




**ISTITUTO
ITALIANO DI
TECNOLOGIA**


Procedura per la Gestione degli Incidenti di Sicurezza ICT e Log
--

Revisione	Descrizione Modifica	Autore	Approvazione	Data
01	Prima versione	ICTD	S.D. D.G.	04/11/2020


 ISTITUTO ITALIANO DI TECNOLOGIA	Procedura per la Gestione degli Incidenti di Sicurezza ICT	IO IT 07
--	---	-----------------

SOMMARIO

1	Obiettivi e finalità	4
2	Premessa e definizioni	4
3	Premessa	4
3.1	Definizioni	4
4	Principali attori e responsabilità	5
5	Documenti e strumenti	6
6	Gestione degli Eventi di Sicurezza	8
6.1	Generazione e raccolta degli Eventi di Sicurezza	8
6.2	Triage	8
6.3	Analisi degli Eventi di Sicurezza e generazione di alert	9
7	Gestione degli Incidenti di Sicurezza	9
7.1	Raccolta e registrazione delle segnalazioni	9
7.2	Validazione delle segnalazioni	10
a.	attuazione delle misure urgenti non procrastinabili	11
b.	possono essere coinvolti dati personali	11
c.	sono possibili ripercussioni amministrative o penali	11
7.3	Analisi e diagnosi	12
7.4	Contenimento e risoluzione	13
7.5	Ripristino e chiusura	14
7.6	Lesson learned	14
8	Comunicazione degli Incidenti di Sicurezza all'Organismo di Vigilanza	14
9	Coinvolgimento delle Terze Parti	15
10	Comunicazioni esterne	15
11	Requisiti per la generazione, la raccolta e il monitoraggio degli Eventi di Sicurezza	15
11.1	Gestione dei requisiti ed impostazione iniziale	16
11.2	Insiemi minimi di Eventi di Sicurezza	16
11.3	Timestamp	17
11.4	Formato dei log degli Eventi di Sicurezza	17
11.5	Libreria dei log degli Eventi di Sicurezza	17
11.6	Protezione del sottosistema di log	17

 ISTITUTO ITALIANO DI TECNOLOGIA	Procedura per la Gestione degli Incidenti di Sicurezza ICT	IO IT 07
--	---	-----------------

11.7	Raccolta dei log degli Eventi di Sicurezza	18
11.8	Tempi di conservazione dei log degli Eventi di Sicurezza	18
11.9	Gestione del pregresso.....	18
12	Matrice RACI.....	19
13	Flusso.....	20
14	Appendice A: valutazione economica dell'Incidente di Sicurezza.....	21

 ISTITUTO ITALIANO DI TECNOLOGIA	Procedura per la Gestione degli Incidenti di Sicurezza ICT	IO IT 07
--	---	-----------------

1 Obiettivi e finalità

- Oggetto della presente Procedura sono gli eventi e incidenti che interessino i sistemi ICT della Fondazione IIT (di seguito, anche "Fondazione" o "IIT"), e in particolare:
 - la generazione, raccolta e analisi di eventi di sicurezza ICT;
 - la gestione degli incidenti ICT, con particolare attenzione agli incidenti di Sicurezza ICT, comprensiva di una procedura di escalation per la segnalazione all'autorità giudiziaria e/o alla polizia postale di attività illecite o presunte tali;
 - la gestione dei log (generazione, registrazione, conservazione, gestione, estrazione ed analisi).
- Destinatario della presente Procedura è la Direzione ICT e tutti i referenti ICT che gestiscono sistemi informatici della Fondazione.
- Destinatari della presente Procedura sono anche tutte le terze parti, quali fornitori ed enti di ricerca, che gestiscono informazioni della Fondazione IIT tramite sistemi e dotazioni informatiche e di telecomunicazione. Le suddette categorie di soggetti saranno di seguito denominate anche "Terze Parti".

Nelle seguenti disposizioni si farà anche riferimento alla Procedura di Gestione del Data Breach già adottata dalla Fondazione, nonché ai protocolli operativi derivanti dagli accordi tempo per tempo vigenti con il GARR e con il Compartimento Polizia Postale della Polizia di Stato.

2 Premessa e definizioni


3 Premessa

La Fondazione adotta strumenti, processi e procedure utili al fine di garantire la sicurezza delle informazioni e incoraggiare la responsabilizzazione dei singoli Utenti.

I Sistemi Informatici messi a disposizione degli Utenti dalla Fondazione costituiscono uno dei punti di forza di quest'ultima, ma, allo stesso tempo, possono essere fonte di rischio per la sicurezza delle informazioni trattate, compresi i dati personali, e per l'immagine della Fondazione. Per questo motivo, è necessario individuare e contenere tempestivamente eventuali incidenti di sicurezza.

3.1 Definizioni


Nome	Sigla	Descrizione
Utente	UT	Chiunque abbia un rapporto di lavoro dipendente, di collaborazione e il personale esterno affiliato alla Fondazione IIT che svolge attività di ricerca scientifica, professionale o di studio all'interno delle strutture di IIT.

 ISTITUTO ITALIANO DI TECNOLOGIA	Procedura per la Gestione degli Incidenti di Sicurezza ICT	IO IT 07
--	---	-----------------

Nome	Sigla	Descrizione
Sistema Informatico	S.I.	I sistemi e le dotazioni informatiche e di telecomunicazione di proprietà o nella disponibilità della Fondazione IIT.
Evento di Sicurezza		Un evento o un'informazione utile alla rilevazione di un Incidente di Sicurezza
Incidente di Sicurezza		Un evento che comprometta o possa compromettere riservatezza, integrità o disponibilità del sistema informatico e/o delle informazioni trattate, e/o che rappresenti una violazione delle politiche di sicurezza definite dalla Fondazione.
Rete di Telecomunicazione	R.T.	Insieme di dispositivi e dei loro collegamenti (fisici o logici) che consentono la trasmissione e la ricezione di informazioni di qualsiasi tipo tra due o più utenti situati in posizioni geograficamente distinte, effettuandone il trasferimento attraverso cavi, sistemi radio o altri sistemi elettromagnetici o ottici.
Dati Personali	D.P.	Qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.
Riservatezza		L'informazione non è resa disponibile o comunicata a individui, entità o processi non autorizzati
Integrità		Tutela dell'accuratezza e della completezza delle informazioni
Disponibilità		L'informazione deve essere accessibile ed utilizzabile dietro richiesta di un'entità autorizzata
Autenticità		L'integrità dell'informazione può essere verificata
Non ripudiabilità		L'origine e la consistenza delle informazioni sono dimostrate e certificate
Riservatezza, Integrità e Disponibilità	RID	Caratteristiche di sicurezza a protezione delle informazioni e dei S.I.
Rischio		Eventualità di subire un danno connessa a circostanze più o meno prevedibili.
SIEM	SIEM	Sistema di Security Information and Event Management; strumenti per la gestione e analisi degli eventi di sicurezza
Sistema di Trouble Ticketing	TT	Sistema utilizzato dalla Direzione ICT per la gestione delle richieste
Referente ICT		Figura tecnica che ha in carico la gestione di sistemi ICT non gestiti direttamente dalla Direzione ICT.

4 Principali attori e responsabilità


Attore	Sigla	Maggiori responsabilità
Direzione ICT	ICT	Analisi e raccolta dei log centralizzati e degli eventi di sicurezza dei sistemi nel perimetro di competenza. Raccolta e registrazione degli Incidenti di Sicurezza. Valutazione ed applicazione di azioni immediate, analisi e diagnosi degli Incidenti di Sicurezza. Applicazione di azioni di contenimento/risoluzione, ripristino dei sistemi.

 ISTITUTO ITALIANO DI TECNOLOGIA	Procedura per la Gestione degli Incidenti di Sicurezza ICT	IO IT 07
--	---	-----------------


Attore	Sigla	Maggiori responsabilità
Utente	UT	Supportare e agevolare la Direzione ICT e i Referenti ICT durante tutte le fasi del processo di gestione e risoluzione degli Incidenti di Sicurezza.
Direttore ICT	Direttore ICT	Valutare ed eventualmente approvare la segnalazione ad enti esterni alla Fondazione di Incidenti di Sicurezza. Valutare ed approvare azioni immediate per specifiche categorie di Incidenti di Sicurezza particolarmente gravi.
Principal Investigator	P.I.	Supportare e agevolare la direzione ICT e i Referenti ICT durante tutte le fasi del processo di gestione e risoluzione degli Incidenti di Sicurezza. Supportare il Direttore ICT nella valutazione degli Incidenti di Sicurezza gravi.
Referente ICT		Analisi e raccolta dei log e degli eventi di sicurezza. Insieme alla Direzione ICT valutazione ed applicazione di opportune azioni correttive.
Incaricato		Soggetto individuato dalla Direzione ICT a cui viene assegnata la gestione dell'Incidente di Sicurezza

5 Documenti e strumenti

Tipo	Nome	Utilizzo	Link
Policy	Policy ICT	Stabilisce il corretto utilizzo dei Sistemi Informatici nella Fondazione IIT (di seguito, anche "Fondazione" o "IIT"). proteggendo IIT e gli Utenti dal rischio di compromissione dei Sistemi Informatici, dalla indebita divulgazione di dati personali e riservati, e dalle relative conseguenze legali, rendendo inoltre più efficace l'utilizzo dei Sistemi Informatici	https://short.iit.it/ictpolicy
Policy	Policy per la Sicurezza delle Informazioni	Stabilisce la politica per la sicurezza delle informazioni all'interno della Fondazione IIT.	https://short.iit.it/information-security-policy
Procedura	Esempi di classificazione dei rischi delle Informazioni	Riporta esempi di valutazione dei rischi di sicurezza per le informazioni.	https://short.iit.it/risk-classification
Procedura	Misure per la sicurezza delle informazioni	Riporta l'elenco delle misure di sicurezza da implementare sulla base della classificazione del livello di rischio della sicurezza delle informazioni dei sistemi ICT della Fondazione.	https://short.iit.it/information-security-measures
Procedura	Sistemi ICT approvati per livello di rischio di sicurezza delle informazioni	Riporta un elenco di sistemi ICT della Fondazione ed il livello di rischio della sicurezza delle informazioni per il quale ne è approvato l'uso.	https://short.iit.it/approved-services

 ISTITUTO ITALIANO DI TECNOLOGIA	Procedura per la Gestione degli Incidenti di Sicurezza ICT	IO IT 07
--	---	-----------------

Tipo	Nome	Utilizzo	Link
Procedura	Procedura Data Breach	Definisce le modalità di gestione dei data Breach secondo la vigente normativa in materia di data protection	https://short.iit.it/data-breach

 ISTITUTO ITALIANO DI TECNOLOGIA	Procedura per la Gestione degli Incidenti di Sicurezza ICT	IO IT 07
--	---	-----------------

6 Gestione degli Eventi di Sicurezza

6.1 Generazione e raccolta degli Eventi di Sicurezza

Gli Eventi di Sicurezza sono generati dai diversi componenti del sistema informativo della Fondazione: apparati di sicurezza (firewall, antivirus, ecc.), sistemi operativi, apparati di rete, applicazioni, strumenti di monitoraggio e gestione del sistema informativo, dispositivi personali ecc.

L'insieme minimo e le caratteristiche degli Eventi di Sicurezza che devono essere generate dai componenti del sistema informativo sono descritti in sezione 11. Tali Eventi di Sicurezza saranno gestiti attraverso i sottosistemi di log dei diversi componenti.

Laddove possibile, la generazione di Eventi di Sicurezza deve tenere conto di logiche di correlazione (ad es. numero elevato di login falliti, login da più postazioni contemporaneamente, ecc.).

Gli Eventi di Sicurezza sono raccolti almeno nelle seguenti modalità:

- attraverso sistemi centralizzati di gestione dei log della Fondazione o di Terze Parti, quando disponibili
- localmente sul sistema che li genera, quando non sia disponibile un sistema di raccolta centralizzato; in questo caso, il sistema deve essere configurato in modo da minimizzare la possibilità di manomissione, danneggiamento o cancellazione dei log di sicurezza, anche attraverso un'opportuna configurazione degli accessi al sottosistema di log.

È responsabilità della figura tecnica che ha in carico il componente (Direzione ICT o Referente ICT) assicurare che la generazione e raccolta degli Eventi di Sicurezza sia coerente con le indicazioni in sezione 11.


6.2 Triage

Laddove il numero di Eventi di Sicurezza sia rilevante, è opportuno adottare un sistema di triage che classifichi gli Eventi di Sicurezza per potenziale criticità ed evidenzii quelli la cui analisi è prioritaria.

La prioritizzazione degli Eventi di Sicurezza deve considerare come minimo i seguenti elementi, se disponibili:

- la criticità del componente o dei componenti interessati
- la classificazione delle informazioni trattate nell'ambito dei flussi interessati, con particolare riguardo ai dati personali
- la criticità dell'evento in sé, come eventualmente classificato dal componente che ha generato l'evento

Gli Eventi di Sicurezza devono quindi essere analizzati secondo la priorità definita. In particolare, eventi ad alta priorità devono generare un alert, dove il componente o il sistema centralizzato lo consentano, in modo da permetterne l'analisi quanto più possibile immediata.

 ISTITUTO ITALIANO DI TECNOLOGIA	Procedura per la Gestione degli Incidenti di Sicurezza ICT	IO IT 07
--	---	-----------------

6.3 Analisi degli Eventi di Sicurezza e generazione di alert

Gli Eventi di Sicurezza raccolti devono essere analizzati da parte del Referente ICT o, quando centralizzati o riferiti a componenti in carico alla Direzione ICT, da parte della Direzione ICT stessa, attraverso personale specificamente incaricato. L'analisi può avvenire:

- attraverso strumenti automatizzati quali:
 - o sistemi SIEM, quando disponibili per gli eventi raccolti in modo centralizzato
 - o strumenti automatici, locali o centralizzati, per la selezione ed evidenziazione degli Eventi di Sicurezza e la generazione di allarmi, inclusi eventuali script
- manualmente, se non siano disponibili o adeguati altri strumenti, almeno una volta al giorno

L'analisi deve evidenziare eventuali Eventi di Sicurezza che possano suggerire un Incidente di Sicurezza. A questo scopo, gli strumenti automatici dovranno generare allarmi per una tempestiva analisi più approfondita.

L'esito dell'analisi, che non potrà durare più di 72 ore, deve portare a classificare gli Eventi di Sicurezza come:

- Incidenti di Sicurezza
 - o che possono coinvolgere dati personali
 - o che non coinvolgono dati personali
- altri Eventi di Sicurezza

In caso di Incidenti di Sicurezza, la persona che ha effettuato l'analisi provvederà immediatamente ad aprire un ticket sul sistema di TT, provvedendo ad una prima classificazione dell'evento sulla base:

- delle casistiche sopra indicate
- del rischio (alto, medio, basso) associato agli asset interessati dall'incidente corredando il ticket delle informazioni raccolte e degli esiti delle analisi effettuate, che dovranno comprendere anche un'estrazione dell'evento o degli Eventi di Sicurezza rilevanti, corredata da timestamp.

Per il dettaglio si vedano i paragrafi successivi da 7 a 10.

.

7 Gestione degli Incidenti di Sicurezza

7.1 Raccolta e registrazione delle segnalazioni

Gli Incidenti di Sicurezza possono essere segnalati da diverse fonti:

- generazione di ticket su TT in seguito all'analisi di Eventi di Sicurezza
- riclassificazione di incidenti, riconosciuti come Incidenti di Sicurezza
- chiamate al Service Desk

- segnalazioni da parte del GARR, nell'ambito della convenzione fra i due Enti e attraverso i canali concordati
- segnalazioni da parte della Polizia Postale, nell'ambito della convenzione fra i due Enti e attraverso i canali concordati
- Altro (email al Direttore ICT, email all'indirizzo cyber.security@iit.it)
- La persona che riceve la segnalazione deve provvedere immediatamente ad aprire un ticket su TT classificato come Incidente di Sicurezza, o a riclassificare il ticket esistente. Il ticket deve comprendere le informazioni raccolte e una cronologia degli Eventi di Sicurezza rilevanti, con una indicazione dei tempi quanto più corretta possibile, compreso il primo momento di segnalazione. Tale cronologia dovrà essere mantenuta aggiornata nel corso della gestione dell'Incidente di Sicurezza, registrando gli Eventi di Sicurezza rilevanti, i dati e le estrazioni utili ai fini di eventuali indagini e procedimenti che la Fondazione intendesse avviare.

Qualora la persona che riceve la segnalazione non abbia la possibilità di aprire un ticket, ad esempio perché non autorizzato, dovrà provvedere a segnalare immediatamente l'Incidente di Sicurezza al Service Desk ICT, che provvederà ad aprire il ticket, o ad altro soggetto specificamente indicato come referente nell'ambito del rapporto di collaborazione con la Fondazione.

Il ticket dovrà essere quindi assegnato da parte della Direzione ICT ad uno specifico Incaricato, secondo le prassi e procedure definite per la gestione dei ticket.

7.2 Validazione delle segnalazioni


L'Incaricato dovrà innanzitutto provvedere a validare le informazioni fornite nell'ambito della segnalazione, al fine di accertare:

- se si tratti di un falso positivo o di un Incidente di Sicurezza
- se possano essere interessati dei dati personali
- se, in prima analisi, l'incidente possa essere generato da personale o collaboratori della Fondazione o da soggetto esterno.

Nel corso di tale validazione, qualora risultasse necessario contattare soggetti al di fuori di quelli che hanno effettuato la segnalazione o al di fuori della Direzione ICT, l'Incaricato dovrà prima informare il Direttore ICT e ottenerne l'approvazione, al fine di non diffondere impropriamente informazioni sull'esistenza e la natura dell'incidente.

Qualora l'incidente non sia validato come Incidente di Sicurezza, si possono presentare due casi:

- l'incidente, pur non essendo di sicurezza, può essere un incidente di altro tipo; in questo caso, l'Incaricato provvede a riclassificare l'incidente, registrando tale evento nel ticket; il ticket sarà eventualmente riassegnato secondo le procedure e le prassi della Direzione ICT;
 - o l'incidente è un falso positivo; l'Incaricato provvederà a segnalare gli esiti delle verifiche al soggetto segnalante, attendendo 48 ore lavorative per eventuali comunicazioni da parte del soggetto prima di chiudere il ticket; i tempi per l'attività di validazione dovranno essere commisurati alla gravità e urgenza dell'incidente, in particolare in relazione a vincoli esterni o normativi, quali ad esempio tempistiche di intervento indicate dal GARR,

 ISTITUTO ITALIANO DI TECNOLOGIA	Procedura per la Gestione degli Incidenti di Sicurezza ICT	IO IT 07
--	---	-----------------

eventuali indicazioni o richieste da parte della Polizia Postale, o il coinvolgimento di dati personali. In caso di dubbio che comporti tempistiche di validazione non compatibili con quanto sopra descritto, l'incidente dovrà essere considerato validato.

Le azioni da mettere in atto immediatamente da parte dell'Incaricato in caso di Incidente di Sicurezza validato sono di seguito elencate. Tutte le azioni dovranno essere registrate all'interno del ticket, seppure in modalità sintetica quando la gestione di un'emergenza lo richieda, e con apposito timestamp.

a. attuazione delle misure urgenti non procrastinabili

Qualora l'Incidente di Sicurezza sia suscettibile di provocare danni importanti e immediati a persone o cose, l'Incaricato identifica le misure urgenti atte a mitigare tali danni, che non compromettano la validità delle fonti di prova e allo stesso tempo diano minore evidenza possibile, al di fuori della Direzione ICT, del rilevamento e della gestione dell'Incidente di Sicurezza. Tali azioni possono comprendere quanto indicato nell'ambito di una segnalazione da parte del GARR_CERT, ferma restando l'esigenza sopra indicata di non compromettere le fonti di prova. L'Incaricato potrà quindi considerare misure alternative a quelle indicate dal GARR-CERT, che ottengano effetti comparabili in termini di riduzione dell'impatto sulla rete GARR, e soddisfino maggiormente i requisiti interni della Fondazione.

b. possono essere coinvolti dati personali

L'Incaricato comunica immediatamente l'Incidente di Sicurezza alla Direzione Affari Legali all'indirizzo legaloffice@iit.it, comprendendo i dettagli dell'Incidente di Sicurezza stesso ed in particolare come minimo:

- Tipologia di malfunzionamento;
- Asset elettronico e/o cartaceo interessato;
- Numero approssimativo di soggetti interessati coinvolti;
- Natura dei dati oggetto dell'Incidente di Sicurezza


attivando così la Procedura di Gestione del Data Breach. Nel seguito, la gestione dell'Incidente di Sicurezza dovrà avvenire secondo quanto previsto da tale procedura. In caso di dubbi o discrepanze fra la procedura qui descritta e la Procedura di Gestione del Data Breach, prevale quest'ultima.

c. sono possibili ripercussioni amministrative o penali

L'Incaricato attiva immediatamente i canali per la notifica alla Polizia Postale in coerenza con il Protocollo Operativo concordato, previa autorizzazione da parte del Direttore ICT. Quest'ultimo si avvarrà del parere della Direzione Affari Legali, in particolare anche per valutare la segnalazione dell'Incidente di Sicurezza all'autorità giudiziaria. Qualora la Direzione Affari Legali valuti come opportuna tale segnalazione, la Direzione ICT fornirà alla Direzione Affari Legali le informazioni raccolte e utili alla predisposizione della segnalazione. La Direzione Affari Legali provvederà quindi ad avviare le azioni interne necessarie per effettuare la segnalazione.

L'Incaricato acquisisce quindi le eventuali indicazioni da Parte della Polizia Postale sulle modalità di gestione dell'Incidente di Sicurezza per quanto riguarda l'assicurazione delle fonti di prova; in particolare:

1. l'acquisizione e messa in sicurezza, secondo le buone pratiche di digital forensics, dei log rilevanti, anche secondo quanto concordato nel Protocollo Operativo;

 ISTITUTO ITALIANO DI TECNOLOGIA	Procedura per la Gestione degli Incidenti di Sicurezza ICT	IO IT 07
--	---	-----------------

2. laddove questo non comporti disservizi importanti per la Fondazione, l'isolamento dei sistemi interessati dall'Incidente di Sicurezza;
3. dove siano disponibili le competenze e gli strumenti per operare in modo secondo le buone pratiche di digital forensics, l'acquisizione e messa in sicurezza delle immagini delle macchine colpite e/o di altri supporti di immagazzinamento delle informazioni; laddove tali competenze non siano disponibili, o dove la Polizia Postale dia diverse indicazioni, tale acquisizione sarà demandata alla Polizia Postale stessa;
4. qualora l'isolamento dei sistemi comporti disservizi importanti per la Fondazione, l'Incaricato coinvolgerà il Direttore ICT, e quest'ultimo se del caso la Direzione Affari Legali, per valutare le diverse opzioni che consentano di limitare i danni pur senza compromettere la validità delle fonti di prova.

d. sono possibili danni rilevanti per la Fondazione

Anche quando non siano ipotizzabili impatti su dati personali, l'Incidente di Sicurezza potrebbe comunque avere conseguenze importanti per la Fondazione, ad esempio quando siano interessate informazioni relative a proprietà intellettuale. In questo caso l'Incaricato provvederà ad informare immediatamente il Direttore ICT, che valuterà se interessare la Direzione Affari Legali, il Direttore Scientifico, il Direttore Generale o altre figure o strutture pertinenti.

e. L'Incidente di Sicurezza sta causando disservizi importanti alla Fondazione

Quando l'Incidente di Sicurezza stia provocando importanti disservizi alla Fondazione o a parte dei suoi processi operativi, l'Incaricato dovrà immediatamente avvertire il Direttore ICT, affinché questi possa valutare l'opportunità e l'efficacia dell'attivazione del piano di Disaster Recovery, se sia opportuno attivare le procedure di escalation opportune per gestire le tematiche di continuità operativa della Fondazione stessa.

f. L'Incidente di Sicurezza può avere origine internamente


In questo caso, l'Incaricato provvederà ad informare immediatamente il Direttore ICT, che a sua volta coinvolgerà il Direttore Scientifico, il Direttore Generale, la Direzione Affari Legali e le altre funzioni di volta in volta coinvolte

7.3 Analisi e diagnosi

L'Incaricato procede con le attività di analisi e diagnosi, fermo restando quanto eventualmente stabilito in conseguenza delle azioni immediate, ad esempio in tema di tutela delle fonti di prova. Scopo dell'attività di analisi e diagnosi è arrivare ad individuare le caratteristiche dell'Incidente di Sicurezza, al fine di mettere in atto le misure di contenimento, risoluzione e ripristino più efficaci. Le informazioni raccolte dovranno essere tracciate all'interno del ticket.

La possibilità di coinvolgere nell'attività di analisi soggetti esterni alla Direzione ICT (ad esempio, personale della Fondazione che abbia utilizzato i sistemi e servizi interessati dall'Incidente di Sicurezza), è subordinata alle cautele già evidenziate. In particolare, l'Incaricato dovrà evitare di:

- diffondere dettagli riservati dell'Incidente di Sicurezza

 ISTITUTO ITALIANO DI TECNOLOGIA	Procedura per la Gestione degli Incidenti di Sicurezza ICT	IO IT 07
--	---	-----------------

- allertare eventuali soggetti coinvolti nella generazione dell'Incidente di Sicurezza
- diffondere notizie sull'Incidente di Sicurezza al di fuori della Fondazione, o rendere possibile ad altri di farlo, al di fuori dei canali di comunicazioni istituzionali della Fondazione

7.4 Contenimento e risoluzione

Una volta individuate le caratteristiche dell'Incidente di Sicurezza, l'Incaricato procede nelle attività di contenimento e risoluzione dell'Incidente di Sicurezza, nei limiti posti da quanto eventualmente stabilito in conseguenza delle azioni immediate, ad esempio in tema di tutela delle fonti di prova. Dovrà in particolare considerare le esigenze di riservatezza sull'Incidente di Sicurezza acclarate con i diversi soggetti interni ed esterni, agendo di conseguenza quando sia necessario contattare qualcuno nell'ambito delle attività di contenimento e risoluzione.


L'Incaricato farà riferimento alle istruzioni operative eventualmente disponibili nella knowledge base della Direzione ICT. Potrà discostarsi da tali istruzioni, informandone il Direttore ICT, laddove le sue competenze individuino delle aree di miglioramento o esigenze specifiche non completamente coperte dalle istruzioni stesse.

L'Incaricato dovrà tracciare nel ticket le attività svolte, comprese le variazioni rispetto alle istruzioni operative e le ragioni di tali variazioni.

L'attività dovrà focalizzarsi in generale prima di tutto sul contenimento degli impatti, immediati e potenziali, causati dalla minaccia. In second'ordine dovrà operare per eradicare la minaccia. L'Incidente di Sicurezza si considera risolto quando le cause correnti sono state rimosse ed è possibile procedere con le attività di ripristino. Per la risoluzione non è necessario individuare il soggetto che ha originato l'Incidente di Sicurezza, né essere in grado di impedire il ripetersi dell'Incidente di Sicurezza stesso. Questi aspetti potranno essere oggetto di indagini successive e potranno eventualmente generare ulteriori e separate azioni quali ad esempio interventi sul codice degli applicativi per la correzione di vulnerabilità, modifiche architetturali ecc.

Per la chiusura di un Incidente di Sicurezza, con l'esclusione di quelli gestiti in piena conformità con le istruzioni operative, il Direttore ICT, con il supporto dell'Incaricato, dovrà effettuare e documentare un'analisi al fine di:

1. Valutare l'esigenza di avviare un'analisi del rischio sulle risorse informatiche interessate dall'Incidente di Sicurezza, anche al fine di identificare l'esigenza di interventi correttivi rispetto a vulnerabilità del sistema informativo o dei processi di gestione, o di evidenziare variazioni nei rischi a cui siano esposti i sistemi e le informazioni, con particolare attenzione ai dati personali. Questo comprende la valutazione dell'opportunità di avviare azioni di prevenzione anche in termini di sensibilizzazione degli utenti;
2. Svolgere eventuali ulteriori attività di indagine, in coordinamento con la Direzione Affari Legali ed eventualmente la Polizia Postale
3. Effettuare una stima economica del danno effettivamente causato dall'Incidente di Sicurezza (si prenda in considerazione l'Appendice A: valutazione economica dell'Incidente di Sicurezza).

 ISTITUTO ITALIANO DI TECNOLOGIA	Procedura per la Gestione degli Incidenti di Sicurezza ICT	IO IT 07
--	---	-----------------

Per ogni Incidente di Sicurezza, con l'esclusione di quelli gestiti in piena conformità con le istruzioni operative, il Direttore ICT, con il supporto dell'Incaricato, dovrà inoltre predisporre un rapporto sintetico comprendente almeno:

1. data e ora dell'accadimento o della prima manifestazione dell'Incidente di Sicurezza;
2. risorse e servizi coinvolti;
3. cause, tempi e modalità previsti per il pieno ripristino dei livelli di disponibilità e sicurezza definiti e per il completo accertamento dei fatti connessi;
4. descrizione delle azioni intraprese e dei risultati ottenuti; a questo scopo, il sistema di supporto alla gestione degli Incidenti di Sicurezza e le procedure dovranno prevedere la registrazione con timestamp di tutti gli eventi e le attività significativi nel corso della gestione dell'Incidente di Sicurezza
5. una valutazione dei danni delle perdite economiche o danni d'immagine

Questo rapporto dovrà essere reso disponibile alla Direzione Affari Legali, al Direttore Generale, al Direttore Scientifico ed all'Organismo di Vigilanza, nonché alla Polizia Postale quando dovuto.

7.5 Ripristino e chiusura

Le attività di ripristino riportano i componenti del sistema informativo ad un livello di operatività analogo a quello precedente all'Incidente di Sicurezza, salvo eventuali variazioni che siano state stabilite nel corso della gestione dell'Incidente di Sicurezza stesso. Qualora siano necessari interventi estensivi, potranno essere aperti ticket specifici.

Fermo restando quanto già stabilito in tema di riservatezza e di tutela delle fonti di prova, per l'individuazione delle attività di ripristino più opportune, laddove utile, l'Incaricato coinvolgerà i responsabili dei sistemi, servizi o processi impattati dall'Incidente di Sicurezza.


La chiusura dell'Incidente di Sicurezza coincide con la chiusura del ticket.

7.6 Lesson learned

Una volta chiuso l'Incidente di Sicurezza, l'Incaricato dovrà valutare quanto appreso nel corso dell'Incidente di Sicurezza, in particolare in riferimento alle modalità ed al processo di gestione dell'incidente stesso. Provvederà quindi ad integrare le istruzioni operative nella knowledge base della Direzione ICT, nonché a suggerire eventuali modifiche al processo di gestione Incidenti di Sicurezza. Infine, evidenzierà le possibili aree di miglioramento nella gestione complessiva del sistema informativo.

8 Comunicazione degli Incidenti di Sicurezza all'Organismo di Vigilanza

Qualora l'Incidente di Sicurezza abbia rilevanza ai fini del d.lgs. 231/01, l'Incaricato dovrà immediatamente contattare il Direttore ICT, che valuterà la gravità della situazione e contatterà senza indebito ritardo l'Organismo di Vigilanza.

 ISTITUTO ITALIANO DI TECNOLOGIA	Procedura per la Gestione degli Incidenti di Sicurezza ICT	IO IT 07
--	---	-----------------

9 Coinvolgimento delle Terze Parti

La presente procedura si applica a tutti i servizi in outsourcing, compresi quelli forniti in modalità cloud, in conformità con le procedure IIT e le condizioni di contratto sottoscritte.

Le Terze Parti possono essere coinvolte nella gestione di un Incidente di Sicurezza in diverse modalità:

- in quanto gli Incidenti di Sicurezza, interessano risorse da loro gestite; in coerenza con le condizioni di contratto, segnalano l'Incidente di Sicurezza alla Fondazione entro i tempi stabiliti; l'Incaricato opererà per assicurare:
 - il necessario supporto alle Terze Parti nelle attività di analisi, contenimento, risoluzione e ripristino;
 - che le Terze Parti forniscano efficacemente e tempestivamente le informazioni necessarie per la gestione di quanto di competenza della Fondazione, .

Rimarrà comunque responsabilità delle Terze Parti adottare le misure più adeguate, laddove trattino dati personali.

- in quanto l'Incidente di Sicurezza interessa risorse gestite dalla Fondazione o da Terze Parti, ma è necessario il supporto delle Terze Parti nella gestione dell'Incidente di Sicurezza; in questo caso, l'Incaricato che prende in carico il ticket presso la Fondazione richiederà la fattiva collaborazione delle Terze Parti, nelle modalità contrattualizzate;


Laddove le Terze Parti non risultassero collaborative, ed in particolare qualora non operasse in coerenza con quanto contrattualizzato, l'Incaricato ne informerà il Direttore ICT, che provvederà alle escalation del caso.

10 Comunicazioni esterne

Fatto salvo quanto strettamente necessario per la gestione operativa dell'Incidente di Sicurezza, e con le cautele di riservatezza e di tutela delle fonti di prova sopra discusse, è fatto divieto al personale della Direzione ICT, di comunicare all'esterno ed in particolare con organi di stampa o altri soggetti analoghi, senza specifica ed esplicita autorizzazione. Sarà compito del Direttore ICT gestire la comunicazione dell'Incidente di Sicurezza, il quale, nel caso in cui la comunicazione assuma carattere istituzionale e/o con organi di stampa o soggetti analoghi, si coordinerà con la Direzione Affari Legali e con la Direzione Comunicazione e Relazioni Esterne.

11 Requisiti per la generazione, la raccolta e il monitoraggio degli Eventi di Sicurezza

La generazione/estrazione e raccolta corrette e complete di Eventi di Sicurezza sono presupposto per l'analisi di tali eventi e per il loro utilizzo come fonte di prova. Le attività di analisi e monitoraggio devono gestire grandi quantità di eventi, identificando e comprendendo quelli che possono essere indicativi di un Incidente di Sicurezza, in tempi stretti, e con strumenti per quanto possibile automatizzati. Per questo motivo, è necessario che la generazione e la raccolta siano effettuate in modalità che facilitino la comprensione e l'analisi automatica degli eventi stessi.

 ISTITUTO ITALIANO DI TECNOLOGIA	Procedura per la Gestione degli Incidenti di Sicurezza ICT	IO IT 07
--	---	-----------------

La generazione e la raccolta di Eventi di Sicurezza avvengono in linea con le prassi e procedure di generazione dei log, salvo per quanto più specificamente indicato in questa sezione.

11.1 Gestione dei requisiti ed impostazione iniziale

In linea con le logiche di security by design & by default, nonché di personal data protection by design & by default (questi ultimi in linea con quanto richiesto dall'art. 25 del GDPR), i requisiti per la generazione/estrazione e la raccolta degli Eventi di Sicurezza devono essere definiti in fase di raccolta dei requisiti, integrandoli e dettagliandoli in fase di progettazione, per tutte le nuove iniziative ICT che comportino lo sviluppo o evoluzioni significative di componenti ICT o dell'architettura del sistema informativo. Le specificità degli Eventi di Sicurezza da raccogliere e l'implementazione dei requisiti devono essere documentate per l'intero ciclo di vita del software e dei sistemi, e devono comprendere sempre almeno quanto sotto indicato.

In fase di progettazione deve anche essere stimato il volume di Eventi di Sicurezza generati a regime ed in condizioni di massimo carico (ad esempio, nel corso di un attacco), in modo da prevedere un adeguato dimensionamento del sottosistema di log. Tale dimensionamento, nonché l'utilizzo di buffer locali in caso di centralizzazione dei log, deve permettere di non perdere Eventi di Sicurezza anche in caso di massimo carico. È opportuno, dove possibile, prevedere la generazione di alert in caso di generazione di Eventi di Sicurezza con una frequenza al di sopra di una soglia di attenzione.

11.2 Insiemi minimi di Eventi di Sicurezza


Per ogni classe di componenti del sistema informativo, deve essere raccolto un insieme minimo di Eventi di Sicurezza. In particolare, devono essere raccolti almeno:

- le operazioni di login e, dove presenti, di logout, nonché i login falliti; particolare attenzione deve essere posta alla raccolta degli eventi legati agli accessi degli amministratori di sistema
- le operazioni di (ri)configurazione dei sistemi di sicurezza, quali ad esempio la creazione di nuove utenze, le modifiche ai permessi di accesso agli applicativi, la modifica di file di configurazione rilevanti per la sicurezza dei componenti del sistema informativo

Dove gli strumenti e le risorse lo consentano, devono essere raccolti anche:

- le attività riconoscibili come potenziali attacchi, quali ad esempio messaggi non coerenti con quelli legittimamente generati dai componenti del sistema informativo (es. fallimenti nella validazione dell'input ad un servizio, che non possano derivare dall'utilizzo corretto del corrispondente client)
- gli accessi da indirizzi IP anomali
- in generale, gli eventi che in fase di progettazione e analisi siano riconosciuti come rilevanti dal punto di vista della sicurezza.

Per quanto riguarda gli apparati di sicurezza (firewall, IDS ecc.), dovranno essere configurati per tracciare almeno gli eventi sopra indicati, nonché le violazioni delle specifiche regole definite quando riconducibili a indirizzi della Fondazione.

 ISTITUTO ITALIANO DI TECNOLOGIA	Procedura per la Gestione degli Incidenti di Sicurezza ICT	IO IT 07
--	---	-----------------

11.3 Timestamp

Tutti gli Eventi di Sicurezza devono riportare un timestamp corretto. A questo scopo, tutti i sistemi che possano generare Eventi di Sicurezza dovranno essere sincronizzati con un unico riferimento temporale accurato (es. sistema di timeserver NTP).

11.4 Formato dei log degli Eventi di Sicurezza

I log di sicurezza devono essere generati/estratti per quanto possibile in formati standard, e comunque in formati documentati. È preferibile l'adozione di un formato uniforme per l'intero sistema informativo, e comunque per gli applicativi e in generale i componenti sviluppati da o per conto della Fondazione. Il formato deve prevedere una chiara delimitazione dei campi, e la presenza e il posizionamento quanto più standardizzati possibile dei campi all'interno del record. Sono infine da prediligere i formati riconosciuti dagli strumenti di analisi centralizzata eventualmente adottati dalla Fondazione.

Il log relativi agli Eventi di Sicurezza devono essere ben riconoscibili dagli altri, ad esempio perché marcati specificamente o perché registrati in sottosistemi separati (es. file o tabelle separati).

I log devono comprendere almeno, dove possibile:

- il timestamp relativo al momento di generazione del log
- gli indirizzi associabili all'evento (es. indirizzo IP dal quale è effettuata l'autenticazione)
- un codice numerico univoco del tipo di evento
- le eventuali utenze a cui sia riconducibile l'evento
- un messaggio identificativo dell'evento, che permetta di comprendere l'esito delle attività oggetto di tracciamento, quali ad esempio accessi in lettura anche legittimi, ma ad informazioni di particolare criticità, o l'effettuazione di estrazioni o copie di dati particolarmente riservati.

11.5 Libreria dei log degli Eventi di Sicurezza


L'insieme dei possibili Eventi di Sicurezza generati/estratti dai diversi componenti deve essere per quanto possibile documentato, insieme ad una spiegazione esauriente, per un tecnico della Direzione ICT, sulle condizioni che portano alla loro generazione e sul loro significato. In particolare, la documentazione deve essere completa per i componenti sviluppati da o per la Fondazione.

11.6 Protezione del sottosistema di log

I log dei diversi componenti devono essere accessibili in modifica solo agli amministratori di sistema per i quali l'accesso sia strettamente necessario, tracciando dove possibile come Eventi di Sicurezza tutti gli accessi in scrittura a tale sottosistema. L'accesso in lettura deve essere consentito agli amministratori che abbiano necessità di esaminare i log, ad esempio nelle attività di gestione del componente. Tale accesso non deve comportare necessariamente l'accesso in scrittura/modifica.

In generale, la configurazione di sicurezza del sottosistema di log deve seguire le buone pratiche di settore e quelle specificamente indicate dal produttore.

Allo stesso modo deve essere protetto e configurato il sottosistema di gestione dell'orologio di sistema.

 ISTITUTO ITALIANO DI TECNOLOGIA	Procedura per la Gestione degli Incidenti di Sicurezza ICT	IO IT 07
--	---	-----------------

11.7 Raccolta dei log degli Eventi di Sicurezza

I log raccolti/estratti centralmente, dove tecnicamente possibile, devono essere trasmessi attraverso canali cifrati, utilizzando standard di mercato (es. TLS). I meccanismi adottati devono assicurare che gli Eventi di Sicurezza non vengano persi o modificati in nessuna fase della raccolta e memorizzazione, eventualmente integrandosi con componenti locali delle macchine e agenti che contribuiscano a tale obiettivo. La memorizzazione locale degli Eventi di Sicurezza deve comprendere strumenti di rilevazione delle modifiche (es. checksum crittografiche). L'accesso in qualità di amministratore ai sistemi di log centralizzati deve essere ridotto a pochi amministratori di sistema di massima fiducia. In nessun modo deve essere prevista la modifica dei log, se non per la cancellazione al termine del periodo di conservazione.

11.8 Tempi di conservazione dei log degli Eventi di Sicurezza


I tempi di conservazione dei log devono rispettare i seguenti requisiti:

- per i log che contengano dati personali, i tempi di conservazione sono quelli specificati nel registro dei trattamenti; più in particolare, per i log relativi agli accessi degli amministratori di sistema il tempo di conservazione è di sei mesi.
- per gli ulteriori log di Eventi di Sicurezza, ove possibile, il tempo di conservazione è di almeno sei mesi.

Al termine del periodo di conservazione, i log devono essere definitivamente cancellati. Qualora i log siano necessari per un tempo maggiore nell'ambito di indagini o procedimenti in corso, i log necessari dovranno essere estratti e conservati quali fonti di prova, secondo le buone pratiche di digital forensics e in conformità alla normativa vigente.

11.9 Gestione del pregresso

Per i sottosistemi già in essere che non soddisfino i requisiti sopra indicati, deve essere effettuato un assessment, partendo da quelli più critici per la Fondazione, per valutare le modalità disponibili e l'onerosità delle attività di adeguamento, e pianificare quindi gli interventi. L'adeguamento alle indicazioni del Provvedimento amministratori di sistema e ai tempi di conservazione previsti nel registro dei trattamenti, quando i sottosistemi non siano già adeguati, è comunque prioritario.

 ISTITUTO ITALIANO DI TECNOLOGIA	Procedura per la Gestione degli Incidenti di Sicurezza ICT	IO IT 07
--	---	-----------------

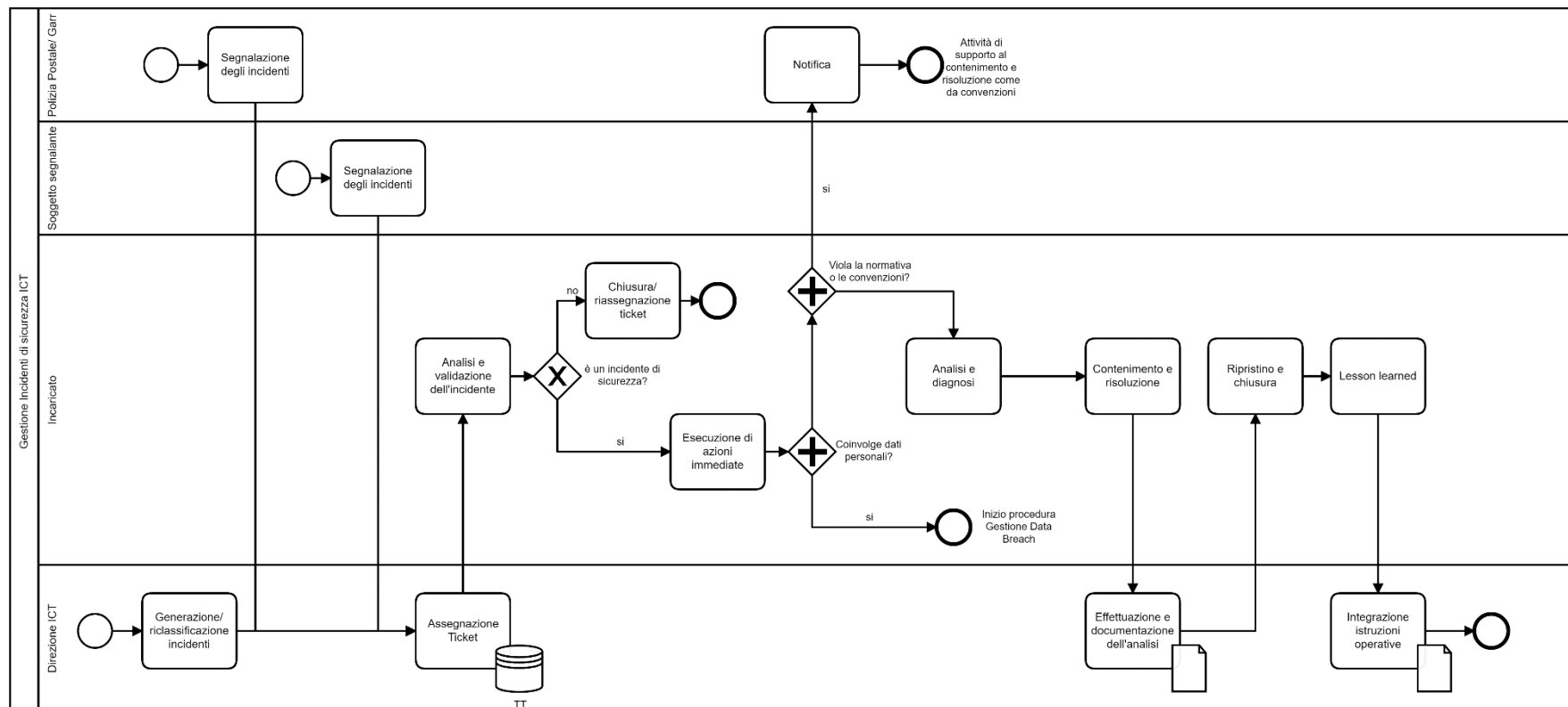
12 Matrice RACI

<div>Fasi</div> <div>Ruolo</div>	Direzione ICT	Soggetto segnalante	Incaricato	Terze Parti	Direzione Affari Legali	GARR / Polizia Postale	Direzione Comunicazioni e	Direttore Generale e Direttore Scientifico
1) Segnalazione degli Incidenti di Sicurezza	A	R	I/R	R		R		
2) Analisi e validazione dell'Incidente di Sicurezza	A		R	C		C/I		
3) Esecuzione di azioni immediate	A		R	R/C	C/I	C/I		C/I
4) Analisi e diagnosi	A		R	C		C/I		
5) Contenimento e risoluzione	A		R	R/C		R/C		
6) Ripristino e chiusura	A	I	R	R/C		C/I		
7) Lezioni apprese	A		R	C/I		C/I		
8) comunicazioni esterne	A/R				C/I		C/I	C/I

Legenda:

- A (Accountable) = colui che approva il lavoro completato e ne è pienamente responsabile (dovrebbe esservi un solo Accountable per ogni attività);
- R (Responsible) = colui che lavora al pacchetto di lavoro, possono essere più di uno nel caso di lavoro in team;
- C (Consulted) = chi possiede le informazioni o le capacità per svolgere il lavoro e deve essere interpellato dai responsabili dell'attività (tipicamente una comunicazione bidirezionale);
- I (Informed) = colui che deve essere informato dello stato di avanzamento e dei risultati (tipicamente una comunicazione monodirezionale)

13 Flusso



14 Appendice A: valutazione economica dell'Incidente di Sicurezza

La valutazione economica dell'Incidente di Sicurezza tiene conto dei costi che l'Ente deve sostenere in conseguenza dell'Incidente di Sicurezza. Questa valutazione aiuta ad effettuare un'adeguata valutazione del rischio di ulteriori occorrenze dello stesso incidente o di incidenti simili, nonché a valutare l'opportunità di investimenti in misure di difesa. Può inoltre essere utile o necessaria per la gestione di polizze assicurative o in caso di procedimenti che possano comportare un risarcimento.

La valutazione economica dovrebbe tenere conto almeno delle seguenti voci, dove rilevanti:

Voce di costo	Responsabilità della stima
tempo speso dal personale della Fondazione, e in particolare della Direzione ICT, nella gestione dell'Incidente di Sicurezza	Direttore ICT e Responsabili delle Direzioni direttamente coinvolte
disservizi a processi operativi della Fondazione, ad esempio in conseguenza del fermo di sistemi o servizi, e quindi anche del personale coinvolto nei processi stessi; in alcuni casi, le attività di ripristino potrebbero comportare	Responsabili dei processi operativi impattati
Costi per l'acquisizione di prodotti o servizi nell'ambito della gestione dell'Incidente di Sicurezza (es. consulenze per attività di forensics, consulenze legali ecc.)	Direttore ICT e Responsabili delle Direzioni direttamente coinvolte
Costi diretti, ad esempio in caso di frodi, sottrazione di proprietà intellettuale	Direttore Amministrativo e Responsabili delle Direzioni direttamente coinvolte
Costi (stimati) per risarcimenti	Direttore Amministrativo e Direttore affari legali
Costi (stimati) per sanzioni	Direttore Amministrativo e Direttore affari legali
Danno di immagine (stimato)	Direttore Scientifico, Direttore Amministrativo e Direttore affari legali