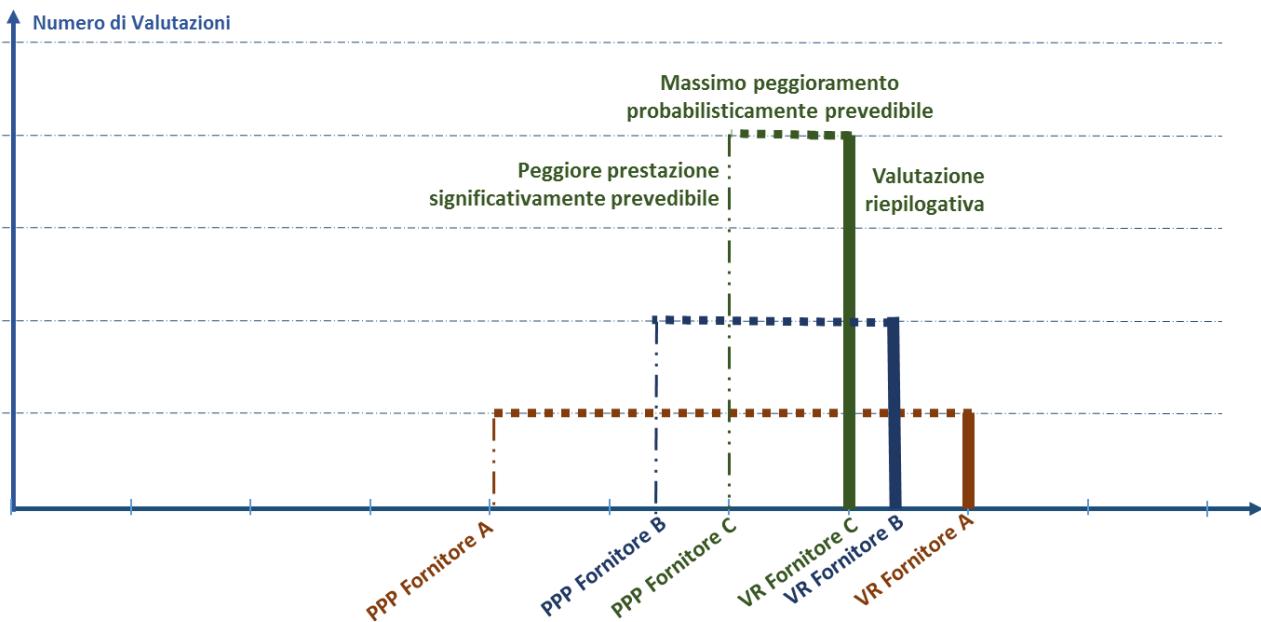
Con questo metodo è possibile riportare alla data attuale tutte le valutazioni con un valore medio “pesato” in funzione della distribuzione temporale delle rilevazioni ed ottenere un valore che identifica il numero di rilevazioni “equivalenti” sulle quali si basa il valore medio se fossero state rilevate tutte in data odierna.

15.2.1.3 Confronto fra le valutazioni riepilogative di vari fornitori

La valutazione attesa più probabile per ogni fornitore coinciderà sempre con la valutazione riepilogativa ottenuta come sopra indicato. È però evidente che esiste una probabilità significativa che la prossima prestazione differisca dalla valutazione riepilogativa.

Cautelativamente, nel confronto fra più fornitori, è opportuno valutare il valore più basso atteso con probabilità “significativa” e non banalmente il valore più probabile.

In pratica è preferibile scegliere un fornitore che ha una valutazione pari a 7 che deriva da molte valutazioni recenti piuttosto che un fornitore che, in una sola occasione e lontana nel tempo, ha ottenuto una valutazione pari a 8 perché la probabilità che la prestazione del primo fornitore non dovrebbe discostarsi da 7 è molto alta mentre è possibile che la prestazione del secondo fornitore si discosti anche di molto da 8.



Per confrontare le valutazioni di vari fornitori è da tener presente, quindi, non solo il valore riepilogativo, ottenuto come indicato in precedenza, ma anche l'attendibilità di questo valore in funzione del numero di rilevazioni "equivalenti".

Al crescere del numero di rilevazioni diminuisce la possibilità che una futura valutazione differisca molto da questo; per contro una singola valutazione, anche positiva, non garantisce che la prossima rilevazione non differisca anche notevolmente⁶⁹.

In una prima approssimazione possiamo pensare significativo attendersi che la prossima valutazione non possa essere peggiore della valutazione riepilogativa di un valore inversamente proporzionale alle rilevazioni "equivalenti" in relazione all'errore previsto nelle valutazioni (ER) per la tipologia di fornitori⁷⁰.

15.3 Modalità operative

15.3.1.1 Tipologie di Fornitori

Per prima cosa è necessario definire le Tipologie di Fornitori (Subappaltatori, Fornitori di Materiali, Fornitori di Macchinari, Consulenti, ecc.).

Per ogni Tipologia è necessario definire il **Criterio di Qualifica** ed i **Criteri per il mantenimento** della qualifica.

Dovranno essere indicati i **Mesi di dimezzamento** (in genere un valore compreso fra 6 e 36). Un valore alto permetterà di considerare significative anche le rilevazioni più vecchie mentre un valore basso considererà soprattutto le ultime rilevazioni (ad esempio nel caso di un subappaltatore con grosso turnover interno).

⁶⁹ In una distribuzione normale o di Gauss possiamo ipotizzare una minor varianza all'aumentare del numero delle rilevazioni. Si ricorda che il 68,3% dei valori differirà dal valore medio per meno della varianza.

⁷⁰ Massimo peggioramento prevedibile = Peggioramento per Rilevazione / Numero di Rilevazioni

L'ultima informazione di carattere generale relativamente alla tipologia di fornitori è il **Peggioramento prevedibile per rilevazione** (in genere un valore compreso fra 1 e 3). Un valore alto indica rilevazioni non troppo significative o su elementi variabili, un valore basso indica valutazioni approfondite su forniture "ripetitive".

È quindi necessario definire gli elementi da utilizzare per la valutazione. È possibile definire fino a 5 criteri (Qualità, Costi, Rispetto dei tempi, ecc.) per ogni tipologia; per i vari criteri va definito il Peso relativo (il totale deve essere pari al 100%).

NOTA Per un utilizzo semplificato: è possibile definire, per tutte le tipologie:

- *Mesi di dimezzamento: 12 mesi.*
- *Peggioramento prevedibile: 2.*
- *Un solo criterio riepilogativo con peso = 100%*

15.3.1.2 Fornitori

Anagrafica

È possibile inserire i vari dati anagrafici fra i quali:

- Un codice univoco (ad esempio quello utilizzato nel programma contabile).
- L'indirizzo, il telefono e la mail aziendale.
- L'eventuale persona di Riferimento, con telefono e mail.

Per ogni Fornitore è necessario definire la tipologia.

Se un fornitore appartiene a più tipologie (ad esempio fornisce materiale ma, in alcuni casi, effettua anche la posa in opera) è necessario inserirlo più volte una per ogni tipologia (dopo aver inserito i dati Anagrafici è possibile duplicarlo modificando il Codice e la Tipologia e specificando la tipologia nella descrizione).

Qualifica

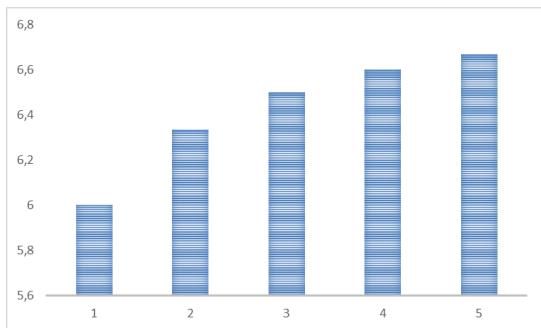
Vengono richiesti i dati relativi all'ultima qualifica (oltre alla prima qualifica è possibile prevedere sistematiche operazioni di riqualifica anche tenendo conto delle valutazioni di ritorno).

È quindi necessario definire la qualifica iniziale indicando:

- L'eventuale documento interno utilizzato per la qualifica (es. Questionario).
- La data dell'ultima valutazione.
- La Valutazione di sintesi.
- Responsabile della qualifica.
- Note relative alla modalità utilizzata per la qualifica (soprattutto se differiscono da quanto previsti per i criteri di qualifica previsti per la tipologia di fornitore).

Viene inoltre richiesto il "peso" della qualifica rispetto alle rilevazioni periodiche (numero di rilevazioni "equivalenti"). In funzione dell'accuratezza delle attività di qualifica o del numero di informazioni sulla quale essa si basa è necessario definire il suo effetto sulla valutazione complessiva sul fornitore in relazione alle singole rilevazioni periodiche. Un peso maggiore alla qualifica del fornitore permetterà di "attenuare" eventuali oscillazioni puntuali delle valutazioni periodiche.

Peso uguale a 1 indica che la valutazione di qualifica ha lo stesso peso delle valutazioni periodiche, con 2 varrà il doppio ecc. Ovviamente verranno considerate solo le valutazioni periodiche successive alla valutazione di qualifica (che racchiude già tutte le informazioni in possesso dell'azienda fino a quella data).



Supponendo di avere una qualifica pari a 7 ed una prima valutazione (nello stesso mese) pari a 5 il valore medio assegnato al fornitore risentirà della qualifica iniziale tanto più alto sarà il peso assegnato a questa.

Esclusione

È ovviamente possibile prevedere l'esclusione di alcuni Fornitori dall'albo.
Qualora si decida di escludere un fornitore è opportuno indicarne le motivazioni.
Il fornitore potrà essere riammesso attraverso una nuova operazione di qualifica.

15.3.1.3 Valutazioni

Per ogni Fornitore possono essere registrate le varie valutazioni (ovviamente in funzione della Tipologia).

15.4 Registro

Nel Registro vengono riportate, per ogni Fornitore, tutte le informazioni e la valutazione di sintesi che sintetizza tutte le rilevazioni pesandole fra di loro come indicato ed in funzione dei parametri definiti. Vengono inoltre riportate tutte le rilevazioni.

16 APPENDICE: Comunicazioni

16.1.1 Elementi da Comunicare

Base

Ogni Comunicazione è caratterizzata da:

- Data di Aggiornamento del Documento.
- File in formato PDF (il documento firmato da chi di dovere).
- Il file in formato WORD (opzionale) per permettere di effettuare il confronto versioni con eventuali nuovi documenti per evidenziare, in automatico, le novità.
- Delle note.

NOTA: è possibile inserire le consegne (vedi sotto) utilizzando un apposito file di Excel. In questo caso è necessario richiedere l'esportazione del file con i dati attuali relativi alle Consegne. Il file dovrà essere aggiornato con i nuovi dati e quindi importato.

Mail

È possibile definire il contenuto delle Mail che si desidera inviare:

NOTA: Ad ogni nuovo elemento vengono proposti dei testi d'esempio che devono essere personalizzati dall'utente.

- Oggetto della Mail.

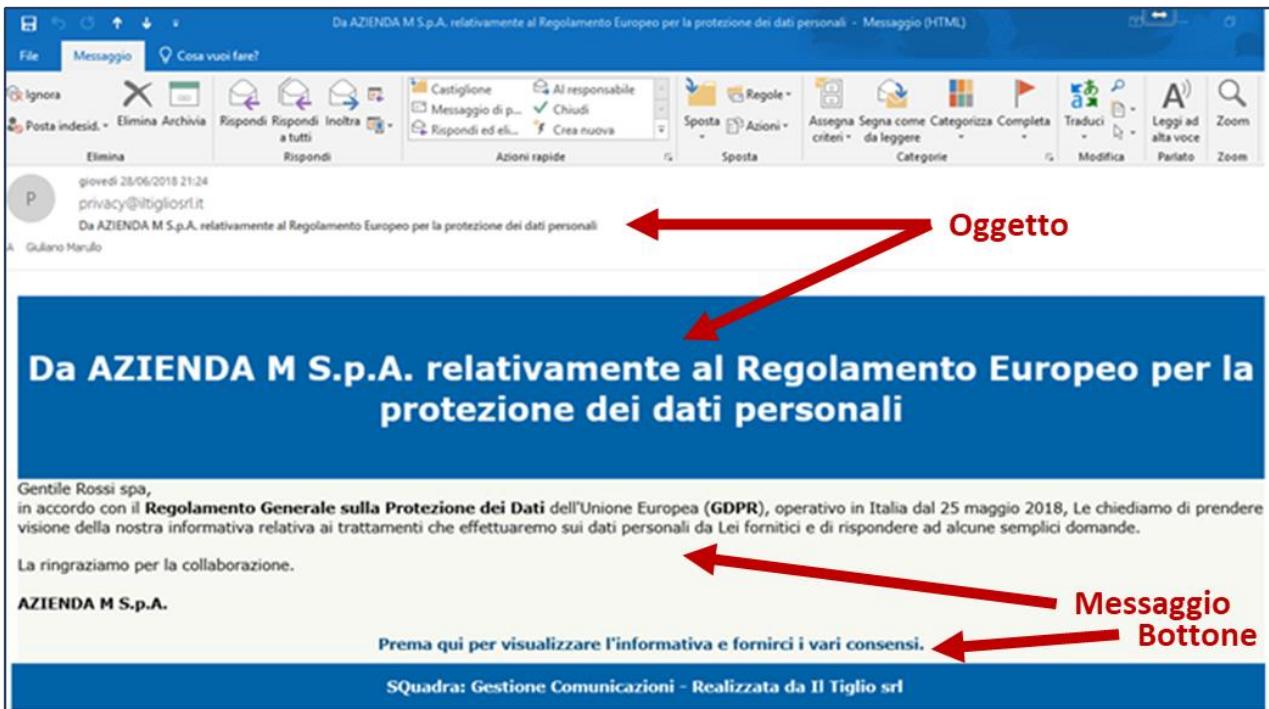
NOTA: Le mail vengono inviate da una casella di proprietà de "IL TIGLIO SRL" quindi è opportuno che nell'oggetto venga riportato il nome dell'azienda per evitare che i destinatari, non conoscendo il mittente, possano scambiarle per posta indesiderata.

Le mail vengono comunque inviate "per conto" dell'indirizzo mail indicato:

- Per le comunicazioni Privacy: come "Indirizzo di spedizione" fra le informazioni Aziendali (Vedi Documenti forniti da SQuadra).
- Per le altre comunicazioni: come "Mail per ricezione risposte alle comunicazioni" fra i Dati Aziendali.

In questo modo, se l'utente prova a rispondere, le risposte arrivino effettivamente all'azienda.

- Messaggio (contenuto della mail).
- Bottone per il richiamo della pagina di richiesta.
- Giorni per il sollecito (se viene inserito un numero maggiore di 0 verranno effettuati dei solleciti periodici fino all'ottenimento della risposta).
- Numero di Solleciti previsti (se vuoto verranno inviati solleciti fino all'ottenimento della risposta).
- Testo della Mail di Sollecito.



Esempio di mail (relativa alla Privacy) inviata da SQuadra sulla base dei dati impostati dall'utente.

Pagina di richiesta

- File con un Logo (se presente l'immagine verrà presentata in cima alla pagina).
- Testo Iniziale.
- Testo del Bottone tramite il quale sarà possibile accedere al file con il documento emesso.
- Testo Finale (se presente verrà riportato dopo le Domande).

All'interno dei testi è possibile utilizzare delle "etichette" che SQuadra provvederà a "tradurre", in base alle informazioni aziendali, al momento della presentazione.

Etichetta	Contenuto
[TITOLARE]	È il Titolare del trattamento dei dati. In genere l'azienda come indicato fra le Informazioni. Deve essere utilizzato per i documenti Privacy.
[Azienda]	È la ragione sociale dell'azienda inserita fra i Dati Aziendali. (Deve essere utilizzata per i documenti non relativi alla Privacy).
[DESTINATARIO]	È il destinatario della singola Mail.

Domande

È possibile inserire fino ad un massimo di 10 Domande.

Ogni Domanda è caratterizzata da un Titolo e la Domanda vera e propria.

NOTA: La Domanda dovrà essere formulata in modo che accetti risposte del tipo Si/No.

Ad esempio: "Confermate di aver preso visione della informativa?", "Autorizzate il trattamento sopra descritto?", ecc.

Il Regolamento Generale sulla Protezione dei Dati dell'Unione Europea (GDPR), operativo in Italia dal 25 maggio 2018, Le dà il diritto di conoscere come trattiamo i dati personali da Lei forniti. Di seguito può leggere l'informativa nella quale, fra l'altro, descriviamo i riferimenti ai quali potrà rivolgersi per ogni chiarimento, le finalità dei trattamenti, i destinatari e le modalità dei trattamenti, i diritti esercitabili.

La preghiamo di leggerla e quindi di rispondere alle domande sotto riportate.

Visualizza l'informativa

Presa visione dell'informativa
Dopo aver letto il documento allegato dichiaro di aver preso visione dell'informativa fornita.
 SI NO

Informazioni commerciali dirette
Autorizzo il trattamento dei dati personali per l'invio di offerte da parte Vostra.
 SI NO

Informazioni commerciali indirette
Autorizzo il trattamento dei dati personali per l'invio di offerte da parte di Società a Voi collegate.
 SI NO

Inserire note

INVIA

La ringraziamo per la collaborazione.
Le ricordiamo che potrà accedere a questa pagina in ogni momento per modificare le Sue scelte relative ai consensi.

Esempio, relativo alla Privacy, di Pagina di richiesta predisposta da SQuadra sulla base dei valori inseriti dall'utente.

Versioni: Da consegnare o Consegname

Ogni versione deve essere consegnata a tutti gli interessati.

È possibile definire, per ogni consegna:

- Il Destinatario (è possibile inserire anche il codice utilizzato aziendalmente).
- L'eventuale indirizzo fisico o di posta elettronica al quale è stata fatta la spedizione.
- Il tipo di consegna (diretta, via e-mail, ecc.).
- La data di Consegnna.
- L'eventuale data di accettazione (o di risposta alla mail).
- L'eventuale data dell'ultimo sollecito.
- È possibile inserire il documento PDF con l'eventuale firma del Destinatario.
- È possibile richiedere l'invio automatico della Mail con ottenimento delle risposte via internet (in caso di risposta da parte del destinatario vedi sotto).
- È possibile indicare una comunicazione come superata se il destinatario ha fornito una diversa risposta successivamente.
- Eventuali note.

Risposte

In funzione delle domande definite per il Documento emesso sarà possibile riportare le risposte del Destinatario.

ATTENZIONE: in caso di richiesta da parte del destinatario di modificare le risposte fornite, qualora in base alle vecchie risposte sia già stato effettuato qualche trattamento, sarà necessario duplicare la "consegna" lasciando le vecchie risposte come "superate".

Se, ad esempio, il Destinatario ha dato il consenso all'invio di comunicazioni commerciali e, in un secondo momento lo revoca, qualora siano già state inviate comunicazioni commerciali in base al consenso a suo tempo ricevuto, è necessario conservare traccia del precedente consenso.

Risposte automatizzate

Se un destinatario fornisce le risposte dall'apposito link queste non saranno più modificabili ed appariranno nell'apposito elenco.

Il destinatario potrà sempre accedere al link per modificare le proprie risposte; quelle precedenti saranno considerate come superate.

16.1.1.1 Controllo della Completezza delle informazioni per l'invio automatico

Per essere sicuri di aver inserito tutte le informazioni necessarie per un invio automatico è possibile richiedere [Controllo completezza dati per mail] un controllo che fornisce una informazione sulle eventuali informazioni mancanti o, se tutte le informazioni sono state inserite attiva il flag "spedibile".

16.1.1.2 Importazione da Excel

Squadra permette di importare i dati di chi deve ricevere la comunicazione (es. l'elenco di tutti i Fornitori).

Per prima cosa è opportuno richiedere [Importazione / File BASE di Excel] la produzione di un file di Excel contenente i dati delle consegne già registrate al fine di rendere chiaro il significato dai vari campi che dovranno essere riempiti. Il file può essere riempito con le informazioni opportune, ed esempio provenienti dal programma di contabilità.

Il file così riempito deve essere riportato come "File EXCEL per importazione delle consegne" e quindi deve essere richiesto [Importazione / Importazione dal file Excel] l'inserimento di tutti i dati.

NOTA: Non verranno modificati i dati già inseriti (verranno trascurate le righe del file di Excel con Destinatario già presente).

16.1.1.3 Spedizione Comunicazioni

Una volta inseriti o aggiornati i dati dei destinatari è possibile richiedere l'invio automatico delle mail a tutti i destinatari per i quali è stata richiesta questa funzionalità.

Il sistema provvede all'invio delle mail per le quali è stato inserito un indirizzo mail formalmente corretto ed aggiorna la data di Consegna.

I dati di queste Consegne verranno presentati nell'apposito folder "Risposte automatizzate".

16.1.1.4 Stato delle Consegne

In ogni momento è possibile ottenere un file di excel con lo stato delle comunicazioni.

17 APPENDICE: Conformità legislativa e ad altre prescrizioni

17.1 Introduzione

Nella ISO 45001 viene richiesto che, all'interno della Politica della sicurezza e salute sul lavoro, sia incluso l'impegno a soddisfare i requisiti legali e altri requisiti. Viene quindi richiesta, al punto "6.1.3 – Determinazione dei requisiti legali e altri requisiti".

Nelle "Linee Guida per un Sistema di Gestione della salute e sicurezza sul lavoro" UNI-INAIL è richiesto che il SGSL, fra le altre attività, preveda di: "identificare le prescrizioni delle leggi e dei regolamenti applicabili".

La Norma UNI EN ISO 14001:2015, al punto 6.1.3- Obblighi di conformità, definisce che gli obblighi di conformità possono dare luogo a rischi e opportunità per l'organizzazione.

L'organizzazione deve:

- d) determinare e avere accesso agli obblighi di conformità relativi ai propri aspetti ambientali;
- e) determinare come questi obblighi di conformità si applicano all'organizzazione;
- f) tenere conto di questi obblighi di conformità nell'istituzione, attuazione, mantenimento e miglioramento continuo del proprio sistema di gestione ambientale.

SQquadra ha sviluppato lo strumento per la "Gestione della sorveglianza ambientale" sviluppato nel 2008 e presentato all'interno del 7° Convegno nazionale AICQ (Associazione Italiana Cultura Qualità) Settore Costruzioni Civili – SICUREZZA E AMBIENTE – LE NUOVE SFIDE DEL SETTORE PER UNO SVILUPPO SOSTENIBILE svoltosi presso la sala convegni dell'ANCE – Roma il 31/10/2008.

Oggi SQquadra permette di identificare tutte le Prescrizioni ritenute significative e di tenere sotto controllo le attività correlate.

17.1.1.1 Prescrizioni

Le Prescrizioni sono gli elementi, di Legge o relativi agli Obiettivi aziendali, dei quali si desidera controllare le attività per la loro corretta gestione.

Ogni Prescrizione è caratterizzata, fra l'altro, dall'argomento, dalla frequenza fra una scadenza e la successiva, i giorni necessari per svolgere l'attività e dal Responsabile.

Per ogni Prescrizione viene richiesta la Modalità:

- Verifica di 1° Livello (la registrazione dell'attività attesta la conformità).
- Verifica di 2° Livello (verifica effettuata su attività svolte da altri e registrate in altro modo).

Per ogni Prescrizione è possibile definire una Rilevanza relativa rispetto alle altre Prescrizioni relative allo stesso Argomento.

17.1.1.2 Attività relative alle Prescrizioni

Per ogni Prescrizione verranno svolte le Attività previste.

Applicabilità

Alcune Prescrizioni "standard" possono non essere significative per l'Azienda. In questo caso è necessario definire la Scadenza come "NON SIGNIFICATIVA" (ad esempio, per una azienda stabilmente sotto i 15 dipendenti non è necessario effettuare la Riunione Periodica per la sicurezza).

Una scadenza può diventare "NON SIGNIFICATIVA" anche a seguito della modifica della Legge o degli Obiettivi (ad esempio, il Documento Programmatico per la Sicurezza dei dati, prima obbligatorio, adesso è diventato facoltativo quindi è possibile trasformare l'eventuale relativa Scadenza da "APPLICABILE" a "NON SIGNIFICATIVA").

Alcune Prescrizioni possono essere non applicabili al momento. In questo caso la Scadenza andrà definito come "NON APPLICABILE". A differenze delle Scadenze "NON SIGNIFICATIVE" le Scadenze "NON APPLICABILI" verranno ripianificate dal programma perché è opportuno verificare

periodicamente il mantenimento della non Applicabilità (ad esempio, una azienda con poco meno di 15 dipendenti non è obbligata ad effettuare la Riunione Periodica per la sicurezza ma è opportuno che verifiche periodicamente il non superamento della soglia).

Tutte le altre Scadenze saranno “APPLICABILI”.

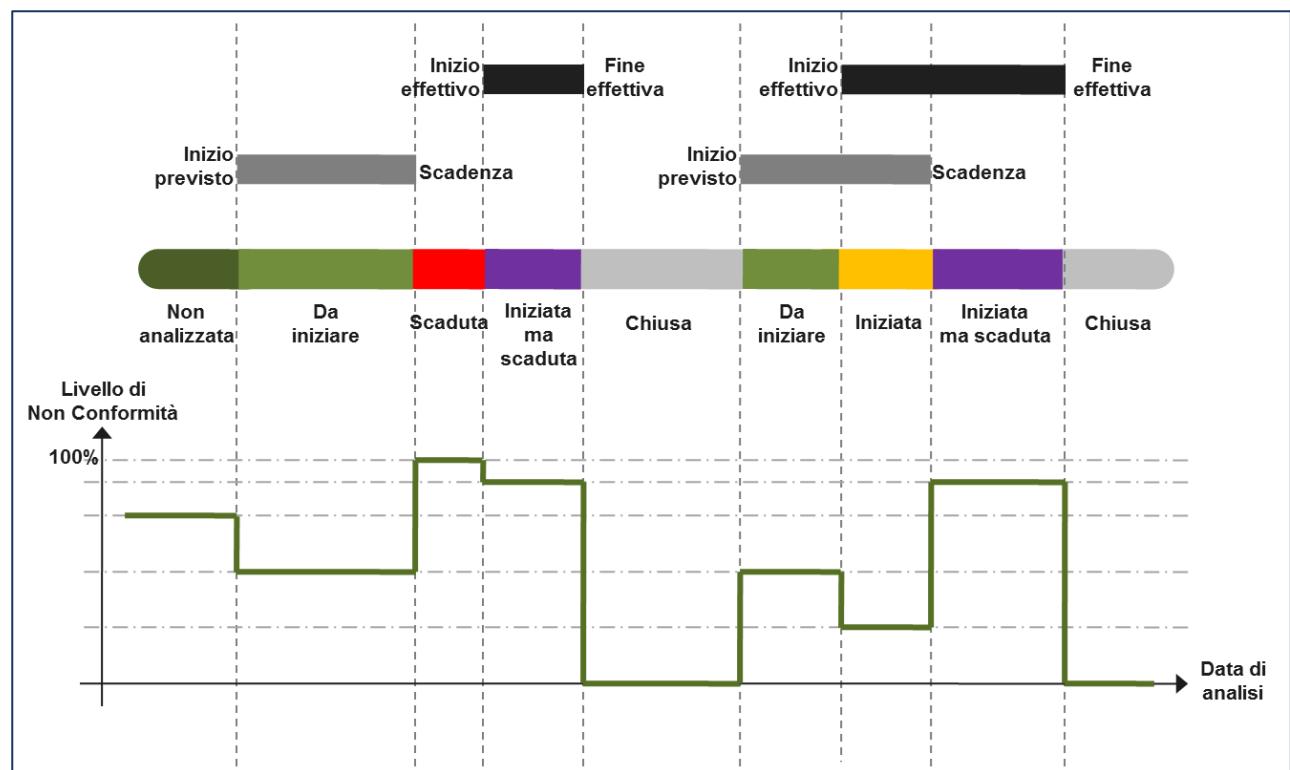
17.1.1.3 Oggetti

Ogni Attività relativa ad una Prescrizione può essere duplicata, se necessario, per ogni Oggetto (ad esempio per ogni Cantiere, per ogni Impianto, ecc.) per il quale va applicata.

Quando, per la stessa Prescrizione, esistono Attività con differenti Oggetti queste verranno gestite “in parallelo” (per ogni Oggetto ci saranno specifiche scadenze e stati d'avanzamento).

Per ogni Attività relativa ad ogni Oggetto è possibile confermare la Rilevanza definita a livello di Prescrizione o modificarla (ad esempio potrebbe essere differente in funzione dell’Oggetto in esame).

17.1.1.4 Gli Stati delle Attività relative alla Prescrizioni



Gli Stati nei quali può trovarsi una Attività relativa ad una Prescrizione sono i seguenti:

- Non analizzata.
- Non iniziato e scaduto.
- Iniziato ma scaduto.
- Da iniziare.
- Iniziato.
- Chiuso.
- Futuro.

17.1.1.5 Conformità

La media dei Livelli di Non Conformità pesati rispetto alla Rilevanza relativa per ogni Argomento forniscono una indicazione sulla Conformità per Argomento. Considerando il Peso percentuale

assegnato ad ogni Argomento è possibile ottenere una misurazione della Conformità aziendale in ogni momento.

17.2 Modalità operative

17.2.1.1 Impostazioni

Argomenti

Ogni azienda può definire gli Argomenti rispetto ai quali intende suddividere le Prescrizioni.

Al fine di avere una visione di insieme sul livello di conformità aziendale, per ogni Argomento, viene richiesto il Peso percentuale.

Le Prescrizioni relative ad Argomenti con Peso = 0 non verranno considerati

NOTA: In automatico vengono predefiniti gli Argomenti "standard".

Frequenze

Le frequenze indicano i mesi dopo i quali verrà ripianificata una scadenza dopo la sua chiusura.

NOTA: In automatico vengono definite le Frequenze "standard".

Stati

Ogni azienda può definire il Livello di Non Conformità da assegnare ad ogni Stato (che, ovviamente, sarà nullo per gli ultimi stati).

NOTA: In automatico vengono predefiniti valori "standard" per i vari stati.

17.2.1.2 Prescrizioni

È necessario definire le Prescrizioni di interesse.

NOTA: In automatico vengono definite alcune Prescrizioni "standard".

Prescrizioni di Base ed Aziendali

Il programma segnala, in griglia, se una Prescrizione è Aziendale (definita specificatamente per l'Azienda) o "standard" (generata in automatico da quelle di Base). Per le "standard" indica se la Prescrizione attualmente presente in azienda è aggiornata rispetto alla Prescrizione di base o se sono state apportate delle modifiche; eventuali modifiche apportate rispetto alle attuali Prescrizioni di base sono visualizzabili entrando nella singola Prescrizione.

Prescrizioni Superate

A seguito di abolizione dell'obbligo relativo una Prescrizione può essere "Superata".

In caso di una modifica significativa della norma dalla quale ha origine la Prescrizione è opportuno considerarla "Superata" e crearne una nuova.

Informazioni caratteristiche di ogni Prescrizione

Ogni Prescrizione è caratterizzata da:

- Un Codice ed una descrizione.
- Tipo (Scadenza Aziendale, Prescrizione di legge o normativa, legata alle attività di Comunicazione).
- Modalità di Verifica (nelle verifiche di 1° Livello le scadenze sono, in genere, tassative mentre nelle verifiche di 2° Livello le scadenze sono indicative).

- Argomento e Frequenza (vedi quanto descritto nel precedente paragrafo relativo alle impostazioni).
- Ambito.
- Il Sito di riferimento, se la Prescrizione è specifica per un Sito (per la definizione dei Siti vedi SG / Varie / Tabelle Varie).
- Rilevanza (rappresenta l'importanza relativa all'interno delle Prescrizioni relative allo stesso Argomento).
- Descrizione della Prescrizione:
 - Legge o Obiettivo.
 - Articolo della Legge o Traguardo dell'Obiettivo.
 - Norma o Attività prevista.
 - Punto.
- Frequenza (per la ripianificazione).
- Giorni previsti per la preparazione.
- Funzione Responsabile (verranno proposte oltre alle Funzioni Responsabile già inserite anche gli eventuali Ruoli per i Lavoratori definiti [vedi nella sezione relativa ai Lavoratori]).
- Sarà possibile indicare le Prescrizioni sicuramente Non Significative per l'Azienda.

NOTA: La frequenza proposta per le prescrizioni “standard” va ritenuta solo indicativa. In caso di rilevazione di Non Conformità sarà necessario, oltre al trattamento della specifica Non Conformità rilevata, aumentare la frequenza delle verifiche.

NOTA: Tutte le prescrizioni “standard” devono essere considerate unicamente come indicative e come primo suggerimento. Sarà responsabilità del Datore di Lavoro valutare attentamente tutte le Prescrizioni applicabili integrando, dove necessario, quelle proposte. Sempre il Datore di Lavoro dovrà valutare l'adeguatezza della frequenza proposta per le varie attività.

17.2.1.3 Attività relative alle Prescrizioni

Per ogni Prescrizione non ancora pianificata Squadra genera, in automatico, una Attività.

Le Attività così generare sono “da analizzare” a cura dei responsabili aziendali.

Le scadenze sono “analizzate” quando è stato definito:

- L'applicabilità.
- Il Responsabile.
- L'eventuale persona incaricata dell'esecuzione (se diversa dal Responsabile).
- La data di Inizio attività prevista.
- La data di Fine prevista.

Oggetti

Nel caso che una Prescrizione richiede Attività differenti per vari “Oggetti” è necessario Duplicare l'Attività specificare i vari Oggetti.

È anche possibile inserire il Sito di interesse (per la definizione dei Siti vedi SG / Varie / Tabelle Varie).

Se la Prescrizione è specifica per un Sito l'attività verrà già generata con lo specifico riferimento altrimenti è possibile indicare liberamente il Sito per la specifica attività.

Avanzamento delle attività

Quando l'attività viene iniziata (preparazione dei documenti, convocazione di una riunione, ecc.) è opportuno aggiornare lo specifico campo e quando viene conclusa andrà indicata la data di chiusura effettiva.

Quando viene inserita la data di Fine Effettiva il programma considera “Chiusa” la scadenza.

Vengono considerate "Chiuse" anche tutte le Scadenze considerate "Non Significative" o quelle derivanti da Prescrizioni ad oggi "Superate".

17.2.1.4 Analisi delle Attività relative alle Prescrizioni

Esportazione di Word

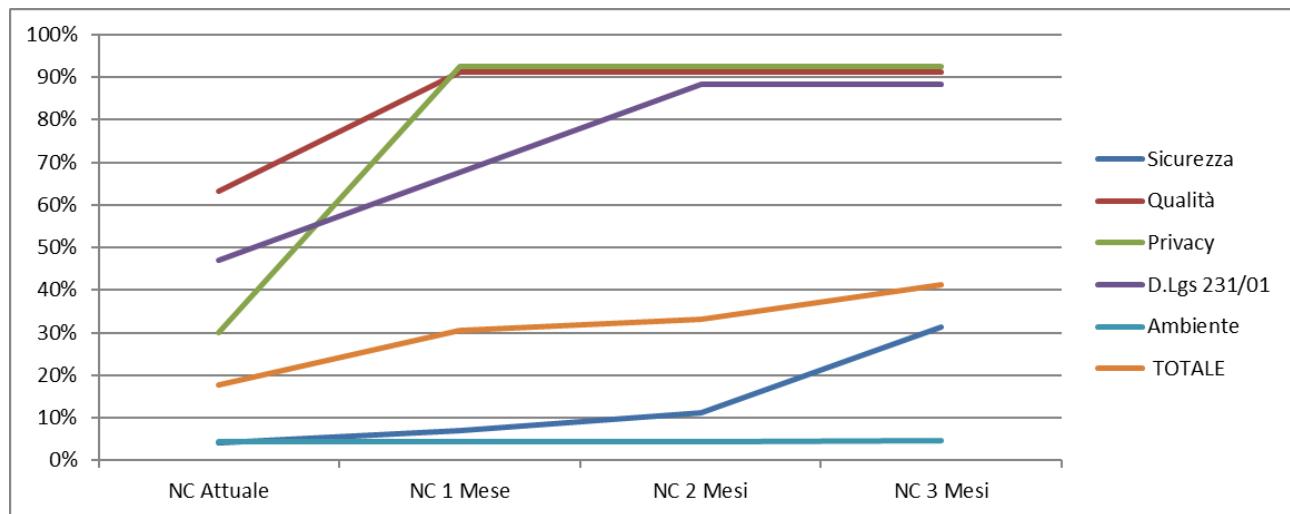
Il Programma produce un documento di Word nel quale, per ogni Argomenti / Ambito / Prescrizione ed eventuale Oggetto vengono riportate l'eventuale ultima attività svolta e l'eventuale attività prevista.

È possibile ottenere anche la stampa per Responsabile.

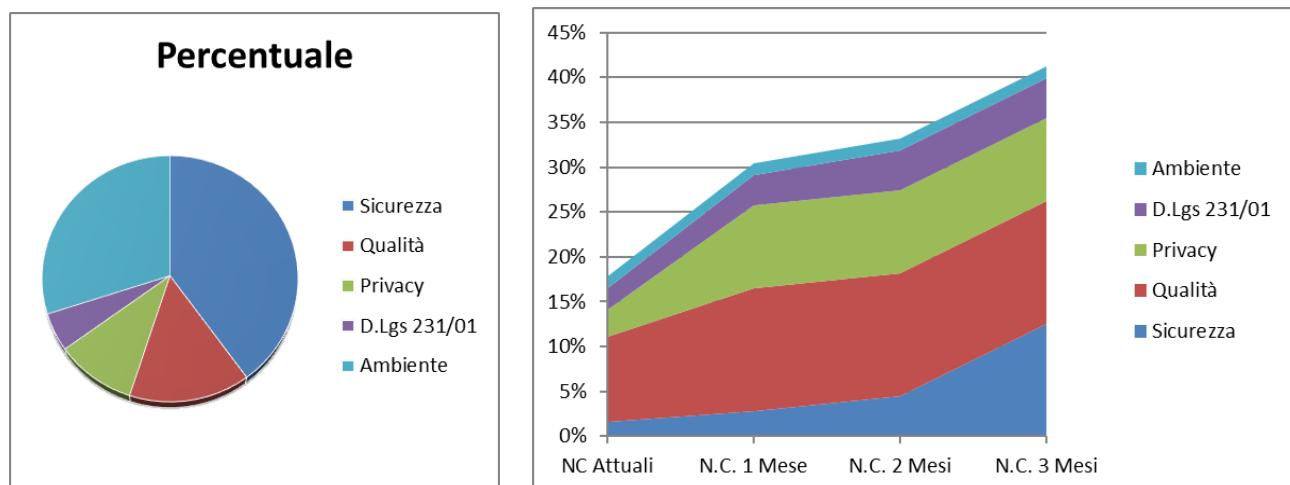
Analisi su Excel

Il Programma mostra, per ogni Scadenza, lo stato attuale e quello previsto fra 1, 2 e 3 mesi permettendo di pianificare le attività da iniziare.

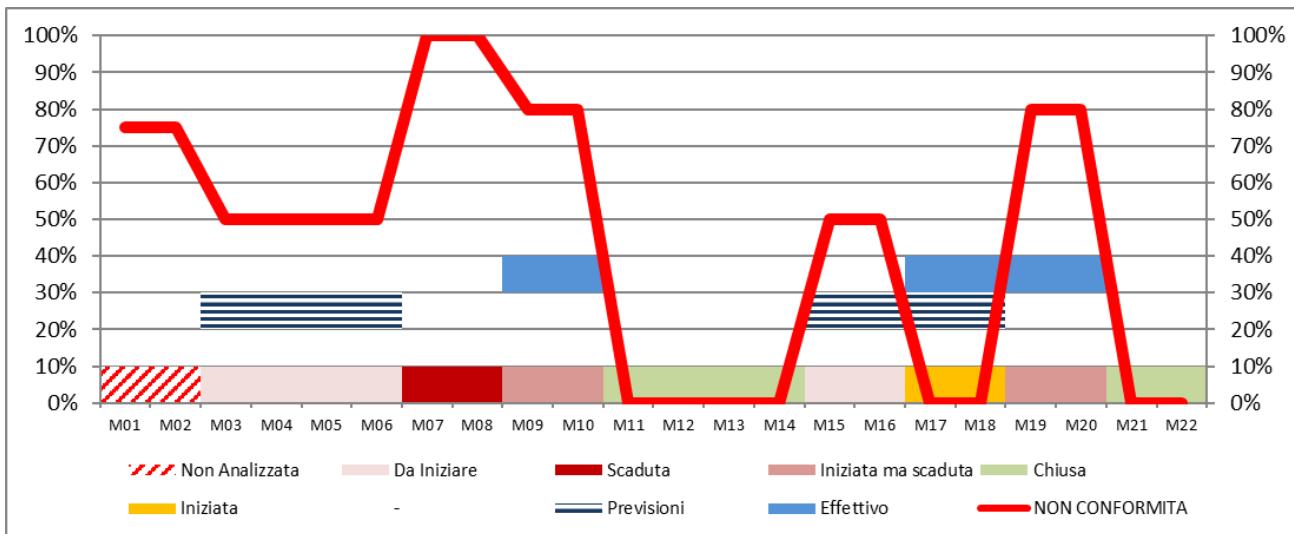
Viene mostrata anche una sintesi del Livello di Non Conformità per singolo Argomento e complessivo. Anche in questo caso verrà mostrato, oltre al dato attuale, il valore atteso (in assenza di azioni) fra 1,2 e 3 mesi.



Il valore complessivo tiene conto dei pesi relativi assegnati ai vari Argomenti



Ovviamente i calcoli della Non Conformità totale si basano anche sulla valutazione di Non Conformità assegnata ad ogni possibile Stato (vedi figura successiva).



Viene quindi mostrata una analisi riepilogativa del Livello di Non Conformità per Referente e per Esecutore.

Grafici

È possibile visualizzare il livello di conformità ai vari livelli:

- Argomento.
- Ambito.
- Prescrizione.
- Attività specifica (eventualmente per i vari Oggetti).

Gli stessi dati possono essere analizzati per Responsabile e per Esecutore.

17.2.1.5 Aggiornamento dei Responsabili dai Ruoli dei Lavoratori

Se sono stati definiti i Ruoli per i Lavoratori [Vedi sezione relativa ai Lavoratori] il programma provvede ad aggiornare il nominativo dei Responsabili per le Attività relative alle Prescrizioni quando:

- La Funzione Responsabile della Prescrizione coincide con uno dei Ruoli definiti.
- Al Ruolo è stato associato un solo Lavoratore.
- Per l'Attività relativa alla Prescrizione non è ancora stata definita la Data di Fine.

Questa funzione dovrà essere richiamata se:

- È stata modificata la Funzione Responsabile in una o più Procedure.
- È stata modificata la Persona associata ad uno o più Ruoli.

La funzione provvede, inoltre, ad eliminare eventuali Attività non ancora eseguite collegate ad una Prescrizione ritenuta Non Significativa.

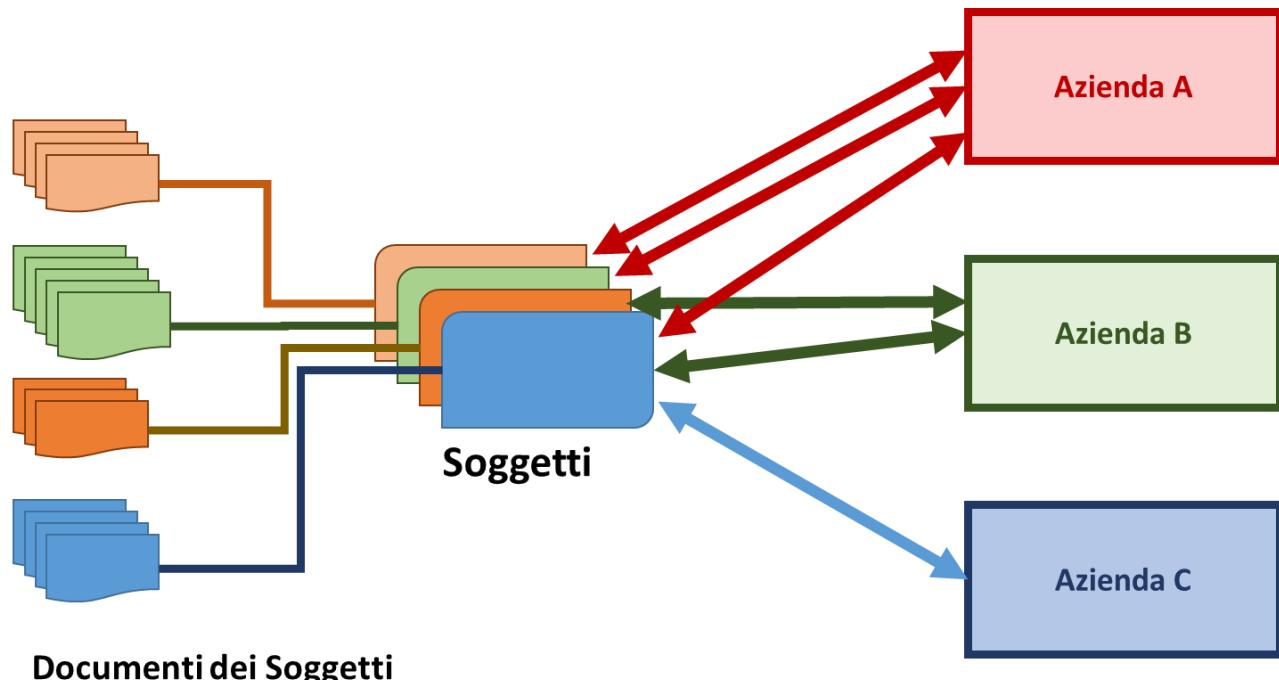
18 APPENDICE: Idoneità Tecnico Professionale

18.1 Premessa

L'Allegato XVII del D.Lgs 81/08 individua i documenti necessari ai fini dell'idoneità tecnico professionale.

Ogni Soggetto (sia Impresa che Lavoratore autonomo) può liberamente utilizzare SQuadra per archiviare e tenere sotto controllo i propri documenti.

Ogni Soggetto potrà quindi, semplicemente comunicando il proprio Codice di Controllo, permettere a tutte le Aziende clienti (che utilizzano la versione completa di SQuadra) di accedere direttamente a questi Documenti e verificare all'occorrenza la correttezza e l'aggiornamento dei documenti messi a disposizione.



Fra i Documenti di Supporto (richiamabili dal menu VARIE) è presente un esempio di comunicazione che ogni Azienda può inviare ai propri Fornitori per i quali deve effettuare il controllo dell'Idoneità tecnico professionale per invitarli ad utilizzare le funzionalità di SQuadra.

18.2 Archivio documenti aziendali.

Tutti i Soggetti (Imprese o Lavoratori autonomi) che lo desiderano possono liberamente archiviare i propri documenti che attestano l'idoneità nell'archivio di SQuadra.

18.2.1.1 Accesso al programma

L'accesso al programma è libero per chiunque dall'indirizzo:

<https://231.squadra.iltigiosrl.it/>

Effettuando la LOG IN con Nome utente e Password: “**Idoneità**”

18.2.1.2 Dati Anagrafici

Scegliendo Idoneità e quindi Soggetti viene richiesto di scegliere il Codice corrispondente alla propria azienda. La prima volta dovrà essere scelto “Nuovo Soggetto”.

Premendo il bottone ANAGRAFICA E DOCUMENTI verranno richiesti i dati anagrafici che, oltre alle normali informazioni di identificazione del Soggetto, comprendono:

- **Codice del Soggetto:** questa informazione sarà visibile da tutti gli utenti di SQuadra e permetterà di identificare il Soggetto. Il codice deve essere univoco per tutti i Soggetti quindi qualora il Codice sia già stato utilizzato da altri il programma chiederà di modificarlo.
- **Codice di controllo interno (Riservato):** permetterà solo al Soggetto di accedere alle informazioni Anagrafiche ed ai Documenti per effettuare qualunque modifica o integrazione. Dovrà essere conservata e conosciuta solo dal Soggetto.
- **Codice di Controllo da comunicare:** questo Codice dovrà essere comunicato, insieme al Codice del Soggetto, alle Aziende Clienti che vorranno controllare l'idoneità utilizzando SQuadra.
- **Tipo:** il Soggetto dovrà definire se è un Lavoratore autonomo o una Impresa per differenziare i documenti obbligatori.

Premendo il bottone SALVA verranno salvati i dati Anagrafici e verranno predisposti (e presentati in basso) i documenti previsti in base al tipo di Soggetto.

Ai successivi accessi al posto di “Nuovo Soggetto” andrà selezionato il proprio Codice Azienda ed inserita il proprio Codice di Controllo Interno corretto.

18.2.1.3 Documenti

Ogni Soggetto può inserire tutti i documenti che desidera rendere pubblici.

In particolare, dovrà inserire quelli obbligatori per l'Idoneità Tecnico Professionale.

Ogni Documento è caratterizzato da:

- Tipo documento.
- Eventuale Specifica (necessaria per i documenti con Tipo = “Altro”).
- Eventuali Note.
- Data del documento (obbligatoria).
- Data di Scadenza (da inserire solo se il documento ha una scadenza).
- Data dell'ultima Verifica (per i documenti per i quali non è prevista una scadenza, come ad esempi l'iscrizione alla Camera di Commercio, è opportuno verificare periodicamente la validità del documento).

Il programma calcola lo STATO del Documento:

- Superato (per tutti i Documenti per i quali è presente un Documento più nuovo dello stesso Tipo e, se presente, con la stessa Specifica).
- Ultimo Scaduto (per gli ultimi Documenti che risultano scaduti alla data odierna).
- Ultimo Vecchio (per gli ultimi Documenti verificati da più di 6 mesi o mai verificati e più vecchi di 6 mesi).
- Ultimo (per i Documenti non sostituiti da altri più nuovi, non scaduti e inseriti o verificati da meno di 6 mesi).

NOTA: Si ricorda che i documenti saranno inseriti una sola volta ma saranno disponibili a tutte le Aziende Cliente alle quali sarà stato trasmesso il Codice di Controllo.

18.2.1.4 Committenti

Ogni Soggetto può verificare quali Committenti (vedi capitolo successivo) hanno accesso ai documenti e, se presenti, quali note hanno inserito ed eventualmente se hanno ritenuto la Documentazione attualmente presente “Non Adeguata”.

18.3 Archivio aziendale dei Soggetti Fornitori.

L’Azienda che desidera controllare i Documenti relativi all’Idoneità Tecnico Professionale utilizzando SQuadra dovrà richiedere ai propri Fornitori di inserire i propri dati su SQuadra (come indicato precedentemente) e quindi comunicare il Codice Azienda ed il Codice di Controllo.

Sotto SG / OPERATIVO / IDONEITÀ TECNICO PROFESSIONALE è necessario inserire i vari Soggetti Fornitori.

Per aggiungere un nuovo Soggetto dovrà essere scelto di Codice Soggetto e quindi inserito il Codice di Controllo ricevuto dal Soggetto che autorizza così all’accesso alla consultazione ed alla verifica dei propri dati.

L’Azienda può inserire:

- Note interne relative al Soggetto.
- Note per il Soggetto.
- Eventuale valutazione di Non Adeguatezza dei Documenti attualmente presenti.

Ogni Azienda verrà presentata con lo Stato corrispondente al peggiore degli Stati dei Documenti non superati.

18.3.1 Documenti del Soggetto.

Per tutti i Soggetti Fornitori presenti verranno visualizzati tutti i documenti inseriti dal Soggetto.

L’Azienda può controllare e confermare o modificare la data di scadenza inserita dal Soggetto (questa informazione sarà utilizzata solo per l’Azienda).

Potrà essere inoltre inserita la data dell’ultima Verifica positiva effettuata sulla completezza e validità del Documento.

I documenti dei Soggetto Fornitori potranno quindi assumere i seguenti STATI:

- Superato (se il Fornitore ha inserito un nuovo documento aggiornato).
- Scaduto per l’Azienda (qualora risulti scaduto rispetto alla data di scadenza definita aziendalmente).
- Vecchio per l’Azienda (qualora sia stato verificato da più di 6 mesi).
- Valido per l’Azienda (qualora per l’Azienda non risulti scaduto e sia stato verificato da meno di 6 mesi).
- Negli altri casi assumerà lo Stato definito dal Soggetto Fornitore.

Stampa dei Documenti

È possibile richiedere al programma di produrre un PDF con degli ultimi Documenti del Soggetto.

È anche possibile richiedere la stessa stampa ma con evidenziato lo Stato del documento e l’ultima verifica effettuata aziendalmente sul documento.

19 APPENDICE: Regolamento Europeo protezione dei dati personali (GDPR)

19.1 Premessa

Il Regolamento Europeo [2016/679] relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati è entrato in vigore il 24 maggio 2016 è applicabile dal 24 maggio 2018.

Il legislatore ha adeguato la normativa italiana per recepire il Regolamento.

Dal 24 settembre 2018 è stato modificato il “Codice in materia di protezione dei dati personali” abrogando numerosi articoli e adeguando gli altri al GDPR.

19.1.1.1 Principi applicabili al trattamento dei dati [Art.5]

I dati personali sono:

- Trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»).
- Raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è considerato incompatibile con le finalità iniziali («limitazione della finalità»).
- Adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»).
- Esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»).
- Conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»).
- Trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).

19.1.1.2 Informativa e consenso.

Il Regolamento introduce regole più chiare in materia di informativa e consenso, definisce i limiti al trattamento automatizzato dei dati personali, pone le basi per l'esercizio di nuovi diritti, stabilisce criteri rigorosi per il trasferimento dei dati al di fuori dell'Ue e per i casi di violazione dei dati personali.

L'informativa diventa sempre di più uno strumento di trasparenza riguardo al trattamento dei dati personali e all'esercizio dei diritti. Per facilitare la comprensione dei contenuti, nell'informativa si potrà fare ricorso anche a icone, identiche in tutta l'Unione europea.

Il consenso dell'interessato al trattamento dei dati personali dovrà essere, come oggi, preventivo e inequivocabile, anche quando espresso attraverso mezzi elettronici (ad esempio, selezionando un'apposita casella in un sito web).

Viene esclusa ogni forma di consenso tacito (il silenzio, cioè, non equivale al consenso) oppure ottenuto proponendo a un interessato una serie di opzioni già selezionate.

Il consenso potrà essere revocato in ogni momento.

19.1.1.3 Diritto all'oblio.

Grazie all'introduzione del cosiddetto «diritto all'oblio», gli interessati potranno ottenere la cancellazione dei propri dati personali anche on line da parte del titolare del trattamento qualora ricorrono alcune condizioni previste dal Regolamento: se i dati sono trattati solo sulla base del consenso; se i dati non sono più necessari per gli scopi rispetto ai quali sono stati raccolti; oppure se l'interessato si oppone legittimamente al loro trattamento.

A questo diritto si accompagna l'obbligo per il titolare del trattamento che ha pubblicato i dati di comunicare la richiesta di cancellazione a chiunque li stia trattando, nei limiti di quanto tecnicamente possibile.

19.1.1.4 Gestione delle violazioni.

Il titolare del trattamento dovrà comunicare eventuali violazioni dei dati personali all'Autorità nazionale di protezione dei dati.

Se la violazione dei dati rappresenta una minaccia per i diritti e le libertà delle persone, il titolare dovrà informare in modo chiaro, semplice e immediato anche tutti gli interessati e offrire indicazioni su come intende limitare le possibili conseguenze negative.

19.1.1.5 Titolari e Responsabili della protezione dei dati.

Il Regolamento promuove la responsabilizzazione dei titolari del trattamento e l'adozione di approcci e politiche che tengano conto costantemente del rischio che un determinato trattamento di dati personali può comportare per i diritti e le libertà degli interessati.

Il principio-chiave è «privacy by design», ossia garantire la protezione dei dati fin dalla fase di ideazione e progettazione di un trattamento o di un sistema, e adottare comportamenti che consentano di prevenire possibili problematiche.

Viene inoltre introdotta la figura del «Responsabile della protezione dei dati» (Data Protection Officer o DPO), incaricato di assicurare una gestione corretta dei dati personali nelle imprese e negli enti.

19.1.1.6 I codici di condotta.

Il Regolamento promuove il ricorso a codici di condotta da parte di associazioni di categoria e altri soggetti, sottoposti all'approvazione dell'Autorità nazionale di protezione dei dati.

L'adesione ai codici di condotta e la certificazione del trattamento saranno elementi di cui l'Autorità dovrà tenere conto, per esempio, nell'applicare eventuali sanzioni o nell'analizzare la correttezza di una valutazione di impatto effettuata dal titolare.

Si ricordi che, in caso di inosservanza delle regole, sono previste sanzioni, anche elevate.

19.2 Criteri per determinare la necessità di effettuare una Valutazione Impatto Privacy (PIA)

Al fine di fornire un insieme più concreto di trattamenti che richiedono una valutazione d'impatto sulla protezione dei dati in virtù del loro rischio elevato intrinseco, il Gruppo dei Garanti europei (WP29) ha predisposto *"Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679"* nelle quali vengono descritti i seguenti nove criteri.

1. Valutazione o assegnazione di un punteggio, inclusiva di profilazione e previsione, in particolare in considerazione di "aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato" (considerando 71 e 91). Esempi di ciò potrebbero includere: un ente finanziario che esamina i suoi clienti rispetto a una banca dati di riferimento in materia di crediti oppure rispetto a una banca dati in materia di lotta contro il riciclaggio e il finanziamento del terrorismo (AML/CTF) oppure contenente informazioni sulle frodi; oppure un'impresa di biotecnologie che offre test genetici direttamente ai consumatori per valutare e prevedere i rischi di malattia o per la salute; oppure un'impresa che crea profili comportamentali o per la commercializzazione basati sull'utilizzo del proprio sito web o sulla navigazione sullo stesso;
2. processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente: trattamento che mira a consentire l'adozione di decisioni in merito agli interessati che *"hanno effetti giuridici"* o che *"incidono in modo analogo significativamente su dette persone fisiche"* (articolo 35, paragrafo 3, lettera a)). Ad esempio, il trattamento può portare all'esclusione o alla discriminazione nei confronti delle persone. Il trattamento che non ha effetto o ha soltanto un effetto limitato sulle persone non risponde a questo criterio specifico. Ulteriori spiegazioni in merito a queste nozioni saranno fornite nelle linee guida sulla profilazione che saranno pubblicate prossimamente dal WP29;
3. monitoraggio sistematico: trattamento utilizzato per osservare, monitorare o controllare gli interessati, ivi inclusi i dati raccolti tramite reti o *"la sorveglianza sistematica su larga scala di una zona accessibile al pubblico"* (articolo 35, paragrafo 3, lettera c)). Questo tipo di monitoraggio è un criterio in quanto i dati personali possono essere raccolti in circostanze nelle quali gli interessati possono non essere a conoscenza di chi sta raccogliendo i loro dati e di come li utilizzerà. Inoltre, può essere impossibile per le persone evitare di essere soggette a tale trattamento nel contesto di spazi pubblici (o accessibili al pubblico);
4. dati sensibili o dati aventi carattere altamente personale: questo criterio include categorie particolari di dati personali così come definite all'articolo 9 (ad esempio informazioni sulle opinioni politiche delle persone), nonché dati personali relativi a condanne penali o reati di cui all'articolo 10. Un esempio potrebbe essere quello di un ospedale generale che conserva le cartelle cliniche dei pazienti oppure quello di un investigatore privato che conserva i dettagli dei trasgressori. Al di là di queste disposizioni del regolamento generale sulla protezione dei dati, alcune categorie di dati possono essere considerate aumentare il possibile rischio per i diritti e le libertà delle persone fisiche. Tali dati personali sono considerati essere sensibili (nel senso in cui tale termine è comunemente compreso) perché sono legati ad attività a carattere personale o domestico (quali le comunicazioni elettroniche la cui riservatezza deve essere protetta) oppure perché influenzano l'esercizio di un diritto fondamentale (come ad esempio i dati relativi all'ubicazione, la cui raccolta mette in discussione la libertà di circolazione) oppure perché la violazione in relazione a tali dati implica chiaramente gravi ripercussioni sulla vita quotidiana dell'interessato (si pensi ad esempio a dati finanziari che potrebbero essere utilizzati per frodi relative ai pagamenti). A questo proposito, può essere rilevante il fatto che tali dati siano stati resi pubblici dall'interessato o da terzi. Il fatto che i dati personali siano di dominio pubblico può essere considerato un fattore da considerare nella valutazione qualora fosse previsto che i dati venissero utilizzati ulteriormente per determinate finalità. Questo criterio può includere anche dati quali documenti personali, messaggi di posta elettronica, diari, note ricavate da dispositivi elettronici di lettura dotati di funzionalità di annotazione, nonché informazioni molto personali contenute nelle applicazioni che registrano le attività quotidiane delle persone);
5. trattamento di dati su larga scala: il regolamento generale sulla protezione dei dati non definisce la nozione di *"su larga scala"*, tuttavia fornisce un orientamento in merito al considerando 91. A ogni modo,

il WP29 raccomanda di tenere conto, in particolare, dei fattori elencati nel prosieguo al fine di stabilire se un trattamento sia effettuato su larga scala:

- a. il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento;
 - b. il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento;
 - c. la durata, ovvero la persistenza, dell'attività di trattamento;
 - d. la portata geografica dell'attività di trattamento;
6. creazione di corrispondenze o combinazione di insiemi di dati, ad esempio a partire da dati derivanti da due o più operazioni di trattamento svolte per finalità diverse e/o da titolari del trattamento diversi secondo una modalità che va oltre le ragionevoli aspettative dell'interessato;
 7. dati relativi a interessati vulnerabili (considerando 75): il trattamento di questo tipo di dati è un criterio a motivo dell'aumento dello squilibrio di potere tra gli interessati e il titolare del trattamento, aspetto questo che fa sì che le persone possono non essere in grado di acconsentire od opporsi al trattamento dei loro dati o di esercitare i propri diritti. Gli interessati vulnerabili possono includere i minori (i quali possono essere considerati non essere in grado di opporsi e acconsentire deliberatamente e consapevolmente al trattamento dei loro dati), i dipendenti, i segmenti più vulnerabili della popolazione che richiedono una protezione speciale (infermi di mente, richiedenti asilo o anziani, pazienti, ecc.) e, in ogni caso in cui sia possibile individuare uno squilibrio nella relazione tra la posizione dell'interessato e quella del titolare del trattamento;
 8. uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative, quali la combinazione dell'uso dell'impronta digitale e del riconoscimento facciale per un miglior controllo degli accessi fisici, ecc. Il regolamento generale sulla protezione dei dati chiarisce (articolo 35, paragrafo 1 e considerando 89 e 91) che l'uso di una nuova tecnologia, definita "*in conformità con il grado di conoscenze tecnologiche raggiunto*" (considerando 91), può comportare la necessità di realizzare una valutazione d'impatto sulla protezione dei dati. Ciò è dovuto al fatto che il ricorso a tale tecnologia può comportare nuove forme di raccolta e di utilizzo dei dati, magari costituendo un rischio elevato per i diritti e le libertà delle persone. Infatti, le conseguenze personali e sociali dell'utilizzo di una nuova tecnologia potrebbero essere sconosciute. Una valutazione d'impatto sulla protezione dei dati aiuterà il titolare del trattamento a comprendere e trattare tali rischi. Ad esempio, alcune applicazioni di "Internet delle cose" potrebbero avere un impatto significativo sulla vita quotidiana e sulla vita privata delle persone e, di conseguenza, richiedono la realizzazione di una valutazione d'impatto sulla protezione dei dati;
 9. quando il trattamento in sé "impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto" (articolo 22 e considerando 91). Ciò include i trattamenti che mirano a consentire, modificare o rifiutare l'accesso degli interessati a un servizio oppure la stipula di un contratto. Un esempio di ciò è rappresentato dal caso in cui una banca esamina i suoi clienti rispetto a una banca dati di riferimento per il credito al fine di decidere se offrire loro un prestito o meno.

Nelle stesse Linee Guida si ritiene che una valutazione d'impatto sulla protezione dei dati non sia richiesta nei seguenti casi:

- quando il trattamento non è tale da "presentare un rischio elevato per i diritti e le libertà delle persone fisiche" (articolo 35, paragrafo 1);
- quando la natura, l'ambito di applicazione, il contesto e le finalità del trattamento sono molto simili a un trattamento per il quale è stata svolta una valutazione d'impatto sulla protezione dei dati. In tali casi, si possono utilizzare i risultati della valutazione d'impatto sulla protezione dei dati per un trattamento analogo (articolo 35, paragrafo 1);
- quando le tipologie di trattamento sono state verificate da un'autorità di controllo prima del maggio 2018 in condizioni specifiche che non sono cambiate (cfr. III.C);
- qualora un trattamento, effettuato a norma dell'articolo 6, paragrafo 1, lettere c) o e), trovi una base giuridica nel diritto dell'Unione o nel diritto dello Stato membro, tale diritto disciplini il trattamento specifico o sia già stata effettuata una valutazione d'impatto sulla protezione dei dati nel contesto dell'adozione di tale base giuridica (articolo 35, paragrafo

10), a meno che uno Stato membro non abbia dichiarato che è necessario effettuare tale valutazione prima di procedere alle attività di trattamento;

- qualora il trattamento sia incluso nell'elenco facoltativo (stabilito dall'autorità di controllo) delle tipologie di trattamento per le quali non è richiesta alcuna valutazione d'impatto sulla protezione dei dati (articolo 35, paragrafo 5). Tale elenco può contenere attività di trattamento conformi alle condizioni specificate da detta autorità, in particolare attraverso linee guida, decisioni o autorizzazioni specifiche, norme di conformità, ecc. (ad esempio in Francia, autorizzazioni, esenzioni, norme semplificate, pacchetti di conformità, ecc.). In tali casi e a condizione che venga eseguita una nuova valutazione da parte dell'autorità di controllo competente, non è richiesta una valutazione d'impatto sulla protezione dei dati, ma soltanto se il trattamento rientra a tutti gli effetti nel campo di applicazione della procedura pertinente menzionata nell'elenco e continua a rispettare pienamente tutti i requisiti pertinenti del regolamento generale sulla protezione dei dati.

19.3 Glossario predisposto da Confindustria per il Registro delle attività di Trattamento

19.3.1 Organigramma

Titolare del trattamento: il soggetto (la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo) che, singolarmente o insieme ad altri (contitolare del trattamento), determina le finalità e i mezzi del trattamento di dati personali.

Rappresentante del Titolare del trattamento: la persona fisica o giuridica stabilita nel territorio dell'Unione europea, designata dal Titolare non stabilito nell'Unione affinché lo rappresenti per quanto riguarda gli obblighi previsti dal Regolamento.

Responsabile della protezione dei dati (DPO): il soggetto, interno o esterno alla struttura del Titolare, che in piena indipendenza e autonomia supporta quest'ultimo in merito all'applicazione degli obblighi previsti dal Regolamento, organizza e sorveglia la gestione dei trattamenti e funge da punto di contatto per le questioni in tema di privacy. La figura è obbligatoria quando le attività principali del Titolare consistono in trattamenti che richiedono il monitoraggio regolare e sistematico degli interessati su larga scala oppure in trattamenti su larga scala di dati particolari (ex sensibili) e "giudiziari".

Responsabile del trattamento: il soggetto (la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo) esterno alla struttura del Titolare del trattamento che tratta dati personali per conto di quest'ultimo.

Sub-responsabile del trattamento: il soggetto (la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo) cui il Responsabile del trattamento ricorre per l'esecuzione di specifiche attività di trattamento di dati personali per conto di quest'ultimo. Il ricorso al Subresponsabile deve essere preventivamente autorizzato per iscritto dal Titolare.

Delegato dal Titolare del trattamento – Referente privacy: figura facoltativa, a cui il Titolare può ricorrere a fini meramente organizzativi e che potrebbe sostituire il vecchio "responsabile interno".

19.3.2 Descrizione del trattamento

Ufficio di riferimento: ufficio o funzione che cura prioritariamente il trattamento.

Interessato: la persona fisica identificata o identificabile cui si riferiscono i dati.

Categorie di interessati: es. dipendenti, collaboratori, candidati, familiari dei lavoratori, clienti/utenti, fornitori, professionisti, soggetti terzi (da precisare se minori).

Dato personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile; si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

- **Dati comuni:** es. anagrafici (nome, cognome, data di nascita, cittadinanza, stato civile, indirizzo, qualifica professione); documenti di identità (Cdl, patente, passaporto); codici di identificazione fiscale (CF, partita IVA persone fisiche); dati di contatto (numero di telefono, indirizzo e-mail, indirizzo fisico); codici identificativi lavoratori (matricola, credenziali di accesso ai sistemi informatici); coordinate bancarie (numero CC, codice IBAN); targa veicolo; dati multimediali (vide, audio); dati di navigazione internet (cookie, log, indirizzo IP); dati di geolocalizzazione; dati di profilazione.
- **Dati particolari:** es. dati idonei a rivelare l'appartenenza a partiti, sindacati, organizzazioni a carattere religioso o filosofico; dati genetici; dati biometrici; dati relativi alla salute (es. gravidanza, malattia, appartenenza a categorie protette).
- **Dati giudiziari** es. dati relativi a condanne penali, ai reati e alle connesse misure di sicurezza (es. dati in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti).
- **Informazioni non considerate dati personali:** es. informazioni riconducibili a un soggetto non persona fisica; numero di iscrizione al registro delle imprese di una società; indirizzo e-mail, come info@azienda.com; dati resi anonimi

Destinatario: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Es. Responsabile del trattamento (anche semplicemente per categoria di appartenenza), persone autorizzate al trattamento (incaricati del trattamento), imprese del gruppo, associazioni di imprese, sindacati, imprese assicurative.

Legittimo interesse del titolare o di un terzo: una delle basi giuridiche del trattamento a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato e tenuto conto delle ragionevoli aspettative nutrite dall'interessato in base alla sua relazione con il titolare. Ad esempio, possono perseguire un legittimo interesse i trattamenti effettuati nell'ambito dei rapporti B2C o dei rapporti di lavoro, le comunicazioni dei dati infragruppo per fini amministrativi interni. Affinché il legittimo interesse possa operare come base giuridica del trattamento è necessario, tra l'altro, che:

- il trattamento non abbia a oggetto dati "sensibili" (compresi quelli biometrici) o "giudiziari";
- non operi un'ulteriore base giuridica (es. adempimento di un obbligo legale oppure l'esecuzione di un contratto del quale è parte l'interessato o di misure precontrattuali);
- le finalità perseguiti siano individuate specificamente, in modo da predisporre garanzie adeguate (es. in ambito lavorativo, il legittimo interesse del datore di lavoro può essere invocato come presupposto di liceità a condizione che il trattamento dei dati dei lavoratori sia strettamente necessario per uno scopo legittimo e conforme ai principi di proporzionalità e sussidiarietà);
- prima di procedere al trattamento, sia effettuata la valutazione di impatto qualora sia effettuato con nuove tecnologie o strumenti automatizzati.

Per maggiori informazioni, v. Garante privacy, Provvedimento 22 febbraio 2018, n. 121).

Garanzie per il trasferimento dei dati in un Paese extra UE: decisione di adeguatezza della Commissione europea, norme vincolanti d'impresa, clausole contrattuali standard, codice di condotta, meccanismo di certificazione, clausole ad hoc autorizzate dal Garante privacy. In via

residuale e in mancanza di una decisione di adeguatezza ovvero delle altre citate garanzie, il trasferimento è ammesso, tra l'altro, se l'interessato vi abbia esplicitamente acconsentito oppure se lo stesso trasferimento sia necessario all'esecuzione di un contratto concluso con il titolare o a tra questi e un terzo a favore dell'interessato. Per maggiori informazioni sulle ulteriori condizioni per il trasferimento dei dati extra UE, v. art. 49 GDPR.

19.3.3 Misure di sicurezza: alcuni esempi

La lista fornita non ha carattere esaustivo. Inoltre, si precisa che la lista ha carattere dinamico e non statico – come è stato per l'Allegato B al Codice privacy – pertanto è necessario un costante confronto con gli sviluppi della tecnologia e l'insorgere di nuovi rischi.

19.3.3.1 Tecniche di cifratura e pseudonimizzazione.

NOTA: Cifratura dei dati e pseudonimizzazione sono strumenti differenti tra loro, ma con un medesimo fine: oscurare il dato per renderlo incomprensibile a coloro che non hanno i codici per accedervi. La crittografia si basa, di solito, su un algoritmo di cifratura e su una passphrase che "apre" e "chiude" i dati. La pseudonimizzazione garantisce i dati personali, facendo in modo che gli stessi non siano attribuibili ad una persona fisica identificata o identificabile. Entrambe sono comunemente considerate dal GDPR alcune delle tecniche più efficaci per garantire una reale protezione delle informazioni.

19.3.3.2 Sistemi di autenticazione

La funzione di autenticazione ha lo scopo di accertare l'identità dell'incaricato.

- Credenziali di autenticazione individuate tra:
 - codice identificativo e password esclusivi;
 - dispositivo di autenticazione esclusivo (es. smart card), più eventuale password;
 - rilevazione biometrica (es. impronta digitale), più eventuale password.
- Assegnazione individuale (per ciascun incaricato) di una o più credenziali di autenticazione
- Istruzioni in merito alla segretezza della password e alla corretta custodia dei dispositivi
- Criteri per la creazione della password:
 - almeno 8 caratteri o il massimo di quelli consentiti dall'applicazione;
 - non facilmente ricostruibile (non contiene riferimenti agevolmente riconducibili all'incaricato);
 - da modificare dopo il primo uso; aggiornamento periodico (es. almeno ogni 3 mesi in caso di trattamento di particolari categorie di dati, almeno ogni 6 mesi in caso di altri trattamenti).
- Criteri per il codice identificativo non riassegnabile, nemmeno in tempi diversi.
- Disattivazione delle credenziali per disuso (da almeno 6 mesi), perdita della qualità del profilo di accesso.

19.3.3.3 Sistemi di autorizzazione

La funzione di autorizzazione ha lo scopo di stabilire a quali dati l'incaricato può accedere e quali trattamenti può effettuare.

- Adozione di un sistema di autorizzazione in presenza di più profili.
- Individuazione e configurazione dei profili di autorizzazione prima del trattamento e secondo necessità di uso dei dati.
- Verifica esistenza dei requisiti per la conservazione dei profili (almeno ogni anno).
- Aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici (almeno ogni anno).

19.3.3.4 Protezione da accessi non autorizzati

- Protezione dall'accesso abusivo ai dati:
 - misure preventive, che proteggono le vulnerabilità e riducono l'impatto degli attacchi o li rendono inefficaci (es. antivirus, firewall, software anti-intrusione, reti segmentate);
 - misure correttive, che riducono le conseguenze degli attacchi (es. copie di backup dei dati, software che rilevano le intrusioni o le attività sospette);
 - misure deterrenti, che riducono le probabilità dell'attacco (es. registrazione dei log, formazione del personale);
 - misure investigative, che rilevano quanto avvenuto e forniscono spunto per le successive contromisure (es. test di intrusione, audit, analisi dei log).
- Prevenzione della vulnerabilità dei sistemi: aggiornamento delle patch.
- Istruzioni per la custodia e l'uso dei supporti che contengono dati.
- Distruzione o inutilizzabilità dei supporti non più utilizzati; intelligibilità dei dati in essi contenuti.

19.3.3.5 Ripristino della disponibilità dei dati

Salvataggio almeno settimanale dei dati; implementazione di strategie di backup in funzione degli strumenti utilizzati, della quantità e della tipologia delle informazioni da salvare.

Piano di disaster recovery e/o business continuity.

Ulteriori accorgimenti tecnici per il salvataggio dei dati (sistemi dotati di mirroring, in RAID, di tipo hot-swap, dotati di alimentazione ridondante, sistemi in cluster).

19.3.3.6 Procedura per gestire i Data Breach

Il Data Breach è la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

19.3.3.7 Formazione degli incaricati

Piano di formazione privacy per il personale incaricato al trattamento di dati personali:

- contenuto degli incontri formativi a cui si intende procedere;
- calendario degli incontri svolti o previsti;
- registrazione dei partecipanti agli incontri formativi;
- conservazione della documentazione consegnata durante gli interventi formativi.

19.3.3.8 Sistemi di custodia degli eventuali archivi fisici e/o cartacei.

NOTA: è necessario garantire la corretta custodia degli archivi.

19.3.3.9 Procedure di monitoraggio e aggiornamento dell'efficacia delle misure e delle policy

- Verifiche della conformità ai requisiti di sicurezza e protezione dei dati personali.
- Conformità alla politica di sicurezza dei dati personali.
- Conformità tecnica degli strumenti elettronici.
- Definizione di una corretta applicazione delle misure di sicurezza da parte di fornitori esterni (es. gestione paghe).
- Politica di responsabilizzazione dei soggetti esterni (es. predisposizione di adeguati modelli contrattuali e/o clausole contrattuali).

20 APPENDICE: Sistema di Gestione per la Sicurezza delle Informazioni

20.1 Norma ISO 27001

La norma ISO 27001 ha lo scopo di fornire i requisiti per stabilire, attuare, mantenere e migliorare in modo continuo un sistema di gestione per la sicurezza delle informazioni. L'adozione di un sistema di gestione per la sicurezza delle informazioni è una decisione strategica per un'organizzazione. Stabilire e attuare un sistema di gestione per la sicurezza delle informazioni di un'organizzazione sono influenzati dalle sue necessità e obiettivi, dai suoi requisiti di sicurezza, dai suoi processi organizzativi e dalla sua dimensione e struttura. È previsto che tutti questi fattori cambino nel tempo.

Il sistema di gestione per la sicurezza delle informazioni preserva la riservatezza, l'integrità e la disponibilità delle informazioni mediante l'applicazione di un processo di gestione del rischio e dà fiducia alle parti interessate sull'adeguatezza della gestione dei rischi.

È importante che il sistema di gestione per la sicurezza delle informazioni sia parte integrante dei processi e della struttura gestionale complessiva dell'organizzazione e che la sicurezza delle informazioni sia considerata nella progettazione dei processi, dei sistemi informativi e dei controlli. Ci si attende che un sistema di gestione per la sicurezza delle informazioni sia commisurato alle necessità dell'organizzazione.

La norma ISO 27001 può essere utilizzata da parti interne ed esterne al fine di valutare la capacità di un'organizzazione di soddisfare i propri requisiti relativi alla sicurezza delle informazioni.

20.2 Rischi

L'Articolo 24 del GDPR - Responsabilità del titolare del trattamento. Richiede che "Tenuto conto ... dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche", il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento.

20.2.1.1 Probabilità dell'evento

Una catalogazione della Probabilità dell'evento viene riportata nella tabella seguente (il Rating è in funzione del numero di eventi attesi in 10 anni):

Probabilità dell'evento	Frequenza	Rating
Trascurabile	Accadimento sporadico	1
Molto bassa	2-3 volte ogni 5 anni	5
Bassa	< di una volta l'anno	7,5
Media	< di una volta ogni 6 mesi	15
Alta	< di una volta al mese	90
Molto alta	> di una volta al mese	120

20.2.1.2 Gravità dell'evento

Una catalogazione in funzione della Gravità dell'evento viene riportata nella tabella seguente:

Gravità dell'evento	Gravità	Rating
Insignificante	Di impatto minimo	10
Minore	Non richiede sforzi extra per il ripristino, nessun accesso non autorizzato ai dati	100
Significativo	Danno di entità tangibile che richiede sforzi extra per il ripristino accesso ai dati non autorizzati limitato	1.000
Serio	Danno che richiede un significativo impiego di risorse o che porta un danno all'immagine ed alla credibilità aziendale	10.000
Molto serio	Danno esteso che comporta la compromissione di una grande quantità di dati o servizi	100.000
Grave	Compromissione completa	1.000.000

20.2.1.3 Valutazione del Rischio

Dal prodotto fra Probabilità e Gravità si ottiene il Rischio connesso all'evento. È possibile catalogare i rischi come riportato nella tabella seguente:

Valutazione del Rischio	Sicurezza delle Informazioni	Probabilità x Gravità > di	Peso
Trascurabile	Non dovrebbe essere compromessa.		0%
Basso	È improbabile che sia compromessa.	50	20%
Medio	Potrebbe essere compromessa in condizioni avverse.	500	40%
Alto	Potrebbe essere compromessa in condizioni normali.	5.000	60%
Critico	È possibile che venga realmente compromessa.	50.000	80%
Estremo	È molto probabile che venga compromessa.	500.000	100%

È quindi possibile definire il rischio come riportato nella tabella seguente:

Rischio		Frequenza						
		Non significativo	Accadimento sporadico	2-3 volte ogni 5 anni	< di una volta l'anno	< di una volta ogni 6 mesi	< di una volta al mese	> di una volta al mese
Gravità	Non significativo	Trascurabile	Trascurabile	Trascurabile	Trascurabile	Trascurabile	Trascurabile	Trascurabile
	Di impatto minimo	Trascurabile	Trascurabile	Basso	Basso	Basso	Medio	Medio
	Non richiede sforzi extra per il ripristino, nessun accesso non autorizzato ai dati	Trascurabile	Basso	Medio	Medio	Medio	Alto	Alto
	Danno di entità tangibile che richiede sforzi extra per il ripristino e/o accesso ai dati non autorizzati limitato	Trascurabile	Medio	Alto	Alto	Alto	Critico	Critico
	Danno che richiede un significativo impiego di risorse o all'immagine ed alla credibilità aziendale	Trascurabile	Alto	Critico	Critico	Critico	Estremo	Estremo
	Danno esteso che comporta la compromissione di una grande quantità di dati o servizi	Trascurabile	Critico	Estremo	Estremo	Estremo	Estremo	Estremo
	Compromissione completa	Trascurabile	Estremo	Estremo	Estremo	Estremo	Estremo	Estremo

NOTA: Come è evidenziato dalla tabella precedente la scelta dei Rating è stata effettuata in modo da dare un peso maggiore alla Gravità rispetto alla Frequenza (come indicato anche dalle Linee Guida ENISA – devi Appendice successiva). Si ha, infatti, un Rischio Estremo quando c'è la possibilità di "Compromissione

Completa anche se con probabilità “Trascurabile”; per contro anche se un evento è molto probabile ma ha un impatto minimo viene considerato un Rischio Medio.

20.2.1.4 Priorità di intervento

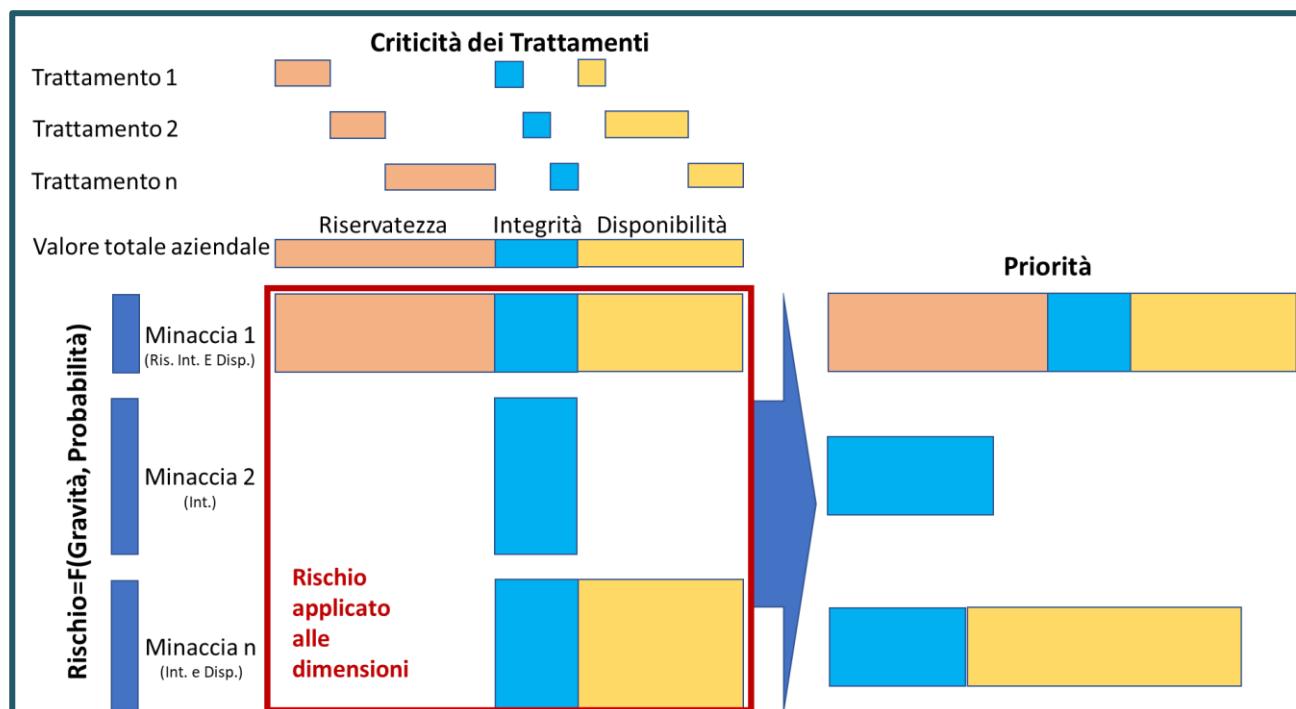
Una volta analizzate tutte le Minacce definendo, come visto in precedenza, per ciascuna il livello di Rischio è necessario definire una Priorità negli interventi da attuare.

Nel valutare la Priorità è opportuno tenere in conto l’analisi dei Trattamenti aziendali e come questi sono sensibili alle tre dimensioni (Riservatezza, Integrità e Disponibilità).

NOTA: SQuadra fornisce un valore dell’importanza aziendale per le tre dimensioni (Vedi “Report generale SGSI”).

Visto che ogni Minaccia può essere significativa solo per alcune delle tre dimensioni è necessario analizzare l’effetto aziendale del verificarsi della minaccia (moltiplicando il peso percentuale del rischio per la somma delle percentuali dell’importanza aziendale delle dimensioni coinvolte).

Si ottiene in questo modo, per ogni Minaccia, il Rischio Pesato e, normalizzandolo, la Priorità di intervento.



È necessario adottare Misure Aggiuntive a fronte di tutte le Minacce che possono avere un Rischio Pesato superiore ad Alto.

20.3 Eventi indesiderati.

20.3.1 Definizioni

20.3.1.1 Vulnerabilità

La Vulnerabilità è un punto di debolezza del sistema di gestione della sicurezza. La vulnerabilità non compromette la risorsa o il sistema di cui fa parte, ma se utilizzata da quella che viene definita una minaccia può trasformarsi in un evento dannoso.

Esempi di vulnerabilità sono:

- Password riportate in chiaro sulle postazioni operatorie.
- Postazioni operatorie con sessioni attive non presidiate.
- Credenziali utente senza scadenza.

- Mancato aggiornamento del SW delle postazioni.

20.3.1.2 Incidente relativo alla Sicurezza delle Informazioni

L'Incidente, di sicurezza delle informazioni o di erogazione di servizi, è un evento non voluto o inatteso che ha una probabilità significativa di compromettere l'operatività aziendale, di minacciare la sicurezza delle informazioni e/o l'erogazione di servizi.

Per il SGSI è un accadimento relativo allo stato di un sistema, servizio o rete, indicante una possibile violazione della politica per la sicurezza delle informazioni, un malfunzionamento delle contromisure o una situazione mai osservata in precedenza, che possa interessare la sicurezza.

Nel caso di erogazione di servizi è una interruzione non pianificata di un servizio, riduzione nella qualità di un servizio o un evento che non ha ancora avuto un impatto su di un servizio al cliente.

Esempi di incidenti sono:

- Manomissione delle apparecchiature del sistema (Server, dischi ecc.) presenti in sala server.
- Manomissione delle apparecchiature di rete e dei cablaggi (sia in sala server che in altri locali).
- Incendi e inondazioni nelle sale server.
- Installazione da parte degli utenti di SW non autorizzato.
- Rallentamento delle prestazioni di un sistema dovuto a traffico non previsto o non autorizzato.

20.3.1.3 Violazione dei dati personali

La Violazione di sicurezza comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

Una violazione dei dati personali può, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali o immateriali alle persone fisiche, ad esempio:

- Perdita del controllo dei dati personali che li riguardano.
- Limitazione dei loro diritti.
- Discriminazione.
- Furto o usurpazione d'identità.
- Perdite finanziarie.
- Decifratura non autorizzata della pseudonimizzazione.
- Pregiudizio alla reputazione.
- Perdita di riservatezza dei dati personali protetti da segreto professionale.

Il titolare del trattamento dei dati deve notificare, non appena viene a conoscenza, la violazione dei dati personali al Garante Privacy (senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza) a meno che il titolare del trattamento non sia in grado di dimostrare che è improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.

20.3.1.4 Problema legato alla sicurezza delle informazioni

Un Problema è la causa originaria di uno o più eventi indesiderati. La causa originaria non è generalmente nota al momento della registrazione dell'evento indesiderato la sua ricerca fa parte del processo di gestione del problema stesso.

20.3.2 Gestione degli eventi imprevisti

Tutto il personale, gli operatori coinvolti nella elaborazione dei dati ed in generale qualsiasi individuo / organizzazione coinvolta nel SGSI che dovessero rilevare eventi imprevisti legati alla Sicurezza delle informazioni o di Erogazione di Servizi, o comunque eventi che manifestino vulnerabilità (effettive o sospette) della sicurezza del sistema informativo, devono avvisare immediatamente il proprio Referente Privacy (che provvederà a verificare l'evento ed in caso a segnalarlo a RSI) o direttamente al RSI.

Una volta ricevuta la segnalazione, RSI deve eseguire le seguenti attività:

- Registrare la segnalazione su SQuadra (Privacy / Incidenti e Violazioni).
- Valutare la segnalazione verificando l'attendibilità, classificandola, valutando il rischio di violazione di dati personali, individuando la minaccia che ha causato l'evento indesiderato.
- Individuare le Misure da intraprendere o rivolgersi ai consulenti IT per avere un supporto e quindi applicare le misure e verificarne l'efficacia.
- Chiudere formalmente l'evento.

Nel caso in cui, conseguentemente ad un evento indesiderato, RSI intraveda la necessità di intraprendere un'azione legale (sia civile che penale) contro una persona od organizzazione, raccoglierà tutte le prove necessarie e le gestirà in maniera conforme alle leggi vigenti.

Le registrazioni degli eventi indesiderati saranno periodicamente estratte da SQuadra in appositi report esaminati allo scopo di individuare:

- La presenza di eventuali problemi che possono aver dato luogo agli incidenti tracciati.
- Possibili opportunità di miglioramento del SGSI.

21 APPENDICE: Controlli sui Sistemi Informativi

21.1 Norma ISO 27001

Nell'Appendice A "Obiettivi di controllo e controlli di riferimento" della Norma ISO 27001 vengono proposti una serie di Controlli.

21.2 Agenzia per l'Italia Digitale

L'Agenzia per l'Italia Digitale (d'ora in poi AgID) ha predisposto delle Misure minime di sicurezza ICT, rivolte alle Pubbliche Amministrazione, che possono comunque essere utilizzate come riferimento per tutte le organizzazioni.

Le Misure sono suddivise in 8 categorie:

A.01	Inventario dei dispositivi autorizzati e non autorizzati
	<i>Gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso</i>
A.02	Inventario dei software autorizzati e non autorizzati
	<i>Gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione</i>
A.03	Proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server
	<i>Istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilità di servizi e configurazioni.</i>
A.04	Valutazione e correzione continua della vulnerabilità
	<i>Acquisire, valutare e intraprendere continuamente azioni in relazione a nuove informazioni allo scopo di individuare vulnerabilità, correggere e minimizzare la finestra di opportunità per gli attacchi informatici</i>
A.05	Uso appropriato dei privilegi di amministratore
	<i>Regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi</i>
A.08	Difese contro i malware
	<i>Controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive.</i>
A.10	Copie di sicurezza
	<i>Procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità.</i>
A.13	Protezione dei dati
	<i>Processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigare gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti</i>

21.2.1 La scelta delle Classi

In funzione della rapida evoluzione della minaccia cibernetica l'AgID ritiene fondamentale la rilevazione delle anomalie operative e ciò rende conto dell'importanza data agli inventari, che costituiscono le prime due classi di misure, nonché la protezione della configurazione, che è quella immediatamente successiva.

La quarta classe deve la sua priorità alla duplice rilevanza dell’analisi delle vulnerabilità. In primo luogo, le vulnerabilità sono l’elemento essenziale per la scalata ai privilegi che è condizione determinante per il successo dell’attacco; pertanto la loro eliminazione è la misura di prevenzione più efficace. Secondariamente si deve considerare che l’analisi dei sistemi è il momento in cui è più facile rilevare le alterazioni eventualmente intervenute e rilevare un attacco in corso.

La quinta classe è rivolta alla gestione degli utenti, in particolare gli amministratori.

La sesta classe deve la sua considerazione al fatto che anche gli attacchi complessi prevedono in qualche fase l’installazione di codice malevolo e la sua individuazione può impedirne il successo o rilevarne la presenza.

Le copie di sicurezza, settima classe, sono alla fine dei conti l’unico strumento che garantisce il ripristino dopo un incidente.

L’ultima classe, la protezione dei dati, deve la sua presenza alla considerazione che l’obiettivo principale degli attacchi più gravi è la sottrazione di informazioni.

L’AgID ha suddiviso le Misure fra:

- **Minime**: che dovrebbero essere applicate da tutte le organizzazioni.
- **Standard**: che dovrebbe essere utilizzata da tutte le organizzazioni.
- **Alte**: che può essere un obiettivo al quale le organizzazioni possono tendere.

Per ogni Misura vengono riportati i Riferimento che l’AgID ha previsto rispetto al “Framework Nazionale per la Cyber Security” predisposto dalla Università “La Sapienza”.

21.3 Framework Nazionale per la Cyber Security”.

21.3.1 Premessa

Il Framework Nazionale per la Cyber Security”, predisposto dalla Università “La Sapienza”, si basa sulla considerazione che il sistema economico e sociale dei paesi avanzati è diventato fortemente dipendente dal cyberspace, quell’insieme di reti e sistemi informativi con i quali vengono erogati servizi indispensabili. Tuttavia, il cyberspace e le sue componenti essenziali sono esposti a numerosi rischi. In primis, trattandosi di sistemi complessi e in rapida evoluzione, vi è una costante presenza di vulnerabilità. Nonostante gli sforzi, siccome non vi è oggi possibilità di disporre di sistemi non vulnerabili, occorre tenere sempre in considerazione eventuali minacce.

L’adesione al Framework, rappresentativo delle pratiche generalmente riconosciute e internazionalmente validate, permette una più agevole dimostrazione della applicazione della “due diligence”, riferendosi a razionali, oggettivi e misurabili, per aver posto in essere quanto era doveroso attendersi in applicazione del principio di “dovuta diligenza”.

21.3.2 La cyber security

21.3.2.1 Generalità

Gli incidenti possono essere naturali o provocati da terroristi, cybercriminali, attivisti ecc. In questi ultimi casi, se la vittima è una impresa, oltre al danno reputazionale, si possono avere danni finanziari ingentissimi: dalla semplice perdita di competitività fino alla completa perdita del controllo degli asset strategici.

La cyber security è quella pratica che consente a una organizzazione la protezione dei propri asset fisici e la confidenzialità, integrità e disponibilità delle proprie informazioni dalle minacce che arrivano dal cyber space (il complesso ecosistema risultante dall'interazione di persone, software e servizi su Internet per mezzo di tecnologie, dispositivi e reti ad esso connesse).

Come ogni rischio aziendale, il rischio cyber non può essere eliminato e ha quindi bisogno di un insieme di azioni coordinate per poter essere gestito. Azioni che coinvolgono gli ambiti organizzativi e tecnologici dell'azienda, oltre che di gestione finanziaria del rischio, anche attraverso la definizione di una strategia di gestione del rischio residuo, abilitando in tal modo l'adozione di un approccio integrato di prevenzione del rischio e di protezione del bilancio dell'impresa.

Il rischio cyber è intrinsecamente altamente dinamico. Esso cambia al cambiare delle minacce, delle tecnologie e delle regolamentazioni.

21.3.2.2 Ruolo del Framework

Il Framework vuole essere neutrale tanto rispetto alle pratiche di risk management aziendali quanto rispetto alla tecnologia, in modo che ogni organizzazione possa continuare a usare i propri strumenti di gestione del rischio e a gestire i propri asset tecnologici continuando anche a mantenere la conformità agli standard di settore.

Il Framework può aiutare una impresa a organizzare un percorso di gestione del rischio cyber, sviluppato nel tempo, in funzione del suo business, della sua dimensione e di altri elementi caratterizzanti e specifici dell'impresa.

21.3.2.3 La gestione del rischio cyber

Il compito fondamentale della cyber security è la protezione e la tutela della missione delle organizzazioni dai rischi derivanti dal cyberspace e dai sistemi informativi.

Il rischio può essere visto come il risultato di tre fattori: la minaccia, la vulnerabilità e l'impatto.

L'analisi delle tre componenti fondamentali può consentire a una organizzazione di ridurre il rischio attraverso una serie di tecniche, che vanno dalla riduzione delle vulnerabilità alla riduzione del possibile danno; in alcuni casi si può anche contemplare la riduzione della minaccia, ove sia possibile.

Ogni organizzazione deve valutare i propri rischi e, in base al proprio livello di tolleranza, decidere quali contromisure adottare. In generale, essendo un concetto altamente legato all'aleatorietà delle variabili che lo determinano, non si considera possibile poter ridurre un rischio a zero, esiste di conseguenza sempre un livello di rischio residuo da considerare. Le organizzazioni devono valutare l'equilibrio tra riduzione del rischio, rischio residuo e la propria "tolleranza" al rischio. Il rischio residuo può essere quindi accettato, oppure trasferito nelle sue conseguenze economiche all'esterno, per esempio attraverso l'uso di prodotti assicurativi.

Le PMI spesso ricorrono a un fornitore di servizi di sicurezza esterno non risultando conveniente allocare risorse umane e tecnologiche al monitoraggio degli eventi di sicurezza. È però necessario ricordare che le valutazioni connesse alla gestione del rischio (valutazione delle opzioni di mitigazione, accettazione, trasferimento) non possono essere delegate rappresentando una componente fondamentale della conduzione di una organizzazione, la loro approvazione è una responsabilità inalienabile del top management.

21.3.3 Organizzazione del Framework

Il Framework analizza le seguenti funzioni:

- **Identificare:** legata alla comprensione del contesto aziendale, degli asset che supportano i processi critici di business e dei relativi rischi associati. Tale comprensione permette infatti a un'organizzazione di definire risorse e investimenti in linea con la strategia di gestione del rischio e con gli obiettivi aziendali.
- **Proteggere:** è associata all'implementazione di quelle misure volte alla protezione dei processi di business e degli asset aziendali, indipendentemente dalla loro natura informatica.
- **Individuare:** è associata alla definizione e attuazione di attività appropriate per identificare tempestivamente incidenti di sicurezza informatica.
- **Rispondere:** è legata alla definizione e attuazione delle opportune attività per intervenire quando un incidente di sicurezza informatica sia stato rilevato. L'obiettivo è contenere l'impatto determinato da un potenziale incidente di sicurezza informatica.
- **Ripristinare.** La Function Recover è associata alla definizione e attuazione delle attività per la gestione dei piani e delle attività per il ripristino dei processi e dei servizi impattati da un incidente. L'obiettivo è garantire la resilienza dei sistemi e delle infrastrutture e, in caso di incidente, supportare il recupero tempestivo delle business operations.

Per ogni funzione sono individuate delle Categorie e delle Sottocategorie con delle raccomandazioni.

21.3.3.1 Profilo

Un Profilo si ottiene attraverso una selezione delle Sottocategorie del Framework. Tale selezione può avvenire in base a diversi fattori, guidati principalmente dal risk assessment, dal contesto di business, dall'applicabilità delle varie Sottocategorie.

I profili possono essere utilizzati come opportunità per migliorare lo stato di sicurezza mettendo a confronto un profilo attuale (anche detto corrente), con un profilo desiderato (anche detto target). Per sviluppare un profilo, un'organizzazione deve esaminare ciascuna delle Sottocategorie e, sulla base delle caratteristiche di business e della valutazione dei propri rischi, determinare quali sono da implementare e quali non sono applicabili nel proprio contesto. Le Sottocategorie potranno essere integrate con ulteriori pratiche non previste dal Framework al fine di gestire in maniera completa il rischio.

Il profilo attuale può quindi essere utilizzato per definire priorità e misurare i progressi verso il profilo desiderato.

I profili possono essere utilizzati per:

- Effettuare un'autovalutazione.
- Comunicare il proprio livello di gestione del rischio all'interno o all'esterno dell'organizzazione.
- Definire i profili minimi richiesti da un'organizzazione per i propri fornitori al fine di rafforzare l'intera supply chain in caso di particolari criticità.

SQaudra permette di definire Profili da richiedere, dove necessario, alle varie tipologie di fornitori.

21.3.3.2 Livello di implementazione

Nel Framework sono previsti quattro livelli di valutazione, dal più debole al più forte per indicare la valutazione aziendale del rischio cyber e i processi posti in essere per gestirlo:

- **Parziale.** Un modello di gestione del rischio di cyber security di una organizzazione è parziale se questo non tiene conto in modo sistematico del rischio cyber o delle minacce ambientali.

- **Informato.** Un modello di gestione del rischio cyber di una organizzazione è informato se l'organizzazione ha dei processi interni che tengono conto del rischio cyber, ma questi non sono estesi a tutta l'organizzazione.
- **Ripetibile.** Un modello di gestione del rischio cyber di una organizzazione è ripetibile se l'organizzazione aggiorna regolarmente le proprie pratiche di cyber security basandosi sull'output del processo di risk management.
- **Adattivo.** Un modello di gestione del rischio cyber di una organizzazione è adattivo se l'organizzazione adatta le sue procedure di cyber security frequentemente attraverso l'utilizzo delle esperienze passate e degli indicatori di rischio.

I Livelli di implementazione non vengono trattati nella contestualizzazione proposta per le PMI.

Per semplicità, all'interno di SQuadra, sono previsti i seguenti livelli di valutazione per l'implementazione delle misure per le varie Sottocategorie:

- Non applicabile.
- Applicato e formalizzato.
- Applicato ma non sempre formalizzato.
- Parzialmente applicato.
- Previsto ma non ancora applicato.
- Non presente / Non applicato.

21.3.3.3 Livello di priorità

I livelli di priorità permettono di supportare le organizzazioni nell'identificazione preliminare delle Sottocategorie da implementare per ridurre maggiormente i livelli di rischio a cui sono sottoposte, bilanciandone l'impegno da profondere per la loro attuazione.

Il Framework suggerisce l'utilizzo di una scala di priorità a tre livelli tra le Sottocategorie. L'obiettivo è quello di:

- Semplificare l'individuazione delle Sottocategorie essenziali da implementare immediatamente e inderogabilmente.
- Supportare le organizzazioni durante il processo di analisi e gestione del rischio.

La determinazione dei livelli di priorità assegnati alle Sottocategorie deve essere effettuata sulla base di due specifici criteri:

- Capacità di ridurre il rischio cyber, agendo su uno o più dei fattori chiave per la determinazione, ovvero:
 - Esposizione alle minacce, intesa come l'insieme dei fattori che aumentano o diminuiscono la facilità con cui la minaccia stessa può manifestarsi;
 - Probabilità di loro accadimento, ovvero la frequenza con cui una specifica minaccia può verificarsi nel tempo.
 - Impatto conseguente sulle Business Operations o sugli Asset aziendali, intesa come l'entità del danno conseguente al verificarsi di una minaccia.
- Semplicità di implementazione delle Sottocategorie, anche considerando il livello di maturità tecnica e organizzativa tipicamente richiesto per realizzare la specifica azione.

La combinazione dei due criteri sopra descritti ha permesso di definire tre livelli distinti di priorità:

- **Priorità Alta:** interventi che permettono di ridurre sensibilmente uno dei tre fattori chiave del rischio cyber. Questi interventi sono prioritari e per loro natura sono da attuare indipendentemente dalla complessità realizzativa degli stessi.

- **Priorità Media:** interventi che permettono di conseguire una riduzione di uno dei tre fattori chiave del rischio cyber e che risultano generalmente anche di semplice implementazione.
- **Priorità Bassa:** interventi che permettono di conseguire una riduzione di uno dei tre fattori chiave del rischio cyber, ma la cui complessità realizzativa è generalmente considerata elevata (ad esempio cambiamenti organizzativi rilevanti e/o modifiche infrastrutturali significative).

Su SQuadra sono riportate le valutazioni relative alle PMI.

21.3.3.4 Livelli di maturità

I livelli di maturità permettono di fornire una misura della maturità di un processo di sicurezza, della maturità di attuazione di una tecnologia specifica o una misura della quantità di risorse adeguate impiegate per l'implementazione di una data Sottocategoria.

I livelli di maturità forniscono un punto di riferimento in base al quale ogni organizzazione può valutare la propria implementazione delle Sottocategorie e fissare obiettivi e priorità per il loro miglioramento. I livelli devono essere in progressione, dal minore al maggiore. Ogni livello deve prevedere pratiche e controlli incrementali rispetto al livello di maturità inferiore.

Un'organizzazione potrà quindi:

- Identificare il livello di maturità raggiunto.
- Identificare il livello desiderato.
- Identificare le pratiche di sicurezza necessarie per raggiungere il livello desiderato.

Su SQuadra sono previsti 4 livelli di maturità.

Sono riportati, dove presenti, i 3 livelli di maturità previsti per le PMI.

21.3.4 Contestualizzazione del Framework

Una organizzazione che voglia utilizzare il Framework, come primo passo, deve identificare una contestualizzazione su cui valutare il proprio profilo di rischio attuale.

Una contestualizzazione del Framework implica la selezione delle sottocategorie del Framework Core e la definizione dei relativi livelli di priorità e di maturità. La contestualizzazione viene fatta rispetto al profilo di business, alle vulnerabilità di settore, alla dimensione dell'organizzazione e ad altre caratteristiche aziendali o di settore.

Una caratterizzazione del Framework si crea attraverso i seguenti passi:

- Selezionare l'elenco delle Funzioni/Categorie/Sottocategorie che sono pertinenti per l'organizzazione (in base a settore produttivo, dimensione, dislocazione sul territorio dell'organizzazione, ecc.).
- Definire i livelli di priorità per l'implementazione per le Sottocategorie selezionate.
- Definire delle linee guida almeno per le Sottocategorie a priorità alta.
- Specificare i livelli di maturità almeno per le Sottocategorie a priorità alta.

È opportuno implementare per tutte le Sottocategorie a priorità alta, almeno al livello minimo di maturità.

21.3.5 Contestualizzazione per le PMI

SQuadra riporta la contestualizzazione del Framework per le piccole e media imprese italiane.

Per ogni Sottocategoria è stato individuato il Livello di Priorità (per quelle ritenute significative).

Per quelle a Priorità Alta sono stati individuati fino a tre livelli di maturità.

Le 18 Sottocategorie con Priorità Alta sono state raggruppate in 11 Sotto Aree suddivise fra 4 Aree di Indirizzo.

Per ciascuna Sotto Area sono indicati i controlli di carattere procedurale, organizzativo e tecnico da attuare.

21.3.6 Controlli essenziali 2016

Nel 2016 sono stati pubblicati i Controlli Essenziali di Cybersecurity derivati, attraverso un processo di progressiva semplificazione, dal Framework Nazionale di Cybersecurity (FNCS), pubblicato nell’Italian Cybersecurity Report 2015. Questa scelta è stata motivata dalla volontà di definire un percorso virtuoso che dovrebbe portare le piccole e micro imprese a implementare misure di sicurezza via via più complesse e articolate aderenti al FNCS, ritrovandosi così avvantaggiate nel processo di definizione del proprio profilo di rischio. I Controlli Essenziali di Cybersecurity sono stati selezionati attraverso un processo di consultazione pubblica al quale hanno partecipato oltre 200 esperti di settore.

22 APPENDICE: Linee Guida ENISA sulla sicurezza dei dati personali

22.1 Introduzione

Nel 2016 l'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA) ha pubblicato le "Linee Guida sulla sicurezza del trattamento dei dati personali" per fornire un supporto alle PMI per le quali può essere difficile comprendere le specificità dei rischi associati al trattamento dei dati personali, nonché valutare e gestire tali rischi secondo una metodologia formale come richiesto dal GDPR.

Nel 2017 la stessa Agenzia ha pubblicato il "Manuale sulla sicurezza di Trattamento dei dati personali" nel quale, utilizzando la metodologia proposta nel 2016, vengono analizzati alcuni casi specifici di trattamenti tipici della PMI.

22.1.1 La Sicurezza delle informazioni

La Riservatezza

La riservatezza è definita come la "proprietà che le informazioni non sono rese disponibili o divulgata a persone, entità o processi non autorizzati". In pratica, tutte le misure adottate per garantire la riservatezza sono volte ad impedire l'accesso alle informazioni da parte di persone, entità o processi non autorizzati, assicurando al contempo che le persone, entità o processi autorizzati vi abbiano accesso. Nella maggior parte dei casi le informazioni sono classificate in base alla quantità e al tipo di danno che potrebbe essere fatto se cadesse in mani non intenzionali. Misure più o meno severe possono quindi essere attuate in base a queste categorie.

L'integrità

L'integrità è definita come la proprietà di "accuratezza e completezza". In questo senso, l'integrità implica il mantenimento della coerenza, dell'accuratezza e dell'affidabilità delle informazioni per l'intero ciclo di vita. I dati non devono essere modificati durante il trasporto e devono essere adottate misure per garantire che i dati non possano essere alterati da persone, entità o processi non autorizzati. Da un punto di vista pratico, ciò significa che i dati non possono essere modificati in modo non autorizzato o non rilevato.

La Disponibilità

La disponibilità è definita come la proprietà di "informazioni accessibili e utilizzabili quando un soggetto autorizzato lo richiede". Ciò significa che i sistemi utilizzati per memorizzare ed elaborare le informazioni e i canali di comunicazione delle informazioni funzionano tutti correttamente. In pratica, ciò è garantito al meglio da una manutenzione senza compromessi dell'hardware, eseguendo riparazioni hardware immediatamente quando necessario e mantenendo un ambiente di sistema operativo correttamente funzionante che è privo di conflitti software.

22.1.2 Gestione del Rischio

Un processo di gestione del rischio comprende quattro fasi chiave, come segue:

- Valutazione dei rischi: Può essere inteso come la generazione di un'istantanea dei rischi attuali. Un rischio è spesso espresso in funzione della probabilità che si verifichi un esito negativo (minaccia) moltiplicato per l'entità dell'eventuale esito negativo (impatto). La valutazione dei rischi inizia con l'individuazione delle minacce, seguita dalla determinazione della probabilità pertinente e dell'impatto di ciascun rischio. Per valutare correttamente il rischio, occorre prendere in considerazione sia la probabilità che l'impatto.
- Trattamento del rischio: Sulla base dei risultati della valutazione dei rischi, in questa fase l'organizzazione seleziona e attua misure di sicurezza per il trattamento dei rischi. Le misure

possono avere effetti diversi, quali: mitigazione, trasferimento, trasferimento, prevenzione o mantenimento dei rischi. Per il trattamento dei rischi possono (e dovrebbero) essere utilizzate molteplici misure di sicurezza di vario tipo.

- Accettazione del rischio: Anche quando i rischi sono stati trattati, i rischi residui probabilmente rimarranno (ad esempio a causa del fatto che alcuni controlli non sono fattibili). Questi rischi dovranno essere accettati. Si tratta di una decisione di gestione che deve seguire l'accettazione del modo in cui i rischi sono stati trattati.
- Comunicazione del rischio: Tutte le parti interessate devono essere informate sui rischi adottati e sui rischi accettati.

La gestione del rischio si è notevolmente ampliata sin dall'inizio ed è attualmente generalmente riconosciuto che il rischio non può essere ridotto a zero e, pertanto, è essenziale che un'organizzazione sia in grado di comprenderlo e valutarlo al fine di dare priorità alle risorse.

22.1.3 *Obblighi di sicurezza nel GDPR*

Sulla base delle disposizioni dell'Art. 32 del GDPR, vi sono alcune importanti osservazioni da fare in merito alla sicurezza dei dati personali nell'ambito del GDPR:

- Approccio basato sul rischio: Le misure tecniche e organizzative per la protezione dei dati personali dovrebbero, secondo il GDPR, essere adeguate al rischio presentato. GDPR pone un accent particolare sulla nozione di rischio, stabilendo parametri specifici di protezione dei dati che devono essere presi in considerazione per la sua valutazione, in particolare la natura, la portata, il contesto e le finalità del trattamento. Inoltre, collega chiaramente il rischio alle misure adottate per preservare i diritti e le libertà degli individui. Questo approccio introduce infatti l'impatto di una potenziale violazione dei dati personali per le persone interessate come un aspetto importante della valutazione dei rischi e dovrebbe essere considerato anche in relazione all'obbligo di una valutazione formale dell'impatto sulla protezione dei dati (ai sensi dell'articolo 35 del GDPR). Detto questo, è anche importante notare che la nozione di rischio è centrale in generale nel GDPR come soglia per l'attuazione da parte del responsabile del trattamento di diversi obblighi, ad esempio per quanto riguarda la notifica delle violazioni dei dati personali (articoli 33 e 34 del GDPR), lo svolgimento della valutazione d'impatto sulla protezione dei dati, la consultazione preliminare delle autorità competenti (articolo 36 del GDPR).
- Un sistema informatico di gestione dei dati personali: La disposizione del GDPR va oltre la semplice adozione di misure di sicurezza specifiche, sostenendo l'istituzione di un sistema di gestione delle informazioni completo per la protezione della riservatezza, dell'integrità, della disponibilità e della resilienza dei dati personali. Ciò è importante da sottolineare in quanto il testo affronta in egual misura tutte le dimensioni della sicurezza dell'informazione, imponendo esplicitamente un processo di verifica, valutazione e valutazione dell'efficacia delle misure adottate.
- Sicurezza per la privacy: Sebbene il GDPR non contenga un riferimento diretto alle tecnologie di rafforzamento della privacy, esso affronta specificamente la pseudonimizzazione e la cifratura come misure fondamentali di protezione della sicurezza dei dati personali. Ciò dimostra che la sicurezza del GDPR è considerata nel contesto generale della vita privata e potrebbe includere, ad esempio, la protezione dell'identità attraverso l'uso di pseudonimi o l'uso di meccanismi di cifratura per costringere la cancellazione sicura dei dati dopo la fine del periodo di conservazione definito. Questo punto dovrebbe anche essere collegato alle disposizioni del GDPR per la protezione dei dati fin dalla progettazione e di default (articolo 25), che pone l'accento sull'ingegnerizzazione dei requisiti di riservatezza nei sistemi e servizi informatici, andando oltre la comprensione "tradizionale" della sicurezza. È interessante

notare che tali disposizioni sono anche collegate al rischio di trattamento dei dati personali (che funge anche in questo caso da soglia per l'adozione di misure pertinenti).

22.2 Valutazione dei Rischi per la sicurezza dei dati personali

22.2.1 Definizione dell'operazione di trattamento e del suo contesto

Per ogni Trattamento è possibile definire:

- Descrizione del trattamento dei dati personali.
- Quali sono i tipi di dati personali trattati.
- Qual è lo scopo del trattamento.
- Quali sono gli strumenti utilizzati per il trattamento dei dati personali.
- Dove avviene il trattamento dei dati personali.
- Quali sono le categorie di persone interessate.
- Quali sono i destinatari dei dati.

Squadra permette di inserire queste informazioni nel Registro dei Trattamenti.

22.2.2 Comprensione e valutazione dell'impatto

22.2.2.1 Livello dell'impatto

È possibile considerare i seguenti valori:

Basso: Gli individui possono incontrare alcuni inconvenienti minori, che possono essere superati senza problemi (tempo passato a reinserire informazioni, fastidi, irritazioni, ecc.).

Medio: I singoli individui possono incontrare notevoli inconvenienti, che potranno superare nonostante alcune difficoltà (costi aggiuntivi, rifiuto di accesso ai servizi aziendali, paura, mancanza di comprensione, stress, disturbi fisici minori, ecc.).

Alto: Le persone possono avere conseguenze significative, che dovrebbero essere in grado di superare, anche se con serie difficoltà (appropriazione indebita di fondi, iscrizione in lista nera da parte degli istituti finanziari, danni materiali, perdita del posto di lavoro, mandati di comparizione, peggioramento della salute, ecc.).

Molto alto: Persone che possono incontrare conseguenze significative, o addirittura irreversibili, che non possono superare (incapacità lavorativa, disturbi fisici o psicologici a lungo termine, morte, ecc.).

L'impatto può essere valutato analizzando i seguenti elementi:

- **Tipo di dati personali:** Questo parametro può, per sua natura, aumentare o diminuire immediatamente il livello di impatto, in base alla criticità dei dati. Ad esempio, quando i dati includono archivi medici o informazioni sulle convinzioni politiche (o qualsiasi altra categoria speciale di dati nell'ambito del GDPR), l'impatto di una violazione della sicurezza può essere grave per gli individui. Tuttavia, la valutazione non può basarsi unicamente sulla distinzione dei dati tra "dati semplici" e categorie speciali di dati. Infatti, anche i dati personali che non rientrano in una categoria speciale possono rivelare informazioni molto critiche su un individuo (ad es. posizione, abitudini, informazioni finanziarie) e, quindi, portare effetti disastrosi su di lui/lei in caso di violazione.
- **Criticità dell'operazione di trattamento:** A seguito del punto precedente, è importante valutare la criticità complessiva del trattamento, al di là delle particolari tipologie di dati. Particolare attenzione dovrebbe essere prestata alle operazioni di trattamento che si basano o possono portare al monitoraggio o alla sorveglianza sistematica delle persone.
- **Volume dei dati personali trattati:** Questo parametro si riferisce alla quantità di dati personali che vengono trattati per un singolo individuo: più i dati sono numerosi, più sono i potenziali effetti negativi. Il volume deve essere considerato sia in termini di tempo (ad esempio, stesso tipo di dati per un certo periodo di tempo) che di contenuto (a complemento di dati dello stesso tipo). Ad esempio, in caso di violazione della riservatezza dei dati relativi al traffico presso un fornitore di servizi di messaggistica,

l'impatto per un individuo sarebbe maggiore se questi dati coprono l'intero periodo di un anno piuttosto che se sono limitati a una sola settimana.

- **Caratteristiche particolari del titolare/responsabile del trattamento:** Questo parametro si riferisce al campo di attività e alle attività aziendali dell'organizzazione, che per loro natura possono rivelare informazioni aggiuntive per un certo insieme di dati (quindi, potenzialmente in grado di influenzare il livello di impatto). Ad esempio, la violazione della riservatezza di una lista di clienti può essere maggiore se questa lista proviene da una farmacia online piuttosto che da un negozio di cartoleria.
- **Caratteristiche particolari degli interessati:** L'impatto potrebbe anche aumentare nel caso in cui le persone interessate appartengano a un gruppo sociale con esigenze particolari (ad esempio, minori, personalità pubbliche). Ad esempio, l'elaborazione di un elenco di numeri telefonici diventa più critica se riguarda i membri noti del parlamento nazionale.

22.2.3 Valutazione dell'impatto

È opportuno valutare l'impatto - nel contesto in cui si svolge l'attività - separatamente per la perdita di riservatezza, integrità e disponibilità:

Riservatezza: impatto che una divulgazione non autorizzata (perdita di riservatezza) di dati personali potrebbe avere sull'individuo.

Ad esempio: Un file cartaceo o portatile contenente dati personali viene perso. Una apparecchiatura è stata smaltita senza distruzione dei dati personali. I dati personali sono inviati erroneamente ad un certo numero di destinatari non autorizzati.

Integrità: impatto che un'alterazione non autorizzata dei dati personali potrebbe avere sull'individuo.

Ad Esempio: Le informazioni recuperate da un backup non tengono conto delle transazioni successive al momento della copia.

Disponibilità: impatto che una distruzione o perdita non autorizzata (perdita di disponibilità) di dati personali potrebbe avere sull'individuo ed esprimere una valutazione di conseguenza.

Ad Esempio: Un servizio non è disponibile per malfunzionamenti del sistema.

In base alle valutazioni si otterranno tre diversi livelli di impatto (per la perdita di riservatezza, integrità e disponibilità). Il più alto di questi livelli può essere considerato come il risultato finale della valutazione dell'impatto, relativo al trattamento complessivo dei dati personali.

NOTA: Squadra utilizza una scala di maggior dettaglio che è possibile riportare ai livelli previsti dal documento in esame: Trascurabile e Bassa = BASSA; Media = MEDIA; Alta e Critica= ALTA.

22.2.4 Definizione delle minacce

Le minacce possono essere legate a quattro dimensioni principali, vale a dire:

Risorse di rete e tecniche (hardware e software): Le connessioni di rete possono introdurre minacce sia da fonti esterne (ad esempio, aggressori esterni che mirano ad ottenere l'accesso remoto al sistema o ad abbattere il sistema), sia da fonti interne (ad esempio, l'interconnessione con altri sistemi IT all'interno della stessa organizzazione che presentano difetti di sicurezza). Le risorse hardware e software possono anche introdurre minacce, ad esempio a causa di scarsa manutenzione e configurazione, così come a causa di bug e backdoor relative allo sviluppo di dispositivi e software. Le minacce comuni associate alle risorse di rete e tecniche (hardware/software) comprendono l'intercettazione dei canali di comunicazione, l'accesso non autorizzato alle banche dati, l'indisponibilità dei servizi forniti, il fallimento dei collegamenti di comunicazione, l'uso improprio/anormale dei sistemi informativi, ecc.

Processi/procedure relative all'operazione di trattamento dei dati: In molti casi le minacce alla sicurezza derivano dalla mancanza di processi e procedure interne adeguate, che impongono regole e pratiche specifiche all'interno dell'organizzazione per il trattamento dei dati personali. Tali minacce comprendono l'accesso ai dati da parte di persone non autorizzate, la corruzione (non intenzionale) dei dati, la modifica/distruzione non autorizzata dei dati, lo smaltimento accidentale o la perdita di apparecchiature per l'elaborazione dei dati, ecc.

Diversi soggetti e persone coinvolte nel trattamento: Le minacce alla sicurezza possono derivare anche da coloro che effettuano il trattamento dei dati personali, ossia i dipendenti dell'organizzazione direttamente

coinvolti nel trattamento, nonché da altri soggetti che svolgono parte del trattamento (responsabili del trattamento). Le minacce rilevanti includono potenziali attacchi interni dannosi (ad esempio con il supporto di specifici dipendenti), uso improprio accidentale di dati personali a causa di errori umani, divulgazione non autorizzata di dati da parte di appaltatori esterni, ecc.

Settore di attività e scala della lavorazione: Il settore di attività di un'organizzazione, così come la scala (volume) dei dati trattati può anche influenzare in modo significativo il tipo e il livello delle minacce alla sicurezza. Ad esempio, se il tipo di dati personali è considerato un bene prezioso e/o se il trattamento riguardasse l'intera popolazione di un paese, gli aggressori potrebbero essere più interessati ad accedere a questi dati.

Tali dimensioni devono essere considerate tenendo conto delle specifiche operazioni di trattamento dei dati personali e delle sue caratteristiche.

È necessario valutare la probabilità di minacce per ognuna delle quattro diverse aree. Se tutte le risposte alle domande per le varie aree sono positive, allora l'organizzazione dovrebbe considerare **ALTA** la probabilità di minaccia per quest'area (valore=3), mentre se tutte sono negative, allora la probabilità di minaccia dovrebbe essere considerata **BASSA** (valore=1). Per i casi con due o tre risposte positive, l'organizzazione dovrebbe assegnare la probabilità di minaccia alla **MEDIA** (valore=2).

Sommando i valori ottenuti potremo valutare la probabilità di accadimento delle minacce:

- BASSA per valore totale < 6
- MEDIA per valore totale < 9
- ALTA negli altri casi.

22.2.5 Valutazione del rischio

Dopo aver valutato l'impatto dell'operazione di trattamento dei dati personali e la relativa probabilità di accadimento della minaccia, è possibile effettuare la valutazione finale del rischio, come illustrato nella tabella seguente.

		LIVELLO DI IMPATTO		
		Basso	Medio	Alto/Altissimo
PROBABILITÀ MINACCIA	Basso	Rischio Basso	Rischio Medio	Rischio Alto
	Medio	Rischio Basso	Rischio Medio	Rischio Alto
	Alto	Rischio Medio	Rischio Alto	Rischio Alto

Come è possibile vedere la tabella non è “simmetrica” nel senso che, a fronte di un impatto “Alto” il Rischio è considerato comunque “Alto” mentre a fronte di un Impatto “Basso”, anche in caso di probabilità di minacce “Alto” non si raggiunge mai il Rischio “Alto”.

23 REVISIONI

Versione	Principali Modifiche
0.a (Ott. 2015)	È la prima presentazione della nuova versione del Modulo Esteso (rilasciato in versione beta).
0.b (Nov. 2015)	Aggiunta illustrazione delle rappresentazioni grafiche.
0.c (Gen. 2016)	Nuovo Modulo: Oneri per la Sicurezza
1a (Feb. 2016)	CUBI di sintesi e Analisi degli aggiornamenti normativi. Funzioni per i Consulenti. Analisi dei Rischi e Interviste. Analisi dei Rischi Residui Rilevati.
1b (Mar 2016)	Stampa dei Documenti approvati. Archivio stampe personalizzate.
1c (Apr 2016)	Mappatura delle Attività a Rischio. Funzioni Aggiuntive per la gestione dei Rapporti con la PA e di alcuni Moduli del SGSL.
2a (Giu 2016)	Segnalazioni all'OdV.
2b (Lug 2016)	Documentazione aziendale relativa alla sicurezza sul lavoro.
3a (Ago 2016)	Nuova organizzazione del Manuale. Gestione dei Provvedimenti Disciplinari proposti dall'OdV.
3b (Set 2016)	Canale di comunicazione sicuro (HTTPS). Grafici per presentazione Azioni e Rischio / Punti di Controllo. Nuova gestione interfaccia utente.
4a (Gen 2017)	Amministratore del Sistema (Creazione nuovi utenti). Sistema di Gestione: Non Conformità, Azioni Correttive, Lavoratori (Formazione, Visite Mediche, DPI), Macchinari, Incidenti, Valutazione Fornitori.
4b (Feb 2017)	Gestione Scadenze e riorganizzazione del Sistema di Gestione. APPENDICE: Specifiche tecniche e livelli del servizio.
4c (Mar 2017)	Ampliamento funzionalità nel Sistema di Gestione. Ampliamento delle funzionalità delle Stampe Personalizzate. APPENDICE: Trattamento dei dati.
4d (Mag 2017)	Aggiunta nell'Appendice 3 la Politica per la "Segnalazione dei sospetti" conforme alla norma UNI ISO 37001 (Punto 8.9). Allineati alla UNI ISO 37001 (Punto 6.2) gli elementi per le azioni per il raggiungimento degli Obiettivi. Aggiunta una sezione specifica per i sistemi conformi alla UNI ISO 37001 sotto i Sistemi di Gestione comprendente anche elementi previsti dalla Legge 190/12. Aggiunta la gestione del Riesame della Direzione sotto i Sistemi di Gestione.
4e (Giu 2017)	Nella Prevenzione della Corruzione è stato aggiunto il modulo per il controllo delle pubblicazioni per la "Amministrazione Trasparente". Aggiunta l'appendice 9 sull'Analisi del Contesto.

	Aggiunta l'appendice 10 sulla Valutazione dei Fornitori.
4f (Lug 2017)	<p>Possibilità di definire utenti con accesso in sola visualizzazione.</p> <p>Aggiunta l'appendice 10 sull'analisi dei singoli Processi (la valutazione dei Fornitori ha preso il numero 11).</p> <p>Aggiunta l'appendice 12 sulla gestione delle Prescrizioni (legislative o aziendali).</p> <p>Aggiornata l'appendice relativa alle Segnalazioni.</p> <p>Riorganizzato il menu relativo ai Sistemi di Gestione.</p>
4g (Ago 2017)	<p>Possibilità di aggiungere documenti di Word per descrivere prassi aziendali collegate alle varie Procedure.</p> <p>Gestione delle Scadenze e invio di Mail per la loro segnalazione.</p>
4h (Ott 2017)	<p>Aggiunta l'appendice 13 relativa all'Idoneità Tecnico Professionale.</p> <p>Analisi dei Rischi con riferimento alla versione 2013 del COSO Internal Control – Integrated Framework - 2013.</p> <p>Aggiunta l'area relativa ai controlli sui Sistemi Informativi.</p>
4i (Nov 2017)	<p>Aggiunta la pianificazione e registrazione dei Controlli (SG/08: Operativo).</p> <p>Aggiunte le importazioni di Persone, Fornitori e Macchinari (SG/Varie).</p>
4l (Dic 2017)	<p>Aggiunta nei Riesami per i Sistemi di Gestione la gestione delle Informazioni documentate e gli elementi Determinati.</p> <p>Aggiunta la correlazione fra Obiettivi del Riesame, i Fattori Interni (punti di forza e di debolezza) ed Esterni (Rischi ed Opportunità) e le aspettative delle Parti Interessate.</p>
4m (Gen 2018)	<p>Aggiunta l'Appendice per l'Asseverazione.</p> <p>Aggiunta l'Appendice per l'introduzione di nuovi Reati.</p> <p>Aggiunta l'Appendice per il Regolamento Europeo per la protezione dei dati personali (GDPR).</p> <p>Aggiunta esportazione check list ed importazione dei controlli di 2° livello.</p>
4n (Feb 2018)	<p>Aggiunta l'Appendice per l'adeguamento dei Modelli predisposti con SQuadra per aggiornamento 2018 del Codice di Comportamento ANCE.</p> <p>Aggiornamento automatico dei Responsabili delle Attività legate alle Prescrizioni in base ai Ruoli definiti per i Lavoratori.</p> <p>Sistemi Informativi: Conformità.</p>
5a (Mar 2018)	<p>Riorganizzazione delle Appendici.</p> <p>Ampliamento delle funzionalità legate all'Asseverazione.</p> <p>Ampliamento delle funzionalità legate al GDPR.</p>
5b (Mag 2018)	<p>Inserimento Appendice: "Informativa sul trattamento dei dati".</p> <p>Inserimento Appendice: "Controlli sul Sistema Informativo".</p>
5c (Giu 2018)	<p>Rilascio ufficiale del Modulo GDPR.</p> <p>Riorganizzazione del Menu [accorpamento delle attività dell'OdV e nuova sezione "GDPR"] e conseguente riorganizzazione del presente Manuale.</p>
6a (Ago 2018)	Riorganizzazione Manuale per SQuadra-EDILIZIA.
6b (Set 2018)	Aggiornamento al Recepimento del GDPR nella normativa italiana.
6c (Ott 2018)	Recepimento documenti ENISA per la protezione dei dati personali.

6d (Dic 2018)	<p>Modifica Appendice: "Specifiche Tecniche" nella più ampia "SGSI de IL TIGLIO SRL".</p> <p>Macchinari: Aggiunta la possibilità di definire Responsabile e Conformità; aggiunta, sotto le scadenze, la possibilità di ottenere le Schede per la rilevazione delle manutenzioni in scadenza.</p>
6e (Feb 2019)	<p>Modifiche all'Appendice "SGSI de IL TIGLIO SRL" a seguito della Certificazione e con indicazioni specifiche per i rischi connessi al Cloud.</p> <p>Collegamento delle Non Conformità e degli Incidenti a una o più Azioni Correttive.</p> <p>Aggiunta la gestione dei Data Base fra l'Inventario Privacy.</p> <p>Aggiunta, nel Registro dei Trattamenti, la sezione relativa al test di bilanciamento per trattamenti in base al legittimo interesse.</p> <p>Aggiunta la catalogazione delle Segnalazioni (Zona e Argomento) e possibilità per OdV di conoscere i dati del Segnalante Riservato.</p> <p>Aggiunta l'Appendice sul CoSO Report sulla "Gestione del rischio aziendale" 2017.</p>
6f (Apr 2019)	<p>Gestione Privacy nelle segnalazioni.</p> <p>Aggiunta in "Privacy – Inventari" la gestione dei Dispositivi Mobili.</p> <p>Aggiunta la gestione del Registro dei Trattamenti semplificato per PMI.</p> <p>Aggiunta la possibilità per l'Amministratore di configurare la Gestione dei Macchinari e le Segnalazioni.</p>
6g (Ago 2019)	<p>PRIVACY: Aggiunta la gestione del Registro dei Trattamenti semplificato per PMI.</p> <p>231: Aggiunta la gestione dei Tipi Procedure e gestione delle Comunicazioni all'OdV (Informative e Divieti).</p> <p>È adesso possibile stampa la Parte Speciale relativa alle versioni precedenti.</p>
6.f (Ott 2019)	<p>Aggiunta l'Appendice relativa alle Comunicazioni.</p> <p>Aggiunta la possibilità di inviare Comunicazioni ai Fornitori per ottenere le Dichiarazioni di interesse.</p> <p>Definizione del GAP delle Procedure per selezione multipla.</p>
6.g (Dic 2019)	<p>Riorganizzata la sezione "ODV" relativa alla gestione del MOG e delle sue versioni.</p> <p>Riorganizzata la sezione relativa al supporto all'OdV ed aggiunta la possibilità di gestire le informative periodiche.</p> <p>Inserito fra i Documenti di base la Politica per la Videosorveglianza.</p> <p>Aggiunto un ulteriore Registro per i Trattamenti (intermedio).</p> <p>Migliorato il Registro dei Fornitori con l'aggiunta dell'Analisi.</p> <p>Migliorato il Registro delle Prescrizioni con l'aggiunta dei grafici.</p>

	<p>Aggiunte stampe per Responsabili (Mansionario) per le Prescrizioni e le checklist dell'Asseverazione.</p> <p>Inserita, fra le Caratteristiche Generali, la presentazione dei Cruscotti con le nuove funzionalità di personalizzazione.</p> <p>Gestione dei Siti aziendali.</p>
6.h (Gen 2020)	<p>Istruzione per il recepimento dell'Aggiornamento 2020 delle Linee Guida ANCE.</p> <p>Aggiunta (SG/Varie/Importazioni) l'importazione dei Giudizi sulla Soddisfazione delle Parti Interessate.</p> <p>È possibile visualizzare i LOG aziendali (VARIE/Amministratore Sistema) anche al fine di verificare accessi non autorizzati.</p>
6.i (Apr 2020)	<p>Aggiunte misure di sicurezza sulle Password.</p> <p>Eliminata Appendice su Segnalazioni (le informazioni sono disponibili fra i Documenti di Supporto).</p> <p>Gestione dinamica del Codice Etico.</p>
6.l (Giu 2020)	<p>Documenti di Supporto per Emergenza COVID-19.</p> <p>Prescrizioni specifiche per COVID-19 (SG/Funzionalità Varie/Varie).</p> <p>Integrazione della Prassi di Riferimento UNI/PdR 83:2020 su SGSSL. (Vedi Documento di supporto relativo).</p>
7.a (Ago 2020)	Analisi dei Rischi aziendali in base al dettaglio degli Illeciti e dei Reati presupposto.