Get Secured,
Stay Compliant

La Direttiva NIS2:

cosa bisogna sapere e come **Digitek** ti può aiutare a raggiungere la **compliance**

DIGITEK

cyberglobal italy

Cos’è la Direttiva

Direttiva (UE) 2022/2555

La Direttiva (UE) 2022/2555 – chiamata anche **Direttiva NIS2** – è la seconda emissione della direttiva sulla sicurezza informatica e la resilienza a livello dell’UE che mira a regolamentare le misure per migliorare il livello di sicurezza informatica nell’UE e stabilire un quadro per la cooperazione, scambio di informazioni sulle violazioni, migliori pratiche, misure di gestione della cybersicurezza, ecc.

Obiettivi principali della Direttiva

– **Aumentare la resilienza** informatica dei fornitori di servizi essenziali

– Semplificare la resilienza informatica attraverso **requisiti di sicurezza più rigorosi e sanzioni per le violazioni**

– **Migliorare la preparazione dell’UE ad affrontare gli attacchi informatici**

Chi coinvolge

Aziende ed Enti Pubblici che ricadono nelle categorie di **Soggetti Essenziali e Importanti**, identificati con criteri basati sulla rilevanza del settore e sulla dimensione.

Saranno comunque coinvolti anche i Fornitori di Aziende ed Enti Pubblici che ricadranno nel perimetro della Direttiva.

Come ottenere la compliance

La Direttiva richiede l’applicazione di specifici controlli in conformità con gli standard internazionali.

E’ necessario dotarsi di una serie di **tecnologie** per il monitoraggio e la gestione degli incidenti, ma anche dotarsi di un **Sistema di gestione** (politiche, procedure, registri, nomine, processi di controllo e monitoraggio, ecc.) e **competenze sia tecniche che trasversali**.

Sanzioni

Sono previste pesanti sanzioni.

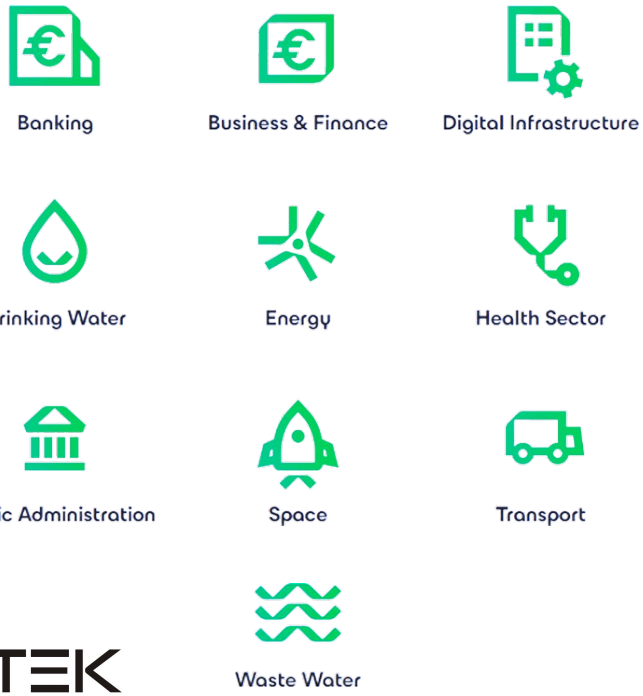
L’alta direzione sarà responsabile della non conformità.

DIGITEK

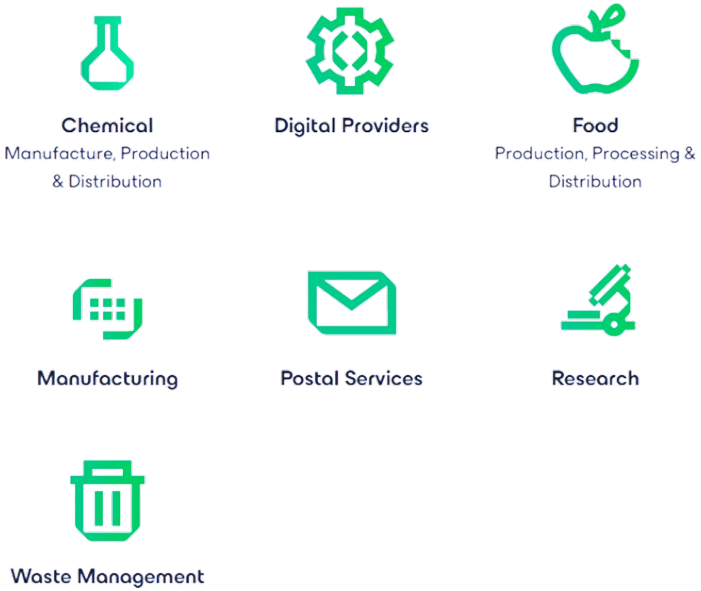
cyberglobal italy

A quali settori si applica la NIS2?

settori essenziali / critici



settori importanti



DIGITEK

cyberglobal italy

A chi si applica la NIS2?

Tutte le organizzazioni **ESSENZIALI** e **IMPORTANTI** con **50 o più dipendenti**

La **Direttiva NIS2** copre l'intera **supply chain** di un'organizzazione.
Possono essere interessate anche le aziende che si trovano **al di fuori dell'UE**, come il **Regno Unito** o la **Svizzera**, ma che operano all'interno dell'UE.

I punti principali

Rafforzamento delle capacità di resilienza

La direttiva promuove una maggiore **resilienza e capacità di gestione delle crisi** a livello sia nazionale che dell'UE, con una maggiore attenzione alla **prevenzione** e alla **mitigazione degli incidenti**.

Requisiti di sicurezza più severi

Le organizzazioni soggette alla direttiva devono implementare **misure di sicurezza più rigorose**, tra cui la gestione dei rischi di sicurezza informatica, la risposta agli incidenti e la continuità operativa.

I punti principali

Obblighi di notifica degli incidenti

Le imprese devono **notificare gli incidenti significativi** alle autorità competenti in tempi definiti (24 ore per la notifica iniziale): questo permette una risposta tempestiva e coordinata agli attacchi informatici.

Principali scadenze

DECRETO LEGISLATIVO 4 settembre 2024, n. 138,
Recepimento della direttiva (UE) 2022/2555 NIS2, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione.

1. **Entro il 31 dicembre 2024 PRIMO ASSESSMENT**
   Aziende e pubbliche amministrazioni dovranno svolgere un assessment per comprendere se siano o meno soggette agli obblighi della Direttiva NIS2.

2. **Tra 1 gennaio e 28 febbraio 2025 REGISTRAZIONE SU ACN**
   I soggetti che a seguito dell'assessment ritengano di rientrare nell'ambito di applicazione del decreto dovranno registrarsi sulla piattaforma digitale ACN.

Principali scadenze

3 **Entro il 17 gennaio 2025 REGISTRAZIONE SU ACN**
Dovranno registrarsi sulla piattaforma ACN i fornitori di servizi di sistema dei nomi di dominio, i gestori di registri dei nomi di dominio di primo livello, i fornitori di servizi di registrazione dei nomi di dominio, i fornitori di servizi di cloud computing, i fornitori di servizi di data center, i fornitori di reti di distribuzione dei contenuti, i fornitori di servizi gestiti, i fornitori di servizi di sicurezza gestiti, nonché i fornitori di mercati online, di motori di ricerca online e di piattaforme di servizi di social network.

4 **Entro il 31 marzo 2025 ELENCO UFFICIALE ACN**
L'ACN redigerà l'elenco dei soggetti essenziali e dei soggetti importanti sulla base delle registrazioni ricevute attraverso la piattaforma.

5 **Tra il 1 aprile 2025 e il 15 aprile 2025 COMUNICAZIONE ACN**
L'ACN comunicherà ai soggetti registrati l'inserimento nell'elenco dei soggetti essenziali o importanti.

Principali scadenze

6 **Entro il 15 aprile 2025 NOMINA RESPONSABILE**
I soggetti che avranno ricevuto la comunicazione dovranno nominare con un apposito atto un soggetto che abbia la responsabilità dell'adempimento degli obblighi del decreto.

7 **Tra il 15 aprile e il 31 maggio 2025 ULTERIORI INFORMAZIONI AD ACN**
I soggetti che avranno ricevuto la comunicazione attraverso la piattaforma ACN dovranno fornire ulteriori informazioni richieste dalla normativa.

8 **A partire dal 1 gennaio 2026 PRIMI ADEMPIMENTI**
Si dovrà adempiere all'obbligo di notifica degli incidenti.

9 **Entro il 1 ottobre 2026 ULTERIORI ADEMPIMENTI**
Si dovrà adempiere agli obblighi degli organi di amministrazione e direttivi, agli obblighi in materia di misure di sicurezza, all'obbligo di raccolta e mantenimento di una banca dei dati di registrazione dei nomi di dominio, laddove applicabile.

La nuova **Direttiva NIS 2** rappresenta una sfida e un’opportunità per migliorare la **resilienza cibernetica** della tua organizzazione.
I nuovi obblighi richiedono un **approccio proattivo alla sicurezza**.

Scopri come possiamo aiutarti a soddisfare gli **adempimenti richiesti**, trasformando la conformità in un **vantaggio competitivo**.

DIGITEK

cyberglobal italy

Il percorso per la certificazione in 5 Fasi

Fase 1: Valutazione e Gap Analysis.
Obiettivo: Identificare lo stato attuale e mappare le lacune rispetto alla conformità NIS2.

Fase 2: Sviluppo e implementazione di politiche e procedure.
Obiettivo: Creare politiche di sicurezza, governance e piani di gestione del rischio.

Fase 3: Implementazione delle misure tecniche.
Obiettivo: Installazione e configurazione di strumenti di sicurezza (es. firewall, sistemi di monitoraggio, gestione delle vulnerabilità).

Fase 4: Formazione e sensibilizzazione.
Obiettivo: Educare il personale e creare una cultura di sicurezza all'interno dell'azienda.

Fase 5: Testing e audit.
Obiettivo: Eseguire simulazioni e test di sicurezza per valutare l'efficacia delle misure implementate e rispondere agli incidenti.

1 Fase 1: Gap Analisys

La **Gap Analysis** fornirà una mappa dettagliata di ciò che è già presente a livello di c**ontrolli di sicurezza**, **governance** e **capacità operative**, e ciò che manca o deve essere migliorato.

Questa fase sarà il fondamento per la successiva fase di progettazione.

- Valutazione dello stato attuale dell'organizzazione rispetto ai **requisiti di conformità** della **direttiva NIS2**.
- Identificazione dei **punti di forza** e le **aree di miglioramento** nel loro sistema di **cybersecurity**.
- Definizione dei **requisiti di sicurezza specifici** per il loro settore e le loro operazioni.

Il servizio viene erogato da personale altamente qualificato, certificato Lead Auditor ISO 27001 e ISO 22301.

2 Fase 2: Implementazione sistemi di gestione

Servizio di Implementazione (o supporto all'implementazione) di sistemi di gestione certificati e non, **ISO 27001** e **ISO 22301**, Framework Nazionale per la Cybersecurity e la Data Protection, **NIST Cybersecurity Framework**, **GDPR**.

- **Governance della Cybersecurity**
- **Gestione del Rischio**
- **Misure tecniche ed organizzative**
- **Incident Response e Business Continuity**

Il servizio viene erogato da personale altamente qualificato, certificato Lead Auditor ISO 27001 e ISO 22301.

DIGITEK

cyberglobal italy

3 Fase 3: Implementazione misure tecniche

Progettazione ed implementazione soluzioni **Cybersecurity** e **IT**.

- **Soluzioni di monitoraggio SOC / SIEM 24x7**
- **Servizio di vulnerabilità**
- **Servizio di Penetration Test**
- **Soluzioni di business continuity: disaster recovery, backup, cloud**

Il servizio viene erogato da personale altamente qualificato, certificato Lead Auditor ISO 27001 e ISO 22301.

DIGITEK

cyberglobal italy

4 Fase 4: Formazione

Programma di formazione per il personale.
Sensibilizzazione dei dipendenti sui rischi di sicurezza informatica e sulle buone pratiche per la protezione delle informazioni aziendali.

Simulazioni di phishing e attacchi simulati.
Esecuzione di test pratici, come campagne di phishing simulate, per valutare la prontezza del personale e rafforzare la consapevolezza sui rischi.

Il servizio viene erogato da personale altamente qualificato, certificato Lead Auditor ISO 27001 e ISO 22301.

5 Fase 5: Audit & Test

Audit di verifica anche tramite il servizio di PenTest

Servizio di audit annuale per verificare che tutte le procedure ed I sistemi siano conformi alla Direttiva nel tempo.

Il servizio viene erogato da personale altamente qualificato, certificato Lead Auditor ISO 27001 e ISO 22301.

Il tuo partner Locale di Cybersecurity
con esperienza Globale

Andrea Anderlini
Amministratore Unico - Digitek Srl
Mail: anderlini@digi-tek.eu

DIGITEK

https://www.digi-tek.eu/servizi-cybersicurezza