REGIONE PIEMONTE

CSI your digital partner

WEBINAR
SICURI di essere SICURI?

NIS2: le misure di sicurezza

NIS2 e d.lgs. 138/2024: Impatti sulla Supply Chain e Responsabilità

Avv. Maria Livia Rizzo Studio Legale Stefanelli & Stefanelli

Il contesto normativo europeo: la Direttiva NIS2

Evoluzione normativa

La Direttiva (UE) 2022/2555 (NIS2), rappresenta l'evoluzione della precedente NIS1.

Mira a innalzare il livello di cybersicurezza su scala europea.

Obiettivi principali

Rafforzare la resilienza e le capacità di risposta agli incidenti cyber.

Stabilire un quadro normativo armonizzato tra tutti gli Stati membri.

Il recepimento italiano: d.lgs. 138/2024

1. ### Pubblicazione ufficiale

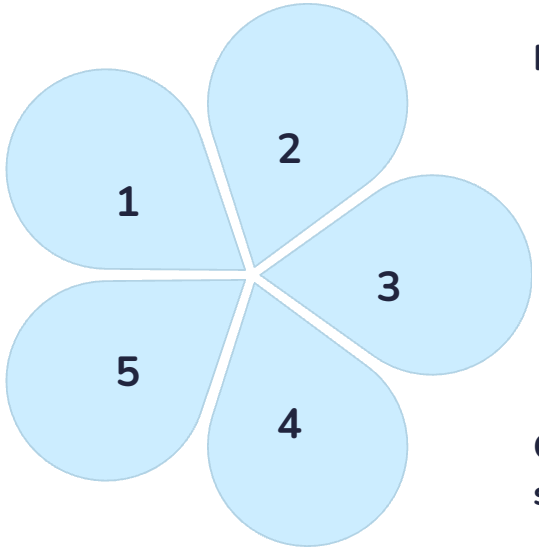
   Il decreto è stato pubblicato in Gazzetta Ufficiale il 4 ottobre 2024.

2. ### Recepimento formale

   Integra la NIS2 nell'ordinamento giuridico italiano.

Gli adempimenti chiave della normativa

Misure di gestione dei rischi di cybersecurity



Formazione

Sicurezza della supply chain

Gestione degli incidenti di sicurezza

Audit e monitoraggio

Considerando 85 Direttiva NIS2

Affrontare i **rischi derivanti dalla catena di approvvigionamento di un soggetto e dalla sua relazione con i fornitori,** ad esempio i fornitori di servizi di conservazione ed elaborazione dei dati o di servizi di sicurezza gestiti e gli editori di software, è particolarmente importante data la prevalenza di incidenti in cui i soggetti sono stati vittime di attacchi informatici e in cui i responsabili di atti malevoli sono stati in grado di compromettere la sicurezza dei sistemi informatici e di rete di un soggetto sfruttando le vulnerabilità che interessano prodotti e servizi di terzi. I soggetti essenziali e importanti dovrebbero pertanto valutare e tenere in considerazione la qualità e la resilienza complessive dei prodotti e dei servizi, delle **misure di gestione dei rischi di cibersicurezza** in essi integrate e delle pratiche di cibersicurezza dei loro fornitori e fornitori di servizi, comprese le loro procedure di sviluppo sicuro. In particolare, i soggetti essenziali e importanti dovrebbero essere incoraggiati a **integrare misure di gestione dei rischi di cibersicurezza negli accordi contrattuali** con i loro fornitori e fornitori di servizi diretti. Tali soggetti potrebbero prendere in considerazione i rischi derivanti da altri livelli di fornitori e fornitori di servizi.

Supply chain & NIS2

La normativa impone ai soggetti essenziali e importanti di gestire la sicurezza della catena di approvvigionamento, includendo i rapporti con i propri fornitori e sub-fornitori

Fornitori che, pur non essendo direttamente soggetti NIS2, sono elementi sistemici della catena di approvvigionamento, digitale o non, di soggetti essenziali o importanti.

Fornitori che erogano servizi ICT critici ai soggetti NIS2 quali imprese collegate o che forniscono beni e servizi che possono impattare la sicurezza dei sistemi informativi dei soggetti NIS2

Art. 24 Decreto 138/2024

2. Le misure di cui al comma 1 sono basate su un approccio multi-rischio, volto a proteggere i **sistemi informativi e di rete nonché il loro ambiente fisico** da incidenti, e comprendono almeno i seguenti elementi:

[...] d) sicurezza della catena di approvvigionamento, ivi compresi gli aspetti relativi alla sicurezza riguardanti i rapporti tra ciascun soggetto e i suoi diretti fornitori o fornitori di servizi;

Procedure di onboarding e monitoraggio continuo

Valutazione preventiva

Assessment di sicurezza preliminare sui nuovi fornitori.

Contrattualizzazione

Integrazione di clausole specifiche di cybersecurity.

Monitoraggio periodico

Riesame completo dei requisiti in base al rischio.

Esiti del monitoraggio

Eventuale esigenza di rivalutare il fornitore

Valutazione preventiva

Valutazione sull'out-sourcing

Analisi costi-benefici-rischi

Definizione dei requisiti

Individuazione e documentazione dei criteri di scelta da considerare in fase di selezione dei fornitori

Qualifica iniziale

Questionari, richiesta di documentazione, audit, riunioni, ricerca di informazioni

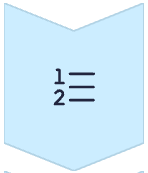
Criticità

Fornitore imposto dal cliente o dalla capogruppo, fornitore monopolista.

Contratti con i fornitori: le clausole da inserire

- Conformità alle normative applicabili in tema di sicurezza informatica
- Requisiti di sicurezza tecnica e organizzativa
- Regolamentazione attività di audit presso fornitore/supply chain e azioni conseguenti
- Gestione dei sub-fornitori
- Obbligo di disclosure delle vulnerabilità e delle minacce
- Formazione e sensibilizzazione
- Accordi di condivisione delle informazioni
- Piani di gestione degli incidenti e resilienza operativa
- Polizze assicurative, penali e risoluzione per inadempimento

Mappatura e classificazione dei fornitori esistenti



Identificazione

Censimento di tutti i fornitori dell'organizzazione.

Categorizzazione

Classificazione in base al livello di criticità.

Rivalutazione del rischio

In base ai parametri introdotti dalla NIS2 per verificare che i fornitori rispettino i requisiti di sicurezza aggiornati

Ricontrattualizzazione o aggiornamento contrattuale

Inserimento di clausole specifiche che impongano la conformità ai requisiti di sicurezza previsti dalla NIS2

Rivalutazione periodica

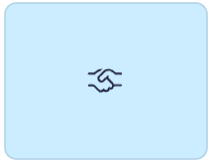
Estensione del perimetro della fornitura

Modifiche a processi, sistemi, normativa

Controlli di routine

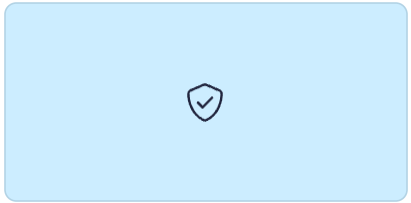
Incidenti, provvedimenti, criticità emerse da audit

Se l'esito della valutazione è negativo



Valutare la strategicità del fornitore

Verifica dell'impatto della sua esclusione o sostituzione



Richiesta al fornitore di attuazione di misure correttive

Adeguamento ai requisiti di sicurezza, controlli aggiuntivi, aggiornamento procedure, ottenimento certificazioni, rinegoziazione contratto, monitoraggio e rivalutazione

Ricerca di fornitori alternativi

Criticità: Fornitore imposto dal cliente o dalla capogruppo, fornitore monopolista, costi di uscita elevati

Offboarding del fornitore

Revoca accessi, recupero o eliminazione i dati, risoluzione lacune di sicurezza e documentazione azioni intraprese

Obblighi degli organi amministrativi e direttivi

Supervisione attiva

I vertici devono garantire la supervisione diretta sulla compliance NIS2.

Decisioni strategiche

Il board deve essere coinvolto nelle scelte di sicurezza dell'organizzazione.

Approvazione policy

Gli amministratori approvano formalmente le policy di cybersecurity.

Formazione

I vertici sono chiamati a seguire e a promuovere una formazione periodica in materia di sicurezza informatica

Formazione

Art. 23 comma 2 lett. b) Decreto 138/2024

Deve favorire l'acquisizione di conoscenze e competenze **sufficienti** al fine di **individuare** i rischi e valutare le pratiche di **gestione** dei rischi per la sicurezza informatica e il loro **impatto sulle attività** del soggetto e sui servizi offerti.

Rischi sanzionatori per le organizzazioni

Sanzioni amministrative pecuniarie

Le sanzioni amministrative previste dal d.lgs. 138/2024 possono raggiungere **fino al 2% del fatturato globale annuo dell'esercizio precedente se superiore, con un massimo di 10 milioni di euro** per i soggetti essenziali e 7 milioni per i soggetti importanti.

Sospensione temporanea di certificati o autorizzazioni

Se un soggetto non adempie nei termini stabiliti da una diffida dell'ACN (Art. 37, commi 6 e 7), la ACN può sospendere temporaneamente o chiedere a un organismo di certificazione/autorizzazione o a un organo giurisdizionale di sospendere un certificato o un'autorizzazione relativi a servizi o attività del **soggetto essenziale.**

Rischi reputazionali

Oltre alle sanzioni dirette, le violazioni comportano significativi rischi reputazionali per l'azienda, con potenziali azioni di responsabilità per i danni conseguenti.

Rischi sanzionatori e responsabilità personale

Responsabilità degli amministratori

Gli organi di amministrazione, i legali rappresentanti e i dirigenti responsabili possono essere soggetti a **sospensione temporanea dall'esercizio delle funzioni dirigenziali** in caso di violazioni degli obblighi imposti dal decreto. La sospensione dura fino a quando l'ente non adotta le misure necessarie a porre rimedio alle carenze riscontrate dall'Agenzia per la Cybersicurezza Nazionale (ACN) o non si conforma alle prescrizioni impartite.

Rischi reputazionali

Oltre alle sanzioni dirette, le violazioni comportano significativi rischi reputazionali per i vertici aziendali, con potenziali azioni di responsabilità per i danni conseguenti.

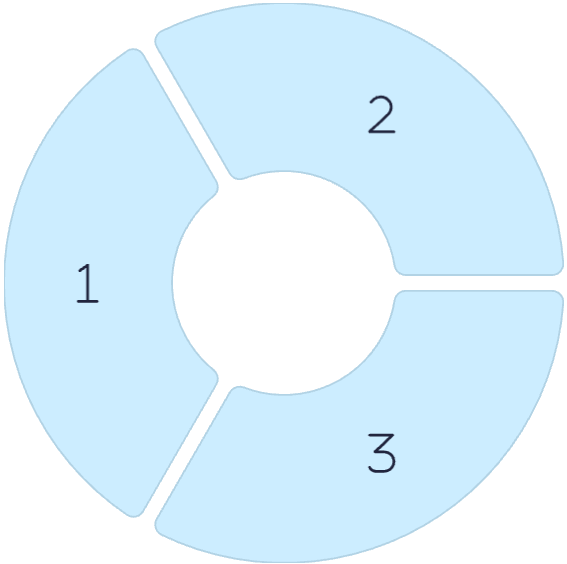
Responsabilità dei dipendenti pubblici

Ai manager pubblici si applicano le norme in materia di responsabilità disciplinare e amministrativo-contabile dei dipendenti pubblici.

Organi amministrativi e direttivi e accountability

Documentazione delle attività di compliance

Analisi dei rischi, misure adottate e relativa efficacia, rapporti di audit, formazione, contrattualistica e gestione dei rapporti con la catena di fornitura, incidenti e misure correttive, …



Archiviazione efficace

Consente di dare conto agevolmente del proprio operato

Elenco aggiornato norme vigenti

Documentare la presa in carico di una nuova norma o motivare la non applicabilità

EU Cybersecurity Strategy

- Direttiva NIS2 (Network and Information Security Directive 2)
- Cyber Resilience Act
- Cybersecurity Act
- Direttiva CER (Critical Entity Resilience)
- Regolamento DORA (Digital Operational Resilience Act)

“La rivoluzione digitale accade una volta sola, e cioè adesso”

Luciano Floridi

Grazie

www.studiolegalestefanelli.it

Le nostre risorse online

STEFANELLI & STEFANELLI STUDIO LEGALE