



Direttiva NIS2

Introduzione alla Direttiva NIS2	2
Punti principali della normativa.....	3
Autori del paper	5
Dalla NIS alla NIS2	6
Contesto e obiettivi della Direttiva NIS2	7
Chi deve conformarsi a NIS2	7
Quali misure di sicurezza informatica prevede NIS2	10
Obblighi di notifica.....	12
Impatto della NIS2 sulle attività delle PMI	14
Attuazione della Normativa NIS2	15
Creazione di awareness e formazione dei dipendenti.....	17
Assesment competenze in-house e formazione differenziata per tipologia di dipendenti e/o per comparti organizzativi.	17
Ruolo dei dipendenti nella prevenzione delle minacce informatiche e nell'attuazione delle misure di sicurezza.	19
L'anello debole della Cybersecurity è legato al "comportamento umano"	19
Formazione	20
Strategie e suggerimenti proposti dal centro Cyber 4.0 per implementare efficacemente programmi di formazione e sensibilizzazione nelle PMI.	20

Introduzione alla Direttiva NIS2


La direttiva sulla sicurezza delle reti e dei sistemi informativi, Network and Information Security Directive 2 (NIS2) dell'Unione europea delinea i requisiti di cybersicurezza per le organizzazioni operanti nell'Unione Europea (UE) al fine di garantire un livello elevato e comune di protezione tra gli Stati membri.

La direttiva affronta le limitazioni della precedente direttiva NIS inizialmente istituita nel 2016 con requisiti più rigorosi, un'estensione dell'ambito di applicazione delle entità e dei settori che devono conformarsi e maggiori sanzioni per l'inosservanza.

Si stima che circa 350.000 organizzazioni in tutta l'UE siano interessate dalla direttiva NIS2. Le organizzazioni, soprattutto quelle che si avvicinano alla NIS2 per la prima volta, dovranno investire risorse significative per comprendere le proprie responsabilità e garantire la conformità. La direttiva si applica alle grandi e medie organizzazioni operanti in settori critici come l'energia, i trasporti, la manifattura, l'acqua e la sanità, nonché la banca, la finanza, i servizi digitali e altro ancora. Inoltre, la NIS2 potrà essere applicata anche alle **piccole imprese** nel caso in cui queste ultime siano fornitrici di aziende che rientrano nella normativa oppure se coinvolte in specifici settori definiti critici dalla NIS2.

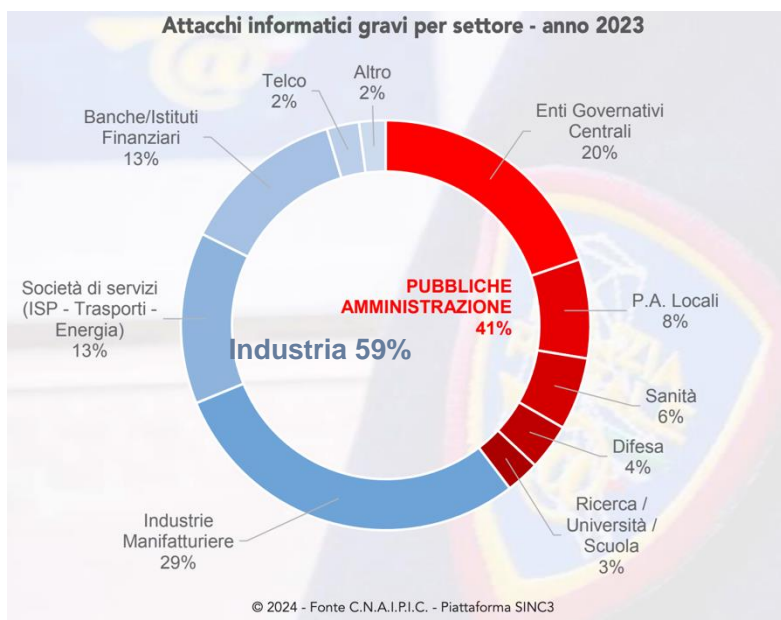
A seconda delle loro dimensioni e del settore in cui operano, le organizzazioni rientrano nelle categorie "**Essenziali**" o "**Importanti**". Entrambe devono rispettare le stesse misure di sicurezza, ma le Entità Essenziali sono monitorate proattivamente e sono soggette a sanzioni più gravi in caso di inosservanza. Poiché NIS2 è una direttiva europea, spetta a ciascuno Stato membro dell'UE recepirla nella propria legislazione nazionale e farla rispettare. I requisiti chiave sono gli stessi, ma le leggi locali definiscono procedure e linee guida di attuazione specifiche, puntando agli stessi obiettivi in tutta l'UE: garantire che le organizzazioni che fanno parte della catena di fornitura delle infrastrutture critiche comprendano la loro esposizione ai rischi informatici, applichino le best practice di cybersicurezza e siano in grado di rilevare, gestire e segnalare gli incidenti in tempi molto brevi. Con l'aumento drammatico degli attacchi informatici contro le organizzazioni europee e l'attuale situazione geopolitica globale, NIS2 rappresenta un passo cruciale per garantire la sicurezza delle infrastrutture critiche europee.

La Direttiva NIS originale, adottata nel 2016, è stata la prima normativa a livello europeo che ha stabilito requisiti minimi di sicurezza informatica per gli "operatori di servizi essenziali" (OSE) e i "fornitori di servizi digitali" (DSP) in settori strategici come l'energia, i trasporti, la sanità e le infrastrutture digitali. Questa direttiva ha rappresentato un importante passo avanti nella promozione della cybersicurezza nell'Unione Europea, introducendo obblighi di segnalazione degli incidenti, di adozione di misure di sicurezza e di designazione di autorità nazionali competenti.



La direttiva NIS2 richiede a ciascuno Stato membro di designare almeno un'autorità competente per guidare l'attuazione della direttiva nel paese e monitorare la conformità delle entità all'interno del campo di applicazione della direttiva. Devono inoltre essere istituiti CSIRT per monitorare e analizzare le minacce e gli incidenti, raccogliere evidenze forensi, avvisare le entità e altri stakeholder rilevanti e fornire assistenza quando necessario. Le autorità hanno il potere di controllare le entità nel modo elencato nella tabella seguente.

Secondo i dati del Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (C.N.A.I.P.I.C.) della Polizia Postale, nel 2023 sono stati rilevati e investigati 632 gravi attacchi cyber contro Infrastrutture Critiche, Operatori di Servizi Essenziali, Piccole Amministrazioni Locali e aziende. Di questi, 192 eventi sono stati considerati particolarmente gravi a causa del loro impatto negativo a livello nazionale, causando sospensioni nell'erogazione di servizi essenziali o di pubblico interesse. Il 59% dei gravi attacchi cyber ha colpito le Imprese Private con particolare focus sul settore manifatturiero, società di servizi e sul settore finanziario.



Punti principali della normativa

Di seguito si riporta un quadro di alto livello dei punti chiave della normativa:

- **Emanazione:** la Direttiva 2022/2555/UE è stata rilasciata il 14 dicembre 2022
 - è una evoluzione ed estensione della Direttiva NIS;
 - è entrata in vigore lo scorso 17 gennaio 2023;
- **Scadenza:** gli Stati membri dovranno recepirla entro il 17 ottobre 2024;
- **Ambiti di applicazione:**
 - Energia;
 - Trasporti;
 - Banche e infrastrutture finanziarie;

-
- Sanità (ospedali, laboratori, produttori di strumenti medicali, settore farmaceutico);
 - Idrico;
 - Gestione rifiuti;
 - Infrastrutture digitali;
 - Gestione servizi ICT;
 - Pubblica Amministrazione (Centrale e Locale);
 - Spazio;
 - Servizi postali;
 - Settore chimico;
 - Alimentare;
 - Manifatturiero;
 - Fornitori di servizi digitali;
 - Ricerca
- **Destinatari**
 - **diretti** – Operatori essenziali e importanti - limite dimensionale della “media impresa” ai sensi della raccomandazione 2003/361/CE corrisponde a più di 50 dipendenti o fatturato > 10Mln, derogabile in presenza di particolari condizioni;
 - **indiretti** – Fornitori degli operatori essenziali e importanti (dettaglio nei capitoli successivi);
 - **Obblighi:**
 - *Per i governi*
 - recepire la normativa calandola in una strategia nazionale di cybersecurity;
 - definire le autorità competenti per i controlli;
 - istituire un Computer Security Incident Response Team (CSIRT) nazionale;
 - coordinare la risposta agli incidenti;
 - *Per le imprese*
 - Obblighi per le imprese e le PA se identificati come soggetti “essenziali” e “importanti”;
 - Non solo operatori nei settori indicati dalla NIS, ma estensione anche a numerosi altri settori;
 - Si devono adeguare sulla base della dimensione e del settore di appartenenza;
 - Devono prepararsi a differenti meccanismi di supervisione e controllo che possono comportare differenti sanzioni
 - **Sanzioni:**
 - le organizzazioni essenziali sono soggette a sanzioni “pari a un massimo di almeno 10.000.000 euro o a un massimo di almeno il 2 % del fatturato mondiale annuo”;
 - le organizzazioni importanti sono soggette a sanzioni “pari a un massimo di almeno 7.000.000 euro o a un massimo di almeno l’1,4% del fatturato mondiale annuo”.
-

Autori del paper

Tenendo in considerazione questa importante direttiva e le sue indicazioni, il **Centro di Competenza Cyber 4.0 e TIM Enterprise** hanno voluto realizzare il presente documento che ne riassume i punti fondamentali e descrive le azioni principali che le imprese italiane coinvolte dovranno intraprendere per adeguarsi.

Cyber 4.0 è il Centro di Competenza nazionale ad alta specializzazione per la cybersecurity, uno degli 8 centri di competenza ad alta specializzazione istituiti e cofinanziati dal Ministero delle Imprese e del Made in Italy (MIMIT). Avviato nel contesto del piano Industria 4.0, il Centro è oggi riconosciuto come polo di trasferimento tecnologico nazionale ed è soggetto attuatore del PNRR per conto del MIMIT (Missione 4, Componente 2, Investimento 3). Cyber 4.0 è costituito nella forma di un'Associazione di diritto privato, che esprime un partenariato pubblico-privato largamente rappresentativo del contesto di cyber security nazionale, cui partecipano oltre 40 attori di rilevanza nazionale, tra cui TIM, rappresentanti di università ed enti di ricerca, istituzioni pubbliche, grandi aziende, fondazioni e PMI altamente specializzate.

TIM Enterprise è la business unit di TIM che offre ad Aziende e Pubblica Amministrazione soluzioni digitali a 360 gradi innovative, sostenibili e sicure.

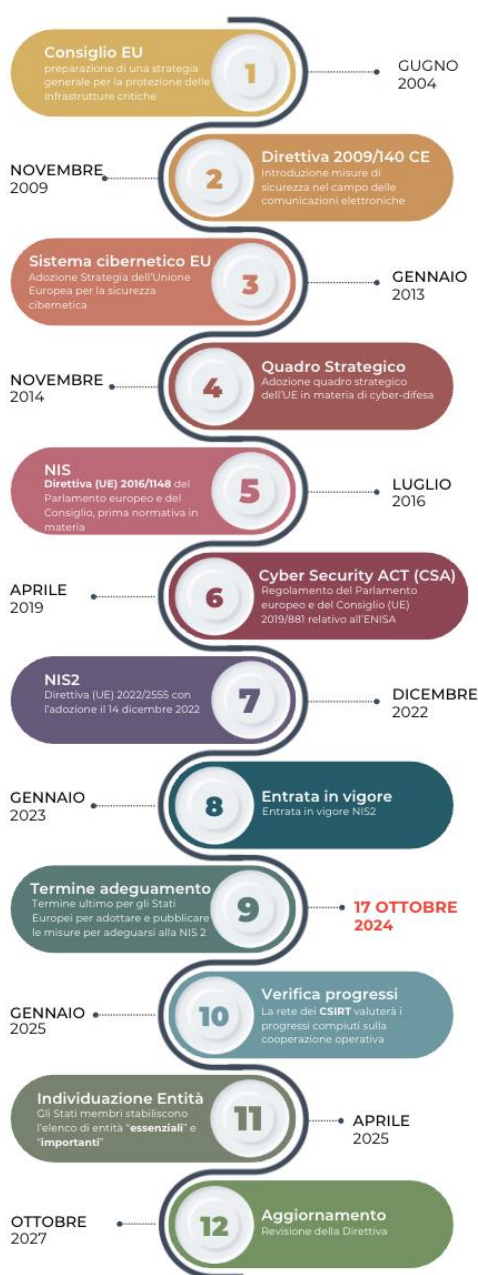
TIM Enterprise ha maturato una pluriennale esperienza nella gestione della sicurezza dei suoi importanti asset di telecomunicazione, dalle reti nazionali e internazionali ai datacenter di ultima generazione. Infrastrutture altamente critiche che TIM ha dovuto adeguatamente proteggere adottando opportune soluzioni tecnologiche, stringenti requisiti di conformità e sviluppando forti competenze al proprio interno. Esperienze e competenze che poi sono state ulteriormente rafforzate con l'acquisizione di Telsy, Centro di Competenza specializzata nella Cybersecurity, e sviluppando partnership con i principali vendor mondiali di Cybersicurezza.

Tutto questo ha portato TIM Enterprise a diventare uno dei principali attori nazionali in ambito cybersicurezza con un portafoglio di soluzioni completo che aiutano le aziende e le istituzioni a prevenire, proteggere e mitigare i rischi informatici.

Dalla NIS alla NIS2

Il consiglio europeo è partito a giugno 2004 per definire una strategia per la protezione delle infrastrutture critiche (*figura NIS2 timeline*). La Direttiva presentata dalla Commissione sulla sicurezza delle reti e

NIS2 TIMELINE



dell'informazione, più nota come **Direttiva NIS**, che in data **6 luglio 2016** è stata pubblicata come Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, ha costituito de facto la prima normativa in materia di cybersecurity. Ad Aprile 2019 è stato approvato il Cyber Security Act (2019/881) dal Parlamento Europeo e dal Consiglio (UE). Nell'ambito della relazione annuale 2021 sull'attuazione del quadro strategico in materia di cyber-difesa, in particolare la revisione coordinata annuale sulla difesa (CARD), la cooperazione strutturata permanente (PESCO), il Fondo europeo per la difesa e il patto sulla dimensione civile della PSDC, come pure la revisione del piano di sviluppo delle capacità (CDP) e del piano di sviluppo delle capacità civili, gli Stati membri hanno chiesto un aggiornamento del quadro strategico dell'UE in materia di cyber-difesa.

La Direttiva NIS2 rappresenta un importante aggiornamento della precedente Direttiva NIS. Questa nuova normativa, entrata in vigore nel 2022, ha l'obiettivo di rafforzare ulteriormente la resilienza dei sistemi informatici e la sicurezza delle reti in tutta l'Unione Europea. **Il termine ultimo per adeguarsi alla normativa è il 17 ottobre 2024.**

Il Centro Cyber 4.0 ritiene che la Direttiva NIS2 avrà un impatto significativo anche su piccole e medie imprese (PMI) operanti in diversi settori economici. Queste aziende dovranno adeguarsi a una serie di nuovi requisiti operativi e normativi, con l'obiettivo di migliorare la propria preparazione e capacità di risposta agli incidenti di sicurezza informatica.

La cybersicurezza è una priorità della strategia globale per la politica estera e di sicurezza dell'Unione europea, come pure del livello di ambizione dell'UE. La strategia globale pone l'accento sulla necessità di accrescere le capacità di proteggere l'UE e i suoi cittadini e di rispondere alle crisi esterne, nonché di rafforzare l'UE in quanto comunità di sicurezza. In questo contesto gli sforzi in materia di sicurezza e difesa dovrebbero inoltre rafforzare il ruolo strategico dell'UE e la sua capacità di agire autonomamente, se e quando necessario, e con i partner, quando possibile. Tali obiettivi richiedono una maggiore cooperazione nello sviluppo di capacità civili e militari in maniera congiunta tra gli Stati Membri.

Contesto e obiettivi della Direttiva NIS2

















A dicembre 2022, l'Unione Europea ha adottato una versione aggiornata della direttiva NIS istituita nel 2016. La direttiva NIS2 richiede alle organizzazioni operanti nell'UE di adottare un insieme di best practice e procedure di cybersicurezza per guidare la governance, la gestione dei rischi e la rendicontazione. È stata progettata per garantire la resilienza dei settori critici al fine di salvaguardare le infrastrutture europee ed evitare un effetto domino in caso di gravi attacchi informatici. NIS2 rende obbligatoria la conformità imponendo sanzioni finanziarie significative, stabilendo la responsabilità dell'alta dirigenza e rafforzando il ruolo delle agenzie locali per la cybersicurezza nel monitorare e controllare le organizzazioni. Poiché NIS2 è una direttiva UE, gli Stati membri devono recepirla nel diritto nazionale applicabile entro il **17 ottobre 2024**. NIS2 sarà applicata a partire dal 18 ottobre 2024, anche se gli Stati membri hanno tempo fino al 17 aprile 2025 per finalizzare l'elenco delle organizzazioni che devono conformarsi.


Tuttavia, l'evoluzione del panorama delle minacce cyber e l'emergere di nuove sfide hanno reso necessario un aggiornamento della normativa. La Direttiva NIS2 è stata quindi adottata nel 2022 con l'obiettivo di rafforzare ulteriormente la resilienza e la sicurezza delle reti e dei sistemi informatici in Europa.

Chi deve conformarsi a NIS2

Nella versione 1 della direttiva NIS, spettava agli Stati membri designare le organizzazioni soggette alla regolamentazione. NIS2 non solo si applica a più settori industriali, ma ora tutte le organizzazioni con più di 50 dipendenti e ricavi annui superiori a 10 milioni di euro devono conformarsi, siano esse pubbliche o private.

Gli Stati membri possono decidere di aggiungere entità più piccole all'elenco se ritenute avere un ruolo chiave nell'economia o nella società locale. L'ambito di applicazione di NIS2 è descritto in due allegati che elencano i settori industriali a cui la direttiva si applica automaticamente. L'allegato I elenca i settori altamente critici, mentre l'allegato II elenca gli altri settori critici.

Allegato 1 – Settori ad alta criticità	Allegato 2 – Altri settori critici
 <p>Energia</p> <ul style="list-style-type: none"> • Elettricità* • Gas* • Petrolio* • Idrogeno* • Sistemi di riscaldamento e raffreddamento a più edifici o aree 	<p>Manifatturiero</p> <ul style="list-style-type: none"> • Dispositivi medici • Informatica, elettronica e prodotti ottici • Apparecchiature elettriche • Macchinari • Veicoli a motore, rimorchi, semirimorchi • Altre attrezzature per il trasporto 
 <p>Trasporti</p> <ul style="list-style-type: none"> • Aereo* • Ferroviario* • Idroviario* • Stradale* 	<p>Fornitori digitali</p> <ul style="list-style-type: none"> • Fornitori di mercati online • Fornitori di motori di ricerca online • Fornitori di piattaforme di social network 
 <p>Infrastrutture digitali*</p>	 <p>Servizi postali e di corriere</p>
 <p>Bancario*</p>	 <p>Gestione dei rifiuti</p>
 <p>Infrastrutture di mercato finanziario*</p>	 <p>Produzione, lavorazione e distribuzione di alimenti</p>
 <p>Salute</p> <ul style="list-style-type: none"> • Fornitori di assistenza sanitaria* • Industria farmaceutica 	 <p>Produzione e distribuzione di prodotti chimici</p>
 <p>Acqua potabile*</p>	
 <p>Acque reflue</p>	
 <p>Pubblica amministrazione</p>	
 <p>Gestione dei servizi di tecnologie dell'informazione e della comunicazione</p>	

Allegato 1 – Settori ad alta criticità	Allegato 2 – Altri settori critici
 Spaziale	

Nota: Gli asterischi (*) indicano che il settore era già presente nell'allegato della direttiva NIS originale.

Secondo la direttiva NIS2, il termine "entità" descrive qualsiasi organizzazione che deve conformarsi alla direttiva, che divide le entità in due categorie. Le entità operanti nei settori elencati nell'Allegato 1 possono essere classificate come "Essenziali" o "Importanti", a seconda delle loro dimensioni e dei loro ricavi. Le entità nell'Allegato 2 possono rientrare solo nella categoria "Importanti".

Entrambe le categorie devono seguire gli stessi requisiti e conformarsi alle stesse misure di sicurezza, ma le Entità Essenziali saranno monitorate in modo proattivo, mentre le Entità Importanti saranno sottoposte ad audit solo dopo un incidente di cybersicurezza. Le Entità Essenziali affrontano sanzioni più elevate e i loro manager senior sono ritenuti responsabili in caso di inosservanza. In altre parole, il controllo delle Entità Essenziali è più rigoroso a causa delle possibili conseguenze più gravi se quell'organizzazione risulta non conforme.

Grandezza dell'Entità	Numero di dipendenti (x)	Fatturato annuo (y - M€)		Bilancio annuo (y - M€)
Grandi	$x \geq 250$	$y \geq 50$	In alternativa al fatturato annuo	$y > 43$
Medie	$50 \leq x \leq 250$	$10 \geq y > 50$		$y \leq 43$
Piccole	$x < 50$	$y < 10$		$y \leq 10$
Micro	$x < 10$	$y \leq 2$		$y \leq 2$

Nota: tutte le aziende che rientrano nella supply chain di entità soggette alla NIS2 saranno tenute ad adeguarsi alla normativa. Per la definizione di piccole, medie o micro-imprese si fa riferimento alla raccomandazione 2003/361/CE. Le imprese possono decidere se basarsi sul fatturato o sul bilancio.

Di seguito si riporta una tabella riepilogativa dell'applicazione della NIS2 per dimensione aziendale:

Settore	Grande	Media	Piccola
Energia	Essenziale	Importante	Solo se identificata come essenziale o importante
Trasporto	Essenziale	Importante	Solo se identificata come essenziale o importante
Bancario (DORA)	Essenziale	Importante	Solo se identificata come essenziale o importante
Infrastrutture finanziarie (DORA)	Essenziale	Importante	Solo se identificata come essenziale o importante
Sanità	Essenziale	Importante	Solo se identificata come essenziale o importante
Idrico	Essenziale	Importante	Solo se identificata come essenziale o importante
Infrastrutture digitali			
• Trust service provider qualificati	Essenziale	Essenziale	Essenziale
• DNS			
• TLD			
• Reti di comunicazione pubblica	Essenziale	Essenziale	Importante
• Trust service provider non qualificati	Essenziale	Importante	Importante
• Internet Exchange Point providers			
• Cloud computing service providers	Essenziale	Importante	Solo se identificata come essenziale o importante
• Data centre service providers			
• Content delivery network providers			
Gestione servizi ICT	Essenziale	Importante	Solo se identificata come essenziale o importante
Pubblica Amministrazione*	Importante	Importante	Importante
Spazio	Essenziale	Importante	Solo se identificata come essenziale o importante
Servizi postali	Importante	Importante	Solo se identificata come essenziale o importante
Gestione rifiuti	Importante	Importante	Solo se identificata come essenziale o importante
Chimico	Importante	Importante	Solo se identificata come essenziale o importante
Alimentare	Importante	Importante	Solo se identificata come essenziale o importante
Manifatturiero	Importante	Importante	Solo se identificata come essenziale o importante
Fornitori servizi digitali (es. social network, ecommerce, etc.)	Importante	Importante	Solo se identificata come essenziale o importante
Ricerca	Importante	Importante	Solo se identificata come essenziale o importante

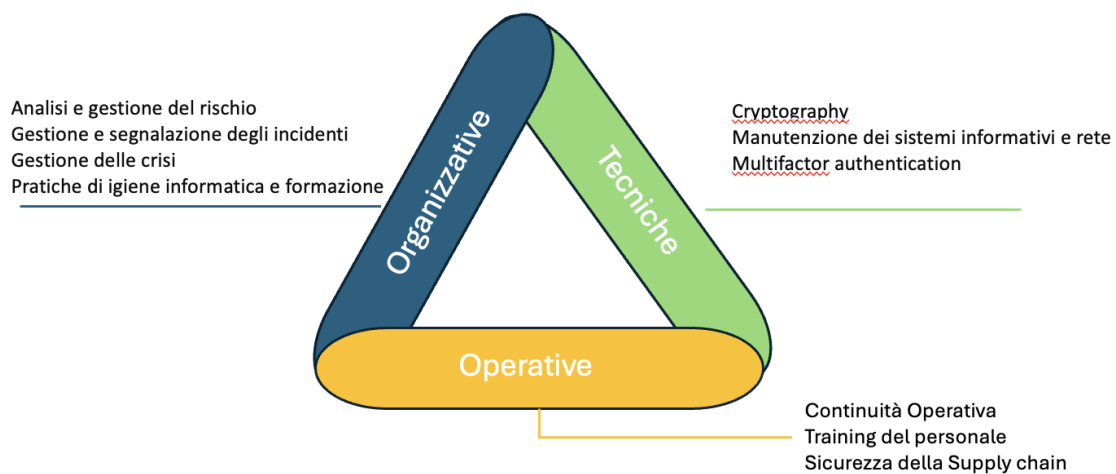
* eccetto: magistratura, parlamento, banca centrale; sicurezza nazionale, pubblica sicurezza, difesa e forze dell'ordine. Secondo quanto stabilito dalla legge n.90 del 28 giugno 2024, vengono incluse anche le regioni e le province autonome di Trento e di Bolzano, le città metropolitane, i comuni con popolazione superiore a 100.000 abitanti e, comunque, i comuni capoluoghi di regione, nonché le società di trasporto pubblico urbano con bacino di utenza non inferiore a 100.000 abitanti, le società di trasporto pubblico extraurbano operanti nell'ambito delle città metropolitane e le aziende sanitarie locali.

Quali misure di sicurezza informatica prevede NIS2

Le misure di sicurezza informatica che le Entità Essenziali e Importanti devono rispettare sono definite da ciascuno Stato membro nella loro trasposizione nazionale della direttiva. Tuttavia, NIS2 impone un approccio di gestione del rischio con un elenco di misure di sicurezza di base da implementare raggruppate come indicato nella figura sotto in organizzative, tecniche e operative:





- Politiche di analisi del rischio e sicurezza dei sistemi informativi;

- Gestione degli incidenti;
- Continuità operativa, come la gestione dei backup e il ripristino in caso di disastro, e gestione delle crisi;
- Sicurezza della catena di fornitura, inclusi gli aspetti relativi alla sicurezza delle relazioni tra ciascun ente e i suoi fornitori o prestatori di servizi diretti;
- Sicurezza nell'acquisizione, sviluppo e manutenzione dei sistemi di rete e informativi, inclusa la gestione e la divulgazione delle vulnerabilità;
- Politiche e procedure per valutare l'efficacia delle misure di gestione del rischio di cybersecurity;
- Pratiche di igiene informatica di base e formazione sulla sicurezza informatica;
- Politiche e procedure riguardanti l'uso della crittografia e, se del caso, della cifratura;
- Sicurezza delle risorse umane, politiche di controllo degli accessi e gestione degli asset;
- Uso di soluzioni di autenticazione multifattore o di autenticazione continua, comunicazioni vocali, video e testuali sicure e sistemi di comunicazione di emergenza sicuri all'interno dell'ente, ove opportuno.



Obblighi di notifica

Sebbene la direttiva NIS abbia sempre richiesto alle organizzazioni di segnalare gli incidenti di sicurezza informatica, NIS2 rende obbligatoria la segnalazione degli incidenti "significativi" e descrive un processo chiaro e rigoroso per farlo. Per mantenere la conformità, le entità devono notificare gli incidenti al Computer Security Incident Response Team (CSIRT) o qualsiasi altra autorità competente del proprio paese secondo la seguente tempistica una volta verificatosi un incidente.

24 Ore	72 Ore	1 Mese	Su richiesta delle autorità
 <p>Obbligati a segnalare qualsiasi incidente significativo entro 24 ore dal momento in cui ne sono venuti a conoscenza, indipendentemente dal fatto che abbia avuto un impatto diretto sulle operazioni.</p>	 <p>Rapporto aggiornato entro 72 ore dal momento in cui si viene a conoscenza dell'incidente, descrivendo la natura dell'incidente, la sua gravità, gli impatti e gli indicatori di compromissione.</p>	 <p>Una descrizione dettagliata dell'incidente deve essere presentata entro 1 mese, spiegando le possibili cause, le misure di mitigazione in corso e l'impatto transfrontaliero.</p>	 <p>Su richiesta delle autorità di regolamentazione potranno essere richiesti aggiornamenti di natura rilevante.</p>

La direttiva richiede alle entità di implementare meccanismi di rilevamento e risposta agli incidenti. Devono identificare rapidamente gli incidenti e valutarne l'impatto. A seconda del contesto, potrebbero essere tenuti a informare i propri clienti e il pubblico.

Di seguito si riporta una tabella riepilogativa dei controlli che verranno effettuati in base alla tipologia di Ente:

Enti Essenziali	Enti Importanti
Controlli completi in anticipo o quando viene segnalato un incidente o se ci sono dubbi sulla conformità (regime di vigilanza ex-ante ed ex-post).	Controlli leggeri quando viene segnalato un incidente o se ci sono dubbi sulla conformità (regime di vigilanza ex-post).
Ispezioni in loco e supervisione a distanza.	Ispezioni in loco ex-post e supervisione a distanza.
Audit di sicurezza regolari e mirati.	Audit di sicurezza mirati.
Scansioni di sicurezza.	Scansioni di sicurezza.
Richieste di informazioni.	Richieste di informazioni.
Richieste di informazioni per valutare le politiche di cybersicurezza e le misure di gestione del rischio in atto.	Richieste di informazioni per valutare, ex-post, le politiche di cybersicurezza e le misure di gestione del rischio in atto.
Audit ad hoc, per esempio dopo un incidente significativo.	

La versione originale della direttiva NIS consentiva agli Stati membri di definire sanzioni per la non conformità, portando a molte disparità in tutta l'UE. La NIS2 impone un regime sanzionatorio comune progettato per essere efficace, proporzionato e dissuasivo.

Le sanzioni sono commissionate in aggiunta agli audit, alle ispezioni e ai controlli elencati precedentemente e possono andare da semplici avvertimenti a ordini di interruzione di condotta, ordini di attuazione di misure, ordini di informare il pubblico, sanzioni amministrative pecuniarie e altro ancora. Inoltre, agli Enti Essenziali può essere sospesa la certificazione o l'autorizzazione a operare. L'autorità può anche designare un funzionario per il monitoraggio e supervisionare la conformità.

I manager senior possono essere ritenuti personalmente responsabili delle violazioni e sono tenuti ad approvare le misure di cybersicurezza adottate, supervisionarne l'attuazione, partecipare a formazioni e offrire analoghe formazioni ai dipendenti. Ultimo ma non meno importante, sia gli Enti Essenziali che quelli Importanti sono soggetti a significative sanzioni pecuniarie quando si dimostra la loro non conformità.

Impatto della NIS2 sulle attività delle PMI

Di seguito si analizzeranno gli obblighi normativi imposti dalla direttiva e come ciò richieda alle PMI di adattare le loro pratiche operative e di sicurezza informatica. Il focus sarà maggiore sulle PMI in quanto, con molta probabilità, sarà il taglio di aziende che necessiteranno maggiormente di supporto per adeguarsi alla normativa NIS2.


Per raggiungere i suoi obiettivi di rafforzamento della resilienza e della sicurezza informatica, la Direttiva NIS2 introduce una serie di nuovi requisiti per le aziende rientranti nel suo ambito di applicazione. Tra i principali requisiti troviamo:

1. **Governance e gestione dei rischi:** la direttiva richiede che gli Operatori di Servizi Essenziali (**OSE**) e i Digital Service Providers (**DSP**) abbiano un organo di gestione che approvi formalmente le misure di gestione dei rischi cyber. Inoltre, è richiesta una maggiore responsabilizzazione del management aziendale sulla cybersicurezza, con l'obbligo di formazione per i membri degli organi di gestione e i dipendenti sui rischi cyber.
2. **Misure di sicurezza:** le aziende devono implementare misure di sicurezza adeguate per proteggere i loro sistemi e reti, inclusi controlli di accesso, protezione dei dati, monitoraggio e rilevamento degli incidenti, e piani di continuità operativa.
3. **Segnalazione degli incidenti:** in caso di incidenti di sicurezza informatica, le aziende hanno l'obbligo di notificarli alle autorità competenti entro 24 ore. Inoltre, devono pubblicare sui propri canali le violazioni subite, in modo da aumentare la consapevolezza e la trasparenza.
4. **Quadro sanzionatorio:** la direttiva stabilisce un apparato sanzionatorio che i singoli Stati Membri sono chiamati a rendere effettivo, proporzionato e dissuasivo in fase di recepimento ed è prevista la proporzionalità delle sanzioni per i soggetti essenziali e importanti.

Le sanzioni amministrative pecuniarie previste, come precedentemente riportato, sono le seguenti:

- a. le organizzazioni essenziali sono soggette a sanzioni “pari a un massimo di almeno 10.000.000 euro o a un massimo di almeno il 2 % del fatturato mondiale annuo”
- b. le organizzazioni importanti sono soggette a sanzioni “pari a un massimo di almeno 7.000.000 euro o a un massimo di almeno l’1,4% del fatturato mondiale annuo”.

Ciò significa che lo Stato italiano dovrà individuare un massimale per le sanzioni non inferiore a 10.000.000 o del 2% del fatturato per i soggetti essenziali e di 7.000.000 o dell’1,4% del fatturato per i soggetti importanti.



-
5. **Promozione della certificazione:** la direttiva incoraggia l'adozione di prodotti e servizi ICT Certificati, al fine di migliorare la sicurezza informatica delle aziende.

Questi requisiti rappresentano una sfida significativa per le PMI, che dovranno investire risorse e competenze per adeguarsi alla Direttiva NIS2. Tuttavia, come centro di ricerca e innovazione, riteniamo che questo processo di adeguamento possa anche rappresentare un'opportunità per le aziende di migliorare la propria resilienza e competitività.

Nello specifico, i principali obiettivi della Direttiva NIS2 sono:

1. **Ampliare il perimetro di applicazione:** la nuova direttiva si applica a un numero maggiore di settori e categorie di aziende rispetto alla precedente normativa, includendo anche le PMI.
2. **Rafforzare gli obblighi di governance e gestione dei rischi:** la direttiva introduce requisiti più stringenti in termini di responsabilizzazione del management aziendale sulla cybersicurezza e di formazione del personale.
3. **Migliorare la segnalazione degli incidenti:** la NIS2 prevede nuovi obblighi di notifica e pubblicazione delle violazioni subite, accompagnati da un quadro sanzionatorio più dettagliato.
4. **Promuovere l'uso di prodotti e servizi TLC certificati:** la direttiva incoraggia l'adozione di soluzioni tecnologiche certificate per migliorare la sicurezza informatica.

Questi obiettivi riflettono l'esigenza di rafforzare la preparazione e la resilienza dell'Unione Europea di fronte alle crescenti minacce cyber, che possono avere gravi ripercussioni sulla fornitura di servizi essenziali e sulla competitività delle imprese.

Attuazione della Normativa NIS2

Per garantire l'attuazione efficace della Direttiva NIS2, il quadro normativo prevede il coinvolgimento di diverse autorità a livello nazionale ed europeo. A livello nazionale, gli Stati membri dell'Unione Europea devono designare una o più autorità competenti responsabili dell'applicazione della direttiva. Queste autorità avranno il compito di:

- Monitorare il rispetto degli obblighi da parte delle aziende rientranti nell'ambito di applicazione della NIS2.
- Ricevere e gestire le notifiche degli incidenti di sicurezza.
- Imporre sanzioni in caso di mancata conformità.
- Fornire orientamenti e assistenza alle aziende per l'attuazione della normativa.

A livello europeo, la Direttiva NIS2 prevede il rafforzamento del ruolo del Gruppo di cooperazione, un organismo composto da rappresentanti degli Stati membri e della Commissione Europea. Il Gruppo di cooperazione avrà il compito di:

- Promuovere la condivisione di informazioni e di buone pratiche tra gli Stati membri.
- Fornire orientamenti e raccomandazioni per l'attuazione uniforme della direttiva.
- Monitorare l'applicazione della normativa a livello europeo.

Inoltre, la Direttiva NIS2 prevede che l'Agenzia dell'Unione Europea per la Cybersicurezza (ENISA) avrà un ruolo centrale nel supportare gli Stati membri e le aziende nell'attuazione della normativa.

Per l'Italia, è stata designata l'Agenzia per la Cybersicurezza Nazionale (**ACN**) per gestire tutte le attività di regolamentazione e attuazione della disciplina cyber, ivi incluso il rapporto con i soggetti vigilati e con le amministrazioni coinvolte, curando anche le attività del Comitato tecnico di raccordo, e il recepimento della Direttiva stessa.

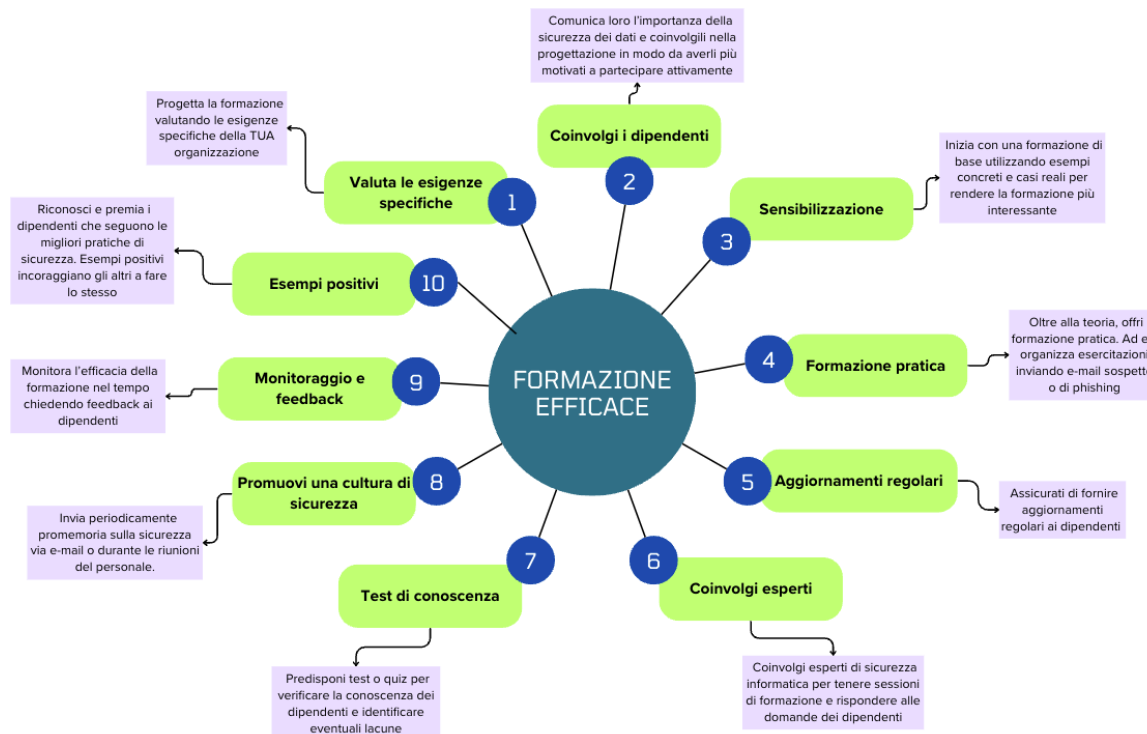
La Direttiva NIS2 rappresenta un importante passo avanti nella promozione della cybersicurezza nell'Unione Europea attraverso l'ampliamento del suo ambito di applicazione, il rafforzamento degli obblighi per le aziende e il coinvolgimento di autorità nazionali ed europee. Questa normativa mira a migliorare la resilienza e la preparazione dell'Europa di fronte alle crescenti minacce cyber. Per le PMI, l'adeguamento alla Direttiva NIS2 rappresenterà una sfida significativa, ma anche un'opportunità per innovare i propri processi e sistemi, contribuendo così alla loro crescita e competitività.

Le PMI, pur essendo fondamentali per l'economia, possono essere particolarmente vulnerabili agli attacchi informatici ed è quindi essenziale che si adeguino alla nuova direttiva.

Creazione di awareness e formazione dei dipendenti

Assesment competenze in-house e formazione differenziata per tipologia di dipendenti e/o per comparti organizzativi.

La direttiva NIS2 rappresenta una sfida significativa per le piccole e medie imprese europee ed italiane, chiamate ad adottare misure adeguate per rafforzare la loro postura di cybersicurezza. Conformarsi ai requisiti normativi richiederà alle PMI un approccio strutturato e una gestione oculata delle proprie risorse, a partire dal capitale umano. In questo contesto, implementare un solido programma di assesment delle competenze interne e di formazione differenziata in funzione dei ruoli e comparti organizzativi diventa un fattore chiave per il successo. Di seguito alcuni suggerimenti concreti per implementare una formazione efficace sulla sicurezza dei dati all'interno di una organizzazione:



Il primo passo è condurre una valutazione approfondita delle conoscenze, abilità e competenze già presenti in azienda in materia di cybersecurity. Questo processo di assesment può avvalersi di una combinazione di strumenti quali test scritti, esercizi pratici, simulazioni, interviste mirate e osservazioni sul campo. L'obiettivo è mappare in dettaglio il livello di preparazione dei dipendenti, evidenziando punti di forza, lacune e aree di miglioramento rispetto ai requisiti imposti da NIS2.

I dati raccolti forniranno alle PMI una visione d'insieme sullo stato dell'arte delle competenze cyber, consentendo di identificare con precisione i gap formativi da colmare.

Oltre ai percorsi formativi mirati, è fondamentale istituire **sessioni di aggiornamento periodiche** per mantenere le competenze al passo con l'evoluzione delle minacce e delle best practice di sicurezza. La formazione continua e l'adozione di una mentalità di "lifelong learning" in ambito cyber sono fattori imprescindibili per rimanere conformi nel lungo periodo con NIS2.

Programmi di assesment e formazione differenziata strutturati in questo modo offrono alle PMI molteplici benefici. Da un lato, consentono di creare e consolidare internamente le competenze chiave richieste per implementare e mantenere



misure di cybersecurity adeguate. Dall'altro, alimentano una cultura aziendale incentrata sui temi della sicurezza informatica, della resilienza e del miglioramento continuo, fattori essenziali per un'organizzazione che voglia rimanere compliant con NIS2 e proteggersi efficacemente dalle minacce cyber.

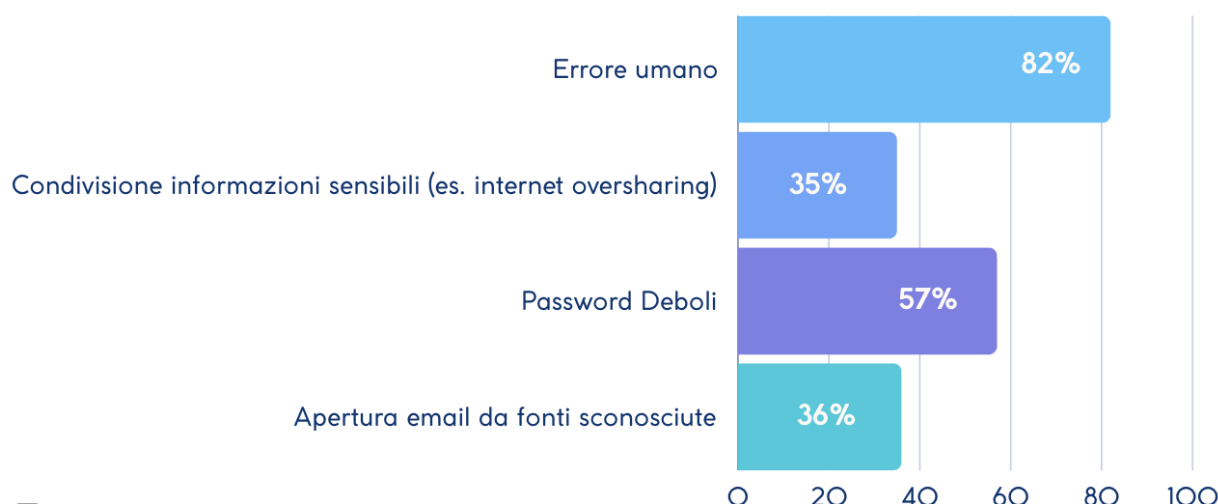
Inoltre, investire nell'**upskilling dei dipendenti in ottica di sicurezza** si traduce anche in un **vantaggio competitivo per le PMI**. Personale adeguatamente formato è infatti in grado di gestire i rischi cyber in modo più efficiente, riducendo l'esposizione a potenziali violazioni, interruzioni di servizio e conseguenti danni reputazionali ed economici.

Ruolo dei dipendenti nella prevenzione delle minacce informatiche e nell'attuazione delle misure di sicurezza.

Nel contesto della direttiva NIS2, il ruolo dei dipendenti riveste un'importanza fondamentale nella prevenzione delle minacce informatiche e nell'attuazione delle misure di sicurezza. I dipendenti sono spesso considerati il primo livello di difesa contro le minacce cibernetiche, poiché le loro azioni possono influenzare direttamente la sicurezza dei sistemi e dei dati aziendali. Inoltre, il coinvolgimento attivo dei dipendenti è essenziale per garantire il successo e l'efficacia delle politiche e delle procedure di sicurezza informatica adottate dalle organizzazioni.

L'anello debole della Cybersecurity è legato al "comportamento umano"

Le attività di un individuo, nella sua interazione con il web, con colleghi, clienti e fornitori possono mettere a rischio la sua sicurezza, quella dell'organizzazione di cui fa parte e di tutta la catena di fornitori (supply chain).



Formazione

Solo con un corretto programma di formazione è possibile migliorare la postura digitale degli utenti e ridurre l'importante componente di vulnerabilità legata all'errore umano.

Un aspetto chiave del ruolo dei dipendenti è la **consapevolezza** e la formazione sulla sicurezza informatica. La direttiva NIS2 sottolinea l'importanza di fornire ai dipendenti una formazione adeguata sulle minacce informatiche, sui protocolli di sicurezza e sulle migliori pratiche per proteggere i dati sensibili dell'azienda. I dipendenti devono essere in grado di riconoscere e segnalare potenziali minacce, come *phishing*, *malware* o *tentativi di accesso non autorizzato*, contribuendo così alla tempestiva identificazione e mitigazione degli incidenti di sicurezza.

Un'altra componente cruciale del ruolo dei dipendenti nella prevenzione delle minacce informatiche è la collaborazione e la comunicazione con le funzioni aziendali pertinenti, come il team IT e il team di sicurezza informatica. Le risorse interne devono essere incoraggiate a segnalare eventuali anomalie o comportamenti sospetti ai responsabili della sicurezza informatica, consentendo loro di rispondere prontamente e di adottare misure correttive necessarie per proteggere l'azienda da potenziali attacchi.

Strategie e suggerimenti proposti dal centro Cyber 4.0 per implementare efficacemente programmi di formazione e sensibilizzazione nelle PMI.

L'Associazione Cyber 4.0 si dedica alla promozione della cultura cyber e all'implementazione di progetti innovativi, impegnandosi a fornire strategie e suggerimenti efficaci per implementare programmi di formazione e sensibilizzazione all'interno delle PMI in linea con la direttiva NIS2. La formazione e la sensibilizzazione sono elementi fondamentali per migliorare la sicurezza informatica all'interno delle PMI, poiché i dipendenti sono spesso il primo punto di contatto con le minacce cibernetiche e possono svolgere un ruolo cruciale nel prevenire e mitigare gli attacchi.

Alcuni punti chiave

Minimizzare gli errori umani

La maggior parte delle violazioni dei dati è causata da errori umani. La formazione sulla sicurezza informatica aiuta i dipendenti a riconoscere e prevenire le minacce, riducendo così il rischio di commettere errori che potrebbero compromettere la sicurezza dei dati.

Promuovere una cultura di sicurezza

La formazione crea una cultura di conformità alla sicurezza all'interno dell'organizzazione. Quando i dipendenti sono coinvolti e consapevoli, diventano parte attiva nella protezione dei dati e dei sistemi.

Adattare i contenuti e le modalità di formazione

Questa attività include anche la creazione di materiali formativi personalizzati che riflettano i rischi e le sfide uniche affrontate dall'azienda, e la pianificazione di sessioni interattive che coinvolgono attivamente i dipendenti.

Valutare regolarmente l'efficacia dei programmi di formazione

Apportare eventuali aggiornamenti o miglioramenti in base ai feedback dei dipendenti e agli sviluppi nel panorama della sicurezza informatica.

Riconoscere le minacce comuni

La formazione sensibilizza i dipendenti sulle tattiche utilizzate dagli attaccanti, come l'hacking tramite e-mail di phishing. Quando i dipendenti sono consapevoli delle minacce, sono più propensi a adottare comportamenti sicuri.

Proteggere la reputazione aziendale

Le violazioni della sicurezza possono danneggiare gravemente la reputazione di un'azienda. La formazione aiuta a prevenire incidenti e a gestire meglio le conseguenze in caso di violazione.

Coinvolgere la leadership aziendale

Dovrà supportare attivamente i programmi di formazione e sensibilizzazione sulla sicurezza informatica. I dirigenti e i responsabili devono dimostrare un forte impegno nei confronti della sicurezza informatica, promuovendo la partecipazione dei dipendenti alla formazione.

Per minimizzare gli errori umani (figura punti chiave) è necessario puntare sul training e su una strategia chiave per implementare con successo programmi di formazione e sensibilizzazione all'interno delle PMI italiane, adattando i contenuti e le modalità di formazione alle esigenze specifiche dell'organizzazione. Questa attività include anche la creazione di materiali formativi personalizzati che riflettano i rischi e le minacce e le sfide uniche affrontate dall'azienda, nonché la pianificazione di sessioni interattive che coinvolgano attivamente i dipendenti.

E' importante integrare la formazione sulla sicurezza informatica all'interno dei processi di aggiornamento regolari ai dipendenti per mantenere la consapevolezza e le competenze aggiornate, promuovendo una cultura sulla sicurezza. Questo può essere realizzato attraverso webinar, sessioni di formazione in persona, moduli online o altre modalità di apprendimento flessibili che si adattino alle esigenze e agli impegni dei dipendenti. Inoltre le imprese devono mantenere alta l'attenzione sulla propria reputazione, educando i propri dipendenti a non diffondere informazioni riservate.

Inoltre, per massimizzare l'efficacia dei programmi di formazione e sensibilizzazione, è importante adottare un approccio completo che includa la verifica della preparazione del personale sui rischi cyber e sulle best practice per proteggere i dati aziendali, identificando e segnalando eventuali minacce e adottando comportamenti sicuri durante l'uso dei dispositivi e delle risorse aziendali.