Confcom

Assintel
Associazione Italiana
Imprese Digitali

CYBER
Think Tank
ASSINTEL

European
DIGITAL SME
Alliance

Small
Business
Standards

# GUIDA PER LE PMI:

## IMPLEMENTAZIONE DELLA ISO/IEC 27001:2022 SULLA GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI

**GIUGNO 2026**

# INDICE

# PREFAZIONE

Nell'ambito delle azioni finanziate dall'UE, promosse dalla Small Business Standards (SBS) - associazione europea che rappresenta gli interessi delle piccole e medie imprese (PMI) nel processo di normazione, la European DIGITAL SME Alliance ha sviluppato e aggiornato una Guida per le PMI per l'implementazione della ISO/IEC 27001 sulla gestione della sicurezza delle informazioni.

L'obiettivo principale della Guida sulla gestione della sicurezza delle informazioni è supportare le PMI nella comprensione e nell'applicazione della ISO/IEC 27001 per la gestione dei sistemi di sicurezza delle informazioni. Con la pubblicazione della revisione del 2022 della norma, si è reso necessario un aggiornamento per recepire i nuovi requisiti e adattare i contenuti al panorama europeo della cybersecurity. La nuova edizione della Guida continua a fornire alle PMI uno strumento pratico e accessibile per rafforzare la gestione della sicurezza delle informazioni in linea con gli standard internazionali.

Questa pubblicazione è il risultato del lavoro del gruppo di lavoro DIGITAL SME "WG27K", che ha riunito esperti con esperienza nelle problematiche di standardizzazione relative ai sistemi di gestione della sicurezza delle informazioni. Tali attività sono state coordinate da Guido Sabatini e presiedute da Fabio Guasconi. I recenti aggiornamenti sono stati guidati da Davide Iaccarino, Cybersecurity & Data Project Manager presso la European DIGITAL SME Alliance, in collaborazione con Davide Giribaldi, esperto di cybersecurity e normazione, nonché uno dei coautori originari della guida. Hanno contribuito alla Guida esperti con una solida conoscenza della sicurezza delle informazioni e della normazione, tra cui Georgia Papadopoulou, George I. Sharkov, David Bulavrishvili, Sergio Oteiza, Holger Berens, Ermal Çifligu, Sebastiano Toffaletti, Nanuli Chkhaidze, Yuri V. Metchev, Thorsten Dombach e Alexander Häußler.

La Guida, elaborata nella sua versione originale in inglese dalla European DIGITAL SME Alliance e Small Business Standards, è stata tradotta in italiano dal Cyber Think Tank di Assintel, con il contributo di Mark Alan Barlow, Jim Biniyaz, Vittorio Orefice, Marco Scognamiglio e Sofia Scozzari, con la supervisione di Antonio Assandri e di Davide Giribaldi.

*Disclaimer: la presente Guida ha carattere puramente informativo nei suoi contenuti. L'implementazione di questa Guida non implica la piena conformità alla ISO/IEC 27001. Il presente documento non è inteso e non può essere utilizzato come sostituto della certificazione ISO/IEC 27001. Questa Guida riflette esclusivamente il punto di vista di Small Business Standards e della European DIGITAL SME Alliance. La Commissione Europea e gli Stati membri dell'EFTA non sono responsabili per l'uso che potrà essere fatto delle informazioni in essa contenute.*

Assintel è l'associazione nazionale di riferimento delle imprese ICT e Digitali di Confcommercio.

Il Cyber Think Tank di Assintel è l'hub di collaborazione in cui aziende e professionisti lavorano insieme per affrontare le sfide più pressanti in materia di sicurezza informatica.

Corso Venezia 47, 20121 Milano, Italia

segreteria@assintel.it

www.assintel.it

Tel. +39027750231

European DIGITAL SME Alliance è la più grande rete europea di piccole e medie imprese del settore ICT e rappresenta circa 45.000 PMI tecnologiche.

Rue Marie Thérèse 21, 1000 Bruxelles, Belgio

office@digitalsme.eu

www.digitalsme.eu

Tel. +32(0)2 893 02 35

Registro per la trasparenza: 082698126468-52

La Small Business Standards (SBS) è l'associazione europea che rappresenta gli interessi delle piccole e medie imprese (PMI) nel processo di normazione, sia a livello europeo sia a livello internazionale.

Rue Jacques de Lalaing 4, 1000 Bruxelles, Belgio

info@sbs-sme.eu

www.sbs-sme.eu

Tel. +32(0)2 285 07 27

Registro per la trasparenza: 653009713663-08

Cofinanziato dall'Unione europea e dall'EFTA

# GLOSSARIO

Per facilitare la comprensione della presente Guida, di seguito sono riportate le definizioni dei termini più comuni e specifici:

**Asset:** qualsiasi elemento che rivesta valore per l'organizzazione. Esistono diverse tipologie di asset, ad esempio dati, hardware, software, fornitori di servizi, personale e sedi fisiche.

**Attacco:** forma deliberata di minaccia, ad esempio un atto indesiderato o ingiustificato finalizzato a ottenere vantaggi o a danneggiare una terza parte agendo su un insieme di asset.

**Disponibilità:** proprietà di essere accessibile ed utilizzabile su richiesta da parte di un'entità autorizzata.

**Riservatezza:** proprietà che consente l'accesso o la divulgazione di informazioni esclusivamente a individui, entità o processi autorizzati.

**Controllo:** misura adottata per modificare il rischio. I controlli comprendono processi, politiche, dispositivi, pratiche o altre azioni in grado di modificare efficacemente il rischio.

**Integrità:** proprietà che garantisce accuratezza e completezza.

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

**Rischio (sicurezza delle informazioni):** rischio relativo alla sicurezza delle informazioni consistente nella possibilità che delle minacce sfruttino le vulnerabilità di un asset informativo, causando danni a un'organizzazione.

**Valutazione del rischio (sicurezza delle informazioni):** processo complessivo di identificazione, analisi e valutazione del rischio.

**Trattamento del rischio (sicurezza delle informazioni):** processo di modifica del rischio, generalmente evitando, condividendo, mitigando o accettando il rischio.

**Minaccia:** causa potenziale di un incidente indesiderato, che può provocare un danno.

**Vulnerabilità:** debolezza di un asset o di un controllo che può essere sfruttata da una o più minacce.

# 1. INTRODUZIONE ALLA CYBERSECURITY

Oggigiorno, le informazioni costituiscono uno degli asset principali per la maggior parte delle aziende e, per molte di esse, rappresentano il fondamento della creazione di valore. Altre dipendono fortemente dal trattamento delle informazioni per supportare le proprie attività operative.

Tuttavia, il panorama delle minacce è diventato più complesso, con attaccanti che utilizzano metodi avanzati e persistenti per sfruttare tale dipendenza. Abbiamo infatti assistito a numerosi esempi di comportamenti illeciti, come attacchi ransomware su larga scala (WannaCry, Petya), fughe di dati personali da grandi aziende (ad esempio Equifax, Marriott), divulgazione di strumenti di spionaggio appartenenti ad agenzie di intelligence e persino violazioni che hanno colpito infrastrutture critiche, come nel caso di Colonial Pipeline.

Con l'aumento del numero di minacce e la crescita dei rischi, le aziende sono chiamate ad adottare un approccio proattivo e orientato alla resilienza nella gestione delle informazioni, ad esempio attraverso l'implementazione di semplici misure di protezione quali:

- implementare l'accesso a computer e sistemi mediante password;
- installare software antivirus sulle postazioni di lavoro degli utenti finali e negli ambienti server;
- disabilitare l'utilizzo di chiavette USB all'interno dell'azienda;
- acquisire soluzioni più avanzate e costose.

Sebbene molte di queste misure siano efficaci nel proteggere i sistemi, altre rappresentano un puro spreco di risorse economiche e umane. Ciò non dipende dal fatto che gli strumenti sopra menzionati siano scadenti o inefficienti. Il problema principale risiede piuttosto nella scelta degli strumenti da adottare, nella valutazione dei loro costi e nella loro effettiva implementazione in funzione delle esigenze operative di ciascuna azienda.

**PERCHÉ UNA GUIDA PER LE PICCOLE E MEDIE IMPRESE (PMI)?**

- Le PMI costituiscono la maggioranza delle imprese in Europa, superando numericamente le grandi aziende e impiegando un numero maggiore di persone. Sono inoltre riconosciute come un importante motore di innovazione in Europa.

- La maggior parte delle PMI sottovaluta il proprio livello di rischio rispetto ai cyber attacchi, nella convinzione di non gestire informazioni che valga la pena rubare.

- Tuttavia, le piccole imprese dispongono di numerosi asset digitali rispetto a un singolo utente e spesso adottano misure di sicurezza inferiori rispetto alle grandi aziende.

A causa della crescente complessità dell'attuale contesto digitale e delle interdipendenze dei flussi informativi, molte aziende riconoscono la necessità di ruoli dedicati, quali i responsabili della sicurezza delle informazioni, i professionisti della cybersecurity e i comitati di governance. Sempre più spesso vengono inoltre istituiti team o strutture specifiche dedicate alla risposta agli incidenti e alla resilienza.

Tuttavia, in molte aziende permane l'incertezza sull'effettivo valore degli investimenti in misure di sicurezza. Le carenze in ambito cybersecurity possono infatti continuare a generare problemi significativi, riconducibili principalmente a tre categorie:

- perdita di disponibilità, che ostacola le attività aziendali;
- perdita di riservatezza, che può causare danni alla reputazione dell'azienda o persino dar luogo ad azioni legali;
- perdita di integrità, che comporta l'utilizzo di dati errati o addirittura falsificati.

La cybersecurity è fondamentale per proteggere gli asset delle imprese di ogni tipo e dimensione. Ma che cos'è esattamente la cybersecurity?

### 1.1 DEFINIZIONE DI CYBERSECURITY

Non esiste una definizione formale di **cybersecurity**, ma il suo significato è affine a quello di sicurezza delle informazioni. La cybersecurity è spesso considerata come l'insieme degli aspetti più tecnici della **sicurezza delle informazioni**, la quale a sua volta mira a proteggere le informazioni conservate su supporto cartaceo, nei sistemi informatici o persino detenute dalle persone. La cybersecurity riguarda principalmente la protezione delle informazioni archiviate elettronicamente e del loro relativo trattamento.

Può essere definita come uno stato in cui i rischi associati all'uso dell'IT, tenendo conto di eventuali minacce e vulnerabilità, sono ridotti a un livello accettabile mediante misure appropriate. Anche il fattore umano, inclusi gli interessi nazionali, assume un ruolo sempre più rilevante nella cybersecurity. Pertanto, la cybersecurity implica l'adozione di misure adeguate per proteggere la riservatezza, l'integrità e la disponibilità delle informazioni e delle tecnologie dell'informazione.

## 2. AMBITO DI APPLICAZIONE

La presente Guida è stata redatta per le PMI che fanno affidamento su asset tecnologici ed è applicabile a esse. Le relative linee guida possono essere facilmente adottate anche da altre tipologie di aziende, indipendentemente dalla loro dimensione o complessità.

Sulla base dei contenuti della ISO/IEC 27001, questa Guida descrive una serie di attività pratiche che possono contribuire in modo significativo a introdurre o ad accrescere il livello di sicurezza delle informazioni all'interno di una PMI. Ciò può supportare il business e favorire le opportunità di collaborazione nei mercati locali e dell'UE.

Tutte le attività elencate concorrono a garantire un ciclo di vita della sicurezza delle informazioni all'interno dell'azienda. Questo comprende la definizione, la pianificazione, l'implementazione, l'esercizio e il miglioramento di tutti i processi correlati, sulla base di una cultura del rischio e del miglioramento continuo.

# 3. GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI IN UNA PMI

## 3.1 FASE 1: DEFINIRE LE BASI DELLA SICUREZZA DELLE INFORMAZIONI

La gestione della sicurezza delle informazioni presenta numerose analogie con altre iniziative strategiche che un'azienda può intraprendere. Prima di avviare qualsiasi attività, è essenziale definirne l'ambito, la tempistica e il livello di coinvolgimento del personale. Fin dall'inizio, il top management e un esperto della materia dovrebbero essere coinvolti per stabilire le basi delle attività successive.

La prima fase richiede una chiara assunzione di responsabilità da parte del top management, che deve assicurarsi che siano definiti l'indirizzo e gli obiettivi dell'azienda in materia di sicurezza delle informazioni. L'Information Security Manager detiene la responsabilità operativa, mentre i responsabili dei sistemi e delle informazioni dovrebbero essere regolarmente aggiornati sullo stato di avanzamento delle attività. Di seguito viene fornita una descrizione dettagliata dei ruoli che, all'interno di una PMI, possono essere attribuiti a supporto della gestione sicura delle informazioni.

### 3.1.1 FASE 1.1: ASSEGNARE RUOLI E RESPONSABILITÀ

In ogni impresa e per ogni attività, è essenziale che ruoli e responsabilità siano attribuiti in modo chiaro ed appropriato. Le start-up o le piccole aziende spesso considerano la sicurezza delle informazioni come un processo autonomo, che non dipende dal loro coinvolgimento. Alcune finiscono persino per trascurarla del tutto.

Quando si decide di adottare misure per definire o rivedere la gestione della sicurezza delle informazioni all'interno di un'azienda, è importante definire e formalizzare ruoli e responsabilità prima di procedere oltre. Tutte le fasi successive riportano i "ruoli tipicamente coinvolti" con la relativa matrice RACI:

**R =** Responsible (Responsabile dell'esecuzione)

**A =** Accountable (Responsabile ultimo)

**C =** Consulted (Soggetto consultato)

**I =** Informed (Soggetto informato)

I principali ruoli e le relative responsabilità per la gestione della sicurezza delle informazioni sono generalmente descritti nel presente paragrafo. Si noti che nelle aziende più piccole più ruoli potrebbero essere attribuiti alla stessa persona o esternalizzati, con l'unica eccezione del top management.

Come requisito preliminare per l'applicazione della presente Guida, ogni azienda deve assegnare in modo specifico e formale i ruoli e le responsabilità in materia di sicurezza delle informazioni, coerentemente con la propria struttura e cultura organizzativa.

**Top management**

La responsabilità ultima della governance della sicurezza delle informazioni ricade sul top management, nell'ambito della governance complessiva dell'azienda. Il compito principale del top management consiste nel garantire che la sicurezza delle informazioni contribuisca al raggiungimento degli obiettivi aziendali, dimostrando l'allineamento con la creazione di valore dell'azienda, con una corretta gestione delle risorse e con adeguati sistemi di misurazione delle performance. Il top management non deve necessariamente conoscere ogni singolo asset dell'azienda, ma ci si attende che disponga di una visione di insieme degli asset critici e del loro valore per le attività aziendali.

A seconda della struttura organizzativa, il top management include tipicamente il Chief Executive Officer (CEO), il Chief Operating Officer (COO) o il consiglio di amministrazione. Ai fini della presente Guida, è necessario individuare chi debba assumere tali ruoli.

**IL PERSONALE ASSEGNATO AI DIVERSI RUOLI PER LA SICUREZZA DELLE INFORMAZIONI RILEVANTI ALL'INTERNO DELL'ORGANIZZAZIONE DOVREBBE METTERE PER ISCRITTO E FORMALMENTE RICONOSCERE LE PROPRIE RESPONSABILITÀ E I COMPITI ASSEGNATI.**

Una matrice RACI può aiutare a chiarire l'assegnazione delle responsabilità e può includere, ad esempio, le seguenti attività:

- Determinazione dei requisiti di sicurezza delle informazioni e loro classificazione;
- Esecuzione della valutazione del rischio;
- Definizione, implementazione e mantenimento delle misure di sicurezza;
- Accettazione del rischio residuo;
- Documentazione della sicurezza dei sistemi (norme, procedure, ecc.);
- Redazione e aggiornamento della politica di sicurezza;
- Monitoraggio della sicurezza dei sistemi;
- Piani di miglioramento della sicurezza;
- Piani di sensibilizzazione e formazione piani di continuità operativa.

Per ciascuna di queste attività, le seguenti responsabilità dovrebbero essere assegnate ai ruoli individuati:

- **Responsabile** (indicato come "R"), incaricato di svolgere l'attività. Dovrebbe esserci almeno una persona responsabile per ciascuna attività (che può delegarla per supporto);
- **Accountable** (indicato come "A"), incaricato di approvare il corretto completamento dell'attività;
- **Consultato** (indicato come "C"), il cui parere può essere richiesto per sviluppare le attività, in una comunicazione bidirezionale; tali soggetti sono generalmente considerati esperti;
- **Informato** (indicato come "I"), che viene tenuto aggiornato sull'avanzamento delle attività tramite una comunicazione unicamente unidirezionale.

**Comitato direttivo per la sicurezza delle informazioni**

In alcuni casi, le PMI possono istituire un comitato direttivo per la sicurezza delle informazioni composto da rappresentanti delle principali funzioni aziendali. È una buona pratica dotarsi di un regolamento del comitato, che funge principalmente da strumento per favorire il consenso tra i principali decisori. Il comitato per la sicurezza delle informazioni può operare in collaborazione con il top management ed è responsabile delle attività di audit e monitoraggio.

Nell'istituire un comitato direttivo per la sicurezza delle informazioni, è consigliabile coinvolgere le prime linee di riporto verso il top management e pianificare riunioni con cadenza trimestrale. Il comitato dovrebbe riunirsi per affrontare diverse tematiche relative alla sicurezza delle informazioni, quali:

- approvazione di norme e procedure di sicurezza;
- revisione dell'analisi dei rischi e del piano di trattamento dei rischi;
- risultati degli audit e azioni correlate;
- monitoraggio del piano di sicurezza delle informazioni;
- indicatori di obiettivi e performance della sicurezza delle informazioni;
- pianificazione di attività di sensibilizzazione e formazione;
- gestione delle emergenze.

**Responsabile/manager della sicurezza delle informazioni**

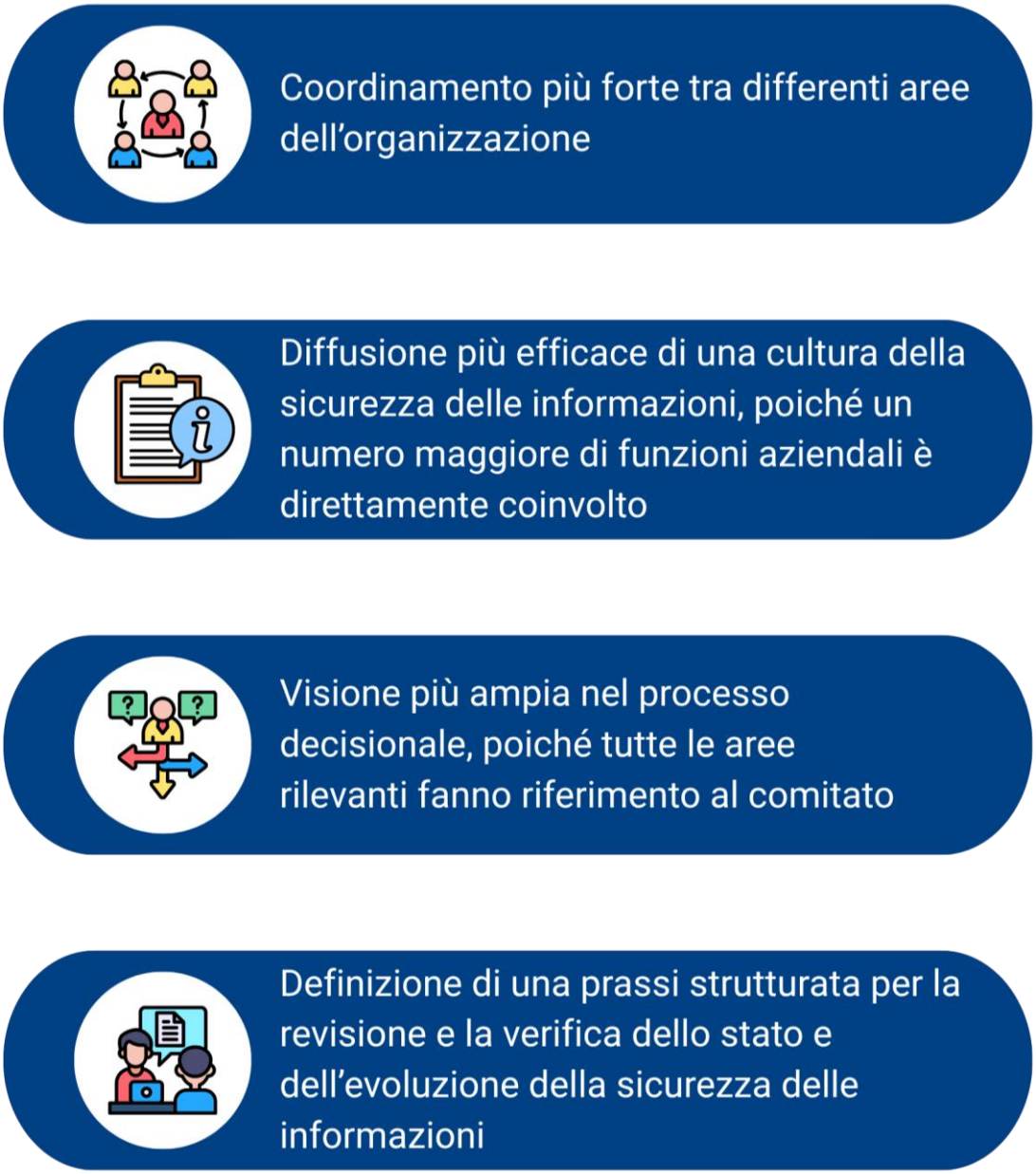
Anche se la sicurezza delle informazioni riguarda tutte le funzioni dell'organizzazione, è sempre più frequente la presenza di un responsabile della sicurezza delle informazioni incaricato di coordinare le attività pertinenti. Questo ruolo può essere ricoperto da una figura apicale (ad esempio IT Manager o Chief Technology Officer) con una buona conoscenza dei flussi informativi.

Poiché la sicurezza delle informazioni raramente è una competenza generale del management, il responsabile della sicurezza delle informazioni fornisce normalmente indicazioni al top management sugli aspetti principali prima dell'adozione di una strategia di sicurezza delle informazioni. Ottenere l'impegno del top management è una componente essenziale. Una attività chiave in tal senso è l'allineamento tra obiettivi di business e obiettivi di sicurezza delle informazioni. Altre responsabilità comprendono spesso: l'identificazione dei budget, l'utilizzo di modelli rischio/beneficio per la stima e il trattamento dei rischi, la redazione di politiche e procedure di sicurezza delle informazioni e la revisione dei risultati delle attività di monitoraggio.

Il responsabile della sicurezza delle informazioni è solitamente incaricato anche di promuovere la consapevolezza sulla sicurezza delle informazioni; ulteriori responsabilità possono includere la definizione dei canali di comunicazione e dei meccanismi di reporting. Il successo della sicurezza delle informazioni dipende in larga misura da una comunicazione efficace, sia interna sia esterna.

Il responsabile della sicurezza delle informazioni è una figura chiave nell'applicazione della presente Guida e dovrebbe essere selezionato in base alle competenze e all'esperienza maturate nel settore. Se la funzione è dedicata, il profilo può variare da Security Manager a Chief Information Security Officer (CISO). Ulteriori dettagli sui profili professionali e sulle competenze correlate sono disponibili nel documento CWA 16458 sui profili professionali ICT europei.

## VANTAGGI DELL'ISTITUZIONE DI UN COMITATO DIRETTIVO PER LA SICUREZZA DELLE INFORMAZIONI



**QUANDO SI ISTITUISCE UN COMITATO DIRETTIVO PER LA SICUREZZA DELLE INFORMAZIONI, OCCORRE CONSIDERARE I SEGUENTI ASPETTI**

- Ogni funzione aziendale dovrebbe essere rappresentata dall'appropriata autorità decisionale, al fine di evitare squilibri tra i diversi dipartimenti, nel caso in cui alcune aree non siano rappresentate dal proprio top management
- L'ordine del giorno delle riunioni dovrebbe essere pianificato e distribuito in anticipo
- Le riunioni dovrebbero essere svolte con periodicità (ad esempio ogni tre mesi) e in modo sistematico
- Dovrebbero essere definite regole di svolgimento delle riunioni, incluse eventuali decisioni su chi le presiede e su come risolvere potenziali conflitti
- Le decisioni rilevanti in materia di sicurezza delle informazioni dovrebbero essere assunte all'interno di questo comitato
- Le tempistiche pianificate dovrebbero essere rispettate

**Responsabili dei sistemi e delle informazioni**

Le organizzazioni più strutturate potrebbero dover individuare una serie di persone incaricate di svolgere attività quotidiane per proteggere i sistemi informativi sotto il loro controllo. Questi soggetti sono i *responsabili dei sistemi*. Parallelamente, i responsabili dei processi e dei dati dovrebbero essere coinvolti nella definizione dei requisiti di protezione delle informazioni, indipendentemente dai sistemi informativi. Questi soggetti sono i *responsabili delle informazioni*. Entrambe le categorie supportano l'organizzazione assicurando che i controlli di sicurezza delle informazioni siano in essere e funzionino in modo adeguato.

Normalmente i responsabili possono autorizzare modifiche agli asset di propria competenza, ad esempio miglioramenti dei sistemi o soluzioni operative semplificate. Tali decisioni devono sempre tenere conto degli impatti sulla sicurezza delle informazioni. Affinché il modello funzioni, è necessario chiarire formalmente chi siano i responsabili dei sistemi e delle informazioni all'interno dell'organizzazione. Ciò richiede almeno il coinvolgimento dell'IT Manager e del Chief Operating Officer (COO). Spesso le organizzazioni incontrano difficoltà nell'individuare responsabili dei sistemi e delle informazioni ai livelli più bassi della gerarchia manageriale, ossia le persone che decidono in merito a miglioramenti degli asset o a soluzioni operative semplificate. Questo richiede una delega decisionale chiara e una cultura organizzativa coerente.

**Personale**

Il successo della sicurezza delle informazioni dipende da una formazione e un'istruzione adeguate del personale. Dipendenti e collaboratori devono comprendere pienamente le ragioni del sistema di controlli adottato, in modo da mantenere il livello corretto di sicurezza delle informazioni senza comprometterlo.

Dipendenti e collaboratori devono essere in grado di riconoscere comportamenti anomali e segnalare tempestivamente eventuali preoccupazioni al responsabile della sicurezza delle informazioni, al fine di ridurre al minimo le perdite per l'organizzazione. Spesso dipendenti e collaboratori sono i principali bersagli degli attacchi. Quindi disporre di personale formato migliora sensibilmente l'ambiente complessivo di sicurezza delle informazioni e contribuisce allo sviluppo della cultura organizzativa. Questi dipendenti potrebbero anche essere in grado di trasformare quella conoscenza ed esperienza in una cultura organizzativa.

## 3.2 FASE 2: COMPRENDERE COSA DEVE ESSERE PROTETTO

A partire da questo capitolo, la Guida integra la descrizione di ciascuna attività suggerita per la gestione sicura delle informazioni all'interno di un'organizzazione con esempi (es. figure, tabelle, ecc.). Questi esempi aiuteranno il lettore a comprendere la Guida.

Prima di applicare qualsiasi misura di sicurezza delle informazioni, un'organizzazione deve avere una visione iniziale chiara di quali elementi abbiano realmente valore per essa.

Tali elementi, solitamente definiti asset, possono essere generalmente classificati come informazioni (Fase 2.1), tipicamente intangibili, oppure come altri asset (Fase 2.2), tipicamente tangibili.

L'obiettivo principale di questa attività è rappresentare gli asset chiave sotto il controllo dell'organizzazione che necessitano di protezione. Ciò è particolarmente importante per identificare le relazioni tra gli asset e definire le responsabilità.

Ruoli tipicamente coinvolti: top management (A), responsabili delle informazioni (C), responsabili dei sistemi (C), responsabile/manager della sicurezza delle informazioni (R).

### 3.2.1 FASE 2.1: IDENTIFICARE QUALI INFORMAZIONI VENGONO UTILIZZATE

È utile costruire una mappa degli asset partendo dagli asset intangibili, ossia le informazioni dell'organizzazione.

**Approccio top-down**

Un'organizzazione può adottare un approccio top-down, in cui le informazioni (riquadri bianchi sottostanti) vengono identificate lungo i flussi dei processi (riquadri colorati sottostanti).

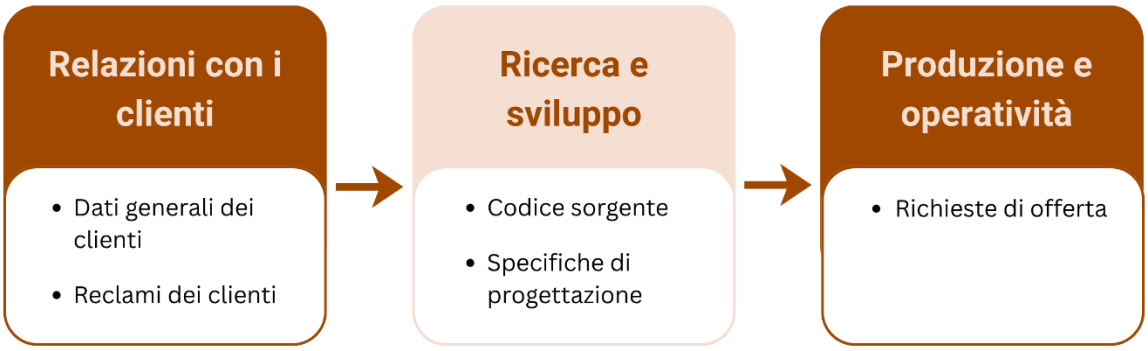



Figura 1: Esempio di mappa degli asset riferita a informazioni ipotetiche all'interno di un'organizzazione

Per un utilizzo efficace dell'approccio top-down, l'organizzazione deve avere una buona comprensione dei propri processi, ad esempio essere consapevole della loro natura e sapere chi è responsabile di ciascun processo. Il collegamento tra le attività e le informazioni dell'organizzazione può essere reso chiaro partendo da una visione d'insieme dei processi per poi scendere nel dettaglio fino agli asset informativi. I responsabili delle informazioni, di norma manager di funzione o di reparto, sono le figure più idonee a classificare e valutare la rilevanza di tali informazioni all'interno dell'organizzazione. È consigliabile effettuare brevi interviste con ciascun responsabile delle informazioni, al fine di ottenere una visione completa delle informazioni gestite dall'organizzazione.


**Approccio bottom-up**

L’approccio top-down richiede una buona conoscenza dei processi organizzativi, mentre ciò non è necessario per l’approccio bottom-up. Quest’ultimo può essere utilizzato da qualsiasi organizzazione, indipendentemente dal livello di maturità. Quando si implementa un approccio bottom-up, un punto di partenza ideale è darsi una risposta alla domanda *“Che tipo di informazioni tratta complessivamente l’organizzazione?”*. Questa domanda può essere rivolta alla persona/persone che hanno una visione d'insieme dell'organizzazione. Di seguito è riportato un semplice elenco per assicurarsi che tutti gli aspetti importanti siano stati presi in considerazione:

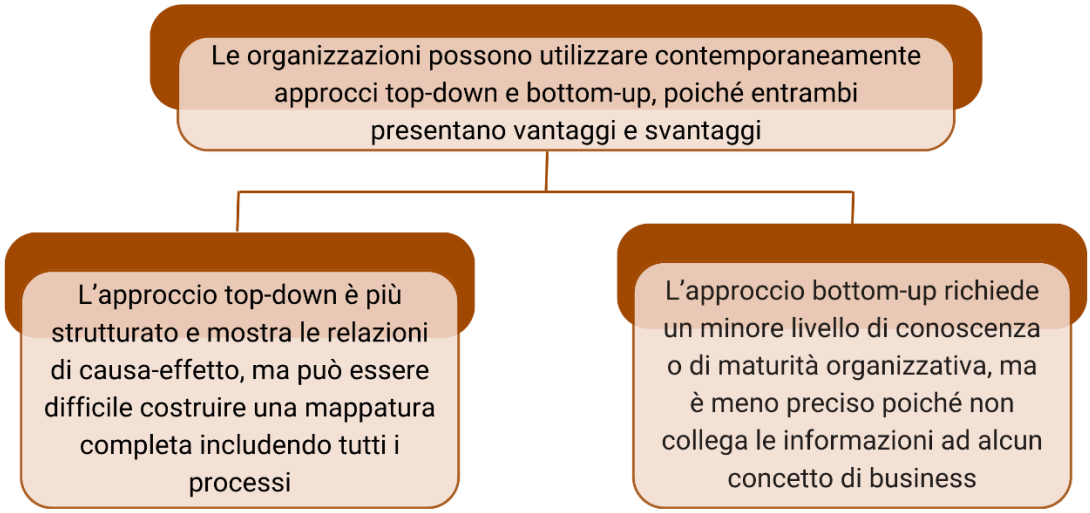
a) dati personali (es. nomi, indirizzi, codici fiscali, buste paga);

b) dati personali sensibili (es. diagnosi sanitarie, opinioni politiche, dati di pagamento);

c) dati strategici aziendali (es. piani di business, previsioni, budget);

d) dati di progetto/design (es. progettazione di prodotto, codice sorgente proprietario);

e) altri dati aziendali (es. dati di monitoraggio, statistiche di produzione, dati fiscali).




Dopo aver costruito la mappa degli asset, l'organizzazione dovrebbe avere una chiara comprensione degli asset informativi a livello concettuale, indipendentemente dai dispositivi utilizzati per conservarli o elaborarli.

### 3.2.2 FASE 2.2: IDENTIFICARE QUALI ALTRI ASSET VENGONO UTILIZZATI

Le informazioni identificate possono essere archiviate, elaborate o trasmesse mediante altri asset, in larga parte, ma non esclusivamente, tecnologici. Tali asset sono spesso componenti software eseguiti su sistemi informativi, ma possono comprendere anche documenti cartacei, dischi o servizi forniti da soggetti esterni. Per individuarli correttamente è generalmente necessario un approccio bottom-up, che coinvolga il personale IT e gli amministratori delle applicazioni, indipendentemente dal fatto che siano formalmente designati come responsabili dei sistemi. Si raccomanda di non trascurare gli asset chiave che rientrano almeno nelle seguenti categorie:

1) endpoint (laptop, desktop, tablet, smartphone), server e apparati;
2) software utente finale (escluse le suite per l'automazione d'ufficio e i sistemi operativi);
3) fornitori di servizi (compresi fornitori di forza lavoro, Housing/Hosting e Cloud);
4) personale (dipendenti diretti e personale esterno o subappaltato);
5) sedi fisiche (uffici e sale server di proprietà diretta).

Tali elementi possono essere esaminati inizialmente durante un'interazione top-down con i responsabili delle informazioni, come descritto nella fase precedente, subito dopo aver definito le informazioni relative ai processi, per poi essere perfezionati insieme ai responsabili dei sistemi.

Costruendo sull'esempio precedente, si può ottenere un elenco strutturato come il seguente:

| Software | Hardware | Personale | Fornitori | Sedi |
|---|---|---|---|---|
| Applicazioni CRM | Server di Produzione | Staff Interno | Fornitore Cloud | Uffici Principali |
| Applicazioni ERP | Server di Test | | Fornitore TLC | |
| Cartelle Condivise | Laptop | | | |
| | Smartphone | | | |

Figura 2: Esempio di mappa degli asset che identifica gli asset chiave diversi dalle informazioni all'interno di una determinata organizzazione

### 3.2.3 FASE 2.3: COMPRENDERE LA CONNESSIONE TRA INFORMAZIONI E ALTRI ASSET

Una volta identificati tutti gli asset chiave, stabilire quali asset supportano specifiche informazioni è un modo semplice ma efficace per comprendere cosa deve essere protetto e, successivamente, con quale livello di protezione. A tal fine, è possibile creare una matrice come quella sottostante. Qui le celle compilate indicano una relazione tra asset e informazioni; le celle bianche indicano che non c'è relazione.

| | Dati generali dei clienti | Reclami dei clienti | Codice sorgente | Specifiche di progettazione | Richieste di offerta |
|---|---|---|---|---|---|
| **Applicazione CRM** | x | x | | | |
| **Server di produzione** | x | x | | | x |
| **Server di test** | | | x | | |
| **Laptop** | x | x | x | x | x |
| **Smartphone** | x | x | | | |
| **Cartelle condivise** | | | | x | |
| **Applicazione ERP** | | | | | x |
| **Personale interno** | x | x | x | x | x |
| **Fornitore di servizi cloud** | x | x | | | x |
| **Fornitore di servizi TLC** | x | x | | | x |
| **Sedi principali** | x | x | x | x | x |

Tabella 1: Esempio di matrice per identificare la connessione tra informazioni e altri asset

Con tali relazioni chiaramente definite, la mappa degli asset risulta completa. Questa sarà di grande aiuto per le fasi successive. Naturalmente è possibile raccogliere ulteriori informazioni per ciascun asset fino a creare un inventario completo per gestirli meglio tutti. È importante ricordare che la mappa degli asset deve essere costantemente aggiornata, altrimenti perde rapidamente utilità.

## 3.3 FASE 3: VALUTARE I RISCHI PER LA SICUREZZA DELLE INFORMAZIONI

La valutazione dei rischi per la sicurezza delle informazioni ha l'obiettivo di individuare in anticipo ciò che potrebbe andare storto rispetto agli asset e avere un impatto negativo sui flussi di cassa, sugli obblighi legali o sulla reputazione di una determinata organizzazione. Questa fase è fondamentale per comprendere le minacce a cui l'organizzazione è esposta, in modo da poter implementare controlli adeguati per evitarle, contenerle o garantire il ripristino in caso si verifichino.

Attraverso la prioritizzazione dei rischi, ogni organizzazione può concentrare le proprie risorse difensive dove è più probabile che si verifichino le perdite maggiori, ottimizzando così l'efficacia complessiva di tali risorse.

**Ruoli tipicamente coinvolti:** top management/comitato direttivo per la sicurezza delle informazioni (A), responsabili delle informazioni (C), responsabili dei sistemi (C), responsabile della sicurezza delle informazioni (R).

### 3.3.1 FASE 3.1: COMPRENDERE IL VALORE DEGLI ASSET

Per rendere la mappa degli asset (vedi Fase 2.3) pienamente adeguata al processo di valutazione dei rischi, è necessario aggiungere un elemento chiave: una valutazione dell'importanza di ciascun asset all'interno dell'organizzazione.

Il modo più semplice per effettuare questa valutazione è partire dalle informazioni definite e considerare almeno due delle principali proprietà legate alla sicurezza delle informazioni: **disponibilità e riservatezza**. L'integrità può essere aggiunta, ma nei contesti più semplici può essere considerata strettamente correlata alla disponibilità. Dovrebbe essere effettuata una valutazione di base delle informazioni definite nella Fase 2.1, con ciascun responsabile delle informazioni che utilizza la seguente tabella come riferimento, assegnando un valore di disponibilità e riservatezza a ciascun elemento informativo identificato.

| | Valore basso | Valore alto |
|---|---|---|
| **Disponibilità (Av.)** | L'indisponibilità di queste informazioni potrebbe avere un impatto significativo sulle attività aziendali o sulla reputazione dell'organizzazione? | |
| | **No** | **Sì** |
| **Riservatezza (Conf.)** | La diffusione non autorizzata di queste informazioni potrebbe causare un danno competitivo rilevante all'organizzazione o violare leggi o obblighi contrattuali importanti? | |
| | **No** | **Sì** |

Tabella 2: Valutazione degli asset in termini di disponibilità e riservatezza

Applicando la tabella sopra riportata all'esempio, si potrebbero ottenere i seguenti valori:

| Dati generali dei clienti | Reclami dei clienti | Codice sorgente | Specifiche di progettazione | Richieste di offerta | Ordini di acquisto |
|---|---|---|---|---|---|
| Disp.: bassa<br>Ris.: alta | Disp.: bassa<br>Ris.: bassa | Disp.: bassa<br>Ris.: alta | Disp.: bassa<br>Ris.: alta | Disp.: alta<br>Ris.: bassa | Disp.: bassa<br>Ris.: alta |

Tabella 3: Esempio di valutazione delle informazioni in termini di disponibilità e riservatezza

Poiché tutti gli altri asset hanno il loro valore principale legato alle informazioni che memorizzano, elaborano o trasmettono, questa prima valutazione può essere estesa a tutti gli asset collegati alle informazioni valutate nella mappa degli asset. Ciò presuppone che la loro relazione con le informazioni con il valore più elevato determini il loro reale valore per l'organizzazione, come mostrato di seguito.

| | Dati generali clienti | Reclami clienti | Codice sorgente | Specifiche progettazione | Richieste di offerta | |
|---|---|---|---|---|---|---|
| | Disp.: bassa<br>Ris.: alta | Disp.: bassa<br>Ris.: bassa | Disp.: bassa<br>Ris.: alta | Disp.: bassa<br>Ris.: alta | Disp.: alta<br>Ris.: bassa | |
| **Applicazione CRM** | X | X | | | | Disp.: bassa<br>Ris.: alta |
| **Server di produzione** | X | X | | | X | Disp.: alta<br>Ris.: alta |
| **Server di test** | | | X | | | Disp.: bassa<br>Ris.: alta |
| **PC del personale** | X | X | X | X | X | Disp.: alta<br>Ris.: alta |
| **Smartphone del personale** | X | X | | | | Disp.: bassa<br>Ris.: alta |
| **Cartelle condivise** | | | | X | | Disp.: bassa<br>Ris.: alta |
| **Applicazione ERP** | | | | | X | Disp.: alta<br>Ris.: bassa |
| **Personale interno** | X | X | X | X | X | Disp.: alta<br>Ris.: alta |
| **Fornitore cloud** | X | X | | | X | Disp.: alta<br>Ris.: alta |
| **Fornitore TLC** | X | X | | | X | Disp.: alta<br>Ris.: alta |
| **Sedi principali** | X | X | X | X | X | Disp.: alta<br>Ris.: alta |

Tabella 4: Esempio di matrice per identificare in modo completo la relazione tra gli asset e la loro valutazione in termini di disponibilità e riservatezza

Questa mappa degli asset, completata e arricchita, indipendentemente da come venga rappresentata, fornisce una buona risposta alla domanda su cosa debba essere protetto in termini di sicurezza delle informazioni e in quale misura, in funzione del ruolo effettivo dell'asset.

Per valutare gli asset possono essere utilizzate diverse scale (ad esempio una valutazione basso/medio/alto). Per rendere l'analisi più approfondita, l'impatto può essere valutato tenendo in considerazione criteri aggiuntivi, quali:

- **Requisiti legali**
- **Interessi economici o commerciali**
- **Reputazione (immagine pubblica)**
- **Sicurezza**

### 3.3.2 FASE 3.2: VALUTARE IL CONTESTO IN CUI OPERA L'ORGANIZZAZIONE

Una comprensione approfondita dell'ambiente in cui opera l'organizzazione è di fondamentale importanza per definire i requisiti di sicurezza delle informazioni. ENISA, l'Agenzia dell'UE per la sicurezza delle reti e dell'informazione, ha sviluppato un modello di minacce informatiche: questo è utile per considerare tutte le minacce probabili a cui l'organizzazione è esposta. Il modello di ENISA prevede le seguenti categorie di minaccia:

a. Disastro (ad es. terremoto, alluvione, incendio);
b. Interruzione (ad es. sciopero, indisponibilità di servizi essenziali);
c. Attacco fisico (ad es. furto, sabotaggio);
d. Aspetti legali (ad es. violazione di normative, ordine del tribunale);
e. Danno non intenzionale (ad es. fuga di informazioni, smarrimento di un dispositivo);
f. Guasti/malfunzionamenti (ad es. guasto o malfunzionamento hardware);
g. Attività malevola/abuso (ad es. malware, social engineering, brute force);
h. Ascolto clandestino-intercettazione-dirottamento (ad es. spionaggio, attacco man-in-the-middle).

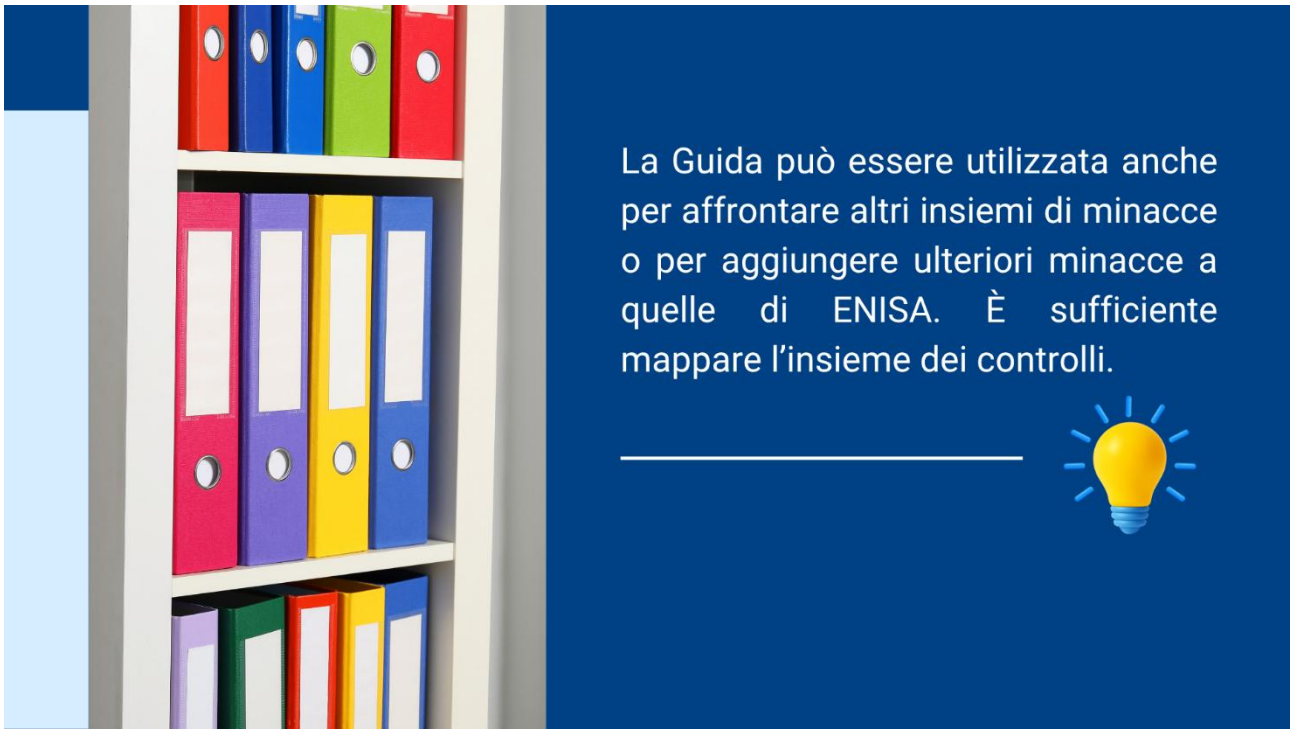
L'applicabilità di tali minacce dovrebbe essere valutata considerando i dati storici sugli incidenti (ove disponibili) e l'esperienza del personale. Una valutazione di questo tipo può almeno consentire di stabilire come, ad esempio, le seguenti condizioni si applichino all'ambiente dell'organizzazione:

1) Quanto sono esposti i locali dell'organizzazione a disastri naturali o incidenti (alluvioni, incendi, terremoti)?
2) Quanto sono esposti i locali dell'organizzazione a interruzioni di servizio (connessione Internet, mancanza di energia, scioperi)?
3) Quanto è affidabile il personale (basso turnover, assenza di tensioni, coesione del team)?
4) In che misura normative o requisiti contrattuali incidono sull'attività?
5) Quanto è esposta l'organizzazione agli errori umani del personale?
6) Quanto dipende il business da fornitori esterni?
7) In che misura i servizi ICT espongono l'organizzazione a Internet?
8) Quanto è importante la reputazione pubblica dell'organizzazione?

LE INFORMAZIONI E I RESPONSABILI DEGLI ASSET RILEVANTI PER RISPONDERE A TALI DOMANDE POSSONO ESSERE:

- **IT MANAGER** per le categorie di minaccia: danno non intenzionale, disastri, guasti/malfunzionamenti, interruzioni, ascolto clandestino-intercettazione-dirottamento, attività malevola/abuso;
- **SECURITY / FACILITY MANAGER** per le categorie di minaccia: attacchi fisici, disastri, guasti/malfunzionamenti;
- **LEGAL MANAGER** per la categoria di minaccia legale;
- **HUMAN RESOURCES MANAGER** per la categoria di minaccia relativa alle interruzioni.

Le risposte a tali domande (che possono tradursi in valori Alto/Basso/Nullo), ottenute consultando i responsabili delle informazioni e degli asset pertinenti, possono essere di grande aiuto nel determinare le minacce probabili a cui l'organizzazione sarà esposta, collegandosi direttamente (1 con a, 2 con b, ecc.) al modello di minacce informatiche di ENISA. Tali considerazioni dovrebbero essere mantenute separate dalle misure già in essere all'interno dell'organizzazione.




Tutte le minacce per le quali le relative domande sono state valutate diversamente da "Nullo", e che risultano applicabili a uno qualsiasi degli asset identificati come descritto nella seguente tabella, devono essere considerate come potenziali cause di rischio per l'organizzazione.

| | Disastro | Interruzioni | Attaco fisico | Aspetti legali | Danno non intenzionale | Gustati/ malf. | Arrività malevola/ abuso | Ascolto/ intercettazione/ dirottamento |
|---|---|---|---|---|---|---|---|---|
| **Hardware** | X | | X | | X | X | X | |
| **Software** | | | | X | X | X | X | X |
| **Fonitori di servizi** | | X | | X | | X | | X |
| **Personale** | X | X | | X | | | X | X |
| **Sedi fisiche** | X | | X | | | | | |

Tabella 5: Esempio di matrice per valutare il contesto in cui opera l'organizzazione

Ad esempio, se la risposta alla domanda 3) fosse "Basso", la corrispondente minaccia c) relativa agli attacchi fisici si applicherebbe agli asset hardware e alle sedi fisiche. Nell'esempio di mappa

degli asset (Figura 2), questi includerebbero server di produzione, server di test, PC del personale, smartphone aziendali e sedi principali.

### 3.3.3 FASE 3.3: IDENTIFICARE I CONTROLLI GIÀ IN ESSERE

I controlli di sicurezza delle informazioni sono gli elementi fondamentali incaricati di ridurre i rischi: se ben implementati, possono farlo in modo significativo. Diversi controlli sono spesso già presenti, ma sono numerosi e dovrebbero essere considerati non solo a livello organizzativo, ma, nella maggior parte dei casi, anche a livello di singolo asset, al fine di individuare eventuali carenze nelle misure di protezione.

L'Allegato A della norma ISO/IEC 27001 rappresenta un elenco significativo di controlli, concepito appositamente per consentire a un'organizzazione di effettuare una verifica di "completezza" dei controlli potenzialmente applicabili. Questo elenco è stato semplificato per l'applicazione alle PMI nell'Allegato A della presente Guida, mantenendo comunque il riferimento ai controlli originali dell'ISO/IEC 27001. Ogni controllo nell'elenco dovrebbe essere contrassegnato indicando se è già pienamente applicato o meno (le applicazioni parziali saranno considerate, in modo prudenziale, come non applicate) per ciascun gruppo di asset correlati a uno specifico elemento informativo.

## 3.4 FASE 4: PROGETTARE, APPLICARE E MONITORARE I CONTROLLI DI SICUREZZA DELLE INFORMAZIONI

Una volta che l'organizzazione è pienamente consapevole di cosa deve essere protetto e di come è attualmente protetto, è possibile prendere decisioni sui controlli da implementare ex novo o da migliorare. Il top management / comitato di indirizzo per la sicurezza delle informazioni dovrebbe valutare cosa deve essere fatto per affrontare ciascun rischio specifico, insieme alle tempistiche e ai finanziamenti per ogni soluzione. La maggior parte delle proposte proviene generalmente dal responsabile della sicurezza delle informazioni. Le misure di protezione selezionate dovrebbero essere efficaci ed efficienti in termini di costi.

**Ruoli tipicamente coinvolti**: top management / comitato di indirizzo per la sicurezza delle informazioni (A), responsabili delle informazioni (R), responsabili dei sistemi (R), personale (R), responsabile della sicurezza delle informazioni (R).

### 3.4.1 FASE 4.1: IDENTIFICARE I CONTROLLI E DEFINIRE UN PIANO DI SICUREZZA DELLE INFORMAZIONI

Decidere quali controlli implementare in uno specifico contesto è la decisione più complessa in tutto il campo della sicurezza delle informazioni. Nessuna combinazione di controlli è perfetta per ogni situazione, poiché ciò potrebbe comportare costi superiori al necessario, oltre alla creazione di numerosi controlli e alla gestione di incidenti non sempre facilmente prevedibili, e così via.

In linea con le fasi precedenti e secondo le buone pratiche di riferimento, questa Guida propone nel suo Allegato A la classificazione dei controlli in due principali categorie:

1) controlli di base, idealmente da implementare in ogni situazione;
2) controlli discrezionali, da utilizzare per proteggere asset di alto valore, soggetti a minacce probabili.

I controlli di base sono raggruppati nella prima sezione dell'Allegato A (A.1) e, salvo situazioni particolari, dovrebbero essere sempre implementati. L'Allegato X della presente Guida è proposto come esempio ideale di controllo di base: la politica di sicurezza delle informazioni. Una volta completato, questo documento dovrebbe essere formalmente approvato dal top management dell'organizzazione, al fine di definire correttamente priorità e risorse nel contesto organizzativo.

I controlli discrezionali sono raggruppati nella seconda sezione dell'Allegato A (A.2). In questa sezione, ciascun controllo è associato alle minacce che contribuisce a mitigare nella terza sezione dell'Allegato A (A.3). Se nella cella corrispondente alla minaccia, nella sezione A.3, non è presente alcun valore, significa che il controllo non la mitiga in modo significativo. Se è presente il valore "Secondario", significa che la mitiga in modo sensibile. Infine, se è presente il valore "Primario", significa che la mitiga in modo più efficace. Poiché ogni asset ha ricevuto un valore nella Fase 3.1 ed è stato associato alle minacce applicabili nella Fase 3.2, questi elementi possono essere utilizzati per decidere se applicare o meno un determinato controllo. Se un asset presenta un alto valore di riservatezza o disponibilità oppure è soggetto a una minaccia altamente probabile, dovrebbero essere applicati solo i controlli contrassegnati come "Primario" per quella specifica minaccia. Se invece un asset presenta sia un alto valore di riservatezza o disponibilità sia è esposto a una minaccia altamente probabile, allora è opportuno considerare anche i controlli contrassegnati come "Secondario" per quella specifica minaccia.

Ad esempio, gli smartphone del personale – la cui valutazione nella Tabella 4 è "Disp: bassa, Conf: alta" – sono asset hardware e quindi soggetti a una minaccia di attacco fisico classificata come "Bassa". Tutti i controlli che hanno una relazione "Primaria" con la minaccia di attacco fisico dovrebbero essere applicati agli smartphone del personale, oltre ai controlli di base. Ciò significa che:

- A2.06 Gestione dei supporti rimovibili;
- A2.10 Sicurezza fisica;
- A2.11 Protezione dalle minacce ambientali;
- A2.12 Manutenzione delle apparecchiature;

- A2.16 Backup.

La Guida può essere utilizzata anche quando si adottano fonti di controllo diverse da quelle presentate nell'Allegato A o quando vi si aggiungono altri controlli. In tal caso, l'insieme delle minacce deve essere nuovamente mappato.


Dovrebbe essere effettuata una verifica dei controlli applicati individuati nella fase precedente, insieme a quelli risultanti dalle tre categorie sopra menzionate, a livello di singolo asset. Qualora la situazione attuale evidenzi un controllo meno efficace rispetto a quanto raccomandato o la sua assenza, tale situazione dovrebbe essere annotata e ulteriormente analizzata. L'elenco di questi controlli costituisce la base per la costruzione di un Piano di Sicurezza delle Informazioni, che consentirà all'organizzazione di migliorare in modo selettivo la propria protezione. Il Piano di Sicurezza delle Informazioni dovrebbe includere più elementi rispetto a un semplice elenco di controlli. Ad esempio, potrebbe comprendere un insieme di azioni con i relativi responsabili, tempistiche, costi e altre informazioni. Può essere, in modo efficace, anche semplice come un foglio di calcolo con i seguenti campi:

| **Codice** | ID |
|---|---|
| **Fonte** | Attività di origine |
| **Descrizione dell'azione** | Testo descrittivo |
| **Responsabile** | Funzione o persona |
| **Causa** | Motivazione dell'attività |
| **Priorità** | Bassa |
| **Stato** | Aperta/Chiusa |
| **Avanzamento** | O%-100% |
| **Risorse** | Costi, personale |
| **Data di inizio** | gg/mm/aa |
| **Data di fine** | gg/mm/aa |
| **Note** | Altre annotazioni |

Tabella 6: Modello per il monitoraggio delle azioni da implementare nell'ambito di un Piano di Sicurezza delle Informazioni

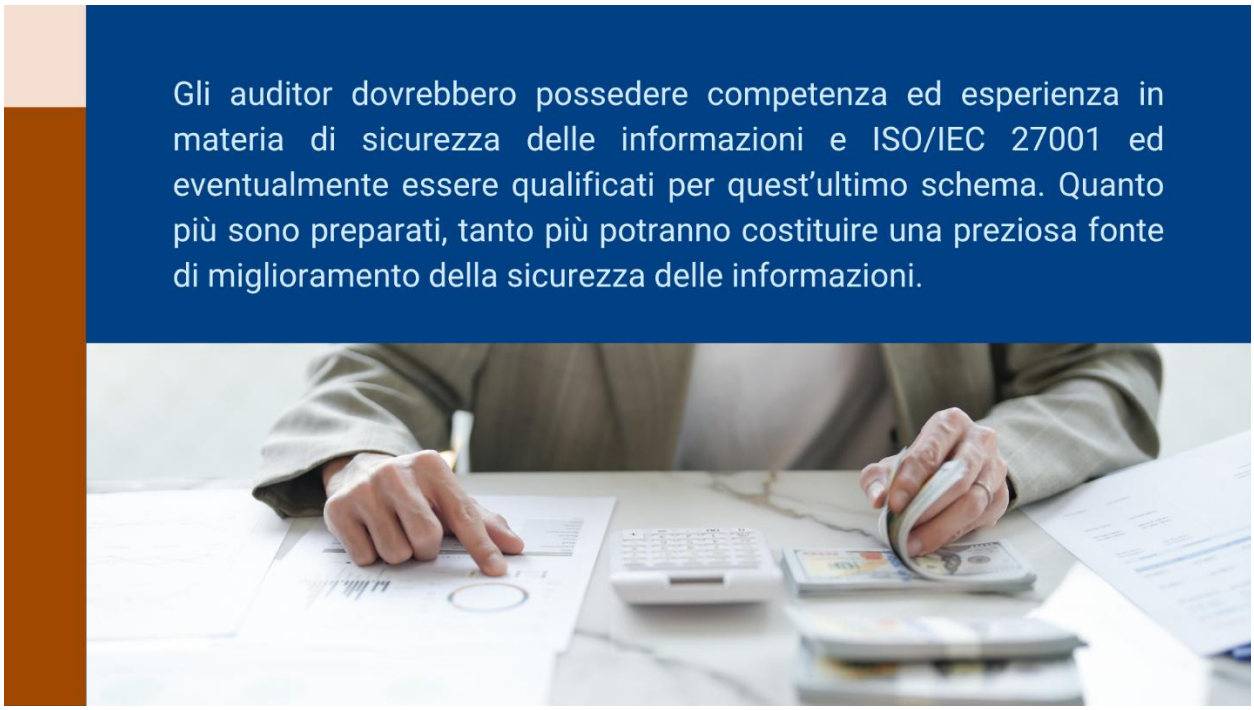
### 3.4.2 FASE 4.2: GESTIRE IL PIANO DI SICUREZZA DELLE INFORMAZIONI

Una volta approvato, il responsabile della sicurezza delle informazioni dovrebbe essere incaricato del monitoraggio periodico (ad esempio mensile o trimestrale), al fine di verificare che il Piano di Sicurezza delle Informazioni proceda correttamente e garantisca il massimo coinvolgimento possibile delle altre parti interessate. Questo monitoraggio dovrebbe essere svolto attraverso riunioni di un comitato formale (ad esempio il comitato di indirizzo per la sicurezza delle informazioni): tutti i professionisti coinvolti dovrebbero riferire sui propri progressi, sulle difficoltà incontrate e sulle eventuali modifiche da apportare al piano. Il piano dovrebbe essere aggiornato di conseguenza e, nel caso vengano introdotte modifiche significative che richiedano nuove risorse, dovrebbe essere nuovamente sottoposto all'approvazione del top management. Se invece non venissero apportate modifiche rilevanti, il piano dovrebbe comunque essere riapprovato periodicamente dal top management (almeno una volta all'anno, possibilmente prima della finalizzazione dei budget dell'anno successivo, per consentire una corretta allocazione delle risorse).

Il piano dovrebbe inoltre includere i risultati delle nuove azioni suggerite o comunque richieste dalle attività svolte nella successiva Fase 4.3.

### 3.4.3 FASE 4.3: CONTROLLARE LA SICUREZZA DELLE INFORMAZIONI

Un modo efficace per verificare se la sicurezza delle informazioni è mantenuta correttamente consiste nel pianificare e svolgere audit di sicurezza delle informazioni, almeno una volta all'anno. Gli auditor dovrebbero essere scelti tra esperti imparziali della materia e incaricati di verificare la conformità dei processi di sicurezza delle informazioni ai requisiti interni ed esterni. Se l'audit è svolto da personale interno, l'auditor non deve avere responsabilità operative nella gestione della sicurezza delle informazioni, così da evitare conflitti di interesse.




A seguito dell'audit, il top management dell'organizzazione dovrà ricevere un rapporto contenente:

- Non conformità, ovvero gli aspetti in cui l'organizzazione non rispetta lo standard;
- Opportunità di miglioramento, ossia raccomandazioni per operare in modo più sicuro (pur in presenza di conformità allo standard).

Le non conformità dovranno essere attentamente analizzate e dovranno essere implementate le azioni necessarie, così da evitarne il ripetersi in futuro. Tali azioni dovranno essere incluse in una versione aggiornata del Piano di Sicurezza delle Informazioni, insieme alle azioni necessarie per correggere le non conformità. Le opportunità di miglioramento dovranno essere valutate e, se ritenute pertinenti, incluse nel Piano di Sicurezza delle Informazioni, solitamente con una priorità meno stringente rispetto alle azioni volte a gestire le non conformità.

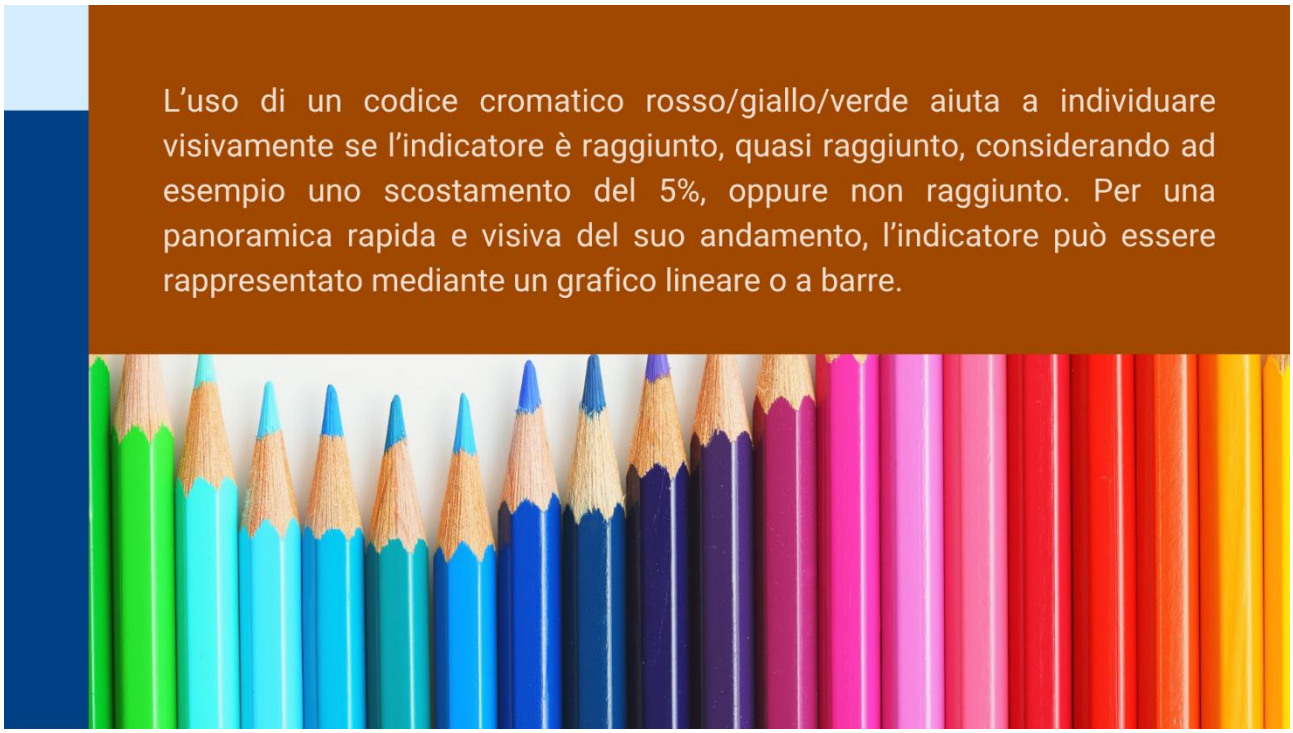
### 3.4.4 FASE 4.4: MONITORARE LA SICUREZZA DELLE INFORMAZIONI

Una volta definite e progettate le misure di protezione incluse nel passaggio precedente, l'organizzazione può tornare alla normale operatività. Per garantire l'efficacia del sistema, le attività di monitoraggio contribuiranno a limitare le deviazioni rispetto al Piano di Sicurezza delle Informazioni iniziale.

Il modo più pratico per svolgere le attività di monitoraggio consiste nell'elaborare indicatori di obiettivo o di prestazione semplici ma efficaci, da aggiornare periodicamente. Indicatori di questo tipo possono essere basati su obiettivi o controlli: si tratta essenzialmente di formule per calcolare soglie che, una volta superate o raggiunte, devono attivare determinate azioni. È importante

assegnare la responsabilità dell'applicazione periodica della formula dell'indicatore. La norma ISO/IEC 27004 può essere d'ausilio nello sviluppo di questa attività.

Gli indicatori di obiettivo sono i più semplici da impostare. Possono essere utilizzati per misurare il raggiungimento di un obiettivo rilevante per l'organizzazione, come l'ottenimento della conformità alla presente guida o a una normativa/standard pertinente, un livello o uno stato di servizio correlato alla sicurezza. Dovranno essere verificati ogni pochi mesi.




Gli indicatori di prestazione possono essere correlati ai risultati dei processi di sicurezza delle informazioni, ad esempio la valutazione del rischio, oppure all'efficacia dei controlli. In quest'ultimo caso, i controlli di base proposti nella Fase 3.1 possono essere associati a indicatori come quelli riportati di seguito:

| Controllo | Formula dell'indicatore | Target | Periodicità |
|---|---|---|---|
| Policy di sicurezza delle informazioni | % di dipendenti che hanno ricevuto la policy | 100% | annuale |
| Organizzazione della sicurezza delle informazioni | # di riunioni del comitato direttivo per la sicurezza delle informazioni | 4 | annuale |
| Consapevolezza, formazione e addestramento | % di dipendenti che hanno ricevuto formazione, # di | 100% | annuale |

| | | | |
|---|---|---|---|
| sulla sicurezza delle informazioni | iniziative di sensibilizzazione sulla sicurezza | | |
| Inventario degli asset | % di asset inclusi nell'inventario entro 1 mese dall'acquisizione | 100% | trimestrale |
| Protezione da malware | # di workstation infette / workstation ripristinate | 1 | mensile |
| Patching delle vulnerabilità software | # di patch di sicurezza critiche non ancora applicate | 0 | mensile |
| Sicurezza nei contratti con i fornitori | % di contratti con clausole di sicurezza delle informazioni specificate | 100% | trimestrale |
| Gestione degli incidenti | # di incidenti di sicurezza delle informazioni chiusi / incidenti aperti nello stesso giorno | 95% | mensile |

Tabella 7: Periodicità suggerita per il monitoraggio dei controlli

Questi sono solo alcuni esempi di base. Ogni organizzazione dovrà determinare in modo coerente i propri indicatori. Tali indicatori, che possono essere monitorati in un semplice foglio di calcolo, potranno essere esaminati periodicamente dal responsabile/manager della sicurezza delle informazioni o presentati al comitato direttivo per la sicurezza delle informazioni.

Per ogni target dovranno essere fissate scadenze da rispettare. Le altre soglie possono variare nel tempo ed essere inizialmente impostate a un valore inferiore al target, aumentando con la maturazione del processo o del controllo interessato. Il comitato direttivo per la sicurezza delle informazioni potrà monitorare periodicamente lo stato e lo sviluppo della gestione della sicurezza delle informazioni.

# 4. CERTIFICAZIONE ISO/IEC 27001

L'approccio finora suggerito è strettamente correlato ai requisiti della norma ISO/IEC 27001, come indicato nella seguente tabella di corrispondenza. Laddove non vi sia corrispondenza tra lo standard internazionale e la presente Guida, ciò è dovuto all'approccio semplificato adottato dagli autori della Guida: tale approccio mira a eliminare gli aspetti più formali e metodologici, concentrandosi su quelli più pratici.

| ISO/IEC 27001:2013 capitoli principali | | Fase della Guida Digital SME |
|---|---|---|
| 4.1 | Comprensione del contesto dell'organizzazione | Fase 3 |
| 4.2 | Comprensione delle esigenze e delle aspettative delle parti interessate | Fase 2 |
| 4.3 | Determinazione del campo di applicazione del sistema di gestione della sicurezza delle informazioni | N/A |
| 4.4 | Sistema di gestione della sicurezza delle informazioni | N/A |
| 5.1 | Leadership e impegno | N/A |
| 5.2 | Policy | *Controllo di base A1.01* |
| 5.3 | Ruoli, responsabilità e autorità organizzative | Fase 1 |
| 6.1 | Azioni per affrontare rischi e opportunità | Fase 2 Fase 3 |
| 6.2 | Obiettivi di sicurezza delle informazioni e piani per conseguirli | N/A |
| 7.1 | Risorse | N/A |
| 7.2 | Competenza | N/A |
| 7.3 | Consapevolezza | *Controllo di base A1.03* |
| 7.4 | Comunicazione | *Controllo discrezionale A2.01* |
| 7.5 | Informazioni documentate | N/A |
| 8.1 | Pianificazione e controllo operativi | Fase 4 |
| 8.2 | Valutazione del rischio per la sicurezza delle informazioni | Fase 2<br>Fase 3 |
| 8.3 | Trattamento del rischio per la sicurezza delle informazioni | Fase 4 |
| 9.1 | Monitoraggio, misurazione, analisi e valutazione | Fase 4 |
| 9.2 | Audit interno | Fase 4 |

| | | |
|---|---|---|
| 9.3 | Riesame della direzione | |
| 10.1 | Non conformità e azione correttiva | Fase 4 |
| 10.2 | Miglioramento continuo | |

Tabella 8: Contenuti principali della norma ISO/IEC 27001:2013

Ciononostante, qualora una certificazione formale secondo la norma ISO/IEC 27001 diventasse un obiettivo da perseguire dopo che la gestione della sicurezza delle informazioni sia stata condotta per un certo periodo sulla base di questa Guida, sarà necessario affrontare tutti i casi senza corrispondenza. Più nello specifico, le seguenti attività aggiuntive dovranno essere eseguite dopo la Fase 1.1, come illustrato nel capitolo 3.

### 4.1.1 FASE 4.1: ISTITUIRE IL SISTEMA DI GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI (SGSI)

Un Sistema di Gestione della Sicurezza delle Informazioni (SGSI) dovrebbe essere considerato un approccio più formale alla gestione della sicurezza delle informazioni rispetto a quello descritto nella presente Guida. Un SGSI comprende policy, procedure, linee guida, risorse e attività collegate, gestite collettivamente dall'organizzazione al fine di proteggere le proprie informazioni. Il top management dovrà essere direttamente coinvolto nella pianificazione di un SGSI, che introduce maggiori formalità ma consente anche di avanzare verso una certificazione riconosciuta a livello internazionale per una parte dell'organizzazione. Nella selezione di tale parte occorrerà prestare attenzione, poiché la sua estensione inciderà direttamente sui costi di certificazione. La scelta di certificare l'intera organizzazione è percorribile, ma non l'unica possibile, in quanto è possibile dare priorità a servizi o processi chiave in linea con le strategie aziendali dell'organizzazione. Si noti che è anche possibile certificare una sola parte di un SGSI più ampiamente consolidato.

Il coinvolgimento precoce del top management sarà fondamentale nella definizione del perimetro, nonché per ottenere un impegno (e le conseguenti risorse) aggiuntivo da utilizzare nei passaggi successivi. I progressi nell'implementazione dovranno essere comunicati regolarmente, con scadenze fissate per la stessa.

In questa fase dovranno essere proposti e selezionati obiettivi misurabili e correlati al business. Tali obiettivi, come tutto il resto del SGSI, dovranno essere sempre orientati al miglioramento continuo, iterazione dopo iterazione.

### 4.1.2 ALTRI ELEMENTI

L'approccio alla gestione documentale, da adottare nell'ambito di un SGSI formale (e di qualsiasi sistema di gestione), richiede inoltre che ogni documento prodotto:

- rechi i metadati completi (titolo, data, autore come requisiti minimi);
- sia redatto secondo formati e modelli stabiliti;
- sia soggetto al controllo delle modifiche/versioni;
- sia distribuito ai destinatari previsti.

Dovrà essere prodotta e mantenuta aggiornata una Dichiarazione di Applicabilità ai sensi del requisito 6.1.3 d) della norma ISO/IEC 27001. Il modello proposto per la selezione dei controlli nella presente Guida è un buon punto di partenza, ma dovrà includere almeno la giustificazione dell'inclusione o dell'esclusione di ciascun controllo.

Dovrà essere eseguito periodicamente anche un riesame formale della direzione, che includa tutti gli elementi di input specificati nel requisito 9.3 della norma ISO/IEC 27001. Dovrà seguire lo stesso approccio suggerito nella Fase 3.2, ma dovrà essere anche messo per iscritto.

Potrà essere aggiunta anche l'attività formale di certificazione da parte di terzi, da condurre con le stesse modalità di un audit interno, avvalendosi però di una visione esterna e competente sul SGSI.

# 5. RIFERIMENTI E RISORSE LIBERAMENTE ACCESSIBILI

## RIFERIMENTI

- Famiglia ISO/IEC 27000 – Sistemi di gestione della sicurezza delle informazioni. Disponibile online all'indirizzo: https://www.iso.org/isoiec-27001-information-security.html

## RISORSE LIBERAMENTE ACCESSIBILI

- BSI. ISO/IEC 27001 per le piccole e medie imprese (PMI). Disponibile online all'indirizzo: https://www.bsigroup.com/en-GB/iso-27001-information-security/ISO-27001-for-SMEs/
- Centre for Cyber Security Belgium. Guida alla sicurezza informatica per le PMI. Disponibile online all'indirizzo: https://cybersecuritycoalition.be/resource/cyber-security-guide-sme/
- ETSI. Implementazione della Direttiva riveduta sulla sicurezza delle reti e dei sistemi informativi (NIS2) applicando i controlli di sicurezza critici – ETSI TS 103 992 – rapporto tecnico pubblicato dal comitato tecnico ETSI sulla Cybersecurity (TC CYBER).

Disponibile online all'indirizzo: https://www.etsi.org/deliver/etsi_ts/103900_103999/103992/01.01.01_60/ts_103992v010101p.pdf

- ISO. Standard liberamente accessibili (incluso ISO/IEC 27000). Disponibile online all'indirizzo: https://www.iso.org/sectors/security-safety-risk
- ENISA. Standard per la gestione del rischio. Disponibile online all'indirizzo: https://www.enisa.europa.eu/sites/default/files/publications/O.7.2-T2-Risk_Management_standards.pdf
- ENISA. Cybersecurity per le PMI – Sfide e raccomandazioni. Disponibile online all'indirizzo: https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes
- ENISA. Guida alla cybersecurity per le PMI – 12 passi per mettere in sicurezza la tua azienda. Disponibile online all'indirizzo: https://www.enisa.europa.eu/publications/cybersecurity-guide-for-smes

# ALLEGATO A

## A.1 CONTROLLI DI BASE

| ID | Nome del controllo | Rif. Allegato A ISO/IEC 27001 | Descrizione del controllo e linee guida |
|---|---|---|---|
| 01 | Policy per la sicurezza delle informazioni | 5.1 | Dovranno essere definite, approvate dalla direzione, pubblicate, comunicate e riconosciute dal personale rilevante e dalle parti interessate rilevanti, e riesaminate ad intervalli pianificati e in caso di cambiamenti significativi, policy di sicurezza delle informazioni e policy specifiche per argomento.<br><br>Frequenza di revisione suggerita: annuale |
| 02 | Ruoli e responsabilità per la sicurezza delle informazioni Separazione dei compiti | 5.2<br>5.3 | I ruoli e le responsabilità in materia di sicurezza delle informazioni dovranno essere definiti e assegnati in base alle esigenze dell'organizzazione. I compiti e le aree di responsabilità in conflitto dovranno essere separati.<br><br>Frequenza di revisione suggerita: annuale |
| 03 | Consapevolezza, formazione e addestramento sulla sicurezza delle informazioni | 6.3 | Il personale dell'organizzazione e le parti interessate rilevanti dovranno ricevere un'adeguata consapevolezza, formazione e addestramento sulla sicurezza delle informazioni, nonché aggiornamenti periodici sulle policy di sicurezza delle informazioni, le policy specifiche per argomento e le procedure dell'organizzazione, in relazione alla propria funzione lavorativa.<br><br>Frequenza di formazione suggerita: annuale |
| 04 | Inventario degli asset Uso accettabile degli asset Restituzione degli asset Classificazione delle informazioni | 5.9<br>5.10<br>5.11<br>5.12 | Dovrà essere sviluppato e mantenuto un inventario delle informazioni e degli altri asset associati, comprensivo dei rispettivi proprietari.<br><br>Dovranno essere identificate, documentate e implementate le regole per l'utilizzo accettabile e le procedure per la gestione delle informazioni e degli altri asset associati.<br><br>Il personale e le altre parti interessate, se del caso, dovranno restituire tutti gli asset dell'organizzazione in loro possesso al momento della cessazione o della modifica del rapporto di lavoro, del contratto o dell'accordo.<br><br>Le informazioni dovranno essere classificate in base alle esigenze di sicurezza delle informazioni dell'organizzazione, tenendo conto di riservatezza, |

| | | | |
|---|---|---|---|
| | | | integrità, disponibilità e dei requisiti delle parti interessate rilevanti.<br><br>Frequenza di revisione suggerita: mensile |
| 05 | Classificazione delle informazioni<br>Etichettatura delle informazioni<br>Trattamento delle informazioni | 5.12<br><br>5.13<br><br>5.14 | Le informazioni dovranno essere classificate in base alle esigenze di sicurezza delle informazioni dell'organizzazione, tenendo conto di riservatezza, integrità, disponibilità e dei requisiti delle parti interessate rilevanti.<br><br>Dovrà essere sviluppato e implementato un appropriato insieme di procedure per l'etichettatura delle informazioni, in conformità con lo schema di classificazione adottato dall'organizzazione.<br><br>Dovranno essere in vigore regole, procedure o accordi per il trasferimento delle informazioni, per tutti i tipi di strutture di trasferimento all'interno dell'organizzazione e tra l'organizzazione e soggetti esterni.<br><br>Frequenza di revisione suggerita: annuale |
| 06 | Gestione delle identità<br>Informazioni di autenticazione | 5.16<br><br>5.17 | Dovrà essere gestito l'intero ciclo di vita delle identità.<br><br>L'assegnazione e la gestione delle informazioni di autenticazione dovranno essere controllate tramite un processo di gestione, che includa la formazione del personale sulla corretta gestione delle informazioni di autenticazione.<br><br>Frequenza di revisione suggerita: al verificarsi di cambiamenti organizzativi |
| 07 | Diritti di accesso<br>Diritti di accesso privilegiato | 5.18<br><br>8.2 | I diritti di accesso alle informazioni e agli altri asset associati dovranno essere assegnati, riesaminati, modificati e revocati in conformità con la policy specifica e le regole di controllo degli accessi dell'organizzazione.<br><br>L'assegnazione e l'utilizzo dei diritti di accesso privilegiato dovranno essere limitati e gestiti.<br><br>Frequenza di revisione suggerita: al verificarsi di cambiamenti organizzativi |
| 08 | Informazioni di autenticazione | 5.17 | L'assegnazione e la gestione delle informazioni di autenticazione dovranno essere controllate tramite un processo di gestione, che includa la formazione del personale sulla corretta gestione delle informazioni di autenticazione.<br><br>Frequenza di revisione suggerita: al verificarsi di cambiamenti organizzativi |

| | | | |
|---|---|---|---|
| 09 | Monitoraggio della sicurezza fisica Protezione da minacce fisiche e ambientali Desk libero e schermo libero | 7.4<br>7.5<br>7.7 | I locali dovranno essere continuamente monitorati per individuare accessi fisici non autorizzati.<br>Dovrà essere progettata e implementata la protezione contro minacce fisiche e ambientali, quali calamità naturali e altre minacce fisiche intenzionali o non intenzionali all'infrastruttura.<br>Frequenza di revisione suggerita: mensile |
| 10 | Protezione da malware | 8.7 | Dovrà essere implementata la protezione da malware, supportata da un'adeguata sensibilizzazione degli utenti.<br>Frequenza di revisione suggerita: mensile |
| 11 | Responsabilità della direzione | 5.4 | La direzione dovrà richiedere a tutto il personale di applicare la sicurezza delle informazioni in conformità con la policy di sicurezza delle informazioni, le policy specifiche per argomento e le procedure stabilite dall'organizzazione.<br>Frequenza di revisione suggerita: mensile |
| 12 | Gestione delle vulnerabilità tecniche | 8.8 | Dovranno essere ottenute informazioni sulle vulnerabilità tecniche dei sistemi informativi in uso, dovrà essere valutata l'esposizione dell'organizzazione a tali vulnerabilità e dovranno essere adottate le misure appropriate.<br>Frequenza di revisione suggerita: mensile |
| 13 | Sicurezza delle reti Sicurezza dei servizi di rete | 8.20<br>8.21 | Le reti e i dispositivi di rete dovranno essere protetti, gestiti e controllati per tutelare le informazioni nei sistemi e nelle applicazioni.<br>I meccanismi di sicurezza, i livelli di servizio e i requisiti dei servizi di rete dovranno essere identificati, implementati e monitorati.<br>Frequenza di revisione suggerita: mensile |
| 14 | Sicurezza delle informazioni nei rapporti con i fornitori Inserimento della sicurezza delle informazioni negli accordi con i fornitori | 5.19<br>5.20 | Dovranno essere definiti e implementati processi e procedure per gestire i rischi per la sicurezza delle informazioni associati all'utilizzo di prodotti o servizi dei fornitori.<br>I requisiti di sicurezza delle informazioni rilevanti dovranno essere stabiliti e concordati con ciascun fornitore in base alla tipologia del rapporto con il fornitore stesso.<br>Frequenza di revisione suggerita: annuale |

| | | | |
|---|---|---|---|
| 15 | Gestione degli incidenti di sicurezza delle informazioni<br>Pianificazione e preparazione<br>Valutazione e decisione sugli eventi di sicurezza delle informazioni<br>Risposta agli incidenti di sicurezza delle informazioni<br>Apprendimento dagli incidenti di sicurezza delle informazioni | 5.24<br>5.25<br>5.26<br>5.27 | L'organizzazione dovrà pianificare e prepararsi alla gestione degli incidenti di sicurezza delle informazioni, definendo, stabilendo e comunicando processi, ruoli e responsabilità per la gestione degli incidenti.<br>L'organizzazione dovrà valutare gli eventi di sicurezza delle informazioni e decidere se classificarli come incidenti di sicurezza delle informazioni.<br>Gli incidenti di sicurezza delle informazioni dovranno essere gestiti in conformità con le procedure documentate.<br>Le conoscenze acquisite dagli incidenti di sicurezza delle informazioni dovranno essere utilizzate per rafforzare e migliorare i controlli di sicurezza delle informazioni.<br>Frequenza di revisione suggerita: al verificarsi di cambiamenti organizzativi |
| 16 | Requisiti legali, normativi e contrattuali<br>Diritti di proprietà intellettuale | 5.31<br>5.32 | I requisiti legali, normativi, regolamentari e contrattuali rilevanti per la sicurezza delle informazioni e l'approccio dell'organizzazione per soddisfarli dovranno essere identificati, documentati e mantenuti aggiornati.<br>L'organizzazione dovrà implementare procedure appropriate per proteggere i diritti di proprietà intellettuale.<br>Frequenza di revisione suggerita: annuale |

## A.2 CONTROLLI DISCREZIONALI

| ID | Nome del controllo | ISO/IEC 27001<br><br>Rif. Allegato A | Descrizione del controllo e linee guida |
|---|---|---|---|
| 01 | Contatti con le autorità<br><br>Contatti con gruppi di interesse speciale | 5.5<br><br>5.6 | L'organizzazione deve stabilire e mantenere contatti con le autorità competenti.<br><br>L'organizzazione deve stabilire e mantenere contatti con gruppi di interesse speciale o con altri forum specialistici sulla sicurezza e associazioni professionali. |
| 02 | Lavoro da remoto | 6.7 | Devono essere implementate misure di sicurezza quando il personale lavora da remoto, al fine di proteggere le informazioni a cui si accede, trattate o archiviate al di fuori delle sedi dell'organizzazione. |
| 03 | Inventario delle informazioni e degli altri asset associati<br><br>Uso accettabile delle informazioni e degli altri asset associati<br><br>Restituzione degli asset | 5.9<br><br>5.10<br><br>5.11 | Deve essere sviluppato e mantenuto un inventario delle informazioni e degli altri asset associati, inclusi i relativi proprietari.<br><br>Devono essere individuate, documentate e implementate regole per l'uso accettabile e procedure per la gestione delle informazioni e degli altri asset associati.<br><br>Il personale e le altre parti interessate, ove appropriato, devono restituire tutti gli asset dell'organizzazione in loro possesso in caso di modifica o cessazione del rapporto di lavoro, del contratto o dell'accordo. |
| 04 | Verifiche preliminari | 6.1 | Devono essere effettuate verifiche preliminari su tutti i candidati che devono entrare a far parte del personale, prima del loro ingresso nell'organizzazione e su base continuativa, tenendo conto delle leggi applicabili, delle normative e dei principi etici, e in modo proporzionato ai requisiti di business, alla classificazione delle informazioni a cui si accederà e al rischio percepito. |

| ID | Nome del controllo | ISO/IEC 27001<br><br>Rif. Allegato A | Descrizione del controllo e linee guida |
|---|---|---|---|
| 05 | Termini e condizioni di impiego.<br><br>Sensibilizzazione, istruzione e formazione sulla sicurezza delle informazioni. | 6.2<br>6.3 | Gli accordi contrattuali di lavoro devono indicare le responsabilità del personale e dell'organizzazione in materia di sicurezza delle informazioni.<br><br>Il personale dell'organizzazione e le parti interessate rilevanti devono ricevere adeguata consapevolezza, istruzione e formazione sulla sicurezza delle informazioni, nonché aggiornamenti periodici sulla politica di sicurezza delle informazioni dell'organizzazione e sulle policy e procedure specifiche pertinenti alla loro funzione lavorativa. |
| 06 | Supporti di archiviazione | 7.1 | I supporti di archiviazione devono essere gestiti durante tutto il loro ciclo di vita - acquisizione, utilizzo, trasporto e smaltimento - in conformità con lo schema di classificazione dell'organizzazione e con i requisiti di gestione applicabili. |
| 07 | Smaltimento sicuro o riutilizzo delle apparecchiature | 7.14 | Gli elementi dell'apparecchiatura contenenti supporti di memorizzazione devono essere verificati per assicurare che eventuali dati sensibili e software con licenza siano stati rimossi o sovrascritti in modo sicuro prima dello smaltimento o del riutilizzo. |
| 08 | Controllo degli accessi | 5.15 | Devono essere stabilite e implementate regole per controllare l'accesso fisico e logico alle informazioni e agli altri asset associati, sulla base dei requisiti di business e di sicurezza delle informazioni. |
| 09 | Uso della crittografia | 8.24 | Devono essere definite e implementate regole per l'uso efficace della crittografia, inclusa la gestione delle chiavi crittografiche. |
| 10 | Perimetri di sicurezza fisica.<br><br>Accesso fisico<br><br>Messa in sicurezza di uffici, locali e strutture. | 7.1<br>7.2<br>7.3<br>7.4 | Devono essere definiti e utilizzati perimetri di sicurezza per proteggere le aree che contengono informazioni e altri asset associati.<br><br>Le aree sicure devono essere protette da controlli di ingresso e punti di accesso adeguati.<br><br>La sicurezza fisica di uffici, locali e strutture deve essere progettata e implementata. |

| ID | Nome del controllo | ISO/IEC 27001<br><br>Rif. Allegato A | Descrizione del controllo e linee guida |
|---|---|---|---|
| | Monitoraggio della sicurezza fisica | | Le sedi devono essere monitorate in modo continuo per rilevare accessi fisici non autorizzati. |
| 11 | Protezione contro minacce fisiche e ambientali | 7.5 | La protezione contro minacce fisiche e ambientali, come disastri naturali e altre minacce fisiche intenzionali o non intenzionali alle infrastrutture, deve essere progettata e implementata. |
| 12 | Manutenzione delle apparecchiature | 7.13 | Le apparecchiature devono essere mantenute correttamente per garantire disponibilità, integrità e riservatezza delle informazioni. |
| 13 | Scrivania pulita e schermo pulito | 7.7 | Devono essere definite e opportunamente applicate regole di scrivania pulita per i documenti cartacei e i supporti di memorizzazione rimovibili, nonché regole di schermo pulito per le strutture di elaborazione delle informazioni. |
| 14 | Gestione delle modifiche | 8.32 | Le modifiche alle strutture di elaborazione delle informazioni e ai sistemi informativi devono essere soggette a procedure di gestione delle modifiche. |
| 15 | Separazione degli ambienti di sviluppo, test e produzione | 8.31 | Gli ambienti di sviluppo, test e produzione devono essere separati e protetti. |
| 16 | Backup delle informazioni | 8.13 | Le copie di backup di informazioni, software e sistemi devono essere mantenute e testate regolarmente in conformità con la policy specifica concordata in materia di backup. |
| 17 | Registrazione degli eventi (logging)<br>Attività di monitoraggio | 8.15<br>8.16 | I log che registrano attività, eccezioni, guasti e altri eventi rilevanti devono essere prodotti, archiviati, protetti e analizzati.<br>Reti, sistemi e applicazioni devono essere monitorati per individuare comportamenti anomali e devono essere intraprese azioni appropriate per valutare potenziali incidenti di sicurezza delle informazioni. |

| ID | Nome del controllo | ISO/IEC 27001<br><br>Rif. Allegato A | Descrizione del controllo e linee guida |
|---|---|---|---|
| 18 | Sincronizzazione degli orologi | 8.17 | Gli orologi dei sistemi di elaborazione delle informazioni utilizzati dall'organizzazione devono essere sincronizzati con fonti temporali approvate. |
| 19 | Segmentazione delle reti | 8.22 | I gruppi di servizi informativi, gli utenti e i sistemi informativi devono essere separati nella rete dell'organizzazione. |
| 20 | Trasferimento delle informazioni | 5.14 | Devono essere in vigore regole, procedure o accordi per il trasferimento delle informazioni per tutti i tipi di strutture di trasferimento, all'interno dell'organizzazione e tra l'organizzazione e altre parti. |
| 21 | Architettura di sistema sicura e principi di ingegneria | 8.27 | I principi per l'ingegnerizzazione di sistemi sicuri devono essere stabiliti, documentati, mantenuti e applicati a tutte le attività di sviluppo dei sistemi informativi. |
| 22 | Requisiti di sicurezza delle applicazioni | 8.26 | I requisiti di sicurezza delle informazioni devono essere identificati, specificati e approvati durante lo sviluppo o l'acquisizione di applicazioni. |
| 23 | Ciclo di vita dello sviluppo sicuro | 8.25 | Devono essere stabilite e applicate regole per lo sviluppo sicuro di software e sistemi. |
| 24 | Test di sicurezza nello sviluppo e nell'accettazione | 8.29 | I processi di test di sicurezza devono essere definiti e implementati nel ciclo di vita dello sviluppo. |
| 25 | Monitoraggio, riesame e gestione delle modifiche dei servizi dei fornitori | 5.22 | L'organizzazione deve monitorare, riesaminare, valutare e gestire regolarmente i cambiamenti nelle pratiche di sicurezza delle informazioni dei fornitori e nell'erogazione dei servizi. |
| 26 | Pianificazione e preparazione della gestione degli incidenti di sicurezza delle informazioni | 5.24 | L'organizzazione deve pianificare e prepararsi alla gestione degli incidenti di sicurezza delle informazioni definendo, stabilendo e comunicando processi, ruoli e responsabilità per la gestione degli incidenti di sicurezza delle informazioni. |

| ID | Nome del controllo | ISO/IEC 27001<br><br>Rif. Allegato A | Descrizione del controllo e linee guida |
|---|---|---|---|
| 27 | Apprendimento dagli incidenti di sicurezza delle informazioni | 5.27 | Le conoscenze acquisite dagli incidenti di sicurezza delle informazioni devono essere utilizzate per rafforzare e migliorare i controlli di sicurezza delle informazioni. |
| 28 | Ridondanza delle strutture di elaborazione delle informazioni | 8.14 | Le strutture di elaborazione delle informazioni devono essere implementate con una ridondanza sufficiente a soddisfare i requisiti di disponibilità. |
| 29 | Diritti di proprietà intellettuale | 5.32 | L'organizzazione deve implementare procedure adeguate per proteggere i diritti di proprietà intellettuale. |
| 30 | Riesame indipendente della sicurezza delle informazioni.<br><br>Conformità a policy, regole e standard per la sicurezza delle informazioni | 5.35<br>5.36 | L'approccio dell'organizzazione alla gestione della sicurezza delle informazioni e la sua attuazione, comprese persone, processi e tecnologie, devono essere riesaminati in modo indipendente a intervalli pianificati o quando si verificano cambiamenti significativi.<br>La conformità alla politica di sicurezza delle informazioni dell'organizzazione, alle policy specifiche, alle regole e agli standard deve essere riesaminata regolarmente. |

# A.3 RELAZIONE TRA CONTROLLI DISCREZIONALI E MINACCE (MITIGAZIONE)

| Controllo | ISO/ IEC 27001 | Attacco fisico | Danno non intenzionale | Disastro | Guasti/ malfunziona-menti | Interruzioni | Ascolto clandestino/ intercettazione /dirottamento | Legale | Attività malevola/ abuso |
|---|---|---|---|---|---|---|---|---|---|
| **Contatti con le autorità Contatti con gruppi di interesse speciali** | 5.5 5.6 | Secondario | | Primario | | | Primario | Primario | Secondario |
| **Lavoro da remoto** | 6.7 | Secondario | Secondario | | Secondario | Primario | Primario | | Primario |
| **Inventario delle informazioni e degli altri asset associati** | 5.9 5.10 5.11 | Secondario | Primario | Secondario | Secondario | Secondario | Primario | Secondario | Primario |
| **Uso accettabile delle informazioni e degli altri asset associati** | 6.1 | Secondario | | | | | | Primario | Primario |
| **Restituzione degli asset** | 6.2 6.3 | | | | | | Secondario | Primario | Primario |
| **Verifiche preliminari** | 7.1 | Secondario | | Secondario | Primario | Secondario | Primario | | Secondario |
| **Termini e condizioni di impiego** | 7.14 | Secondario | | Primario | Secondario | Secondario | Primario | | Secondario |
| **Sensibilizzazione, istruzione e formazione sulla sicurezza delle informazioni** | 5.15 | Primario | | Secondario | | | Primario | Secondario | Primario |
| **Supporti di archiviazione** | 8.24 | | | | | | Primario | | Primario |
| **Smaltimento sicuro o riutilizzo delle apparecchiature** | 7.1 7.2 7.3 7.4 | Primario | Secondario | Primario | | | Secondario | Secondario | Primario |
| **Controllo degli accessi** | 7.5 | Primario | Secondario | Primario | Secondario | Primario | | | |
| **Uso della crittografia** | 7.13 | Secondario | Primario | Secondario | Primario | Primario | | | |
| **Perimetri di sicurezza fisica** | 7.7 | Secondario | Secondario | Secondario | | | Primario | | Secondario |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **Accesso fisico** | 8.32 | | | | Primario | Secondario | Secondario | Secondario | Primario |
| **Messa in sicurezza di uffici, locali e strutture** | 8.31 | | | | Secondario | Secondario | Secondario | | Primario |
| **Monitoraggio della sicurezza fisica** | 8.13 | | | Primario | Secondario | Primario | Secondario | | |
| **Protezione dalle minacce fisiche e ambientali** | 8.15<br>8.16 | | | | | | Primario | Primario | Primario |
| **Manutenzione delle apparecchiature** | 8.17 | | | | | Primario | | | Secondario |
| **Scrivania pulita e schermo pulito** | 8.22 | | | | | | Primario | | Primario |
| **Gestione delle modifiche** | 5.14 | | | | | | Primario | Primario | Secondario |
| **Separazione degli ambienti di sviluppo, test e produzione** | 8.27 | | | | | | Secondario | Primario | Primario |
| **Backup delle informazioni** | 8.26 | | | | | | Secondario | Primario | Primario |
| **Registrazione degli eventi (logging)** | 8.25 | | | | | | Secondario | Primario | Primario |
| **Attività di monitoraggio** | 8.29 | | | | | | Secondario | Primario | Primario |
| **Sincronizzazione degli orologi** | 5.22 | | | | Primario | Primario | Secondario | Primario | Primario |
| **Segmentazione delle reti** | 5.24 | | | Primario | Primario | Primario | Secondario | Primario | Primario |
| **Trasferimento delle informazioni** | 5.27 | | | | | | | Primario | Primario |
| **Architettura di sistema sicura e principi di ingegneria** | 8.14 | | | Primario | Primario | Primario | | | |
| **Requisiti di sicurezza delle applicazioni** | 5.32 | | | | | | Primario | Primario | Primario |
| **Ciclo di vita dello sviluppo sicuro** | 5.35<br>5.36 | | | | | | | Primario | Primario |

# ALLEGATO X

| Politica di Sicurezza delle Informazioni | | |
|---|---|---|
| **Policy #:** | **Data di entrata in vigore:** | **Email:** |
| **Versione:** | **Contatto:** | **Telefono:** |

## Scopo

La politica di sicurezza delle informazioni, insieme alle politiche e procedure correlate dell'azienda, ha lo scopo di proteggere la riservatezza, l'integrità e la disponibilità (CIA) di tutti i dati e gli asset critici dell'organizzazione, in linea con i suoi interessi aziendali.

## Ambito

La presente politica si applica ai dipendenti, ai collaboratori esterni, ai consulenti, ai lavoratori temporanei e a tutti gli altri lavoratori dell'organizzazione, incluso il personale appartenente a soggetti terzi. La presente politica si applica a tutti gli asset, materiali e immateriali, posseduti o utilizzati dall'organizzazione.

## Politica

L'alta direzione dell'organizzazione considera la sicurezza delle informazioni uno dei fattori abilitanti chiave per il proprio business ed è attivamente impegnata a promuovere e finanziare tutte le iniziative che consentano di ridurre in modo economicamente sostenibile i rischi per la sicurezza delle informazioni, garantire la conformità alle leggi e agli obblighi contrattuali pertinenti e seguire le buone pratiche di settore. Tutto il personale interno ed esterno dell'organizzazione è tenuto a seguire diligentemente l'intento e le prescrizioni della presente politica e di tutte le politiche e procedure correlate. In caso contrario, potrà essere soggetto ad azioni disciplinari. Più nello specifico, i principi di sicurezza delle informazioni che tutti sono tenuti a comprendere e osservare sono:

1) La sicurezza delle informazioni non è assoluta; deve sempre essere proporzionata ai rischi che deve contrastare.
2) Ogni accesso deve essere strettamente limitato alla necessità di conoscere, in relazione al personale e alle sue esigenze operative.

3) Le risorse devono essere separate e protette in base ai rispettivi requisiti di sicurezza delle informazioni.
4) L'uso di standard e soluzioni aperte è sempre preferibile a scelte proprietarie e poco trasparenti.
5) Un singolo livello di controlli di sicurezza delle informazioni potrebbe non essere sufficiente in tutti i casi, poiché laddove un guasto sarebbe critico è opportuno adottare approcci multilivello.
6) Studiare, esercitarsi e testare situazioni rilevanti per la sicurezza delle informazioni è fondamentale per garantire un'efficace prontezza di risposta.
7) La sicurezza delle informazioni è responsabilità e dovere di tutti; non è un problema che riguarda qualcun altro.

L'organizzazione definisce e misura un insieme di specifici obiettivi di sicurezza delle informazioni, che vengono costantemente monitorati e migliorati. Tali obiettivi orientano le decisioni tattiche in materia di sicurezza delle informazioni, così come i principi sopra richiamati guidano le decisioni strategiche. Il miglioramento continuo è un fattore abilitante essenziale per mantenere sotto controllo i rischi, sempre crescenti, legati alla sicurezza delle informazioni e consentire all'organizzazione di conseguire con successo i propri obiettivi di business nel complesso contesto in cui opera oggi.

**Approvazione e titolarità**

| Responsabile | Titolo | Data | Firma |
|---|---|---|---|
| Autore della policy | Titolo | GG/MM/AAAA | |
| **Approvato da** | **Titolo** | **Data** | **Firma** |
| Direzione aziendale | Titolo | GG/MM/AAAA | |