**Cesare Gallotti**

**Sicurezza delle informazioni**

**CAPITOLO 1**

**Introduzione**

Da sempre l’uomo sente la necessità di avere le proprie informazioni al sicuro e di rendere i dati personali accessibili solo a poche persone fidate.

La sicurezza però non può essere assoluta e incontrovertibile nella realtà, è impossibile, anche Fort Knox, conosciuto come uno dei luoghi più sicuri al mondo, è vulnerabile ad un meteorite.

Bisogna individuare un livello adeguato di sicurezza che si vuole ottenere attraverso la valutazione del rischio, raggiungerlo attraverso opportune azioni di trattamento e, se il livello non può essere raggiunto, bisogna analizzare ed accettare le carenze.

Le valutazioni devono essere ripetute nel tempo per verificare che siano ancora valide e si possono usare controlli di sicurezza, cioè misure utili per garantire la sicurezza delle informazioni.

La sicurezza delle informazioni è sempre stata rilevante nella storia, prima si riferiva a documenti cartacei come messaggi di guerra da mantenere segreti o la contabilità in partita doppia da mantenere integra.

Negli anni 90 si verificarono fenomeni importanti relativamente all’informatica ed al contesto economico e sociale:

* Diffusione degli strumenti informatici grazie ai PC
* Aumento di persone e dispositivi connessi ad internet.
* Aumento delle minacce informatiche note al grande pubblico come il virus di Morris
* La pubblicazione di normative con riferimento alla sicurezza informatica
* L’aumento della conflittualità sociale dovuto alle ristrutturazioni di imprese

Negli anni 90 cambia anche l’approccio alla sicurezza delle organizzazioni: si specializzano gli ambiti di intervento, si stabiliscono le priorità e si percepisce la sicurezza come attività indispensabile per garantire la sostenibilità, per questi motivi vennero introdotte metodologie e pratiche per rendere più strutturate le attività riguardanti la sicurezza delle informazioni.

Negli anni 2000 molti paesi presero consapevolezza dell’importanza della protezione delle reti informatiche e di Internet e furono considerati come “sempre più importanti” i diritti dei cittadini in ambito digitale (GDPR e New Deal for Consumers dell’UE), queste normative chiedevano di valutare il rischio di sicurezza e aumentare la sicurezza delle informazioni e degli oneri burocratici per molte organizzazioni.

Negli stessi anni abbiamo avuto anche lo sviluppo di IoT, Operational technology e domotica diffondendo i dispositivi smart ovunque, i potenziali impatti diventano riguardanti non solo la sicurezza delle informazioni, ma anche quella fisica e della salute.

**CAPITOLO 2**

**Sicurezza delle informazioni e organizzazione**

ISO/IEC 27000:

**Informazione (Information data):** conoscenza o insieme di dati che hanno valore per un individuo o un’organizzazione*.*

Le informazioni sono archiviate e trasmesse su supporti analogici (carta, foto, pellicola, uomo…) o digitali (computer e memorie removibili).

Per la trasmissione si possono usare: posta tradizionale, telefono, reti informatiche e

conversazioni tra persone.

Quando si parla di sicurezza delle informazioni non ci si limita a quella digitale ma a tutti i sistemi utilizzati per raccogliere, modificare, conservare, trasmettere e distruggere informazioni.

La sicurezza delle informazioni include le quattro rappresentazioni di conoscenza:

1. Dati: singoli fatti, immagini e impressioni
2. Informazioni: dati organizzati e significativi
3. Conoscenza: informazioni recepite e comprese
4. Sapienza: conoscenze tra loro connesse che permettono di prendere decisioni.

ISO/IEC 27000:

**Sicurezza delle informazioni**: preservazione della riservatezza, integrità e disponibilità delle informazioni.

Proprietà RID/CIA:

* **Riservatezza** (Confidentiality): proprietà di un’informazione di non essere disponibile o rivelata a individui, entità o processi non autorizzati;

Il livello di riservatezza può variare nel tempo (es: Freedom information act).

* **Integrità** (Integrity): proprietà di accuratezza e completezza, comprende la “cancellazione di informazioni” che è un’alterazione estrema.
* **Disponibilità** (Availability): proprietà di essere accessibile e utilizzabile [entro i tempi previsti] su richiesta di un’entità autorizzata. Es: utilizzo di back-up.

Altre proprietà:

* **Autenticità**: informazioni che attestano la verità. 🡪integrità
* **Completezza**: informazioni che non hanno carenze (cancellazioni totali o parziali non autorizzate). 🡪integrità.
* **Non ripudio**: le informazioni corrette non devono poter essere smentite dall’autore. Es: documenti firmati.
* **Tracciabilità**: possibilità di sapere chi ha o ha avuto accesso ad un’informazione e chi l’ha modificata. I dati per tracciare l’informazione devono far parte dell’informazione stessa 🡪integrità.

Diritto all’oblio: le informazioni relative a una persona fisica vengono eliminate quando dichiarato in fase di raccolta dei dati e se non in contrasto con la norma vigente quando richiesto dalla persona stessa.

Ogni evento può avere impatti su uno o più parametri RID e bisogna considerare sia l’effetto diretto che quello indiretto.

**Sicurezza informatica vs sicurezza delle informazioni.**

Sicurezza informatica: sicurezza delle informazioni sui sistemi informatici.

Cybersecurity: la capacità di rendere sicuri gli oggetti vulnerabili attraverso l’informatica, riguarda sistemi informatici che trattano informazioni e anche che trattano i parametri di configurazione (essenziali per il funzionamento delle infrastrutture).

Include anche Internet of things (IoT) e operational technology (sistemi industrali, reti…)

Organizzazione: ogni forma di impresa, azienda, ente, associazione, agenzia…

**Processi**: insieme di attività tra loro interrelate o interagenti che trasforma elementi in input in elementi in output. Devono essere tenuti sotto controllo.

Input: costi, budget, date, disponibilità. Offerte, fatture…

Output: valutazioni dei costi, richieste di offerta, ordini, pagamenti, risultati…

Ci sono numerose attività che possono essere svolte con diversi strumenti informatici o non informatici.

Efficacia: grado rispetto al quale le attività pianificate sono realizzate e i risultati raggiunti.

Efficienza: relazione tra risultati ottenuti e risorse utilizzate.

Ogni processo:

* Ha elementi input provenienti da funzioni interne o entità esterne
* Per ogni attività utilizza degli strumenti
* Per ogni attività indica responsabili ed esecutori.
* Stabilisce le modalità per controllare il processo.
* Ha elementi output e destinatari.

Si mappano i processi così come sono e si modellano come si desidera modificarli.

**Funzioni**: un’organizzazione è strutturata in funzioni, cioè gruppi di persone corrispondenti alle caselle degli uffici in organigramma.

Le comunicazioni nelle funzioni devono avvenire con modalità concordate e comunicate tramite e-mail, applicazioni informatiche, moduli cartacei o oralmente.

Oltre ai processi sono importanti anche le persone ed i prodotti (3P).

Persone: le persone devono essere qualificate in grado di comprendere la sicurezza delle informazioni attraverso l’applicazione dei giusti processi e dei prodotti idonei.

**CAPITOLO 3**

**Sistema di gestione per la sicurezza delle informazioni**

La sicurezza delle informazioni si può raggiungere attraverso idonei processi Organizzativi che permettono di stabilire il livello di sicurezza adeguato, carenze, come colmarle, con quali prodotti…

Buoni prodotti di sicurezza NON garantiscono il raggiungimento dei risultati 🡪 strumenti inutilizzati perché non integrabili o per mancanza di formazione.

I processi non sono tra loro isolati e indipendenti, ma correlati e interagenti.

**Sistema di gestione** (management system): Insieme di elementi interrelati o interagenti di un’organizzazione per stabilire politiche, obiettivi e processi per raggiungere tali obiettivi.

Ogni organizzazione ha uno scopo (**missione**), il sistema di gestione di un’organizzazione è il suo sistema di pratiche organizzative (**processi**) e di altri strumenti, i processi sono interrelati e ciascun cambiamento organizzativo può avere impatti su molte aree dell’organizzazione e sugli stakeholder.

**Sistema di gestione per la sicurezza delle informazioni** (SGSI): la parte di un sistema di gestione che riguarda la sicurezza delle informazioni. Altre parti del sistema riguardano qualità, ambiente, sicurezza e salute dei lavoratori.

Bisogna saper distinguere i diversi ambiti, le loro interrelazioni e sovrapposizioni per evitare di trattare materie estranee a una disciplina moltiplicando gli sforzi.

Per un SGSI è molto importante la Direzione che è proprietaria del sistema e deve utilizzarlo come strumento per assicurare l’efficacia degli elementi.

**Certificazioni**: occorre effettuare valutazioni condotte da un dipendente o da un ente terzo e controllate da appositi organismi per raccogliere e analizzare gli elementi di prova secondo criteri stabiliti in modo da valutarli obiettivamente nel rispetto delle norme. Il risultato finale è la **certificazione**.

Esistono schemi per la certificazione dei processi, dei prodotti, dei servizi e delle persone.

La certificazione serve a dare fiducia che:

* Le decisioni siano prese da persone competenti
* Le persone impieghino prodotti a loro volta verificati e ritenuti affidabili
* Le procedure impiegate siano state a loro volta verificate.

**CAPITOLO 4**

**Rischi e valutazione del rischio**

Fasi di valutazione rischio: identificazione 🡪analisi 🡪ponderazione.

Rischio: effetto dell’incertezza sugli obiettivi. (ISO/IEC 27000)

I rischi possono essere potenziali e/o conseguenze.

L’incertezza è dovuta ad eventi che possono avere effetti positivi o negativi.

Non si può identificare un rischio reale ma solo quello percepito e le valutazioni sono soggettive.

Rischi con effetti negativi: danno di immagine, perdita di quota, perdita di competitività, rallentamenti, riduzione di liquidità, costi…

Rischi con conseguenze positive: sono generati da eventi chiamati opportunità.

Possono essere: miglioramento di immagine o reputazione, aumento clientela, guadagni…

Rischi sia positivi che negativi: nuovo cliente… ma cattivo pagatore, nuova apertura… ma scarso guadagno.

La sicurezza delle informazioni si occupa solo di rischi negativi.

**Livello di rischio**: grandezza di un rischio espresso come combinazione delle sue conseguenze e della loro verosimiglianza.

Permette di comprendere la gravità delle conseguenze e le priorità.

Il rischio r è direttamente proporzionale alla probabilità p di accadimento di un evento e alle sue conseguenze i: r  p ⋅ i.

Il rischio dipende dall’evento o minaccia m: r(m)  p(m) ⋅ i(m).

Il rischio aumenta in base al valore degli oggetti (asset a) su cui agisce: r(m,a)  p(m) ⋅ i(m,a).

Il rischio dipende dalla vulnerabilità v e dalla gravità g(v): **r(m,a,v)  p(m) ⋅ i(m,a) ⋅g(v).**

Il rischio dipende dai controlli di sicurezza c (inverso della vulnerabilità/gravità).

r(m,a,v)  p(m) ⋅ i(m,a) /r(c).

Il rischio ha probabilità e conseguenze che dipendono dai controlli:

r(m,a,v)  p(m,c) ⋅ i(m,a,c).

Un controllo carente rappresenta una vulnerabilità🡪posso sostituire i controlli c con vulnerabilità v: **r(m,a,v)  p(m,v) ⋅ i(m,a,v)**.

Parametri di valutazione rischio:

* Contesto
* Asset e valore
* Minaccia e verosimiglianza/probabilità
* Vulnerabilità e gravità o controlli e robustezza.

Una volta calcolato il livello di rischio bisogna decidere come trattarlo:

* Prevenirlo (non imbarco il bagaglio)
* Ridurre il rischio (imbarco solo una parte)
* Evitarlo (non vado in aereo)
* Eliminare il rischio eliminando l’asset (non porto il bagaglio)
* Condividere il rischio con una compagnia di assicurazioni
* Accettarlo: dipende dal livello di accettabilità personale.

**Valutazione del rischio** (risk assessment): processo complessivo di identificazione, analisi e ponderazione del rischio 🡪insieme di attività per identificare i rischi, calcolarne il livello e decidere se sono accettabili.

Dicitura completa: “valutazione del rischio relativo alla sicurezza delle informazioni”.

La **piramide di Anthony**:

Immagine che contiene testo, linea, triangolo, diagramma

Descrizione generata automaticamenteA livello strategico sono richiesti dati stimati e approssimati utili per dare indirizzi con prospettive a lungo termine.

A livello tattico sono richiesti dati consuntivi, arrotondati e abbastanza tempestivi per avere indicazioni sull’andamento delle attività operative e per prendere decisioni a medio termine.

A livello operativo i dati devono essere esatti e in tempo reale per effettuare e tenere sotto controllo le attività.

Per realizzare un sistema di gestione bisogna individuare gli elementi (processi e interrelazioni) e prendere decisioni in merito alle misure da adottare.

Iniziare da un’analisi non molto accurata a livello tattico per evidenziare necessità di analizzare a livello operativo e con maggior dettagli i sistemi informatici.

**Metodi per valutare il rischio**.

La valutazione del rischio può essere fatta con approcci più classici o altri che però sono comunque riconducibili a quello classico anche se usano termini e punti di partenza diversi.

Il metodo classico parte dagli asset per individuare vulnerabilità, quello “basato sugli eventi” parte dalle minacce per poi individuare gli asset a rischio.

Il metodo classico veniva usato a fine anni 80 quando si aveva un altro concetto di sicurezza, per questo non è raccomandato.

Viene consigliato un metodo simile ma che prevede una valutazione indipendente di asset e minacce.

Un metodo valido deve essere: completo, ripetibile, comparabile e coerente.

**Programmi software per valutazione rischio.**

Ci sono in commercio molti programmi per la valutazione del rischio che permettono di censire asset, minacce e vulnerabilità assegnando valori ed elaborando prospetti sul livello di rischio.

Questi programmi possono aiutare ad organizzare le attività delle persone interessate e ad inserire tutti i dati raccolti, anche quando le persone coinvolte non sono esperti.

Ogni programma ha dei difetti:

1. Qualità dei dati da inserire: molti dati🡪molto tempo 🡪risultati imprecisi o non utili.
2. Segretezza dell’algoritmo🡪se ho risultati non accettabili non posso comprenderne l’origine e sistemarli.
3. Configurazione iniziale inadeguata al contesto.
4. Difficoltà di riconfigurare gli strumenti soprattutto se voglio modificare i parametri.
5. Gli utilizzatori lo usano in modo meccanico non adottandolo al contesto.

Nella realtà per identificare le minacce devo sapere quali elementi (asset) le minacce possono sfruttare e quali controlli di sicurezza le contrastano.

**Chi coinvolgere?**

Tutte le parti interessate (stakeholder) dovrebbero essere coinvolte nella valutazione del rischio: personale interno, responsabili, clienti, fornitori, partners ma conoscendo solo le informazioni che riguardano la loro fase.

Il loro coinvolgimento può aiutare a: identificare il rischio, valutarlo, ponderarlo, stabilire il piano di trattamento del rischio, ridurre le incomprensioni o le resistenze al cambiamento, avere conseguenze positive sull’immagine percepita…

**I responsabili del rischio.**

**Responsabile del rischio** (risk owner): persona o entità con la responsabilità e con il potere per gestire un rischio. Coincide con la Direzione che è sempre responsabile ultimo del rischio.

I responsabili del rischio devono essere individuati a livello gerarchico con adeguati poteri decisionali per decidere quali controlli di sicurezza attuare e mantenere.

Se le informazioni sono conservate, archiviate, comunicate o elaborate, il responsabile del rischio deve essere una persona interna e può coincidere con il referente.

**Facilitatori**: conducono gli incontri tra le parti interessate e per coordinare le diverse attività di descrizione del contesto, individuazione dell’ambito, identificazione, analisi, ponderazione e trattamento del rischio. Spesso questo ruolo è coperto da consulenti esterni ma a volte anche da persone interne competenti.

**Documenti di gestione del rischio**: per la gestione del rischio vengono prodotti alcuni documenti che possono riportare carenze e vulnerabilità, per questo devono essere mantenuti e riservati e possono essere scambiati tra persone; quindi, vanno controllati mediante controlli di sicurezza.

**CAPITOLO 5 - Il contesto e l’ambito.**

Fasi preliminari della valutazione del rischio: prevedono analisi del contesto in cui si vuole operare in modo da decidere in quale ambito valutare il rischio (es: tutta l’organizzazione, anche parti esterne o perimetro più limitato).

**Contesto di un’organizzazione**: combinazione di fattori interni ed esterni che possono avere degli effetti sullo sviluppo e sul raggiungimento degli obiettivi di un’organizzazione. (ISO 9000)

Elenco degli elementi da prendere in considerazione:

Fattori interni:

* Strategie attuali e future e le loro priorità
* Livello di innovazione attuale e prevista.
* Caratteristiche delle attività principali svolte in termini di servizi e prodotti offerti + modifiche previste.
* Struttura organizzativa inclusi fornitori e processi.
* Caratteristiche delle sedi.
* Tipologia di informazioni trattate.
* Caratteristiche principali del sistema informativo: servizi informatici e tecnologie.
* Tipo di dispositivi portatili in uso.
* Archivi non informatici (cartacei).
* Luoghi dove sono collocati i sistemi informatici condivisi e quali sono.
* Rapporti con il personale interno e le loro competenze.
* Aspettative degli stakeholder.

Fattori esterni:

* Concorrenti e potenziali tali
* Normativa applicabile e modifiche previste
* Situazione economica attuale e prevista
* Clima politica e sociale
* Disponibilità sul mercato e costi delle risorse utili
* Strategie di mercato attuali e previste e aspettative degli stakeholders.

Di questi punti per descrivere il contesto bastano i principali.

**L’ambito:** dopo aver individuato il contesto posso decidere l’ambito in cui effettuare la variazione del rischio. La percezione può ridurre l’ambito ai soli servizi offerti.

Si potrebbe ad esempio limitare l’ambito della produzione a causa degli impatti sui clienti perché richiesto da una normativa.

Alcuni processi NON possono essere completamente esclusi dall’ambito, soprattutto se la finalità della valutazione del rischio è la certificazione del sistema di gestione per la sicurezza delle info.

L’ambito deve essere descritto riportando:

* Tipologie di informazioni che voglio proteggere
* Caratteristiche dei servizi erogati o dei prodotti realizzati dall’organizzazione
* La struttura organizzativa coinvolta nelle attività comprese nell’ambito e i suoi rapporti.
* La tecnologia adottata
* Le sei ed i locali in cui viene tratta l’informazione.
* I fornitori più importanti coinvolti nella sicurezza delle informazioni.

**CAPITOLO 6**

**Identificazione del rischio**

**Identificazione del rischio**: processo di individuazione, riconoscimento e descrizione del rischio. (ISO 27000)

Richiede l’identificazione di: asset, minacce, vulnerabilità e controlli di sicurezza e relazioni tra asset/minacce/vulnerabilità.

**Asset** (bene): qualsiasi cosa cha abbia valore per l’organizzazione.

Tra i tipi di asset: informazioni, software, programmi, elementi fisici, servizi, persone, competenze…

I primi asset da identificare sono le informazioni per poi correlarle agli altri asset che le contengono e trattano.

Categorie di asset:

* Informazioni in formato digitale: conservarle in un archivio è pericoloso e bisogna trattarle in modo adeguato (crearle, modificarle, conservarle, distruggerle, condividerle…), Le informazioni riguardano clienti, fornitori, personale, magazzino, produzione…
* I server fisici o virtuali
* Applicazioni (DBMS, server…)
* PC fissi e dispositivi portatili
* Rete informatica e apparecchiature legate
* Personale interno ed esterno
* Fornitori: devono essere identificati perché bisogna applicare controlli di sicurezza.
* Documenti e archivi cartacei
* Sedi e locali
* Processi e unità organizzative
* Organizzazione nel suo complesso.

Non è necessario individuare ogni singolo asset ma le loro aggregazioni basate su omogeneità geografica, procedure omogenee e asset owner e bisogna disporre di una descrizione dettagliata dei diversi gruppi di asset.

CRM: gestione delle relazioni con i clienti 🡪aggregazione di asset.

Le analisi del rischio basate sulla valutazione minuziosa degli asset portano a degli errori di valutazione.

Chi identifica gli asset?

Spetta ai responsabili delle aree dell’organizzazione comprese nell’ambito che identificano le informazioni della propria area, vengono chiamati responsabili delle informazioni o referenti per le informazioni.

Bisognerebbe coinvolgere tutti i livelli gerarchici dell’organizzazione in riunioni congiunte: i responsabili della sicurezza fisica dovrebbero fornire indicazioni su come organizzare le sedi e archivi, quelli dei sistemi dovrebbero descrivere applicazioni e server e così via.

È consigliabile un incontro personale tra facilitatori e referenti per le informazioni.

**Minacce**: causa potenziale di un incidente, che può comportare danni a un sistema o all’organizzazione. (ISO 27000). Chiamato anche risk source.

Evento relativo alla sicurezza delle informazioni: occorrenza identificata dello stato di un sistema, servizio o rete che identifica una possibile violazione delle politiche di sicurezza o un errore nei controlli o una situazione precedentemente sconosciuta che può essere significativa per la sicurezza.

Incidente relativo alla sicurezza delle informazioni: uno o più eventi relativi alla sicurezza delle informazioni che hanno una significativa probabilità di compromettere le attività di un’organizzazione e minacciare la sicurezza delle informazioni.

La minaccia è potenziale, mentre l’evento accade realmente.

Eventi e incidenti potrebbero non comportare danni (near miss).

L’identificazione di una minaccia può essere svolta a diversi livelli di dettaglio: normalmente si effettua una prima analisi non troppo dettagliata, per poi migliorarla nei successivi riesami periodici.

L’analisi del rischio relativo alla sicurezza delle informazioni richiede di identificare e valutare tutte le minacce relative alla sicurezza delle informazioni non solo quelle informatiche.

Prima si individuano gli **agenti di minaccia**: entità responsabili del manifestarsi della minaccia.

Possono essere: persone malintenzionate o non malintenzionate, strumenti tecnici o natura.

Le persone malintenzionate possono essere Interne o esterne e diverse in base alla motivazione: esibizioniste, attiviste, spie, ladri, truffatori, entità straniere ostili, personale scontento…

**Hacker**: esperti di informatica o persone che attaccano sistemi informatici spinti da diverse motivazioni. I cracker sono malintenzionati, gli ethical hacker non lo sono.

**Tecniche di minaccia**:

* Esaurimento di risorse per DoS, sciopero o malattia.
* Rappresentazione scorretta delle informazioni
* Distorsione
* Sorveglianza
* Blocco alla conoscenza dei dati.

Le minacce possono essere individuate da chiunque, è utile coinvolgere i responsabili dei sistemi informatici, della sicurezza fisica, della gestione del personale, dell’ufficio legale, ufficio acquisti…

1. **Associare le minacce agli asset**: si stima la probabilità di accadimento degli asset raggruppati in categoria, il valore della minaccia cambia, non in funzione dell’asset, ma dei fattori interni ed esterni e delle motivazioni e capacità degli agenti.
2. **Collegare le minacce alle conseguenze**: bisogna collegare le minacce alla possibile violazione di uno dei requisiti CIA.
3. **Vulnerabilità e controlli di sicurezza.** Vulnerabilità = debolezza di un asset o controllo di sicurezza che può essere sfruttato da più minacce.

Correlare le vulnerabilità agli asset e agi controlli alle minacce.

I controlli di sicurezza possono essere:

* Alternativi: si dà per scontato che il sistema sia sicuro in tutti i punti allo stesso modo per lo stesso asset. Meccanismi alternativi (es: porte in legno vs acciaio) hanno diversi livelli di robustezza.
* Compensativi: controlli di minore efficacia usati in sostituzione o alternativa a quelli ideali.
* Complementari: controlli che possono essere usati insieme per fornire un livello di sicurezza più alto.
* Correlati: non efficaci singolarmente ma solo insieme. ES: porta + meccanismo di identificazione.

I controlli di sicurezza possono dividersi anche in:

* Prevenzione: permettono di prevenire un attacco o il suo successo.
* Recupero: permettono di ricostruire la situazione precedente l’attacco e ridurne le conseguenze. Chiamati anche di mitigazione o protezione.
* Rilevazione: permettono di registrare quanto avviene e lanciare allarmi. Svolgono anche funzioni di prevenzione perché scoraggiano alcuni agenti e di recupero perché riducono i danni aiutando a tornare alla situazione precedente.

**CAPITOLO 7**

**Analisi del rischio**

**Analisi del rischio**: processo di comprensione della natura del rischio e di determinazione del livello di rischio 🡪 attività di stima del rischio senza alcun tipo di giudizio.

* Per garantire una maggiore oggettività dei risultati bisogna fornire linee guida per l’attribuzione dei valori.
* Per garantire la ripetibilità dei risultati (risultati uguali se analisi effettuate nello stesso contesto) è utile giustificare i valori.
* Documentare le scelte permette di effettuare affinamenti futuri

**Metodi di analisi**: i valori dipendono dalla scelta del metodo di calcolo 🡪quantitativi e qualitativi.

Immagine che contiene testo, Carattere, schermata, linea

Descrizione generata automaticamente-Metodi **quantitativi**: richiedono di valutare il potenziale danno economico dovuto alla perdita di riservatezza (aiuta la concorrenza), integrità e disponibilità.

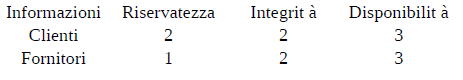
Utilizzano la probabilità statistica o la frequenza delle minacce per p(m,c) e la valutazione economica dei danni per i(m,a,c). 🡪controlli c

Sembrano precisi e oggettivi, ma nella realtà non si hanno dati statistici affidabili su minacce e attacchi. Forniscono parametri economici facilmente interpretabili.

-Metodi **qualitativi**: usano scale (alto/medio/basso) e la formula

Sembrano meno rigorose ma entrambe hanno valori soggettivi. 🡪vulnerabilità v.

Esistono metodologie semi-quantitative con valori quantitativi come linea guida di assegnazione valori (es: alto 🡪80-100).



**Valutare gli asset.**

Come metodo pratico è utile determinare inizialmente il valore dell’asset i(a) in termini di riservatezza, integrità e disponibilità (parametri RID): **i(a) = (i\_ris(a), i\_int(a), i\_disp(a))**.

Il valore degli asset: ISO 27000 richiede di valutare le conseguenze dei rischi in caso si dovessero concretizzare 🡪valutazione delle conseguenze i(m,a).

-Metodi quantitativi: Il valore dell’asset è determinato dalla somma dei valori delle informazioni trattate o conservate. i(a) = (ris(a), int(a), dis(a)) = (€ 0, € 5.000, € 400.000)

-Metodi qualitativi: il valore dell’asset è determinato dal massimo del valore delle informazioni da esso trattate o conservate.

Il valore può essere riesaminato e modificato considerando le interdipendenze.

Anche le **informazioni** sono asset da valutare in termini di:

* Costi diretti: costi per ripristino e sanzioni.
* Costi indiretti: costi per perdita di vantaggio competitivo e mancati ricavi.
* Costi sequenziali: impatto su personale e stakeholder ed errori decisionali.

**Rischio privacy**: per valutarlo è necessario considerare le conseguenze per l’organizzazione ma anche per gli interessati.

Alle informazioni viene assegnato il valore dal referente, se vengono usate in più aree bisogna considerare l’area con valutazione peggiore e bisogna renderle tra loro coerenti.

**Valutare la verosimiglianza delle minacce**: attribuire un valore a p(m) stabilendo se un evento negativo m può avvenire e con quale probabilità.

Assegnare valori alle minacce:

-Metodi **quantitativi**: assegnano ad ogni minaccia una probabilità matematica (50%) o frequenza quantistica (0.1), per favorire l’oggettività ci si basa su statistiche di diversi enti ma non sono affidabili per mancate denunce, calcolo approssimativo, accorpamenti… I centri per la rilevazione degli incidenti informatici e le assicurazioni non forniscono abbastanza dati, bisogna ragionare analizzando le capacità tecniche, le risorse disponibili, opportunità e motivazioni.

-Metodi **qualitativi**: utilizzano scale spesso su 4 livelli o 10.

-È necessario annotare le ragioni per cui è stato assegnato un certo valore quantitativo o qualitativo a una minaccia. Le note devono riportare le ricerche consultate, eventi registrati dall’organizzazione…

Chi assegna i valori alle minacce? Referenti per le informazioni, responsabil di sistemi informatici o di sicurezza fisica, responsabili della gestione del personale, ufficio legale, responsabili d’ell’ufficio acquisti…

**Rischio intrinseco (o puro)**: combinazione tra valore degli asset e probabilità di una minaccia senza considerare vulnerabilità o controlli di sicurezza attuali. 

-Quantitativo: osservare su quale parametro RID ha impatto la minaccia e moltiplicarne la frequenza per il valore pertinente di riservatezza, integrità e disponibilità dell’asset. Se la minaccia ha impatto su più asset si sommano.

ri(m, a) = p(m)\*ris(m)\* ris(a)+ p(m)\*int(m)\*int(a) + p(m)\*dis(m)\*dis(a) Σ =

Utilizzando i valori dell’asset: ri(m,a) = Σ p(m)\*z(m)\*z(a) per z=ris,int,dis = p(m)\*ris(m)\*ris(a) + p(m)\*int

Il risultato potrebbe essere riesaminato e modificato se consideriamo l’effetto di distribuzione, dipendenza o di cumulo.

Annual loss expectance (ALE): perdita annua prevista dovuta alla minaccia m sull’asset a.

ALE (m, a) = ARO (m) ⋅ SLE (m, a)

-Qualitativo: la formula è la stessa delle metodologie quantitative ma con valori qualitativi e il massimo. ri(m, a) = max p(m) ⋅ z(m) ⋅ z(a) per z=ris,int,dis.

**Valutare le vulnerabilità e i controlli:** bisogna prima individuare i controlli ideali sulla base del livello di rischio intrinseco e poi valutare quanto si discostano da quelli attualmente attivi nell’ambito.

A ciascuna minaccia si associa un rischio intrinseco, quindi possiamo determinare i dettagli di come i controlli devono essere realizzati in modo proporzionale.

Un rischio può essere controllato con misure preventive (manutenzione, scelta di componenti resistenti), di recupero (back-up, firewall) e di rilevazione.

Dobbiamo identificare i controlli ideali per l’ambito e ideali assoluti (non tengono conto del contesto).

**Valori**: vengono assegnati in base al confronto tra controlli attuali ed ideali.

**Controllo non adeguato o insufficiente**: non è progettato come quello ideale (es: manca la cassaforte).

**Controllo non conforme o non corretto**: controllo adeguato ma non attuato correttamente (es: cassaforte aperta).

-Metodi **quantitativi**: calcolare quanto ridurre la probabilità della minaccia P o le conseguenze I grazie alla presenza di controlli. 

Es: sicurezza relativa al backup non disponibile.

Probabilità: non ha impatti sulla verosimiglianza della minaccia. p(m, c) = p(m) = 0,5

Riservatezza: non ha effetti sulla riservatezza. ris(a, c) = r(a) = € 0;

Integrità: permette di avere dati coerenti e correnti di 24h fa. int(a, c) = € 500

Disponibilità: riduzione del disagio, ritardi… dis(a, c) = € 80.000

-Metodi **qualitativi**: 

È possibile assegnare un valore a g(v) secondo una scala di valori basata sull’adeguatezza e conformità dei controlli.

Asset compositi: applicazione di uno stesso controllo per più componenti di ogni singolo asset.

Si possono riportare le singole valutazioni componente per componente o si possono raggruppare le valutazioni riportando il g(v) massimo.

Uniformità dei controlli: utilizzare le stesse politiche e procedure in tutta l’organizzazione per ogni asset rende il lavoro più semplice e veloce.

Controlli compensativi: un controllo inadeguato potrebbe avere dei controlli compensativi; quindi, bisogna controllare anche il livello di sicurezza per vedere se equivalente al controllo ideale.

I valori dei controlli dovrebbero essere assegnati da persone diverse che usufruiscono di quel servizio nel quotidiano tramite interviste e questionari, piuttosto che chiedere al manager che non sa tutto.

**Livello di rischio**: stesse formule del rischio intrinseco aggiungendo la “vulnerabilità”.

Quantitativo: r(m, a, c) = Σ p(m, c) ⋅ z(m) ⋅ z(a, c) per z = ris, int, dis.

Per conoscere il rischio complessivo di un asset su tutte le minacce bisogna sommare i singoli rischi, ma così non sappiamo quali rischi sono i più pericolosi.

Qualitativo: moltiplicare il valore del rischio intrinseco per il valore della vulnerabilità.

r(m, a, v) = max[p(m)\*ris(m)\*ris(a), p(m)\*int(m)\*int(a), p(m)\*dis(m)\*dis(a)].

Il metodo quantitativo rappresenta meglio i risultati, ma la raccolta dei dati è onerosa e non sono sempre affidabili; invece, il metodo qualitativo è efficiente perché non richiede dati precisi (più veloce) e permette di individuare i rischi più elevati.

Le aggregazioni possono rendere più veloce l’analisi del rischio, anche se le minacce riguardano asset diversi, le motivazioni, possibilità di errori, controlli ed eventi naturali sono comuni a tutta l’organizzazione.

**CAPITOLO 8**

**Ponderazione del rischio.**

**Ponderazione del rischio** (risk evaluation): processo di comparazione dei risultati dell’analisi del rischio rispetto ai **criteri di rischio** (valori di riferimento) per determinare se il rischio è accettabile o tollerabile.

Consiste nel giudicare se un rischio è accettabile o non accettabile rispetto a dei criteri prestabiliti.

Esempi di criteri iniziali:

* Livello di sicurezza ≥ livello richiesto dalle clausole contrattuali e dalla normativa.
* Rischio accettabile bilancia il rischio di impresa e la sua sostenibilità in termini economici (costa troppo = rischio accettabile).
* Controlli compensativi efficaci 🡪rischio accettabile.
* Priorità ai rischi elevati e alle minacce che possono compromettere l’organizzazione con una sola ricorrenza.

Si ordinano i rischi dal meno accettabile al più accettabile.

**CAPITOLO 9**

**Trattamento del rischio.**

**Trattamento del rischio**: processo per modificare il rischio.

* **Evitare il rischio**: non iniziare o smettere un’attività (es: ramo e-commerce), spesso per le spese da sostenere. Non sempre elimina tutti i rischi.
* **Accettare/aumentare il rischio** per cogliere un’opportunità: può avvenire in modo inconsapevole (pericoloso) o consapevole perché i controlli sono ritenuti troppo onerosi (es: troppe telecamere, controlli per clienti abituali, troppe autorizzazioni).

Un controllo troppo oneroso è una vulnerabilità perché smetteranno di seguirlo.

* **Rimuovere la sorgente di rischio** (minaccia)
* **Modificare la probabilità (prevenire)**: non si può modificare la probabilità di una minaccia (fenomeni naturali, errori o hacker), ma della riuscita di un attacco. Si aggiungono/migliorano i controlli di prevenzione e rilevazione per ridurre le vulnerabilità.
* **Modificare le conseguenze** (recuperare): facilitare il recupero dei dati (es: backup) per ridurre i danni causati.
* **Condividere il rischio** con altri soggetti: ricorso a fornitori e polizze assicurative per un trasferimento parziale del rischio.

I fornitori possono pagare penali in caso di attacco, ma il cliente avrà comunque rallentamenti ed interruzione del servizio. .

Assicurazione: controllo che riduce gli impatti economici conseguenti a un incidente di sicurezza delle informazioni.

* **Mantenere (accettare) il rischio**:si mantiene il rischio perché basso, ci sono controlli compensativi, il costo dei rinnovi è troppo alto, risolverlo porterebbe altre vulnerabilità…

Trattamenti per conseguenze negative: mitigazione, eliminazione, prevenzione e riduzione del rischio.

Solitamente si modificano i controlli di sicurezza per prevenzione oppure si riducono le conseguenze 🡪 🡪le altre opzioni richiedono di modificare il valore delle informazioni o minacce che è molto difficile.

**Piani di trattamento del rischio**: insieme delle decisioni prese rischio per rischio con la relativa motivazione, deve essere approvato dalla Direzione che fornisce le risorse per attuarlo.

Prima di ridurre il rischio bisogna conoscere le azioni necessarie, per ognuna vanno elencati i benefici attesi (what-if analysis) e l’elenco deve essere riesaminato per accertarsi che siano coerenti, fattibili e non introducano rischi.

Il miglioramento continuo deve essere interpretato come una costante capacità di analisi del contesto, in modo da individuare i rischi e controllarli in modo che siano accettabili, e di completamento delle azioni pianificate.

Coerenza delle azioni: azioni che non introducono disomogeneità inutili.

Fattibilità delle azioni: bisogna valutare se un’azione si può compiere a livello economico ma anche a livello tecnico.

Bisogna tenere d’occhio i nuovi rischi introdotti ad ogni azione come l’aggiunta di controlli inutili ed efficienti.

**Piano delle azioni**: dopo aver scelto le azioni da intraprendere vanno pianificate coinvolgendo le parti interessate riportando il responsabile, la data, le risorse per l’attuazione, le modalità di verifica…

La pianificazione deve includere anche la formazioni del personale.

L’elenco delle azioni deve essere approvato dai responsabili dei rischi.

Dopo aver concluso un’azione bisogna verificarne l’efficacia.

**CAPITOLO 10**

**Monitoraggio e riesame del rischio**

Asset, informazioni, valori, minacce, vulnerabilità… tutto cambia con il tempo; quindi, è necessario tenerli sotto controllo per identificare i cambiamenti.

È necessario mantenere aperti i canali di comunicazione con le parti interessate coinvolte per poter segnalare rapidamente novità rilevanti.

Tutte le segnalazioni andrebbero registrate e possono richiedere interventi immediati.

Bisogna svolgere la valutazione del rischio ad intervalli periodici o dopo cambiamenti rilevanti.

**Analisi del rischio operativo**: la valutazione, tattica o strategica, del rischio permette di identificare aree di miglioramento e porta ad avviare progetti di lunga durata.

Bisogna monitorare il rischio attraverso: monitoraggio del canali di informazione, analisi della pertinenza delle segnalazioni e decisioni operative rapide.

Quando si analizzano le segnalazioni bisogna tenere conto anche della valutazione dei possibili impatti.

Un’altra valutazione del rischio relativo alla sicurezza delle informazioni operative è quella riguardo i progetti.

**Integrazione dell’analisi del rischio**

Entreprise risk management (ERM): gestione del rischio complessivo per tutta un’organizzazione e relativo a tutte le aree, approccio che promuove un’organizzazione basata su una visione complessiva dei rischi.

**Minacce e controlli di sicurezza delle informazioni**

**Capitolo 11 - Tecniche di minaccia**

Possibili minacce:

* **Intrusione** di malintenzionati nella sede/locali: gli agenti di minaccia possono essere esterni o interni che entrano con la forza, l’inganno o il furto attraverso infiniti possibili modi.
* Intrusioni di malintenzionati nei sistemi informatici: gli utenti possono essere sia persone interne che esterne ma anche amministratori di sistema o utenti.

Un buon modo per proteggersi sono le password, ma sensibili ad attacchi a forza bruta ed altre tecniche di hacking (fasi: investigazione🡪intrusion🡪attacco🡪uscita).

* + Supply-chain attack: intrusione nei sistemi di un’organizzazione sfruttando le vulnerabilità dei sistemi fornitori.
* **Social engineering** e frodi: inganno, frode e raggiro usate per intrusioni fisiche o informatiche. ES: fingersi qualcuno, phishing…
* **Furto d’identità**: l’attaccante usa un’altra identità per nascondersi o danneggiare.
* **Danneggiamento** di apparecchiature fisiche: danneggiamento di apparecchiature in sede (PC), fuori sede (ATM), portatili, comunicazioni o anche documenti e la sede stessa. Possono essere volontari, involontari o a causa di fenomeni esterni/naturali.
* Danneggiamo di programmi informatici: utenti malintenzionati potrebbero esaurire le risorse o accedere a informazioni riservate, mentre utenti non malintenzionati potrebbero usare in modo incorretto le apparecchiature.
* **Furti** di apparecchiature informatiche o impianti fisici: solitamente si ruba l’apparecchiatura per il valore dell’oggetto, può avvenire anche all’esterno se trasportato da un dipendente.
* Lettura, furto, copia o alterazione dei **documenti**.
* Intercettazione di **emissioni elettromagnetiche**: intercettare le emissioni dei dispositivi per ricostruire quanti visualizzato. Richiede vicinanza fisica.
* Interferenze da emissioni elettromagnetiche: interferenze che possono alterare integrità o disponibilità delle informazioni.
* Lettura, copia e modifica non autorizzata dei **documenti informatici**.
* Trattamento scorretto delle informazioni rispetto alla normativa.
* **Malware**: installato volontariamente o involontariamente.
* Copia e uso illegale di **softwares**: un interno che copia software e licenze dell’organizzazione per usarli all’esterno o rivenderli facendo possibilmente ricadere le colpe sull’azienda.
* Uso non autorizzato di **sistemi e servizi informatici** esterni: causano perdita di tempo e rallentamenti o diffusione di malware.
* Uso non autorizzato di sistemi e servizi informatici offerti dall’organizzazione.
* Recupero di informazioni: recuperare informazioni cancellate.
* Esaurimento o riduzione delle **risorse**: come per attacchi DoS o scioperi.
* Intercettazione delle **comunicazioni**: per attacchi MITM.
* **Invio di dati** a persone non autorizzate: anche per errore.
* Invio/ricezione di dati non accurati.
* Ripudio di messaggi e documenti inviati.
* Oggetti digitali: IoT, OT, IIOT, es: telecamere.
* Attacchi a sistemi IA: risultati errati, comportamenti inattesi, avvelenamento…

**Capitolo 12**

**Controlli di sicurezza**

I controlli di sicurezza delle informazioni sono spesso indicati come misure e contromisure, mentre “meccanismo di sicurezza” indica i controlli tecnologici.

**Controllo**: misura che modifica il rischio (ISO 27.000) includono processi, politiche, dispositivi, pratiche o azioni che modificano il rischio e potrebbero anche non ottenere l’effetto atteso o previsto di modifica del rischio.

I controlli possono essere:

* Organizzativi
* Relativi a singole persone
* Di sicurezza fisica
* Tecnologici

Attributi dei controlli:

* Tipologia: preventivo, di rilevazione e correttivo,
* Proprietà di sicurezza: riservatezza, integrità, disponibilità
* Concetti di cybersecurity: identificare, proteggere, rilevare, rispondere e ripristinare.

**Documenti**: vanno fornite indicazioni al personale riguardo come trattare le informazioni, specialmente se le attività sono svolte da più persone, raramente o sono nuove.

L’organizzazione deve stabilire quali documenti sono necessari e devono essere identificabili, riportare l’autore e la data, scritti in modo comprensibile (disegni, frasi brevi, ripetizioni, giustificazioni…), in formato cartaceo o digitale.

Bisogna stabilire tempi di conservazione, verifica e manutenzione dei documenti.

I documenti possono essere:

* **Procedure**: “modo specifico di effettuare un’attività o processo”, può essere documentata (procedura scritta) o no (prassi), andrebbero seguite sempre ma non è così.
* **Registrazioni**: “documento che riporta i risultati ottenuti o fornisce evidenza delle attività svolte”, possono avere l’approvazione dei partecipanti o dell’esecutore. Sono utili per contestazioni, coordinamento, passaggio di consegne, elaborazione di report utili…

Bisogna stabile un modo per archiviarle su un server in modo sicuro e accessibile.

* **Politiche** (policies): “intenzioni e indirizzi di un’organizzazione espressi formalmente da parte della Direzione”. Deve riportare:
  + Cosa si intende per “sicurezza delle informazioni”? perché è importante? Cosa lo è di più?
  + Quali sono i principi generali da seguire?
  + Come sono state assegnate le responsabilità?

Deve essere approvata, emessa dalla Direzione e riesaminata regolarmente.

**Organizzazione per la sicurezza delle informazioni**.

Bisogna assegnare esplicitamente le responsabilità per ogni responsabilità e processo.

Ruoli più importanti:

* **Direzione**: “persona o gruppo di persone che dirigono e tengono sotto controllo un’organizzazione al più alto livello.” Può delegare parte della sua autorità e fornire risorse. Ha la responsabilità ultima nelle decisioni di sicurezza delle informazioni e assegna le responsabilità. Si occupa di governance e management.
* **Responsabile della sicurezza**: non è obbligatorio, ma è utile in organizzazioni dalla struttura complessa. Si può aggiungere il Data Protection Officer responsabile della protezione dei dati personali.
* **Amministratori di sistema**: addetti alla configurazione e manutenzione dei sistemi informatici e dei meccanismi tecnologici di sicurezza fisica.

I vari ruoli devono coordinarsi tra loro e vanno istituite **commissioni** da riunire periodicamente per analizzare i nuovi eventi e incidenti, riesaminare l’avanzamento delle attività e stabilire variazioni.

Alla fine di una commissione bisogna scrivere un resoconto in modo da non poter cambiare le cose dette oralmente.

**Separazione dei ruoli** l’assegnazione dei ruoli deve evitare possibili abusi, volontari o involontari, di poteri, per questo si effettua la separazione dei compiti.

* Non si può essere il responsabile dei controlli sulle proprie attività
* L’autorizzazione per le operazioni molto critiche non può essere affidata ad una sola persona.
* Bisogna separare le funzioni per evitare che alcuni obiettivi vengano ignorati, ad esempio le funzioni relative alla sicurezza e all’IT devono essere indipendenti dalle altre. Se il personale non basta per assegnare tutti i ruoli devono essere attuate misure compensative.

**Gestione dei progetti**.

Progetto: insieme di attività con termini di tempo e obiettivi definiti. Es: aperura di un nuovo sistema informatico o di una nuova sede. Il risultato di un progetto è il prodotto.

Fasi di un progetto: pianificazione🡪definizione dei requisiti🡪incontri tra le parti 🡪verifica e test.

Requisiti: controllo degli accessi, informare dei cambiamenti, tracciare le azioni, requisiti legali, rapporti con terzi.

**Rapporti con le autorità**: è necessario costruire una rete di contatti con le forze dell’ordine per coordinare meglio le autorità quando necessario. Per alcune organizzazioni come banche sono istituite autorità di vigilanza nazionale o sovrannazionale.

**Gestione del personale**: dipendenti, consulenti, collaboratori temporanei e stagisti.

Selezione: controllare che le competenze dichiarate siano quelle effettive e, se necessario, formarle.

Contratto: accordo di riservatezza, obbligo di rispettare politiche e procedure e sanzioni disciplinari.

Uscita e cambiamenti di personale: assicurare il continuo dell’attività e avvisare gli altri lavoratori per organizzarsi meglio.

Competenze: istruzione, formazione, addestramento ed esperienza. Si può valutare in scala:

non competente < competente non autonomo < competente autonomo < competente e capace di insegnare ed aiutare gli altri. Bisogna pianificare azioni per disporre delle competenze mancanti.

Il personale deve rimanere aggiornato partecipando ad associazioni e **gruppi di interesse**.

È importante favorire consapevolezza e sensibilizzazione riguardo la sicurezza, anche mettendo alla prova i lavoratori, se possibile fornendo strumenti che obbligano i dipendenti alla sicurezza.

Bisogna considerare la sicurezza anche nel lavoro fuori sede, studiando la sicurezza fisica dei locali in cui si lavora e fornire una formazione specifica per i lavoratori fuori sede.

**Gestione degli asset**

**>Informazioni**: devono essere identificate, classificate, etichettate e trattate a seconda della classificazione.

Per ogni informazione bisogna identificare il **responsabile**.

Le informazioni vanno **classificate**: si attribuisce loro i pertinenti livelli di riservatezza per stabile chi è autorizzato ad accedervi e modificarle. Es livelli: informazioni pubbliche: a uso interno e ad uso ristretto.

**Etichettatura**: le informazioni classificate possono essere etichettate indicando il livello di classificazione e quali gruppi di personale possono accederci.

**Trattamento**: a seconda del livello di classificazione sono previste diverse modalità di trattamento che riguardano: conservazione, copia, trasmissione, distruzione o scambio di informazioni.

Le regole vanno rese note mediante istruzioni.

**Data loss prevention**: programmi che controllano automaticamente il rispetto delle regole stabilite possono anche classificare le informazioni in automatico tramite parole chiave, monitorare i canali di trasmissione, reagire ad attività sospette…

Si possono applicare **tecniche di mascheramento** che sostituiscono o cancellano parte dei dati o **di anonimizzazione** cancellando i riferimenti alle persone fisiche.

>**Identificazione, censimento e proprietà degli asset**.

Identificare gli asset al corretto livello di dettaglio è necessario, si fanno tanti inventari diversi che riguardano tipi diversi di merce, a volte vengono chiamati configuration management system (CMS) o database (CMDB). Ad ogni asset viene assegnato un proprietario.

**>Controllo degli accessi**: a ciascuna persona sono assegnate autorizzazioni per accedere alle informazioni o agli strumenti per trattarli. Per ottenere un accesso un utente deve identificarsi attraverso credenziali. Per l’assegnazione di identità condivise o utenze per entità non umane è necessario stabili processi e responsabilità.

**Autorizzazioni**: operazioni che una persona può effettuare seguono i principi**: minimum privilege, need to know to use e segregation of duties**. L’ufficio del personale e l’ufficio acquisti devono gestire anche i casi di ritiri o cambiamenti di autorizzazioni. Vanno riesaminate periodicamente.

**Cifratura**: algoritmo simmetrico per avere chiavi lunghe + chiave criptata con algoritmo asimmetrico.

Le chiavi di cifratura devono essere conservate in modo sicuro e deve esserci un meccanismo sicuro di recupero delle chiavi.

La crittografia permette di firmare documenti, verificare la validità delle firme e apporre marche temporali, questi meccanismi devono essere approvati da autorità per avere validità legale (servizi fiduciari).

**Sicurezza**: importante in tutti i locali, specialmente nei data centre (CED).

**Applicazione**: software direttamente utilizzato dall’utente finale, attraverso opportune interfacce.

**Infrastruttura informatica**: insieme di hardware e sistemi operativi, inclusi quelli di rete, che costituiscono la base di ogni sistema informatico e sono necessari per il funzionamento e l’utilizzo delle applicazioni**.**

Principi della sicurezza: secuirity by design, defence in depth, default deny, fail securely (i malfunzionamenti non devono introdurre vulnerabilità) e least privilege.

L’analisi degli impatti sui sistemi preesistenti deve valutare se i seguenti meccanismi di sicurezza rimangono validi dopo il cambiamento: sistemi di monitoraggio, logging, controllo degli accessi, controllo della rete, backup (completi, incrementali, differenziali…), prestazioni HW e comunicazioni con altri sistemi.

**Monitoraggio**: svolto da un gruppo di operatori come il Network operation centre che monitora qualsiasi evento anomalo e il Security operation centre che cerca incidenti di sicurezza.

**Blockchain**: registro distribuito nato per i bitcoin complesso e poco flessibile, sono molto apprezzate ma spesso un’applicazione centrale ben progettata è più economica, semplice e veloce.

Regole d’uso dei dispositivi:

* Non farli usare a persone non autorizzate
* Bloccarli con password
* Cifrare i dati memorizzati

Se portatili:

* Non lasciarli incustoditi
* Non usarli in luoghi pubblici
* Non intrattenere conversazioni riservate on pubblico.

BYOD: Bring your own device: lavorare utilizzando i propri dispoitivi Hardware 🡪vulnerabilità: sicurezza minore dei dispositivi lavorativi.

**Sicurezza delle comunicazioni**:

* Quali servizi esterni possono essere utilizzati dentro un’organizzazione? A volte un firewall blocca i social o la messaggistica 🡪superabile facendo da router con cellulare🡪rischi di infettare tutti.
* Quali servizi interni possono essere usati all’esterno?
* Quali servizi terzi devono essere usati dal personale per lavoro? Considerare la loro sicurezza.

Servizi: social network, file sharing, servizi di configurazione…

Reti: wi-fi, reti dei visitatori, segmentazione della rete.

**Fornitori**: di prodotti HW/SW e assistenza, di servizi non informatici (vigilanza, pulizie) e di servizi informatici. Stabilire i requisiti🡪verificare se i fornitori possono garantirli 🡪accettare 🡪accordo o contratto 🡪controllare il rispetto di quanto concordato.

**Gestione degli incidenti**:

Rilevazione di eventi, incidenti e vulnerabilità attraverso sistemi automatici o manuali di monitoraggio.

Registrazione degli eventi, del segnalatore, della persona che li tratta…

Categorizzazione: poche analisi per comprendere se la segnalazione riguarda un incidente o una vulnerabilità, l’impatto, quale funzione è la più adeguata a trattare l’incidente o la vulnerabilità…

Categorizzazione 🡪priorità🡪diagnosi più approfondita🡪 se la tecnica della diagnosi non può affrontare l’incidente da sola deve coinvolgere altre strutture (escalation tecniche o gerarchiche).

Notifica di eventi rilevanti al cliente.

**Patching**: se una vulnerabilità è dovuta a un errore software il produttore può risolverla mettendo a disposizione aggiornamenti correttivi (fix o patch) o segnalando strade alternative per evitare il problema (workaround) 🡪installare le patch subito o aspettare che le provino gli altri?

**Crisis management**: si occupa di aspetti strategici conseguenti a un incidente grave.

Si basa su tecniche di pubbliche relazioni nei confronti degli stakeholder, i piani di gestione delle crisi devono indicare chi ha l’incarico di rappresentare l’organizzazione nei mezzi di informazione e riportare esempi di messaggi da diffondere.

**Digital forensics**: uso di metodi scientifici e provati per preservare, raccogliere, validare, identificare, analizzare, interpretare, documentare e presentare i mezzi di prova digitali derivati da dispositivi digitali, allo scopo di facilitare o portare avanti la ricostruzione di eventi criminali o aiutare ad anticipare azioni non autorizzate.

Quando si ha il sospetto che qualcuno stia compiendo dei reati con strumenti informatici: consultarsi con un legale e scollegare il sistema dalla rete senza spegnerlo o altro.

**Business continuity** (Continuità operativa): capacità di un’organizzazione di continuare a fornire prodotti o servizi a un livello accettabile predefinito, dopo un incidente di disturbo.

1. Business impact analysis: individuare i tempi massimi accettabili di interruzione delle attività.
2. Valutare rischio della continuità operativa: indisponibilità sede, archivi, servizi informatici, connessione internet, del personale…
3. Stabilire obiettivi e strategie di ripristino:

**RTO**: recovery time objective: tempo massimo per ripristinare la disponibilità delle informazioni.

**RPO**: recovery point objective: punto nel tempo con dati coerenti da ripristinare.

**MBCO**: minimum business continuity objective: risorse minime necessarie in emergenza.

1. Impostare piani di continuità: procedure che descrivono cosa fare in caso di incidente con impatti sulla continuità.
2. Effettuare test e mantenere piani: simulazioni di situazioni o errori.

Un’organizzazione deve rispettare diverse normative come quella sulla criminalità informatica, sui diritti d’autore, sul commercio elettronico…

**Audit**: processo sistematico, indipendente e documentato volto all’ottenimento di prove, al fine di valutarle per determinare quanto i criteri di audit (politiche e procedure) sono soddisfatti.

Audit: interni (di prima parte), esterni (di seconda parte🡪parte interessata) e di certificazione (di terza parte 🡪organismi indipendenti).

Gli auditor possono richiedere di connettersi a sistemi per effettuare analisi e raccogliere dati e potrebbero voler verificare i comportamenti dei sistemi interagendo con essi.

**Vulnerability assessment**: analisi dei sistemi informatici e ricerca/valutazione delle vulnerabilità presenti, possono riguardare infrastruttura o applicazioni.

Può essere condotto in modalità white box o black box.

Si possono condurre penetration test per analizzare una determinata applicazione informatica prima di renderla disponibile al pubblico.

L’identificazione e valutazione delle vulnerabilità è divisa in 2 parti: teorica (vulnerability assessment) e sperimentale (penetration test).

**I requisiti di un sistema di gestione per la sicurezza delle informazioni**

**Capitolo 13**

**Le norme ISO e l’HLS.**

**Standard verificabili**: norme con specifiche rispetto alle quali può essere condotto un audit da parte di personale indipendente; usano il verbo imperativo shall (deve);

**Linee guida**: manuali o raccolte di best practice al fine di raggiungere un certo obiettivo; si riconoscono perché sono usano i verbi al condizionale should/can/may (dovrebbe/può/potrebbe).

Le norme possono riguardare: prodotti, servizi, sistemi organizzativi, competenze…

**Norme ISO 27000**: standard verificabile (“requisiti nel titolo”) .

In Italia gli organismi corrispondenti all’ISO e IEC sono l’UNI (ente nazione per uniformazione) e CEI (comitato elettrotecnico italiano).

**27.001**: linee guida che forniscono supporto ad attuazione dei requisiti.

27.002: descrive i controlli di sicurezza, non è possibile dichiarare conformità rispetto a questa ISO.

27.003: guida all’interpretazione della 27.001.

27.004: guida per misurazione e monitoraggio di un sistema di gestione per la sicurezza delle info.

27.005: guida per la gestione del rischio relativo alla sicurezza delle informazioni.

27.017: controlli di sicurezza per servizi cloud.

27.018: controllo di privacy per servizi cloud.

27.019: controlli di sicurezza per settore energetico.

**27.701**: riguarda la certificazione del sistema di gestione per la protezione dei dati personali, aggiunge alcuni requisiti alla 27.001.

**HLS**: High level structure: standard per la scrittura degli standard, pubblicato nell’Annex SL delle ISO, tutti gli standard adesso lo seguono.

**Capitolo 14**

**Il miglioramento continuo e il ciclo PDCA**

Le norme ISOS sui sistemi di gestione impongono il miglioramento continuo della qualità totale: ogni processo contribuisce alla qualità dei prodotti e servizi offerti 🡪migliorare (adattare) tutti i processi di un’organizzazione.

Immagine che contiene diagramma, cerchio, Carattere, linea

Descrizione generata automaticamenteLe organizzazioni tendono a non modificare nulla se non sono costrette perché spaventate dalle conseguenze di possibili cambiamenti, i cambiamenti devono essere controllati per evitare rischi e inefficienze dovute alla novità e all’inesperienza.

Ciclo PDCA: Plan-do-check-act: individuare attività, processi e strumenti 🡪 realizzare il piano 🡪verificare se si ha ottenuto il risultato sperato 🡪intervenire in caso di carenze.

Pianificare: attività a lungo termine e caratteristiche di prodotti e processi (l. strategico), i miglioramenti dei processi (l. tattico) e le attività quotidiane per prodotti e servizi (l. operativo). Fare: realizzare il piano. Verificare: controllo l’efficienza quotidianamente.

Intervenire: per correggere o migliorare, non per trovare il colpevole.

Ogni fase del PDCA può essere scomposta in un PDCA (natura frattale circolare o gerarchica).

**Capitolo 15**

**I requisiti di sistema**

L’ordine con cui sono presentati i requisiti nello standard ISO 27000 non rifletté né l’importanza né l’ordine di implementazione.

I requisiti standard sono applicabili a tutte le organizzazioni.

Il termine **ambito** può essere legato all’applicazione di una norma, al sistema di gestione per la sicurezza delle informazioni o alle certificazioni.

**Contesto**: fattori interni ed esterni, parti interessate e le loro aspettative.

**Ambito**: può essere tutta l’organizzazione o solo parte di essa, bisogna descriverlo e fornire le motivazioni della scelta considerando.

La descrizione dell’ambito dovrebbe riportare: le caratteristiche dei servizi/prodotti, le informazioni di cui garantire la sicurezza, i processi, la struttura…

**Leadership**: ruolo della Direzione di appoggio ma anche esempio e guida.

La direzione deve stabilire le policies di sicurezza, garantire la disponibilità delle risorse, comunicare e dirigere/sostenere le persone affinché contribuiscano al miglioramento del sistema di gestione.

**Politica**: la politica per la sicurezza delle informazioni deve riportare uno schema di riferimento per stabilire gli obiettivi e la volontà della Direzione di soddisfare i requisiti. Deve essere documentata e comunicata senza esporre informazioni sensibili.

**Pianificazione**:

* Strategica: scelte generali, preparazione e pubblicazione della politica per la sicurezza e scelta degli obiettivi strategici.
* Tattica: stabilisce i dettagli dei processi e dei controlli di sicurezza, i loro obiettivi, le risorse, le attività che compongono i processi…
* Operativo: stabilisce esattamente quando effettuare attività come manutenzione o test.

I processi, rischi e obiettivi nascono da una valutazione dei rischi relativi all’efficacia del sistema.

Le **opportunità** vengono valutate come minacce, se un’opportunità non viene colta l’impatto negativo è la perdita di benefici.

**Minacce relative alla qualità**: indisponibilità di materie prime, forniture inadeguate, errori del personale o di fornitori e guasto dei macchinari.

La valutazione del rischio è **periodica** quindi va ripetuta almeno una volta all’anno, potremmo fare una rivalutazione del rischio solo per gli asset che hanno subito modifiche.

**Le azioni**: l’ISO 27001 non fornisce esplicitamente i requisiti relativi alle azioni ma ad ogni azione deve essere collegato almeno un obiettivo per il quale devono essere soddisfatti dei requisiti precisi.

Per ogni azione bisogna pianificare: le risorse, i responsabili, le aziende e le valutazioni.

Un’azione può essere semplice o richiedere molto tempo per essere realizzata.

La valutazione dell’efficacia di un’azione prevede di analizzare se è stata realizzata come pianificato e se ha raggiunto gli obiettivi previsti e deve essere svolta a intervalli durante la pianificazione ed attuazione e tempo dopo la sua conclusione.

**Obiettivo**: risultato da raggiungere. Può essere strategico, tattico o operativo, può essere applicato in molti modi e devono essere SMART (Specifici, misurabili, achivable, relevant e time-bound (scadenza)).

Bisogna stare attenti a non ridurre l’analisi ai soli obiettivi misurabili.

Gli obiettivi possono essere misurati per attributi (valori discreti) o per variabili (var. continue).

* Generici strategici: es. garantire la riservatezza delle informazioni.
* Di azione: riguardano azioni (realizzare un’azione relativa al backup) e progetti
* Di rischio.
* Di conformità: “le procedure devono essere applicate”, “procedure/processi devono essere conformi alle normative e agli standard”, “i prodotti e servizi devono essere conformi a quanto stabilito dalle specifiche e standard”.
* Di prestazione: per raggiungere un certo livello.

**Processi di supporto**: gestione delle risorse, delle competenze e consapevolezza, della comunicazione e dei documenti.

**Valutazioni delle prestazioni:**

**-Monitoraggi**: determinazione dello stato di un sistema, di un processo o di un’attività.

Principalmente dei processi non delle persone (limitati) e non solo tecnologici.

**-Misurazione**: processo per determinare un valore. **Metodo di misurazione**: sequenza di operazioni per quantificare un attributo rispetto una scala.

Cosa misuro? Tempo di indisponibilità, tempi di risoluzione degli incidenti e livello di rischio.

Falsi miti:

-Se non lo misuri non puoi gestirlo.

-Servono sempre numerose informazioni.

-Serve un obiettivo per ogni misurazione.

**Non conformità**: mancato soddisfacimento di un requisito. ES: backup ogni 2 mesi invece di 1.

Bisogna reagire eliminandole e affrontando le conseguenze.

-Di processo.

-Di produzione o progettazione. Es: mancata connessione di un nuovo servizio informatico ai sistemi di monitoraggio degli eventi e delle vulnerabilità.

-Di fornitura.

**Azione correttiva**: azione per eliminare la causa di una non conformità e prevenirne il ripetersi.

**Azione preventiva**: azione per eliminare la causa di una potenziale non conformità.