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 (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


Banking


Business & Finance


Digital Infrastructure


Drinking Water


Energy


Health Sector


Public Administration


Space


Transport


Waste Water

settori importanti


Chemical
Manufacture, Production & Distribution


Digital Providers


Food
Production, Processing & Distribution


Manufacturing


Postal Services


Research


Waste Management

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 Luglio 2025 Comunicazione .....

Per effetto della Determina ACN n. 136117/2025, entro il 31 maggio 2025 i soggetti NIS sono chiamati, oltre che a designare il sostituto punto di contatto, a fornire e aggiornare il censimento degli utenti quali la segreteria e gli operatori che accedono al Portale di ACN e, in particolare, accedono ai Servizi NIS. Sarà necessario segnalare all'Agenzia i componenti degli organi di amministrazione e direttivi del soggetto NIS, gli Stati Membri entro i quali vengono erogati i propri servizi (qualora sia applicabile), gli indirizzi IP (pubblici e statici), unitamente ai nomi di dominio, in uso o nella disponibilità del soggetto e, qualora siano presenti, notificare gli accordi di condivisione delle informazioni sulla sicurezza informatica sottoscritti su base volontaria a partire dall'entrata in vigore del decreto NIS.

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.

2

Entro 1 gennaio 2026

IPer effetto della Determina ACN n.164179/2025, a far data da gennaio 2026, ovvero nove mesi dalla ricevimento della PEC dell'Agenzia, qualsiasi soggetto 1 / 2 NIS è tenuto ad adempiere all'obbligo di notifica degli incidenti significativi di base in caso di :

- perdita di riservatezza di dati digitali di sua proprietà o sui quali esercita il controllo, anche parziale;
- perdita di integrità, anche parziale, di dati di sua proprietà o sui quali esercita il controllo;
- violazione dei livelli di servizio attesi dei suoi servizi e/o delle sue attività, sulla base dei livelli di servizio atteso per i sistemi informativi e di rete rilevanti per rilevare tempestivamente gli incidenti significativi.

La nostra proposta

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**.

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

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

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

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

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

DIGITEK

cyberglobal italy

Il tuo partner Locale di Cybersecurity
con esperienza Globale

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