22 novembre 2024

Cenni sulla compliance alla normativa NIS2 sulla Cybersicurezza

Avv. Alberto Rigoni
ModernLex

Avv. Maria Margherita Parini
ModernLex

Luigi Pandolfino
Coordinatore Azure Meetup Veneto

Andrea Marchi
Moderatore

veneto@azuremeetup.it

Il gruppo nasce con l'obiettivo di creare una community per la condivisione di informazioni ed esperienze su **Microsoft Azure** e **365**.

Si rivolge a professionisti del settore IT ma anche ad appassionati di tecnologia, studenti e imprenditori interessati ad approfondire le **soluzioni cloud** e **ibride messe** a disposizione da **Microsoft**.

azuremeetup VENETO

meetup

Microsoft

veneto@azuremeetup.it

Sessioni tecniche in **presenza** ed eventi dedicati al mondo **Microsoft**

Webinar con esperti di tecnologie **Microsoft**

| Cosa facciamo |

azuremeetup VENETO

meetup Microsoft

veneto@azuremeetup.it

Prossimo evento: **10 dicembre 2024**

«Ogni docker è bello a mamma sua! Dopo due lustri di containerizzazione a che punto siamo?»

Giuliano Latini

«Artigiano d'infrastrutture IT»

| Call4Speaker |

D.LGS. 138/2024
di recepimento della Direttiva UE 2022/255 sulla cybersicurezza

Avv. Alberto Rigoni – Avv. Maria Margherita Parini

www.modernlex.com

Oggetto del Decreto

- L'**Articolo 1** del Decreto Legislativo 138/2024 (il «**Decreto**») di recepimento della **Direttiva UE 2022/2055 NIS II (Network and Information Security)** definisce le misure volte a garantire un livello elevato di sicurezza informatica a livello nazionale e a contribuire alla sicurezza comune nell'Unione Europea, migliorando il funzionamento del mercato interno.

- Gli obiettivi specifici includono:

  - **Strategia nazionale di cybersicurezza**, che prevede azioni per assicurare un'elevata sicurezza informatica.
  - **Integrazione del quadro di gestione delle crisi informatiche** all'interno dell'organizzazione nazionale.
  - **Conferma dell'Agenzia per la Cybersicurezza Nazionale** come autorità nazionale competente per la gestione della sicurezza informatica e le sue funzioni di coordinamento a livello nazionale e internazionale.
  - **Designazione delle Autorità di Settore NIS** per collaborare con l'Agenzia nel garantire l'applicazione delle misure di sicurezza informatica.
  - **Obblighi specifici in materia di sicurezza e di notifica degli incidenti** in capo ai soggetti a cui si applica la normativa

Definizioni Art. 2 (esempi)

- **Autorità nazionale competente NIS**: l'Agenzia per la cybersicurezza nazionale, che ha il compito di far rispettare le misure di sicurezza stabilite dal decreto.
- **Punto di contatto unico NIS**: un organismo che coordina le attività di sicurezza informatica tra le diverse autorità italiane e quelle di altri paesi.
- **CSIRT Italia**: il team italiano di risposta agli incidenti di sicurezza informatica, incaricato di intervenire in caso di attacchi cibernetici.
- **Autorità di settore NIS**: Autorità settoriali che collaborano con l'Agenzia per la cybersicurezza nell'applicazione delle misure di sicurezza.
- **Incidente**: un evento che compromette la disponibilità, autenticità, integrità o riservatezza dei dati o dei servizi informatici.
- **Minaccia informatica**: qualsiasi evento o azione che potrebbe danneggiare o disturbare i sistemi informatici.

Definizioni Art. 2

- **Quasi-incidente (Near-miss)**: un evento che avrebbe potuto diventare un incidente informatico, ma che è stato evitato.
- **Incidente di sicurezza informatica su vasta scala**: un incidente che causa una perturbazione talmente grande da superare la capacità di risposta di uno Stato membro o che ha un impatto significativo su almeno due Stati membri.
- **Gestione degli incidenti**: azioni e procedure per prevenire, rilevare, analizzare, contenere e rispondere agli incidenti informatici, oltre a recuperare da essi.
- **Rischio**: la combinazione del danno potenziale causato da un incidente e la probabilità che esso si verifichi.
- **Minaccia informatica**: Qualsiasi evento o azione che potrebbe danneggiare o disturbare i sistemi informatici o gli utenti.
- **Minaccia informatica significativa**: Una minaccia che potrebbe avere un grave impatto sui sistemi informativi e causare perdite considerevoli.
- **Approccio multi-rischio**: Un approccio che considera tutti i tipi di minacce, come furti, incendi o interruzioni, che possono influenzare i sistemi informativi.

AMBITO APPLICAZIONE DEL DECRETO

- Rilevante ampliamento rispetto all'ambito di applicazione della NIS 1 e del relativo decreto di attuazione
- Introduzione di una distinzione tra soggetti essenziali e importanti (non prevista dalla NIS 1)

Art. 3

- Soggetti sia pubblici che privati della tipologia di cui agli allegati I, II, III e IV
  - L’allegato I descrive i settori considerati come altamente critici
  - L’allegato II descrive i settori considerati come critici
  - L’allegato III descrive le categorie di Pubbliche amministrazioni alle quali si applica il decreto
  - L’allegato IV descrive le ulteriori tipologie di soggetti a cui si applica il decreto

IMPRESE INTERESSATE

Requisiti dimensionali soggetti delle tipologie di cui agli allegati 1 e 2

Il decreto si applica ai soggetti di cui agli allegati 1 e 2 che superano i massimali per le piccole imprese ai sensi dell'art. 2, par. 2 dell'allegato della raccomandazione 2003/361 CE, ovvero che:

- occupano più di 50 persone
- o realizzano un fatturato annuo o un totale di bilancio annuo superiori a 10 milioni di euro

Piccole imprese – come individuarle

- I dati impiegati per calcolare gli effettivi e gli importi finanziari sono quelli riguardanti l'ultimo esercizio contabile chiuso e vengono calcolati su base annua. L'importo del fatturato è calcolato al netto dell'imposta sul valore aggiunto (IVA) e di altri diritti o imposte indirette.
- Per le **imprese autonome** (ovvero le imprese che non possono qualificarsi come associate o collegate) i dati, compresi quelli relativi agli effettivi, vengono dedotti dai conti dell'impresa stessa.
- **Se invece le imprese possono considerarsi come collegate o associate per verificare i dati bisogna effettuare verifiche che tengano in considerazione anche le imprese associate o collegate (!!!)**

Soggetti allegato 1 (settori ad alta criticità)

Settori	Sottosettore	Tipologia di soggetto
Energia	Energia elettrica, teleriscaldamento e raffrescamento, petrolio, gas, idrogeno	Specifici soggetti individuati
Trasporti	Aereo, ferroviario, per vie d'acqua, su strada	Specifici soggetti individuati
Settore bancario		Enti creditizi
Infrastrutture mercati finanziari		Specifici soggetti individuati
Settore sanitario		Specifici soggetti individuati
Acqua potabile		Specifici soggetti individuati

(segue) Soggetti allegato 1

Settori	Sottosettore	Tipologia di soggetto
Acque Reflue		Specifici soggetti individuati
Infrastrutture digitali		Segue slide specifica
Gestione servizi TIC		Fornitori di servizi gestiti, fornitori di servizi di sicurezza gestiti
Spazio		Specifici soggetti individuati

Specifica: infrastrutture digitali

Fornitori di punti interscambio internet
Fornitura di servizi sistema dei nomi di dominio (DNS)
Gestori di registri dei nomi di dominio di primo livello (top level domain - TLD)
Fornitori di servizi di cloud computing
Fornitori di servizi di data center
Fornitori di reti di distribuzione dei contenuti (c.d. content delivery network)
Prestatori di servizi fiduciari
Fornitori di reti

Soggetti allegato 2 (altri soggetti critici)

Settori	Sottosettore	Tipologia di soggetto
Servizi postali e di corriere		Specifici soggetti
Gestione rifiuti		Specifici soggetti
Fabbricazione, produzione e distribuzione di sostanze chimiche		Specifici soggetti
Produzione, trasformazione e distribuzione di alimenti		Specifici soggetti
Fabbricazione	Vari sottosettori	Specifici soggetti
Fornitori servizi digitali		Fornitori di mercati on line, fornitori di motori di ricerca on line, fornitori di servizi registrazione nomi a dominio
Ricerca		Organizzazioni di ricerca

IRRILEVANZA DEL FATTORE DIMENSIONALE NEI SEGUENTI CASI:

Indipendentemente dalle dimensioni il decreto si applica (art. 3.5):

a. ai soggetti identificati come critici dal decreto che recepisce la Dir. CER
b. ai fornitori di reti pubbliche di comunicazione elettronica o servizi di comunicazione elettronica accessibili al pubblico,
c. ai prestatori di servizi fiduciari,
d. ai gestori di registri dei nomi di dominio di primo livello, fornitori di servizi di sistema dei nomi di dominio e di registrazione dei nomi di dominio,

IMPRESE COLLEGATE A SOGGETTI ESSENZIALI O IMPORTANTI

Il decreto si applica a prescindere dalle dimensioni alle imprese collegate ad un soggetto essenziale o importante, se soddisfa almeno uno dei seguenti criteri:

- a) adotta decisioni o esercita una influenza dominante sulle decisioni relative alle misure di gestione del rischio per la sicurezza informatica di un soggetto importante o essenziale;
- b) detiene o gestisce sistemi informativi e di rete da cui dipende la fornitura dei servizi del soggetto importante o essenziale;
- c) effettua operazioni di sicurezza informatica del soggetto importante o essenziale; d) fornisce servizi TIC o di sicurezza, anche gestiti, al soggetto importante o essenziale.

Ulteriori soggetti essenziali o importanti

Ulteriori soggetti essenziali o importanti potrebbero essere individuati in futuro secondo specifiche procedure

- si raccomanda di consultare il sito periodicamente il sito ACN per l'ambito di registrazione: https://www.acn.gov.it/portale/nis/ambito-registrazione

Schema di ambito applicazione NIS2 in Italia

- Stando a quanto riportato ad oggi nel sito NCS: https://www.acn.gov.it/portale/documents/d/guest/faq-1-5_dettaglio-ambiti-di-applicazione

Allegato I: Settori ad alta criticità

Settore	Sottosettore o tipologia di soggetto	Grandi imprese (occupano almeno 250 dipendenti oppure hanno un fatturato di almeno 50M€ oppure hanno un bilancio di almeno 43M€)	Medie imprese (occupano almeno 50 dipendenti oppure hanno un fatturato di almeno 10M€ oppure hanno un bilancio di almeno 10M€)	Piccole e micro imprese
1. Energia	1. Energia elettrica 2. Teleriscaldamento e teleraffrescamento 3. Petrolio 4. Gas 5. Idrogeno	Essenziali	Importanti[1]	Non in ambito[2]
2. Trasporti	1. Trasporto aereo 2. Trasporto ferroviario 3. Trasporto per vie d'acqua 4. Trasporto su strada			
3. Settore bancario	1. Enti creditizi quali definiti all'articolo 4, punto 1), del regolamento (UE) n. 575/2013 del Parlamento europeo e del Consiglio **(DORA lex specialis)**			
4. Infrastrutture dei mercati finanziari	1. Gestori delle sedi di negoziazione quali definiti all'articolo 4, punto 24), della direttiva 2014/65/UE del Parlamento europeo e del Consiglio 2. Controparti centrali (CCP) quali definite all'articolo 2, punto 1), del regolamento (UE) n. 648/2012 del Parlamento europeo e del Consiglio **(DORA lex specialis)**			
5. Settore sanitario	1. Prestatori di assistenza sanitaria quali definiti all'articolo 3, lettera g), della direttiva 2011/24/UE del Parlamento europeo e del Consiglio 2. Laboratori di riferimento dell'UE quali definiti all'articolo 15 del regolamento (UE) 2022/2371 del Parlamento europeo e del Consiglio 3. Soggetti che svolgono attività di ricerca e sviluppo relative ai medicinali quali definiti all'articolo 1, punto 2), della direttiva 2001/83/CE del Parlamento europeo e del Consiglio 4. Soggetti che fabbricano prodotti farmaceutici di base e preparati farmaceutici di cui alla sezione C, divisione 21, della NACE Rev. 2 5. Soggetti che fabbricano dispositivi medici considerati critici durante un'emergenza di sanità pubblica (elenco dei dispositivi critici per l'emergenza di sanità pubblica) di cui all'articolo 22 del regolamento (UE) 2022/123 del Parlamento europeo e del Consiglio			
6. Acqua potabile	1. Fornitori e distributori di acque destinate al consumo umano, quali definiti all'articolo 2, punto 1, lettera a), della direttiva (UE) 2020/2184 del Parlamento europeo e del Consiglio, ma esclusi i distributori per i quali la distribuzione di acque destinate al consumo umano è una parte non essenziale dell'attività generale di distribuzione di altri prodotti e beni			
7. Acque reflue	1. Imprese che raccolgono, smaltiscono o trattano acque reflue urbane, domestiche o industriali quali definite all'articolo 2, punti da 1), 2) e 3), della direttiva 91/271/CEE del Consiglio, escluse le imprese per cui la raccolta, lo smaltimento o il trattamento di acque reflue urbane, domestiche o industriali è una parte non essenziale della loro attività generale			

8. Infrastrutture digitali	1. Fornitori di punti di interscambio Internet (Internet exchange point – IXP)	Essenziali	Importanti[1]	Non in ambito[2]
	2. Fornitori di servizi di sistema dei nomi di dominio (domain name system – DNS), esclusi gli operatori dei server dei nomi radice 3. Gestori di registri dei nomi di dominio di primo livello (top level domain – TLD)	Essenziali		
	4. Fornitori di servizi di cloud computing 5. Fornitori di servizi di data center 6. Fornitori di reti di distribuzione dei contenuti (content delivery network – CDN)	Essenziali	Importanti[1]	Non in ambito[2]
	7. Prestatori di servizi fiduciari qualificati e non qualificati	Essenziali	Essenziali i servizi fiduciari qualificati/Importanti[1] quelli non qualificati	
	8. Fornitori di reti pubbliche di comunicazione elettronica 9. Fornitori di servizi di comunicazione elettronica accessibili al pubblico	Essenziali		Importanti[1]
9. Gestione dei servizi TIC (business-to-business)	1. Fornitori di servizi gestiti 2. Fornitori di servizi di sicurezza gestiti	Essenziali	Importanti[1]	Non in ambito[2]
10. Spazio	1. Operatori di infrastrutture terrestri possedute, gestite e operate dagli Stati membri o da privati, che sostengono la fornitura di servizi spaziali, esclusi i fornitori di reti pubbliche di comunicazione elettronica	Essenziali	Importanti[1]	Non in ambito[2]

Allegato II: altri settori critici

1. Servizi postali e di corriere	1. Fornitori di servizi postali quali definiti all'articolo 2, punto 1 bis), della direttiva 97/67/CE, tra cui i fornitori di servizi di corriere	**Importanti[1]**	**Non in ambito[2]**
2. Gestione dei rifiuti	1. Imprese che si occupano della gestione dei rifiuti quali definite all'articolo 3, punto 9), della direttiva 2008/98/CE del Parlamento europeo e del Consiglio, escluse quelle per cui la gestione dei rifiuti non è la principale attività economica		
3. Fabbricazione, produzione e distribuzione di sostanze chimiche	1. Imprese che si occupano della fabbricazione di sostanze e della distribuzione di sostanze o miscele di cui all'articolo 3, punti 9) e 14), del regolamento (CE) n. 1907/2006 del Parlamento europeo e del Consiglio e imprese che si occupano della produzione di articoli quali definite all'articolo 3, punto 3), del medesimo regolamento, da sostanze o miscele		
4. Produzione, trasformazione e distribuzione di alimenti	1. Imprese alimentari quali definite all'articolo 3, punto 2), del regolamento (CE) n. 178/2002 del Parlamento europeo e del Consiglio che si occupano della distribuzione all'ingrosso e della produzione industriale e trasformazione		
5. Fabbricazione	1. Fabbricazione di dispositivi medici e di dispositivi medico-diagnostici in vitro 2. Fabbricazione di computer e prodotti di elettronica e ottica 3. Fabbricazione di apparecchiature elettriche 4. Fabbricazione di macchinari e apparecchiature n.c.a. 5. Fabbricazione di autoveicoli, rimorchi e semirimorchi 6. Fabbricazione di altri mezzi di trasporto		
6. Fornitori di servizi digitali	1. Fornitori di mercati online 2. Fornitori di motori di ricerca online 3. Fornitori di piattaforme di social network		
	4. Fornitori di servizi di registrazione dei nomi di dominio	**Importanti[1]**	
7. Ricerca	1. Organizzazioni di ricerca	**Importanti[1]**	**Non in ambito[2]**

Allegato III: Amministrazioni centrali, regionali, locali e di altro tipo

Pubbliche Amministrazioni	Amministrazioni centrali: 1. Gli Organi costituzionali e di rilievo costituzionale 2. La Presidenza del Consiglio dei ministri e i Ministeri 3. Le Agenzie fiscali 4. Le Autorità amministrative indipendenti	**Essenziali**
	Amministrazioni regionali: 1. Le Regioni e le Province autonome	**Importanti[1]**
	Amministrazioni locali: 1. Le Città metropolitane 2. I Comuni con popolazione superiore a 100.000 abitanti 3. I Comuni capoluoghi di regione 4. Le Aziende sanitarie locali	
	Altri soggetti pubblici: 1. Gli Enti di regolazione dell'attività economica 2. Gli Enti produttori di servizi economici 3. Gli Enti a struttura associativa 4. Gli Enti produttori di servizi assistenziali, ricreativi e culturali 5. Gli Enti e le Istituzioni di ricerca 6. Gli Istituti zooprofilattici sperimentali	

Allegato IV: Ulteriori tipologie di soggetti

Ulteriori tipologie di soggetti	1. Soggetti che forniscono servizi di trasporto pubblico locale	**Soggetti a eventuale individuazione dell'Autorità**
	2. Istituti di istruzione che svolgono attività di ricerca	
	3. Soggetti che svolgono attività di interesse culturale	
	4. Società in house, società partecipate e società a controllo pubblico, come definite nel decreto legislativo 19 agosto 2016, n.175	

[1] Possibile individuazione dell'Autorità come essenziali
[2] Possibile individuazione dell'Autorità come importanti o essenziali

Soggetti essenziali

Sono considerati soggetti **essenziali**:

- **Imprese di grandi dimensioni** elencate nell'allegato I che superano i massimali previsti per le medie imprese, secondo la raccomandazione 2003/361/CE. Ad esempio, una grande società energetica o una banca che eccede le soglie delle medie imprese rientrerebbe in questa categoria.
- **Soggetti critici indipendentemente dalle dimensioni**, identificati come tali secondo il decreto che recepisce la direttiva UE 2022/2557. Un esempio potrebbe essere un ospedale che, anche se di piccole dimensioni, svolge un ruolo cruciale per la salute pubblica.
- **Fornitori di reti pubbliche e servizi di comunicazione elettronica** che sono considerati medie imprese. Ad esempio, un operatore di telecomunicazioni che fornisce accesso a Internet rientrerebbe tra i soggetti essenziali.
- **Prestatori di servizi fiduciari qualificati** (come i fornitori di firma digitale) e **gestori di registri di domini di primo livello**. Indipendentemente dalle loro dimensioni, queste entità sono considerate essenziali per la sicurezza informatica.
- **Pubbliche amministrazioni centrali**, come i ministeri, che devono garantire la protezione delle proprie infrastrutture digitali.

Soggetti importanti

- I **soggetti importanti** includono tutte le entità indicate che non sono classificate come essenziali. Per esempio, un’azienda che offre servizi di cloud storage di piccole dimensioni potrebbe essere considerata un soggetto importante anziché essenziale, pur dovendo rispettare normative sulla sicurezza informatica
- **I soggetti essenziali e importanti sono in ogni caso soggetti agli obblighi alla normativa, fatto salvo le sanzioni (v. slide successive)**

Soggetti essenziali e importanti

- Per il settore informatico, un esempio concreto potrebbe essere:
  - una società media (> 50 dipendenti o > 10M€ fatturato) che fornisce servizi cloud → soggetto essenziale
  - un piccolo fornitore di servizi IT che gestisce l'infrastruttura critica di un ospedale → soggetto essenziale indipendentemente dalle dimensioni
  - una media società di consulenza IT che fornisce servizi non critici → soggetto importante
  - un piccolo sviluppatore software senza clienti critici e sotto le soglie dimensionali → non rientra nell'ambito

Agenzia per la Cybersicurezza Nazionale

- **L'Agenzia per la Cybersicurezza Nazionale ha il compito di:**
  - identificare i soggetti essenziali e importanti secondo i criteri e le modalità stabiliti;
  - gestire la piattaforma per l'elencazione di tali soggetti e fornire un riscontro sulla conformità delle comunicazioni effettuate dai soggetti, con un termine massimo di 90 giorni;
  - stabilire le modalità di aggiornamento delle liste di soggetti essenziali e importanti e fornire le linee guida per il rispetto delle misure di sicurezza;
  - coordinare le attività di risposta agli incidenti informatici
  - operare come punto di contatto unico per le comunicazioni con l'UE;
  - sovrintendere l'implementazione della strategia nazionale;
  - monitorare il rispetto delle misure di sicurezza e può effettuare ispezioni, anche senza preavviso, presso i soggetti essenziali e importanti per garantire la conformità agli obblighi previsti dalla normativa.

Autorità di settore

- **Autorità di settore NIS**
  - Le Autorità di settore NIS sono identificate per supportare l'Agenzia per la Cybersicurezza Nazionale nella gestione delle minacce specifiche per settori particolarmente critici, come le telecomunicazioni, l'energia, la finanza e i trasporti.

CSIRT

- **CSIRT Italia**
  - Il CSIRT Italia (Computer Security Incident Response Team) è il gruppo designato per monitorare e rispondere agli incidenti informatici a livello nazionale. Ha il compito di analizzare, prevenire e mitigare gli incidenti di sicurezza, oltre a coordinare gli sforzi con altri CSIRT europei e internazionali.

- **Divulgazione coordinata delle vulnerabilità**
  - Il CSIRT Italia è incaricato della gestione della divulgazione coordinata delle vulnerabilità, facilitando il dialogo tra i soggetti che rilevano vulnerabilità e i fornitori di servizi o prodotti TIC interessati. Il CSIRT agisce come intermediario per garantire che le vulnerabilità siano gestite e divulgate in modo sicuro e responsabile, minimizzando i rischi per la sicurezza nazionale.

Misure per la gestione della sicurezza informatica

- **Adozione di misure proporzionate**
  - **I soggetti essenziali e importanti** devono adottare misure tecniche, operative e organizzative adeguate e proporzionate per gestire i rischi per la sicurezza dei sistemi informativi e di rete utilizzati nelle loro attività. Tali misure devono prevenire o ridurre al minimo l'impatto degli incidenti per i destinatari dei servizi e per altri servizi correlati. Le misure devono:
    - assicurare un livello di sicurezza dei sistemi informativi e di rete adeguato ai rischi esistenti, tenendo conto delle conoscenze più aggiornate, dello stato dell'arte e, ove applicabile, delle norme nazionali, europee e internazionali, nonché dei costi di attuazione.
    - essere proporzionate al grado di esposizione ai rischi del soggetto, alle sue dimensioni, alla probabilità che si verifichino incidenti e alla loro gravità, compreso l'impatto sociale ed economico.

Misure per la gestione della sicurezza informatica

- **Componenti delle misure di sicurezza :** le misure devono seguire un approccio multi-rischio, volto a proteggere i sistemi informativi e di rete, nonché il loro ambiente fisico. Queste misure devono comprendere **almeno** i seguenti elementi:
  - **Politiche di analisi dei rischi e di sicurezza** per i sistemi informativi e di rete.
  - **Gestione degli incidenti**, incluse le procedure e gli strumenti per le notifiche di incidenti, come previsto dagli articoli 25 e 26.
  - **Continuità operativa**, compresa la gestione dei backup, il ripristino in caso di disastro e la gestione delle crisi.
  - **Sicurezza della catena di approvvigionamento**, che includa la gestione della sicurezza nei rapporti con fornitori di servizi e fornitori diretti.
  - **Sicurezza dell'acquisizione, sviluppo e manutenzione** dei sistemi informativi e di rete, con gestione e divulgazione delle vulnerabilità.

Misure per la gestione della sicurezza informatica

- ✓ **Politiche e procedure** per valutare l'efficacia delle misure di gestione dei rischi.
- ✓ **Pratiche di igiene di base e formazione** in materia di sicurezza informatica.
- ✓ **Politiche sull'uso della crittografia**, inclusa la cifratura, ove opportuno.
- ✓ **Sicurezza e affidabilità del personale**, politiche di controllo dell'accesso e gestione dei beni.
- ✓ **Uso di soluzioni di autenticazione a più fattori** o autenticazione continua, e comunicazioni sicure per emergenze.

Misure per la gestione della sicurezza informatica

- **Sicurezza della catena di approvvigionamento**
  - Quando si valutano le misure di sicurezza per la catena di approvvigionamento, i soggetti devono considerare le vulnerabilità specifiche dei fornitori e la qualità complessiva dei loro prodotti e pratiche di sicurezza, comprese le procedure di sviluppo sicuro. Devono anche tenere conto dei risultati delle valutazioni di sicurezza delle catene di approvvigionamento critiche condotte dal Gruppo di cooperazione NIS.
- **Conformità e azioni correttive**
  - Se un soggetto rileva di non essere conforme alle misure stabilite, deve adottare senza indebito ritardo tutte le misure correttive necessarie, che siano appropriate e proporzionate alla violazione riscontrata.
- **Formazione periodica del personale**

Obblighi in materia di notifica di incidente (cenni art. 25)

- **Notifica di incidenti significativi: i soggetti essenziali e importanti** devono notificare al CSIRT Italia ogni incidente che ha un impatto significativo sulla fornitura dei loro servizi. Questa notifica deve avvenire senza ingiustificato ritardo
- **Contenuto della notifica**: la notifica deve includere tutte le informazioni necessarie per permettere al CSIRT Italia di determinare un possibile impatto transfrontaliero dell'incidente.
- **Responsabilità**: la notifica non aumenta la responsabilità del soggetto notificante oltre a quella già derivante dall'incidente.
- **Criteri di significatività.** Un incidente è considerato significativo se:
  - ha causato o è in grado di causare gravi perturbazioni operative o perdite finanziarie per il soggetto;
  - ha o potrebbe avere impatti su altre persone fisiche o giuridiche, causando perdite materiali o immateriali significative.
- **Procedure di notifica. L**e fasi della notifica sono:
  - entro 24 ore dal riconoscimento dell'incidente significativo, viene inviata una pre-notifica che include informazioni preliminari e, se possibile, una valutazione iniziale.
  - entro 72 ore, viene inviata una notifica più completa con una valutazione dell'incidente;
  - se richiesto, vengono fornite relazioni intermedie e una relazione finale entro un mese dalla notifica iniziale.

Obblighi in materia di notifica di incidente (cenni art. 25)

- Qualora si sospetti che l'incidente significativo abbia carattere criminale, il CSIRT Italia fornisce al soggetto notificante anche orientamenti sulla segnalazione dell'incidente significativo, all'organo centrale del Ministero dell'interno per la sicurezza e per la regolarità dei servizi
- Sentito il CSIRT Italia, se ritenuto opportuno e qualora possibile, i soggetti essenziali e i soggetti importanti comunicano, senza ingiustificato ritardo, ai destinatari dei loro servizi gli incidenti significativi che possono ripercuotersi negativamente sulla fornitura di tali servizi.
- L'Agenzia per la cybersicurezza nazionale, nello svolgimento delle funzioni di Autorità nazionale competente NIS e di CSIRT Italia, anche sentendo, se del caso, le autorità competenti e gli CSIRT nazionali degli altri Stati membri interessati, può informare il pubblico riguardo all'incidente significativo per evitare ulteriori incidenti significativi o per gestire un incidente significativo in corso, o qualora ritenga che la divulgazione dell'incidente significativo sia altrimenti nell'interesse pubblico

Notificazione volontaria

- Oltre agli obblighi di notifica, i soggetti possono volontariamente segnalare al CSIRT Italia anche quasi-incidenti o minacce informatiche rilevanti, anche se non hanno avuto un impatto diretto sulla fornitura dei servizi. Le notifiche volontarie saranno trattate dal CSIRT in base alle stesse procedure delle notifiche obbligatorie, ma avranno una priorità inferiore.

Certificazioni

- **Certificazione di prodotti, servizi e processi TIC**
  - I soggetti essenziali e importanti sono incoraggiati ad utilizzare prodotti, servizi e processi TIC certificati secondo standard di sicurezza riconosciuti, per garantire l'integrità e la protezione delle infrastrutture informatiche.
  - Inoltre, l'Autorità nazionale competente NIS, secondo le modalità previste dal Decreto, può imporre ai soggetti essenziali e ai soggetti importanti di utilizzare categorie di prodotti TIC, servizi TIC e processi TIC, sviluppati dal soggetto essenziale o importante o acquistati da terze parti, che siano certificati nell'ambito di schemi di certificazione riconosciuti a livello nazionale o europeo

Organi di amministrazione e direttivi (art. 23)

- **Approvazione e supervisione:**
  - gli organi di amministrazione e direttivi devono approvare le modalità di implementazione delle misure di gestione dei rischi per la sicurezza informatica (art. 24 Decreto), sovrintendere all'implementazione degli obblighi per la gestione dei rischi informatici e per la protezione delle infrastrutture digitali.
- **Formazione obbligatoria:**
  - è richiesto che questi organi ricevano una formazione specifica in materia di sicurezza informatica per essere adeguatamente preparati ad affrontare i rischi. Oltre alla propria formazione, devono promuovere regolarmente corsi di formazione per i dipendenti,
- **Informazione su incidenti e notifiche:**
  - gli organi direttivi devono essere informati periodicamente o tempestivamente, quando necessario, sugli incidenti di sicurezza e sulle notifiche rilevanti, permettendo loro di intervenire prontamente in caso di minacce.
- **Responsabilità:**
- **sono ritenuti responsabili di eventuali violazioni del Decreto**, quindi sono chiamati a rispondere direttamente di mancanze o inefficienze nella gestione della sicurezza informatica

Sanzioni

- **Sanzioni per i soggetti essenziali**: I soggetti essenziali che violano gli obblighi sono puniti con una sanzione amministrativa pecuniaria che può raggiungere il 2% del fatturato annuo su scala mondiale o fino a 10 milioni di euro, a seconda di quale dei due importi sia maggiore.
- **Sanzioni per i soggetti importanti**: Le violazioni da parte di soggetti importanti possono essere punite con una multa fino all'1,4% del fatturato annuo globale o fino a 7 milioni di euro.
- **Sanzioni per le pubbliche amministrazioni**: Per le pubbliche amministrazioni che violano gli obblighi di sicurezza informatica, le multe possono variare da 25.000 a 125.000 euro per i soggetti essenziali. Per i soggetti importanti, le multe vengono ridotte di un terzo rispetto ai soggetti essenziali.
- Incapacità sanzionatoria
- **Reiterazione delle violazioni**: In caso di violazioni ripetute, le sanzioni possono essere raddoppiate. Nei casi più gravi, è previsto l'aumento fino al triplo della sanzione per la violazione più grave.
- **Procedimento sanzionatorio**: L'Autorità nazionale competente (Agenzia per la Cybersicurezza Nazionale) **può disporre la sospensione temporanea dei servizi** o delle attività per i soggetti non conformi, finché non adottano le misure necessarie per rimediare alle carenze.

RESPONSABILITA' PERSONALI

I componenti dell'organo amministrativo o direttivo e le persone che rappresentano il soggetto essenziale o il soggetto importante potrebbero essere soggetti a sanzioni e responsabilità personali in caso di inosservanza degli enti alle richieste di regolarizzazione formalizzate dall'Autorità nazionale competente NIS. Potrebbe essere comminata

La sanzione accessoria dell'incapacità di svolgere funzioni dirigenziali all'intero del medesimo soggetto

Monitoraggio, vigilanza, sanzioni

- **Vigilanza e controlli**: l'Autorità NIS monitora che i soggetti rispettino le regole, richiedendo informazioni, facendo ispezioni e verificando i sistemi informatici. Le ispezioni possono essere fatte anche senza preavviso.
- **Sanzioni**: se un soggetto non rispetta le regole, può essere multato. Le sanzioni possono essere in base al fatturato o fisse, a seconda della gravità della violazione.
- **Misure correttive**: l'Autorità può anche imporre misure per correggere le violazioni, come l'adozione di specifiche azioni di sicurezza o, nei casi gravi, sospendere temporaneamente i servizi del soggetto.
- **Ricorsi**: i soggetti sanzionati possono fare ricorso contro le decisioni prese dall'Autorità, sia tramite una revisione interna che ricorrendo a un giudice.
- **Cooperazione internazionale**: quando un incidente coinvolge più Stati, l'Autorità collabora con le autorità di altri paesi per coordinare la risposta e condividere risorse e informazioni.

Fase di prima applicazione

- Registrazione su Piattaforma Digitale: entro il 28 febbraio 2025, i fornitori gli enti pubblici e privati a cui si applica la NIS 2 devono registrarsi sulla piattaforma digitale prevista dall'art. 7 (disponibile dal 1° dicembre 2024) fornendo i dati richiesti e secondo le procedure previste dall'articolo
- A valle della fase di registrazione, nel mese di aprile 2025, i soggetti che si sono registrati riceveranno una comunicazione per confermare, o meno, il loro l'inserimento nell'elenco dei soggetti NIS.
- Sino al 31 dicembre 2025, il termine per l'adempimento degli obblighi di cui all'articolo 25 (obbligo di notifica degli incidenti) e' fissato in nove mesi dalla ricezione della comunicazione di cui al precedente paragrafo
- Per adempiere agli obblighi relativi agli artt. 23, 24, e 29 (obblighi in capo agli Organi di Amministrazione e direttivi, obblighi in materia di misure di gestione per la sicurezza informatica, obblighi relativi alla banca dati di registrazione dei nomi di domini), i soggetti hanno fino a 18 mesi dalla comunicazione di registrazione per conformarsi.

Elencazione, caratterizzazione e categorizzazione delle attività e dei servizi (art. 30)

- 1. **Comunicazione annuale**: Dal 1° maggio al 30 giugno di ogni anno, i soggetti essenziali e importanti devono comunicare e aggiornare, tramite una piattaforma digitale, l'elenco delle loro attività e servizi, includendo elementi necessari alla caratterizzazione e attribuendo una categoria di rilevanza.
- 2. **Definizione delle categorie**: L'Autorità nazionale competente NIS stabilisce le categorie di rilevanza, il processo, le modalità e i criteri per l'elencazione, caratterizzazione e categorizzazione, seguendo quanto previsto dall'articolo 40 e tenendo conto dell'articolo 25.
- 3. **Verifica e riscontro**: Entro 90 giorni dalla comunicazione, l'Autorità verifica la conformità di quanto comunicato. Questo termine può essere prorogato una sola volta fino a 60 giorni per approfondimenti. Se richieste integrazioni, i termini si interrompono fino alla ricezione delle informazioni, che devono essere fornite entro 30 giorni.
- 4. **Convalida tacita**: Se l'Autorità non fornisce riscontro entro i termini, la conformità si intende convalidata.
- 5. **Collaborazione**: L'Autorità può avvalersi dei tavoli settoriali per supportare il processo.

Alcuni consigli dello Studio

- Creazione di una policy aziendale che rispetti tutti i requisiti della normativa, con coinvolgimento di un legale al fine di assicurare la miglior compliance
- Consigliamo la creazione di un team interno (o anche con membri esterni) dedicato alla cybersicurezza
- Riteniamo che l'assesment (valutazione dei rischi e azioni correttive) vada fatto da un fornitore terzo, in quanto soggetto indipendente.
- Collaborazione tra legali specializzati e IT, interni ed esterni (indipendenti)
- Consultazione anche del NIST Cybersecurity Framework (di matrice americana ma spesso usato anche in Italia)