

DIRETTIVA NIS2: PRATICHE DI SICUREZZA DIGITALE E FORMAZIONE IN CYBERSECURITY

La Direttiva NIS2 (Direttiva (UE) 2022/2555 sulla Sicurezza delle Reti e dell'Informazione) è entrata in vigore nell'UE il 17 ottobre 2024, imponendo nuovi obblighi per rafforzare la cybersecurity nelle organizzazioni. Tra questi, l'esecuzione di audit regolari, la segnalazione tempestiva degli incidenti e l'adozione di misure adeguate per prevenire le minacce informatiche, come stabilito nell'articolo 21, comma 2, lettera g) della Direttiva, che richiede alle organizzazioni di garantire che i dipendenti siano consapevoli dei rischi e adottino pratiche di igiene informatica.

Per rispettare la direttiva NIS2, è fondamentale garantire che il personale sia adeguatamente formato in materia di sicurezza informatica. La formazione non solo aiuta a soddisfare gli obblighi normativi, ma rappresenta anche un pilastro chiave per proteggere la tua organizzazione da attacchi e incidenti informatici.

1 - Sensibilizzazione e pratiche di sicurezza

1.1 Obblighi di sensibilizzazione

Le organizzazioni devono garantire che i dipendenti:

- Comprendano i rischi di cybersecurity.
- Conoscano l'importanza della sicurezza informatica.
- Adottino buone pratiche di sicurezza.

Esempi pratici:

- Programmi di formazione su workshop, webinar o e-learning.
- Comunicazione tramite e-mail, intranet o newsletter per aggiornamenti e consigli.

1.2 Contenuti del programma di sensibilizzazione

Il programma deve:

- Essere regolare e rivolto a tutto il personale, inclusi nuovi assunti e dirigenti.
- Seguire le politiche di sicurezza dell'organizzazione.
- Trattare pratiche chiave come:
 - Uso sicuro di password e autenticazione.
 - Protezione da phishing e attacchi sociali.
 - Sicurezza nelle connessioni e backup.
 - Gestione sicura di dispositivi mobili e telelavoro.

Esempi pratici:

- Formazione per riconoscere phishing, pre-texting e altre minacce.
- Consapevolezza sui rischi di dati esposti involontariamente (es. dispositivi persi o invii errati).
- Consigli su sicurezza delle reti domestiche per i lavoratori remoti.
- Distribuire materiali di formazione (dispense, e-mail, moduli online).

1.3 Valutazione e aggiornamento del programma di sensibilizzazione

Il programma deve essere:

- Testato per verificarne l'efficacia (es. quiz).
- Aggiornato annualmente o in base all'evoluzione delle minacce.

Esempi pratici:

- Quiz di verifica e moduli di feedback.
- Revisione regolare dei materiali formativi.

2 – Formazione sulla sicurezza

2.1 Identificazione dei ruoli e formazione sulla sicurezza

Le organizzazioni devono identificare i dipendenti i cui ruoli richiedono competenze in materia di sicurezza e garantire che ricevano una formazione continua sulla sicurezza delle reti e dei sistemi informativi.

- Identificare i ruoli che necessitano di competenze in materia di sicurezza.
- Offrire formazione mirata sui temi di sicurezza per i ruoli identificati.
- Considerare l'uso del Quadro europeo delle competenze in materia di sicurezza informatica (ECSF).

2.2 Programma di formazione per ruoli specifici

Sviluppare, attuare e applicare un programma di formazione conforme alle politiche di sicurezza delle reti e delle informazioni, che soddisfi le necessità di formazione per specifici ruoli e posizioni in base a criteri definiti.

- Fornire formazione sulla sicurezza delle reti e delle informazioni per ogni ruolo identificato.
- Offrire vari metodi di formazione, tra cui corsi online, workshop, laboratori pratici e simulazioni.
- Prevedere corsi, certificazioni o la partecipazione a conferenze/webinar sulla sicurezza.
- Esempi di corsi includono il Corso Cybersecurity Blue Team per professionisti IT, il Corso Web Application Security per sviluppatori e il Corso Cybersecurity Awareness per tutti i dipendenti aziendali.

2.3 Pertinenza e valutazione della formazione

La formazione deve essere pertinente al ruolo del dipendente e deve essere valutata per verificarne l'efficacia. Dovrebbe comprendere aspetti legati alle misure di sicurezza esistenti e ai seguenti temi:

- Istruzioni sulla configurazione sicura di reti e sistemi, inclusi dispositivi mobili.
- Conoscenza delle minacce informatiche.
- Comportamento da adottare in caso di eventi rilevanti per la sicurezza.

Esempi pratici:

- Formare il personale su autenticazione sicura, gestione delle password, identificazione delle minacce, conservazione e distruzione dei dati sensibili.
- Addestrare il personale a riconoscere potenziali incidenti, come allegati email sospetti e comportamenti strani nei sistemi.
- Fornire indicazioni su come segnalare tempestivamente gli eventi e segnalare software obsoleti o malfunzionamenti nei processi automatizzati.
- Mantenere aggiornamenti sulle minacce informatiche e verificare le conoscenze attraverso test e quiz.

2.4 Formazione per nuovi ruoli

Gli enti competenti devono fornire formazione ai dipendenti che passano a nuovi ruoli che richiedono competenze aggiuntive in sicurezza.

Esempi pratici:

- Verificare se un nuovo ruolo necessita di formazione aggiuntiva sulla sicurezza delle reti e delle informazioni.

2.5 Aggiornamento periodico del programma di formazione

Il programma di formazione deve essere aggiornato periodicamente, tenendo conto di nuove normative, minacce informatiche e sviluppi tecnologici.

Esempi pratici:

- Organizzare corsi di aggiornamento periodici sulla sicurezza informatica.
- Rivedere e aggiornare il programma almeno una volta all'anno.

Formazione Nexsys per la NIS2

Percorsi formativi su misura per ogni livello, tutti orientati allo stesso obiettivo: scegli il corso Nexsys più adatto alle tue esigenze.

User



Security Awareness per utenti
Phishing Awareness
Sicurezza informatica Liv. 2



Responsabile DPO
Risk Evaluation e BIA
Privacy e sicurezza informatica

Beginner



Cybersecurity Fundamentals

Intermediate



Cybersecurity Specialist

Advanced



Defense
Cybersecurity Blue Team



Attack
CEH Ethical Hacking



Integrato
Cybersecurity Purple Team

Specialist



Defense
Incident Responder
Ransomware Attack



Attack
Red Team: Attack and Defense
Penetration Test on Azure

CONTATTI

www.nexsys.it

+390452456669

info@nexsys.it