CYBERSECURITY

DALLA MINACCIA INFORMATICA AL RISCHIO AZIENDALE

“Comprendere il rischio cyber nelle aziende e costruire un modello di gestione integrato, documentato e sostenibile.”

CompliWare
Digital Facilities for Audit Risk Compliance

TABLE OF CONTENTS

LO SCENARIO CYBER

PERCHÈ PARLIAMO DI CYBERSECURITY?

La cybersecurity oggi riguarda **ogni organizzazione** che utilizza:

- dati,
- sistemi digitali,
- software gestionali,
- cloud,
- dispositivi mobili,
- piattaforme collaborative o fornitori tecnologici.

Un incidente cyber può **bloccare attività operative**, **compromettere dati**, generare obblighi di notifica, esporre l'impresa a **sanzioni** e compromettere la fiducia di clienti, partner e stakeholder.

La cybersecurity è l'insieme di **misure tecniche**, **organizzative** e procedurali volte a **proteggere sistemi informatici,** reti, dati e **servizi digitali** da:

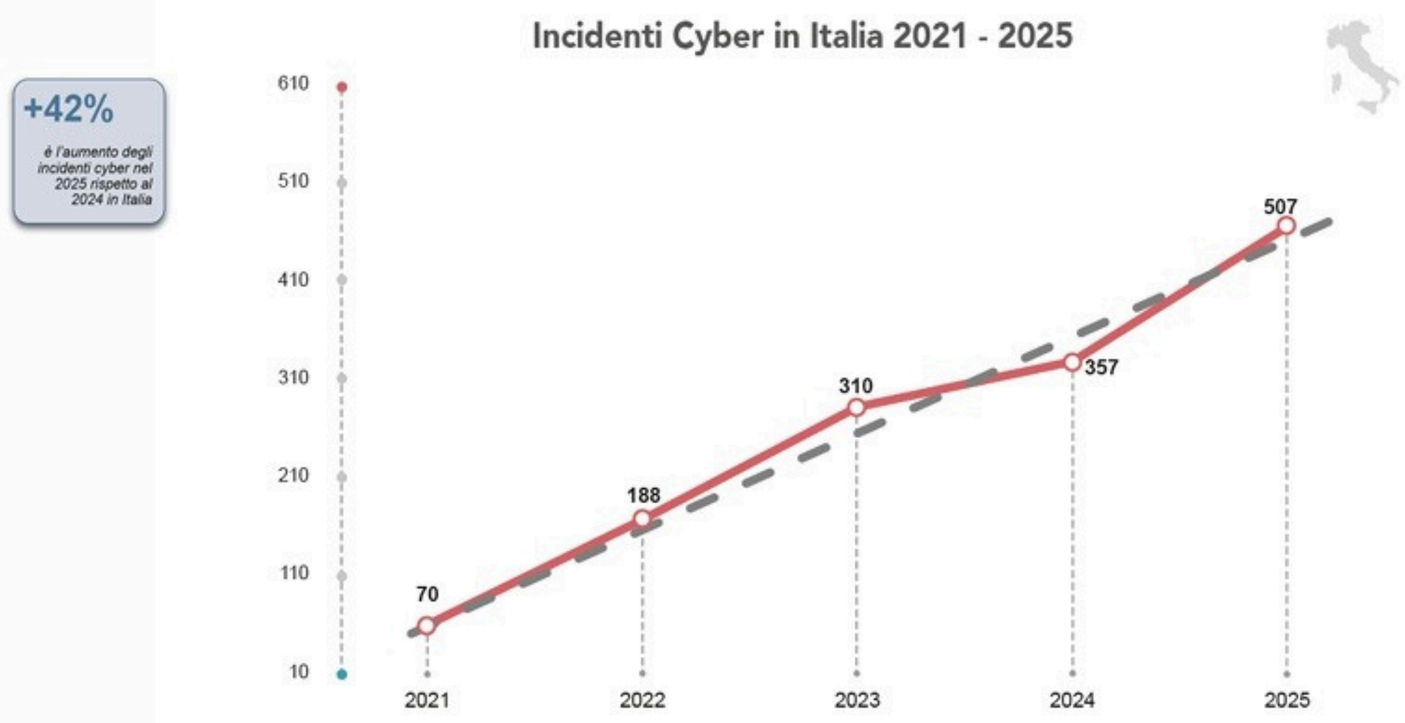
- accessi non autorizzati,
- attacchi,
- danni o interruzioni.

Essa deve garantire tre dimensioni fondamentali:

- **protezione dei dati;**
- **continuità dei servizi;**
- **resilienza organizzativa.**

PERCHÉ OGGI È COSÌ IMPORTANTE

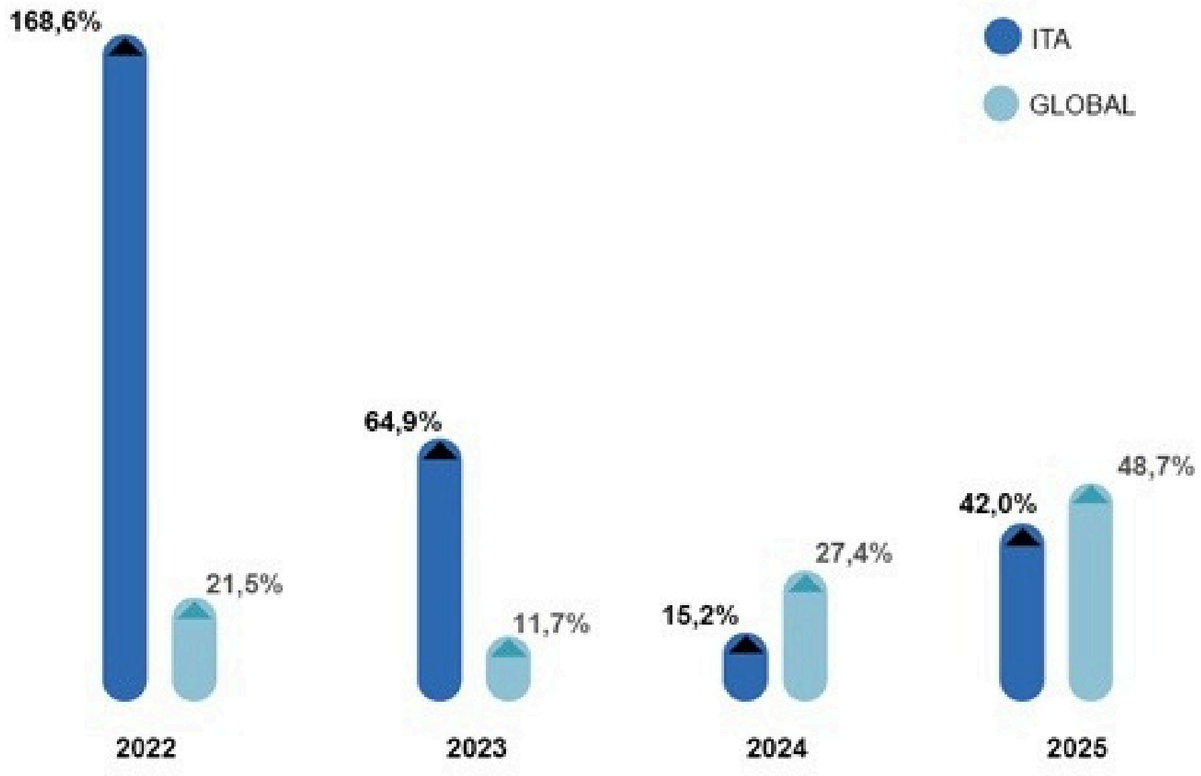
Il **rischio cyber cresce** perché le **aziende** sono sempre **più digitalizzate** e interconnesse. I processi aziendali dipendono da software, cloud, piattaforme gestionali, dispositivi mobili, fornitori ICT e servizi online.



La superficie di attacco aumenta con:

- **digitalizzazione** dei processi;
- **cloud** e piattaforme collaborative;
- lavoro da **remoto**;
- dispositivi mobili;
- **accessi esterni**;
- **integrazione con fornitori e partner**;
- maggiore valore economico dei dati;
- attacchi più frequenti e sofisticati.

Confronto crescita % Italia vs Global



Il grafico evidenzia come l'Italia continui a essere **fortemente esposta al rischio cyber**, con una crescita degli incidenti che, pur oscillando negli anni, resta costantemente significativa. **Nel 2025 gli attacchi in Italia aumentano del 42%**, un dato vicino alla crescita globale del 48,7%, confermando che il fenomeno non riguarda solo grandi scenari internazionali, ma c**oinvolge direttamente** anche il **tessuto economico e istituzionale italiano**. Il **cyber risk** si presenta quindi come un rischio attuale, concreto e in **progressiva espansione**.

+37%

È la crescita del numero degli incidenti a danno dei settori GOV / Mil / LE

1 su 5

è un incidente derivante da una campagna generalizzata su più settori

Fonte: Clusit - Rapporto 2026 sulla Cybersecurity

Il grafico mostra che gli attacchi cyber in Italia colpiscono settori molto diversi tra loro: **pubblica amministrazione, manifatturiero, trasporti, commercio, servizi professionali, ICT, finanza, energia e sanità**. Questo conferma che **la cybersecurity** non riguarda solo le infrastrutture critiche o le grandi organizzazioni, ma **interessa l'intero sistema produttivo.**

RISCHI E IMPATTI DEGLI ATTACCHI CYBER

DAL RISCHIO INFORMATICO
AL RISCHIO AZIENDALE

Un incidente cyber non è soltanto un problema tecnico o informatico, ma **un vero e proprio evento aziendale.** In qualsiasi contesto aziendale, l'indisponibilità di sistemi digitali, software gestionali, piattaforme documentali, sistemi di comunicazione, infrastrutture amministrative, ambienti cloud o applicativi utilizzati nei processi produttivi e commerciali può determinare il **blocco o il rallentamento di attività essenziali**, con **effetti immediati su clienti, fornitori, dipendenti e stakeholder**.

Per questo motivo, la gestione dell'incidente richiede:

- **ruoli chiari**,
- **flussi** decisionali **definiti**,
- **procedure formalizzate**,
- **obblighi di comunicazione** verso autorità e stakeholder,
- una **capacità di risposta coordinata**, documentata e tempestiva.

LE PRINCIPALI TIPOLOGIE DI ATTACCO

Phishing

Si realizza attraverso **email o messaggi ingannevoli** finalizzati al **furto delle credenziali**

Ransomware

Comporta il **blocco o la cifratura dei dati** con possibile **interruzione dell'attività aziendale**

Malware

Ossia l'utilizzo di **software malevoli** in grado di **compromettere** sistemi, dispositivi o infrastrutture

Social engineering

Sfrutta la **manipolazione** delle **persone** per **ottenere informazioni riservate** o accessi non autorizzati

DDoS

Basati sul **sovraccarico dei sistemi** e capaci di determinare il **blocco dei servizi online**

Data breach

Consistono nella **violazione, perdita o diffusione non autorizzata di dati**, con conseguenti obblighi privacy e possibili **danni reputazionali**

Supply chain attack

Colpiscono **fornitori o partner tecnologici** e possono **propagare il rischio** all'intera organizzazione

Business email compromise

Consistono nella **compromissione di caselle email aziendali** e possono **generare frodi, pagamenti illeciti o comunicazioni fraudolente**

GLI IMPATTI PRINCIPALI
DI UN INCIDENTE CYBER

IMPATTO OPERATIVO

può determinare il **blocco o il rallentamento** delle **attività aziendali**, **l'indisponibilità** di software gestionali, piattaforme documentali, sistemi di comunicazione o infrastrutture digitali essenziali.

IMPATTO REPUTAZIONALE E ORGANIZZATIVO

incidendo sulla fiducia di clienti, partner e stakeholder e richiedendo decisioni rapide, comunicazioni urgenti e una gestione coordinata della crisi interna.

IMPATTO ECONOMICO

costi di ripristino, delle **consulenze** specialistiche, del fermo attività e delle eventuali **perdite di produttività**.

IMPATTO SUI DATI

può comportare **perdita, alterazione, esfiltrazione o indisponibilità** di informazioni aziendali, dati personali, documenti riservati o know-how.

IMPATTO LEGALE E SANZIONATORIO

connesso agli obblighi di notifica, alle **possibili contestazioni** da parte di clienti, fornitori o autorità e all'applicazione di sanzioni in caso di violazione della normativa applicabile.

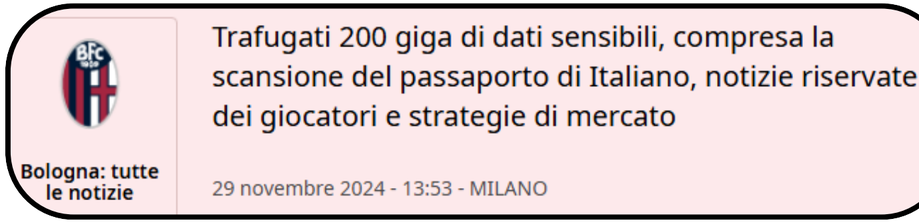
CYBER ATTACCHI IN ITALIA:
CASI REALI E LEZIONI APPRESE

SYNLAB ITALIA – RANSOMWARE E DATA BREACH

Nel 2024 SYNLAB Italia è stata colpita da un attacco ransomware che ha comportato l'interruzione di diversi servizi e la possibile esfiltrazione di circa 1,5 TB di dati sensibili. Il caso evidenzia il collegamento tra blocco operativo, violazione dei dati, obblighi privacy e danno reputazionale.

BOLOGNA FC 1909 – RANSOMWARE ED ESFILTRAZIONE DATI

Nel 2024 il Bologna FC ha confermato un attacco ransomware con sottrazione di dati aziendali. Il gruppo RansomHub ha rivendicato circa 200 GB di dati, inclusi documenti societari e informazioni personali. Il caso dimostra che il rischio cyber riguarda anche settori non tradizionalmente percepiti come critici.



PREVENZIONE, PROTEZIONE E RISPOSTA

LE PRINCIPALI DIFESE:
1)IL FATTORE UMANO

Molti incidenti cyber non derivano necessariamente da tecnologie particolarmente sofisticate, ma da **comportamenti inconsapevoli o da errori operativi**:

- l'apertura di **allegati sospetti**,
- l'utilizzo di **password deboli**,
- il **mancato riconoscimento** di email fraudolente,
- la **condivisione impropria** di informazioni,
- l'**uso non controllato** di dispositivi personali

Per questo motivo, la **protezione** aziendale deve partire anche dalle **persone**, attraverso:

- **formazione periodica**,
- **simulazioni** di phishing,
- **regole chiare** sulla gestione delle password,
- **autenticazione multifattore**,
- **procedure** realmente applicabili nella quotidianità lavorativa.

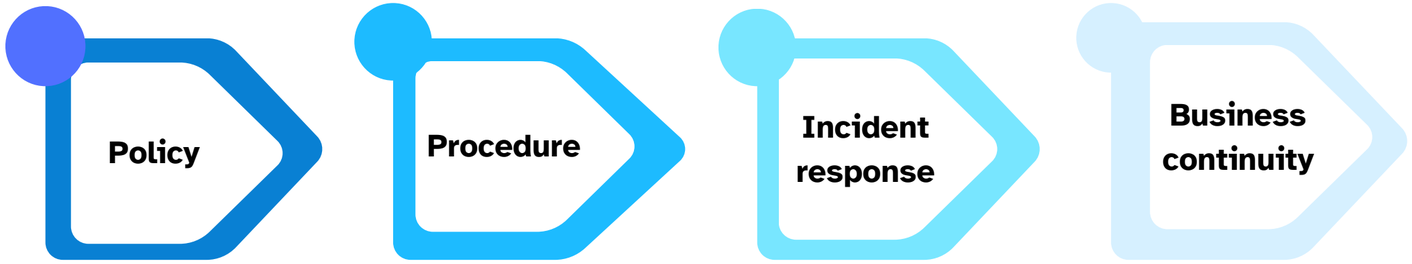
LE PRINCIPALI DIFESE:
2)I PROCESSI

I processi consentono di **trasformare la cybersecurity** da semplice insieme di strumenti tecnici a un **sistema organizzato, tracciabile e controllabile**. Per garantire un adeguato presidio dei rischi cyber, è **necessario formalizzare**, approvare, comunicare alle funzioni interessate, aggiornare periodicamente i principali documenti aziendali. In particolare:

- **policy** interne,
- **procedure** di gestione degli incidenti,
- regole per la gestione degli accessi,
- **controlli** sui fornitori,
- **backup**,
- business continuity e **disaster recovery**.

In questo modo l'azienda:

- **previene** gli incident,
- **reagisce** tempestivamente,
- **dimostra** di aver **adottato** le **adeguate misure.**

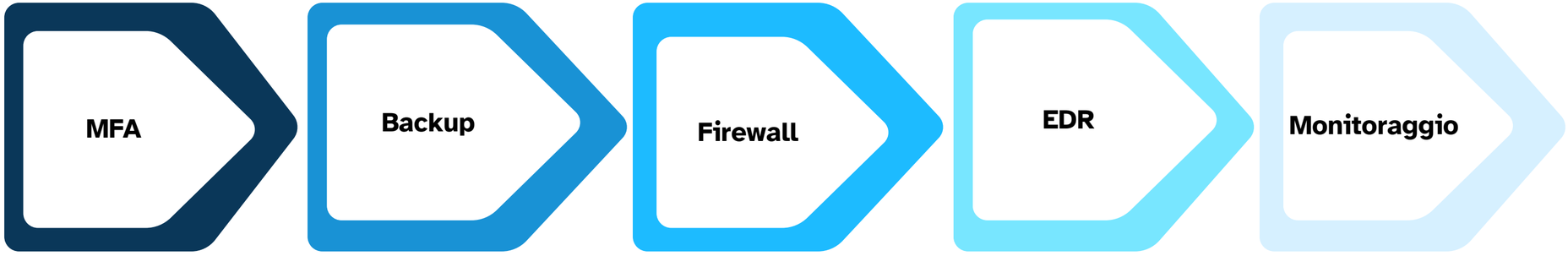


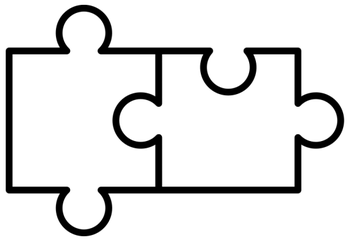
LE PRINCIPALI DIFESE:
3)TECNOLOGIA

La tecnologia rappresenta il livello di protezione che consente all'organizzazione di **prevenire, rilevare e gestire** tempestivamente gli **attacchi informatici** attraverso i seguenti strumenti:

- l'autenticazione multifattore (**MFA**),
- i **firewall**,
- gli **antivirus**/EDR,
- la **crittografia**,
- gli **aggiornamenti di sicurezza** e i sistemi di monitoraggio,
- la **gestione** delle **vulnerabilità** e la protezione degli endpoint.

Tuttavia, tali strumenti sono realmente efficaci solo se configurati correttamente, aggiornati nel tempo e integrati in un modello organizzativo più ampio, fondato su procedure, responsabilità e controlli.





LA CYBERSECURITY COME SISTEMA INTEGRATO

La cybersecurity efficace si costruisce attraverso un **modello integrato** di gestione del rischio cyber, capace di **collegare aspetti tecnici, organizzativi, procedurali e di governance.** L'efficacia delle misure di sicurezza dipende infatti:

- dalla **presenza** di **ruoli** e **responsabilità** chiaramente definiti,
- procedure **formalizzate**,
- controlli **periodici**,
- adeguate **attività** di **formazione** e sensibilizzazione del personale.

Allo stesso modo, **policy e procedure** devono essere applicate **nei processi aziendali**, conosciute dalle funzioni coinvolte e aggiornate rispetto all'evoluzione delle minacce, delle tecnologie e degli obblighi normativi.

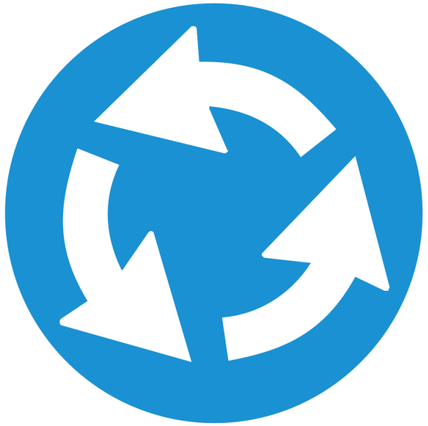
La **cybersecurity** deve quindi essere gestita come un **processo ciclico e continuo**, che **integra analisi dei rischi, definizione e attuazione dei presidi**, formazione, monitoraggio, gestione degli incidenti e **miglioramento progressivo** del sistema.

LA CYBERSECURITY COME SISTEMA INTEGRATO

Governance

Audit e miglioramento continuo

Risk assessment



Incident response

Misure tecniche organizzative

Monitoraggio

Policy e Procedure

Formazione

IL QUADRO NORMATIVO

PERCHÈ LE NORMATIVE SULLA CYBER SECURITY SONO IN AMUENTO?

Le **normative europee e nazionali sulla cybersecurity sono aumentate** perché la digitalizzazione ha reso imprese, pubbliche amministrazioni e settori essenziali, sempre più dipendenti da sistemi informativi, infrastrutture connesse, dati e servizi digitali. In questo scenario, gli **attacchi informatici** sono diventati più **frequenti**, **sofisticati** e capaci di generare **impatti economici**, **strategici** e **operativi** rilevanti.

L'obiettivo del legislatore è quindi rafforzare la resilienza dei sistemi informativi nazionali ed europei, definendo **standard minimi di sicurezza** per i settori strategici e armonizzando le regole a livello europeo.

Le organizzazioni devono quindi dimostrare di avere:

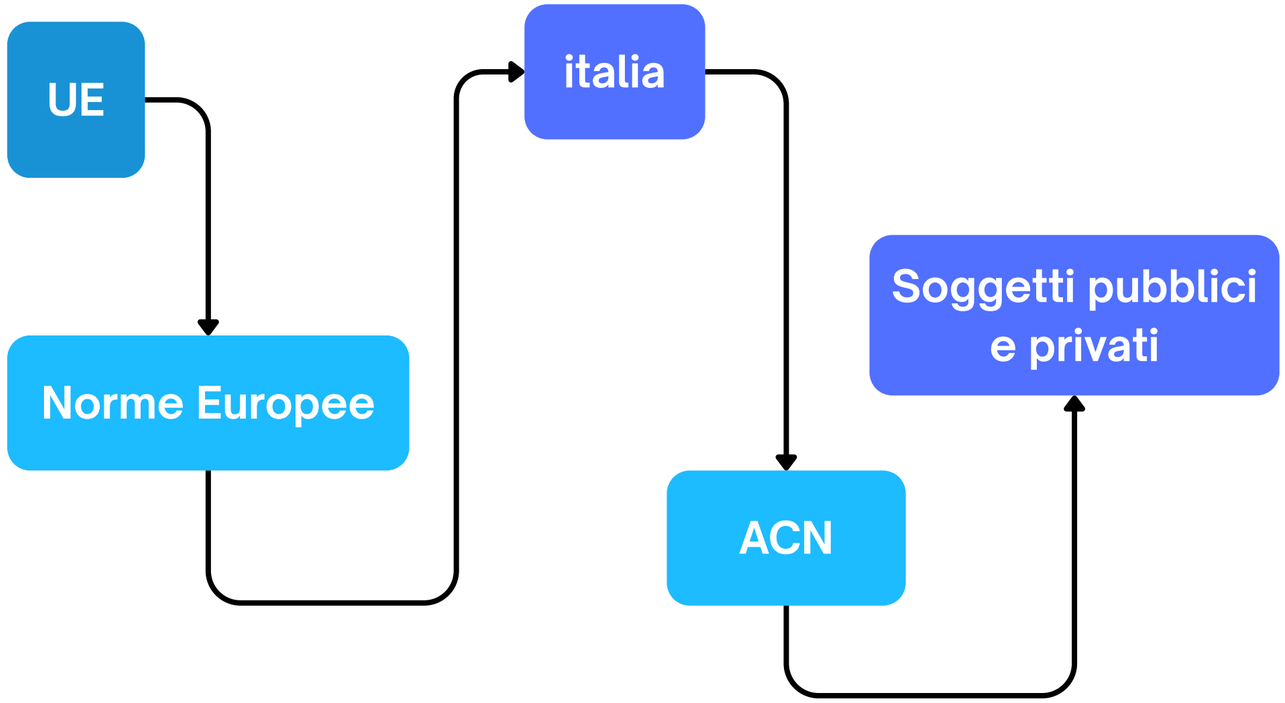
- una **governance chiara**,
- misure **adeguate**,
- **ruoli definiti**,
- **processi** di gestione del rischio,
- **capacità operative** per prevenire, gestire e documentare gli incidenti cyber.

IL CONTESTO ITALIANO

In Italia la cybersecurity è diventata una **priorità nazionale.** La crescita degli incidenti, la digitalizzazione dei servizi pubblici e privati, la dipendenza da fornitori ICT e la protezione delle infrastrutture strategiche hanno portato a un rafforzamento del sistema nazionale di cybersicurezza.

In questo percorso assumono un ruolo centrale:

- **Agenzia per la Cybersicurezza Nazionale**, come autorità di riferimento;
- la **Strategia Nazionale di Cybersicurezza**;
- il recepimento della **Direttiva NIS2** con il D.Lgs. 138/2024;
- il Perimetro di **Sicurezza Nazionale Cibernetica**;
- la **Legge 90/2024** per il rafforzamento della cybersicurezza nazionale;
- gli obblighi di gestione, notifica, vigilanza e responsabilizzazione dei soggetti coinvolti.



GDPR
Regolamento (UE) 2016/679
Regolamento generale sulla protezione dei dati

CYBERSECURITY ACT
Regolamento (UE) 2019/881
Quadro di certificazione della cybersicurezza per prodotti, servizi e processi ICT

DORA
Regolamento (UE) 2022/2554
Resilienza operativa digitale per il settore finanziario

CER
Direttiva (UE) 2022/2557
Resilienza delle entità critiche (recepita con D.Lgs 134/2024)

CYBER RESILIENCE ACT
Regolamento (UE) 2024/2847
Requisiti orizzontali di cybersicurezza per i prodotti con elementi digitali

NIS
Direttiva (UE) 2016/1148
Misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione

PSNC
D.L. 21 settembre 2019, n. 105
Disposizioni urgenti per il perimetro di sicurezza nazionale cibernetica

NIS2
Direttiva (UE) 2022/2555
Misure per un livello comune elevato di cybersicurezza nell'Unione (recepita con D.Lgs 138/2024)

LEGGE 28/06/2024
n. 90
Disposizioni per il rafforzamento della cybersicurezza nazionale e per il contrasto ai reati informatici nella PA

Legenda:
- Normativa vigente
- Situazione attuale
- Normativa abrogata

L'EVOLUZIONE DELLE NORMATIVE

LE NORME NEL DETTAGLIO

CER – Direttiva UE 2022/2557

È dedicata alla **resilienza** delle **entità critiche**. Mira a garantire la **continuità dei servizi essenziali**, non solo rispetto ai rischi cyber, ma anche rispetto a eventi fisici, organizzativi e sistemici che possono comprometterne il funzionamento.

DORA – Regolamento UE 2022/2554

Riguarda la **resilienza operativa digitale** del **settore finanziario**. Impone presidi specifici su gestione del rischio ICT, incidenti, test di resilienza, continuità operativa e controllo dei fornitori tecnologici critici.

Legge 90/2024

Rafforza la **cybersicurezza nazionale** e introduce **misure** per il **contrasto** ai **reati informatici**, con particolare attenzione alla **Pubblica Amministrazione** e alla capacità dello Stato di prevenire, gestire e rispondere alle minacce cyber

D.Lgs. 231/2001 – art. 24-bis

Rileva ai fini della **responsabilità amministrativa degli enti** per **reati informatici e trattamento illecito di dati.** Collega la cybersecurity anche al sistema di controllo interno, ai presidi organizzativi e al Modello 231, ove adottato.

GDPR – Regolamento UE 2016/679

Disciplina la protezione dei dati personali e impone alle organizzazioni di adottare misure tecniche e organizzative adeguate per **garantire riservatezza, integrità e disponibilità dei dati**. È centrale in caso di data breach, obblighi di notifica, accountability e tutela degli interessati.

Cybersecurity Act – Regolamento UE 2019/881

Introduce un **quadro europeo di certificazione della cybersicurezza** per prodotti, servizi e processi ICT. Rafforza il principio secondo cui la sicurezza deve essere considerata anche nella progettazione, valutazione e certificazione delle soluzioni digitali.

PSNC – Perimetro di Sicurezza Nazionale Cibernetica

Tutela reti, sistemi e servizi informatici rilevanti per la sicurezza nazionale. È rivolto ai soggetti che gestiscono funzioni essenziali o servizi strategici per il Paese.

Direttiva NIS – Direttiva UE 2016/1148

Ha introdotto il **primo quadro europeo** per la **sicurezza delle reti e dei sistemi informativi**, rivolto agli operatori di servizi essenziali e ai fornitori di servizi digitali. Oggi è stata superata dalla NIS2, che ne amplia il perimetro e rafforza gli obblighi.

Cyber Resilience Act – Regolamento UE 2024/2847

Introduce **requisiti orizzontali di cybersicurezza** per i **prodotti con elementi digitali.** Sposta l'attenzione anche sui produttori, imponendo requisiti di sicurezza lungo il ciclo di vita del prodotto.

NIS2: AMBITO E APPLICABILITÀ

La Direttiva NIS2 mira a garantire un **livello comune elevato di cybersicurezza** nell'Unione europea, rafforzando gli obblighi per le organizzazioni che operano in settori critici o che erogano servizi rilevanti per il sistema economico e sociale. La cybersecurity non è più soltanto un tema tecnico, ma un **sistema di governance, gestione del rischio, continuità operativa, gestione degli incidenti e responsabilità aziendale.**

In Italia, la **NIS2 è stata recepita dal D.Lgs. 138/2024,** che disciplina gli obblighi applicabili ai soggetti essenziali e ai soggetti importanti, individuati in base al settore di attività, alla dimensione e alla criticità del servizio svolto.

Tra **i principali adempimenti** rientrano:

- la registrazione e l'aggiornamento sulla piattaforma ACN,
- l'adozione di misure di gestione del rischio,
- la sicurezza della supply chain,
- la notifica degli incidenti,
- la formazione e il coinvolgimento degli organi amministrativi e direttivi.

Rientrano nel **perimetro** NIS2, a determinate condizioni: **Localizzazione(UE), Dimensione e Settore**, tra cui energia, trasporti, finanziario, infrastrutture digitali,pubblica amministrazione, sanità, acqua, servizi TIC, manifatturiero, alimentare, chimico, gestione dei rifiuti, fornitori di servizi digitali e ricerca.

NIS2: REQUISITI

GESTIONE DEI RISCHI

- **Analisi** dei rischi
- **Sicurezza** dei sistemi **informatici**, compresi controlli specifici: **Backup, MFA, crittografia**...
- Sicurezza delle risorse umane

CONTINUITÀ OPERATIVA

- Gestione della **continuità operativa**
- Business **impact** analysis
- **Gestione** delle crisi

GESTIONE DEGLI INCIDENTI

- **Gestione** e segnalazione degli **incidenti**

SICUREZZA DELLA CATENA DI FORITURA

- **Sicurezza** della **catena** di **fornitura**
- **Sicurezza** dei **rapporti** tra **ciascun soggetto** e i suoi diretti fornitori o fornitori di servizi

GOVERNANCE

- **Modello organizzativo** per la gestione della cybersecurity
- **Responsabilità degli organi** di amministrazione e organi direttivi

NIS2: BENEFICI

La conformità alla Direttiva NIS2 è un obbligo normativo, ma gli investimenti necessari per l'adeguamento possono essere valorizzati anche per migliorare la sicurezza e la resilienza aziendale.

1. Maggiore **sicurezza e resilienza** dell'**infrastruttura** dell'**organizzazione**
2. **Conformità e allineamento** con standard internazionali
3. Migliore **gestione del rischio**
4. **Resilienza** della **supply chain**
5. Migliore **preparazione** agli **incidenti** e **capacità** di **risposta**
6. Aumento **della trasparenza** e del **reporting interno**
7. **Minimizzazione** delle **sanzioni** e dei **rischi legali**
8. **Miglioramento** della **fiducia** di clienti, partner e stakeholder e della **reputazione aziendale**

IL RUOLO DELL'ACN NEL SISTEMA NAZIONALE DI CYBERSICUREZZA

L'Agenzia per la Cybersicurezza Nazionale – ACN è l'autorità centrale del sistema italiano di cybersicurezza. È stata istituita per tutelare gli interessi nazionali nel cyberspazio e per rafforzare la sicurezza dello sviluppo digitale del Paese.

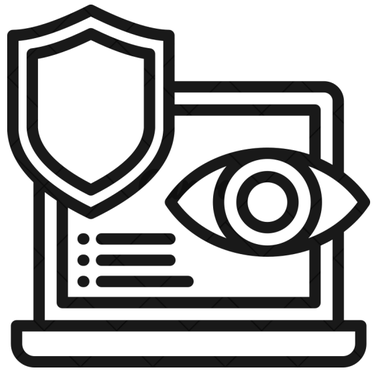
Nel quadro normativo attuale, l'ACN svolge un ruolo di **indirizzo, coordinamento, prevenzione e vigilanza**, supportando il **rafforzamento** della **resilienza cyber** di soggetti pubblici e privati. L'Agenzia opera anche in raccordo con il quadro europeo e con **CSIRT Italia**, soprattutto per la gestione e la comunicazione degli incidenti informatici rilevanti.

Le principali funzioni dell'ACN possono essere ricondotte a:

- **indirizzo** e coordinamento nazionale;
- **supporto** alla resilienza cyber del Paese;
- **gestione** di piattaforme e flussi informativi;
- **vigilanza** sui soggetti coinvolti;
- **raccordo** con CSIRT Italia;
- **emanazione** di linee guida, determinazioni e indicazioni operative.

VIGILANZA, LINEE GUIDA E SOFT LAW ACN

L’ACN non ha soltanto un ruolo istituzionale generale, ma **può esercitare poteri di vigilanza e indirizzo** nei confronti dei soggetti essenziali e importanti, al fine di verificare l’effettiva attuazione degli obblighi previsti dalla normativa.



Gli atti della soft law dell’ACN contribuiscono a definire concretamente modalità di accesso alle piattaforme, obblighi di base, gestione degli incidenti, ruoli operativi, termini di adeguamento e indicazioni per dirigenti, dipendenti e fornitori IT.

Poteri di vigilanza

- informazioni
- audit
- verifiche
- ispezioni
- raccomandazioni.

Soft law ACN

- determinazioni
- linee guida
- specifiche operative
- indicazioni applicative

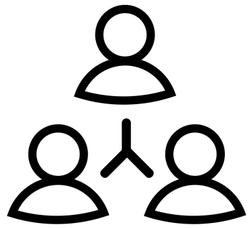
CYBERSECURITY E RESPONSABILITÀ DEGLI ORGANI AMMINISTRATIVI

Le normative più recenti richiedono un **coinvolgimento diretto degli organi di amministrazione e del management** nella definizione, approvazione e supervisione delle misure di sicurezza.

Gli organi amministrativi e direttivi devono assicurare che l'organizzazione disponga di un **modello adeguato** per la **gestione del rischio cyber,** approvando le **strategie di sicurezza**, **verificando** l'attuazione degli **obblighi** e **ricevendo informazioni** tempestive sugli incidenti rilevanti.

Le principali responsabilità riguardano:

- **approvazione** delle **misure** di gestione del rischio cyber;
- **supervisione** dell'attuazione degli obblighi;
- definizione di ruoli e **responsabilità** interne;
- allocazione di **risorse adeguate**;
- **monitoraggio** della compliance;
- promozione della **formazione**;
- **informazione periodica** sugli incidenti;
- **accountability** in caso di inosservanza.



DAL VERTICE AZIENDALE AI RUOLI OPERATIVI

In sistema di cybersecurity efficace richiede una **chiara distribuzione delle responsabilità** tra organi di vertice, funzioni aziendali e soggetti tecnici.

Il rischio cyber, infatti, coinvolge dati, processi, fornitori, persone, **continuità operativa**, comunicazioni e responsabilità normative.

Per questo motivo non può essere gestito in modo isolato dalla sola funzione IT, ma deve essere **coordinato attraverso un modello interfunzionale.**

I principali ruoli coinvolti sono:

- organi di amministrazione e direzione;
- direzione generale;
- funzione IT / ICT;
- responsabile cybersecurity;
- DPO / privacy;
- legal e compliance;
- risk management;
- HR;
- procurement;
- comunicazione;
- organi di controllo;
- eventuale OdV 231;
- fornitori ICT e partner tecnologici.

GESTIONE DEGLI INCIDENTI:
UN TEMA AZIENDALE

Un attacco può generare **impatti su sistemi**, dati, clienti, fornitori, obblighi di notifica, comunicazioni esterne e **continuità operativa**.

Per questo motivo, la **risposta all'incidente** deve essere **preparata prima che l'evento si verifichi**, attraverso ruoli chiari, procedure formalizzate, flussi di escalation, template di comunicazione e attività di simulazione.

Un processo efficace deve prevedere:

- preparazione **preventiva**;
- **rilevazione** e classificazione dell'incidente;
- **escalation** interna;
- **gestione** tecnica;
- gestione **legale, privacy e comunicativa**;
- eventuale **notifica alle autorità** competenti;
- **relazione finale**;
- **follow-up**.

In ambito **NIS2**, la gestione degli incidenti assume particolare rilievo anche per gli obblighi di comunicazione allo CSIRT Italia.

QUADRO SANZIONATORIO:
NON SOLO MULTE

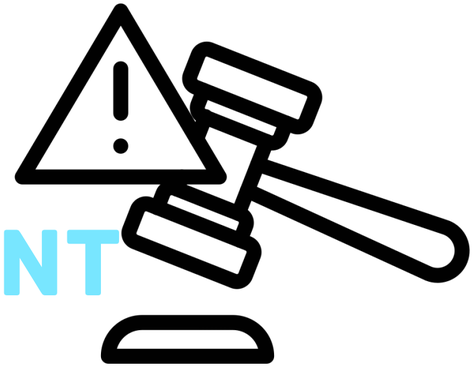
Il **mancato adeguamento** alle normative cyber può generare conseguenze diverse, non limitate alle sole sanzioni pecuniarie. Le **multe** rappresentano solo una parte del rischio complessivo.

Un'organizzazione non adeguata può infatti trovarsi esposta a **prescrizioni, misure correttive, richieste di informazioni, verifiche, responsabilità degli organi di gestione, difficoltà nella gestione degli incidenti e perdita di fiducia** da parte di clienti, partner e stakeholder.

Le principali conseguenze possono riguardare:

- sanzioni amministrative **pecuniarie**;
- prescrizioni e **misure correttive**;
- **richieste di adeguamento** da parte dell'autorità;
- **responsabilità** degli organi di gestione;
- **danni reputazionali**;
- **impatti** operativi;
- **perdita di fiducia** del mercato;
- **effetti su contratti,** clienti, partner e supply chain.

SANZIONI NIS2 E RESPONSABILITÀ DEL MANAGEMENT



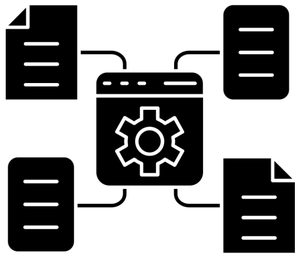
Il D.Lgs. 138/2024 prevede un sistema sanzionatorio differenziato per soggetti essenziali e soggetti importanti, con **conseguenze** che possono riguardare sia **l'organizzazione** sia, in determinati casi, i **soggetti** con ruoli direttivi o rappresentativi.

Per i **soggetti essenziali,** le sanzioni possono arrivare fino a 10 milioni di euro o fino al 2% del fatturato mondiale annuo totale.

Per i **soggetti importanti**, le sanzioni possono arrivare fino a 7 milioni di euro o fino all'1,4% del fatturato mondiale annuo totale.

Le inosservanze possono riguardare, tra l'altro:

- **violazioni rilevanti** delle disposizioni normative;
- **mancata registrazione** o mancato aggiornamento sulla piattaforma ACN;
- **inadempimento** a diffide;
- **mancato rispetto degli obblighi** da parte degli organi dirigenti;
- **possibile incapacità** a svolgere funzioni dirigenziali nei casi previsti.



VERSO UN MODELLO STRUTTURATO DI ADEGUAMENTO

Di fronte a un quadro normativo sempre più articolato, le organizzazioni hanno bisogno di un **approccio strutturato**, capace di c**ollegare obblighi, rischi, processi, ruoli, controlli ed evidenze documentali**.

L'adeguamento alla cybersecurity non può essere gestito come un intervento isolato o puramente tecnico, ma deve diventare un **percorso continuo di governance, compliance, risk management e miglioramento progressivo.**

Un percorso efficace dovrebbe prevedere:

- **verifica** dell'applicabilità normativa;
- **mappatura** di **processi**, asset, dati e fornitori;
- **cyber risk assessment;**
- **gap analysis** rispetto agli obblighi applicabili;
- **definizione** di **ruoli** e responsabilità;
- predisposizione di **policy e procedure**;
- **formazione** di organi direttivi e personale;
- **monitoraggio** delle azioni di adeguamento;
- raccolta di evidenze;
- aggiornamento continuo del sistema

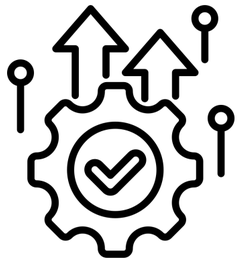
IL MODELLO ORGANIZZATIVO COMPLIWARE

La crescente complessità normativa in materia di cybersecurity richiede alle aziende un **approccio strutturato**, capace di trasformare gli obblighi previsti da NIS2, D.Lgs. 138/2024, GDPR, D.Lgs. 231/2001 e dalle altre normative applicabili in **processi aziendali concreti, responsabilità definite, procedure aggiornate e controlli effettivi.**

CompliWare supporta le organizzazioni nella costruzione di un **modello organizzativo cyber integrato con governance, compliance, risk management, privacy e Modello 231.**

L'obiettivo è rendere l'adeguamento non solo formale, ma realmente efficace nella gestione del rischio cyber.

IL MODELLO OFFERTO DA COMPLIWARE SI FONDA SU



1 ANALISI DEL CONTESTO AZIENDALE E DEI PROCESSI DIGITALI

2 VERIFICA DELLE NORMATIVE APPLICABILI

3 INDIVIDUAZIONE DI RUOLI, RESPONSABILITÀ E FLUSSI DECISIONALI

4 MAPPATURA DI ASSET, DATI, SISTEMI, FORNITORI E PROCESSI CRITICI

5 VALUTAZIONE DEL RISCHIO CYBER

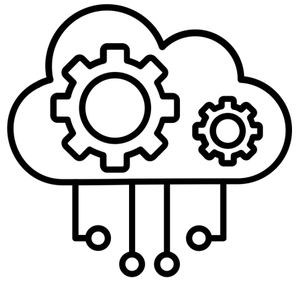
6 DEFINIZIONE DI POLICY, PROCEDURE E CONTROLLI

7 FORMAZIONE DEGLI ORGANI DIRETTIVI E DELLE FUNZIONI AZIENDALI

8 MONITORAGGIO CONTINUO DELLE AZIONI DI ADEGUAMENTO

9 RACCOLTA DI EVIDENZE DOCUMENTALI

10 AGGIORNAMENTO PERIODICO DEL SISTEMA



DCF IL SOFTWARE COMPLIWARE: RENDERE SEMPLICE, EFFICACE ED EFFETTIVA LA COMPLIANCE CYBER

Il software CompliWare consente di rendere la **cybersecurity compliance più semplice, tracciabile ed effettiva,** trasformando gli obblighi normativi in attività operative assegnate, monitorate e documentate.

Attraverso la piattaforma, l'organizzazione può gestire in modo ordinato:

- le **attività di adeguamento**,
- i **remediation plan**,
- le **procedure e le policy**,
- i **documenti organizzativi**,
- le **scadenze**, le **responsabilità,**
- lo **stato di avanzamento** delle azioni previste.

La piattaforma permette inoltre di **assegnare task alle funzioni coinvolte**, **raccogliere evidenze** documentali a supporto della compliance, **monitorare controlli periodici**, **audit e follow-up**, e **mantenere aggiornato il sistema** in caso di modifiche normative, organizzative o tecnologiche. In questo modo, gli obblighi cyber **non restano indicazioni astratte**, ma **vengono tradotti in attività concrete**, **tracciabili e verificabili**.

DCF IL SOFTWARE COMPLIWARE: DAL MODELLO ORGANIZZATIVO ALLA DIMOSTRAZIONE DELLA CONFORMITÀ

Il valore del software non è soltanto documentale: **CompliWare consente di rendere operativo il modello organizzativo**, **monitorando l'effettiva attuazione delle misure** e **collegando il rischio cyber ai processi** aziendali, ai presidi adottati e alle responsabilità assegnate.

Questo permette all'azienda di **rafforzare la propria capacità di mantenere** la **conformità normativa** nel tempo, **ridurre il rischio** di sanzioni e non conformità, **dimostrare l'adozione di misure adeguate** e **migliorare** la governance interna. La piattaforma favorisce inoltre il **coordinamento tra funzioni, responsabili e organi di controllo, integrando cybersecurity, privacy, compliance, risk management** e Modello 231 in un unico percorso strutturato.

In caso di audit, verifiche o contestazioni, l'organizzazione può così **dimostrare** non solo di aver previsto **misure di sicurezza**, ma anche di averle **attuate**, **monitorate** e **documentate** nel tempo.

“CON COMPLIWARE, LA CYBERSECURITY DIVENTA UN SISTEMA CONCRETO, GOVERNABILE E DOCUMENTABILE DI COMPLIANCE, CONTROLLO E RESILIENZA AZIENDALE.”

CompliWare
Digital Facilities for Audit Risk Compliance