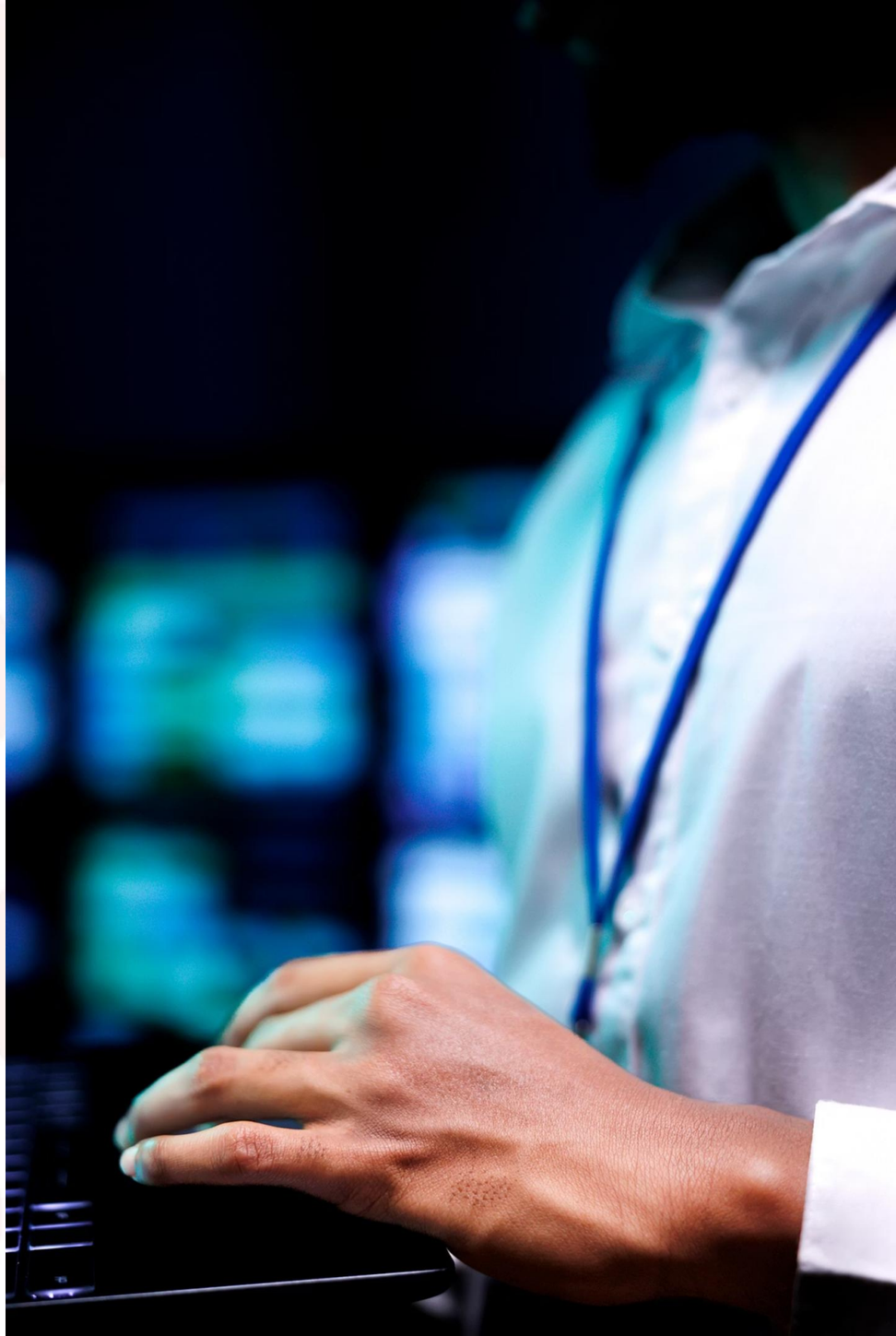
SICUREZZA DELLE INFORMAZIONI

CONTROLLO DEI RISCHI

CISO as a Service: la Sicurezza Strategica per l'Era Digitale

La soluzione su misura per **mettere in sicurezza le informazioni** della tua organizzazione, garantire la conformità NIS2 (D.Lgs. 138/2024), aumentarne la Resilienza e assicurare la Continuità Operativa.



POLO TECNOLOGICO ALTO ADRIATICO Andrea Galvani

Chi è il CISO?

Definizione

Il **CISO** (Chief Information Security Officer) è una competenza specialistica focalizzata sulla **Sicurezza delle Informazioni** e sul **Controllo dei Rischi** dell'organizzazione per cui opera.

Il suo ruolo

Il CISO guida la strategia di sicurezza aziendale, coordina le funzioni operative e IT, e fornisce alla Dirigenza gli strumenti per governare la sicurezza delle informazioni. È consulente strategico e operativo, promotore della cultura della sicurezza e garante della conformità alla Direttiva NIS2 — incluse le responsabilità personali degli organi di vertice (Art. 20 NIS2).

Di cosa si occupa il CISO

Portano la **cultura della sicurezza nell'operatività quotidiana**. Le loro attività coprono l'intero perimetro della sicurezza aziendale, dalla valutazione dei rischi alla formazione del personale.

Analisi dei Rischi

Analisi dei rischi degli asset aziendali tramite Risk Register e Business Impact Analysis (BIA) per identificare vulnerabilità, misurare l’impatto sui processi critici e definire le priorità di intervento in conformità NIS2.

Security Policy

Definizione di regolamenti di sicurezza e procedure operative per una gestione coerente e strutturata delle informazioni.

Formazione

Formazione del personale sulla corretta gestione delle informazioni e degli strumenti informatici aziendali.

Guida al Rischio

Guida dell’azienda nel contenimento dei rischi attraverso azioni mirate e sostenibili, con presidio continuo della conformità normativa e aggiornamento periodico del profilo di rischio.

POLO TECNOLOGICO ALTO ADRIATICO Andrea Galvani

Altre Attività del CISO

Coordinamento IT

Lavora in stretto coordinamento con l'IT e le funzioni operative per aumentare la **Resilienza aziendale**, garantendo che tecnologie e processi siano allineati agli obiettivi di sicurezza.

Programma di Interventi

Definizione e gestione del **Programma di Interventi** sul Sistema di Sicurezza delle Informazioni, con pianificazione delle priorità e monitoraggio dei progressi nel tempo.

Gestione degli Incidenti

Supporto attivo nella gestione di **incidenti di sicurezza e data breach tramite il SIRT aziendale**, con procedure di risposta rapida per minimizzare l'impatto operativo e garantire le notifiche obbligatorie all'ACN nei tempi previsti dalla Direttiva NIS2.

Cos'è il CISO? as a Service?

Il **CISO** è a disposizione dell'organizzazione nella misura delle sue **effettive esigenze**.
Non sostituisce le risorse interne, ma le potenzia con una competenza specialistica altamente qualificata.

Opera come consulente operativo e strategico, in stretto coordinamento con l'IT e le funzioni operative, con un obiettivo chiaro: aumentare la Resilienza, garantire la conformità NIS2 e assicurare la Continuità Operativa dell'organizzazione.

Perché "as a Service"?

Perché si adatta alle reali dimensioni e necessità dell'azienda: nessun costo fisso di una figura full-time, ma tutta la competenza di un CISO senior disponibile quando serve.

Cosa porta il CISOaaS in azienda

Conoscenze e Leadership

Porta nell'organizzazione le conoscenze specialistiche e la leadership necessaria in materia di Sicurezza delle Informazioni, colmando il gap di competenze interne.

Coordinamento Operativo

Opera in stretto coordinamento con l'IT e le funzioni operative per aumentare la Resilienza aziendale e assicurare la Continuità Operativa anche in scenari di crisi.

Supporto alla Dirigenza

Fornisce alla Dirigenza gli elementi per governare la Sicurezza delle Informazioni a livello strategico e adempiere alle responsabilità previste dall'Art. 20 NIS2, che coinvolge direttamente CdA e CEO nella governance della sicurezza.

POLO TECNOLOGICO ALTO ADRIATICO Andrea Galvani

A chi si rivolge il CISOaaS

Il servizio è pensato per **PMI**, di qualunque settore o mercato, soggette agli obblighi della Direttiva NIS2 (D.Lgs. 138/2024) o che riconoscono l'importanza di presidiare la sicurezza delle informazioni in modo strutturato.

- Sono consapevoli di operare in uno scenario di **rapida evoluzione tecnologica** e di minacce informatiche in continuo aumento.
- Vogliono **prepararsi per tempo** e garantire la conformità NIS2: Assessment Cybersecurity, Risk Register, BIA e piano strutturato di gestione degli incidenti.
- Hanno **limiti in termini di competenze interne** o non hanno le dimensioni strutturali per dotarsi di un CISO full-time in autonomia.

Il vantaggio chiave

Spesso solo le organizzazioni più strutturate sono adeguatamente attrezzate. Il CISOaaS consente anche alle realtà meno strutturate di aumentare la propria Resilienza, raggiungere la conformità NIS2 e affrontare le ispezioni ACN — previste a partire da fine 2026.

Un dubbio frequente

> "La nostra azienda è piccola. Non siamo un obiettivo per gli hackers..."

Oggi gli attacchi informatici **colpiscono dove trovano vulnerabilità**: chiunque è un potenziale bersaglio. Con la Direttiva NIS2 (D.Lgs. 138/2024), le aziende soggette rischiano sanzioni fino a € 7.000.000 — o l'1,4% del fatturato mondiale — e la responsabilità personale di CdA e CEO (Art. 20 NIS2). Le ispezioni ACN sono attese a partire da fine 2026.

⚠ Le PMI soggette a NIS2 sono spesso i soggetti meno preparati: obblighi stringenti, stesse vulnerabilità. Non aspettare un incidente o un'ispezione ACN per agire.

POLO TECNOLOGICO ALTO ADRIATICO Andrea Galvani

Le 4 Fasi del Servizio CISO as a Service

L'obiettivo del servizio è **"mettere in sicurezza"** l'organizzazione, promuovendo un processo di trasformazione che richiede il coinvolgimento attivo di tutte le parti interessate, in particolare della **Dirigenza**.

1

1 — Stimare

Valutare la postura di sicurezza con un Assessment Cybersecurity: analisi del contesto, degli asset critici e dei gap di conformità NIS2 dell'organizzazione.

2

2 — Progettare

Progettare il Programma di Sicurezza su misura: Risk Register, Business Impact Analysis (BIA), roadmap di conformità NIS2 e piano di gestione degli incidenti.

3

3 — Implementare

Implementare il Programma coordinando persone, processi e tecnologie: Security Policy, SIRT aziendale, procedure di notifica ACN e misure di protezione degli asset critici.

4

4 — Verificare

Verificare i risultati e far evolvere nel tempo il Programma di Sicurezza, adattandolo ai cambiamenti del contesto e delle minacce.

POLO TECNOLOGICO ALTO ADRIATICO Andrea Galvani

La Sicurezza delle Informazioni non si acquista sul mercato

La sicurezza è il risultato di **processi che comprendono persone, competenze, comportamenti, strumenti e servizi**. Non è un prodotto da acquistare, ma un percorso da intraprendere con metodo, tempo e guida qualificata.

Il CISO as a Service è la risposta concreta per le organizzazioni che vogliono intraprendere questo percorso con una guida esperta, flessibile e su misura — senza rinunciare a competenze di livello enterprise.

Pronto a iniziare? Contattaci per il tuo Assessment Cybersecurity e scopri il tuo reale livello di sicurezza e conformità NIS2.

Contattaci

Marco Giacomini
B.U. Manager Cyber Polo Tecnologico Alto Adriatico
marco.giacomini@poloaa.it

Paolo Alberghetti
paolo.alberghetti@poloaa.it

POLO TECNOLOGICO ALTO ADRIATICO Andrea Galvani