Rischi Cyber e Resilienza

Percorso Formativo NIS2

Modalità di Fruizione:
Modulo 1: on line asincrono
Modulo 2: aula virtuale o frontale
Modulo 3: aula virtuale o frontale
Rivolto a:
Modulo 1: corso base per tutti i dipendenti
Modulo 2: corso avanzato esperti sicurezza, sistemi IT, responsabili di servizi, referenti privacy
Modulo 3**:** corso per dirigenti e figure apicali
Test di valutazione: previsto per il corso online asincrono

Descrizione del percorso

La NIS2 (Network and Information Security 2) è la nuova direttiva europea, che aggiorna e sostituisce la precedente Direttiva NIS (2016/1148) sulla sicurezza delle reti e dei sistemi informativi. È stata introdotta per rafforzare ulteriormente la cybersicurezza all'interno dell'Unione Europea, adattandosi ai nuovi rischi e alle sfide poste dall'evoluzione tecnologica e dagli attacchi informatici sempre più complessi.

Per l'Italia la Direttiva è stata recepita attraverso il **Decreto Legislativo 4 settembre 2024, n. 138**, pubblicato nella Gazzetta Ufficiale il 1° ottobre 2024.

Il percorso offre una panoramica sugli elementi principali di una strategia di Cybersicurezza e approfondisce la Direttiva NIS2, permettendo di comprendere i nuovi obblighi normativi introdotti dalla direttiva europea, inclusa l'estensione degli ambiti di applicazione, i soggetti in perimetro e le varie fasi di adeguamento necessarie.

Obiettivi del Percorso:

- Comprendere l'importanza di adottare una strategia basata sull'analisi dei rischi e l'adozione di misure Cyber
- Comprendere il contesto , motivazioni e obblighi alla base della Direttiva NIS2.

- Identificare e gestire le responsabilità di governance e supervisione legate alla sicurezza delle reti e dei sistemi informativi.
- Sviluppare strategie per l'implementazione di misure tecniche e organizzative adeguate per la gestione del rischio cyber.
- Approfondire le procedure di segnalazione degli incidenti e le responsabilità degli operatori di servizi essenziali e delle infrastrutture critiche.
- Valutare gli aspetti sanzionatori previsti dalla Direttiva.

Il percorso sarà diviso in tre moduli: base, avanzato e figure apicali per fornire un supporto efficacie, per l'intera organizzazione, nel percorso di adozione della NIS2.

MODULO 1

Questo modulo, della durata di 2 ore, fornisce una panoramica della Direttiva NIS2. Verranno discussi gli obiettivi della direttiva, il suo ambito di applicazione e le implicazioni per le organizzazioni; i partecipanti saranno accompagnati ad un'introduzione alla Direttiva che permetterà un avvicinamento al nuovo approccio di rafforzamento della cybersicurezza attraverso l'incremento della consapevolezza rispetto alle tematiche dei rischi e della resilienza cyber.

I contenuti formativi del corso sono orientati a:

- Fornire una panoramica generale della Direttiva NIS2 e del suo recepimento in Italia.
- Sensibilizzare i dipendenti sull'importanza della cybersecurity nella PA.
- Illustrare le buone pratiche per proteggere dati e sistemi IT da minacce informatiche.
- Riconoscere e gestire potenziali minacce o incidenti.

DESTINATARI

Tutti i dipendenti

TEMPISTICHE

Disponibile nel secondo semestre 2025

MODALITA' DI EROGAZIONE

Corso Fad (asincrono)

MODULO 2

Il modulo 2, di livello avanzato, della durata 8 ore sulla base delle esigenze di approfondimento dell'Ente, si focalizzano sulle tematiche della NIS2 con un approccio sulla gestione del rischio di Cybersecurity, obblighi e segnalazioni e controllo di conformità delle verifiche effettuate.

I contenuti formativi del modulo sono finalizzati a:

- Comprendere i requisiti della Direttiva NIS2 e il relativo recepimento normativo in Italia.
- Analizzare le responsabilità operative in ambito tecnico e le misure da adottare per la gestione della sicurezza informatica.
- Approfondire le tecniche di monitoraggio, gestione delle vulnerabilità, sicurezza della supply chain e risposta agli incidenti.
- Sviluppare un piano tecnico per garantire la resilienza dei sistemi IT in conformità alla normativa.

Prima sessione (4 ore)

- NIS2

Seconda sessione (4 ore)

- Gestione del Rischio (1 ora)
- Business Continuity (1 ora)
- Gestione degli incidenti (1 ora)
- Piano di sicurezza da proporre (1 ora). Una sorta di vademecum per iniziare a far capire all'ente in che stato si trova rispetto alla NIS2, una sorta di compito da fare in autonomia a casa propria)

DESTINATARI

Esperti sicurezza, responsabili di sistemi IT, responsabili di servizi, referenti privacy

TEMPISTICHE

Disponibile dal secondo trimestre 2025 (aprile '25)

MODALITA' DI EROGAZIONE

Aula fisica (max 20 partecipanti)

(presso Ente o presso la sede di CSI Piemonte)

MODULO 3

Il modulo, della durata di 4 ore, è progettato per dirigenti, funzionari e figure apicali (organi direttivi e amministrativi) della Pubblica Amministrazione, CISO e DPO, con l'obiettivo di fornire una comprensione di base delle tematiche Cyber e della Direttiva NIS2 (Network and Information Security) e dei suoi impatti operativi, normativi e strategici.

A) Conoscenze manageriali di base: Inquadramento del rischio Cyber, minacce e vulnerabilità

1. Il contesto odierno: Cyberspazio e Cybersecurity
2. La direttiva NIS 2: Figure chiave e responsabilità degli organi Direttivi
3. Le Competenze degli organi Direttivi

3a - l'evoluzione del rischio Cyber

Qualche dato (il rapporto CLUSIT).
I problemi ed i rischi nelle aziende e negli Enti Pubblici
Quanto può costare alla mia azienda/Ente un attacco informatico

3b Vulnerabilità e tecniche di attacco

Le principali vulnerabilità delle infrastrutture IT
Gli attacchi interni ed esterni
Misure tecniche ed organizzative

3c Il fattore umano

L'errore umano come prima causa (fattore abilitante) di attacco Cyber
Social Engineering: mezzo di attacco sempre più usato
Gli attacchi attraverso la posta elettronica e cellulare: phishing/smishing
I deepfake ed attacchi con l'IA
Gli attacchi al CEO

B) Competenze decisionali del manager: il "Cosa" chiedere ed il "Come" attuare"

1. Cosa significa "Fare Sicurezza": impostare un Sistema Difensivo

Le 3 Fasi Temporali: Prevenzione, Rilevamento, Reazione
L'impostazione del MOGS (modello Organizzativo di gestione della Sicurezza ICT)
La gestione del piano di rischi aziendali (metodologia e azioni)
Il monitoraggio delle attività: l'interazione degli organi direttivi con il CISO, il DPO, il responsabile Formazione, Ufficio Legale/contratti, il fornitore IT

2. Applicazione della NIS 2 in pratica (le azioni di valutazione degli Organi Direttivi)

La security by design: cosa significa e cosa comporta.
L'impianto documentale da mantenere : il governo dei processi e regolamenti, elenchi, mappature
La Data Protection: perché non solo la Cybersecurity
Il piano formativo Cyber per i dipendenti.
La gestione degli incidenti : obblighi di notifica e azioni da attivare

DESTINATARI

Il corso è un modulo base rivolto a dirigenti, funzionari e figure apicali della Pubblica Amministrazione, CISO, DPO. In base anche alle determinazioni di ACN, potranno seguire ulteriori moduli di approfondimento.

TEMPISTICHE

Disponibile febbraio 2025

MODALITA' DI EROGAZIONE

Aula virtuale (max 20 partecipanti)

Aula fisica (max 20 partecipanti)

(presso Ente o presso la sede di CSI Piemonte)