START4.YOU

FORMAZIONE
CYBERSECURITY

Servizi strategici per innovare. Insieme.

Formazione obbligatoria 138/24 (NIS2)

La Direttiva Europea NIS 2, recepita in Italia con il Decreto 138/24, introduce nuovi obblighi in materia di sicurezza informatica per le organizzazioni considerate strategiche o essenziali per il sistema Paese. Non si tratta solo di un adeguamento tecnico, ma di un vero cambio di paradigma nella gestione del rischio cyber, che coinvolge governance, processi e responsabilità del management.

Il servizio di **Formazione Obbligatoria 138/24 (NIS 2)** nasce per accompagnare le organizzazioni in un percorso strutturato di conformità normativa, consapevolezza e rafforzamento della cultura della sicurezza. Attraverso programmi mirati e aggiornati, supportiamo aziende e management nel comprendere responsabilità, rischi e misure operative richieste, trasformando un obbligo normativo in un vantaggio competitivo.

Destinatari dei servizi

- **C-Level**
  CEO, COO, CFO, CIO/CTO, General Counsel, HR Director, Procurement/Supply Chain, Comms/PR, Risk/Compliance/Internal Audit

- **Organi sociali e direzionali**
  Consiglio di Amministrazione, Collegio Sindacale, Alta Direzione

FORMAZIONE OBBLIGATORIA 138/24 (NIS2)

01 Programma di Formazione NIS2 per C-Level

Viene illustrato il ruolo strategico della cybersecurity, il passaggio alla cyberresilienza, l'ambito di applicazione della direttiva e il confronto con gli standard ISO 27001 e ISO 22301, per comprendere l'impatto normativo sull'organizzazione.

02 Programma di formazione NIS2 per Organi sociali e direzionali

Viene illustrato il ruolo strategico della cybersecurity, il passaggio dalla cybersecurity alla cyber resilience, e il quadro normativo con focus sul D.Lgs 138/2024 e la sua correlazione con gli standard ISO 27001:2022 e ISO 22301:2019. Il CdA acquisisce consapevolezza del contesto normativo e dell'impatto sull'organizzazione.

Per maggiori informazioni scrivi a **servizi@start4-0.it**

START4.YOU

Servizi strategici per innovare. Insieme.

01

1/3

Programma di Formazione NIS2 per C-Level

1 . **Introduzione alla Direttiva NIS2 e contesto normativo**

Viene illustrato il ruolo strategico della cybersecurity, il passaggio alla cyberresilienza, l'ambito di applicazione della direttiva e il confronto con gli standard ISO 27001 e ISO 22301, per comprendere l'impatto normativo sull'organizzazione.

Durata
60 minuti

Contenuti
- Ruolo strategico della cybersecurity per il business
- Il nuovo paradigma: dalla cybersecurity alla cyberesilence come parametro di valore
- Introduzione alla direttiva NIS2 e al D.Lgs 138/2024
- Ambito di applicazione: soggetti essenziali e importanti
- Analisi puntuale e confronto tra gli articoli del D.Lgs 138/2024 e i requisiti e controlli della ISO/IEC 27001:2022
- Il D.Lgs 138/2024 e la business continuity – cenni alla ISO 22301:2019

Output atteso
Capacità di leggere il D.Lgs. 138/2024 non come mero adempimento normativo, ma come strumento di governo del rischio e di creazione di valore, integrato con ISO/IEC 27001 e ISO 22301 e comprensibile anche a livello di top management e CdA.

2 . **Governance e responsabilità del management (linee di riporto e deleghe)**

Si approfondiscono gli obblighi degli organi di gestione, i concetti di responsabilità, accountability e liability, la matrice RACI minima NIS2, l'integrazione con i controlli interni e le procedure di audit secondo il D.Lgs 138/2024.

Durata
90 minuti

Contenuti
- Articolo 23 D.Lgs 138/2024: obblighi specifici degli organi di gestione
- La responsabilità generale dei manager
  - Responsibility
  - Accountability
  - Liability
- Accountability operativa: RACI minimo NIS2 (chi decide/cosa approva/chi esegue)
- Integrazione con ERM, controlli interni, policy framework
- Gli audit relativi all'applicazione del D.Lgs. 138/2024
  - Art. 24 del D.lgs 138/2024 criteri ed evidenze di audit
  - Analisi dei risultati delle interviste e formulazione delle risultanze
  - Esempio di scrittura di una non conformità e azione correttiva

Output atteso
Capacità di dimostrare una governance chiara e difendibile in ambito NIS2, con ruoli formalizzati, integrazione nei sistemi di controllo aziendale e gestione consapevole degli audit e delle azioni correttive.

3 . **Risk management NIS2 e misure minime**

Si analizzano le misure tecniche, operative e organizzative per la gestione del rischio cyber, la security convergence, la valutazione delle misure, la gestione degli incidenti, la business continuity, la certificazione obbligatoria e i KPI per monitorare l'efficacia delle misure.

Durata
90 minuti

Contenuti
- Art. 24 D.Lgs 138/2024: obblighi in materia di misure di gestione dei rischi per la sicurezza informatica
  - Misure tecniche, operative ed organizzative per gestire i rischi cyber
  - La Security Convergence: l'approccio multirischio
  - Come leggere un report di rischio cyber in CdA.
  - Come valutare se le misure sono "adeguate e proporzionate"
- Gestione degli incidenti
- Business Continuity
  - Gestione dei backup
  - disaster recovery
  - gestione delle crisi
- Sicurezza ed affidabilità del personale, politiche di controllo dell'accesso e gestione dei beni e degli asset.
- Certificazione obbligatoria per i soggetti essenziali ed importanti
- I KPI per misurare l'efficacia delle misure del D.Lgs. 138/2024
- Indicazioni di ACN sugli indicatori

Output atteso
Capacità di produrre/validare una checklist di conformità e adeguatezza + una mini-dashboard KPI (5–10 indicatori) e di formulare 2–3 decisioni di governance tipiche da portare in CdA (priorità, budget, accettazione rischio, remediation su terze parti).

Programma di Formazione NIS2 per C-Level

4 . **Gestione degli incidenti e obblighi di notifica**

Durata
90 minuti

Contenuti
- Definizione di incidente
- Cos'è un incidente rilevante NIS2 e come si qualifica rapidamente
- Gestione degli incidenti
- Art. 25 D.Lgs 138/2024: obblighi in materia di notifica di incidente
- Flusso decisionale: early warning / notifica / report finale (governance del processo)
- Ruoli di CEO/COO/CFO/Legal/Comms: decisioni critiche e statement discipline

Output atteso
Capacità di qualificare un incidente NIS2 in poche ore, attivare correttamente il flusso di notifica previsto dal D.Lgs. 138/2024 e supportare il management nella formulazione di decisioni e comunicazioni coerenti e tracciabili.

5 . **Supply chain & terze parti (Procurement/Legal/IT)**

Si dettagliano la definizione e qualificazione degli incidenti rilevanti, il flusso decisionale per la notifica, la qualifica e valutazione dei fornitori, gli accordi contrattuali.

Durata
90 minuti

Contenuti
- La qualifica e la validazione del fornitore
- Criteri di valutazione
  - Qualifica iniziale
  - Valutazione dinamica
  - Gli output della valutazione
- I subfornitori
- I controlli della ISO/IEC 27001:2002 sulla catena di fornitura
- Gli standard della famiglia ISO/IEC 27036
- Esempi di rischi e misure da considerare
- Gli accordi contrattuali:
  - Processo
  - Contenuto

Output atteso
Capacità di impostare una scheda di qualifica del fornitore, definire un rating di rischio di terza parte, individuare le clausole contrattuali essenziali e motivare decisioni di accettazione, mitigazione o rifiuto del rischio di supply chain.

6 . **Le attività di vigilanza**

Si dettagliano le attività di vigilanza e preparazione a ispezioni da parte dell'ACN.

Durata
60 minuti

Contenuti
- Principi generali per le attività di vigilanza ed esecuzione svolte da ACN
- Come prepararsi a gestire un'ispezione o un'indagine in loco

Output atteso
Capacità di affrontare un'ispezione o un'indagine ACN in modo ordinato e consapevole, presentando evidenze coerenti, gestendo le interazioni in modo efficace e trasformando eventuali rilievi in azioni di miglioramento governate e tracciabili.

01

3/3

Programma di Formazione NIS2 per C-Level

7 . NIS2 in pratica: **Tabletop Exercise – Gestione dell’incidente**

Durata
90 minuti

Contenuti
- Attivazione della crisi e costituzione del crisis team
- Valutazione dell’impatto su operatività, dati e continuità del servizio
- Processo decisionale sotto pressione
- Comunicazione interna ed escalation
- Interazioni tra funzioni (IT, sicurezza, legale, HR, comunicazione, direzione)

Output atteso
Simulazione delle decisioni critiche e dei flussi di gestione dell’incidente.

8 . NIS2 in pratica: **Tabletop Exercise – Gestione della crisi e comunicazione**

Durata
60 minuti

Contenuti
- Comunicazione verso stakeholder interni ed esterni
- Rapporti con autorità competenti e obblighi di notifica NIS2
- Gestione del rischio reputazionale
- Continuità operativa e priorità di ripristino

Output atteso
Test delle capacità di crisis management e comunicazione aziendale.

9 . NIS2 in pratica: **Debriefing e lezioni apprese**

Durata
30 minuti

Contenuti
- Analisi delle decisioni prese durante la simulazione
- Punti di forza e aree di miglioramento
- Gap organizzativi, procedurali e tecnologici
- Raccomandazioni operative per l’adeguamento a NIS2

Output atteso
Consapevolezza concreta dei miglioramenti necessari.

10 . NIS2 in pratica: **Test di verifica**

Simulazione operativa che consente al management di testare la resilienza organizzativa e la capacità decisionale in scenario di crisi cyber conforme alla NIS2. Rafforza leadership, coordinamento interfunzionale e gestione del rischio reputazionale e normativo.

02

1/3

Programma di formazione NIS2 per Organi sociali e direzionali

1 . Introduzione alla Direttiva NIS2 e contesto normativo

Viene illustrato il ruolo strategico della cybersecurity, il passaggio dalla cybersecurity alla cyber resilience, e il quadro normativo con focus sul D.Lgs 138/2024 e la sua correlazione con gli standard ISO 27001:2022 e ISO 22301:2019. Il CdA acquisisce consapevolezza del contesto normativo e dell'impatto sull'organizzazione.

Durata
60 minuti

Contenuti
- Ruolo strategico della cybersecurity per il business
- Il nuovo paradigma: dalla cybersecurity alla cyberesilence come parametro di valore
- Introduzione alla direttiva NIS2 e al D.Lgs 138/2024
- Ambito di applicazione: soggetti essenziali e importanti
- Analisi puntuale e confronto tra gli articoli del D.Lgs 138/2024 e i requisiti e controlli della ISO/IEC 27001:2022
- Il D.Lgs 138/2024 e la business continuity – cenni alla ISO 22301:2019

Output atteso
Capacità di interpretare il D.Lgs. 138/2024 come strumento di governance e creazione di valore, integrato con i framework ISO/IEC 27001 e ISO 22301, e di comunicarne il significato in modo chiaro ed efficace anche a livello di CdA.

2 . Obblighi e responsabilità del CDA

Si approfondiscono gli obblighi specifici degli organi di gestione secondo l'articolo 23 del D.Lgs 138/2024, la responsabilità generale dei manager, le sanzioni amministrative e l'importanza della documentazione. Viene sottolineata la necessità di formazione, supervisione, approvazione delle misure di sicurezza e integrazione della cyber risk governance nella governance aziendale.

Durata
60 minuti

Contenuti
- Articolo 23 D.Lgs 138/2024: obblighi specifici degli organi di gestione
- La responsabilità generale dei manager.
  - Responsibility
  - Accountability
  - Liability
- Sanzioni amministrative
- L'importanza della documentazione
- Due attività basilari: la formazione e l'igiene informatica
- Dovere di supervisione e approvazione delle misure di sicurezza
- Integrazione della cyber risk governance nella governance aziendale
- Modelli di governance efficace

Output atteso
Capacità del management di dimostrare una governance cyber consapevole e documentata, con decisioni formalizzate, supervisione effettiva e integrazione del rischio cyber nei meccanismi ordinari di governo dell'organizzazione. Consapevolezza da parte del CDA di ciò che non può delegare.

02

2/3

Programma di formazione NIS2 per Organi sociali e direzionali

3 . I pilastri delle misure di sicurezza

Il modulo tratta l'analisi dei rischi, le politiche di sicurezza, le misure tecniche e organizzative, la security convergence, la valutazione dei report di rischio, i KPI di efficacia, la sicurezza della supply chain, la crittografia, il modello Zero Trust e la business continuity.

Durata
60 minuti

Contenuti
- Analisi dei rischi e politiche di sicurezza
  - Misure tecniche, operative ed organizzative per gestire i rischi cyber
  - La Security Convergence: l'approccio multirischio
  - Come leggere un report di rischio cyber in CdA
  - I KPI per misurare l'efficacia delle misure del D.Lgs. 138/2024
  - Indicazioni di ACN sugli indicatori
  - Come valutare se le misure sono "adeguate e proporzionate"
- Sicurezza della Supply Chain
  - Valutare la vulnerabilità dei fornitori critici
- Crittografia e Zero Trust
  - Concetti chiave per decisioni di investimento consapevoli
- Business Continuity:
  - Gestione dei backup
  - disaster recovery
  - gestione delle crisi

Output atteso
Il CdA sa leggere e valutare il rischio cyber a livello strategico, scegliere misure adeguate e proporzionate, definire le priorità di investimento, utilizzando KPI e reportistica comprensibili e allineati alle aspettative di governance e di ACN.

4 . Incidenti di sicurezza, crisi cyber e reporting

Il modulo definisce cosa costituisce un incidente rilevante secondo NIS2, gli obblighi di notifica, il ruolo del CdA durante la crisi, le decisioni critiche su continuità operativa e comunicazione, il coordinamento con funzioni aziendali e la gestione della comunicazione di crisi e delle ispezioni.

Durata
60 minuti

Contenuti
- Cosa è un incidente rilevante secondo NIS2
- Obblighi in materia di notifica di incidente (early warning, notifica, report finale)
- Ruolo del CdA durante una crisi cyber
- Decisioni critiche: continuità operativa, comunicazione, impatti reputazionali
- Coordinamento con IT, legale, comunicazione e assicurazioni cyber
- Comunicazione di crisi: gestire il danno reputazionale e le relazioni con gli stakeholder.
- Gestire un'ispezione

Output atteso
Capacità del CdA di governare una crisi cyber in modo strutturato, adempiendo agli obblighi NIS2, proteggendo la continuità operativa e la reputazione aziendale e gestendo in modo efficace comunicazioni e ispezioni.

02

3/3

Programma di formazione NIS2 per Organi sociali e direzionali

5 . NIS2 in pratica: **Tabletop Exercise – Gestione dell’incidente**

Durata
90 minuti

Contenuti
- Attivazione della crisi e costituzione del crisis team
- Valutazione dell’impatto su operatività, dati e continuità del servizio
- Processo decisionale sotto pressione
- Comunicazione interna ed escalation
- Interazioni tra funzioni (IT, sicurezza, legale, HR, comunicazione, direzione)

Output atteso
Simulazione delle decisioni critiche e dei flussi di gestione dell’incidente.

6 . NIS2 in pratica: **Tabletop Exercise – Gestione della crisi e comunicazione**

Durata
60 minuti

Contenuti
- Comunicazione verso stakeholder interni ed esterni
- Rapporti con autorità competenti e obblighi di notifica NIS2
- Gestione del rischio reputazionale
- Continuità operativa e priorità di ripristino

Output atteso
Test delle capacità di crisis management e comunicazione aziendale.

7 . NIS2 in pratica: **Debriefing e lezioni apprese**

Durata
30 minuti

Contenuti
- Analisi delle decisioni prese durante la simulazione
- Punti di forza e aree di miglioramento
- Gap organizzativi, procedurali e tecnologici
- Raccomandazioni operative per l’adeguamento a NIS2

Output atteso
Consapevolezza concreta dei miglioramenti necessari.

8 . NIS2 in pratica: **Test di verifica**

Simulazione operativa che consente al management di testare la resilienza organizzativa e la capacità decisionale in scenario di crisi cyber conforme alla NIS2. Rafforza leadership, coordinamento interfunzionale e gestione del rischio reputazionale e normativo.