NIS 2: LA NUOVA DIRETTIVA EUROPEA SULLA CYBERSICUREZZA ↗

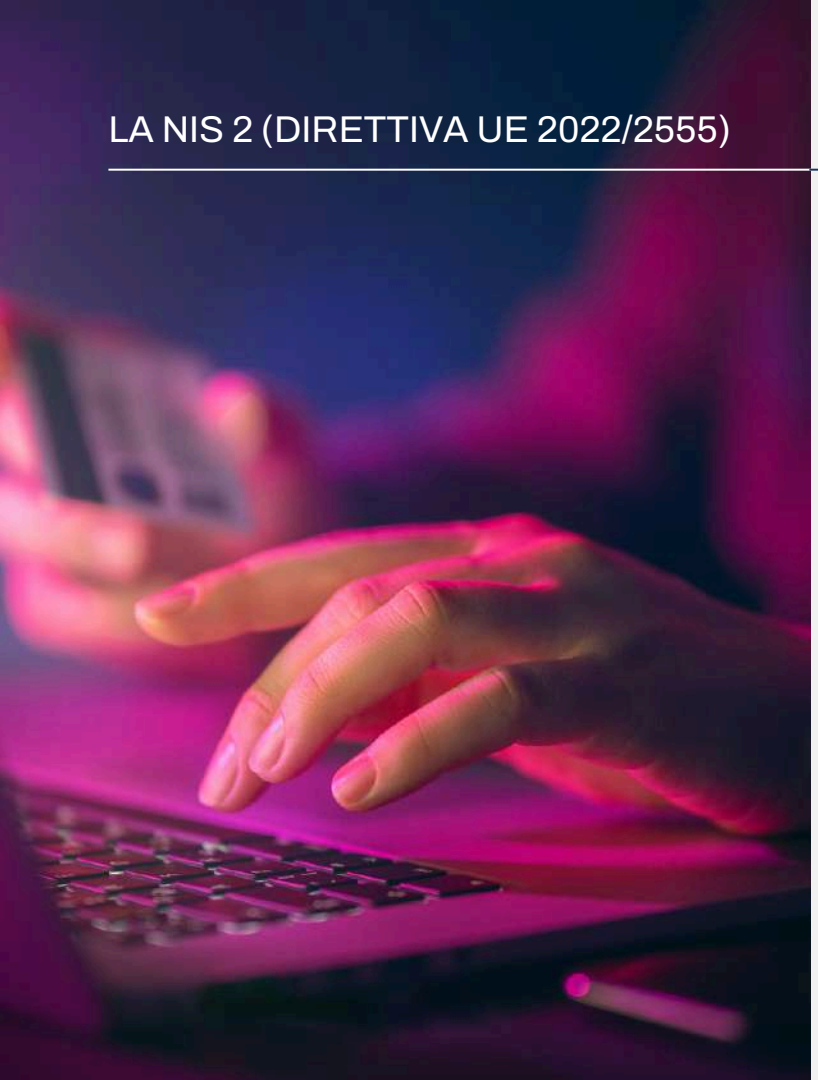
l'mprove EVOLUZIONE

Improve S.r.l. ha predisposto un servizio di consulenza e orientamento relativo agli imminenti cambiamenti introdotti dalla NIS 2 – La nuova direttiva europea in materia di Cyber Sicurezza.

È nostra concreta volontà supportare le aziende illustrando le linee guida, i passaggi normativi e la gestione delle scadenze normative in materia di Cyber Sicurezza.

A tal fine, siamo lieti di indicare un canale di comunicazione diretto a cui rivolgersi per avere ulteriori informazioni dal nostro team di esperti:
avsec@improvesrl.it

INDICE



LA NIS 2 (DIRETTIVA UE 2022/2555) È ENTRATA IN VIGORE A GENNAIO 2023

PER SOSTITUIRE LA NIS 1 (DIRETTIVA UE 2016/114) E RAGGIUNGERE **I SEGUENTI OBIETTIVI**:

- Elevare ed armonizzare il livello comune di cybersicurezza di tutti gli Stati membri
- Rafforzare la resilienza e la sicurezza delle infrastrutture critiche
- Migliorare il livello collettivo di consapevolezza e capacità di gestione e risposta delle minacce informatiche
- Aumentare la cooperazione tra gli stati per garantire la gestione coordinata in caso di incidenti e crisi su vasta scala e il regolare scambio di informazioni pertinenti tra gli Stati membri e le istituzioni, gli organi e gli organismi dell'Unione.

LA NIS 2 SOSTITUIRÀ LA PRECEDENTE NORMATIVA NIS 1 PER SUPERARNE I LIMITI.

1. Copre una gamma più ampia di settori critici, ritenuti vitali per il funzionamento delle principali attività sociali ed economiche del mercato interno europeo

2. Fornisce un elenco più dettagliato di misure tecniche, operative e organizzative per gestire i rischi, garantire la sicurezza delle reti e delle informazioni, prevenire incidenti informatici e ridurre al minimo gli effetti negativi

3. Prevede in capo ai soggetti NIS2 un obbligo di notifica tempestivo al CSIRT in caso di «incidente significativo» e, se opportuno, ai destinatari dei loro servizi

4. Stabilisce un apparato sanzionatorio simile a quello presente nel GDPR attribuendo poteri di vigilanza alle Autorità competenti

I SOGGETTI GIÀ IMPATTATI NELLA NIS 1 DEVONO RIVEDERE SISTEMI E PRATICHE DI CYBERSICUREZZA

I nuovi soggetti aggiunti dalla NIS 2 devono introdurre nuovi sistemi e pratiche di cybersecurity

TEMPISTICHE

Entro il 17 ottobre 2024 ogni stato UE dovrà recepire la NIS 2 nella legislazione nazionale e convertirla in legge

SANZIONI

Tutte i soggetti NIS2 dovranno adempiere ai requisiti di cybersicurezza prescritti In caso di inadempienza: Sanzioni pecuniarie amministrative pari a:

1. un massimo di almeno 7-10 milioni di euro;
2. o ad un massimo di almeno il 1,4%-2% del totale del fatturato mondiale annuo per l'esercizio; precedente dell'impresa cui il soggetto essenziale appartiene;
3. nei casi più gravi, sospensione o il divieto temporaneo a qualsiasi persona che svolga funzioni dirigenziali (come amministratore delegato o rappresentante legale) di svolgere le suddette funzioni.

Criteri per stabilire se un soggetto è impattante dalla NIS2

SETTORI DI APPARTENENZA
(settori critici)

DIMENSIONI
(medie o grandi dimensioni)

RUOLO
(soggetti ritenuti critici indipendentemente dalle loro dimensioni)

La NIS 2 inoltre definisce due tipi di soggetti critici cui applicare la direttiva in funzione del tipo di servizi che forniscono nonché delle loro dimensioni:

1. SOGGETTI ESSENZIALI
2. SOGGETTI IMPORTANTI

Ambedue i soggetti avranno gli stessi obblighi ma quelli essenziali saranno sottoposti a misure di cybersicurezza e sanzioni più rigorose e un diverso regime di vigilanza (ex-ante)

PRINCIPALI OBBLIGHI

LE AZIENDE SOGGETTE ALLA NIS 2 DEVONO IMPLEMENTARE MISURE SPECIFICHE PER RAFFORZARE LA PROPRIA CYBERSICUREZZA E GARANTIRE LA CONTINUITÀ OPERATIVA, TRA LE QUALI, A TITOLO ESEMPLIFICATIVO:

1. PIANO DI GESTIONE DEL RISCHIO:

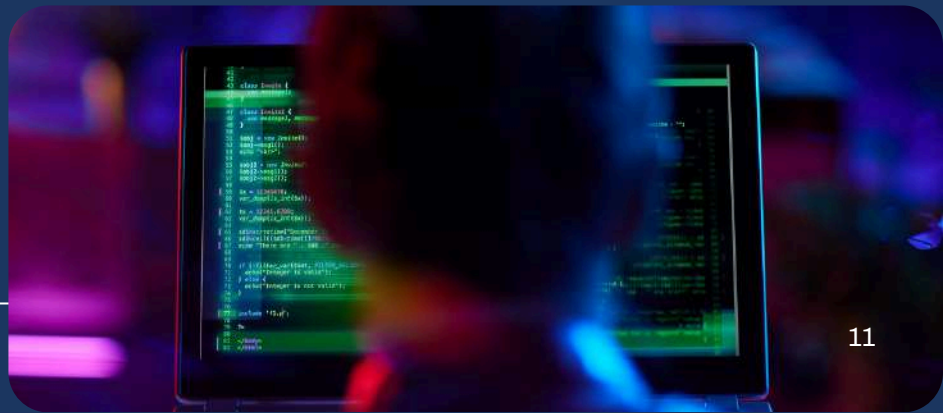
   definire e implementare un piano completo per la gestione del rischio informatico, che includa misure tecniche e organizzative adeguate a prevenire e mitigare cyber attacchi.

2. NOTIFICA DEGLI INCIDENTI DI SICUREZZA:

   in caso di incidenti significativi, sarà necessario notificare all'Agenzia per la Cybersicurezza Nazionale (ACN) entro 24 ore, fornendo un rapporto dettagliato entro 72 ore.

3. VALUTAZIONE DELLA CATENA DI FORNITURA:

   la verifica della conformità dovrà essere estesa ai fornitori critici, con audit periodici per garantire che anche la catena di approvvigionamento rispetti i requisiti di sicurezza imposti dalla NIS 2.



LE PRINCIPALI SCADENZE DA TENERE IN CONSIDERAZIONE SONO:

1. entro il 31 dicembre 2024, completare un assessment per determinare se l'organizzazione rientra tra quelle soggette agli obblighi previsti dalla normativa in questione, alla luce di quanto disposto dagli artt. 6 e 7, dagli Allegati I, II, III e IV;
2. tra il 1° gennaio e il 28 febbraio 2025, i soggetti rientranti nell'ambito di applicazione, dovranno provvedere alla registrazione sulla piattaforma digitale, in fase in rilascio, predisposta dall'Agenzia per la Cybersicurezza Nazionale (ACN);
3. entro il 31 marzo 2025 (e a seguire entro il 31 marzo di ogni anno successivo), ACN pubblicherà l'elenco ufficiale dei soggetti essenziali e importanti sulla base delle registrazioni ricevute tramite la piattaforma digitale;
4. tra il 1° aprile e il 15 aprile 2025, attraverso la piattaforma, ACN comunicherà ai soggetti registrati la loro classificazione ufficiale come soggetti essenziali o importanti;
5. entro il 15 aprile 2025, le organizzazioni/Aziende che avranno ricevuto la comunicazione dovranno nominare formalmente un soggetto che abbia la responsabilità dell'adempimento degli obblighi in questione;
6. maggio 2025, i soggetti che avranno ricevuto la comunicazione dovranno fornire alcune ulteriori informazioni e aggiornare eventuali dati mancanti o incompleti.

SECONDA FASE ATTUATIVA (METÀ APRILE 2025 – METÀ APRILE 2026)

Dopo la definizione delle aziende soggette alla normativa, inizia la fase di monitoraggio e implementazione progressiva degli obblighi. Le tappe fondamentali:

A partire da gennaio 2026:

Scatta l'obbligo di notifica degli incidenti informatici. Le aziende dovranno segnalare ogni attacco significativo al CSIRT Italia.

Entro aprile 2026:

ACN si adopererà per l'elaborazione e definizione del modello di categorizzazione delle attività e dei servizi oltre che l'elaborazione e definizione degli obblighi a lungo termine.

Entro settembre 2026:

Tutte le aziende dovranno aver completato l'implementazione delle misure di sicurezza di base.
Questo periodo sarà caratterizzato da controlli e verifiche per valutare il grado di conformità delle aziende.

TERZA FASE ATTUATIVA (DA METÀ APRILE 2026 IN POI)

Questa fase segnerà l'inizio della piena operatività della NIS 2, con un'attenzione particolare alla categorizzazione delle attività e alla definizione di obblighi avanzati:

1. 1. APPLICAZIONE INTEGRALE DEL MODELLO DI CATEGORIZZAZIONE DELLE ATTIVITÀ E DEI SERVIZI DEFINITO DA ACN

2. Piena attuazione degli obblighi a lungo termine, con un rafforzamento continuo delle misure di sicurezza

1. RISKMANAGEMENT

   Strutturare politiche di analisi dei rischi e di sicurezza dei sistemi informatici organizzativi (SISTEMA DI GESTIONE DI SICUREZZA INFORMATICA)

2. GESTIONE INCIDENTI

   Creare piani operativi e procedure standardizzate di gestione degli incidenti informatici

3. BUSINESS CONTINUITY

   Gestione della continuità operativa, definendo politiche di backup, piani di ripristino (DRP, Disaster Recovery Plan) per fronteggiare scenari di crisi

4. VERIFICA DELLA CATENA DI APPROVIGGIONAMENTO

   Garantire la sicurezza della catena di approvvigionamento, compresi i rapporti con i fornitori

5. SICUREZZA DEI SISTEMI

Gestione degli asset, indispensabile per avere il pieno controllo del perimetro da mettere al riparo dalle minacce più rilevanti in ogni fase, dallo sviluppo alla manutenzione

6. STRATEGIE CYBER

Creare strategie e procedure per valutare l'efficacia delle misure di contrasto ai rischi di cyber sicurezza e verifica dell'efficacia delle misure adottate, ricorrendo, ad esempio, a simulazioni periodiche di attacchi informatici e incidenti di sicurezza

7. FORMAZIONE

Creare e rispettare pratiche di igiene informatica di base e garantire formazione in materia di cybersecurity

8. CRITTOGRAFIA E CIFRATURA

Stabilire politiche e procedure relative all'uso della crittografia e della cifratura per le attività organizzative

9. CONTROLLO ACCESSI

   Garantire la sicurezza informatica per il personale, attraverso la gestione ed il controllo degli accessi fisici e logici

10. AUTENTICITA' A PIU' FATTORI

    Usare soluzioni di autenticazione a più fattori o di autenticazione continua e sistemi di comunicazione protetti

Gli ampi requisiti non possono essere soddisfatti solo implementando soluzioni tecniche, ma richiedono anche un attento esame dei processi all'interno dell'azienda.

1 Valutare il rischio

Analisi dettagliata delle reti e dei sistemi informativi dell'organizzazione al fine di identificare tutte le potenziali minacce, determinare il proprio livello di esposizione e dare priorità alle aree che necessitano di interventi immediati.

2 Pianificare misure di sicurezza

Sviluppo di un piano di sicurezza che includa politiche, procedure e controlli specifici allineati con i requisiti della Direttiva che coprano le aree critiche dell'infrastruttura IT.

3 Effettuare controlli di sicurezza

Firewall, sistemi di rilevamento delle intrusioni, autenticazione multifattoriale (MFA) e crittografia. Dovranno inoltre integrare controlli di tipo organizzativo, tra cui adeguate politiche di segregazione dei compiti, di gestione degli accessi alle informazioni, di change e patch management e, naturalmente, regolari backup del proprio patrimonio informativo.

4 Promuovere la formazione del personale

Formazione regolare per il personale (inclusi gli organi direttivi), dando particolare rilievo a temi quali la gestione delle password, il riconoscimento delle e-mail di phishing e le procedure di risposta agli incidenti: la formazione continua è strumento essenziale per mantenere alta la consapevolezza rispetto alle minacce e la propensione alla valutazione dei rischi.

Gli ampi requisiti non possono essere soddisfatti solo implementando soluzioni tecniche, ma richiedono anche un attento esame dei processi all'interno dell'azienda.

5 Monitoraggio e revisione continui

Gestione delle vulnerabilità e la revisioni periodiche di tutte le politiche e procedure di sicurezza, per appurarne l'efficacia e procedere laddove opportuno con gli aggiornamenti necessari all'emergere di nuove minacce.

6 Collaborazione e condivisione delle informazioni

Invito alla collaborazione inteso a diffondere informazioni rilevanti per aiutare la comunità europea a fronteggiare minacce cibernetiche.

IMPROVE S.R.L.
Via della Salute, 97
40132 Bologna – Italia

P.IVA 3154681203

Tel. +39 348 78 25 308
segreteria@improvesrl.it
www.improvesrl.it