Che cos'è la Direttiva NIS2?

Nell'era digitale la sicurezza informatica è una delle principali preoccupazioni sia per i singoli sia per le organizzazioni, a causa della crescente frequenza e complessità degli attacchi informatici. Per questo motivo nel 2016 la Commissione Europea ha introdotto la direttiva UE sulla sicurezza delle reti e delle informazioni (Network and Information Security, NIS) per migliorare la sicurezza informatica nell'Unione Europea. Tuttavia la direttiva mancava di accountability, spingendo la Commissione a prevedere la sua sostituzione con la più robusta direttiva NIS2.

NIS2 impone alle aziende di implementare misure fondamentali di cybersecurity, tra cui la sicurezza della supply chain, la crittografia e la cifratura (articolo 18). L'articolo 89 evidenzia l'adozione di pratiche di igiene informatica di base, come i principi di zero-trust, gli aggiornamenti del software, la configurazione dei dispositivi, la segmentazione della rete e l'Identity and Access Management per i soggetti classificati come essenziali e importanti.

Confronto NIS e NIS2 - cosa è cambiato?

Ci sono alcune differenze importanti tra la vecchia e la nuova Direttiva:

- La nuova proposta elimina la distinzione tra Operatori di Servizi Essenziali (Operators of Essential Services, OES) e Fornitori di Servizi Digitali (Digital Service Providers, DSP), classificando invece i soggetti come essenziali o importanti.
- Il campo di applicazione della Direttiva viene ampliato per coprire nuovi settori in base alla loro criticità per l'economia e la società, includendo tutte le aziende di medie e grandi dimensioni in tali settori. Gli Stati membri possono anche identificare entità più piccole con un profilo ad alto rischio.
- Viene proposta l'istituzione di una Rete Europea di Organizzazioni di Collegamento per le Crisi Informatiche (European Cyber Crisis Liaison Organization Network EU-CyCLONe) per lavorare collettivamente nella preparazione e nell'implementazione di piani di risposta rapida alle emergenze, ad esempio in caso di incidenti o crisi informatiche su larga scala.
- Maggiore coordinamento nella divulgazione di nuove vulnerabilità scoperte nell'Unione Europea. Viene stabilito un elenco di sanzioni amministrative (simili a quelle del GDPR), incluse multe per la violazione degli obblighi di reporting e gestione del rischio di cybersecurity.
- NIS2 impone obblighi diretti al management per implementare e supervisionare la conformità della propria organizzazione alla legislazione – risultanti in potenziali multe e divieto temporaneo di esercitare funzioni di gestione, anche a livello di C-suite in caso di inadempienze.

Inoltre, introduce disposizioni più precise sul processo di segnalazione degli incidenti, sul contenuto dei report e sulla tempistica (entro 24 ore dalla scoperta dell'incidente). A livello europeo la proposta rafforza la sicurezza informatica per le tecnologie ICT chiave. Gli Stati membri, in collaborazione con la Commissione e l'Agenzia dell'Unione Europea per la Cybersecurity ENISA, dovranno effettuare risk assessment coordinati per le supply chain critiche.

A chi si applica?

Mentre la vecchia direttiva NIS attribuiva agli Stati membri la responsabilità di determinare quali soggetti avrebbero soddisfatto i criteri per qualificarsi come operatori di servizi essenziali, la nuova direttiva NIS2 introduce una regola dimensionale. Ciò significa che tutte le entità di medie e grandi dimensioni che operano nei settori o forniscono servizi coperti dalla direttiva rientreranno nel suo ambito di applicazione.

Di seguito può trovare la classificazione:

Soggetti essenziali (EE) Soglia dimensionale: varia a seconda del settore, ma in genere 250 dipendenti, ricavi annui di 50 milioni di euro o bilancio di 43 milioni di euro.	**Soggetti importanti (IE)** Soglia dimensionale: varia a seconda del settore, ma generalmente 50 dipendenti, ricavi annui di 10 milioni di euro o bilancio di 10 milioni di euro.
Energia	Servizi postali
Trasporti	Gestione dei rifiuti
Finanza	Prodotti chimici
Pubblica Amministrazione	Ricerca
Salute	Alimentari
Spazio	Industria manifatturiera
Approvvigionamento idrico (acqua potabile e acque reflue)	Provider digitali (ad es. social network, motori di ricerca, marketplace online)
Infrastrutture digitali (ad es. fornitori di servizi di cloud computing e gestione ICT)	

NIS2 copre anche gli enti della pubblica amministrazione a livello centrale e regionale, ma esclude i parlamenti e le banche centrali.

Quando entra in vigore NIS2?

Tutti gli Stati membri dell'UE devono recepire i nuovi obblighi nelle proprie leggi nazionali entro il 17 ottobre 2024, avendo a disposizione per conformarsi una finestra di 21 mesi dopo l'entrata in vigore della direttiva (approvata il 16 gennaio 2023).

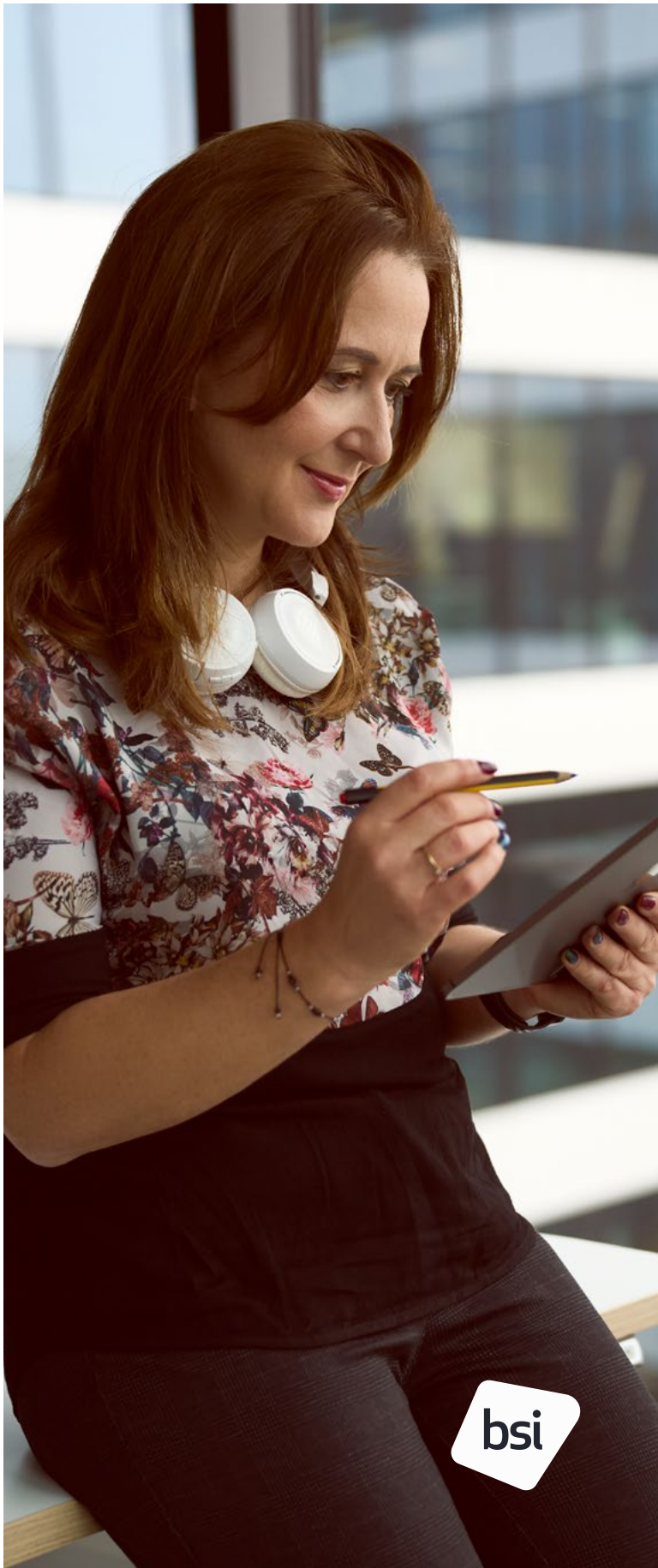
Queste le tappe di sviluppo della NIS:

- **6 luglio 2016:** adozione della NIS
- **9 maggio 2018:** termine ultimo per il recepimento della NIS nella legislazione nazionale da parte degli Stati membri
- **7 luglio 2020:** la Commissione Europea avvia una consultazione sulla riforma della NIS
- **16 dicembre 2020:** la Commissione Europea pubblica la proposta per NIS2
- **22 novembre 2021:** il Parlamento europeo definisce la sua posizione negoziale
- **3 dicembre 2021:** il Consiglio europeo definisce la sua posizione negoziale
- **13 gennaio 2022:** primo ciclo di negoziati a tre
- **16 febbraio 2022:** secondo ciclo di negoziati a tre
- **13 maggio 2022:** accordo politico raggiunto
- **10 novembre 2022:** il Parlamento europeo vota per l'adozione della NIS2
- **28 novembre 2022:** NIS2 approvata dal Consiglio dell'UE
- **27 dicembre 2022:** NIS2 viene pubblicata sulla Gazzetta Ufficiale ed entra in vigore 20 giorni dopo, il 16 gennaio 2023
- **17 ottobre 2024:** termine ultimo per il recepimento della NIS2 nella legislazione nazionale da parte degli Stati membri

Come possiamo aiutare le aziende ad essere conformi alla NIS2?

In BSI abbiamo un grande team di esperti altamente qualificati e specializzati, che contribuiranno a garantire che le aziende abbiano tutti i requisiti di sicurezza necessari per essere al passo con la Direttiva NIS2. Con il nostro aiuto le organizzazioni possono evitare le possibili sanzioni e ispirare ulteriore fiducia ai propri clienti.

Dall'identificazione iniziale degli operatori di servizi essenziali (Operators of Essential Services, OES) all'autovalutazione, al risk assessmente e risk treatment, la nostra esperienza di collaborazione con le organizzazioni di tutti i settori può supportarle nel percorso verso la conformità alla Direttiva NIS2.



Attualmente BSI offre i seguenti servizi in relazione ai requisiti NIS2:

- Strategia/governance informatica
- Assessment del posizionamento/maturità della cybersecurity rispetto ai framework standard del settore
- Sviluppo di una strategia di sicurezza informatica/cyber e presentazioni al board
- Gap Analysis e supporto all'implementazione (ISO/IEC 27001, SOC 2, NIST CSF/800-53)
- Sensibilizzazione sulla sicurezza informatica e formazione sulla Business Continuity (ISO 22301)

Gestione delle crisi e risposta agli incidenti

- Business Continuity (ISO 22301)
  - Business Impact Analysis (BIA)/Sviluppo di policy/Pianificazione della Business Continuity
- Supporto, implementazione e test periodici di Disaster Recovery
- Penetration test threat-led
- Intelligence Open-Source (OSINT)
- Assessment della sicurezza fisica; Simulazione di attacchi (team rosso/blu/viola)
- Pianificazione e implementazione della risposta agli incidenti (ISO/IEC 27035)
- Modellazione delle minacce/assessment delle minacce
- Valutazione delle capacità di pianificazione e segnalazione della risposta agli incidenti attuali
- Test di risposta agli incidenti/formazione del personale

Gestione del rischio e reporting

- Sviluppo e implementazione del framework di gestione del rischio IT (ISO/IEC 27005)
  - Gestione del rischio di terze parti (ISO/IEC 27036-2)
  - Assessment dello stato corrente della gestione del ciclo di vita delle terze parti
  - Sviluppo di un framework end-to-end di gestione dei fornitori
  - Implementazione del quadro di gestione del rischio di terza parte insieme a un supporto continuo alla gestione del rischio
- BSI collabora con partner tecnologici che dispongono di strumenti per facilitare la gestione dell'intero ciclo di vita del fornitore
  - Threat Intelligence/Certificazione Computer Emergency Response Team (CERT)
  - Valutazione della situazione corrente e determinazione dello stato futuro
  - Costruzione di un quadro di reporting

Perché ISO/IEC 27001 e ISO 22301 sono fondamentali per la conformità NIS2?

Le normative NIS raccomandano che le aziende, nei loro sforzi di conformità, diano priorità alla "conformità agli standard internazionali". Inoltre, le linee guida tecniche dell'Agenzia dell'Unione Europea per la Cybersecurity (ENISA) allineano ciascun obiettivo di sicurezza agli standard di best practice come la ISO/IEC 27001.

Tra tutti i servizi che BSI può fornire alle aziende in relazione al NIS2 due standard sono in evidenza: ISO/IEC 27001 e ISO 22301.

- L'implementazione di un Information Security Management System (ISMS) conforme alla norma ISO/IEC 27001 consente alle organizzazioni di ridurre al minimo i rischi e l'esposizione alle minacce alla sicurezza. Comporta l'identificazione delle policy necessarie, l'impiego di tecnologie adeguate e la formazione del personale per prevenire gli errori. Imponendo valutazioni annuali del rischio, ISO/IEC 27001 consente alle organizzazioni di affrontare in modo proattivo il panorama dei rischi in evoluzione.
- ISO/IEC 27001 non solo facilita il rispetto dei requisiti NIS2, ma consente anche alle organizzazioni di ottenere una certificazione con audit indipendente. Questa certificazione serve come prova tangibile per i fornitori, gli stakeholder e le autorità di regolamentazione, dimostrando che sono state adottate misure tecniche e organizzative "appropriate e proporzionate" e determinando un vantaggio competitivo sul mercato.
- Per le organizzazioni che desiderano un approccio evoluto è raccomandata anche l'adozione della ISO 22301 per la gestione della business continuity. La ISO 22301 aiuta a implementare, mantenere e migliorare continuamente le pratiche di business continuity. Mentre ISO/IEC 27001 incorpora aspetti di business continuity management (BCM), ISO 22301 fornisce un processo definito per l'implementazione del BCM. La certificazione rispetto alla ISO 22301 rafforza ulteriormente la conformità al NIS2.

La sinergia tra ISO/IEC 27001 e ISO 22301 consente alle organizzazioni di sviluppare un sistema di gestione integrato che comprenda sia un ISMS che un BCMS. Questo approccio olistico non solo aiuta nel conseguire la conformità, ma favorisce anche lo sviluppo di una solida resilienza informatica.

Perché BSI?

I clienti si possono affidare con fiducia a BSI e alle sue ampie capacità in materia di cybersecurity e igiene informatica. Offriamo una profonda esperienza nella cybersecurity, nella gestione del rischio e nella resilienza delle informazioni, con un punto di vista globale che abbraccia i diversi settori. La nostra expertise copre diverse tematiche che riguardano il settore pubblico, le minacce emergenti e l'esperienza pratica del settore nella gestione del rischio informatico e della resilienza.

Quali sono i prossimi passi?

- Verificare se l'organizzazione rientra nell'ambito di applicazione
- Informare il management /il CdA dell'imminente recepimento della normativa
- Contattarci, per avere supporto nella conformità NIS2: **marketing.italy@bsigroup.com**