Small Business Standards

Guida ai controlli di sicurezza delle informazioni per le piccole e medie imprese

European DIGITAL SME Alliance

Italian DIGITAL SME Alliance

Con il supporto di:

CNA Milano

ASSINTEL ASSOCIAZIONE NAZIONALE IMPRESE ICT

confimi industria DIGITALE

ASSOCIAZIONE ITALIA4BLOCKCHAIN

La presente guida è stata redatta da una equipe dedicata, creata da esperti del gruppo di lavoro SBS "Digitalisation" (Digitalizzazione), nonché dai gruppi di lavoro DIGITAL SME "Standards and Cybersecurity" (Standard e sicurezza informatica) e "Data Protection" (Protezione dei dati). Di tale equipe dedicata hanno fatto parte specialisti in materia di normazione, con una conoscenza approfondita delle problematiche relative alla sicurezza informatica, in grado di comprendere pienamente le esigenze delle PMI in questo ambito.

Presidente:
Jean-Luc Allard

Coordinatore:
Omar Dhaher

Specialisti:

Andrea Caccia

Daniele Tumietto

Davide Giribaldi

Francisco Menéndez

Samuel Fricker

Data di pubblicazione:
Aprile 2022

INFORMAZIONI SULLA GUIDA

Small Business Standards (SBS) è l'associazione che rappresenta, a livello europeo e internazionale, gli interessi delle piccole e medie imprese (PMI) europee nel processo di normazione. I suoi obiettivi principali derivano dal regolamento (UE) n. 1025/2012 sulla normazione europea. SBS ha l'obbiettivo di aumentare la consapevolezza e l'influenza delle PMI durante l'elaborazione degli standard, facilitandone l'adozione da parte delle stesse, rappresentando i loro interessi e motivandole a impegnarsi nel processo di normazione.

La European DIGITAL SME Alliance (DIGITAL SME) è un membro di SBS. DIGITAL SME è il più grande network europeo di PMI appartenenti al settore ICT e rappresenta circa 45.000 PMI digitali.

Al fine di sensibilizzare e aiutare le PMI a adottare e utilizzare gli standard di sicurezza informatica, nel 2017 SBS ha pubblicato una guida per le PMI sullo standard ISO/IEC 27001. Data la crescente necessità da parte delle PMI di conformarsi ai requisiti in materia di sicurezza informatica e di sviluppare le proprie capacità tecniche al riguardo, SBS ha redatto questa guida sullo standard ISO/IEC 27002, inerente al controllo della sicurezza delle informazioni, rivolta alle piccole e medie imprese.

SBS è l'unica proprietaria della presente guida, messa gratuitamente a disposizione del pubblico.

La Guida è stata tradotta in italiano dalla Italian Digital SME Alliance con il contributo di ASSINTEL, CONFIMI Industria Digitale, CNA Milano e Italia4Blockchain.

Elenco degli acronimi utilizzati

BYOD: Bring Your Own Device (Porta il tuo dispositivo)
CEO: Chief Executive Officer (Amministratore Delegato)
CERT: Computer Emergency Response Team (Squadra per la risposta alle emergenze informatiche)
COBIT: Control Objectives for information and related technologies (Obiettivi di controllo per le informazioni e le tecnologie correlate) (ISACA.org)
DAC: Discretionary Access Control (Controllo dell'accesso discrezionale)
DTG: Date-Time Group (Gruppo data-orario)
DPO: Data Protection Officer (Responsabile della protezione dei dati)
EGIT: Enterprise Governance of Information and Technology (Governance aziendale delle informazioni e delle tecnologie)
GDPR: General Data Protection Regulation (Regolamento generale sulla protezione dei dati)
IEC: International Electrotechnical Commission (Commissione elettrotecnica internazionale)
ICT: Information and Communications Technology (Tecnologia dell'informazione e della comunicazione)
IoT: Internet of Things (Internet delle cose)
IP: Internet Protocol (Protocollo Internet)
ISMS: Information security management system (Sistema di gestione della sicurezza delle informazioni)
ISO: Information Security Officer (Responsabile della sicurezza delle informazioni)
ISO: International Organization for Standardization (Organizzazione internazionale per la standardizzazione)
LAN: Local Area Network (Rete locale)
MAC: Mandatory Access Control (Controllo dell'accesso obbligatorio)
OS: Operating System (Sistema operativo)
PII: Personally Identifiable Information (Informazioni di identificazione personale)
PIMS: Privacy information management system (Gestione delle informazioni sulla privacy)
RACI: Matrice di assegnazione di responsabilità RACI. L'acronimo sta per:
Responsible, persone che hanno la responsabilità di eseguire un'attività;
Accountable, persona che ha la responsabilità finale di conseguire gli obiettivi e riferire agli organi direttivi;
Consulted, persone che collaborano e vengono consultate per stabilire gli obiettivi e definire le attività; e
Informed, persone che devono essere informate delle attività e dei risultati previsti.
VPN: Virtual Private Network (Rete privata virtuale)
WAN: Wide Area Network (Rete geografica)

INDICE

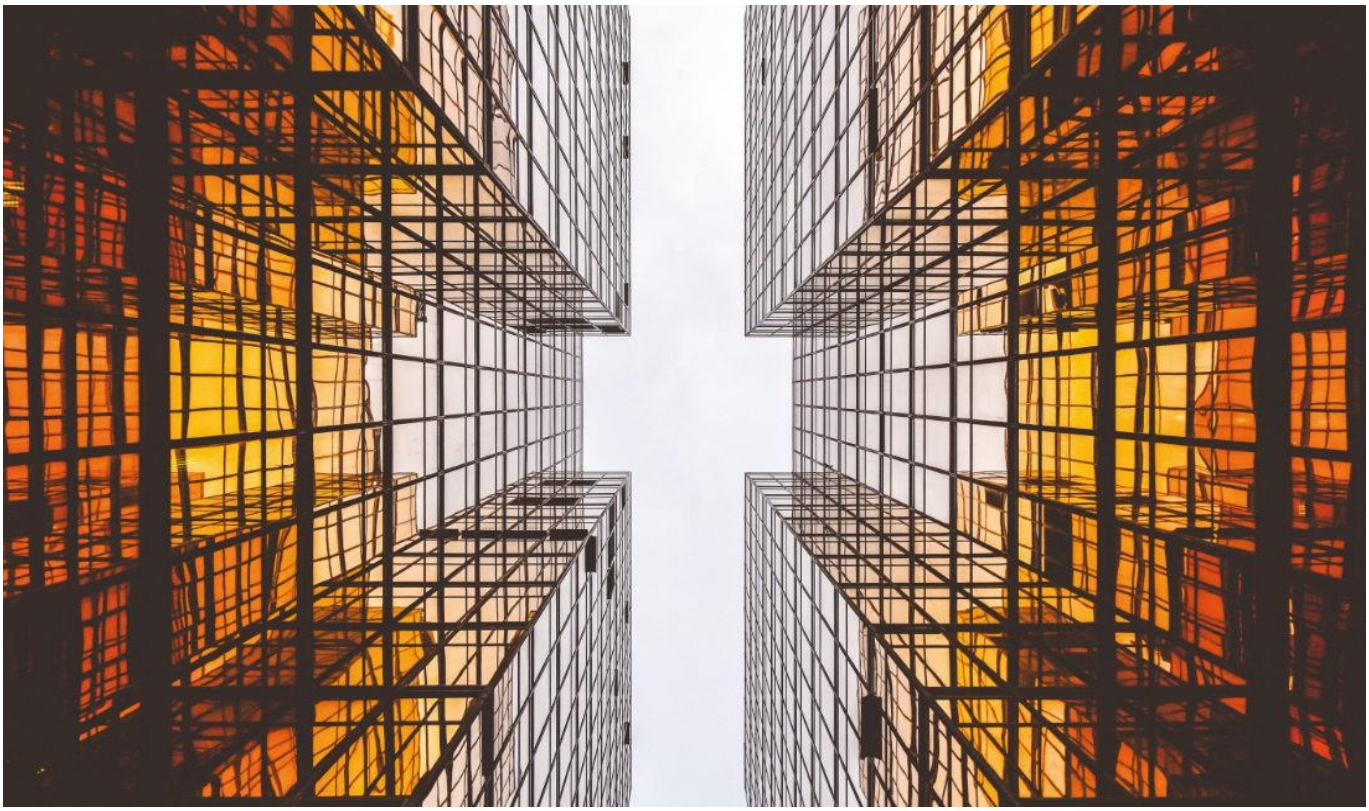
INDICE

1. INTRODUZIONE

La trasformazione digitale sta assumendo un ruolo importante nella ristrutturazione delle aziende di tutto il mondo. Tecnologie abilitanti quali 5G, Intelligenza Artificiale, Blockchain, Edge Computing e Internet delle cose (IoT) costituiscono il nucleo principale di tale trasformazione. Riconoscendo il loro ruolo strategico per gli obiettivi a lungo termine dell'UE, la Commissione europea ha sviluppato la propria strategia 2030 – il Decennio DIGITALE – che comprende i seguenti obiettivi:

1. L'utilizzo di servizi di *cloud computing*, *big data* e intelligenza artificiale da parte del 75% delle imprese europee;
2. Il raggiungimento di almeno un livello di intensità digitale di base da parte di oltre il 90% delle PMI;
3. L'aumento del numero di *scale-up* e finanziamenti per raddoppiare gli "unicorni" dell'UE;

Le PMI digitali stanno fornendo soluzioni innovative in settori quali le tecnologie 5G, IoT ed *Edge Computing*, per consentire ad altre aziende di acquisire competenze digitali e realizzare la trasformazione digitale. In questo contesto, la sicurezza rimane un aspetto cruciale nell'adozione delle tecnologie e delle soluzioni di cui le aziende necessitano.



La sicurezza informatica è un requisito per l'intera catena di approvvigionamento, al fine di garantire il passaggio graduale dei processi industriali dal mondo fisico al cyberspazio[1]. Poiché il 99% delle aziende in Europa sono PMI, la protezione dagli attacchi informatici è fondamentale per l'economia europea.

Tuttavia, l'adozione delle ICT e dei criteri di sicurezza delle informazioni risulta ancora bassa. Nel 2019, Eurostat ha stimato che il 33% delle imprese europee dispone di documenti relativi a provvedimenti, prassi o procedure sulla sicurezza delle ICT e che il 24% ha definito o rivisto questi documenti negli ultimi 12 mesi.

1. SBS (2020, pagina 3), EU Cybersecurity Act and the role of standards for SMEs (Legge dell'Unione Europea sulla sicurezza informatica e ruolo delle normative per le PMI).

Gli standard sulla sicurezza informatica possono aiutare le aziende a adottare una serie di requisiti, che forniscono il necessario livello di protezione di base. Tuttavia, tali requisiti sono complessi e costosi da implementare per le PMI. Nel 2020[2], esistevano circa 32.000 certificati per il sistema di gestione della sicurezza delle informazioni ISO/IEC 27001 in tutto il mondo, a fronte di circa 190 milioni di imprese che operano a livello globale.

La presente guida è stata redatta da proprietari di PMI e professionisti che lavorano o collaborano con PMI, dotati di esperienza e conoscenza approfondita delle problematiche relative alla sicurezza, che la maggior parte delle piccole imprese affronta quotidianamente. La guida è divisa in due parti. La prima parte illustra la necessità di una strategia e di obiettivi chiari per un'implementazione ottimale dei controlli di sicurezza e presenta i concetti di base in tema di privacy e la loro rilevanza per i controlli di sicurezza, le certificazioni e la conformità al GDPR. La seconda parte suggerisce i controlli minimi indispensabili, che le PMI devono implementare per proteggere le proprie informazioni e per conformarsi al GDPR.

2. AMBITO

L'ambito della guida è la sicurezza delle informazioni, intesa nel senso più ampio. La guida si rivolge sia al management delle PMI (CEO e DPO) sia alle equipe tecniche (provider di sicurezza informatica per le PMI, professionisti/esperti di sicurezza informatica), nonché alle PMI che operano nel settore ICT. Per quanto riguarda il management delle PMI, la guida vuole sensibilizzare sulle problematiche affrontate dalle PMI e aiutare i dirigenti a indirizzare le attività che il proprio personale tecnico o i provider di servizi di sicurezza devono svolgere. La presente guida si prefigge lo scopo di aumentare la consapevolezza in merito a questioni relative a:

- L'importanza della protezione delle informazioni (capitolo 4)
- La protezione della privacy e conformità al GDPR (capitolo 5)
- La governance della sicurezza delle informazioni (capitolo 6)
- I controlli per la sicurezza delle informazioni (capitolo 7.1)

La gestione del rischio per la sicurezza delle informazioni non viene affrontata direttamente. Tale argomento viene trattato nella guida di SBS per le PMI ai fini dell'implementazione dello standard ISO/IEC 27001 sulla gestione della sicurezza delle informazioni (SBS SME Guide for the implementation of ISO/IEC 27001 on Information Security Management).

Le PMI con adeguate competenze e consapevolezza in materia di sicurezza informatica[3] possono quindi passare al capitolo 7.2, che fornisce una descrizione generale dei 16 controlli selezionati, ritenuti essenziali per qualsiasi PMI ai fini della tutela delle proprie informazioni e della conformità alle disposizioni del GDPR. La guida intende fornire un supporto per l'evoluzione delle PMI che desiderano acquisire "sicurezza informatica tramite l'adozione di pratiche corrette". Le equipe tecniche e le PMI che operano nel settore della sicurezza informatica possono fare riferimento ai controlli illustrati nel capitolo 7, per garantire l'implementazione ottimale delle misure di sicurezza per l'infrastruttura delle piccole e medie imprese.

Si raccomanda che le PMI, comprese le microimprese, che non dispongono di un DPO dedicato o di professionisti della sicurezza, si rivolgano a PMI e/o a professionisti della sicurezza informatica per garantire un'adeguata protezione dei propri dati.

3. DEFINIZIONI

3.1 Definizioni generali

Business Continuity (BC) (Continuità operativa): si riferisce al mantenimento delle funzioni aziendali principali dell'intera azienda o alla loro rapida ripresa in caso di interruzioni, come ad esempio un attacco da parte di criminali informatici.

Business continuity plan (Piano di continuità operativa): insieme di procedure e istruzioni che un'azienda deve seguire per reagire tempestivamente a un incidente.

2. SBS (2020, pagina 4), EU Cybersecurity Act and the role of standards for SMEs (Legge dell'Unione Europea sulla sicurezza informatica e ruolo delle normative per le PMI).
3. Shojaifar e Järvinen (2021, pagina 3), Una PMI che rientra nelle colonne "CSTA" e "GSGP" dovrebbe essere in grado di proseguire con il capitolo 7.2. Le altre PMI necessiteranno dell'aiuto di PMI o professionisti in materia di sicurezza informatica per attuare i controlli di cui alla sezione 7.2. Cliccare qui per maggiori informazioni sul modello Shojaifar e Järvinen.

Il Piano di continuità operativa riguarda i processi aziendali, gli asset, le risorse umane, i partner commerciali, nonché tutte le parti interessate coinvolte nell'ecosistema aziendale.

Business impact analysis (Analisi dell'impatto aziendale): si tratta di un'ulteriore parte fondamentale di un Piano di continuità operativa. Identifica l'impatto della perdita aziendale (solitamente quantificata in termini di costi) e aiuta a esaminare i processi dell'intera azienda e a valutarli, stabilendo quali sono i più importanti.

Control (Controllo): misura (processo, politica, dispositivo, pratica o azione) che modifica il rischio.

Confidentiality (Riservatezza): proprietà delle informazioni che non devono essere rese disponibili o divulgate a persone, entità o processi non autorizzati.

Disaster recovery plan (Piano di ripristino di emergenza): si tratta di una parte importante di un Piano di continuità operativa, ma non costituisce il piano stesso. Si focalizza principalmente sul ripristino di un'infrastruttura informatica e di tutte le operazioni correlate dopo un incidente.

Governance of Information Security (Governance della sicurezza delle informazioni): sistema mediante il quale le attività relative alla sicurezza delle informazioni di un'azienda vengono disciplinate e controllate.

Information Security (Sicurezza delle informazioni): mantenimento della riservatezza, dell'integrità e della disponibilità delle informazioni.

Information Security risk (Rischio per la sicurezza delle informazioni): il rischio per la sicurezza delle informazioni è associato alla possibilità che le minacce sfruttino le vulnerabilità di un asset informatico o di un gruppo di asset informatici per accedere a dati o processi aziendali, causando danni a un'azienda (Nota 6 a 3.61).

Information System (Sistema informativo): insieme di applicazioni, servizi, asset informatici o altri componenti per la gestione delle informazioni.

Integrity (Integrità): proprietà di precisione e completezza.

Policy (Politica): intenti e direttive di un'azienda, espressi formalmente dalla dirigenza della stessa.

Process (Processo): insieme di attività correlate o interagenti, che trasformano gli input in output.

Risk management (Gestione del rischio): attività coordinate per dirigere e controllare un'azienda in materia di gestione del rischio.

3.2 Definizioni relative alla privacy

Le seguenti definizioni sono conformi al GDPR. Lo standard ISO/IEC 27701 e, più in generale, tutti gli standard ISO utilizzano il termine "Personally Identifiable Information (PII) (Informazioni di identificazione personale)", mentre il GDPR impiega il termine "Personal Data (Dati personali)". Pertanto, la presente guida utilizzerà il termine "Dati personali".

Personal data (Dato personale): qualsiasi informazione riguardante una persona fisica identificata o identificabile.

Data subject (Interessato): una persona fisica identificabile è una persona che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

Personal data processing o Processing (Trattamento dei dati personali o trattamento): qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

Controller (Titolare del trattamento): la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.

Processor (Responsabile del trattamento): la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

Availability (Disponibilità): proprietà di accessibilità e fruibilità su richiesta da parte di un'entità autorizzata.

Confidentiality (Riservatezza): proprietà delle informazioni che non vengono rese disponibili o divulgate a persone, entità o processi non autorizzati.

Documented information (Informazioni documentate)[4]: informazioni che devono essere controllate e conservate da un'azienda, nonché il supporto che le contiene.

Information Security event (Evento di sicurezza delle informazioni): evento identificato di un sistema, di un servizio o di uno stato della rete, che indica una possibile violazione della politica di sicurezza delle informazioni, un malfunzionamento dei controlli o una situazione precedentemente non nota, che può essere rilevante per la sicurezza.

Information Security incident (Incidente di sicurezza delle informazioni): uno o più eventi di sicurezza delle informazioni indesiderati o imprevisti, che hanno una probabilità significativa di compromettere le attività aziendali e minacciare la sicurezza delle informazioni.

Likelihood (Probabilità): possibilità che accada un fatto.

Malware: esiste una vasta gamma di tipologie di malware:

- **Virus:** si replica in file eseguibili.
- **Worm:** viaggia attraverso i canali di comunicazione tramite i contatti degli utenti.
- **Spyware:** monitora le attività degli utenti e invia informazioni al server di un hacker.
- **Ransomware:** blocca il sistema crittografando i file e l'hacker promette agli utenti di restituire l'accesso ai file dopo il pagamento di un riscatto.
- **Logic bomb (bomba logica):** malware che permane inattivo nel sistema fino al verificarsi di specifiche condizioni programmate, che "attivano la bomba", causando danni irreparabili.
- **Trojan (Cavallo di Troia):** inserito in programmi innocui, acquistati o scaricati, che svolge diverse attività nascoste.

Vulnerability (Vulnerabilità): debolezza di un asset o di un controllo, che può essere sfruttata da una o più minacce.

4. PERCHÉ LE PMI DEVONO PROTEGGERE LE INFORMAZIONI?

Le informazioni sono probabilmente gli asset più importanti per qualsiasi azienda, comprese le PMI. Cosa può fare un'azienda se le informazioni sono inaffidabili o già in possesso di qualcuno che può bloccare gli utenti o modificare i dati senza che lo si sappia? Oppure, più semplicemente, cosa succede se le informazioni non sono disponibili o accessibili quando se ne ha necessità? Tutte le informazioni accessibili su Internet sono affidabili?

Quasi tutti conoscono lo standard ISO 9001, il famoso sistema di gestione della qualità, ma quanti sanno dell'esistenza dello standard ISO/IEC 27001, che riguarda il sistema di gestione della sicurezza delle informazioni? La sua prima pubblicazione risale al 2005 e la sua struttura e il suo contenuto sono molto simili a quelli dello standard ISO 9001. Qualora sia stato adottato il primo, sarà possibile adottare anche il secondo senza troppi sforzi. Si rimanda alla guida di SBS per le PMI ai fini dell'implementazione dello standard ISO/IEC 27001 sulla gestione della sicurezza delle informazioni (SBS SME Guide for the implementation of ISO/IEC 27001 on Information Security Management).

4. Nota 1 al termine: le informazioni documentate possono essere in qualsiasi formato e su qualunque supporto, nonché provenire da qualsiasi fonte. Nota 2 al termine: Le Informazioni documentate possono fare riferimento al sistema di gestione, compresi i relativi processi, alle informazioni generate ai fini dell'operatività aziendale (documentazione), nonché ai riscontri dei risultati raggiunti (registrazioni).

Sarà tuttavia necessario comprendere l'ambito e i motivi per cui si deve adottare tale standard. Che cosa sono le informazioni? Perché è necessario proteggerle? Qual è il legame con il GDPR? Queste sono le domande a cui la presente guida intende rispondere.

Che cosa sono le informazioni?

Le informazioni sono un insieme di dati interpretabili che, all'interno di un dato contesto, hanno un significato e un valore. Per garantire e migliorare questi dati di valore, l'interpretabilità e il contesto devono essere preservati e tutelati.

Perché? Semplicemente perché senza informazioni – e, soprattutto, senza informazioni affidabili – non possiamo realizzare praticamente niente nella nostra vita. Gli esseri umani – e ancor più naturalmente e inconsciamente il nostro corpo – non fanno altro che gestire dati e informazioni: ad esempio, preparare il pane, guidare un'auto e curare un disturbo fisico. Le informazioni sono strettamente correlate a qualsiasi attività umana.

Le informazioni sono essenziali in quanto servono a:

- aumentare le proprie conoscenze e competenze (sappiamo tutti che la conoscenza conferisce potere[5] su coloro che non ce l'hanno);
- adottare decisioni efficaci;
- agire per realizzare i propri obiettivi;
- misurare i propri risultati.

Cosa succede se le informazioni utilizzate non sono affidabili perché:

- sono già a conoscenza di chi può impedirci di raggiungere i nostri obiettivi (riservatezza)?
- sono state modificate in modo incontrollato in una qualsiasi delle fasi della loro gestione (integrità)?
- non sono disponibili e raggiungibili quando ne abbiamo necessità (disponibilità)?

Che cos'è la sicurezza delle informazioni?

Riservatezza, integrità e disponibilità vengono da molto tempo considerate come i tre principali criteri per garantire la sicurezza delle informazioni. Il rispetto di leggi e regolamenti, nel cui ambito il trattamento dei dati personali è sicuramente uno dei temi più rilevanti da affrontare, sta diventando sempre più una priorità per le PMI, non foss'altro a causa delle sanzioni previste.

5. Potere 1: Di colui che sa su colui che non sa; Potere 2: Sapere qualcosa su qualcun altro e usarlo per ottenere qualcosa (ricatto); Potere 3: Impedire l'accesso alle informazioni necessarie (bloccare la persona).

I due standard "chiave" sulla sicurezza delle informazioni sono l'ISO/IEC 27001 [ISMS - *Information Security Management System* (Sistema di gestione della sicurezza delle informazioni)] e l'ISO/IEC 27002 [*Code of Practice for information security control* (Codice di pratica per la gestione della sicurezza delle informazioni)]. L'applicazione dello standard ISO/IEC 27701 alle Informazioni di identificazione personale (PII) migliora inoltre direttamente il livello di conformità al Regolamento generale sulla protezione dei dati (GDPR), sebbene non lo garantisca. Ma va tenuto presente che ora esiste anche lo standard ISO/IEC 27701, una normativa specifica che affronta tale questione.

È tuttavia richiesta una gestione complessa delle informazioni utilizzate. Lo standard ISO/IEC 27002 fornisce un elenco di 114 controlli per garantire la sicurezza delle informazioni, generalmente definiti all'interno di un processo di gestione del rischio, come spiegato nello standard ISO/IEC 27005, in particolare per quanto riguarda la loro implementazione in ciascun contesto.

Il GDPR impone una gestione controllata delle Informazioni di identificazione personale, che sono una categoria di informazioni gestita da tutte le PMI, e riguardano il proprio personale, i clienti e i fornitori, a partire dal momento in cui il nome di una persona viene associato a qualcos'altro. In questo ambito, sono altresì applicabili gli standard ISO/IEC 27001 e 27002, integrati dallo standard ISO/IEC 27701.

Il processo di valutazione del rischio per la sicurezza delle informazioni identifica anche i rischi connessi al trattamento dei dati personali e, in particolare, alla perdita di riservatezza, integrità e disponibilità di tali dati personali. I controlli e le altre raccomandazioni contenute nella presente guida mirano a ridurre i rischi valutati. Maggiori informazioni sul processo di gestione del rischio sono disponibili nella guida di SBS per le PMI ai fini dell'implementazione dello standard ISO/IEC 27001 sulla gestione della sicurezza delle informazioni (SBS SME Guide for the implementation of ISO/IEC 27001 on Information Security Management).

Perché è necessario disporre di una normativa in materia?

Le leggi e i regolamenti europei, attuali e futuri, fanno sempre affidamento sul principio di responsabilità e su un approccio basato sul rischio, specialmente per quanto riguarda le nuove tecnologie, che sono particolarmente rilevanti per le *start-up*. In assenza di un solido approccio strutturato, la complessità e il costo della conformità possono rapidamente diventare ingestibili per qualsiasi azienda. Gli standard rappresentano una soluzione efficace per affrontare questo problema.

Chiunque parli la lingua della società in cui vive utilizza di fatto due standard per comprendere le situazioni e per essere compreso: l'ortografia e la grammatica. Allo stesso modo, gli standard per la sicurezza delle informazioni ci aiutano ad adottare le azioni più idonee, in conformità ai regolamenti, per gestire una situazione specifica di una determinata entità e ad aumentare la competitività.

Gli standard di sicurezza delle informazioni sono di competenza del Sottocomitato 27 appartenente al Comitato tecnico congiunto all'interno dell'Organizzazione internazionale per la standardizzazione (ISO) e del Comitato elettrotecnico internazionale (IEC), note come ISO/IEC JTC 1 SC 27: Information Security, Cybersecurity and Privacy Protection (Sicurezza delle informazioni, sicurezza informatica e protezione della privacy).

Gli standard sono stati sviluppati per imprese di qualsiasi dimensione. Tuttavia, individuare quelli più adeguati e adattarli all'uso può costituire un ostacolo al loro utilizzo, in particolare per le PMI. Questo documento vuole essere una guida rivolta alle PMI per la scelta e l'adattamento degli standard.

4.1 Differenze tra sicurezza delle informazioni e delle ICT

La sicurezza delle informazioni riguarda la protezione delle informazioni, indipendentemente dal supporto (fisico, audio o video, e su supporti e sistemi digitali). La sicurezza delle ICT riguarda la protezione dei sistemi ICT e dei dati che contengono ed elaborano.

4.2 Influenza di Internet e degli aspetti informatici

Internet e, più in generale, il cyberspazio offrono molte opportunità, congiuntamente a vulnerabilità e nuovi rischi in continua evoluzione. Questo è il motivo per cui la presente guida contiene utili indicazioni sulla sicurezza informatica e di rete.

5. PROTEZIONE DELLA PRIVACY

5.1 Concetti principali

Il GDPR stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati (Articolo 1). L'obiettivo è tutelare i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali.

Questo processo è solitamente associato al termine "protezione della privacy".

Ciascuna azienda deve trattare dati personali per il proprio corretto funzionamento. Pertanto, qualsiasi PMI europea deve affrontare adeguatamente la questione della conformità al GDPR. Il presente documento fornisce una guida di base per la conformità al GDPR, basata sullo standard ISO/IEC 27701, che integra gli standard ISO/IEC 27001 e ISO/IEC 27002, fornendo requisiti e linee guida per la gestione della riservatezza delle informazioni. Questo rende l'approccio valido e, se necessario, getta le basi anche per la conformità in altri ambiti.

Tuttavia, va tenuto presente che questo documento non mira ad essere esaustivo, bensì ad aiutare le PMI ad adottare i controlli più importanti. Per questo, considerando anche la sensibilità della materia e le cospicue sanzioni previste in caso di trattamento non conforme, è sempre necessario fare riferimento al testo del GDPR. In particolare, qualora il trattamento dei dati personali costituisca l'attività principale della PMI, si raccomanda vivamente di leggere e applicare lo standard ISO/IEC 27701, per il quale questa guida può essere considerata un'utile introduzione.

Nel caso in cui la PMI adotti un tipo di trattamento che possa comportare una situazione ad alto rischio per i diritti e le libertà delle persone fisiche, sarà necessario effettuare una valutazione dell'impatto delle attività di trattamento previste sulla protezione dei dati personali (per maggiori informazioni in merito, si prega di fare riferimento all'Articolo 35 del GDPR). La certificazione prevista dagli articoli 42 e 43 del GDPR, descritta nel capitolo 5.2, mette a disposizione un ulteriore strumento, che, qualora venga adottato, si rivelerà utile per ridurre il rischio di non conformità.

5.2 Certificazioni relative alla privacy

Lo standard ISO/IEC 27001 supporta la certificazione di soggetti terzi quale sistema di gestione della sicurezza delle informazioni e, pertanto, un Organismo di certificazione che attesti la conformità a tale standard dovrà essere accreditato in conformità all'ISO 17021-1:2015, lo standard che stabilisce "i principi e i requisiti per la competenza, la coerenza e l'imparzialità degli organismi che forniscono audit e certificazione di tutti i tipi di sistemi di gestione"[6].

L'Articolo 42 del Regolamento (UE) 2016/679 raccomanda l'istituzione di meccanismi di certificazione della protezione dei dati, per dimostrare la conformità al GDPR del trattamento effettuato da titolari e responsabili del trattamento stesso.

Inoltre, l'articolo 43 stabilisce le caratteristiche degli Organismi di certificazione che attesteranno la conformità del trattamento dei dati personali al GDPR; questi Organismi devono essere accreditati dall'Autorità di controllo o dall'organismo nazionale di accreditamento in conformità allo standard ISO/IEC 17065:2012, che definisce i requisiti per la competenza, il funzionamento coerente e l'imparzialità degli organismi di certificazione per prodotti, processi e servizi.

Lo standard ISO/IEC 27701 integra lo standard ISO/IEC 27001 e pertanto richiede che l'organismo di certificazione sia accreditato ai sensi dello standard ISO 17021-1:2015, come avviene nel caso dello standard ISO/IEC 27001. Di conseguenza, non è possibile utilizzare lo standard ISO/IEC 27701 quale base per una certificazione conforme all'Articolo 42, in quanto l'Articolo 43 prevede che l'organismo di certificazione sia accreditato ai sensi dello standard ISO/IEC 17065:2012.

Quindi, mentre il GDPR (Regolamento (UE) 2016/679) richiede una certificazione relativa al "prodotto" per dimostrare la conformità al GDPR, lo standard ISO/IEC 27001 è certificabile come un'integrazione dello standard ISO/IEC 27001 e richiede una certificazione relativa al "sistema di gestione".

Al fine di scindere questo legame che è stato creato tra lo standard ISO/IEC 17021 e lo standard ISO/IEC 17065, è auspicabile che il Comitato europeo per la protezione dei dati (EDPB) sia in grado di dichiarare valida o meno la certificazione in conformità all'integrazione dello standard ISO/IEC 27701:2019. Questo è l'unico modo per mantenere uno dei principi chiave su cui si basa il GDPR: regole uguali per il trattamento dei dati in tutti gli Stati membri dell'UE.

Le aziende che hanno già implementato un sistema di gestione della sicurezza delle informazioni (ISMS) in conformità allo standard ISO/IEC 27001 possono estenderlo alla gestione della privacy, compreso il trattamento dei dati personali, utilizzando lo standard ISO/IEC 27701.

6. Tutti gli organismi di certificazione DEVONO essere accreditati; in caso contrario il certificato ISMS/GDPR non sarà né valido, né riconosciuto. La certificazione dimostra la conformità (per un periodo di 3 anni). La certificazione non è obbligatoria, bensì facoltativa. La maggior parte delle organizzazioni (e delle PMI) opta per un'implementazione verificata da un soggetto terzo attendibile.

Le aziende che non dispongono di un sistema di gestione della sicurezza delle informazioni (ISMS) possono anche implementare congiuntamente gli standard ISO/IEC 27001 e 27701 in un unico progetto, poiché l'ISO/IEC 27701 sostanzialmente integra i requisiti previsti dal 27001 e dal suo "codice di condotta" (ISO/IEC 27002). Non sarà quindi necessario ottenere due certificazioni distinte.

Una certificazione basata sullo standard ISO/IEC 27701 è uno strumento riconosciuto a livello internazionale, che può aiutare a dimostrare la conformità alla legislazione sulla protezione dei dati, anche se non è strettamente in linea con la certificazione di cui all'Articolo 42 del GDPR.

Questo in attesa di ottenere chiarimenti circa la possibilità di usare lo standard ISO/IEC 27701 quale mezzo per dimostrare la conformità al GDPR del trattamento dei dati personali effettuato, sia in qualità di titolari che di responsabili.

In ogni caso, un Sistema di gestione delle informazioni sulla privacy (PIMS) conforme allo standard ISO/IEC 27701 risulta utile per qualsiasi azienda soggetta a obblighi di protezione dei dati. È di particolare interesse per le imprese che svolgono la propria attività a livello internazionale, lavorano con clienti in altre giurisdizioni oppure operano all'interno di catene di approvvigionamento internazionali. Queste aziende sono spesso tenute a rispettare un grande numero di regolamenti e leggi sulla privacy e questo nuovo standard può semplificare la gestione della conformità.

Implementando un Sistema di gestione delle informazioni sulla privacy (PIMS), conforme allo standard ISO/IEC 27001, a integrazione di un sistema di gestione della sicurezza delle informazioni (ISMS) già esistente, un'azienda può raccogliere ed elaborare dati, anche personali, in modo sistematico. Si possono anche gestire i rischi associati alla riservatezza, all'integrità e alla disponibilità delle informazioni e rispondere alle minacce e ai rischi in costante evoluzione per tali dati e per la privacy.

Un PIMS consente inoltre alle aziende di ridurre i costi associati alla tutela della privacy e alla sicurezza delle informazioni, adattandosi costantemente ai cambiamenti interni ed esterni all'impresa, aumentando la resilienza agli attacchi informatici.

Un PIMS offre diversi vantaggi:

- Genera fiducia nella capacità dell'azienda di gestire le informazioni personali, sia nei clienti che nei dipendenti.
- Facilita la dimostrazione della conformità al GDPR e ad altre normative sulla privacy applicabili.
- Chiarisce ruoli e responsabilità all'interno dell'azienda.
- Migliora la competenza interna e i processi per evitare violazioni.
- Offre trasparenza in merito ai controlli di gestione della privacy stabiliti.
- Semplifica gli accordi con i partner commerciali, qualora la gestione delle PII (Informazioni di identificazione personale) sia importante per entrambe le parti.
- Consente una facile integrazione con lo standard principale per la sicurezza delle informazioni ISO/IEC 27001.

Lo standard ISO/IEC 27701 contiene una serie di allegati che aiutano a elaborare controlli appropriati, sia per l'implementazione delle necessarie misure di sicurezza e conformità, sia per lo sviluppo di valutazioni del rischio.

5.3 Controlli sulla privacy

Lo standard ISO/IEC 27701 è uno strumento progettato per affrontare correttamente le questioni inerenti alla sicurezza e gestione del rischio in relazione al trattamento dei dati personali basandosi sullo standard ISO/IEC 27001, creando valore oltre che le condizioni per una rapida integrazione. Lo stesso vale per i controlli sulla privacy ai sensi dello standard ISO/IEC 27701, che sono stati inclusi nel capitolo 7, che illustra i più importanti controlli sulla sicurezza delle informazioni e sulla privacy ai sensi degli standard ISO/IEC 27001 e ISO/IEC 27701.

Per ciascun controllo, è stato aggiunto un sottoparagrafo specifico (Estensione alla privacy), nel caso in cui un controllo generale definito nello standard ISO/IEC 27001 venga maggiormente dettagliato nello standard ISO/IEC 27701. Gli specifici e ulteriori controlli sulla privacy vengono descritti alla fine del capitolo 7 (Controlli 14-16).

6. GOVERNANCE DELLA SICUREZZA DELLE INFORMAZIONI

6.1 Che cos'è la governance della sicurezza delle informazioni?

La governance della sicurezza delle informazioni riguarda l'uso di asset per garantire un'implementazione efficace della sicurezza delle informazioni e fornisce la garanzia che:

- vengano rispettate le direttive in materia di sicurezza delle informazioni; e
- l'organo direttivo riceva una reportistica affidabile e pertinente in merito alle attività inerenti alla sicurezza delle informazioni.

L'implementazione di controlli di sicurezza, in assenza di una precisa strategia e di obiettivi chiari può renderli inefficaci e persino dannosi per l'azienda. Per questo motivo, la governance aziendale è essenziale. La governance IT, che indirizza l'implementazione delle tecnologie dell'informazione e della comunicazione, e la governance della sicurezza delle informazioni, che guida la gestione delle informazioni, fanno entrambe parte della governance aziendale.

La governance aziendale dell'informazione e della tecnologia (EGIT - *Enterprise Governance of Information and Technology*) è complessa e sfaccettata. Pertanto, i membri degli organi direttivi e i vertici aziendali in genere devono adattare le azioni proprie in materia di EGIT e attuarle in base al proprio contesto e alle proprie esigenze specifiche.

Fondamentalmente, l'EGIT riguarda il valore ottenuto tramite la trasformazione digitale, nonché la mitigazione del rischio aziendale che ne deriva.

Più specificamente, ci si possono aspettare tre risultati principali dopo aver efficacemente implementato l'EGIT:

- ottenimento di vantaggi
- ottimizzazione del rischio
- ottimizzazione degli asset.

6.2 ISO/IEC 27014

Lo standard ISO/IEC 27014 stabilisce la strategia da seguire in relazione alla governance della sicurezza delle informazioni. Definisce 6 obiettivi:

1. garantire che l'approccio alla sicurezza delle informazioni a livello di organizzazione sia in linea con gli obiettivi aziendali;
2. garantire che le decisioni vengano prese adottando un approccio basato sul rischio;
3. garantire che l'acquisizione di prodotti e servizi segua procedure e direttive definite (imposta le direttive per l'acquisizione);
4. garantire che la sicurezza delle informazioni sia conforme ai requisiti interni ed esterni;
5. promuovere una cultura orientata alla sicurezza;
6. garantire che le prestazioni in materia di sicurezza siano conformi ai requisiti attuali e futuri dell'azienda.

Questi obiettivi possono essere raggiunti se viene stabilita una strategia di governance della sicurezza basata sui seguenti quattro processi:

1. valutazione
2. regolamentazione
3. monitoraggio
4. comunicazione.

Lo standard ISO/IEC 27014 introduce una distinzione tra l'organo direttivo, che valuta, indirizza e monitora, e l'organo di gestione, incaricato di implementare l'ISMS, facendo riferimento allo standard ISO/IEC 27001.

Come avviene di consueto negli standard, l'ISO/IEC 27014 dice cosa fare, ma non come farlo; di conseguenza, è necessaria una conoscenza approfondita per applicare la strategia definita dall'organo direttivo ai processi e alle procedure concrete e misurabili. Questa conoscenza può essere fornita dal COBIT.

6.3 COBIT

Che cos'è il COBIT?

Il COBIT (*Control Objectives for Information and related Technology* - Obiettivi di controllo per le informazioni e le tecnologie correlate) è un modello per la governance e la gestione delle informazioni e delle tecnologie aziendali, comprese le problematiche di sicurezza, rivolto all'intera impresa. L'I&T aziendale riguarda tutta la tecnologia relativa all'elaborazione delle informazioni che l'azienda utilizza per raggiungere i propri obiettivi, indipendentemente da dove ciò avvenga all'interno dell'azienda. In altre parole, l'I&T aziendale non si limita al reparto IT di un'organizzazione, ma certamente lo include.

Il modello COBIT stabilisce una chiara distinzione tra governance e gestione. Queste due discipline comprendono attività diverse, richiedono strutture organizzative diverse che servono a scopi diversi.

La **governance** garantisce che:

- le esigenze, le condizioni e le scelte delle parti interessate vengano valutate per determinare obiettivi aziendali equilibrati e concordati;
- le direttive vengano stabilite attraverso la definizione delle priorità e il processo decisionale;
- le prestazioni e la conformità vengano monitorate rispetto alle direttive e agli obiettivi concordati.

La **gestione** pianifica, definisce, gestisce e monitora le attività, in linea con l'indirizzo stabilito dall'organo direttivo, per raggiungere gli obiettivi aziendali.

Struttura del COBIT:

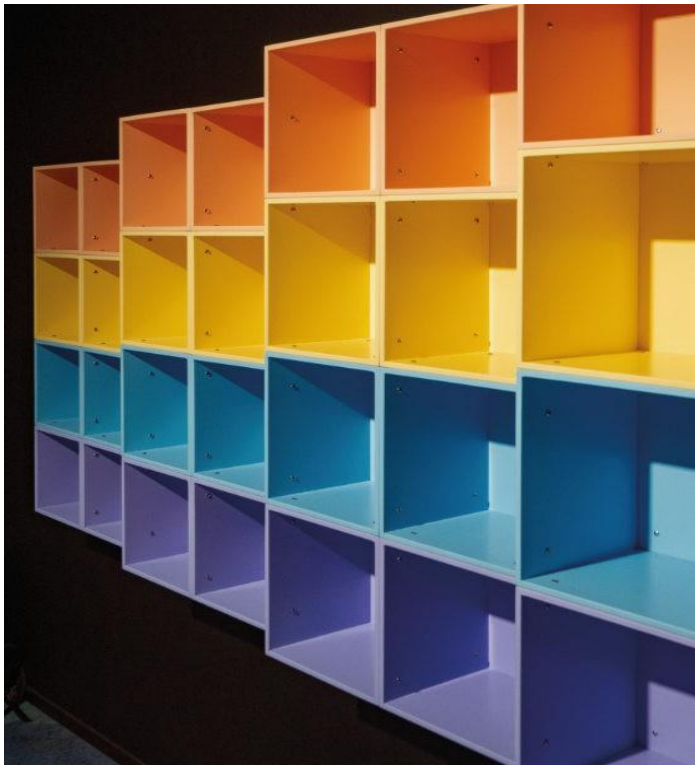
Affinché le informazioni e le tecnologie contribuiscano agli obiettivi aziendali, è indispensabile raggiungere una serie di obiettivi di governance e gestione. Nel modello COBIT, gli obiettivi di governance e gestione sono raggruppati in cinque domini (1 nella sezione A e 4 nella sezione B):

- A. Gli obiettivi di governance sono raggruppati nel dominio "Evaluate, Direct and Monitor" (**EDM** – Valutazione, Indirizzo e Monitoraggio). In questo dominio, l'organo direttivo valuta le opzioni strategiche, indirizza i vertici aziendali in merito alle opzioni strategiche scelte e monitora i risultati della strategia.
- B. Gli obiettivi di gestione sono raggruppati negli altri quattro domini:
  - Il dominio "Align, Plan and Organise" (**APO** – Allineamento, Pianificazione e Organizzazione) riguarda l'azienda nel suo complesso, la strategia e le attività di supporto in ambito I&T;
  - Il dominio "Build, Acquire and Implement" (**BAI** –Sviluppo, Acquisizione e Attuazione) riguarda lo sviluppo, l'acquisizione e l'attuazione delle soluzioni I&T, nonché la loro integrazione nei processi aziendali;
  - Il dominio "Deliver, Service and Support" (**DSS** – Erogazione, Servizio e Assistenza) riguarda l'effettiva erogazione e il supporto per i servizi I&T, compresa la sicurezza;
  - Il dominio "Monitor, Evaluate and Assess (**MEA** – Monitoraggio, Analisi e Valutazione) riguarda il monitoraggio del risultato e la conformità dell'I&T rispetto agli obiettivi prestazionali e di controllo interni, nonché ai requisiti esterni.

Perché applicare il modello COBIT?

L'applicazione della metodologia COBIT alla sicurezza delle informazioni offre diversi vantaggi, tra cui:

- riduzione della complessità e maggior efficacia in termini di costi, attraverso una migliore e più facile integrazione e allineamento degli standard di sicurezza delle informazioni, delle buone pratiche e/o delle linee guida specifiche del settore;
- maggior soddisfazione delle parti interessate, grazie a una miglior comprensione della sicurezza delle informazioni e dei suoi risultati;
- miglior integrazione della sicurezza delle informazioni in tutta l'azienda;
- adozione di decisioni più ponderate e maggior consapevolezza dei rischi;
- miglioramenti in ambito di prevenzione, rilevamento e ripristino;
- riduzione, sia in termini di impatto che di probabilità, degli incidenti di sicurezza delle informazioni;



- miglior sostegno all'innovazione e alla competitività;
- miglior gestione e ottimizzazione dei costi relativi alla sicurezza delle informazioni;
- miglior comprensione della sicurezza delle informazioni da parte degli interessati.

7. CONTROLLI PER LA SICUREZZA DELLE INFORMAZIONI E LA PROTEZIONE DELLA PRIVACY

7.1 Introduzione

Lo standard ISO/IEC 27002 comprende ben 114 controlli. Data la complessità, nonché l'onerosità economica dell'implementazione di tali controlli da parte delle PMI, questo capitolo illustra e raccomanda l'applicazione di 16 controlli[7], al fine di garantire una protezione minima efficace dei dati aziendali. Riguardano differenti livelli di protezione e sono stati classificati come di seguito indicato:

Categoria	Controllo
Controlli sulle persone	**Controllo N° 13**[8]: Consapevolezza in materia di sicurezza delle informazioni
Controlli organizzativi	**Controllo N° 1**: Gestione degli asset (compresa la procedura di classificazione) **Controllo N° 2**: Politiche, standard e linee guida **Controllo N° 3**: Gestione degli incidenti **Controllo N° 14**: Aspetti di sicurezza delle informazioni in relazione ai fornitori **Controllo N° 15**: Organizzazione della sicurezza delle informazioni **Controllo N° 16**: Ulteriori controlli sulla privacy
Controlli parzialmente organizzativi/tecnologici	**Controllo N° 4**: Gestione del controllo degli accessi
Controlli tecnologici (relativi all'ICT)	**Controllo N° 5**: Sicurezza di rete e scambi di dati **Controllo N° 6**: Gestione delle vulnerabilità **Controllo N° 7:** Protezione contro i malware **Controllo N° 8:** Gestione dei backup **Controllo N° 9:** Gestione delle misure di salvaguardia **Controllo N° 10:** Prontezza ICT per la continuità operativa **Controllo N° 11**: Lavoro a distanza **Controllo N° 12**: Monitoraggio delle minacce informatiche

La categoria "Controlli sulle persone" mira a sensibilizzare il personale delle PMI in materia di sicurezza delle informazioni. L'intento di questa tipologia di controllo è quello di stabilire delle linee guida per il personale e gli utenti delle PMI, che consentano loro di conformarsi agli obiettivi di sicurezza delle informazioni mediante la consapevolezza, l'addestramento e la formazione.

7. Nello standard ISO/IEC 27002, alcuni dei 16 controlli elencati sono costituiti da più controlli correlati.
8. I numeri dei controlli si riferiscono a quelli illustrati nel capitolo 7.2.

La categoria "Controlli organizzativi" si rivolge al lato gestionale della sicurezza delle informazioni, utilizzando la matrice RACI. Nel momento in cui una PMI organizza la sicurezza delle proprie informazioni, deve definire e assegnare i ruoli principali relativi alla sicurezza al personale responsabile, stabilendo precisi meccanismi di reportistica alla dirigenza. Inoltre, la PMI deve:

- gestire e proteggere i propri asset digitali,
- rispondere adeguatamente agli incidenti che compromettono i propri dati,
- sviluppare politiche e linee guida per garantire e mantenere la conformità per quanto riguarda la gestione delle informazioni,
- condividere informazioni pertinenti e affidabili con i propri fornitori e garantire un'adeguata gestione e protezione dei dati condivisi da parte dei fornitori mediante adeguati meccanismi di risposta agli eventuali incidenti,
- il controllo N° 16 illustra gli ulteriori controlli definiti nello standard ISO/IEC 27701, che riguardano esclusivamente la protezione della privacy ritenuta importante per le PMI.

L'accesso alle informazioni comporta competenze sia di tipo direttivo che di tipo tecnico, al fine di assicurare che le persone autorizzate possano accedere ai dati in modo continuativo. La gestione del controllo degli accessi si occupa di questi aspetti.

Infine, **la categoria "Controlli tecnologici (relativi all'ICT)"** riguarda la maggior parte delle attività tecniche necessarie per proteggere la rete dell'impresa. Questi controlli affrontano i seguenti aspetti:

- facilitare lo scambio dei dati e impostare procedure adeguate per il backup degli stessi, nonché per il lavoro a distanza
- affrontare e gestire vulnerabilità, minacce informatiche e malware
- garantire adeguate misure di salvaguardia e preservare la continuità operativa a seguito di un attacco informatico

Come spiegato nel capitolo 5, lo standard ISO/IEC 27701 integra i requisiti previsti dallo standard ISO/IEC 27001, nonché i controlli specificati nello standard ISO/IEC 27002. Questo capitolo utilizza il medesimo approccio: è presente un paragrafo per ciascun controllo di sicurezza delle informazioni che sia stato selezionato come rilevante per le PMI. Qualora nello standard ISO/IEC 27701 un controllo della sicurezza delle informazioni presenti ulteriori requisiti in relazione alla privacy, a tale controllo è stato aggiunto un sottoparagrafo denominato "Estensione alla privacy".

È importante tener presente che i 16 controlli di seguito illustrati costituiscono le raccomandazioni minime richieste che le PMI devono implementare per essere conformi ai requisiti del GDPR.

7.2 Controlli

Tutti i controlli di seguito illustrati presentano la medesima struttura. La denominazione e la descrizione del controllo sono seguite da una "guida", che spiega cosa devono fare le PMI per implementare il controllo e raggiungere il relativo obiettivo. Tale guida fornisce la **"base minima" da implementare.** Come riportato nel capitolo 4, questi controlli NON sono soggetti alla gestione del rischio.

La struttura di ciascun controllo è composta da:

- **Controllo**: una descrizione chiara dell'azione da avviare e portare a termine.
- **Obiettivo**: illustra, per quanto possibile, l'obiettivo che il controllo intende raggiungere, in modo SMART[9].
- **Ambito**: il contesto che il controllo intende considerare.
- **Situazione attuale**: una visione pragmatica dell'attuale situazione del controllo all'interno delle PMI. Alcune PMI sono, naturalmente, molto più conformi e abituate alle buone pratiche.
- **Guida**: un elenco di azioni obbligatorie dettagliate necessarie per effettuare il controllo, corredato, se del caso, da una procedura pratica riportata in un allegato.

9. SMART significa: Specifico e Semplice, Misurabile (quindi, concreto), Accettabile / Ambizioso / realizzabile (sufficiente per motivare le persone ad agire), Realistico e con Tempistiche precise. In generale, la T è da intendersi come "CONTINUATIVO", in quanto i controlli proposti sono considerarsi quale base minima, senza la quale non è possibile una reale gestione della sicurezza delle informazioni.

- **Privacy**: alcune considerazioni che collegano le linee guida alla protezione delle informazioni personali.

CONTROLLO N° 1: GESTIONE DEGLI ASSET

Controllo

La gestione degli asset deve essere implementata per consentire una corretta amministrazione delle informazioni e degli asset collegati, nonché stabilire l'idoneo livello di protezione.

Obiettivo

Far sì che le PMI abbiano la possibilità di accertarsi che i propri investimenti (anche per quanto riguarda la sicurezza e la protezione dei dati) siano giustificati.

Ambito

Questo controllo riguarda le informazioni, i processi, i supporti che contengono le informazioni, le apparecchiature ICT che memorizzano, gestiscono e trasmettono le informazioni, nonché i luoghi fisici in cui si trovano. È costituito da un complesso di sette controlli coordinati, che sono tutti necessari per raggiungere l'obiettivo previsto.

Situazione attuale

Gli asset ICT, gli arredi e i materiali di consumo vengono gestiti, quantomeno in modo essenziale, mentre le informazioni non lo sono affatto. Gli asset vengono gestiti come di seguito indicato:

- **Acquisizione degli asset**: l'acquisizione degli asset consente alle PMI di conoscere e registrare il fornitore. Gli asset vengono generalmente acquistati presso fornitori di fiducia. Non è così per le informazioni: la fonte non sembra essere ritenuta importante e non viene registrata. Di conseguenza, qualora si verifichi un problema al riguardo, non è possibile inoltrare alcun reclamo e, nel caso in cui le informazioni siano essenziali per la PMI, non c'è nulla che si possa fare.

- **Identificazione e valutazione degli asset**: mentre l'identificazione e la valutazione sono frequenti e indispensabili nel caso di asset materiali, raramente vengono applicate alle informazioni. Non esiste alcun inventario delle informazioni, né dei supporti su cui vengono memorizzate. Le informazioni non vengono valutate. La valutazione delle informazioni viene denominata "Classificazione delle informazioni". Il valore dell'asset è un fattore cruciale per poter determinare le conseguenze di un rischio che si manifesti concretamente.

Il valore facilita anche la decisione sulla solidità e tenuta della protezione (e quindi anche del suo costo). Determinare il valore delle informazioni consente alle PMI di valutare il rischio di violazioni della riservatezza, dell'integrità e della disponibilità, nonché di determinare cosa si potrebbe fare (valore rispetto al costo) per contrastare tale rischio.

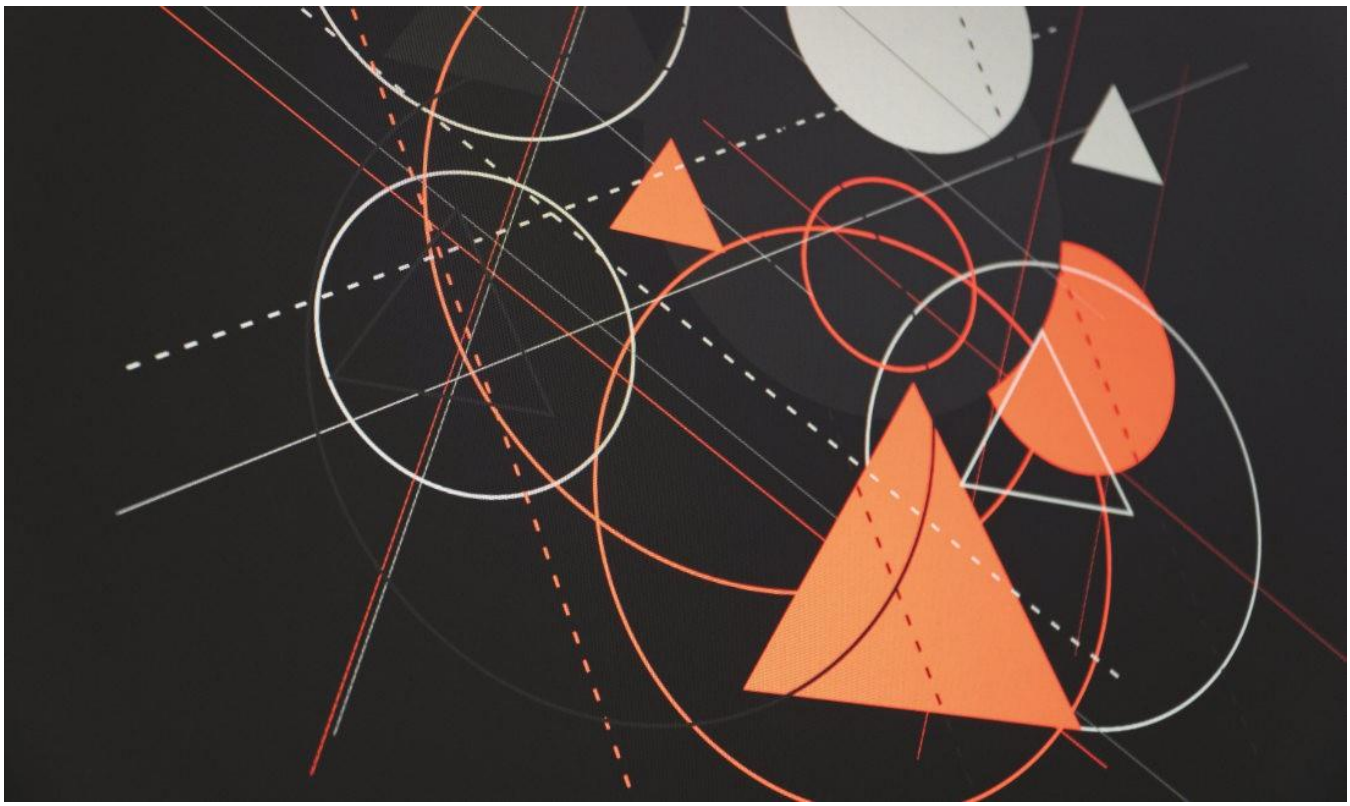
- **Conservazione degli asset**: gli asset non direttamente utilizzati vengono conservati e ne viene registrata l'evoluzione nel tempo. Le apparecchiature ICT vengono conservate secondo le specifiche del fornitore e il denaro è al sicuro in cassaforte.
Le informazioni vengono invece archiviate in cartelle, raccoglitori o registri e nella memoria dei computer. Nessuno ha tuttavia un'idea chiara di dove si trovino esattamente e quale sia il loro stato. Questo significa che è possibile che non tutti gli utenti utilizzino la medesima versione delle informazioni. Generalmente non esiste un luogo sicuro in cui conservare le informazioni più importanti.

- **Uso degli asset**: gli asset materiali vengono utilizzati in base all'uso raccomandato ed esistono politiche e regole in merito. Sugli asset ICT viene apposta un'etichetta che ne indica il proprietario e il relativo codice di inventario. Le informazioni vengono utilizzate attraverso processi aziendali, che controllano il flusso e le operazioni effettuate su di esse. I processi informatici non sono sempre descritti formalmente (persino nelle grandi imprese), il che causa problemi qualora il processo sia automatizzato all'interno di un programma per PC.

- **Manutenzione degli asset**: la manutenzione degli asset materiali viene eseguita in base alle raccomandazioni del fornitore, ma, per quanto riguarda le informazioni, la manutenzione risulta davvero scarsa. Possono infatti esistere più versioni delle medesime informazioni e il controllo effettuato è minimo.

- **Scambio di asset**: viene registrato lo scambio di asset materiali all'interno dell'azienda e con soggetti terzi. Il trasferimento avviene attraverso canali riconosciuti e l'imballaggio garantisce che non si verifichino danni durante il trasporto.
Gli scambi di informazioni, invece, avvengono spesso senza un'adeguata protezione e c'è generalmente uno scarso controllo su chi può o non può farlo.

- **Smaltimento degli asset**: qualora gli asset materiali vengano danneggiati, diventino obsoleti o non più utilizzabili, vengono smaltiti, generalmente tramite gli appositi circuiti ecologici. Invece, le informazioni vengono purtroppo di solito semplicemente "cancellate" e i relativi supporti vengono eliminati senza prestare la dovuta attenzione a ciò che contenevano, né che la cancellazione sia avvenuta in modo corretto.



Guida

Lo standard ISO /IEC 27002 raccomanda di gestire le informazioni come se fossero asset materiali.

- **Le informazioni devono essere acquisite da fonti affidabili e attendibili**. Le informazioni provenienti da Internet devono essere verificate due volte.
Ad esempio, le Informazioni di identificazione personale (PII) – denominate Dati personali nel GDPR - fornite da dipendenti, clienti e fornitori vengono verificate e i dati finanziari e contabili vengono sempre controllati e monitorati. Lo stesso deve essere fatto per le informazioni che costituiscono un valore per la PMI.

- **Le informazioni devono essere inventariate e classificate** in base ai tre criteri di sicurezza - Riservatezza, Integrità, Disponibilità – a seconda della loro importanza per il raggiungimento degli obiettivi aziendali. L'Allegato A propone una tecnica semplice per classificare le informazioni e gli asset materiali che contengono e gestiscono le informazioni.
La classificazione e l'inventario delle informazioni non devono necessariamente avvenire per ogni singola informazione, ad eccezione di quelle che sono del massimo valore. È più pratico assegnare la medesima classificazione a ciascuna categoria di informazioni (ad esempio PII per conformarsi al GDPR). L'inventario delle informazioni deve riportare la fonte e la data di acquisizione, poiché in molti casi diventano rapidamente obsolete. **Nota:** da ora in poi, con il termine "**Informazioni protette**" si intenderanno le informazioni che ottengono il livello 3 o superiore applicando la tecnica di cui all'Allegato A).

- **Le Informazioni protette devono essere contrassegnate.** I file di dati dei computer possono essere contrassegnati usando i campi disponibili delle "Proprietà dei file". Si raccomanda l'impiego delle indicazioni di riservatezza, integrità e/o disponibilità. Anche contrassegnare i documenti nel piè di pagina o nell'intestazione può costituire una buona soluzione.
I supporti dei dati devono essere contrassegnati in base al livello di riservatezza (ad esempio utilizzando un codice a colori), per indicare al personale come devono gestirli.

- Le informazioni devono essere conservate in conformità alla relativa classificazione, indipendentemente dal supporto o dal formato, con ulteriori regole specifiche per quanto riguarda le Informazioni protette.

    - Per le informazioni e le applicazioni devono essere implementare misure di salvaguardia e backup commisurate al valore delle informazioni (proprio come se fossero valori finanziari), ad esempio numero, frequenza e ubicazione;

    - Si devono adottare misure per preservare l'integrità delle informazioni, indipendentemente dalla durata della loro conservazione; le Informazioni protette devono essere soggette a test regolari, per verificare che siano leggibili e utilizzabili qualora debbano essere ripristinate;

    - Devono essere implementati controlli di accesso, per garantire che solo le persone e le applicazioni autorizzate abbiano accesso alle informazioni nelle condizioni specificate (fare riferimento al Controllo N° 4).

- Le informazioni non classificate quali "Informazioni protette" devono essere gestite e utilizzate con un livello standard di attenzione, mentre le "Informazioni protette" devono essere usate esclusivamente da personale autorizzato e in conformità alle regole specifiche riportate nelle politiche (fare riferimento al Controllo N° 2), poiché un uso improprio delle stesse, anche accidentale, potrebbe esporre l'azienda a un rischio.

- Le Informazioni protette devono essere soggette un processo di manutenzione formale, per garantire che siano sempre pertinenti, precise e disponibili.

- Lo scambio e la comunicazione di informazioni sono essenziali per il raggiungimento degli obiettivi aziendali. È tuttavia necessario adottare e documentare regole finalizzate a garantire che le Informazioni protette vengano scambiate esclusivamente con parti interessate interne ed esterne autorizzate e all'interno di un contenitore adeguato (ad esempio un contenitore sigillato accompagnato da una descrizione del suo contenuto, file crittografati, VPN, ecc.). La comunicazione di Informazioni protette a soggetti esterni:

    - deve essere vietato durante incontri informali e in luoghi pubblici;

    - durante incontri formali, riunioni e conferenze, deve avvenire secondo regole specifiche e dopo aver ricevuto l'espressa autorizzazione dei vertici aziendali.

- Nel caso in cui le informazioni diventino inutili o non più rilevanti per l'azienda, ciò non significa che abbiano perso il proprio valore per altre parti (non autorizzate):
    - infatti, tali parti non autorizzate potrebbero scoprire qualche dato da usare a proprio vantaggio e a sfavore dell'azienda;
    - inoltre, i supporti digitali di memorizzazione smaltiti (chiavette USB, dischi fissi, ecc.) potrebbero contenere software e applicazioni per i quali sono state pagate le licenze e il successivo uso illegale degli stessi da parte di terzi potrebbe causare problemi di natura legale.

    Lo smaltimento delle informazioni deve avvenire con cura e la regola standard è che devono essere cancellate o distrutte. Le Informazioni protette devono essere triturate (carta, carte bancarie, CD/DVD), debitamente cancellate o crittografate (dati digitali).

Estensione alla privacy

La privacy costituisce una categoria speciale di informazioni, che richiede un diverso processo di classificazione, fornito dalla Valutazione d'impatto sulla privacy (PIA), che misura l'impatto delle violazioni della sicurezza sull'Interessato.

CONTROLLO N° 2: POLITICHE, STANDARD E LINEE GUIDA

Controllo

Devono esistere informazioni documentate, per dichiarare e rendere noti a tutte le parti interessate gli obiettivi, le linee guida e i requisiti relativi alla sicurezza delle informazioni.

Obiettivo

Far sì che le PMI siano in grado di garantire che il proprio personale e tutte le persone coinvolte nella gestione delle informazioni dell'impresa siano a conoscenza e si attengano a quanto sopra, in modo da poter essere e rimanere conformi ai requisiti esterni e legali relativi alle informazioni.

Ambito

Questo controllo riguarda tutti gli obiettivi, le regole e le raccomandazioni che le parti interne ed esterne coinvolte devono seguire e rispettare.

Situazione attuale

Le PMI documentano raramente i propri obiettivi, le proprie regole e le proprie aspettative in materia di gestione e sicurezza delle informazioni, mentre lo fanno per le risorse umane e le risorse finanziarie. Tuttavia, in conformità al Controllo N° 1, le informazioni costituiscono un valore importante, che deve essere tutelato.

Guida

Gli obiettivi, le regole e le direttive in materia di sicurezza delle informazioni devono essere formalizzati e comunicati a tutto il personale, per assicurarsi che siano ben definiti, noti e applicati.

Devono essere disponibili due politiche importanti:

- la politica generale in materia di sicurezza delle informazioni, che definisce gli obiettivi da raggiungere su base continuativa e che contiene quelli ritenuti conformi al GDPR (Politica sulla protezione della privacy);
- la politica di riservatezza che stabilisce, per le persone di cui si raccolgono e gestiscono i dati personali (dipendenti, clienti/acquirenti, fornitori, partner), quali informazioni sono necessarie, con chi vengono condivise, per quale motivo e per quanto tempo vengono conservate, come possono essere esercitatati i diritti di cui godono gli interessati e come presentare un reclamo, qualora i suddetti interessati ritengano vi siano state delle irregolarità.

Dovrebbero inoltre essere formalizzate regole specifiche in materia di archiviazione, gestione, controllo degli accessi, distruzione, backup, comunicazione a soggetti esterni mediante:

- uno **standard** è un regolamento che deve essere applicato in qualsiasi circostanza e a cui si può fare riferimento in caso di mancata conformità;
- una **linea guida** è una raccomandazione relativa al "modo migliore" di gestire le informazioni e la loro sicurezza.

È essenziale che le "politiche" vengano approvate dai vertici aziendali e vengano regolarmente riviste e aggiornate, per allinearle ai cambiamenti delle condizioni operative e delle circostanze. La "linea guida" raccomandata è soggetta a una revisione annuale. Le "politiche" devono costituire un punto di riferimento e altresì devono focalizzarsi sulle persone a cui sono rivolte. L'ampiezza e il tipo di formulazione dipendono dalla situazione e dalle esigenze specifiche. La documentazione è la base fondamentale per informare, addestrare e formare le persone.

Estensione alla privacy

Deve essere redatta e rivista regolarmente una politica specifica in materia di protezione della privacy.

CONTROLLO N° 3: GESTIONE DEGLI INCIDENTI

Controllo

Gli incidenti di sicurezza delle informazioni devono essere gestiti.

Obiettivo

Far sì che le PMI siano preparate a rispondere adeguatamente agli incidenti di sicurezza delle informazioni, per garantire una risoluzione rapida e coerente di tutte le turbative operative, finanziarie, legali e commerciali e contenere i danni entro limiti predefiniti.

Ambito

Questo controllo riguarda tutti gli incidenti causati da violazioni della riservatezza, dell'integrità e della disponibilità delle informazioni. Riguarda ovviamente anche le violazioni della privacy.

Situazione attuale

La gestione del rischio, scarsamente applicata nelle PMI, non è sempre perfetta, perché non esiste il "rischio zero". Un incendio, ad esempio, può verificarsi anche se vengono adottate tutte le necessarie misure preventive. Gli esseri umani possono commettere errori e possono insorgere guasti tecnici.

Nel caso le informazioni siano mal gestite e mal protette, si verificano molti eventi e incidenti senza che vengano rilevati e senza che si applichino le opportune contromisure. Qualora l'impatto diretto non sia eccessivo, le conseguenze sull'azienda si manifestano spesso in tempi successivi e possono anche essere di ampia portata, senza che sia possibile associarle direttamente all'incidente verificatosi in precedenza.

Guida

Qualunque sia l'attività svolta, le misure che si adottano e i controlli che si implementano e gestiscono per prevenire i rischi, gli eventi si verificheranno comunque e turberanno lo svolgimento delle attività. Qualora influiscano sugli obiettivi aziendali, si trasformeranno in incidenti aziendali. Nel caso in cui influiscano sugli obiettivi di sicurezza delle informazioni, diventeranno incidenti di sicurezza delle informazioni. L'unico standard ISO/IEC che descrive i concetti, i principi e il processo di gestione degli incidenti è l'ISO/IEC 27035-1. La presente guida offre una breve panoramica su ciò che deve essere fatto per essere in grado di rispondere in modo soddisfacente a tali incidenti.

È di importanza fondamentale predisporre una risposta agli incidenti tramite procedure predefinite e testate oltre all'addestramento del personale, al fine di far emergere eventi e situazioni anomali, nonché di squadre specializzate, che si occuperanno di applicare le opportune contromisure.

Una gestione coerente degli incidenti prevede 5 fasi:

1. **Plan and Prepare (Pianificazione e Preparazione)**

In questa fase, l'azienda decide di affrontare gli incidenti, per evitare che diventino ingestibili. Per farlo, deve realizzare quanto di seguito descritto:

- redigere una politica per organizzare e gestire gli incidenti;
- designare una persona, facente parte dei vertici aziendali, che sarà responsabile della gestione degli incidenti;
- elencare gli incidenti che si desidera affrontare;
- documentare (se necessario avvalendosi della collaborazione di esperti interni ed esterni) la procedura o le procedure che si intende adottare qualora si verifichi un incidente;
- decidere e nominare la persona incaricata di gestire l'incidente e coordinare le azioni (gestore dell'incidente);
- stabilire i criteri e la procedura per dichiarare che un determinato evento costituisce un "incidente";
- individuare e nominare la squadra che interverrà per reagire all'incidente secondo la procedura;
- stabilire e predisporre i mezzi necessari per consentire al gestore dell'incidente di essere informato, nonché il tipo di informazioni da comunicare; tali mezzi potranno essere automatizzati o attivati manualmente;
- predisporre e implementare un piano di sensibilizzazione e addestramento, per assicurarsi che tutte le persone coinvolte sappiano cosa fare.

2. **Detect (Rilevamento)**

Assicurarsi che tutto il personale abbia la possibilità di segnalare l'evento al gestore dell'incidente (come avviene in caso di incendi o lesioni alle persone), senza rischiare una sanzione. La segnalazione dovrà essere la più tempestiva possibile, poiché un ritardo nella risposta potrebbe causare danni irreparabili.

3. **Evaluate and Decide (Valutazione e Decisione)**

Il gestore dell'incidente segue la procedura per valutare l'evento e dichiararlo o meno un "incidente".

- Qualora non si tratti di un incidente, il gestore dell'incidente informa della situazione la persona responsabile del processo, dell'asset o dei servizi ICT, per consentirle di cercare un rimedio;
- Nel caso in cui si tratti di un incidente, il gestore dell'incidente attiva la squadra di risposta (interna o esterna), che ha le competenze e la capacità per intervenire.

4. Respond (Risposta)

Il gestore dell'incidente rimane responsabile del coordinamento delle azioni fino a quando l'incidente non viene dichiarato chiuso. Verranno registrate le azioni intraprese durante la sequenza temporale. La squadra di risposta comunicherà regolarmente con i gestori dell'incidente, per tenerli informati sull'evoluzione dei fatti:

- Qualora la situazione peggiori o necessiti di ulteriori risorse, il gestore dell'incidente le convoca, previa autorizzazione da parte dei vertici aziendali, se necessario;
- Nel caso in cui la situazione risulti fuori controllo, il gestore dell'incidente informa i vertici aziendali e viene attivato il Piano di continuità operativa (*Business Continuity Plan*) (parzialmente o integralmente).

Il gestore dell'incidente dichiara l'incidente chiuso dopo averne discusso con la squadra aziendale coinvolta e averne ottenuto l'approvazione.

Una volta chiuso l'incidente, il gestore dell'incidente prepara la relativa reportistica, usando il modello predefinito, e la inoltra ai vertici aziendali.

Qualora in seguito all'incidente fosse necessario intraprendere delle ulteriori azioni (ad esempio azioni legali), il gestore dell'incidente manterrà informate le squadre sull'evoluzione della situazione.

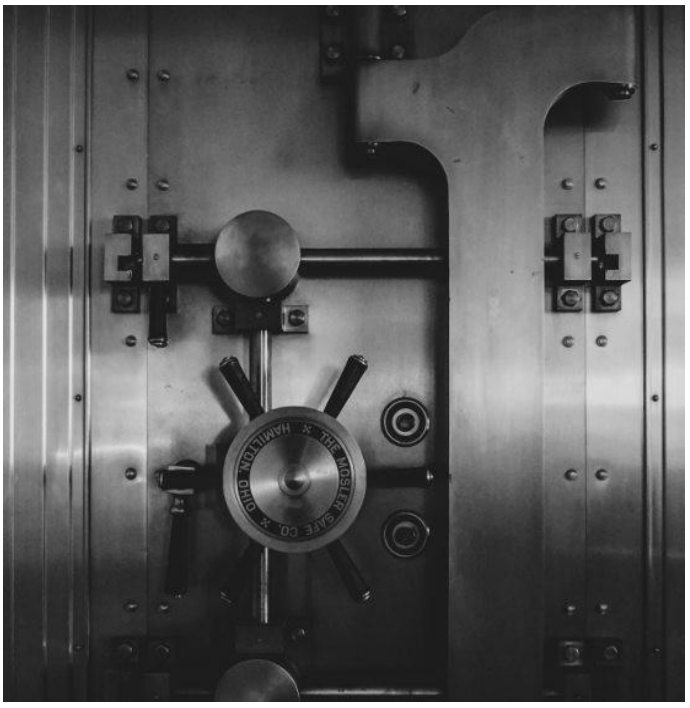
5. Learn lessons (Apprendere dall'esperienza)

Tutti gli eventi o incidenti e il modo in cui sono stati affrontati forniscono informazioni essenziali sulla capacità di prevenirli e gestirli in futuro. Per questo motivo, è importante imparare dalle esperienze acquisite. Di conseguenza, verrà riunita una squadra (possibilmente la stessa che ha preparato il piano di gestione o di risposta), per capire se è possibile introdurre dei miglioramenti:

- miglior prevenzione dell'evento (miglioramento dei controlli o delle procedure operative);
- miglior capacità di risposta (risorse, competenze, supporto delle attrezzature);
- miglior reportistica e comunicazione.

6. Ulteriori informazioni

In alcuni casi, il GDPR richiede che la persona/le persone interessate o l'autorità per la protezione dei dati – la "parte esterna" – vengano informate. Pertanto, le regole aziendali devono anche prevedere che il "titolare delle informazioni (a cui l'impresa ha avuto accesso)" venga informato qualora accada qualcosa a tali informazioni. Analogamente, nel caso in cui qualcuno possa subire delle conseguenze a causa di un errore, bug o incidente, questi dovrà essere informato, in modo che possa reagire adeguatamente. In alcuni casi, la "parte esterna" potrà anche aiutare l'impresa a risolvere il problema.



Affinché ciò sia possibile, deve essere predisposto un piano di comunicazione formale, che indichi chi è autorizzato a comunicare con i soggetti terzi e come. Una comunicazione scorretta o impropria può avere gravi conseguenze sulla reputazione di un'impresa.

Estensione alla privacy

Gli incidenti relativi ai dati personali seguono il medesimo processo generico previsto per gli incidenti di sicurezza delle informazioni. Il GDPR richiede che, a seconda dell'impatto sull'Interessato, quest'ultimo e l'Autorità nazionale per la protezione dei dati vengano informati entro 72 ore.

CONTROLLO N° 4: GESTIONE DEL CONTROLLO DEGLI ACCESSI

Controllo

Il controllo degli accessi deve essere interamente e costantemente gestito in tutti i suoi componenti, nonché essere basato sul ruolo, al fine di raggiungere gli obiettivi aziendali.

Obiettivo

Far sì che le PMI siano in grado di gestire l'accesso alle informazioni, qualunque esse siano, ovunque si trovino e in qualsiasi momento.

Ambito

Questo controllo è una combinazione di diversi controlli interconnessi, che devono essere definiti e implementati contemporaneamente per poter raggiungere gli obiettivi previsti. Riguarda l'accesso alle informazioni (digitali o su supporti fisici) e alle strutture operative, quali uffici e apparecchiature ICT.

Situazione attuale

Troppo spesso il controllo degli accessi risiede nei PC e consiste in un identificatore (user ID) e una password (generalmente debole e identica per tutti gli usi). Una volta che l'utente ha effettuato il login, acquisisce tutti i privilegi.

Una corretta gestione degli accessi si basa su sei elementi:

1. **Gestione delle identità**: tutti gli utenti autorizzati vengono identificati in modo standard. La gestione non è tuttavia sempre aggiornata, in quanto generalmente gli account temporaneamente inattivi non vengono supervisionati e gli account di ex utenti/dipendenti non vengono chiusi con sufficiente tempestività ed è pertanto possibile che si verifichino accessi incontrollati.

2. **Gestione dei privilegi di accesso**: a seconda dei ruoli ricoperti, i privilegi di accesso assegnati consentono di accedere alle informazioni, ma anche di regolamentare le attività, nonché le fasce orarie e i luoghi da cui tali attività sono consentite.
   Molte PMI, tuttavia, il più delle volte concedono i privilegi di accesso senza gestirli correttamente. Questo significa che tutti hanno accesso a tutto oppure gli utenti hanno accesso alle informazioni da una posizione remota, senza che l'impresa sia in grado di intervenire o sapere chi ha commesso un errore, nel caso in cui si verifichino dei problemi.

3. **Gestione dell'autenticazione**: tutti gli utenti identificati utilizzano credenziali dedicate per accedere a risorse e informazioni, a seconda del loro livello di classificazione.
   Il più delle volte, l'unico strumento per l'autenticazione è costituito da una password – generalmente debole – che viene raramente modificata ed è valida per tutti gli account e i servizi. Questo significa che, qualora dipendenti disonesti oppure malintenzionati vengano a conoscenza di tale password, le suddette persone avranno accesso alle informazioni dell'azienda con tutti i privilegi.

4. **Controllo degli accessi**: gli accessi vengono consentiti solo se l'identità, lo strumento di autenticazione e i privilegi corrispondono.
   Questo controllo viene generalmente applicato in maniera abbastanza corretta.

5. **Registrazione degli eventi**: tutti gli accessi e i tentativi di accesso vengono registrati, congiuntamente alla data e all'orario in cui avvengono (DTG), in base al livello di classificazione. Le anomalie vengono segnalate al responsabile degli accessi. Tuttavia, la dimensione del file di log è spesso troppo piccola e, una volta superati i limiti, il sistema inizia a sovrascrivere i dati meno recenti, che di solito risalgono solo a qualche giorno prima. Di conseguenza, le PMI perdono molte informazioni estremamente importanti, che sarebbe invece necessario conoscere qualora si verifichi un incidente.

6. Analisi dei file di log: I file di log devono essere analizzati regolarmente, per identificare i comportamenti anomali e adottare, se necessario, le opportune contromisure.
La maggior parte delle PMI, invece, analizza raramente i file di log, perdendo traccia di eventi che potrebbero per lo meno far sospettare un tentativo di intrusione.

Qualora il controllo degli accessi venga applicato, anche parzialmente, ai sistemi ICT e agli edifici, le persone non autorizzate possono comunque accedere alle Informazioni protette senza eccessivi controlli. L'applicazione del controllo degli accessi a uffici e locali è, tuttavia, più rara. Ai dipendenti non viene generalmente concesso l'accesso agli uffici (non hanno le chiavi) al di fuori dell'orario di lavoro, ma, ad esempio, la pulizia degli uffici avviene solitamente al di fuori dell'orario di lavoro e gli addetti alle pulizie hanno accesso a tutti i locali, in cui le informazioni non sono sempre adeguatamente protette.

Le norme generali relative all'accesso e all'uso del denaro sono un buon esempio da applicare alle informazioni.

Guida

Le regole generali e fondamentali di seguito riportate devono essere applicate sia ai sistemi ICT che ai luoghi fisici, su base continuativa. Il principio generale è che l'accesso degli utenti (comprese le applicazioni) alle informazioni, alle applicazioni, ai servizi e ai locali deve essere concesso esclusivamente qualora sia strettamente necessario per svolgere un determinato incarico.

- **Gestione delle identità**
  - tutti gli utenti, interni ed esterni, vengono registrati in modo standard;
  - gli account temporaneamente inattivi devono essere bloccati (blocco dei privilegi e della possibilità di autenticazione, con monitoraggio costante del loro stato);
  - gli account di tutto il personale e degli utenti che hanno lasciato l'azienda dovranno essere bloccati, per evitarne l'uso illecito, e verranno cancellati dopo un periodo non superiore a tre mesi.
- **Gestione dei privilegi di accesso**
  - I privilegi di accesso alle informazioni riguardano la lettura, la scrittura, la modifica, la copia, la trasmissione/comunicazione (ad esempio via e-mail) e la stampa.
    I privilegi di accesso agli asset riguardano l'uso, la manutenzione, la modifica e lo spostamento (all'interno e/o all'esterno delle strutture aziendali);
  - I privilegi di accesso dovranno essere concessi per eseguire le attività direttamente correlate al ruolo ricoperto nell'impresa e alla necessità di accedere e usare le informazioni; si dovrà verificare su base regolare la correlazione rispetto alla classificazione delle informazioni (fare riferimento all'Allegato A);
  - Alle persone che ricoprono ruoli particolari, quali Amministratori di sistema, Responsabili delle risorse umane, Analisti degli accessi, verranno concessi privilegi particolari (supervisione, ecc.);
  - I privilegi di accesso dovranno inoltre contenere gli orari consentiti e i luoghi autorizzati (interni e/o esterni all'impresa);
  - I privilegi di accesso dovranno essere regolarmente rivisti e aggiornati in base a eventuali cambiamenti di ruolo all'interno dell'impresa.
- **Gestione dell'autenticazione**
  - Esistono tre strumenti di autenticazione utilizzati per verificare l'identità degli utenti autorizzati: qualcosa che si conosce (password, codice pin, ecc.), qualcosa che si possiede (una tessera, una chiave, ecc.) e qualcosa che si è (impronte digitali, firma autografa);
  - La scelta degli strumenti di autenticazione dovrà essere basata sulle tabelle riportate nell'Allegato A;
  - Le password e i codici PIN dovranno essere regolarmente cambiati, soprattutto nel caso in cui l'utente autorizzato abbia lasciato l'azienda;
  - La password avrà una lunghezza minima di otto caratteri (che dovranno comprendere maiuscole e minuscole, cifre e caratteri speciali) e non dovrà essere facilmente intuibile da parte di altri utenti.

- **Controllo degli accessi**
    - Ogni tentativo di accesso richiede la compresenza dell'identificatore e dello strumento di autenticazione associato e deve essere conforme all'orario consentito e al luogo autorizzato per l'accesso;
    - In caso di accesso negato, dovrà comparire un messaggio che segnali che le credenziali di accesso non sono corrette;
    - Si dovrà stabilire un numero massimo di tentativi possibili, dopo di che l'account verrà bloccato per un periodo di tempo predefinito.
- **Registrazione degli eventi**
    - Tutti i tentativi di accesso alle informazioni verranno registrati congiuntamente a data e orario e all'origine della richiesta di accesso;
    - Tutti i dati verranno registrati in un file e conservati per un determinato periodo di tempo (almeno una settimana per gli accessi autorizzati e due settimane per gli accessi negati), al fine di consentirne l'analisi.
- **Analisi dei file di log**
    - L'analisi dei file di log verrà associata a un ruolo privilegiato con un account speciale;
    - Qualora l'analisi dei file di log faccia presumere che vi siano stati tentativi di accesso illeciti oppure si individui un modello noto di intrusione informatica, scatteranno gli allarmi tramite i canali di gestione degli incidenti;
    - Le registrazioni dubbie verranno conservate (salvandole in modalità di sola lettura[10]) in modo tale che (1) non possano essere cancellate, (2) non possano essere modificate e (3) possano essere utilizzate quali prove in caso di reclami o cause legali.

Estensione alla privacy

L'accesso e l'utilizzo dei dati personali richiedono un controllo degli accessi completo, che rispetti le regole definite nel precedente paragrafo "Guida".

10. La memoria di sola lettura (ROM: Read Only Memory) impedisce eventuali ulteriori modifiche.

CONTROLLO N° 5: SICUREZZA DI RETE E SCAMBI DI DATI

Controllo

Le PMI devono gestire e controllare le proprie reti, per proteggere le informazioni contenute nei sistemi e nelle applicazioni a fronte di qualsiasi metodo di connessione.

Obiettivo

Garantire la protezione delle informazioni nelle reti e nelle relative strutture di supporto per l'elaborazione delle informazioni.

Ambito

Questo controllo si applica alla gestione della sicurezza di tutti i dispositivi fisici e logici che fanno parte delle infrastrutture di rete e di comunicazione, a partire dai dispositivi *endpoint* fino alla connessione a Internet. Comprende dispositivi mobili (ad esempio i computer portatili), dispositivi personali (ad esempio gli smartphone), Wi-Fi e dispositivi connessi (ad esempio le telecamere di sicurezza).

Situazione attuale

Fondamentalmente, esistono due tipi di reti: la rete LAN (Local Area Network) e la rete WAN (Wide Area Network). La LAN è la rete controllata dall'azienda, mentre la WAN è controllata da soggetti esterni all'azienda. La più famosa delle reti WAN è Internet. La separazione tra LAN e WAN viene denominata "perimetro".

Prima dell'avvento di Internet e dei cellulari, il perimetro costituiva una barriera robusta, difficile da penetrare da parte di criminali informatici.

Attualmente, invece, il perimetro risulta meno definito. Laptop, smartphone e altri dispositivi mobili escono frequentemente dal perimetro, stabilendo connessioni al di fuori del controllo dell'azienda. Inoltre, il trasferimento di informazioni tra la LAN e la WAN avviene in modo continuo.

Guida

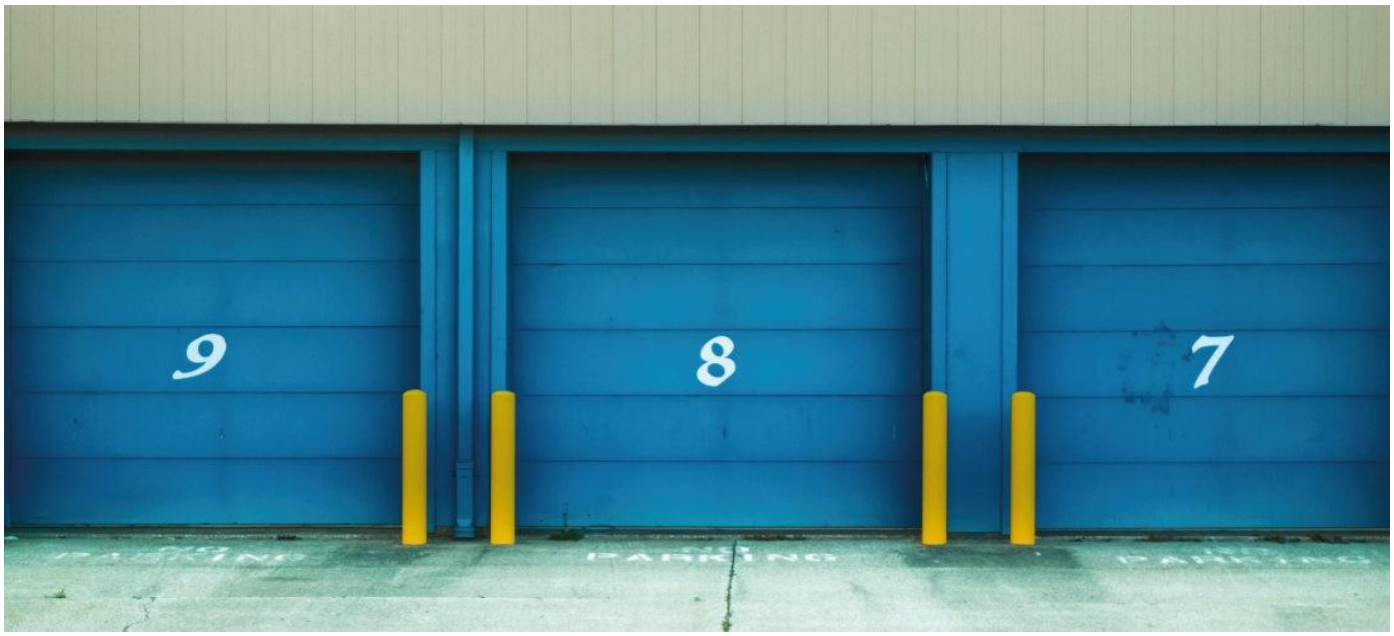
Di seguito si evidenzieranno le fasi più importanti per implementare un adeguato livello di sicurezza per la rete aziendale:

- **Stabilire e mantenere una politica per la sicurezza della connessione**. Tale politica dovrà tenere in considerazione il resto dei punti presentati di seguito.
- Dovranno essere stabilite le **responsabilità e le procedure** per la gestione dei dispositivi di rete.
- **Segregazione della rete**. È necessario suddividere la rete locale (LAN) in domini di rete separati, a seconda delle esigenze di accesso degli utenti, e applicare la regola del "privilegio minimo". Gli utenti dell'area finanziaria, ad esempio, non hanno alcuna necessità di accedere alle informazioni dall'area di ricerca e sviluppo. Se l'azienda ha un'area di produzione, tale area dovrà essere separata dall'area di gestione. La segregazione potrà essere fisica o virtuale. Le connessioni tra domini di rete potranno essere consentite, ma dovranno essere controllate utilizzando un *gateway* (*firewall*, router di filtraggio, ecc.). Pertanto, la rete dovrà essere il più possibile segmentata. È una procedura complessa, ma molto importante, **raggiungere una condizione di equilibrio** tra una corretta segregazione della rete e l'ottimizzazione delle attività aziendali.
- La politica dovrà stabilire se l'azienda intenda consentire o meno ai dispositivi personali utilizzati per le attività professionali, noti come BYOD (**Bring Your Own Device**), di connettersi alla rete. Tali dispositivi sono molto pericolosi, sia perché uniscono attività di natura personale a quelle di natura professionali, sia perché non sono dotati di misure minime di sicurezza. Qualora venga consentito l'accesso alla rete, l'utente dovrà accettare di adottare determinate politiche e misure di sicurezza sul proprio dispositivo.

- Dovrà esistere un'architettura che mostri l'interconnessione delle diverse **funzioni dei dispositivi** in rete e la loro posizione rispetto al *firewall* (il *gateway* protetto per Internet).
- Si dovranno implementare meccanismi di **filtraggio di rete**, quali *firewall* o software per il rilevamento delle intrusioni; adottare politiche di *firewall* per controllare il traffico in entrata e in uscita; applicare la regola "*deny by default*" (negare l'accesso come impostazione predefinita).
- Dovrà esistere uno schema dell'infrastruttura, che indichi gli indirizzi IP interni, il sistema operativo (SO) e il tipo di dati ospitati.
- **Limitare l'accesso fisico e logico ai dispositivi di rete.** Tutti i sistemi in rete dovranno essere autenticati e i sistemi connessi alla rete dovranno essere limitati. Inoltre, dovrà essere garantita l'impossibilità di manipolazione fisica dei dispositivi di rete.
- Un utente al di fuori del perimetro dovrebbe evitare di collegarsi tramite **connessioni WI-FI** che non siano sotto il proprio controllo o sotto il controllo della propria azienda, poiché sono particolarmente pericolose. È molto più sicuro collegarsi mediante il cellulare.
- La pandemia di Covid-19 ha notevolmente aumentato il **telelavoro**. Questo significa che gli utenti, per poter lavorare, si connettono alla rete locale (LAN) dell'azienda attraverso una rete pubblica come Internet (WAN). Per le connessioni di telelavoro, si raccomanda di utilizzare, se possibile, una rete privata virtuale (**VPN**), con crittografia IPSec. Durante la pandemia, molte aziende, in particolare le PMI, hanno abbassato i propri requisiti di sicurezza per consentire il telelavoro, provocando un numero maggiore di incidenti di sicurezza.
- Per consentire la registrazione e l'individuazione di azioni che possono influire o essere rilevanti per la sicurezza delle informazioni, si devono applicare procedure di **registrazione e monitoraggio**.
- Eseguire **test di penetrazione** periodici, per determinare l'adeguatezza della protezione della rete.

Estensione alla privacy

Gran parte delle informazioni che viaggiano attraverso le reti (LAN e WAN) possono essere classificate quali dati personali. Pertanto, è necessario implementare controlli speciali[11] per garantire l'integrità e la sicurezza di tali informazioni. La misura più comune è la crittografia delle comunicazioni, in modo tale da evitare attacchi "*man in the middle*", che consistono nell'intrusione della linea di comunicazione tra il mittente e il destinatario e nell'acquisizione dei frame di rete durante i trasferimenti delle informazioni.



11. Fare riferimento all'Allegato A della guida di SBS per le PMI ai fini dell'implementazione dello standard ISO/IEC 27001 sulla gestione della sicurezza delle informazioni (SBS SME Guide for the implementation of ISO/IEC 27001 on Information Security Management), pagina 30: 10.1.1. e 10.1.2

CONTROLLO N° 6: GESTIONE DELLE VULNERABILITÀ

Controllo

Le PMI devono ridurre al minimo i rischi derivanti dallo sfruttamento doloso di vulnerabilità note. È pertanto fondamentale predisporre misure di salvaguardia per eliminare o controllare le vulnerabilità, mantenere un elenco delle vulnerabilità note rimanenti e accrescere la consapevolezza di tali vulnerabilità all'interno della PMI.

Obiettivo

Ridurre al minimo la presenza di vulnerabilità e promuovere nel personale delle PMI un comportamento prudente in termini di sicurezza.

Ambito

Sulla base dell'inventario aggiornato e completo della PMI, quest'ultima deve verificare ciascun asset ai fini dell'applicazione di patch o altri meccanismi di protezione. Bisogna dare priorità agli asset cruciali per l'attività della PMI o esposti a nuove e serie minacce (fare riferimento al Monitoraggio delle minacce informatiche), compreso il sistema operativo.

Situazione attuale

Per ogni tipo di asset digitale vengono continuamente individuate nuove vulnerabilità. I fornitori rilasciano patch e pubblicano raccomandazioni relative alle vulnerabilità dei propri prodotti, man mano che diventano note. Tuttavia, molte PMI non tengono conto di questo aspetto e, ad esempio, lavorano ancora con sistemi operativi obsoleti e applicazioni che non vengono più aggiornate, a causa di vincoli operativi o finanziari.

Guida

Il problema delle vulnerabilità deve essere affrontato almeno una volta al mese e in particolare nel caso in cui la PMI abbia subito incidenti. La gestione delle vulnerabilità può essere eseguita da una persona designata a tale scopo, che assista gli utenti degli asset nella verifica e nella rimozione delle vulnerabilità o nel loro controllo.

La gestione delle vulnerabilità è un processo in più fasi, costituito da una fase preliminare e da tre fasi che dovranno essere ripetute regolarmente (almeno una volta al mese) oppure a seguito di un incidente subito dalla PMI.

1. **Identificaregli asset digitali**: la PMI deve creare un inventario degli asset digitali (capitolo 7.1) e, per ciascuno di essi, individuare in che modo il fornitore rilascia le patch o pubblica le raccomandazioni.

2. **Assegnare priorità agli asset per la valutazione delle vulnerabilità**: la PMI deve assegnare una priorità a ciascun asset presente nell'inventario, in base alla rispettiva criticità per l'azienda ed esposizione a nuove e serie minacce (fare riferimento al Monitoraggio delle minacce informatiche).

3. **Applicazione di patch o di altri meccanismi di protezione agli asset**: ogni asset deve essere controllato per verificare la presenza di nuove patch o raccomandazioni. Tali patch devono essere controllate per verificare se implicano rischi o costi che la PMI non può sostenere ed essere testate prima dell'installazione su tutti gli asset del medesimo tipo. Sarà necessario installare tutte le patch idonee. Per i fornitori affidabili e qualora siano disponibili i backup degli asset interessati, l'applicazione delle patch può avvenire automaticamente. Gli asset sui quali non è possibile installare le patch, dovranno essere protetti con mezzi alternativi, disattivati o tutelati tramite i controlli degli accessi, quali i *firewall*, oppure rigorosamente monitorati.

4. **Comunicare le vulnerabilità rimanenti**: la PMI deve tenere traccia dell'applicazione delle patch nell'inventario degli asset digitali, informare il personale circa gli asset privi di patch e offrire raccomandazioni per un'interazione sicura o prudente degli utenti con tali asset.

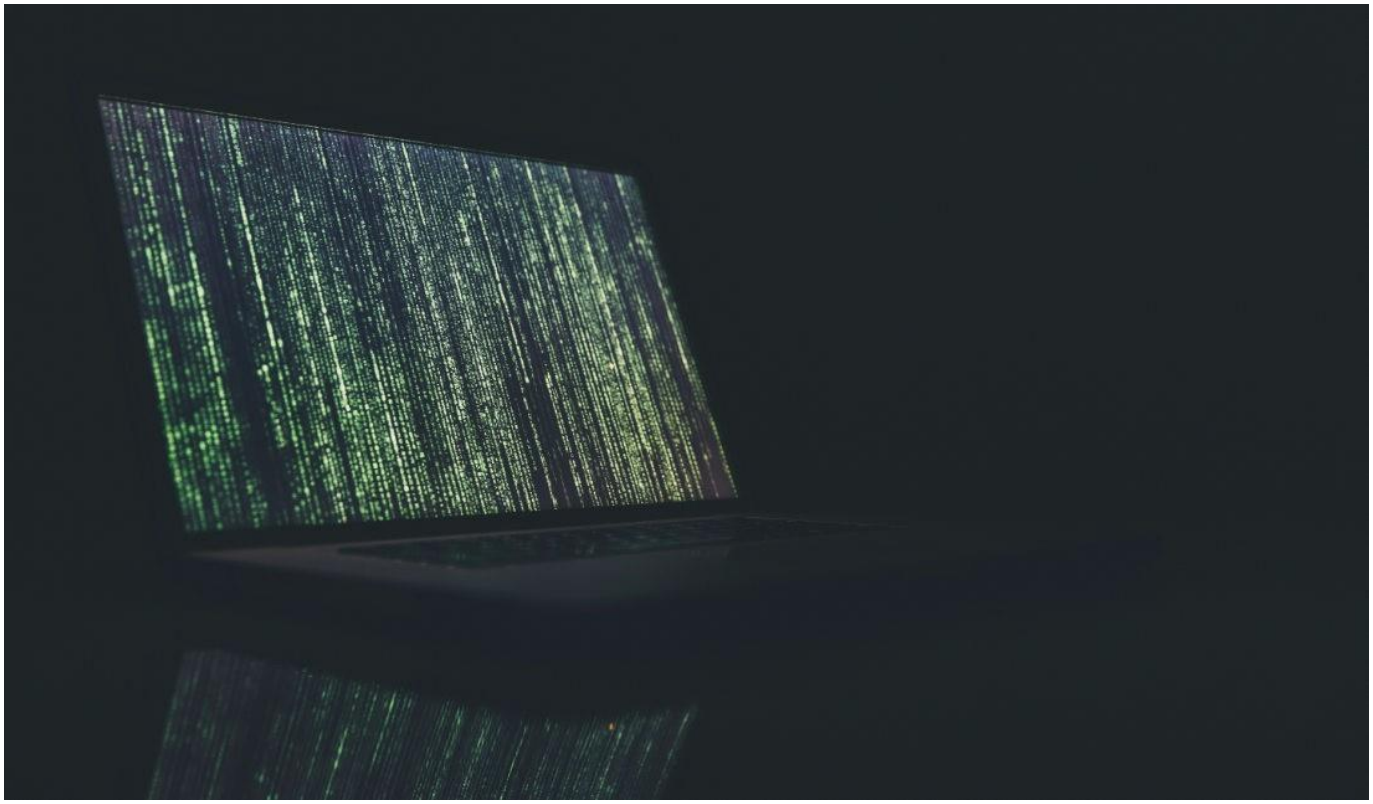
5. **Implementare periodicamente patch e raccomandazioni**: le patch e le raccomandazioni devono essere implementate dalla PMI il più rapidamente possibile qualora il vantaggio offerto dalla protezione superi i rischi impliciti derivanti dall'eliminazione della vulnerabilità.

Sebbene tali patch e raccomandazioni debbano essere implementate dalla PMI il più rapidamente possibile qualora il vantaggio offerto dalla protezione superi i rischi impliciti derivanti dall'eliminazione della vulnerabilità, le PMI raramente le applicano.

Si raccomanda alle PMI di condividere le proprie esperienze in relazione all'installazione delle patch con altre PMI. Adottando tale pratica, le PMI possono trarre un mutuo vantaggio, migliorando l'efficienza e l'efficacia della propria gestione delle vulnerabilità e condividendo informazioni su asset o patch problematiche.

Estensione alla privacy

Nel valutare le vulnerabilità, la PMI devono dare priorità agli asset utilizzati per la gestione delle informazioni che riguardano clienti e utenti.



CONTROLLO N° 7: PROTEZIONE CONTRO I MALWARE

Controllo

Le PMI devono implementare e mantenere una politica contro i malware e utilizzare degli strumenti adeguati a tale scopo.

Obiettivo

Proteggersi dai danni che i malware possono causare ai sistemi ICT, nonché ai processi e agli obiettivi aziendali.

Ambito

I malware sono molto più complessi di quanto generalmente pensino le PMI e le singole persone. Si diffondono nel sistema informativo attraverso:

- file o contatti "infetti";
- e-mail di phishing;
- azioni di hacker;

- navigazione di siti web “infetti” (o malevoli).

Qualunque sia il tipo di “infezione”, le conseguenze possono essere molto diverse (da benigne a estremamente gravi).

Situazione attuale

Proprio come le singole persone, le PMI prestano scarsa attenzione alla vasta gamma di modalità di “infezione” da malware e considerano sufficiente risolvere il problema con l'acquisto e l'aggiornamento[12] regolare di un software "antivirus", mantenendo spesso la stessa soluzione per decenni.

Guida

In modo tale da implementare una protezione efficiente le PMI devono:

- rivedere regolarmente la propria politica anti-malware, per mantenerla aggiornata rispetto alle minacce esistenti e al contesto aziendale/tecnologico; questo significa verificare, avvalendosi di esperti e siti affidabili, le soluzioni migliori, dato che la loro efficacia nel corso del tempo è destinata a cambiare;
- assicurarsi che tutti i computer siano costantemente protetti;
- installare su computer, server e nodi di comunicazione diverse tecnologie di protezione anti-malware, per poter usufruire di capacità di rilevamento incrociato;
- verificare che il proprio programma di sensibilizzazione aziendale in materia di sicurezza si soffermi regolarmente sulle esercitazioni anti-phishing, in modo che dipendenti e utenti non cadano nelle trappole predisposte dagli hacker;
- analizzare con cadenza regolare la situazione relativa alle minacce informatiche, avvalendosi di segnalazioni pubbliche/private o consultando un organismo specializzato, e aggiornando la propria preparazione in merito.

Estensione alla privacy

[Nessun problema specifico relativo alla protezione della privacy]

CONTROLLO N° 8: GESTIONE DEI BACKUP

Controllo

È necessario eseguire e verificare periodicamente copie di backup di informazioni, software e configurazioni di sistema, in conformità alla politica di backup definita.

Obiettivo

Le informazioni sono gli asset più preziosi di un'azienda, pertanto è necessario disporre di copie che ne garantiscano la disponibilità, l'integrità e la riservatezza.

Ambito

Il presente controllo si applica a tutte le informazioni, ai software e alle configurazioni di sistema dell’azienda.

Situazione attuale

Diversi rischi minacciano le informazioni in possesso delle aziende (ransomware e altri attacchi da parte di criminali informatici, guasti hardware o software, errori umani, incendi o inondazioni, ecc.). Tuttavia, in molti casi, si continua a riscontrare la mancanza di copie di backup oppure l’uso di copie di scarsa qualità, da cui è impossibile recuperare il contenuto.

Inoltre, per aver maggiori probabilità di intascare il riscatto per il recupero delle informazioni, i criminali informatici cercano di eliminare le copie di backup prima di procedere alla crittografia delle informazioni, utilizzando un ransomware. Pertanto, sta diventando davvero essenziale disporre di copie conservate all’esterno delle aziende.

12. Il Gruppo europeo di esperti in materia di sicurezza informatica fornisce informazioni aggiornate sulle soluzioni anti-virus. Inoltre, la maggior parte degli anti-virus e delle soluzioni di sicurezza forniscono un elenco dei più recenti malware/spyware/trojan.

Guida

È necessario sviluppare una politica in materia backup, al fine di stabilire i requisiti dell'azienda in merito ai backup di informazioni, software e configurazioni. Inoltre, si dovrà definire una politica di conservazione, nonché i requisiti di protezione dei backup per ciascun tipo di informazione.

Per la procedura di backup, si consiglia di utilizzare la strategia di backup 3-2-1:

- (3) Conservare almeno 3 copie dei dati.
- (2) Conservare 2 copie in due luoghi diversi.
- (1) Conservare almeno 1 copia in un luogo al di fuori della sede dell'azienda.

Una copia sono i dati di produzione, le altre due copie sono i backup. Ciascuna di queste copie deve contenere la stessa versione dei dati, a partire dalla medesima data. Almeno una delle copie deve trovarsi in un luogo diverso, a una distanza sufficiente per essere al sicuro qualora si verifichi una situazione di emergenza nella sede aziendale.

I dati di backup devono essere soggetti a un livello adeguato di protezione fisica e ambientale, coerente con le norme applicate presso la sede dell'azienda (fare riferimento al successivo Controllo N° 9: Gestione delle misure di salvaguardia). Tutti i backup devono essere crittografati. L'accesso al software di backup e al luogo di archiviazione deve essere protetto con credenziali di amministrazione specifiche.

I file di log dei backup devono essere esaminati quotidianamente, per verificare che le copie siano state completate correttamente e che non vi siano stati errori.

Non tutte le informazioni di un'azienda sono ugualmente importanti ai fini delle attività aziendali[13]. Per questo motivo, i piani di backup devono essere progettati in modo tale da ottimizzare il processo in base ai requisiti di sicurezza delle informazioni.

A seconda del tipo di informazione, l'esistenza di politiche diverse in materia di conservazione è uno dei punti più complessi da affrontare durante la progettazione dei piani di backup. Poiché le politiche di conservazione si applicano anche alle informazioni archiviate nei backup, in genere è necessario configurare piani di backup diversi a seconda dei diversi periodi di conservazione.

Infine, si devono eseguire periodicamente dei test di ripristino sui backup effettuati, per garantire che le informazioni possano effettivamente essere recuperate in caso di necessità.

Estensione alla privacy

Nella maggior parte dei casi, le copie di backup contengono dati personali, quindi è particolarmente importante che le copie vengano archiviate dopo essere state crittografate e che vengano rispettati i periodi di conservazione[14] stabiliti ai fini della conformità al GDPR.

CONTROLLO N° 9: GESTIONE DELLE MISURE DI SALVAGUARDIA

Controllo

Le PMI devono proteggere le proprie informazioni importanti e gli asset digitali contro la loro eventuale perdita, distruzione e falsificazione.

13. Anche le considerazioni sui costi giocano un ruolo in questo caso. Ad esempio, l'impresa dovrà copiare ogni giorno il database ERP, che cambia quotidianamente, ma non sarà necessario copiare le foto dell'ultimo congresso, che variano una volta all'anno. Qualora l'impresa si avvalga di servizi di cloud storage, la differenza di costo potrebbe essere significativa.
14. I periodi di conservazione dipendono dai settori, dalla legislazione vigente, dal tipo di informazioni, dai contratti dei clienti e da altri fattori. Non vi soni regole definite per tutte la casistiche.

La protezione include la pianificazione, la creazione e la ripetizione dei test. I backup[15] costituiscono un tipo particolare di salvaguardia.

Obiettivo

Proteggere le informazioni importanti e gli asset digitali della PMI contro l'eventuale perdita, distruzione e falsificazione.

Ambito

Sulla base del proprio inventario di asset digitali, la PMI pianifica, crea e testa ripetutamente le misure di salvaguardia. Le misure di salvaguardia per la protezione dell'hardware includono l'uso di locali o armadi chiusi a chiave e di sistemi antifurto. Le misure di salvaguardia per la protezione di software e informazioni includono l'autorizzazione (ad esempio con password complesse e autenticazione a due fattori), la crittografia dei dati archiviati e trasmessi (ad esempio con un sistema VPN), e la protezione degli asset digitali con anti-malware, *firewall* e log di sistema. Il personale che gestisce le misure di salvaguardia e il personale con accesso a informazioni segrete o personali deve essere controllato per verificarne l'affidabilità. I backup devono essere creati a intervalli regolari e se ne dovrà testare la possibilità di ripristino.

Situazione attuale

Molti tipi di attacchi informatici mirano all'accesso non autorizzato, alle intercettazioni, alla falsificazione e al furto delle informazioni. Inoltre, gli asset digitali possono guastarsi o diventare inutilizzabili a causa di una serie di motivi. Le misure di salvaguardia vengono istituite per proteggere i dati da tali tipi di minacce.

Guida

La gestione delle misure di salvaguardia è un processo in più fasi, costituito da una fase preparatoria, da quattro fasi orientate alla protezione, che dovranno essere ripetute su base regolare (almeno una volta al mese), e da una fase di formazione in materia di cultura della sicurezza, da ripetere per ciascun nuovo assunto e, comunque, almeno una volta all'anno.

1. **Identificazione degli asset digitali**: la PMI deve creare un inventario degli asset digitali (capitolo 7.1) e determinare la criticità di ciascun asset per l'azienda. La PMI deve assegnare una priorità a ciascun asset presente nell'inventario, in base alla rispettiva criticità per l'azienda ed esposizione a nuove e serie minacce (fare riferimento al Monitoraggio delle minacce informatiche).

2. **Protezione dell'accesso agli asset digitali**: la PMI deve determinare in che modo verrà protetto ciascun asset digitale, comprese le misure di salvaguardia fisiche per l'hardware e le misure di salvaguardia digitali per il software (ad esempio con il controllo degli accessi mediante password complesse o autenticazione a due fattori, protezione degli *endpoint* con anti-malware), la rete (ad esempio crittografia e *firewall*) e i dati (ad esempio archiviazione e trasmissione crittografate, utilizzando una VPN).

3. **Protezione contro la perdita di informazioni e software**: la PMI deve creare backup aggiornati dei sistemi e delle informazioni critiche per l'azienda. Le diverse versioni dei backup dovranno essere contrassegnate e si dovrà testare l'effettiva capacità di ripristino dei sistemi e delle informazioni.

4. **Pianificazione delle misure di salvaguardia specifiche per le minacce:** per ogni minaccia nuova o critica, la PMI deve consultare le raccomandazioni per prevenire e difendersi dagli attacchi. I CERT, che forniscono informazioni sulle minacce, offrono generalmente anche tali raccomandazioni.

5. **Verifica dell'affidabilità del personale**: la PMI deve verificare l'affidabilità del personale tecnico e del personale autorizzato ad accedere alle informazioni critiche.

6. **Implementazione di una solida cultura della sicurezza**: la PMI deve istruire tutto il personale circa i comportamenti sicuri o prudenti, comprese le modalità di impiego dei backup, di uso degli asset fondamentali per l'azienda, di protezione dell'accesso agli asset (ad esempio impiegando password uniche e complesse o l'autenticazione a due fattori) e di esecuzione delle operazioni di backup e ripristino. Una solida cultura della sicurezza comprende anche l'addestramento del personale per rilevare gli attacchi informatici (ad esempio gli attacchi basati sulle diverse forme di *phishing* e *social engineering*).

15. Fare riferimento al Controllo N° 8: Gestione dei backup.

Estensione alla privacy

Il GDPR richiede che le PMI garantiscano un'adeguata sicurezza dei dati personali, compresa la protezione contro il trattamento non autorizzato o illecito e contro la perdita, la distruzione o il danneggiamento accidentali. Le PMI devono designare una persona (il "titolare del trattamento"), che avrà la responsabilità di proteggere i dati personali e dimostrare la conformità al GDPR.

CONTROLLO N° 10: PRONTEZZA ICT PER LA CONTINUITÀ OPERATIVA

Controllo

I sistemi ICT devono essere progettati (con sicurezza *by design* e *by default*) e costruiti per resistere a guasti ed altri problemi.

Obiettivo

Garantire che le PMI possano fare affidamento sul fatto che eventuali guasti e problemi dei sistemi ITC non comportino gravi conseguenze negative sui processi, sugli obiettivi e sugli interessi aziendali.

Ambito

Questo controllo riguarda i sistemi ICT e le strutture fisiche che consentono loro di funzionare (ad esempio alimentazione, aria condizionata, copertura e persone qualificate).

Situazione attuale

Qualunque sia la causa, le situazioni impreviste mettono alla prova la competitività e la capacità di un'azienda. Se un'azienda gestisce le crisi in modo efficace, il suo valore di mercato e la sua reputazione possono aumentare. Quindi, per un'impresa è fondamentale essere preparata a garantire la continuità operativa, soprattutto dal punto di vista ICT.

Il Piano di continuità operativa (BCP) aiuta a rendere le aziende il più resilienti possibile perché può:

- limitare le interruzioni (meno tempi di inattività, meno denaro perso); definire soluzioni alternative (per ripristinare rapidamente le attività aziendali);

- responsabilizzare i dipendenti.

Guida

Raramente le aziende si rendono conto di poter essere colpite da un attacco informatico e che ogni incidente sarà diverso dagli altri e si svolgerà quindi in modi inaspettati.

Se un imprenditore o un dirigente di alto livello intende proteggere la propria azienda nel miglior modo possibile durante un'emergenza, deve fornire un piano aggiornato e collaudato a tutto il personale responsabile dell'esecuzione di qualsiasi parte di tale piano; tuttavia, prima di occuparsi di piani, azioni e rimedi, è importante concentrarsi sui tre pilastri principali e sui cinque principi per la continuità operativa.

I tre pilastri sono: cultura/consapevolezza aziendale, politiche e tecnologia.

Cultura/consapevolezza aziendale

L'acquisizione della consapevolezza è fondamentale per integrare la pratica della continuità operativa all'interno dell'impresa. Modificare la cultura aziendale è l'obiettivo più difficile da conseguire, perché necessita molto tempo per essere implementato.

Di seguito si riportano i passaggi che un'azienda dovrebbe compiere per accrescere la propria cultura della continuità operativa:

1. Iniziare dai vertici aziendali. Interagire con l'alta dirigenza a volte può essere difficile, ma risulta fondamentale, perché il cambiamento della continuità operativa avviene attraverso un approccio dall'alto verso il basso. Si dovrà partire introducendo i concetti di continuità operativa, dimostrandone i benefici a lungo termine, soprattutto da un punto di vista finanziario.
2. Costituire una squadra di *influencer*, che comprendano i vantaggi e aiutino a costruire la resilienza aziendale.
3. Usare sempre un approccio di tipo collaborativo, per convincere tutti i dipendenti a cercare di migliorare o cambiare la cultura aziendale.
4. Investire nella formazione, inclusi *webinar*, *white paper* e materiali informativi. Si raccomanda di ripetere le simulazioni tre volte all'anno, tenendo presente che la continuità operativa non si ottiene con una singola azione, bensì tramite un processo continuo e costante nel tempo.

Politiche

Le politiche di continuità operativa vengono create per rafforzare l'organizzazione aziendale, in base ai requisiti di mercato e di conformità. Esse forniscono le direttive necessarie per mantenere in funzione l'azienda sia durante i normali giorni lavorativi, che nel corso di un incidente. Se tali politiche vengono ben definite e scrupolosamente rispettate, l'impresa può fare previsioni realistiche circa la continuità e i processi aziendali. Le politiche vengono utilizzate anche per valutare gli errori eventualmente compiuti durante una crisi, per migliorare la resilienza dell'azienda e per affrontare i problemi.

Uno degli aspetti principali da considerare quando si elabora una politica di continuità operativa sono i rischi particolari che probabilmente l'impresa dovrà affrontare. Facendo riferimento alla prontezza di risposta ICT, la prima domanda da porsi è: ci sono stati problemi con i precedenti incidenti informatici che richiedono una particolare attenzione? Tener conto di tutti questi fattori può facilitare la creazione di politiche efficaci.

La spina dorsale delle politiche di continuità operativa è costituita dall'Analisi dell'impatto aziendale e dalla Valutazione del rischio.

L'Analisi dell'impatto aziendale stabilisce gli effetti di una potenziale situazione di emergenza (*potential disaster*) su un'impresa, individuando le vulnerabilità esistenti, e si concentra principalmente sugli impatti aziendali, sui tempi di ripristino e sui *recovery point objective* (RPO).

Un altro metodo affidabile per rilevare potenziali minacce è determinare la loro probabilità tramite la valutazione del rischio, al fine di identificare i pericoli e definire i modi per diminuirne l'impatto sulle attività aziendali e ridurre tempestivamente i tempi di ripristino delle normali condizioni operative dopo un incidente.

La valutazione del rischio deve contribuire a:

- identificare i pericoli;
- valutare i rischi;
- creare misure di controllo;
- registrare i risultati;
- monitorare i miglioramenti.

Tecnologia

Dopo aver sviluppato la propria cultura e le proprie politiche, l'azienda dovrà individuare le tecnologie più adatte per garantire una migliore resilienza.

Anche nel caso in cui le aziende disponessero di budget limitati da destinare alla sicurezza informatica, devono prestano attenzione ai propri asset, poiché vi è un'elevata probabilità che vengano presi di mira dai criminali informatici. Pertanto, per garantire la prontezza della continuità operativa, è indispensabile avviare le misure di tutela di due importanti asset:

- gli utenti,
- l'ambiente.

Piano di continuità operativa (BCP)

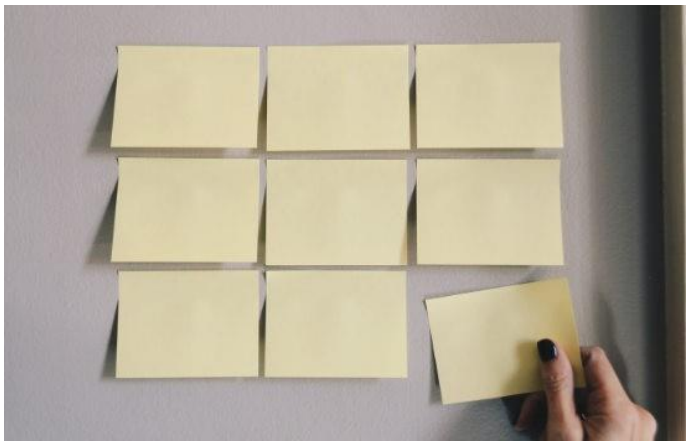
Lo scopo principale di un Piano di continuità operativa è quello di trattenere le risorse umane, proteggere gli asset e mantenere in funzione il maggior numero di attività durante un'emergenza, in modo che le normali attività possano essere riprese il prima possibile.

Sulla base della valutazione, della preparazione, della risposta e del ripristino, il Piano di continuità operativa garantirà:

- impegno delle persone
- qualità
- crescita

- soddisfazione dei clienti.

Perché un'azienda necessita di un BCP?



"A noi non succederà" è quanto di più facile da dire e pensare, qualora non si prospetti alcuna situazione di emergenza. Ma le emergenze non hanno limiti e, indipendentemente dal fatto che si stia verificando una crisi o meno, è più prudente essere preparati e dotarsi di un piano che aiuti la propria azienda a reagire. Di conseguenza, è buona norma essere preparati di fronte agli imprevisti e tener presente che, se si riesce a gestire un problema, si sarà in grado di affrontarlo, valutare cosa sta succedendo e quando si potrà tornare alla normalità.

Quando si verifica un incidente di natura informatica, clienti, dipendenti e partner hanno la necessità di sapere che verranno tutelati e supportati. Il Piano di continuità operativa dovrà riguardare tutte le aree aziendali e servirà inoltre a rafforzare la buona reputazione dell'impresa.

Come sviluppare un Piano di continuità operativa

Innanzitutto, va ricordato che un BCP deve focalizzarsi sui tre seguenti fattori chiave:

- Resilienza,
- Ripristino,
- Contingenza.

Dunque, che cosa deve includere un piano di continuità operativa? La risposta corretta è che dipende dal tipo di emergenza che si deve affrontare.

La soluzione ideale sarebbe poter disporre di piani su misura, da utilizzare per ciascun potenziale problema. Il modo in cui si gestisce un problema di rete non sarà lo stesso con il quale si reagisce a una pandemia e anche il processo di ripristino sarà diverso.

1. Identificazione dei rischi

Iniziare ponendosi le seguenti domande:

- Come arriverà il personale in ufficio?
- Se i dipendenti non possono raggiungere gli uffici, lavoreranno da remoto?
- Avranno necessità di ricevere l'hardware necessario per poter lavorare da casa?
- Dove verranno ospitati i dipendenti che riescono a raggiungere la sede dell'azienda?
- In che modo sarà possibile comunicare al personale, ai membri del consiglio di amministrazione e ai clienti la situazione di emergenza e/o i danni subiti?
- Al termine della situazione di emergenza, sarà necessario sostituire degli asset?
- Il budget a disposizione consente di sostituire gli asset ed eventualmente allestire un altro ufficio?

Queste domande consentono di farsi un'idea di base sul modo in cui verranno influenzate le attività aziendali e su come si dovrà affrontarne l'interruzione.

2. Identificazione degli asset da tutelare

Individuare cosa proteggere e dove potrebbero risiedere le principali vulnerabilità.

Prendere in considerazione le informazioni che potrebbero trovarsi all'interno dell'ufficio e come proteggerle, anche nel caso in cui non siano digitali. Riflettere sulle persone, ricordando che sono le risorse umane che consentono di proseguire le attività aziendali.

Valutare in che modo possono continuare a operare.

Consultare i processi e le politiche. È necessario proteggere le attività operative e i servizi, per il bene dell'azienda e per i clienti che li utilizzano.

3. Identificazione delle misure per gestire i rischi

Valutare quali misure sono già state implementate e quali potrebbero mancare.

4. Sviluppo del/dei proprio/i piano/i di continuità operativa

Ponderare approfonditamente come organizzare il personale, proteggere l'ufficio e garantire che l'azienda nel suo complesso possa essere comunque operativa durante il periodo di emergenza. Tali piani devono riguardare tutti gli aspetti relativi alla sicurezza e, più in generale, tutelare l'intero processo aziendale.

5. Messa in pratica costante

Non lasciare che il proprio piano di continuità resti inutilizzato. Si raccomanda di comprovarne la validità, pianificando delle simulazioni almeno due volte l'anno.

L'esperienza è preziosa. Usare lo scenario peggiore e trasformarlo nella migliore pratica.Le simulazioni offrono la possibilità di verificare l'efficacia del proprio piano di continuità operativa, soprattutto nel caso in cui presenti delle carenze e dei punti deboli, che necessitano di essere pianificati in modo migliore. Si suggerisce di richiedere un *feedback* a dipendenti, clienti e fornitori.

Perché le imprese necessitano di un'Analisi dell'impatto aziendale (BIA)?

L'Analisi dell'impatto aziendale aiuta a identificare e documentare i processi aziendali cruciali e i loro elementi di supporto. Questo consente di comprendere il proprio ambiente e ciò che è più importante, prima di adottare le misure per tutelarli. La BIA rivela come le attività e funzioni fondamentali impatteranno sulla continuità operativa, qualora venissero ostacolate o eliminate.

Cosa consente di ottenere un'analisi dell'impatto aziendale (BIA)?

- Identificazione dei processi e delle funzioni aziendali chiave.
- Sviluppo di priorità, processi aziendali e funzioni.
- Definizione di un elenco dettagliato dei requisiti necessari per il ripristino delle attività aziendali.
- Previsione dell'impatto sulle attività quotidiane.
- Definizione dei tempi necessari per il ripristino.
- Previsione dell'impatto finanziario, operativo e legale provocato dell'interruzione.

Come si conduce un'analisi dell'impatto aziendale (BIA)?

- Il primo passo per eseguire un'efficace analisi dell'impatto aziendale è garantire che vengano considerate le corrette attività e risorse aziendali. Dopo aver identificato i prodotti e i servizi idonei, si dovranno individuare i reparti che sarà necessario includere nel processo di analisi.

- Dopo aver identificato gli opportuni reparti e attività, si dovrà programmare un incontro con i dirigenti di ciascun reparto. Al fine di ottenere i migliori risultati, tutti i partecipanti dovranno:
    - essere a conoscenza delle priorità chiave dell'azienda (in relazione a prodotti e servizi);
    - comprendere le attività quotidiane assegnate al reparto;
    - comprendere le dipendenze delle risorse necessarie per completare ogni attività aziendale.
- Effettuare colloqui per l'analisi dell'impatto aziendale e per la valutazione del rischio, al fine di determinare le attività svolte dal reparto che supportano la fornitura di prodotti e servizi rientranti nell'ambito definito. È importante fissare per ciascuna attività tutti i passaggi necessari per completarla, i picchi di funzionamento, gli impatti dei tempi di inattività (ad esempio finanziari, reputazionali, operativi) e le dipendenze necessarie per eseguire ciascuna attività. Si consiglia di documentare i seguenti tipi di dipendenza:
    - Applicazioni
    - Strutture
    - Fornitori terzi
    - Attrezzature
    - Personale
- Documentare e approvare tutta la reportistica di analisi dell'impatto aziendale, congiuntamente ai risultati delle riunioni. Tale reportistica dovrà contenere tutte le informazioni e le raccomandazioni raccolte durante ciascun colloquio.
- Redigere un riepilogo dell'analisi da sottoporre al controllo e all'approvazione della direzione. Lo scopo di questa attività è fornire una panoramica delle attività chiave, dei requisiti relativi agli asset e dei rischi identificati durante le riunioni tenutesi con il personale di livello inferiore.

CONTROLLO N° 11: LAVORO A DISTANZA

Controllo

Implementazione della politica e delle misure di sicurezza di supporto per proteggere le informazioni accessibili, elaborate o conservate presso i siti di telelavoro.

Obiettivo

Il lavoro a distanza è sempre più diffuso e sta costringendo le aziende a definire misure di sicurezza specifiche per un ambiente in cui il perimetro diventa sempre più ampio. Questo controllo servirà a proteggere l'impresa contro il furto di informazioni e l'intrusione illecita nei propri sistemi ICT attraverso i canali di comunicazione e l'uso improprio di computer, che sono fuori dal proprio controllo.

Ambito

Questo controllo si applica ogni qualvolta gli utenti lavorano da una postazione al di fuori dell'ufficio in cui svolgono abitualmente la propria attività.

Situazione attuale

Il lavoro a distanza è cresciuto progressivamente negli ultimi anni. Tuttavia, a causa della pandemia di COVID-19 e del conseguente confinamento, la necessità di fornire a tutti i lavoratori le attrezzature necessarie e i diritti di accesso per poter lavorare da casa ha portato le aziende ad allentare le misure di sicurezza, per facilitare il lavoro a distanza.

I criminali informatici hanno sfruttato tale situazione per implementare tutti i tipi di meccanismi che consentono loro di ottenere informazioni sugli utenti, dirottare le informazioni, effettuare attacchi mirati, ecc.

Nel periodo post-pandemia, il telelavoro non si svolgerà più nelle condizioni precedenti, ma si prevede che diventerà comunque sempre più importante nello sviluppo delle attività aziendali.

Guida

Di seguito si riportano i passaggi più importanti per ottenere un livello di sicurezza adeguato in relazione al lavoro a distanza:

- Definire, approvare e distribuire una specifica politica di sicurezza per il lavoro a distanza, che contempli il corretto utilizzo delle risorse aziendali e riguardi tutte le possibili variabili, quali l'uso di computer domestici e la possibilità di accedervi per verificarne la sicurezza, la necessità di licenze software, i requisiti per le linee di comunicazione, la sicurezza del luogo di lavoro, la salvaguardia della riservatezza, ecc.
- Laddove possibile, le apparecchiature da utilizzare per il lavoro a distanza dovranno essere computer aziendali e l'utente non dovrà mai usarli per motivi personali. Di conseguenza, gli utenti non dovranno utilizzare i propri computer domestici per le attività professionali.
- Gli utenti dovranno connettersi solo alle reti Wi-Fi sotto il proprio controllo, dotate di sicurezza di tipo WPA2.
- L'azienda dovrà definire e configurare la protezione degli *endpoint* usati per il lavoro a distanza e assicurarsi che sia attiva e aggiornata.
- Anche il sistema operativo dovrà essere sempre aggiornato.
- Le attrezzature aziendali fornite per il lavoro a distanza (generalmente computer portatili) dovranno essere crittografate.
- I canali per le videoconferenze dovranno essere crittografati.
- La connettività dovrà essere fornita attraverso una VPN sicura, utilizzando, se possibile, il protocollo IPSec.
- Si dovrà evitare di utilizzare connessioni in modalità Desktop remoto, in quanto sono uno dei principali vettori di attacco.
- Se possibile, si dovrà adottare l'autenticazione a due fattori.
- L'utente dovrà accertarsi che il proprio lavoro venga salvato nei sistemi aziendali. Quando si lavora da remoto, uno degli errori più comunemente commessi è il salvataggio locale dei documenti di lavoro, che non potranno quindi essere inclusi nei backup programmati dall'azienda.
- Non allentare mai le misure di sicurezza per semplificare il lavoro a distanza.

- Al termine del telelavoro, accertarsi di revocare i diritti di accesso e che le apparecchiature aziendali vengano restituite.
- Addestrare il personale a prevenire l'accesso non autorizzato alle apparecchiature e ai dati, conservandoli in un armadio chiuso a chiave.
- Formare il personale per assicurarsi che eviti di lavorare su "Informazioni protette" (fare riferimento al capitolo 7.3: Gestione degli asset) in presenza di altre persone.

Estensione alla privacy

Quando si lavora a distanza, le informazioni personali vengono trasferite attraverso reti esterne fino a raggiungere la rete aziendale. Di conseguenza, è molto importante utilizzare le connessioni VPN. Inoltre, in ambiente domestico, è necessario prestare particolare attenzione alla riservatezza delle informazioni.

CONTROLLO N° 12: MONITORAGGIO DELLE MINACCE INFORMATICHE

Controllo

Le sempre nuove minacce informatiche costringono le PMI ad adattare le proprie procedure di sicurezza, al fine di essere costantemente tutelate. È quindi fondamentale monitorare gli eventuali cambiamenti in tale ambito.

Obiettivo

Proteggere le PMI dalle minacce nuove ed emergenti, modificando i propri controlli di sicurezza in base a una conoscenza aggiornata dei possibili attacchi informatici.

Ambito

I controlli di sicurezza dovranno essere implementati in base ai rischi derivanti dalle minacce. Di conseguenza, i rischi dovranno essere valutati ogni qualvolta vengano identificate nuove minacce. L'ambito di applicazione di questo controllo è l'identificazione delle minacce per la valutazione del rischio e la pianificazione della mitigazione dello stesso. La gestione del rischio sarà soggetta ad altri controlli.

Situazione attuale

Esiste una vasta gamma di minacce che rappresenta un rischio per la sicurezza delle informazioni e che può ostacolare la continuità operativa. Benché ampie categorie di minacce siano rimaste invariate nel corso dell'ultimo decennio, sono altresì stati continuamente ideati e sperimentati anche nuovi tipi di attacchi. Tali minacce differiscono sia in base alle aree geografiche, sia in base al settore industriale.

Guida

Il monitoraggio delle minacce informatiche è un processo costituito da quattro fasi, di cui una preliminare e tre da ripetere con cadenza regolare:

1. **Identificazione delle fonti**: la PMI dovrà identificare tutte le fonti di informazioni disponibili sulle minacce, per poterle consultare e mantenersi aggiornata in merito. Tali fonti possono includere pubblicazioni e segnalazioni da parte di gruppi di interesse particolari, agenzie di sicurezza informatica, quali i CERT nazionali, nonché aziende e media affidabili, specializzati nel monitoraggio delle minacce.

2. **Identificazione delle nuove minacce**: quando si consulta una fonte, sarà necessario documentare le nuove minacce, che potranno essere contrassegnate come "Non applicabili" oppure come "Importanti", qualora esista un motivo specifico per farlo.

3. **Determinazione dell'impatto sulla valutazione del rischio**: le minacce identificate dovranno essere integrate nella valutazione del rischio, per determinare se comportano nuovi rischi inaccettabili.

4. **Pianificazione della mitigazione del rischio**: qualora, in base alla fase 3, si rilevi l'insorgere di nuovi rischi inaccettabili, sarà necessario pianificare le adeguate contromisure per mitigare tali rischi.

È importante tener presente che il monitoraggio delle minacce informatiche è da considerarsi un'attività da eseguire con cadenza regolare. È importante che le PMI siano consapevoli e sempre aggiornate circa le nuove minacce significative, consultando le fonti almeno ogni tre mesi.

L'identificazione delle fonti tramite le quali ottenere le informazioni sulle nuove minacce potrà invece avvenire con cadenza annuale.

Inoltre, attacchi specifici, quali il malware Flubot scam, possono colpire una PMI entro poche ore dalla loro prima comparsa e richiedono un'azione immediata (ad esempio un avviso da inoltrare tramite i canali di comunicazione interni dell'azienda). Le segnalazioni delle nuove minacce possono fornire avvertimenti tempestivi al riguardo. Adottare le attendibili raccomandazioni suggerite consentirà di rispondere rapidamente alla minaccia informatica.

1. **Identificazione delle fonti di informazione**: le fonti più comuni includono gruppi di interesse particolari, agenzie di sicurezza informatica, quali i CERT nazionali, nonché aziende e media affidabili, specializzati nel monitoraggio delle minacce. Esempi:

   - L'agenzia europea ENISA raccoglie e pubblica informazioni sulle minacce per l'intera Europa circa una volta all'anno. Queste pubblicazioni offrono una panoramica generale, benché non dettagliata, della situazione delle minacce informatiche.
     - Panoramica delle pubblicazioni
     - Principali minacce informatiche del 2020
   - In tutti gli Stati membri dell'Unione Europea e in altri paesi europei sono stati istituiti centri ufficiali per la cybersicurezza[16]. Tali centri offrono alle PMI segnalazioni aggiornate sulle minacce locali, raccomandazioni e abbonamenti. I seguenti riferimenti possono risultare utili per minacce specifiche riguardanti le PMI, in particolare tenendo conto dell'ubicazione geografica. Esempi di CERT che forniscono informazioni per le PMI[17]:
     - Romania, Directoratul National de Securitate Cibernetica
     - Svizzera, National Cybersecurity Centre (NCSC)
     - Paesi Bassi, Dutch Digital Trust Center

2. **Identificazione delle nuove minacce**: le nuove minacce devono essere documentate e utilizzate per ridurre al minimo il tempo necessario per la valutazione del rischio. Le minacce non applicabili alla PMI devono essere comunque incluse nella documentazione e accompagnate da una giustificazione che ne motivi l'esclusione.

3. **Determinazione dell'impatto sulla valutazione del rischio**: dopo aver identificato una nuova minaccia, si dovrà rivedere la propria valutazione del rischio, per garantire un'adeguata protezione della PMI. Potrebbe essere necessario aggiungere uno o più rischi per gli asset che potrebbero essere il probabile bersaglio di una determinata minaccia. Qualora sia già stato previsto un rischio simile, la sua probabilità e il suo impatto dovranno essere riesaminati.

4. **Pianificazione della mitigazione del rischio**: dopo aver eseguito la valutazione del rischio, i relativi risultati andranno analizzati. In caso di nuovi rischi, potrebbe essere necessario introdurre ulteriori controlli di sicurezza, al fine di contenere il rischio entro un livello accettabile. Per quanto riguarda i rischi che vengono modificati a seguito dell'insorgere di una nuova minaccia, la probabilità e l'impatto del rischio modificato potrebbero comportare l'aumento del relativo punteggio e, pertanto, la PMI potrebbe dover adattare i propri controlli di sicurezza.

16. ENISA ha pubblicato un rapporto sui CERT, accompagnato da raccomandazioni sulle funzionalità di base.
17. L'Allegato D contiene un elenco completo dei CERT degli Stati membri e del Regno Unito.

Ai controlli di sicurezza, nuovi e adattati, dovrà essere attribuita la massima priorità e se ne dovrà programmare l'implementazione.

Estensione alla privacy

Nel corso dell'analisi delle minacce durante la valutazione del rischio, la PMI dovrà considerare l'impatto sulla disponibilità, l'integrità e la riservatezza delle informazioni. Per proteggere la privacy, è necessario prestare particolare attenzione agli asset contenenti informazioni personali e alle minacce che potrebbero influire sulla riservatezza delle informazioni contenute in tali asset (fare riferimento al Controllo N° 1: Gestione degli asset).

CONTROLLO N° 13: CONSAPEVOLEZZA DELLA SICUREZZA DELLE INFORMAZIONI

Controllo

Il personale e gli utenti delle informazioni e dei sistemi ICT devono essere consapevoli degli obiettivi e delle norme in materia di sicurezza delle informazioni. Le aspettative dovranno essere chiare e pienamente recepite. Il personale che ricopre ruoli specifici deve essere addestrato a svolgere i propri compiti.

Obiettivo

Far sì che le PMI possano contare sul fatto che il proprio personale e i propri utenti rispettino gli obiettivi di sicurezza delle informazioni e che, nella maggior parte dei casi, si comportino come previsto.

Ambito

Questo controllo si applica a tutte le informazioni gestite dall'impresa, nonché ai sistemi informatici e alle applicazioni che forniscono accesso e consentono la gestione delle informazioni aziendali e delle informazioni correlate, comprese le informazioni finanziarie e private.

Situazione attuale

Per quanto riguarda la sensibilizzazione in materia di sicurezza delle informazioni, esistono quattro modalità di comunicazione:

1. **Modalità informativa**: si comunica semplicemente che sono disponibili delle informazioni in merito alla sicurezza, senza che nessuno sia tenuto a leggerle, né ad applicarle (come se fossero notizie generiche). Questa modalità non è idonea ai fini della sensibilizzazione in materia di sicurezza delle informazioni e non dovrà essere scelta.

2. **Modalità consapevole**: utilizzando questa modalità di comunicazione, il personale e gli utenti saranno tenuti a leggere le informazioni relative alla sicurezza e a prendere coscienza del problema, degli obiettivi e del proprio ruolo e responsabilità. Poiché gli obiettivi e i processi aziendali, le minacce alle informazioni e le soluzioni disponibili cambiano frequentemente, le sessioni (e i programmi) di sensibilizzazione in merito alla sicurezza dovranno essere regolarmente riproposti.

3. **Modalità di addestramento**: con questa modalità di comunicazione, le persone che hanno un ruolo specifico o che devono acquisire nuove attitudini, comportamenti o competenze ricevono tutto ciò di cui necessitano per fare ciò che ci si aspetta da loro.

4. **Modalità di formazione**: si tratta della modalità di comunicazione di grado più elevato, tramite la quale il personale coinvolto ottiene un supplemento di informazioni, in modo che recepisca pienamente l'ambiente in cui opera e comprenda perché sono stati fissati obiettivi specifici, nonché in che modo le direttive, le procedure e i meccanismi consentono di raggiungere tali obiettivi.

Nella maggior parte dei casi, all'interno delle PMI non vengono fissati degli obiettivi di sicurezza, mentre in altri casi i dipendenti vengono semplicemente informati che è stata redatta e pubblicata una politica in materia di sicurezza. La sensibilizzazione su tale problematica avviene raramente, ad esempio in caso di nuove assunzioni, ma non è previsto alcun tipo di aggiornamento con cadenza regolare. Le attività di addestramento risultano limitate allo stretto indispensabile e coloro che ricoprono ruoli chiave ai fini della sicurezza non vengono sufficientemente formati.

Guida

Le PMI dovranno specificare le conoscenze di cui i propri dipendenti (e utenti) necessitano per contribuire a raggiungere gli obiettivi aziendali correlati alla sicurezza delle informazioni, che riguardano:

- la politica in materia di sicurezza;
- la politica in materia di riservatezza (in riferimento ai Dati personali);
- i processi e le procedure di sicurezza da rispettare;
- l'uso corretto delle informazioni, dei sistemi ICT e dei meccanismi di sicurezza;
- le minacce che potrebbero dover essere affrontate durante le attività lavorative;
- le contromisure da adottare in caso di anomalie e incidenti (analogamente a quanto avviene, ad esempio, in caso di incendio).

Si dovranno stabilire i contenuti e la modalità di addestramento/formazione più idonea.

Si dovranno definire e attuare un piano e un programma per accertarsi che tutto il personale e le persone che ricoprono ruoli specifici siano adeguatamente preparati ad agire come previsto.

Al termine di ciascuna sessione, nonché dopo alcuni mesi, si dovrà eseguire un test per verificare le conoscenze e le competenze acquisite. Ciò consentirà di adattare progressivamente i contenuti del programma e il piano al contesto reale e di accertarsi che il personale applichi i regolamenti.

Estensione alla privacy

Il GDPR impone che la sensibilizzazione e l'addestramento in materia di protezione della privacy avvengano con cadenza annuale.

CONTROLLO N° 14: ASPETTI DI SICUREZZA DELLE INFORMAZIONI NEI RAPPORTI CON I FORNITORI

Controllo

I contratti sottoscritti con i fornitori devono indicare chiaramente le aspettative dell'azienda per quanto riguarda la sicurezza delle informazioni, la gestione degli incidenti e la prontezza ICT per la continuità operativa.

Obiettivo

Far sì che le PMI possano contare sul fatto che i propri fornitori sappiano come gestire le informazioni che vengono loro affidate in base al relativo livello di classificazione e siano consapevoli del proprio ruolo e dei requisiti in caso di incidente e crisi.

Ambito

Al fine di garantire la sottoscrizione di contratti affidabili con fornitori e *outsourcer*, questo controllo riguarda:

- informazioni relative alla PMI, necessarie per adempiere il contratto sottoscritto;
- aspettative e requisiti dell'approvvigionamento/fornitura dei beni e dei servizi oggetto del contratto;
- aspettative e requisiti a supporto della PMI in caso di incidente e crisi; regole da seguire in caso di conflitto durante il periodo di validità del contratto; clausole contrattuali e obblighi relativi al periodo di conservazione dei dati (aggiornamento o distruzione delle informazioni fornite/memorizzate).

Per garantire il raggiungimento dell'obiettivo, l'ambito di questo controllo comprende anche i requisiti di sicurezza delle informazioni durante la fase di richiesta delle offerte, la preparazione, la sottoscrizione e la conferma/modifica delle aspettative del contratto.

Situazione attuale

Ciascun partner commerciale è soggetto a determinati rischi. Qualora si verifichi un evento che coinvolga entrambe le parti, le conseguenze potrebbero essere estremamente diverse. Alcuni partner della catena di approvvigionamento possono essere soggetti a minacce/eventi specifici, che potrebbero pregiudicare l'intera catena.

Poiché il fornitore deve conoscere i rischi dell'acquirente (o almeno le potenziali minacce) per poterli contenere, avrà accesso a informazioni chiave, il cui uso improprio potrebbe provocare danni all'acquirente.

Anche il cliente finale (consumatore) è soggetto a rischi specifici, che devono essere identificati e gestiti dalla catena di approvvigionamento.

Rischi relativi all'acquisizione di prodotti (principalmente, ma non solo, ICT)

- Per fornire un "buon" prodotto, il fornitore deve conoscere le "esigenze" dell'acquirente; pertanto, alcune delle informazioni scambiate potrebbero essere informazioni sensibili.
- La mancata conformità del prodotto alle specifiche può influire sulla capacità dell'acquirente di eseguire le attività previste, soprattutto se si tratta di infrastrutture ICT critiche.
- Le vulnerabilità del prodotto possono pregiudicare il livello di sicurezza dell'acquirente.
- Accesso del fornitore ai sistemi ICT e alle informazioni dell'acquirente.
- Accesso dell'acquirente ai sistemi ICT del fornitore.
- L'acquirente può richiedere il monitoraggio dei processi di produzione ed esternalizzazione del fornitore.

Rischi relativi all'acquisizione di servizi

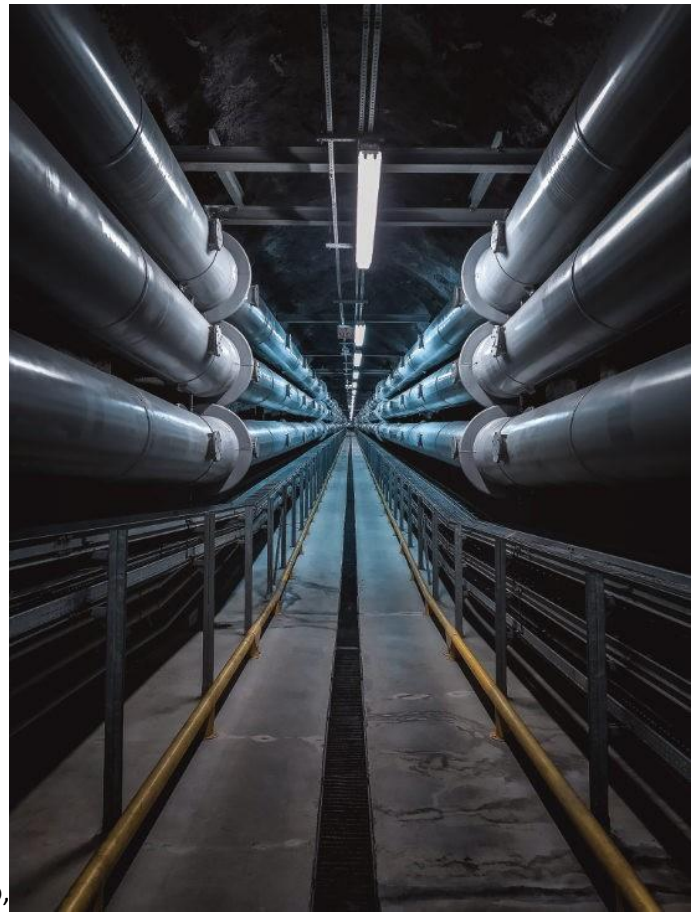
- Accesso del fornitore alle informazioni dell'acquirente (esternalizzazione, cloud, BU, manutenzione delle apparecchiature ICT, ecc.).

- Accesso del fornitore alle strutture dell'acquirente (ad esempio in caso di servizi di pulizia, poiché le attività avvengono molto spesso al di fuori dell'orario di ufficio e gli addetti alle pulizie hanno accesso a tutti gli spazi e ai locali dell'azienda).
- L'acquirente può richiedere il monitoraggio dei processi del fornitore per controllarne la qualità (e la sicurezza del servizio, ad esempio ai fini della conformità al GDPR).

Regole relative al GDPR

- Regole per l'accesso, luogo di archiviazione e conservazione delle informazioni di identificazione personale dell'acquirente.
- L'acquirente deve garantire il controllo della catena di approvvigionamento del fornitore, qualora quest'ultimo esternalizzi parte delle proprie attività, in modo tale che vengano implementate le medesime "regole di conformità".

Situazione attuale



Questo tipo di controllo viene raramente implementato dalle PMI, come del resto accade anche nel caso di imprese di maggiori dimensioni. Probabilmente ciò è dovuto al fatto che le informazioni non vengono gestite correttamente (fare riferimento al controllo N° 1) e, quindi, non viene loro attribuito un valore adeguato per dimostrarne il livello di sensibilità. Questo controllo è particolarmente importante qualora si usufruisca di servizi cloud.

Guida

Per garantire una corretta gestione dei rischi per la sicurezza delle informazioni, è necessario redigere un'apposita politica, che riporti le regole che la PMI deve rispettare quando conclude, sottoscrive, adempie e risolve i contratti con i fornitori di prodotti e gli *outsourcer* dei servizi. Tale politica stabilirà quale tipo di controllo l'impresa vuole avere sulla catena di approvvigionamento di servizi/prodotti del fornitore.

All'interno delle PMI, i contratti devono essere redatti e sottoscritti da un'unica persona appartenente ai vertici aziendali.

Lo scopo del Contratto deve essere chiaramente indicato, come ad esempio l'esigenza dell'acquirente di supportare le attività aziendali oppure attività specifiche che sono al di là delle sue competenze, ma essenziali per il raggiungimento degli obiettivi aziendali (ad esempio ICT).

Per quanto concerne la sicurezza delle informazioni, deve sempre essere tenuto presente il principio del "privilegio minimo", in modo che il fornitore abbia accesso esclusivamente alle informazioni strettamente necessarie per adempiere il contratto. La protezione riguarda l'accesso e il trasferimento di informazioni in base ai tre criteri di sicurezza: riservatezza, integrità e disponibilità. Questo può essere ottenuto attraverso:

- Implementazione di buone pratiche e processi (ad esempio ISMS, GDPR, ecc.)
- Controllo dell'accesso dei fornitori alle informazioni e alle strutture dell'acquirente
- Contratti sul livello del servizio (Service Level Agreement - SLA) e affidamento di incarico

Lista di controllo

Il contratto deve contenere clausole e allegati relativi alla sicurezza accettati da entrambe le parti (ad esempio ai fini del GDPR o per prodotti/servizi correlati ad attività aziendali critiche), che prevedano una serie di controlli e responsabilità per quanto riguarda l'implementazione e il monitoraggio. Il contratto deve contenere inoltre regole per implementare i controlli in caso di soluzioni contrastanti ed in caso di incidenti di sicurezza delle informazioni, compresi gli incidenti relativi alla privacy.

- Il contratto dovrà definire i protocolli di scambio delle informazioni, da utilizzare qualora vengano condivise "Informazioni protette".
- Le PMI devono:
  - informare il proprio personale circa le regole fissate dal contratto in materia di scambio di informazioni con i fornitori.
  - informare il proprio personale circa l'utilizzo di servizi esternalizzati.
  - informare il proprio personale circa l'uso e la manutenzione del prodotto acquistato.
  - definire e monitorare le regole di controllo degli accessi dei fornitori ai sistemi ICT dell'impresa.
  - definire e monitorare l'accesso fisico dei fornitori/*outsourcer* alle strutture, come avviene per i visitatori.
- Si dovrà creare un registro dei prodotti e dei servizi acquisiti, che riporti un elenco delle informazioni coinvolte e scambiate. Tale registro dovrà essere aggiornato e rivisto a fronte di qualsiasi modifica del contratto o del livello di classificazione delle informazioni.

Estensione alla privacy

Qualora il fornitore abbia accesso alle informazioni di identificazione personale (PII) e la necessità di gestirle, dovrà rispettare il GDPR in qualità di Responsabile del trattamento. Tutte queste regole dovranno essere applicate nel caso in cui le informazioni personali vengano gestite da (o scambiate con) un fornitore/*outsourcer*, in conformità al GDPR.

CONTROLLO N° 15: ORGANIZZAZIONE DELLA SICUREZZA DELLE INFORMAZIONI

Controllo

I ruoli essenziali relativi alla sicurezza delle informazioni devono essere definiti, descritti e assegnati a persone sufficientemente formate, che dovranno riferire ai vertici aziendali. Generalmente, si raccomanda l'uso della matrice RACI, poiché tale strumento consente di delineare chiaramente tutte le responsabilità e specificare le modalità di intervento di ciascun ruolo.

Obiettivo

Far sì che il personale delle PMI sappia chi è responsabile della sicurezza delle informazioni e sia a conoscenza dei ruoli essenziali che sono stati assegnati.

Ambito

Questo controllo riguarda tutti i ruoli e le responsabilità in relazione alla sicurezza delle informazioni.

Situazione attuale

All’interno delle PMI, i ruoli relativi alla sicurezza delle informazioni vengono raramente definiti e assegnati, per la semplice ragione che non esiste personale sufficiente e adeguatamente formato. Tali ruoli sono comunque importanti e alcuni di essi, soprattutto per quanto riguarda il GDPR, sono obbligatori.

Guida

Diversi ruoli e funzioni sono fondamentali per garantire una gestione coerente e costante della sicurezza delle informazioni, sia in ambienti IT che non IT. Alcuni ruoli possono essere assegnati alla stessa persona, purché ciò non crei un conflitto di interessi e non sia la stessa persona a compiere l’azione e contemporaneamente ad approvarla. Tutti i ruoli dovranno riferire ai vertici aziendali, che adotteranno le decisioni finali e se ne assumeranno la responsabilità.

La maggior parte di questi ruoli dovrà disporre di una "task force" durante la fase di preparazione, poiché sarà necessario avvalersi delle competenze e della partecipazione di tutti i reparti. Tali ruoli potranno essere esternalizzati, ma il contratto dovrà essere chiaro e rispettare le raccomandazioni definite dal controllo N° 14. Tuttavia, la responsabilità finale ricadrà comunque sulla PMI stessa.

La struttura organizzativa e del personale dovrà essere adattata alla particolare situazione aziendale. Per quanto riguarda la composizione dei comitati, occorrerà distinguere tra fase preparatoria e fase di realizzazione del progetto.

All'inizio, si dovrà nominare un *project manager*, che si occuperà di introdurre il processo di sicurezza delle informazioni in azienda e assumerà il ruolo di Responsabile della sicurezza delle informazioni (ISO).

Il suo compito sarà quello di stabilire, promuovere e coordinare il processo di sicurezza delle informazioni. Per svolgere tale compito, è auspicabile che l'ISO abbia conoscenze ed esperienza nei settori della sicurezza delle informazioni e della tecnologia dell'informazione. Per questo motivo, la persona scelta spesso appartiene al reparto IT. Il ruolo dell'ISO può essere svolto in collaborazione con il Responsabile della protezione dei dati o con un altro dipendente dell'azienda. Tutti i dipendenti devono essere a conoscenza dell'ISO e delle sue responsabilità. L'ISO riferisce direttamente alla direzione aziendale ed è inserito nell'organigramma come "figura del personale".

Si consiglia di considerare i seguenti punti quando si nomina l'ISO. In primo luogo, se possibile, l'ISO non deve essere il responsabile IT, perché si potrebbe compromettere sia i principi d'obiettività che di imparzialità. In secondo luogo, l'ISO deve disporre di tempo sufficiente per svolgere il proprio compito. Si dovrà infatti tenere presente che la fase introduttiva del progetto richiederà un maggior impegno in termini di tempo rispetto alle normali attività. Questo aspetto dovrà essere disciplinato separatamente nella descrizione del ruolo. In terzo luogo, la formazione di una squadra per la sicurezza delle informazioni è una parte essenziale per stabilire, implementare e mantenere il processo di sicurezza delle informazioni.

Dovranno essere incaricati di far parte della squadra per la sicurezza delle informazioni le persone o responsabili di seguito indicati, che ne costituiranno il nucleo principale e riferiranno ai vertici aziendali per quanto attiene alle decisioni e alle risorse necessarie:

Responsabile dei rischi

Questo ruolo deve prendere in considerazione tutti i rischi che la PMI potrebbe essere chiamata ad affrontare (materiali, legali, contrattuali, informativi, informatici, ecc.). La persona nominata a ricoprire tale ruolo sarà responsabile di:

- raccogliere informazioni sulle minacce e le vulnerabilità a esse correlate;
- valutare il livello di rischio in base alla probabilità che si verifichi un evento e alla gravità dell'impatto operativo e delle conseguenze per l'azienda in caso di effettivo accadimento;
- analizzare i potenziali rimedi e controlli per far fronte a tali rischi;
- mantenere i vertici aziendali informati sulla situazione e riceverne le decisioni e le risorse necessarie.

Responsabile della sicurezza delle informazioni

Questo ruolo riguarda tutti i tipi e i mezzi di supporto delle informazioni e la loro gestione. La persona nominata a ricoprire tale ruolo sarà responsabile di:

- collaborare con il Responsabile dei rischi in relazione ai rischi per le informazioni; se sufficientemente addestrata, potrà gestire i rischi per la sicurezza delle informazioni per conto del Responsabile dei rischi;
- preparare, coordinare e monitorare il piano di azioni per la sicurezza delle informazioni stabilito dalla direzione;
- preparare, coordinare e monitorare il programma di sensibilizzazione e addestramento.

Responsabile degli incidenti

Questo ruolo riguarda tutti i tipi di incidenti e, in particolare, quelli relativi alle informazioni nell'applicazione del controllo N° 4. La persona nominata a ricoprire tale ruolo opererà in collaborazione con il Responsabile della sicurezza delle informazioni e sarà responsabile di:

- definire l'elenco degli eventi che la PMI intende controllare;
- preparare e proporre:
  - criteri per classificare un evento di sicurezza delle informazioni quale incidente;
  - insieme di azioni e risorse per controllare l'incidente;
  - procedure e meccanismi per segnalare l'evento al punto di contatto;

- proporre:
    - la struttura e le competenze richieste per la squadra di risposta agli incidenti (IRT - *Incident Response Team*). Va tenuto presente che potranno esistere diverse IRT, a seconda del tipo di incidente, della fonte e delle conseguenze;
    - la creazione del ruolo di gestore dell'incidente, che coordini le attività delle IRT;
    - un processo per apprendere dagli incidenti, volto a ridurre il ripetersi degli eventi e/o a migliorare la risposta.
- criteri per dichiarare chiuso l'incidente;
- riportare tutti gli eventi e gli incidenti in un registro/database.

Responsabile delle vulnerabilità

Questo ruolo riguarda le vulnerabilità ITC e, in particolare, quelle applicabili ai componenti ITC critici. La persona nominata a ricoprire tale ruolo opererà in stretta collaborazione con il Responsabile dei rischi, il Responsabile della sicurezza delle informazioni e il Responsabile degli incidenti e sarà responsabile di:

- identificare le vulnerabilità e comunicarle al Responsabile dei rischi;
- preparare e proporre soluzioni per eliminare le vulnerabilità;
- aiutare il Responsabile degli incidenti a predisporre la risposta all'incidente, causato o veicolato dalle vulnerabilità.

Responsabile delle problematiche

Questo ruolo riguarda tutti gli eventi, le situazioni e le condizioni che non influiscono immediatamente sugli obiettivi di sicurezza delle informazioni, ma possono pregiudicarli, qualora si verifichino congiuntamente. Si occupa delle vulnerabilità non ITC che le PMI potrebbero dover fronteggiare. I suoi compiti sono molto simili a quelli del Responsabile delle vulnerabilità. La persona nominata a ricoprire tale ruolo sarà responsabile di:

- identificare tali eventi e condizioni;
- elaborare soluzioni alternative per consentire la continuità operativa mentre si pone rimedio alla situazione.

Responsabile delle crisi

Questo ruolo riguarda situazioni che compromettono gravemente la capacità aziendale, qualora un ruolo chiave sia inaspettatamente assente e non possa quindi prendere una decisione o agire come previsto oppure nel caso in cui un processo fondamentale (o un componente tecnologico essenziale che ne consente il funzionamento) risulti difettoso. È indispensabile una stretta collaborazione tra questa figura e il Responsabile degli incidenti e il Responsabile dei rischi, poiché le potenziali conseguenze potrebbero comportare la cessazione dell'attività aziendale. La persona nominata a ricoprire tale ruolo sarà responsabile di:

- individuare situazioni e condizioni che possono influire negativamente sugli obiettivi aziendali;
- valutare la durata dell'interruzione del servizio/operatività (o della perdita di dati), considerata quale limite massimo per poter comunque conseguire gli obiettivi aziendali;
- analizzare e proporre soluzioni alternative, procedure e risorse necessarie per creare la resilienza aziendale e tecnologica.

Responsabile della conformità

Questo ruolo riguarda tutti gli aspetti commerciali e operativi disciplinati da leggi o requisiti contrattuali. Questo ruolo deve essere assegnato a un membro del comitato direttivo. La persona nominata a ricoprire tale ruolo sarà responsabile di:

- identificare leggi e requisiti contrattuali;
- identificare le non conformità e proporre rimedi;

- comunicare a cadenza regolare con gli altri ruoli per promuovere la conformità.

Estensione alla privacy

***Responsabile della protezione dei dati (DPO)*:**

Il DPO è il responsabile della conformità per quanto riguarda l'applicazione del GDPR. Questo ruolo è obbligatorio, qualora le PMI eseguano il trattamento delle informazioni di identificazione personale. Il DPO deve essere una figura indipendente rispetto a qualsiasi ruolo decisionale o a qualunque comitato interno della PMI.

CONTROLLO N° 16 ULTERIORI CONTROLLI RELATIVI ALLA PRIVACY

Controllo

Di seguito si riportano alcuni controlli specifici in materia di privacy, che possono essere rilevanti per le PMI che trattano dati personali.

Si basa sullo standard ISO/IEC 27701 "*Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines*" (Integrazione degli standard ISO/IEC 27001 e ISO/IEC 27002 per la gestione delle informazioni sulla privacy — Requisiti e linee guida) e integra i controlli generali di sicurezza precedentemente descritti, nonché le relative specifiche in materia di privacy, se presenti. L'obiettivo è fornire uno strumento che consenta alle PMI di effettuare una valutazione iniziale per identificare potenziali problematiche di conformità al GDPR. La gestione di questa tematica richiede un supporto specializzato.

Obiettivo

In linea generale, i requisiti dello standard ISO/IEC 27001:2013 che menzionano la "sicurezza delle informazioni" devono essere estesi alla protezione della privacy, in quanto potenzialmente influenzata dal trattamento dei dati personali.

Non viene considerato il caso in cui una PMI agisca in qualità di Responsabile del trattamento dei dati personali per conto del Titolare del trattamento, perché i principi sono i medesimi, ma si tratta di un contesto in cui il trattamento dei dati personali rappresenta l'attività principale della PMI e pertanto risulta troppo complesso per essere affrontato efficacemente da una guida semplificata, qual è la presente. Di conseguenza, sarebbe necessaria un'analisi più approfondita.

Ambito

Questo insieme di controlli si riferisce al trattamento dei dati personali da parte di PMI che agiscono in qualità di Titolari del trattamento e riguarda i casi in cui è necessario determinare le finalità e i mezzi del trattamento dei dati personali.

Situazione attuale

L'obiettivo dei controlli sulla privacy descritti in questo capitolo è quello di consentire di affrontare i seguenti aspetti:

- **le condizioni per la raccolta e il trattamento dei dati personali**: le PMI devono accertarsi e documentare che il trattamento dei dati personali è legittimo e ha una base giuridica, in conformità al GDPR o alla legislazione specifica, con finalità chiaramente definite e lecite;
- **gli obblighi nei confronti degli interessati:** le PMI devono garantire che vengano fornite agli interessati informazioni adeguate circa il trattamento dei propri dati personali e che vengano rispettati tutti gli altri obblighi applicabili agli interessati in relazione al processo di trattamento dei dati personali;
- **i principi di privacy *by design* e privacy *by default***: le PMI devono garantire che i processi e i sistemi siano stati progettati in modo tale che la raccolta e il trattamento dei dati personali (compresi l'uso, la divulgazione, la conservazione, la trasmissione e la cancellazione) siano limitati a quanto necessario per la finalità identificata;
- **la condivisione, il trasferimento e la divulgazione dei dati personali**: le PMI devono individuare e documentare i casi in cui i dati personali vengono trasferiti in altre giurisdizioni, a terzi e/o divulgati in conformità agli obblighi applicabili.

Guida

A. Le condizioni per la raccolta e il trattamento dei dati personali

Questo insieme di controlli riguarda le condizioni per la raccolta e il trattamento dei dati personali:

- identificare e documentare le specifiche finalità per le quali i dati personali vengono trattati;
- definire, documentare e rispettare il GDPR, nonché qualsiasi legislazione applicabile (ad esempio la direttiva ePrivacy oppure successivi regolamenti), per le finalità identificate;

- ottenere e registrare il consenso degli interessati, in conformità a procedure documentate, attraverso le quali sia possibile dimostrare se, quando e come è stato ottenuto tale consenso;
- valutare la necessità e implementare, se del caso, una valutazione d'impatto sulla privacy, ogniqualvolta venga pianificato un nuovo trattamento o una modifica del trattamento dei dati personali già esistente;
- garantire che siano stati firmati contratti scritti con tutti gli eventuali responsabili del trattamento dei dati personali esistenti, assicurandosi che i suddetti responsabili abbiano implementato gli idonei controlli;
- determinare i rispettivi ruoli e responsabilità per il trattamento dei dati personali, qualora esista un contitolare del trattamento;
- predisporre e conservare in modo sicuro i registri necessari a supporto dei propri obblighi per il trattamento dei dati personali.

B. Gli obblighi nei confronti degli interessati

Questa serie di controlli riguarda gli obblighi nei confronti degli interessati:

- determinare e documentare gli obblighi legali, normativi e aziendali nei confronti degli interessati, relativi al trattamento dei loro dati personali, e fornire i mezzi per adempiere tali obblighi;
- determinare e documentare le informazioni da fornire agli interessati in merito al trattamento dei loro dati personali e i tempi entro i quali fornirle;
- fornire agli interessati informazioni chiare e facilmente accessibili, che identifichino il titolare del trattamento e descrivano il trattamento dei loro dati personali;
- fornire agli interessati un meccanismo per modificare o revocare il proprio consenso e per opporsi al trattamento dei propri dati personali;
- implementare politiche, procedure e/o meccanismi per adempiere i propri obblighi nei confronti degli interessati, affinché questi ultimi possano accedere, correggere e/o cancellare i propri dati;
- comunicare ai soggetti terzi con i quali sono stati condivisi i dati personali qualsiasi modifica, revoca del consenso o obiezione relativa ai dati personali condivisi e implementare politiche, procedure e/o meccanismi idonei per farlo;
- essere in grado di fornire, su richiesta degli interessati, una copia dei dati personali trattati;
- definire e documentare politiche e procedure per la gestione e la risposta alle legittime richieste degli interessati;
- identificare e adempiere gli obblighi (legali) nei confronti degli interessati derivanti da decisioni basate sul trattamento automatizzato dei dati personali che li riguardano.

C. Privacy *by design* e privacy *by default*

Questo insieme di controlli riguarda la "privacy *by design*" e la "privacy *by default*":

- limitare la raccolta di dati personali alla quantità minima che sia pertinente, proporzionata e necessaria per le finalità identificate;
- limitare il trattamento dei dati personali a quanto sia adeguato, pertinente e necessario per le finalità identificate;
- garantire e documentare che i dati personali siano accurati, completi e aggiornati per le finalità per le quali vengono trattati, per l'intero ciclo di vita degli stessi;
- definire e documentare gli obiettivi di minimizzazione dei dati e quali meccanismi (ad esempio la pseudonimizzazione[18]) vengono utilizzati per raggiungere tali obiettivi;

18. Come da definizione del GDPR: la sostituzione di qualsiasi informazione che potrebbe essere utilizzata per identificare una persona con uno pseudonimo o, in altre parole, un valore che non consenta di identificare direttamente l'individuo .

- cancellare i dati personali o trasformali in modo tale che non consentano l'identificazione o la re-identificazione degli interessati, qualora i dati personali originali non siano più necessari per le finalità identificate;
- disporre di politiche, procedure e/o meccanismi documentati per l'eliminazione (ad esempio la cancellazione o la distruzione) dei dati personali e garantire che i file temporanei creati a seguito del loro trattamento vengano rimossi seguendo procedure documentate ed entro un periodo di tempo specificato e documentato;
- non conservare i dati personali per un periodo di tempo superiore a quello necessario ai fini del loro trattamento;
- sottoporre i dati personali trasmessi attraverso una rete di trasmissione dati a controlli idonei, volti a garantire che i dati raggiungano la destinazione prevista.

D. La condivisione, il trasferimento e la divulgazione di dati personali

Questo insieme di controlli riguarda la condivisione, il trasferimento e la divulgazione di dati personali:

- identificare e documentare la motivazione alla base dei trasferimenti di dati personali tra giurisdizioni diverse;
- specificare e documentare i Paesi e le organizzazioni internazionali a cui i dati personali possono eventualmente essere trasferiti;
- registrare i trasferimenti di dati personali da o verso soggetti terzi e garantire la collaborazione di tali soggetti per supportare le future richieste relative agli obblighi nei confronti degli interessati;
- registrare le divulgazioni di dati personali a soggetti terzi, compresi quali dati personali sono stati divulgati, a chi e quando.

8. CONCLUSIONI

L'utilizzo di tecnologie per innovare, produrre e fornire soluzioni rientra sempre più spesso nei processi aziendali delle PMI, al fine di conseguire l'obiettivo a lungo termine della trasformazione digitale, compreso il livello base di intensità digitale per la maggior parte delle PMI europee, come già reso noto nell'ambito del DECENNIO DIGITALE. Tuttavia, la sicurezza informatica rimane una delle principali problematiche per le PMI, nonché una delle principali minacce per la continuità e la sopravvivenza delle imprese.

Poiché le minacce alla sicurezza sono ricorrenti, è necessario disporre di procedure per la sicurezza delle informazioni, al fine di tutelarne i tre valori fondamentali: la riservatezza, l'integrità e la disponibilità. Pertanto, la tecnologia dell'informazione e la sicurezza informatica sono diventate un prerequisito fondamentale per lo sviluppo personale degli individui e dell'economia, nell'Unione Europea e in tutto il mondo. Alcuni prerequisiti sono necessari per stabilire la sicurezza delle informazioni in un'azienda, al fine di garantire e mantenere il livello richiesto di conformità.

Proteggere le informazioni è una parte cruciale delle politiche, delle linee guida, delle raccomandazioni e degli standard sulla sicurezza informatica, per garantire la conformità. Lo standard ISO/IEC 27002 è una delle tante risorse che si occupano della protezione dei dati. Tuttavia, si tratta di un documento complesso, che molte PMI troverebbero difficile e costoso da implementare. Questa guida intende aiutare le PMI a implementare i controlli minimi raccomandati per proteggere le proprie informazioni, mantenere la fiducia dei consumatori e rispettare le disposizioni del GDPR. Il capitolo 7 è in gran parte una sezione tecnica, che i professionisti ICT e di sicurezza informatica delle PMI - i "facilitatori digitali" – dovrebbero utilizzare per aiutare le PMI a implementare i controlli raccomandati, per ridurre il rischio di attacchi informatici.

I destinatari principali di questa guida sono le PMI (non ICT), che devono comprendere l'importanza di proteggere le informazioni e rispettare le diverse leggi, incluso il GDPR. Pertanto, questa guida mira a sensibilizzare le PMI e a indirizzarne la gestione attraverso una strategia e una politica efficaci in materia di protezione dei dati. Le PMI e i professionisti ITC possono fare riferimento al capitolo 7 per ulteriori informazioni tecniche sull'implementazione dei 16 controlli di sicurezza e utilizzare queste informazioni per supportare e consigliare le PMI sulle azioni più idonee da adottare.

Questa guida ha dimostrato in che modo le normative sono in grado di aiutare le PMI a proteggere le proprie informazioni in maniera rapida ed economica. Ha inoltre sottolineato la necessità per le PMI di conformarsi al GDPR, poiché trattano i dati personali in molte situazioni. A tale riguardo, è stata posta in rilievo la protezione della privacy quale pilastro importante del GDPR, in cui il trattamento e la libera circolazione dei dati personali vengono bilanciati dalla tutela dei diritti e delle libertà fondamentali delle persone, in particolare il diritto di proteggere i propri dati personali (ossia di tutelare la propria privacy).

La guida sostiene inoltre che un'efficace implementazione del controllo della sicurezza non è possibile senza una solida strategia e chiari obiettivi in materia di sicurezza. Mentre gli standard (e i controlli) – in questo caso lo standard ISO/IEC 27014 – si concentrano su ciò che un'impresa ha la necessità di implementare, esistono pochi suggerimenti su come farlo. Pertanto, sono necessarie conoscenze specialistiche per poter applicare la strategia definita dagli organi direttivi ai processi e alle procedure concrete e misurabili attraverso il modello COBIT.

Infine, ha illustrato i 16 controlli di sicurezza che costituiscono i controlli minimi raccomandati che le PMI devono implementare per proteggere le proprie informazioni e rispettare le disposizioni del GDPR. Questi controlli affrontano aspetti relativi alle persone, organizzativi e tecnici, per garantire loro la protezione completa, ed in particolare a:

1. Gestione e protezione degli asset digitali
2. Risposta agli attacchi informatici
3. Definizione delle politiche per la condivisione e i backup dei dati, nonché per il lavoro a distanza
4. Implementazione delle misure di salvaguardia per ridurre al minimo le vulnerabilità e le minacce informatiche e garantire la continuità operativa dopo un attacco informatico

ALLEGATO A: TECNICA PER LA CLASSIFICAZIONE DELLE INFORMAZIONI

1. Introduzione

Come già accennato nell'introduzione di questa guida, le informazioni hanno vari scopi o obiettivi e i processi aziendali servono proprio per raggiungere tali obiettivi. Talvolta, sono le informazioni di input ad essere le più importanti, talvolta lo sono quelle di output e, a volte, entrambe.

Il valore delle informazioni deve essere definito in termini di obiettivi aziendali o di conseguenze, qualora tali obiettivi non vengano raggiunti.

Sono stati identificati quattro parametri per misurare il valore delle informazioni:

- **Valore proprio**: quanto costa acquisire e mantenere le informazioni; ad esempio, le informazioni direttamente disponibili su Internet sono gratuite e non richiedono manutenzione, mentre la situazione è molto diversa per un database e suoi metadati, che devono essere sempre mantenuti aggiornati;
- **Valore d'uso**: la portata e l'importanza di ciò che possiamo fare se le informazioni rispondono esattamente alle nostre esigenze; questo parametro ha una relazione diretta con gli obiettivi aziendali; ad esempio un'automobile ci consente di viaggiare per incontrare i clienti oppure per andare in vacanza;
- **Valore della perdita**: cosa non possiamo più fare se la qualità delle informazioni si deteriora o se i criteri di sicurezza non vengono rispettati; ad esempio una gomma forata o la mancanza di carburante ci impediscono di spostarci ed è pertanto possibile che si perda un'opportunità, un contratto o un volo aereo, con le relative conseguenze finanziarie. Ad ogni modo, l'automobile resta comunque disponibile e può essere riparata;
- **Valore di appetibilità**: quanto potrebbero essere interessanti le informazioni di cui abbiamo bisogno per gli "altri", al fine di impedirci di raggiungere i nostri obiettivi o di raggiungerli prima di noi.

Questi quattro parametri non hanno lo stesso peso per quanto riguarda i criteri di sicurezza (riservatezza, integrità, disponibilità).

Il valore delle informazioni deve essere valutato per ciascun criterio di sicurezza.

2. Procedura

2.1 Da eseguire in collaborazione con i vertici aziendali

1. Elencare le poste in gioco in ordine decrescente di importanza per l'impresa (fare riferimento alla Tabella 1).
2. Definire scale di gravità delle conseguenze di tipo qualitativo nel caso in cui le poste in gioco e i valori fossero compromessi (quattro livelli dovrebbero essere sufficienti; un numero pari di livelli impedisce la scelta semplicistica di una posizione media qualora non si sappia che giudizio esprimere – fare riferimento alla Tabella 2).
3. Creare categorie di informazioni dello stesso tipo (finanziarie, operative, relative alle persone, ecc.) o inerenti allo stesso processo/attività aziendale e scegliere un'informazione rappresentativa per ciascuna categoria.
4. Elencare i DIECI processi aziendali più importanti per l'impresa (in ordine decrescente) al fine di poter raggiungere i propri obiettivi, usando da tre a cinque informazioni chiave (informazioni di input o output).
5. Identificare da tre a cinque componenti ICT chiave, che consentono di raggiungere gli obiettivi dei processi elencati.

Ripetere questa procedura almeno una volta all'anno, magari utilizzando processi e informazioni diverse, per accertarsi che tutte le categorie di informazioni chiave siano state classificate. Con questa procedura, si identificano e classificano (stima del valore) le categorie di informazioni che necessitano di essere protette.

Dopo aver classificato le informazioni chiave, a tutte le informazioni all'interno della stessa categoria verrà attribuito il medesimo valore e, quindi, lo stesso livello di protezione.

Alcune categorie chiave potrebbero essere associate a processi aziendali chiave; tali categorie devono essere adeguatamente protette. Ciò che conta è la categoria di informazioni, non il processo chiave.

Nota: Al processo aziendale viene attribuito il livello di classificazione delle informazioni di maggior valore. I componenti ICT ereditano il livello di classificazione del processo che supportano o delle informazioni che contengono. Questo è essenziale per determinare la loro criticità per l'azienda ai fini del Piano di continuità operativa (BCP) e della gestione degli incidenti.

2.2 Da eseguire in collaborazione con il "titolare" del processo aziendale

Per ciascun processo o informazione scelti:

- Determinare le poste in gioco che verranno compromesse qualora il risultato del processo/attività aziendale non sia conforme alle aspettative (per l'impresa o il cliente). Ciascuna elaborazione di informazioni probabilmente avrà come risultato una serie diversa di poste in gioco.
- Utilizzando la Tabella 2, stabilire per ogni informazione scelta la necessità di protezione/sicurezza in termini di riservatezza, integrità e disponibilità. La necessità di sicurezza verrà ereditata da tutte le informazioni all'interno della categoria rappresentata, siano esse già utilizzate o nuove (acquisite o generate).
- Proteggere le informazioni in base alle esigenze di sicurezza.

Questa procedura deve essere ripetuta almeno una volta all'anno, perché, nel contesto dell'impresa o dei suoi obiettivi, molte situazioni possono cambiare.

A. Poste in gioco

Come nel poker o nelle scommesse, le poste in gioco sono quanto mettiamo sul tavolo e non intendiamo perdere. Ci sono **nove** tipi di poste, ciascuno dei quali contiene potenzialmente differenti livelli:

Posta in gioco	Livello
Reputazione	• Perdita di fiducia all'interno dell'azienda • Perdita di immagine o credibilità all'esterno dell'azienda • Perdita di reputazione tecnologica (competenze, abilità) • Perdita di vantaggio competitivo • Perdita di leadership tecnologica • Perdita di capacità di negoziazione
Conseguenze legali o giudiziarie	• Mancata conformità legale • Incapacità di adempiere gli obblighi di legge • Effetto negativo sul rispetto generale della legge • Conflitto giudiziario • Cause e/o sanzioni giudiziarie

Posta in gioco	Livello
Violazione della privacy	• Riduzione della capacità delle persone di continuare una normale vita personale, familiare, sociale, giudiziaria ed economica • Difficoltà a trovare un lavoro
Perdita finanziaria (diretta o indiretta)	• Perdite di carattere finanziario (quale conseguenza dell'evento) • Costi legati all'emergenza e per la riparazione (risorse umane, attrezzature, studi, perizie, ecc.) • Perdita di quote di mercato • Perdita di beni o asset • Perdita di clienti/acquirenti
Problemi sociali o industriali	• Crisi sociale – Sciopero • Dimissioni forzate • Licenziamento • Chiusura dell'azienda • Disoccupazione a lungo termine
Impatto operativo	• Interruzione del servizio (a seguito dell'evento, ad esempio finché il problema non viene risolto) • Perdita di efficacia interna, interruzioni/disservizi operativi interni • Difficoltà organizzative interne (riorganizzazione, perdita di risorse umane, ecc.) • Perdita di fornitori
Problemi contrattuali (con clienti o fornitori)	• Interruzioni/disservizi operativi di soggetti terzi • Difficoltà contrattuali • Incapacità di rispettare le clausole contrattuali
Pericolo fisico per le persone (salute, infortuni, morte)	• Indebolimento della capacità di proteggere adeguatamente le persone • Rischi per l'ambiente (inquinamento), indebolimento della capacità di preservare l'ambiente e di combattere l'inquinamento
Violazione della riservatezza delle informazioni affidate (classificate o di proprietà di soggetti terzi)	

Tabella 1: Poste in gioco

Si dovranno scegliere diversi impatti per valutare il valore delle informazioni:

- almeno TRE (3) per acquisire una visione non lineare della situazione e consentire una percezione generale meno sensibile all'ovvio (spesso fuorviante) e più stabile nel corso del tempo;
- massimo CINQUE (5), affinché la valutazione sia gestibile nel tempo.

B. Necessità di sicurezza

Nella Tabella 2, ciascun criterio di sicurezza viene suddiviso in diversi livelli in funzione dell'impatto.

- Riservatezza: qualora il processo lo richieda, sarà importante suddividere le informazioni di input e output. A seconda della categoria di informazioni e delle dimensioni delle imprese, sarà essenziale separare le violazioni della riservatezza nei confronti delle persone interne (non coinvolte nel processo) e del mondo esterno.
- Integrità: si dovrà cercare di soddisfare le esigenze relative alle informazioni di input e output, che considerano anche il problema dell'integrità del processo (automatizzato).
- Disponibilità: è essenziale separare le conseguenze (e la necessità di protezione) dovute a problemi di breve durata (disservizi temporanei) da quelle legate a eventi a lungo termine (compresa la distruzione). La tabella 3 consente di delineare chiaramente le due diverse durate.

0	Nessun effetto
1	Effetto significativo ma senza conseguenze; impatto ridotto
2	Effetto accettabile e gestibile; impatto moderato
3	Effetto difficilmente accettabile e gestibile; impatto elevato
4	Effetto catastrofico impossibile da gestire; impatto eccezionale

Tabella 2: Livello di impatto sulle poste in gioco

Criterio/Danno	**Posta 1**	**Posta 2**	**Posta 3**	**Posta 4**	**Posta 5**	**Necessità di sicurezza**
Riservatezza	**0**	**0**	**0**	**0**	**0**	**0**
Compromissione interna delle informazioni di input						0
Compromissione interna delle informazioni di output						0
Compromissione esterna delle informazioni di input						0
Compromissione esterna delle informazioni di output						0
Integrità	**0**	**0**	**0**	**0**	**0**	**0**
Data di output errata						0
Data di input errata						0
Disponibilità	**0**	**0**	**0**	**0**	**0**	**0**
Indisponibilità accettabile						0
Indisponibilità inaccettabile						0
TOTALE (criterio)	**0**	**0**	**0**	**0**	**0**	**0**

Tabella 3: Classificazione delle informazioni

Nota: su ogni riga della Tabella 2, e per ciascun criterio (due righe), la "necessità di sicurezza" corrisponde al valore massimo ottenuto. È infatti la necessità maggiore che deve essere presa in considerazione.

Ci si renderà facilmente conto che le poste in gioco e i valori ottenuti possono essere diversi per ciascuna categoria di informazioni e relativo processo. Si tratta di un obiettivo da raggiungere e rimarrà indipendente dai controlli di sicurezza selezionati e implementati per gestire i rischi.

Durata dell'indisponibilità (delle informazioni o delle tecnologie)	**Livello del danno**	**FAA**	**DIA**	**MIA**
≤ 5 minuti				
≤ 30 minuti				
≤ 1 ora				
≤ ½ giorno				
≤ 1 giorno				
≤ ½ settimana				
≤ 1 settimana				
≤ ½ mese				
≤ 1 mese				

Tabella 4: Determinazione della soglia tra indisponibilità a breve e lungo termine

FAA: Frequenza Annuale Accettabile

DIA: Durata dell'Indisponibilità Annuale: Durata dell'indisponibilità x FAA.

MAU: Media dell'Indisponibilità Annuale (MIA) – somma delle diverse DIA / 9. Nella Tabella 2, tutto ciò che è al di sotto di questa soglia è considerato accettabile, mentre tutto ciò che la supera è considerato inaccettabile.

C. Protezione delle informazioni

In termini generali, il livello di protezione può essere definito come di seguito riportato:

0	Nessuno
1	Elementare
2	Buone pratiche
3	Migliori pratiche
4	Avanzato

Si dovrà innanzitutto garantire i livelli 4 e 3. Le altre esigenze verranno naturalmente considerate dai controlli adottati, almeno nei primi mesi. Qualora fosse necessario, si potranno aggiungere altri controlli.

Nota: oltre alla loro importanza aziendale per raggiungere gli obiettivi, i processi ereditano il livello di protezione dal valore (e dalla protezione) delle informazioni che elaborano o creano.

Gli asset ICT ereditano il livello di protezione dal livello di classificazione dei processi e delle informazioni che contengono.

Per ciascun criterio, il livello di protezione possiede anche un significato più preciso e pratico. Ogni livello di protezione si basa su quello precedente.

Riservatezza

1	Le informazioni sono accessibili a tutto il personale dell'impresa/organizzazione oppure in base alle esigenze di conoscenza. In assenza di esigenze di conoscenza (necessità di condivisione), tali informazioni non devono uscire dalle sedi e dai sistemi dell'impresa/organizzazione. Sarà necessario sottoscrivere idonei accordi di non divulgazione.
2	Le informazioni sono accessibili esclusivamente al personale autorizzato, in base alle esigenze di conoscenza. Si dovrà stilare un opportuno elenco di distribuzione. Questo vale, ad esempio, per le informazioni necessarie per le attività quotidiane, ma protette dalla legge, come le registrazioni dei dati delle chiamate.
3	Controllo di accesso discrezionale (DAC). Le informazioni non possono uscire dalle sedi dell'impresa/organizzazione senza l'approvazione del proprietario dell'asset e il controllo appropriato (crittografia o controllo degli accessi fisici). Archiviazione in ambienti controllati. È consigliata la crittografia. Conservazione in armadi chiusi a chiave (almeno per quanto riguarda le informazioni su supporto cartaceo), database e sistemi di archiviazione (file system). La segregazione dei singoli "elementi" non è obbligatoria (le informazioni riservate possono essere conservate nello stesso database delle informazioni non riservate, purché sia in vigore un livello appropriato di controllo degli accessi). I dati possono essere conservati nel cloud a condizione che: 1) il provider dei servizi cloud sia stato controllato con esito positivo dal punto di vista della sicurezza/gestione del rischio; 2) sussista almeno lo stesso livello di gestione dell'identificazione degli utenti, delle identità e degli accessi adottato all'interno dell'azienda/organizzazione.
4	L'accesso ai dati viene rigorosamente limitato, ossia vige il Controllo dell'accesso obbligatorio (MAC). Ogni "elemento" viene segregato rispetto agli altri in un robusto contenitore singolo. Uso di database diversi (crittografati), a seconda delle serie di dati. I dati devono essere archiviati in una cassaforte o in un caveau. È richiesta la crittografia. Le informazioni non possono essere rimosse dai locali senza l'ausilio di un solido contenitore fisico. La trasmissione dei dati fisici alle persone deve essere registrata. Le informazioni fisiche devono essere singolarmente contrassegnate ogni qualvolta sia possibile (numeri univoci, copie a persone registrate, ecc.) In linea di massima, i dati altamente riservati non devono essere archiviati o elaborati nel cloud, a meno che non vengano implementati gli idonei meccanismi di autenticazione e crittografia. Tali meccanismi (e l'architettura dell'implementazione proposta) dovranno sempre essere rivisti e approvati dai responsabili della sicurezza.

Integrità

1	Nessuna
2	Gestita: l'integrità viene verificata dall'utente alla fonte o alla fine del processo; qualora vengano rilevate discrepanze, le informazioni vengono corrette in base alle direttive ed entro i tempi definiti dal proprietario. I backup sono una delle modalità utilizzate per ripristinare le informazioni corrette.
3	Controllata: prevenzione dei problemi relativi all'integrità per l'intero processo; rilevazione a posteriori (dopo un breve intervallo di tempo, da definirsi da parte del proprietario); le problematiche devono essere segnalate al proprietario dell'asset. Questo controllo, ad esempio, viene effettuato per impostazione predefinita dai sistemi di database e dai sistemi di archiviazione sicura. Documenti in modalità di sola lettura, ad eccezione del personale autorizzato.
4	Inalterabile: Si evitano i problemi relativi all'integrità. Controlli di integrità obbligatori su documenti e database (hash/checksum); i documenti vengono archiviati in formato inalterabile. Rilevamento in tempo reale. I problemi vengono immediatamente segnalati al proprietario, che ne controlla la correzione.

Disponibilità

1	Nessuna RTO: 7 giorni; RPO: 3-7 giorni
2	È prevista la sostituzione; la sostituzione viene pianificata e avviene in base alle condizioni definite dal proprietario o dall'autorità responsabile. RTO: < =48 ore; RPO: <= 24 ore
3	Si raccomanda la manutenzione proattiva. Lo stato viene monitorato. L'indisponibilità viene pianificata e la sostituzione realizzata dopo un breve intervallo di tempo, definito dall'autorità responsabile. RTO: < 24 ore; RPO: < 8 ore
4	L'indisponibilità viene evitata e la sostituzione è immediata; i sistemi sono completamente ridondanti e i dati vengono replicati in tempo reale o quasi (tecniche di mirroring o log shipping). La manutenzione proattiva è obbligatoria su sistemi e applicazioni. Il sistema è continuamente gestito e monitorato. Vengono sottoscritti particolari contratti di assistenza per sistemi e applicazioni (Gold, Platinum o personalizzati). RTO: < 4 ore; 0<= RPO <= 15 minuti, a seconda delle tecnologie disponibili.

RTO (Recovery Time Objective): è la quantità massima di tempo ammesso per la ripresa di un'attività, il ripristino degli asset o la fornitura di prodotti o servizi dopo che si è verificata un'interruzione del sistema. Tale periodo di tempo deve essere sufficientemente breve da garantire che gli impatti negativi non diventino inaccettabili.

RPO (Recovery Point Objective): rappresenta il punto temporale, precedente all'interruzione del sistema, per il ripristino delle informazioni (o del trattamento), al fine di consentire la ripresa di un'attività dopo la suddetta interruzione. In altre parole: quante informazioni possono essere perse (dalle ultime modifiche o aggiornamenti) senza causare troppi problemi.

L'RPO viene utilizzato per garantire che l'RTO sia realizzabile, ma anche per documentare la quantità di informazioni o elaborazioni che possono essere perse in caso di interruzione.

Anche il controllo degli accessi alle informazioni dipende dalle esigenze di protezione identificate.

Controllo degli accessi

1	Accesso consentito al personale aziendale/dell'organizzazione; si applica un controllo degli accessi di tipo standard; autenticazione a un fattore.
2	Accesso controllato, basato sui ruoli (RBAC); solo il personale autorizzato ottiene l'accesso e tali accessi vengono registrati (solo per informazioni ad accesso limitato).
3	Controllo di accesso discrezionale (DAC); il personale autorizzato può accedere qualora sia necessario, la trasmissione (se giustificata) è consentita con il permesso del proprietario. Autenticazione a due fattori.
4	Controllo dell'accesso obbligatorio (MAC); accesso individuale; la richiesta di trasmissione deve essere giustificata e viene eseguita dal proprietario. Autenticazione a più fattori (2 o più).

RBAC (Role based access control): è una modalità mediante la quale agli utenti viene assegnato un profilo funzionale, le cui regole vengono impostate nei sistemi.

DAC (Discretionary access control): è una modalità con cui il proprietario dell'asset determina le regole di accesso per le persone identificate e il cui controllo è delegato al responsabile degli asset.

MAC (Mandatory access control): è una modalità con cui il proprietario dell'asset non solo definisce, ma gestisce anche le regole di accesso (nessuna delega).

Esistono tre tipi di fattori di autenticazione: qualcosa che si conosce (ad esempio una password), qualcosa che si possiede (ad esempio un token o una chiave) e qualcosa che si è (ad esempio la biometria). L'autenticazione a tre fattori (combinazione delle tre modalità) viene utilizzata solo in casi eccezionali e di solito non viene usata nelle società commerciali.

ALLEGATO B: ELENCO DEI TITOLI DEI CAPITOLI RELATIVI AI CONTROLLI, ACCOMPAGNATI DALLA RISPETTIVA NUMERAZIONE E DAI RIFERIMENTI NORMATIVI

Il riferimento principale è lo standard ISO/IEC JTC1 SC27 27002:2013 "*Code of practice for information security controls*" (Codice di pratica per la gestione della sicurezza delle informazioni).

Nella versione più recente dello standard ISO/IEC 27002:2022, la numerazione dei capitoli è diversa. Qualora si utilizzi tale versione, sarà possibile reperire la corrispondenza dei capitoli utilizzando questa pagina.

Capitolo della presente guida	**Riferimento ISO**
5. Protezione della privacy	ISO/IEC 27701
6. Governance della sicurezza delle informazioni	ISO/IEC 27014
Controllo N° 1 Gestione degli asset	ISO/IEC 27002 8.1.1 Inventario degli asset 8.1.2 Proprietà degli asset 8.2.1 Classificazione delle informazioni 8.2.2 Etichettatura delle informazioni 8.2.3 Gestione degli asset 8.3.2 Gestione degli asset rimovibili Smaltimento dei supporti 8.3.3 Trasferimento dei supporti fisici
Controllo N° 2 Politiche, standard e linee guida	ISO/IEC 27002 5.1.1 Politiche per la sicurezza delle informazioni 5.1.2 Revisione delle politiche per la sicurezza delle informazioni
Controllo N° 3 Gestione degli incidenti	ISO/IEC 27002 16.1.1 Responsabilità e procedure 16.1.2 Segnalazione di eventi di sicurezza delle informazioni 16.1.4 Valutazione e decisione sugli eventi di sicurezza delle informazioni 16.1.5 Risposta agli incidenti di sicurezza delle informazioni 16.1.6 Imparare dagli incidenti di sicurezza delle informazioni ISO/IEC 27035-1 "*Information security incident management – Part 1 Principles and process*" (Gestione degli incidenti di sicurezza delle informazioni - Parte 1 Principi e processo)
Controllo N° 4 Gestione del controllo degli accessi	ISO/IEC 27002 9.1.1 Politica di controllo degli accessi 9.2.1 Registrazione e cancellazione degli utenti 9.2.2 Diritti di accesso degli utenti 9.2.3 Gestione dei diritti di accesso privilegiati 9.2.4 Gestione delle informazioni di autenticazione segrete degli utenti 9.2.5 Revisione dei diritti di accesso
Controllo N° 5 Sicurezza di rete e scambi di dati	ISO/IEC 27002 13.1.1 Controlli di rete 13.1.3 Segregazione delle reti 13.2.1 Politiche e procedure per il trasferimento delle informazioni 13.2.2 Accordi per il trasferimento delle informazioni 13.1.4 Accordi di riservatezza o di non divulgazione ISO/IEC 27010 "*Information security management for inter-sector and inter-organizational communications*" (Gestione della sicurezza delle informazioni per le comunicazioni intersettoriali e interorganizzative)

Capitolo della presente guida	Riferimento ISO
Controllo N° 6 Gestione della vulnerabilità	ISO/IEC 27002 12.6.1 Gestione delle vulnerabilità tecniche 12.6.2 Limitazioni all'installazione del software 12.6.3 Segnalazione di punti deboli della sicurezza delle informazioni
Controllo N° 7 Protezione contro i malware	ISO/IEC 27002 12.2.1 Controlli contro i malware
Controllo N° 8 Gestione dei backup	ISO/IEC 27002 12.3.1 Backup delle informazioni
Controllo N° 9 Gestione delle misure di salvaguardia	
Controllo N° 10 Prontezza ICT per la continuità operativa	ISO/IEC 27002 17.1.1 Pianificazione della continuità della sicurezza delle informazioni 17.1.2 Implementazione della continuità della sicurezza delle informazioni 17.1.3 Verifica, revisione e valutazione della continuità delle informazioni ISO/IEC 27031 "*ICT readiness for business continuity*" (Prontezza ICT per la continuità operativa)
Controllo N° 11 Lavoro a distanza	ISO/IEC 27002 6.2.1 Politica sui dispositivi mobili 6.2.2 Lavoro a distanza
Controllo N° 12 Monitoraggio delle minacce informatiche	
Controllo N° 13 Consapevolezza della sicurezza delle informazioni	ISO/IEC 27002 7.2.2 Consapevolezza, istruzione e formazione in materia di sicurezza delle informazioni
Controllo N° 14 Aspetti di sicurezza delle informazioni nei rapporti con i fornitori	ISO/IEC 27002 15.1.1 Sicurezza delle informazioni nei rapporti con i fornitori 15.1.2 Affrontare la sicurezza delle informazioni negli accordi con i fornitori 15.1.3 Filiera ICT 15.2.1 Monitoraggio e revisione dei servizi dei fornitori 15.2.2 Gestione delle modifiche ai servizi ai fornitori ISO/IEC 27036-1 "*Information security for supplier relationships — Part 1: Overview and concepts*" (Sicurezza delle informazioni nei rapporti con i fornitori — Parte 1: Panoramica e concetti)
Controllo N° 15 Organizzazione della sicurezza delle informazioni	ISO/IEC 27002 6.1.1 Ruoli e responsabilità della sicurezza delle informazioni 6.1.2 Segregazione dei compiti
Controllo N° 16 Ulteriori controlli relativi alla privacy	ISO/IEC 27701

ALLEGATO C: PROCESSI COBIT E GESTIONE DELLA SICUREZZA

Ciascuno dei cinque domini COBIT contiene più processi, che hanno la seguente struttura:

- Processo:
  - Descrizione e scopo.
  - Obiettivi e metriche aziendali.
  - Obiettivi e metriche IT.
- Pratiche di gestione:
  - Descrizione delle pratiche di gestione.
  - Metriche.
  - Attività basate sul livello di capacità.
- Strutture organizzative (matrice RACI).
- Flussi di informazioni e voci.
- Persone, abilità e competenze.
- Politiche e procedure.
- Cultura, etica e comportamento.
- Servizi, infrastrutture e applicazioni.

Seguendo i passaggi di questa metodologia, saremo in grado di implementare controlli di sicurezza, in linea con la strategia e gli obiettivi aziendali e otterremo informazioni molto preziose sull'efficienza dei controlli di sicurezza.

La seguente tabella illustra i diversi domini e processi COBIT La seguente tabella illustra i diversi domini e processi COBIT e la loro corrispondenza all'insieme dei controlli di sicurezza più utilizzati in Europa, ossia lo standard ISO/IEC 27001: 2013.

PROCESSO COBIT		**ISO/IEC 27001**
EDM	**Evaluate, Direct and Monitor** (Valutazione, Indirizzo e Monitoraggio)	
	01 Garantire l'impostazione e il mantenimento del modello di governance	4.3 Determinazione dell'ambito di applicazione del sistema di gestione per la sicurezza delle informazioni 5 Leadership 6.2 Obiettivi per la sicurezza delle informazioni e pianificazione per conseguirli A.5 Politiche di sicurezza delle informazioni
	02 Garantire il conseguimento di vantaggi	9.3 Riesame di direzione 10 Miglioramento
	03 Garantire l'ottimizzazione del rischio	6.1 Azioni per affrontare rischi e opportunità 8.2 Valutazione del rischio relativo alla sicurezza delle informazioni 8.3 Trattamento del rischio relativo alla sicurezza delle informazioni
	04 Garantire l'ottimizzazione delle risorse	7.1 Risorse 7.2 Competenza 7.3 Consapevolezza 7.5 Informazioni documentate A.6.1 Organizzazione interna

	05 Garantire il coinvolgimento degli stakeholder	4.1 Comprendere l'organizzazione e il suo contesto 4.2 Comprendere le necessità e le aspettative delle parti interessate 7.4 Comunicazione
APO	**Align, Plan and Organise** (Allineamento, Pianificazione e Organizzazione)	
	01 Modello di gestione IT	4.4 Sistema di gestione per la sicurezza delle informazioni 5 Leadership A.5 Politiche per la sicurezza delle informazioni 8.1 Pianificazione e controllo operativi
	02 Gestione della strategia	4.4 Sistema di gestione per la sicurezza delle informazioni 6.2 Obiettivi per la sicurezza delle informazioni e pianificazione per conseguirli
	03 Gestione dell'architettura aziendale	A.9 Controllo degli accessi A.11 Sicurezza fisica e ambientale A.12 Sicurezza delle operazioni A.13 Sicurezza delle comunicazioni
	04 Gestione dell'innovazione	
	05 Gestione del portafoglio	
	06 Gestione di budget e costi	8.3 Trattamento del rischio relativo alla sicurezza delle informazioni
	07 Gestione delle risorse umane	7.1 Risorse 7.2 Competenza 7.3 Consapevolezza A.7 Sicurezza delle risorse umane
	08 Gestione dei rapporti	4.2 Comprendere le necessità e le aspettative delle parti interessate 7.4 Comunicazione A.6.1 Organizzazione interna
	09 Gestione dei contratti di assistenza	4.2 Comprendere le necessità e le aspettative delle parti interessate 7.4 Comunicazione A.15 Rapporti con i fornitori
	10 Gestione dei fornitori	A.13.2 Trasferimento di informazioni A.14 Acquisizione, sviluppo e manutenzione del sistema A.15 Rapporti con i fornitori A.18.1.1 Identificazione della legislazione applicabile e dei requisiti contrattuali A.18.1.4 Privacy e protezione delle informazioni di identificazione personale
	11 Gestione della qualità	9 Valutazione delle prestazioni 10 Miglioramento
	12 Gestione del rischio	6.1 Azioni per affrontare rischi e opportunità 8.2 Valutazione del rischio relativo alla sicurezza delle informazioni 8.3 Trattamento del rischio relativo alla sicurezza delle informazioni
	13 Gestione della sicurezza	Trattata in tutto lo standard ISO/IEC 27001

	14 Gestione dei dati	A.8 Gestione degli asset A.10 Crittografia A.12 Sicurezza delle operazioni A.18.1.4 Privacy e protezione delle informazioni di identificazione personale
BAI	**Build, Acquire and Implement** (Sviluppo, Acquisizione e Attuazione)	
	01 Gestione dei programmi	
	02 Gestione della definizione dei requisiti	4.2 Comprendere le necessità e le aspettative delle parti interessate
	03 Gestione dell'identificazione e dello sviluppo di soluzioni	A.14 Acquisizione, sviluppo e manutenzione del sistema
	04 Gestione della disponibilità e delle capacità	A.12.1.3 Gestione delle capacità
	05 Gestione delle modifiche organizzative	A.12.1.2 Gestione delle modifiche
	06 Gestione delle modifiche IT	A.12.1.2 Gestione delle modifiche
	07 Gestione dell'accettazione e della transizione delle modifiche IT	A.12.1.2 Gestione delle modifiche A.14 Acquisizione, sviluppo e manutenzione del sistema
	08 Gestione delle conoscenze	7.5 Informazioni documentate A.12.1.1 Procedure operative documentate A.16.1.6 Apprendere dagli incidenti di sicurezza delle informazioni
	09 Gestione degli asset	A.8 Gestione degli asset
	10 Gestione della configurazione	A.9 Controllo degli accessi A.12 Sicurezza delle operazioni
	11 Gestione della qualità	9 Valutazione delle prestazioni 10 Miglioramento
DSS	**Deliver, Service and Support** (Erogazione, Servizio e Assistenza)	
	01 Gestione delle operazioni	8.1 Pianificazione e controllo operativi
	02 Gestione delle richieste di servizi e degli incidenti	A.16 Gestione degli incidenti di sicurezza delle informazioni
	03 Gestione dei problemi	A.16 Gestione degli incidenti di sicurezza delle informazioni
	04 Gestione della continuità	A.17 Aspetti della sicurezza delle informazioni nella gestione della continuità operativa
	05 Gestione dei servizi di sicurezza	Trattata in tutto lo standard ISO/IEC 27001
	06 Gestione dei controlli dei processi aziendali	9 Valutazione delle prestazioni
MEA	**Monitor, Evaluate and Assess** (Monitoraggio, Analisi e Valutazione)	
	01 Gestione del monitoraggio delle prestazioni e della conformità	9.1 Monitoraggio, misurazione, analisi e valutazione 9.3 Riesame di direzione
	02 Gestione del sistema di controllo interno	9.2 Audit interno 4.2 Comprendere le necessità e le aspettative delle parti interessate A.18 Conformità

	03 Gestione della conformità ai requisiti esterni	9.2 Audit interno 4.2 Comprendere le necessità e le aspettative delle parti interessate A.18 Conformità
	04 Gestione dell'*assurance*	9.3 Riesame di direzione

ALLEGATO D: ELENCO DEI CERT (COMPUTER EMERGENCY RESPONSE TEAM)

Paese	Nome
Austria	CERT.at (CERT nazionale austriaco)
Belgio	Centre for Cyber Security Belgium (Centro per la sicurezza informatica – Belgio)
Bulgaria	Bulgarian National Center for Incident Response in Information Security (Centro nazionale bulgaro per la risposta agli incidenti di sicurezza delle informazioni)
Cipro	National CSIRT-CY (CERT nazionale cipriota)
Danimarca	Centre for Cyber Security (CFCS) (Centro per la sicurezza informatica)
Estonia	CERT-EE (CERT nazionale estone)
Finlandia	Finnish National Cyber Security Centre (Centro nazionale finlandese per la sicurezza informatica)
Francia	French National Cyber Security Agency (Agenzia nazionale francese per la sicurezza informatica - in inglese)
Germania	CERT-Bund (CERT nazionale tedesco), link 2
Grecia	Hellenic CSIRT (CERT greco)
Ungheria	National Cyber Security Centre of Hungary (Centro nazionale ungherese per la sicurezza informatica)
Irlanda	IRISS (CERT irlandese)
Italia	Italian National Cybersecurity Agency (Agenzia nazionale italiana per la sicurezza informatica)
Lettonia	Information Technology Security Incident Response Institution (Istituto lettone per la risposta agli incidenti di sicurezza delle informazioni)
Malta	Government CSIRT of Malta (CERT nazionale maltese)
Polonia	CERT POLSKA (CERT polacco)
Portogallo	Portuguese National Cyber Security Centre (Centro nazionale portoghese per la sicurezza informatica)
Romania	Romanian National Directorate for Cybersecurity (Direttorato nazionale rumeno per la sicurezza informatica)
Slovenia	SI-CERT (CERT nazionale sloveno)
Spagna	Spanish National Cybersecurity Institute (Istituto nazionale spagnolo per la sicurezza informatica)
Svizzera	Swiss National Cybersecurity Centre (Centro nazionale svizzero per la sicurezza informatica)
Paesi Bassi	Dutch Digital Trust Center (CERT olandese)
Regno Unito	UK's National Cyber Security Centre (Centro nazionale britannico per la sicurezza informatica)

BIBLIOGRAFIA

ENISA (2015). *National/governmental CERTs - ENISA's recommendations on baseline capabilities*. ENISA. Scaricato dal sito https://www.enisa.europa.eu/publications/national-governmental-certs-enisas-recommendations-on-baseline-capabilities

Commissione europea. (2020). *Decennio digitale europeo: obiettivi digitali per il 2030*. Bruxelles: Commissione europea. https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_it (Scaricato dal sito in data 21 dicembre 2021).

Eurostat. (2019). *ICT security in EU enterprises*. https://ec.europa.eu/eurostat/statistics-explained/index.php?title=ICT_security_in_enterprises#ICT_security_in_EU_enterprises (scaricato dal sito in data 21 dicembre 2021).

ISACA. (2019). *COBIT for Small and Medium Enterprises Using COBIT 2019*. ISACA.

Organizzazione internazionale per la standardizzazione (ISO). (21 dicembre 21). I*SO 9000 FAMILY*

QUALITY MANAGEMENT. Organizzazione internazionale per la standardizzazione (ISO). https://www.iso.org/iso-9001-quality-management.html

Organizzazione internazionale per la standardizzazione (ISO). (2020). *Information security, cybersecurity and privacy protection — Governance of information security*. (ISO/IEC 27014:2020). https://www.iso.org/standard/74046.html

Organizzazione internazionale per la standardizzazione (ISO). (2019). *Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines.* (ISO/IEC 27701:2019). https://www.iso.org/standard/71670.html

Organizzazione internazionale per la standardizzazione (ISO). (2018). *Information technology — Security techniques — Information security risk management*. (ISO/IEC 27005:2018). https://www.iso.org/standard/75281.html

Organizzazione internazionale per la standardizzazione (ISO). (2015). *Conformity assessment — Requirements for bodiesproviding audit and certification of management systems — Part 1: Requirements*. (ISO/IEC 17021-1:2015). https://www.iso.org/standard/61651.html

Organizzazione internazionale per la standardizzazione (ISO). (2013). *Information technology — Security techniques — Information security management systems — Requirements*. (ISO/IEC 27001:2013). https://www.iso.org/standard/54534.html

Organizzazione internazionale per la standardizzazione (ISO). (2022). *Information security, cybersecurity and privacy protection — Information security controls.* (ISO/IEC 27002:2022). https://www.iso.org/standard/75652.html

Organizzazione internazionale per la standardizzazione (ISO). (2013). *Information technology — Security techniques — Code of practice for information security controls*. (ISO/IEC 27002:2013). https://www.iso.org/standard/54533.html

Organizzazione internazionale per la standardizzazione (ISO). (2012). *Conformity assessment — Requirements for bodiescertifying products, processes and services*. (ISO/IEC 17065:2012). https://www.iso.org/standard/46568.html

Shojaifar, A., & Järvinen, H. (2021). Classifying SMEs for Approaching Cybersecurity Competence and Awareness. In *ARES 2021: The 16th International Conference on Availability, Reliability and Security* (pp. 1-7). Vienna; Association for Computing Machinery. Scaricato in data 21 dicembre dal sito https://dl.acm.org/doi/pdf/10.1145/3465481.3469200.

Regolamento (UE) 2016/679 *relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)*. Parlamento europeo, Consiglio dell'Unione europea. https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32016R0679

Small Business Standards (SBS). (2017). *SME Guide for the Implementation of ISO/IEC 27001 on InformationSecurity Management*. Bruxelles: SBS. Scaricato dal sito https://www.sbs-sme.eu/publication/sme-guide-implementation-iso-iec-27001-information-security-management

INFORMAZIONI SUGLI SPECIALISTI

Presidente: Jean-Luc Allard

Ingegnere industriale, attualmente in pensione. Ex ufficiale dell'aeronautica belga. Esperto in governance e gestione della sicurezza delle informazioni, con 25 anni di esperienza. Attivo nella normazione (ISO/IEC JTCI SC27) dal 2002.

Consulente free-lance per la formazione, governance e gestione della sicurezza.

Coordinatore: Omar Dhaher

Senior Technology Manager presso DIGITAL SME. Coordinatore del gruppo di lavoro “Standards” di DIGITAL SME e del gruppo di lavoro “Digitalisation” di SBS. Membro della task force “Rolling Plan” della “European Multi-Stakeholders Platform on ICT Standardisation” della Commissione europea. Esperto in ICT, politica industriale con riferimento ai quadri normativi delle telecomunicazioni, imprenditorialità, apprendimento basato sul lavoro, competenze digitali, ricerca e normazione.

Membri

Andrea Caccia: Consulente senior, Project Manager, conformità agli standard e ai regolamenti, coordinatore per lo sviluppo di prodotti relativi a:

- Servizi fiduciari e prodotti/tecnologie correlati (ad esempio eSignature, eSeal, eDelivery)
- Fatturazione e archiviazione elettronica
- Soluzioni blockchain e DLT

Andrea partecipa alle più importanti attività di normazione europea (ETSI, CEN, ISO, UNI/ UNINFO, OASIS)

Daniele Tumietto

Consulente indipendente, Senior Advisor e Innovation Manager. Daniele è anche professore a contratto presso la Link Campus University di Roma (Italia) e la O.M. Beketov University di Kharkiv (Ucraina).

Membro di diversi comitati tecnici di normazione nazionali, europei e internazionali per quanto riguarda la fatturazione elettronica, e-procurement, eBusiness e servizi finanziari, eIDAS, privacy e protezione dei dati personali, blockchain e DLT, Industria 4.0, Tecnologie quantistiche, Intelligenza Artificiale, Economia circolare ed ESG.

Davide Giribaldi

CEO di EnCybeRisk srl - Senior GRC & Information Security Advisor – Coordinatore del gruppo di lavoro “Cybersecurity” di Assintel, con una approfondita conoscenza nel settore della gestione del rischio per la sicurezza aziendale. Davide ha maturato 27 anni di esperienza in contesti critici, per garantire la continuità operativa e la gestione delle crisi di enti pubblici italiani e grandi multinazionali.

Francisco Menéndez

Francisco è uno specialista di sicurezza delle informazioni, gestione dei servizi e continuità operativa ed è responsabile dei servizi di sicurezza e conformità delle informazioni presso Seresco. È lead auditor di ISO 27001, ISO 28000, ISO 20000-1 e ISO 22301. Membro ISACA Platinum. Certificazioni ISACA: CISA, CISM, CRISC e Fondazione COBIT. Francisco è il coordinatore e membro del gruppo di lavoro itSMF Spagna e del gruppo di lavoro "Industrial Cybersecurity Centre".

Samuel Fricker

Professore presso la Scuola universitaria professionale della Svizzera nordoccidentale e coordinatore del progetto GEIGER[19] nell'ambito di Horizon-2020. GEIGER mira a garantire la cybersicurezza alle piccole e medie imprese, in collaborazione con la DIGITAL SME Alliance europea, ENISA, ECSO e diversi altri enti nazionali. Samuel ha conseguito un dottorato di ricerca presso l'Università di Zurigo.

19. I contributi apportati dal progetto GEIGER a questa guida hanno ricevuto finanziamenti dall'Unione Europea nell'ambito del programma di ricerca e innovazione Horizon 2020, ai sensi della convenzione di sovvenzione N° 883588.

Small Business Standards

sbs-sme.eu

@sbs-sme

European DIGITAL SME Alliance

digitalsme.eu

@EUdigitalsme

Cofinanziata dalla Commissione Europea e dagli Stati membri dell'EFTA