Anteprima

Abstract della «Guida alla Conformità NIS2»

Scopri che cosa ti serve per essere pronto!
NB - La Guida completa (vedi sommario alla slide seguente) è disponibile su richiesta.

G TECH
TECHNOLOGY AT YOUR SERVICE

Guida alla conformità NIS2 - Sommario

G TECH
TECHNOLOGY AT YOUR SERVICE

Introduzione alla Direttiva NIS2

📖 Riferimenti Normativi

- Direttiva (UE) 2022/2555 (NIS2)
- Decreto Legislativo 138/2024

ℹ️ Informazioni

La **Direttiva NIS2** mira a rafforzare la sicurezza informatica in Europa, imponendo nuovi obblighi alle aziende nei settori critici e importanti. Il **D.Lgs. 138/2024** recepisce questa normativa in Italia, stabilendo **sanzioni fino a 10 milioni di euro** per le aziende non conformi.

Verificare se l'organizzazione è soggetta a NIS2

Controllare gli **Allegati I e II del D.Lgs. 138/2024** per verificare se si rientra tra i soggetti regolati.

Creare un team di conformità

Coinvolgere il **CISO (Chief Information Security Officer), il DPO e il team IT/security**. Assegnare un **responsabile della compliance NIS2**.

Definire una roadmap di adeguamento

Creare un **piano di attuazione delle misure di sicurezza**. **Stabilire audit periodici** per monitorare la conformità.

Chi deve conformarsi a NIS2

Soggetti Importanti (impatto medio sulla sicurezza del Paese)

1. Servizi ICT business-to-business (fornitori di servizi gestiti).
2. Fornitori di servizi di comunicazione elettronica (operatori telefonici e internet provider).
3. Produttori di componenti critici per infrastrutture digitali.
4. Servizi postali e corrieri espressi
5. Gestori di infrastrutture logistiche
6. Enti di ricerca e sviluppo su tecnologie critiche

Oltre ai criteri dimensionali, l'appartenenza a settori critici è determinante per la classificazione.

📌 **Regola generale**:
- Un'azienda è considerata "**Importante**" se ha **più** di **50 dipendenti** o un fatturato superiore ai **10 milioni** di euro annui.

G TECH
TECHNOLOGY AT YOUR SERVICE

Chi deve registrarsi successivamente?

✅ Aziende non immediatamente incluse negli Allegati I e II, ma successivamente identificate come critiche dall'Autorità Competente (ACN).

✅ Organizzazioni che ricevono una notifica formale dall'ACN sulla necessità di registrazione.

Quando devono registrarsi?

⏳ **Entro 3 mesi** dalla notifica ufficiale dell'ACN.

📌 **Attenzione :**

- Se un'azienda riceve una notifica di registrazione, deve **adeguarsi immediatamente agli obblighi NIS2**, implementando le misure di sicurezza richieste.

G TECH
TECHNOLOGY AT YOUR SERVICE

Chi NON deve conformarsi a NIS2?

(Categorie escluse dagli obblighi di conformità, salvo eccezioni)

📌 **I seguenti soggetti NON sono obbligati a rispettare la Direttiva NIS2, a meno che non operino in settori strategici o non gestiscano dati critici:**

50	10	0
Piccole imprese	**Microimprese**	**Fornitori minori**
Meno di **50 dipendenti** e fatturato inferiore a **10 milioni di euro**.	Meno di **10 dipendenti** e fatturato inferiore a **2 milioni di euro**.	Se **non gestiscono dati sensibili o servizi essenziali** per i soggetti regolati da NIS2.

📌 **Attenzione**: Anche le aziende escluse potrebbero dover adottare misure di sicurezza se collaborano con **soggetti essenziali o importanti**.

G TECH
TECHNOLOGY AT YOUR SERVICE

Impatti Significativi che Richiedono Notifica Preliminare

Secondo il **D.Lgs. 138/2024, Art. 21**, la **notifica preliminare** entro **24 ore** è richiesta **solo** se l'incidente ha **impatti significativi**. Ma cosa si intende per **impatto significativo**?

G TECH
TECHNOLOGY AT YOUR SERVICE

Criteri di Impatto Significativo

1 Impatto su servizi essenziali o importanti

L'incidente interrompe **servizi critici** (es. ospedali, reti energetiche, trasporti, telecomunicazioni).

Degrada gravemente la qualità del servizio (es. rallentamenti, blackout, perdita di funzionalità).

2 Impatto economico rilevante

Danni finanziari elevati per l'azienda o per i suoi clienti.

Perdite superiori a una soglia economica definita internamente (es. 1 milione di euro).

3 Impatto su un elevato numero di utenti o clienti

L'incidente colpisce **migliaia di utenti contemporaneamente**.

Compromette servizi di pubblica utilità.

4 Compromissione di dati sensibili o critici

Furto di **dati sanitari, finanziari, governativi**.

Esposizione di **credenziali di accesso o informazioni riservate**.

5 Attacco informatico di grande portata

Attacco **coordinato** o **persistente** su larga scala (es. ransomware su un'intera infrastruttura).

Violazione avanzata da parte di gruppi APT (Advanced Persistent Threats).

6 Rischio per la sicurezza nazionale o pubblica

Coinvolgimento di **infrastrutture critiche nazionali**.

Minaccia alla sicurezza pubblica o alla difesa.

Obbligo di revisione periodica

1

Audit annuali

Audit annuali obbligatori con report dettagliati all'ACN.

2

Piani di risposta

Piani di risposta agli incidenti aggiornati e testati con simulazioni periodiche.

3

Aggiornamento misure

Le aziende dovranno aggiornare regolarmente le proprie misure di sicurezza e dimostrare la conformità.

Maggiore attenzione ai fornitori e alla supply chain

Responsabilità estesa

Le aziende saranno responsabili della sicurezza informatica dei propri fornitori.

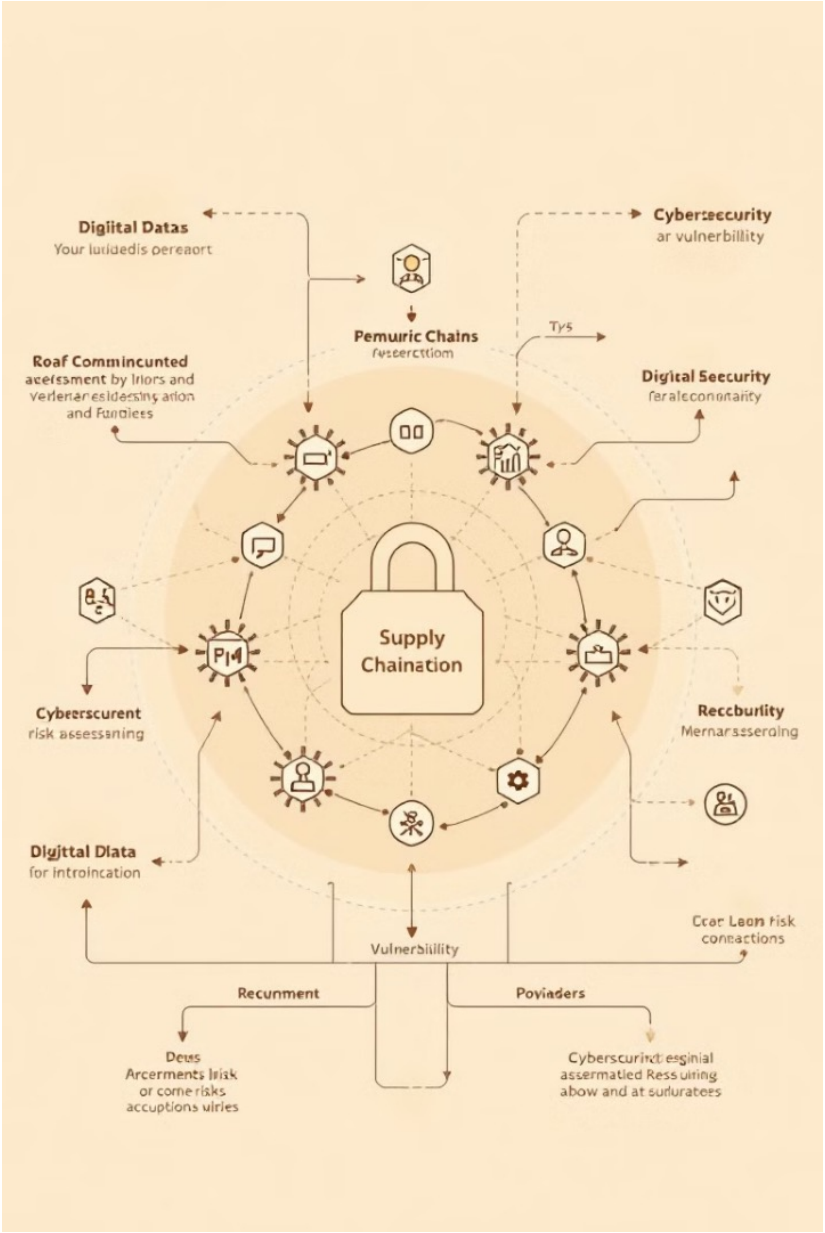
Valutazione dei rischi

Valutazione dei rischi dei fornitori IT per garantire la conformità a NIS2.

Controlli sulle terze parti

Controlli più severi sulle terze parti che gestiscono dati sensibili o infrastrutture critiche.

Rif. ISO 27001:2022 –
Controllo di riferimento: **5.19** – Sicurezza delle relazioni con i fornitori
•**5.20** – Gestione della sicurezza nelle forniture ICT
•**5.23** – Monitoraggio della sicurezza dei fornitori



🚀 Conclusione: chi sarà obbligato in futuro?

1

Oggi

Grandi imprese in **settori critici**.

2

Domani

PMI, startup tecnologiche, tutta la **supply chain digitale e fornitori IT**.

📌 Le aziende devono prepararsi fin da ora per evitare sanzioni e problemi operativi.

G TECH
TECHNOLOGY AT YOUR SERVICE

Vuoi saperne di più?

Se hai domande o desideri richiedere la Guida completa, non esitare a contattaci tramite questo link https://gotech.it/contattaci/ .

GTECH
TECHNOLOGY AT YOUR SERVICE