ISACA®

Sistemi informativi: averne fiducia e trarne valore

Rome Chapter

NIS2 (Network and Information Security)

03/02/2025

PREMESSA

La sicurezza Informatica al 100% NON esiste

Le moderne tecniche di attacco sono sempre più difficili da individuare.
Poter controllare tutti i possibili accessi e tutte le vulnerabilità dell'infrastruttura in tempo utile e intercettare qualsiasi tipo di attacco è solo utopia.

In una realtà in cui comunichiamo attraverso decine di piattaforme diverse, deleghiamo funzioni e servizi al cloud e viviamo connessi 24 ore su 24, pensare di "chiudere" gli spazi per eventuali attacchi è pura fantasia.

Non sappiamo quando, come o dove, sappiamo solo che l'attacco prima o poi arriverà.

l'unico modo per annullare qualsiasi rischio di un attacco sarebbe quello di staccare il cavo di rete e rinunciare all'utilizzo di Internet.

PREMESSA

Le norme e le leggi in materia di cybersicurezza
NON POSSONO ESSERE
Solo Compliance.
Solo documenti riempitivi (fuffa).
Solo certificazioni fini a se stesse.

Servono per farci ragionare, per farci essere più consapevoli, per farci migliorare, per aumentare l'efficienza

E' necessario inoltre impostare le ***EVIDENZE*** effettive
Per la verifica che le misure e le soluzioni siano efficaci e funzionali.
Per il miglioramento continuo della protezione in ambito Cyber Security.

Riferimenti Normativi e Best Practices

- **NIS2**

Le norme dell'UE in materia di cibersicurezza introdotte nel 2016 sono state aggiornate dalla direttiva ***NIS2***, entrata in vigore nel 2023.
Ha modernizzato il quadro giuridico esistente per tenere il passo con una maggiore digitalizzazione e un panorama in evoluzione delle minacce alla cibersicurezza.

Estendendo l'ambito di applicazione delle norme in materia di cibersicurezza a ***nuovi settori e entità***, migliora ulteriormente la resilienza e le capacità di risposta agli incidenti degli ***enti pubblici e privati, delle autorità competenti*** e dell'UE nel suo complesso.

Riferimenti Normativi e Best Practices

I framework più diffusi evidenziano come ognuno sia **focalizzato su un particolare aspetto o su uno specifico approccio** per il governo della sicurezza IT.

I framework servono principalmente ad **orientare l'organizzazione dei modelli operativi**, suggerendo come identificare e utilizzare gli elementi necessari, risultando funzionali al governo della sicurezza IT perché si fondano su presupposti pratici, regole e principi chiaramente definiti.

L 333/164 IT Gazzetta ufficiale dell'Unione europea 27.12.2022

DIRETTIVA (UE) 2022/2557 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO
del 14 dicembre 2022
del Parlamento europeo e del Consiglio relativa alla resilienza dei soggetti critici e che abroga la direttiva 2008/114/CE del Consiglio

(Testo rilevante ai fini del SEE)

IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea, in particolare l'articolo 114,

vista la proposta della Commissione europea,

previa trasmissione del progetto di atto legislativo ai parlamenti nazionali,

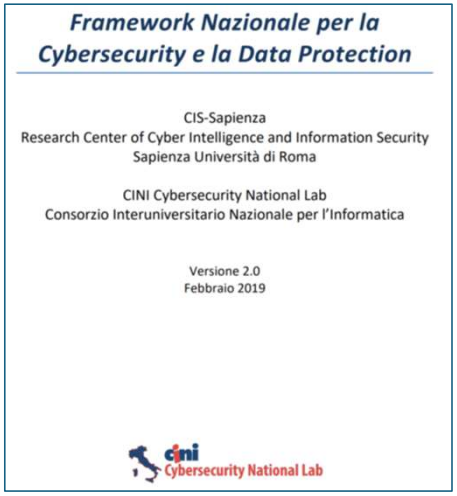
visto il parere del Comitato economico e sociale europeo (1),

visto il parere del Comitato delle regioni (2),

deliberando secondo la procedura legislativa ordinaria (3),

considerando quanto segue:

(1) In quanto fornitori di servizi essenziali, i soggetti critici svolgono un ruolo indispensabile per il mantenimento di funzioni vitali della società o di attività economiche nel mercato interno in un'economia dell'Unione sempre più interdipendente. È pertanto essenziale definire un quadro a livello dell'Unione volto sia a rafforzare la resilienza dei soggetti critici nel mercato interno, stabilendo norme minime armonizzate, sia ad assistere tali soggetti mediante



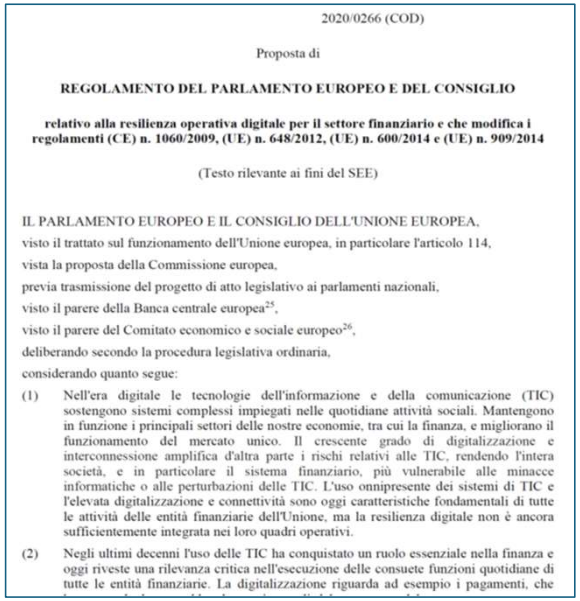
Framework Nazionale per la Cybersecurity e la Data Protection

CIS-Sapienza
Research Center of Cyber Intelligence and Information Security
Sapienza Università di Roma

CINI Cybersecurity National Lab
Consorzio Interuniversitario Nazionale per l'Informatica

Versione 2.0
Febbraio 2019

cini Cybersecurity National Lab



2020/0266 (COD)

Proposta di

REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014 e (UE) n. 909/2014

(Testo rilevante ai fini del SEE)

IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea, in particolare l'articolo 114,

vista la proposta della Commissione europea,

previa trasmissione del progetto di atto legislativo ai parlamenti nazionali,

visto il parere della Banca centrale europea[25],

visto il parere del Comitato economico e sociale europeo[26],

deliberando secondo la procedura legislativa ordinaria,

considerando quanto segue:

(1) Nell'era digitale le tecnologie dell'informazione e della comunicazione (TIC) sostengono sistemi complessi impiegati nelle quotidiane attività sociali. Mantengono in funzione i principali settori delle nostre economie, tra cui la finanza, e migliorano il funzionamento del mercato unico. Il crescente grado di digitalizzazione e interconnessione amplifica d'altra parte i rischi relativi alle TIC, rendendo l'intera società, e in particolare il sistema finanziario, più vulnerabile alle minacce informatiche o alle perturbazioni delle TIC. L'uso onnipresente dei sistemi di TIC e l'elevata digitalizzazione e connettività sono oggi caratteristiche fondamentali di tutte le attività delle entità finanziarie dell'Unione, ma la resilienza digitale non è ancora sufficientemente integrata nei loro quadri operativi.

(2) Negli ultimi decenni l'uso delle TIC ha conquistato un ruolo essenziale nella finanza e oggi riveste una rilevanza critica nell'esecuzione delle consuete funzioni quotidiane di tutte le entità finanziarie. La digitalizzazione riguarda ad esempio i pagamenti, che

Riferimenti Normativi e Best Practices

- **Framework Nazionale – NIST**

Metodologia di cybersecurity assesment basata sul ***Framework Nazionale***, ovvero un percorso che le organizzazioni possono seguire per applicare lo stesso al contesto di riferimento e misurare la propria postura in termini di cybersecurity. Tale metodologia introduce diversi elementi innovativi, strutturando le sue attività in tre fasi: **Contestualizzazione, Misurazione, Valutazione**.

- **ISO 27001/2 - 2022**
- **Implementare, gestire e controllare un Sistema di Gestione della Sicurezza della Informazioni**

ISO 27001:2022 è lo standard internazionale che descrive le best practice per un **ISMS (sistema di gestione della sicurezza delle informazioni, anche detto SGSI, in italiano)**.
La certificazione ISO 27001 permette di dimostrare che l' azienda sta seguendo le best practice sulla sicurezza delle informazioni e fornisce un controllo indipendente e qualificato sul fatto che la sicurezza delle informazioni è gestita in linea con le best practice internazionali e gli obiettivi aziendali.

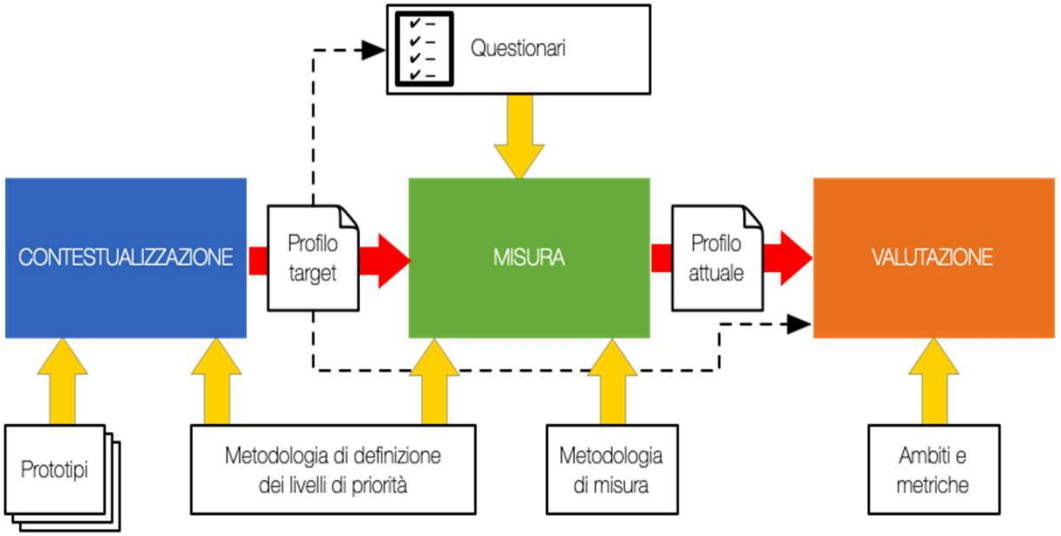
Un SGSI è un sistema di processi, documenti, tecnologie e persone che aiutano a gestire, monitorare, controllare e migliorare la sicurezza delle informazioni dell'azienda attraverso una gestione del rischio efficiente.

Riferimenti Normativi e Best Practices

• **Contestualizzazione**: in questa fase la metodologia seleziona e valuta, in termini di priorità e maturità, le sottocategorie del Framework Nazionale di interesse rispetto alla realtà di riferimento.

• **Misura (Gap Analysis)**: in questa fase si rileva la distanza tra lo stato attuale e lo stato desiderato. Uno o più intervistatori provvedono, tramite l'utilizzo di questionari a valutare il livello di raggiungimento e realizzazione dei controlli individuati.

• **Valutazione**: nella fase finale è possibile leggere i risultati ottenuti nella fase precedente tramite una valutazione della distanza tra il profilo attuale e il profilo target. Il risultato si sostanzia in un punteggio di completamento delle azioni individuate



FONTE: https://www.cybersecurityframework.it/sites/default/files/Metodologia_Assessment_Framework_Nazionale_-_v1.0.pdf

https://www.nist.gov/cyberframeworkhttps://www.nist.gov/cyberframework

NIS2 (Network and Information Security)

NIS 2 (Direttiva UE 2022/2055) è entrata in vigore il **17 gennaio 2023.**
NIS2 dovrà essere recepita dall'Italia entro **l'ottobre 2024**.

La direttiva NIS2 è una normativa a livello dell'UE **sulla cybersicurezza**. Il suo obiettivo è creare un comune livello di cybersicurezza in tutti gli Stati membri dell'Unione europea. Si propone di armonizzare le misure e gli approcci per proteggere le infrastrutture digitali, in questo caso, con l'uso delle «best practice» per affrontare il crescente aumento di attacchi informatici.

NIS2 (Network and Information Security)

L'applicabilità dipende da settore e dimensione.
La NIS2 è applicabile a:
soggetti essenziali;
soggetti importanti.
Ulteriori soggetti potrebbero essere aggiunti dalla normativa nazionale.

Le entità dovranno riconoscersi come soggetti a cui è applicabile la NIS 2, non è più l'autorità che le designa come tali.
Le entità si dovranno registrare secondo regole che saranno fornite.
Entro il **17 aprile 2025**, gli Stati membri definiranno un elenco dei soggetti.

CAPO I	DISPOSIZIONI GENERALI
Articolo 1	Oggetto e ambito di applicazione
Articolo 2	Ambito di applicazione
Articolo 3	Soggetti essenziali e importanti
Articolo 4	Atti giuridici settoriali dell'Unione
Articolo 5	Armonizzazione minima
Articolo 6	Definizioni
CAPO II	QUADRI COORDINATI IN MATERIA DI CIBERSICUREZZA
Articolo 7	Strategia nazionale per la cibersicurezza
Articolo 8	Autorità competenti e punti di contatto unici
Articolo 9	Quadri nazionali di gestione delle crisi informatiche
Articolo 10	Team di risposta agli incidenti di sicurezza informatica (CSIRT)
Articolo 11	Requisiti, capacità tecniche e compiti dei CSIRT
Articolo 12	Divulgazione coordinata delle vulnerabilità e banca dati europea delle vulnerabilità
Articolo 13	Cooperazione a livello nazionale
CAPO III	COOPERAZIONE A LIVELLO DELL'UNIONE E INTERNAZIONALE
Articolo 14	Gruppo di cooperazione
Articolo 15	Rete di CSIRT
Articolo 16	Rete europea delle organizzazioni di collegamento per le crisi informatiche (EU-CyCLONe)
Articolo 17	Cooperazione internazionale
Articolo 18	Relazione sullo stato della cibersicurezza nell'Unione
Articolo 19	Revisioni tra pari
CAPO IV	MISURE DI GESTIONE DEL RISCHIO DI CIBERSICUREZZA E OBBLIGHI DI SEGNALAZIONE
Articolo 20	Governance
Articolo 21	Misure di gestione dei rischi di cibersicurezza
Articolo 22	Valutazioni coordinate a livello dell'Unione del rischio per la sicurezza delle catene di approvvigionamento critiche
Articolo 23	Obblighi di segnalazione
Articolo 24	Uso dei sistemi europei di certificazione della cibersicurezza
Articolo 25	Normazione
CAPO V	GIURISDIZIONE E REGISTRAZIONE
Articolo 26	Giurisdizione e territorialità
Articolo 27	Registro dei soggetti
Articolo 28	Banca dati dei dati di registrazione dei nomi di dominio
CAPO VI	CONDIVISIONE DELLE INFORMAZIONI
Articolo 29	Accordi di condivisione delle informazioni sulla cibersicurezza
Articolo 30	Notifica volontaria di informazioni pertinenti
CAPO VII	VIGILANZA ED ESECUZIONE
Articolo 31	Aspetti generali relativi alla vigilanza e all'esecuzione
Articolo 32	Misure di vigilanza e di esecuzione relative a soggetti essenziali
Articolo 33	Vigilanza ed esecuzione relative a soggetti essenziali
Articolo 34	Condizioni generali per imporre sanzioni amministrative pecuniarie ai soggetti essenziali e importanti
Articolo 35	Violazioni che comportano una violazione dei dati personali
Articolo 36	Sanzioni
Articolo 37	Assistenza reciproca
CAPO VIII	ATTI DELEGATI E ATTI DI ESECUZIONE
Articolo 38	Esercizio della delega
Articolo 39	Procedura di comitato
CAPO IX	DISPOSIZIONI FINALI
Articolo 40	Riesame
Articolo 41	Recepimento
Articolo 42	Modifica del regolamento (UE) n. 910/2014
Articolo 43	Modifica della direttiva (UE) 2018/1972
Articolo 44	Abrogazione
Articolo 45	Entrata in vigore
Articolo 46	Destinatari

Di Interesse	Utili per lavorazione attivtà
Di Interesse Parziale	Quando la direttiva non è diretta ad attività da fare, ma i soggetti sono compunque interessati a sapere
Perimetro Nazionale	Riguardanti solo le attività che deve svolgere lo stato/nazione

NIS2 (Network and Information Security)

CAPO I	DISPOSIZIONI GENERALI
Articolo 2	Ambito di applicazione
Articolo 3	Soggetti essenziali e importanti
Articolo 6	Definizioni
CAPO II	QUADRI COORDINATI IN MATERIA DI CIBERSICUREZZA
CAPO III	COOPERAZIONE A LIVELLO DELL'UNIONE E INTERNAZIONALE
CAPO IV	MISURE DI GESTIONE DEL RISCHIO DI CIBERSICUREZZA E OBBLIGHI DI SEGNALAZIONE
Articolo 20	Governance
Articolo 21	Misure di gestione dei rischi di cibersicurezza
Articolo 23	Obblighi di segnalazione
CAPO V	GIURISDIZIONE E REGISTRAZIONE
CAPO VI	CONDIVISIONE DELLE INFORMAZIONI
Articolo 30	Notifica volontaria di informazioni pertinenti
CAPO VII	VIGILANZA ED ESECUZIONE
Articolo 32	Misure di vigilanza e di esecuzione relative a soggetti essenziali
Articolo 33	Vigilanza ed esecuzione relative a soggetti essenziali
Articolo 34	Condizioni generali per imporre sanzioni amministrative pecuniarie ai soggetti essenziali e importanti
Articolo 36	Sanzioni
CAPO VIII	ATTI DELEGATI E ATTI DI ESECUZIONE
CAPO IX	DISPOSIZIONI FINALI

NIS2 - ambito di riferimento

Identificare se l'organizzazione rientra nell'ambito della NIS2

La NIS2 si applica ai soggetti pubblici o privati indicati negli allegati I e II.

• imprese con più di 250 dipendenti o fatturato annuo maggiore di 50 milioni di euro (o un bilancio annuo superiore a 43 milioni di euro);
• medie imprese con un numero compreso fra 50 e 250 dipendenti o un fatturato annuo compreso fra 10 e 50 milioni di euro, (o con bilancio annuo non superiore a 43 milioni di euro);
• pubbliche amministrazioni;
• categorie di soggetti: quali piccole imprese, (vedi allegati I e II della NIS2).

Se l'organizzazione rientra nell'ambito, si devono fornire alle autorità competenti (punto di contatto unico, che le inoltra a ENISA), i seguenti dettagli di contatto:
• nome del soggetto, settore, sottosettore e tipo di soggetto;
• l'indirizzo di tutti gli stabilimenti legali del soggetto (o del suo rappresentante);
• dati di contatto aggiornati, inclusi indirizzi e-mail e numeri di telefono;
• gli Stati membri in cui il soggetto fornisce i suoi servizi;

Le informazioni devono essere aggiornate entro tre mesi da qualsivoglia modifica.

NIS 2 – Settori di applicazione

Settori ad ALTA CRITICITÀ
1. Energia
2. Trasporti
3. Settore bancario
4. Infrastrutture dei mercati finanziari
5. Settore sanitario
6. Acqua potabile
7. Acque reflue
8. Infrastrutture di gitali
9. Gestione dei ser vizi TIC (business-to-business)
10. Pubblica amministrazione
11. Spazio

ALTRI Settori Critici
1. Servizi postali e di corriere
2. Gestione dei rifiuti
3. Fabbricazione, produzione e distribuzione di sostanze chimiche
4. Produzione, trasformazione e distribuzione di alimenti
5. Fabbricazione

NIS 2 – Settori di applicazione

Settore	Sottosettore	Tipo di soggetto
1. Energia	a) Energia elettrica	— Impresa elettrica quale definita all'articolo 2, punto 57), della direttiva (UE) 2019/944 del Parlamento europeo e del Consiglio(1)che esercita attività di «fornitura» quale definita all'articolo 2, punto 12), di tale direttiva — Gestori del sistema di distribuzione quali definiti all'articolo 2, punto 29), della direttiva (UE) 2019/944 — Gestori del sistema di trasmissione quali definiti all'articolo 2, punto 35), della direttiva (UE) 2019/944 — Produttori quali definiti all'articolo 2, punto 38), della direttiva (UE) 2019/944 — Gestori del mercato elettrico designato quali definiti all'articolo 2, punto 8), del regolamento (UE) 2019/943 —Partecipanti al mercato dell'energia elettrica quali definiti all'articolo 2, punto 25), del regolamento (UE) 2019/943 che forniscono servizi di aggregazione, gestione della domanda o stoccaggio di energia —Gestori di un punto di ricarica responsabili della gestione e del funzionamento di un punto di ricarica che fornisce un servizio di ricarica a utenti finali, anche in nome e per conto di un fornitore di servizi di mobilità
	b) Teleriscaldamento e teleraffrescamento	— Gestori di teleriscaldamento o teleraffrescamento quali definiti all'articolo 2, punto 19), della direttiva (UE) 2018/2001 del Parlamento europeo e del Consiglio(3)
	c) Petrolio	— Gestori di oleodotti, — Gestori di impianti di produzione, raffinazione, trattamento, deposito e trasporto di petrolio — Organismi centrali di stoccaggio quali definiti all'articolo 2, lettera f), della direttiva 2009/119/CE del Consiglio(4)
	d) Gas	— Imprese fornitrici quali definite all'articolo 2, punto 8), della direttiva 2009/73/CE del Parlamento europeo — Gestori del sistema di distribuzione quali definiti all'articolo 2, punto 6), della direttiva 2009/73/CE — Gestori del sistema di trasporto quali definiti all'articolo 2, punto 4), della direttiva 2009/73/CE — Gestori dell'impianto di stoccaggio quali definiti all'articolo 2, punto 10), della direttiva 2009/73/CE — Gestori del sistema GNL quali definiti all'articolo 2, punto 12), della direttiva 2009/73/CE — Imprese di gas naturale quali definite all'articolo 2, punto 1), della direttiva 2009/73/CE; — Gestori di impianti di raffinazione e trattamento di gas naturale
	e) Idrogeno	— Gestori di impianti di produzione, stoccaggio e trasporto di idrogeno

NIS2 - requisiti di sicurezza e gestione del rischio

Comprendere i requisiti di sicurezza, compresa la gestione del rischio e le valutazioni periodiche

L'articolo 21 della NIS2, da indicazione agli Stati membri, affinché i soggetti essenziali e importanti adottino misure tecniche, operative e organizzative adeguate e proporzionate per la gestione dei rischi della sicurezza dei sistemi informatici e di rete utilizzati nelle loro attività o nella fornitura dei loro servizi, per prevenire o ridurre al minimo l'impatto degli incidenti.

Queste misure si basano su un approccio multirischio che includa almeno i seguenti elementi :

le politiche per l'implementazione della sicurezza informatica (o igiene informatica / cyber hygiene) che comprendono l'adozione delle best-practice richieste dalla direttiva NIS2 per l'attuazione di strategie efficaci di cybersecurity e cyber resilience.

considerando (79)
...in linea con le norme europee e internazionali, come quelle di cui alla serie ISO/IEC 27000...

DIRETTIVA NIS 2 – Adeguamento

ART. 21.2 a)	ART. 21.2 b)	ART. 21.2 c)	ART. 21.2 d)	ART. 21.2 e)
Politiche di analisi dei rischi e di sicurezza dei sistemi informatici;	Gestione degli incidenti;	Continuità operativa, come la gestione del backup e il ripristino in caso di disastro, e gestione delle crisi;	Sicurezza della catena di approvvigionamento (supply chain), compresi aspetti relativi alla sicurezza riguardanti i rapporti con i suoi diretti fornitori	Sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informatici e di rete, compresa la gestione delle vulnerabilità;

ART. 21.2 f)	ART. 21.2 g)	ART. 21.2 h)	ART. 21.2 i)	ART. 21.2 j)
Strategie e procedure per valutare l'efficacia delle misure di gestione dei rischi di cibersicurezza;	Pratiche di igiene informatica di base e formazione in materia di cibersicurezza;	Politiche e procedure relative all'uso della crittografia e, se del caso, della cifratura;	Sicurezza delle risorse umane, strategie di controllo dell'accesso e gestione degli asset;	Uso di soluzioni di autenticazione a più fattori o di autenticazione continua, di comunicazioni vocali, video e testuali protette e di sistemi di comunicazione di emergenza protetti da parte del soggetto

METODOLOGIE DI ATTUAZIONE (IMPLEMENTAZIONE)

Sul sito di ACN, sezione NIS, sono pubblicate risorse quali:
La timeline di applicazione
Le FAQ: https://www.acn.gov.it/portale/faq/nis
Ad esempio "Dopo essermi registrato sulla piattaforma di ACN sarò un soggetto NIS?".

QUINDI, COME SI ADEGUA L' ORGANIZZAZIONE ALLE DIRETTIVE PRECEDENTEMENTE INDICATE ?

DI SEGUITO ALCUNI ESEMPI DI IMPLEMENTAZIONE ATTRAVERSO LE PRINCIPALI BEST PRACTICES

NIS2 - valutazione dei sistemi informatici

Effettuare una valutazione dei sistemi informatici e della catena di approvvigionamento per identificare potenziali minacce e vulnerabilità

• **Valutare la sicurezza** per identificare vulnerabilità come password non gestite o account configurati in modo errato o dormienti che sono suscettibili di furto di credenziali.
• **Analizzare le attuali difese contro le principali minacce** cyber, attacchi ransomware, tentativi di intrusione, furto dati
• **Verificare la catena di** approvvigionamento (supply chain): integrare misure di gestione dei rischi di cibersicurezza negli accordi contrattuali con i fornitori dei sistemi e dei servizi.
• Effettuare **revisione delle misure di sicurezza esistenti per adeguarle ai requisiti della direttiva NIS2**.
• **Valutare se le politiche di gestione dei rischi**, i processi di protezione dei dati e le procedure di risposta agli incidenti **sono adeguate e aggiornate**.
• **Verificare le misure con le best practice indicate dalla direttiva**, inclusa **la governance della sicurezza e la formazione continua** del personale e **implementare miglioramenti con audit periodici e aggiornamenti delle politiche** per aumentare il livello di resilienza contro le minacce informatiche.
• Implementare **il processo per segnalare alle autorità designate gli incidenti informatici significativi**, che includa tempestività e informazioni adeguate per consentire alle autorità di valutare l'incidente e fornire supporto

ISO27001/2

DIRETTIVA NIS 2 – ASSESMENT e APPLICAZIONE ISO27001/2 (Esempio)

TITOLO NIS2	CONTROLLI ISO27001-2
Articolo 21 - Punto 2	
a) politiche di analisi dei rischi e di sicurezza dei sistemi informatici;	5.2 - Ruoli e responsabilità per la sicurezza delle informazioni 5.8 - Sicurezza delle informazioni nella gestione dei progetti ISO 27001/22 - 6.1.2 Information security risk assessment ISO 27001/22 - 6.1.3 Information security risk treatment
b) gestione degli incidenti;	5.24 - Pianificazione e preparazione per la gestione degli incidenti relativi alla sicurezza delle informazioni 5.25 - Valutazione e decisione sugli eventi relativi alla sicurezza delle informazioni 5.26 - Risposta agli incidenti relativi alla sicurezza delle informazioni 5.27 - Apprendimento dagli incidenti relativi alla sicurezza delle informazioni 5.28 - Raccolta di evidenze
c) continuità operativa, come la gestione del backup e il ripristino in caso di disastro, e gestione delle crisi;	5.29 - Sicurezza delle informazioni durante le interruzioni 5.30 - Pianificazione della continuità della sicurezza delle informazioni 8.13 - Backup delle informazioni 8.14 - Ridondanza delle strutture di elaborazione delle informazioni
d) sicurezza della catena di approvvigionamento (supply chain), compresi aspetti relativi alla sicurezza riguardanti i rapporti tra ciascun soggetto e i suoi diretti fornitori o fornitori di servizi;	5.19 - Sicurezza delle informazioni nelle relazioni con i fornitori 5.20 - Indirizzare la sicurezza delle informazioni nelle relazioni con i fornitori 5.21 - Gestire la sicurezza delle informazioni nella filiera di fornitura per l'ICT 5.22 - Monitoraggio e riesame dei servizi dei fornitori 5.23 - Sicurezza delle informazioni per l'utilizzo di servizi cloud

DIRETTIVA NIS 2 – ASSESMENT e APPLICAZIONE ISO27001/2 (Esempio)

TITOLO NIS2	CONTROLLI ISO27001-2
e) sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informatici e di rete, compresa la gestione e la divulgazione delle vulnerabilità; Acquisizione e ciclo di vita asset	8.8 - Gestione delle vulnerabilità tecniche 8.20 - Sicurezza delle reti 8.25 - Ciclo di vita dello sviluppo sicuro 8.26 - Requisiti di sicurezza delle applicazioni 8.27 - Sicurezza dell'architettura dei sistemi e dei principi di ingegnerizzazione 8.28 - Sviluppo sicuro 8.29 - Test di sicurezza in fase di sviluppo e di accettazione 8.30 - Sviluppo affidato all'esterno 8.31 - Separazione degli ambienti di sviluppo, test e produzione
f) strategie e procedure per valutare l'efficacia delle misure di gestione dei rischi di cibersicurezza;	9.1 - Monitoraggio, misurazione, analisi e valutazione 9.2 - Audit interno 9.3 - Riesame della direzione 10.1 - Miglioramento continuo 5.35 - Riesame indipendente della sicurezza delle informazioni
g) pratiche di igiene informatica di base e formazione in materia di cibersicurezza;	Clause 7.2 ISO 27001 Competenze Clause 7.3 ISO 27001 Consapevolezza 6.3 - Consapevolezza, istruzione, formazione e addestramento sulla sicurezza delle informazioni

DIRETTIVA NIS 2 – ASSESMENT e APPLICAZIONE ISO27001/2 (Esempio)

TITOLO NIS2	CONTROLLI ISO27001-2
h) politiche e procedure relative all'uso della crittografia e, se del caso, della cifratura;	8.24 Uso della crittografia
i) sicurezza delle risorse umane, strategie di controllo dell'accesso e gestione degli asset;	5.9 - Inventario delle informazioni e degli altri asset relativi 5.10 - Uso accettabile delle informazioni e degli altri asset relativi 5.15 - Controllo degli accessi 5.16 - Gestione delle identità 5.17 - Informazioni di autenticazione 5.18 - Diritti d'accesso 6.1 - Screening 6.2 - Termini e condizioni di impiego 6.4 - Processo disciplinare 6.5 - Responsabilità dopo la cessazione o il cambio d'impiego 6.6 - Accordi di riservatezza o di non divulgazione
j) uso di soluzioni di autenticazione a più fattori o di autenticazione continua, di comunicazioni vocali, video e testuali protette e di sistemi di comunicazione di emergenza protetti da parte del soggetto al proprio interno, se del caso.	5.14 - Trasferimento delle informazioni" 5.16 - Gestione delle identità" 5.17 - Informazioni di autenticazione"

DIRETTIVA NIS 2 – ASSESMENT e APPLICAZIONE ISO27001/2 (Esempio)

TITOLO NIS2	CONTROLLI ISO27001-2	DESCRIZIONE CONTROLLO	FINALITA'	GUIDA
h) politiche e procedure relative all'uso della crittografia e, se del caso, della cifratura;	**8.24 Uso della crittografia**	Per l'uso efficace della crittografia dovrebbero essere definite e attuate regole, inclusa la gestione delle chiavi crittografiche.	Assicurare un uso corretto ed efficace della crittografia per proteggere la riservatezza, l'autenticità o l'integrità delle informazioni in base ai requisiti di business e di sicurezza delle informazioni e tenendo conto dei requisiti legali, statutari, normativi e contrattuali relativi alla crittografia.	**Generale** Quando si utilizza la crittografia, si deve considerare : a) la politica specifica per la crittografia definita dall'organizzazione, inclusi i principi generali per la protezione delle informazioni. b) identificare il livello di protezione richiesto e la classificazione delle informazioni e conseguentemente stabilire il tipo, la robustezza e la qualità degli algoritmi crittografici richiesti; c) l'uso della crittografia per la protezione delle informazioni conservate sugli endpoint mobili degli utenti o nei supporti di memorizzazione d) l'approccio alla gestione delle chiavi, comprese le modalità per gestire la generazione e protezione delle chiavi crittografiche; e) Definizione dei ruoli e responsabilità f) gli standard da adottare, nonché gli algoritmi crittografici, la robustezza della cifratura, le soluzioni crittografiche e le pratiche di impiego approvate o richieste per l'uso nell'organizzazione; g) l'impatto dell'utilizzo di informazioni cifrate sui controlli che si basano sull'ispezione dei contenuti

DIRETTIVA NIS 2 – MAPPING ISO27001/2 e FNCS (Esempio)

TITOLO NIS2	CONTROLLI ISO27002	DESCRIZIONE FNCS
Articolo 21 - Punto 2		
b) **gestione degli incidenti;**	5.24 - Pianificazione e preparazione per la gestione degli incidenti relativi alla sicurezza delle informazioni	**PR.IP-9: Sono attivi ed amministrati piani di risposta (Incident Response e Business Continuity) e recupero (Incident Recovery e Disaster Recovery) in caso di incidente/disastro**
	5.25 - Valutazione e decisione sugli eventi relativi alla sicurezza delle informazioni	**DE.AE-2: Gli eventi rilevati vengono analizzati per comprendere gli obiettivi e le metodologie dell'attacco** **DE.AE-4: Viene determinato l'impatto di un evento** **DE.AE-5: Vengono definite delle soglie di allerta per gli incidenti** **RS.AN-2: Viene compreso l'impatto di ogni incidente**
	5.26 - Risposta agli incidenti relativi alla sicurezza delle informazioni	**RS.RP-1: Esiste un piano di risposta (response plan) e questo viene eseguito durante o dopo un incidente** **RS.AN-1: Le notifiche provenienti dai sistemi di monitoraggio vengono sempre visionate e analizzate** **RS.MI-1: In caso di incidente vengono messe in atto procedure atte a contenerne l'impatto** **RS.MI-2: In caso di incidente vengono messe in atto procedure atte a mitigarne gli effetti** **RC.RP-1: Esiste un piano di ripristino (recovery plan) e viene eseguito dopo un incidente di cybersecurity**
	5.27 - Apprendimento dagli incidenti relativi alla sicurezza delle informazioni	**ID.RA-4: Sono identificati i potenziali impatti sul business e le relative probabilità di accadimento** **PR.IP-7: I processi di protezione sono sottoposti a miglioramenti** **PR.IP-8: L'efficacia delle tecnologie di protezione viene condivisa** **DE.DP-5: I processi di monitoraggio sono oggetto di periodici miglioramenti e perfezionamenti** **RS.AN-2: Viene compreso l'impatto di ogni incidente** **RS.IM-1: I piani di risposta agli incidenti tengono in considerazione le esperienze passate (lesson learned)** **RS.IM-2: Le strategie di risposta agli incidenti sono aggiornate** **RC.IM-1: I piani di ripristino tengono in considerazione le esperienze passate (lesson learned)** **RC.IM-2: Le strategie di recupero sono aggiornate**
	5.28 Raccolta di evidenze	**DE.AE-3: Le informazioni relative agli eventi sono raccolte e correlate da sensori e sorgenti multiple** **RS.AN-3: A seguito di un incidente viene svolta un'analisi forense** **DE.AE-3: Le informazioni relative agli eventi sono raccolte e correlate da sensori e sorgenti multiple**

Framework Nazionale – NIST

FNCS: FRAMEWORK NAZIONALE CYBER SECURITY - NIST

IDENTIFY (ID)

La function IDENTIFY è per la comprensione del contesto aziendale, degli asset che supportano i processi critici di business e dei relativi rischi associati. Permette a un'organizzazione di definire risorse e investimenti in linea con la strategia di gestione del rischio e con gli obiettivi aziendali.

PROTECT (PR)

La function PROTECT è associata all'implementazione di quelle misure volte alla protezione dei processi di business e degli asset aziendali, indipendentemente dalla loro natura informatica.

DETECT (DE)

La function DETECT è associata alla definizione e attuazione di attività appropriate per identificare tempestivamente incidenti di sicurezza informatica

RESPOND (RS)

La function RESPOND è associata alla definizione e attuazione delle opportune attività per intervenire quando un incidente di sicurezza informatica sia stato rilevato.
L'obiettivo è contenere l'impatto determinato da un potenziale incidente di sicurezza informatica.

RECOVER (RC)

La function RECOVER è associata alla definizione e attuazione delle attività per la gestione dei piani e delle attività per il ripristino dei processi e dei servizi impattati da un incidente.

FNCS: FRAMEWORK NAZIONALE CYBER SECURITY - NIST

Function	Category
IDENTIFY (ID)	**Asset Management (ID.AM):** I dati, il personale, i dispositivi e i sistemi e le facilities necessari all'organizzazione sono identificati e gestiti in coerenza con gli obiettivi e con la strategia di rischio dell'organizzazione.
	Business Environment (ID.BE): La mission dell'organizzazione, gli obiettivi, le attività e gli attori coinvolti sono compresi e valutate in termini di priorità. Tali informazioni influenzano i ruoli, le responsabilità di cybersecurity e le decisioni in materia di gestione del rischio.
	Governance (ID.GV): Le politiche, le procedure e i processi per gestire e monitorare i requisiti dell'organizzazione (organizzativi, legali, relativi al rischio, ambientali) sono compresi e utilizzati nella gestione del rischio di cybersecurity.
	Risk Assessment (ID.RA): L'impresa comprende il rischio di cybersecurity inerente l'operatività dell'organizzazione (incluse la mission, le funzioni, l'immagine o la reputazione), gli asset e gli individui.
	Supply Chain Risk Management (ID.SC): Le priorità, i vincoli, le tolleranze al rischio e le ipotesi dell'organizzazione sono stabilite e utilizzate per supportare le decisioni di rischio associate alla gestione del rischio legato alla catena di approvvigionamento. L'organizzazione ha definito e implementato i processi atti a identificare, valutare e gestire il rischio legato alla catena di approvvigionamento.
	Data Management (DP-ID.DM): i dati personali sono trattati attraverso processi definiti, in coerenza con le normative di riferimento.
PROTECT (PR)	**Identity Management, Authentication and Access Control (PR.AC):** L'accesso agli asset fisici e logici ed alle relative risorse è limitato al personale, ai processi e ai dispositivi autorizzati, ed è gestito in maniera coerente con la valutazione del rischio di accesso non autorizzato alle attività ed alle transazioni autorizzate
	Awareness and Training (PR.AT): Il personale e le terze parti sono sensibilizzate in materia di cybersecurity e vengono addestrate per adempiere ai loro compiti e ruoli coerentemente con le politiche, le procedure e gli accordi esistenti
	Data Security (PR.DS): I dati sono memorizzati e gestiti in accordo alla strategia di gestione del rischio dell'organizzazione, al fine di garantire l'integrità, la confidenzialità e la disponibilità delle informazioni.
	Information Protection Processes and Procedures (PR.IP): Sono attuate e adeguate nel tempo politiche di sicurezza (che indirizzano scopo, ambito, ruoli e responsabilità, impegno da parte del management e coordinamento tra le diverse entità organizzative), processi e procedure per gestire la protezione dei sistemi informativi e degli assets.
	Maintenance (PR.MA): La manutenzione dei sistemi informativi e di controllo industriale è fatta in accordo con le politiche e le procedure esistenti.
	Protective Technology (PR.PT): Le soluzioni tecniche di sicurezza sono gestite per assicurare sicurezza e resilienza di sistemi e asset, in coerenza con le relative politiche, procedure ed accordi.

FNCS: FRAMEWORK NAZIONALE CYBER SECURITY - NIST

Function	Category
DETECT (DE)	**Anomalies and Events (DE.AE):** Le attività anomale sono rilevate e il loro impatto potenziale viene analizzato.
	Security Continuous Monitoring (DE.CM): I sistemi informativi e gli asset sono monitorati per indentificare eventi di cybersecurity e per verificare l'efficacia delle misure di protezione.
	Detection Processes (DE.DP): Sono adottati, mantenuti e verificati processi e procedure di monitoraggio per assicurare la comprensione di eventi anomali.
RESPOND (RS)	**Response Planning (RS.RP):** Procedure e processi di risposta sono eseguiti e mantenuti per assicurare una risposta agli incidenti di cybersecurity rilevati.
	Communications (RS.CO): Le attività di risposta sono coordinate con le parti interne ed esterne (es. eventuale supporto da parte degli organi di legge o dalle forze dell'ordine).
	Analysis (RS.AN): Vengono condotte analisi per assicurare un'efficace riposta e supporto alle attività di ripristino.
	Mitigation (RS.MI): Vengono eseguite azioni per prevenire l'espansione di un evento di sicurezza, per mitigare i sui effetti e per risolvere l'incidente.
	Improvements (RS.IM): Le attività di risposta sono migliorate incorporando le "lesson learned" da attività precedenti di monitoraggio e risposta.
RECOVER (RC)	**Recovery Planning (RC.RP):** I processi e le procedure di ripristino sono eseguite e mantenute per assicurare un recupero dei sistemi o asset coinvolti da un incidente di cybersecurity.
	Improvements (RC.IM): I piani di ripristino ed i relativi processi sono migliorati tenendo conto delle "lesson learned" per le attività future.
	Communications (RC.CO): Le attività di ripristino a seguito di un incidente sono coordinate con le parti interne ed esterne (es. le vittime, gli ISP, i proprietari dei sistemi attaccati, i vendor, i CERT/CSIRT).

FNCS: FRAMEWORK NAZIONALE CYBER SECURITY – NIST ESEMPIO COMPLETO

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Governance (ID.GV):** Le politiche, le procedure e i processi per gestire e monitorare i requisiti dell'organizzazione (organizzativi, legali, relativi al rischio, ambientali) sono compresi e utilizzati nella gestione del rischio di cybersecurity.	**ID.GV-1:** È indentificata e resa nota una policy di cybersecurity	· **ISO/IEC 27001:2013** A.5.1.1
		ID.GV-2: Ruoli e responsabilità inerenti la cybersecurity sono coordinati ed allineati con i ruoli interni ed i partner esterni	· **ISO/IEC 27001:2013** A.6.1.1, A.7.2.1, A.15.1.1
		ID.GV-3: I requisiti legali in materia di cybersecurity, con l'inclusione degli obblighi riguardanti la privacy e le libertà civili, sono compresi e gestiti	· **ISO/IEC 27001:2013** A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5
		ID.GV-4: La governance ed i processi di risk management includono la gestione dei rischi legati alla cybersecurity	· **ISO/IEC 27001:2013** Clause 6

Riferimenti Normativi e Best Practices

Grado di copertura: necessario a riportare, in forma numerica, il grado di copertura del controllo (quanto il controllo è soddisfatto). Deve essere espresso con un valore coerente con la scala qualitativa:

Grado di copertura	Criterio qualitativo associato	Descrizione
0	**Nullo**	Il controllo **non è implementato** in alcuna sua parte.
0.2	**Insufficiente**	Implementazione **iniziale** di alcuni aspetti fondamentali del controllo, o implementazione di soli aspetti marginali.
0.4	**Iniziale**	Il controllo risulta **parzialmente implementato** nei suoi aspetti fondamentali, gli elementi mancanti non rendono l'implementazione efficace rispetto agli obiettivi.
0.6	**Incompleto**	Il controllo risulta **parzialmente implementato** e gli elementi implementati riguardano tutti gli aspetti fondamentali. L'implementazione risulta parzialmente efficace rispetto agli obiettivi.
0.8	**Avanzato**	Il controllo risulta **implementato ad eccezione di qualche elemento** marginale.
1	**Completo**	Controllo **completamente implementato**.

DIRETTIVA NIS 2 – ASSESMENT e GAP ANALISI (Esempio)

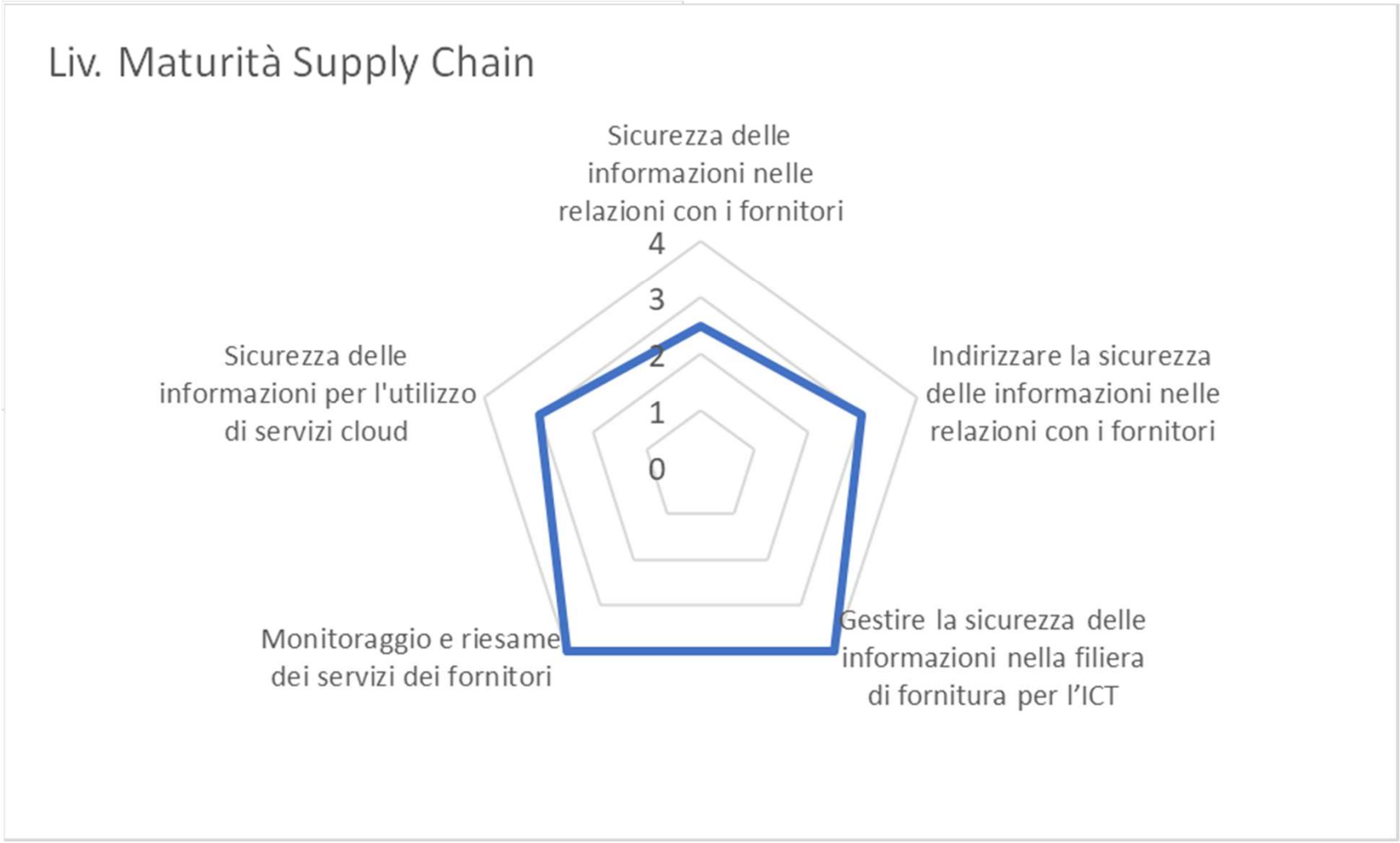
INTERVISTE DI VERIFICA
ANALISI DOCUMENTAZIONE E FUNZIONALITA'
EVENTUALI APPROFONDIMENTI, CHIARIMENTI ED *EVIDENZE*
CONTROLLO FINALE DI CONFORMITA'

ART. NIS2	CONTROLLO ISO27001/2:2022	"RISPOSTE XXXXXXZ Se non specificato diversamente Doc riferimento: Framework Nazionale Cyber Security - XXXXXXZ.pdf"	Evidenze	RICHIESTA Documentazione chiarimento	FEEDBACK XXXXXXZ	Controllo Conforme

DIRETTIVA NIS 2 – ASSESMENT e GAP ANALISI (Esempio)

ARTICOLO NIS2	CONTROLLO ISO27001/2:2022	Mapping > ISO 27001:2013 > FNCS	"RISPOSTE XXXXXXZ Se non specificato diversamente Doc riferimento: Framework Nazionale Cyber Security - XXXXXXZ.pdf"	Evidenze	RICHIESTA Documentazione/ chiarimento	FEEDBACK XXXXXXZ	Controllo Conforme
Articolo 21 - Punto 2 c) continuità operativa, come la gestione del backup e il ripristino in caso di disastro, e gestione delle crisi;	5.29 - Sicurezza delle informazioni durante le interruzioni	A.17.1.2, A.17.2.1 PR.PT-5: Sono implementati meccanismi (es. failsafe, load balancing, hot swap) che permettono di soddisfare requisiti di resilienza sia durante il normale esercizio che in situazioni avverse	PR.PT-5 4.6.5.1 DMSA La facility a supporto dei sistemi infrastrutturali (power, cooling) è in architettura redundancy 2N. Le infrastrutture fisiche dei sistemi sono realizzate in architettura di virtualizzazione VMware ESX Server, che assicurano l'HA e la possibilità di hot swap da un server ad un suo gemello (cisco cluster blade). XXXXXXZ ha definito processi formalizzati di Incident Management, Business Continuity e Disaster Recovery aggiornati al contesto aziendale. Oltre alle revisioni periodiche, il Disaster Recovery Plan viene aggiornato anche a seguito di eventuali anomalie o spunti di miglioramento emersi durante le simulazioni annuali di Disaster Recovery oppure a fronte di modifiche consistenti all'infrastruttura di Disaster recovery o all'introduzione di nuove tipologie di continuità operativa.	4.6.5.2 Descrizione evidenze A dimostrazione di quanto appena dichiarato in merito all'adozione di questo controllo, alleghiamo le seguenti evidenze: · Documento che descrive la configurazione e l'implementazione delle policy di sicurezza sulla rete XXXXXXZ [6] 3.1 Design della rete L'infrastruttura di business continuity che contiene gli ambienti descritti sopra è distribuita su 3 siti: · Xxxx · Xxxx · XXX · Il documento che descrive la procedura di Incident Management [25] · Incident Response Plan [26] · Business Continuity Plan [27] · Disaster Recovery Plan [28] · Policy di continuità operativa [30]			**SI**
	5.30 - Pianificazione della continuità della sicurezza delle informazioni	A.17.1.3 PR.IP-10: I piani di risposta e recupero a seguito di incidenti/disastri sono verificati nel tempo A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 ID.BE-5: Sono identificati e resi noti i requisiti di resilienza a supporto della fornitura di servizi critici per tutti gli stati di esercizio	PR.IP-10 4.4.10.1 DMSA XXXXXXZ ha definito processi formalizzati di Incident Management, Business Continuity e Disaster Recovery aggiornati al contesto aziendale. L'organizzazione ha stabilito le responsabilità e procedure di gestione degli incidenti relativi alla sicurezza delle informazioni; ha istituito inoltre delle sessioni formative per la sensibilizzazione del personale sulle politiche e procedure di Incident Management, Business Continuity e Disaster Recovery. In ambito Business Continuity, le simulazioni periodiche (almeno annuali) effettuate valgono anche come sessione di formazione per tutto il personale potenzialmente coinvolto in un possibile incidente che possa compromettere la disponibilità del servizio e/o dei dati. Ne diamo evidenza nel report di simulazione di Disaster Recovery [28]. In ambito Incident Management, le procedure di gestione degli incidenti sono costantemente testate day by day gestendo gli eventi che vengono segnalati. Le simulazioni di incidente vengono attuate principalmente a fronte di necessità di allineamento del personale neoassunto o a fronte di scostamenti di processo rilevati durante la gestione ordinaria	4.4.10.2 Descrizione evidenze A dimostrazione di quanto appena dichiarato in merito all'adozione di questo controllo, alleghiamo le seguenti evidenze: · Il documento che descrive la procedura di Incident Management [25] · Incident Response Plan [26] · Business Continuity Plan [27] **5.2 Valorizzazione dell'impatto dei servizi (BIA)** · Disaster Recovery Plan [28] · Report della simulazione di Disaster Recovery effettuata a settembre 2023 [29]	Verifica BIA specifica per "xxxxx- yyyyyy" Verifica dell'approvazione della Direzione per i piani di continuità ICT, comprese le procedure di risposta e ripristino di "xxxxx- yyyyyy"	Esiste BIA specifica per "xxxxx- yyyyyy«	**PARZIALE**

DIRETTIVA NIS 2 – Gap Analysis NIS2 Report



DIRETTIVA NIS 2 –REMEDIATION PLAN (Esempio)

PAUSA 10m

TITOLO NIS2	TITOLO ISO27001/2-2022	CONFORME	PIANO DI MIGLIORAMENTO: INTERVENTI RACCOMANDATI E CONSIGLIATI
Articolo 21 - Punto 2			
a) politiche di analisi dei rischi e di sicurezza dei sistemi informatici;	5.2 - Ruoli e responsabilità per la sicurezza delle informazioni ISO 27001-22 6.1.2 Information security risk assesment ISO 27001-22 5.8 Sicurezza delle informazioni nella gestione dei progetti	**SI**	**CONSIGLIATO** Miglioramento del Processo di classificazione degli asset e delle informazioni per il servizio specifico «xxxxx"
c) continuità operativa, come la gestione del backup e il ripristino in caso di disastro, e gestione delle crisi;	"5.29 - Sicurezza delle informazioni durante le interruzioni" "5.30 - Pianificazione della continuità della sicurezza delle informazioni" "8.13 - Backup delle informazioni" "8.14 - Ridondanza delle strutture di elaborazione delle informazioni"	**PARZIALE**	**RACCOMANDATO** Miglioramento della documentazione relativa all"approvazione della Direzione per i piani di continuità ICT, comprese le procedure di risposta e ripristino di «xxxxxxxxx" e feedback documentati dell'approvazione (esiste evidenza sito documenti approvati)
d) sicurezza della catena di approvvigionamento (supply chain), compresi aspetti relativi alla sicurezza riguardanti i rapporti tra ciascun soggetto e i suoi diretti fornitori o fornitori di servizi;	5.19 - Sicurezza delle informazioni nelle relazioni con i fornitori 5.20 - Indirizzare la sicurezza delle informazioni nelle relazioni con i fornitori 5.21 - Gestire la sicurezza delle informazioni nella filiera di fornitura per l'ICT 5.22 - Monitoraggio e riesame dei servizi dei fornitori 5.23 - Sicurezza delle informazioni per l'utilizzo di servizi cloud	SI	**CONSIGLIATO** Miglioramento delle clausole contrattuali relative la cessazione sicura del rapporto di fornitura. **Nel dettaglio, si suggerisce di integrare con clausole contrattuali che facciano riferimento alla restituzione di asset, cancellazione delle utenze, restituzione di proprietà intellettuale e dati di proprietà dell'organizzazione.** **RACCOMANDATO** Introduzione del riesame periodico dei contratti di fornitura, in particolare per i servizi di xxxxxx.
h) politiche e procedure relative all'uso della crittografia e, se del caso, della cifratura;	8.24 Uso della crittografia	**PARZIALE**	Valutare la redazione di una procedura per l'uso della crittografia, specifica per " xxxx»» Consigliato migliorare la procedura di gestione delle chiavi per xxxxxx **(Attualmente Vale la policy generale di cifratura e quanto descritto nella policy di cloud security)** **Al punto 4 Algoritmi si cita:** **Per la gestione delle chiavi si faccia riferimento al NIST SP800-57** **CONSIGLIATO inserire <<si prende come riferimento >> Questo punto inserito potrebbe far sorgere delle NON conformità**

DIRETTIVA NIS 2 – Altri Articoli di interesse

CAPO VII	VIGILANZA ED ESECUZIONE
Articolo 32	**Misure di vigilanza e di esecuzione relative a soggetti essenziali**

Nell'adottare qualsiasi misura di esecuzione di cui al paragrafo 4 o 5, le autorità competenti rispettano i diritti della difesa e tengono conto delle circostanze di ciascun singolo caso e almeno degli elementi seguenti:

a) **la gravità della violazione e l'importanza delle disposizioni violate**, essendo le violazioni seguenti, tra l'altro, da **considerarsi gravi:**

i) **le violazioni ripetute;**

ii) la **mancata notifica** di incidenti significativi o il **mancato rimedio** a tali incidenti;

iii) il **mancato rimedio alle carenze a seguito di istruzioni vincolanti emesse dalle autorità competenti**;

iv) **l'ostacolo degli audit o delle attività di monitoraggio imposte** dall'autorità competente a seguito del rilevamento di una violazione;

v) la fornitura di **informazioni false o gravemente inesatte** relative alle misure in materia di **gestione o segnalazione del rischio di cibersicurezza** di cui agli articoli 21 e 23;

b) la **durata della violazione**;

c) eventuali **precedenti violazioni pertinenti commesse dal soggetto interessato**;

d) qualsiasi **danno materiale o immateriale causato**, incluse le perdite finanziarie o economiche, gli effetti sugli altri servizi e il numero di utenti interessati;

e) un'eventuale **condotta intenzionale o negligenza da parte dell'autore della violazione**;

f) qualsiasi **misure adottata dal soggetto per prevenire o attenuare il danno materiale o immateriale**;

g) qualsiasi **adesione a codici di condotta o meccanismi di certificazione approvati**;

h) il livello di **collaborazione delle persone fisiche o giuridiche ritenute responsabili con le autorità competenti**

7

DIRETTIVA NIS 2 – Altri Articoli di interesse

Comprendere le eventuali sanzioni per non conformità

La sanzione viene stabilita in un importo minimo predefinito, oppure in percentuale rispetto al fatturato annuo; Attualmente in caso di inadempienza, le sanzioni sono attuate indicativamente nelle seguenti modalità:

• Soggetti essenziali:
sanzioni pari a un massimo di **10.000.000 EURO** o a un massimo del **2%** del ex fatturato annuo.

• Soggetti importanti:
sanzioni pari a un massimo di **7.000.000 EURO** o a un massimo del **1,4%** del fatturato annuo.

DIRETTIVA NIS 2 – Altri Articoli di interesse

Articolo 23 Obblighi di segnalazione

1 Ciascuno Stato membro provvede affinché ***i soggetti essenziali e importanti notifichino senza indebito ritardo al proprio CSIRT o, se opportuno, alla propria autorità competente, conformemente al paragrafo 4, eventuali incidenti che hanno un impatto significativo sulla fornitura dei loro servizi*** quali indicati al paragrafo 3 (incidente significativo). Se opportuno, i soggetti interessati notificano senza indebito ritardo ai destinatari dei loro servizi gli incidenti significativi che possono ripercuotersi negativamente sulla fornitura di tali servizi. Ciascuno Stato membro provvede affinché tali soggetti comunichino, tra l'altro, qualunque informazione che consenta al CSIRT o, se opportuno, all'autorità competente di determinare l'eventuale impatto transfrontaliero dell'incidente. La sola notifica non espone il soggetto che la effettua a una maggiore responsabilità.

Qualora i soggetti interessati notifichino all'autorità competente un incidente significativo conformemente al primo comma, lo Stato membro provvede affinché l'autorità competente inoltri la notifica al CSIRT dopo averla ricevuta.

In caso di incidente significativo transfrontaliero o intersettoriale, gli Stati membri provvedono affinché i loro punti di contatto unici ricevano in tempo utile informazioni pertinenti notificate conformemente al paragrafo 4.

2 Se opportuno, gli Stati membri provvedono affinché ***i soggetti essenziali e importanti comunichino senza indebito ritardo ai destinatari dei loro servizi che sono potenzialmente interessati da una minaccia informatica significativa qualsiasi misura o azione correttiva che tali destinatari sono in grado di adottare in risposta a tale minaccia.*** Se opportuno, i soggetti informano tali destinatari anche della minaccia informatica significativa stessa.

3 Un incidente è considerato significativo se:

a) ha causato o è in grado di causare una grave perturbazione operativa dei servizi o perdite finanziarie per il soggetto interessato;

b) si è ripercosso o è in grado di ripercuotersi su altre persone fisiche o giuridiche causando perdite materiali o immateriali considerevoli

DIRETTIVA NIS 2 – Altri Articoli di interesse

CAPO IV	MISURE DI GESTIONE DEL RISCHIO DI CIBERSICUREZZA E OBBLIGHI DI SEGNALAZIONE
Articolo 20	**Governance**
1	Gli Stati membri provvedono affinché ***gli organi di gestione dei soggetti essenziali e importanti approvino le misure di gestione dei rischi di cibersicurezza adottate da tali soggetti per conformarsi all'articolo* 21,** sovraintendano alla sua attuazione e possano essere ritenuti responsabili di violazione da parte dei soggetti di tale articolo. L'applicazione del presente paragrafo lascia impregiudicato il diritto nazionale per quanto riguarda le norme in materia di responsabilità applicabili alle istituzioni pubbliche, nonché la responsabilità dei dipendenti pubblici e dei funzionari eletti o nominati.
2	Gli Stati membri provvedono affinché ***i membri dell'organo di gestione dei soggetti essenziali e importanti siano tenuti a seguire una formazione e incoraggiano i soggetti essenziali e importanti a offrire periodicamente una formazione analoga ai loro dipendenti,*** per far sì che questi acquisiscano conoscenze e competenze sufficienti al fine di individuare i rischi e valutare le pratiche di gestione dei rischi di cibersicurezza e il loro impatto sui servizi offerti dal soggetto.

DIRETTIVA NIS 2 – Riepilogo e conclusioni

I**nformare e coinvolgere la *direzione dell'organizzazione***, assicurandosi che il management comprenda appieno le implicazioni e i requisiti della direttiva.

V**alutare la strategia di cybersecurity**. Analisi dei sistemi IT, controllo delle policy, delle procedure e dei controlli di sicurezza per individuare eventuali punti deboli. S**viluppare un piano di attuazione e remediation** per soddisfare i requisiti della normativa. Le **politiche e le procedure di sicurezza dell'organizzazione devono essere migliorate e aggiornate**, inclusi i piani di risposta agli incidenti.

Implementare i sistemi tecnici di sicurezza, come l'autenticazione a più fattori, la crittografia, la gestione delle vulnerabilità e il monitoraggio.

Assicurarsi che tutti i dipendenti, ***inclusa la Direzione*** ricevano una **formazione adeguata e regolare** sulla consapevolezza della cybersecurity per migliorare e riuscire ad identificare e rispondere alle potenziali minacce.

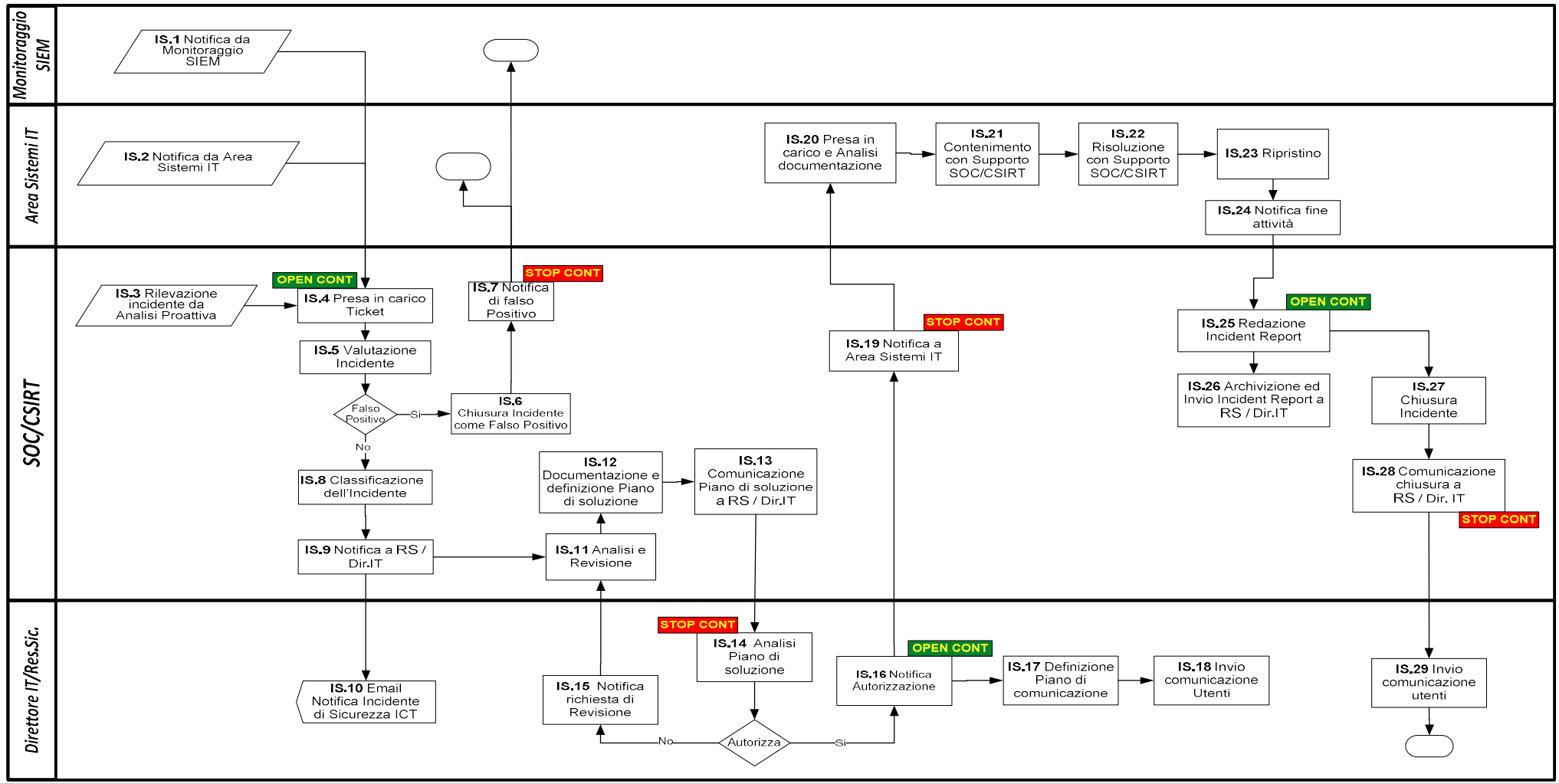
DIRETTIVA NIS 2 – Riepilogo e conclusioni

Garantire **budget e risorse adeguate**, collaborando con la direzione per l'implementazione dei controlli e dei processi di sicurezza richiesti.

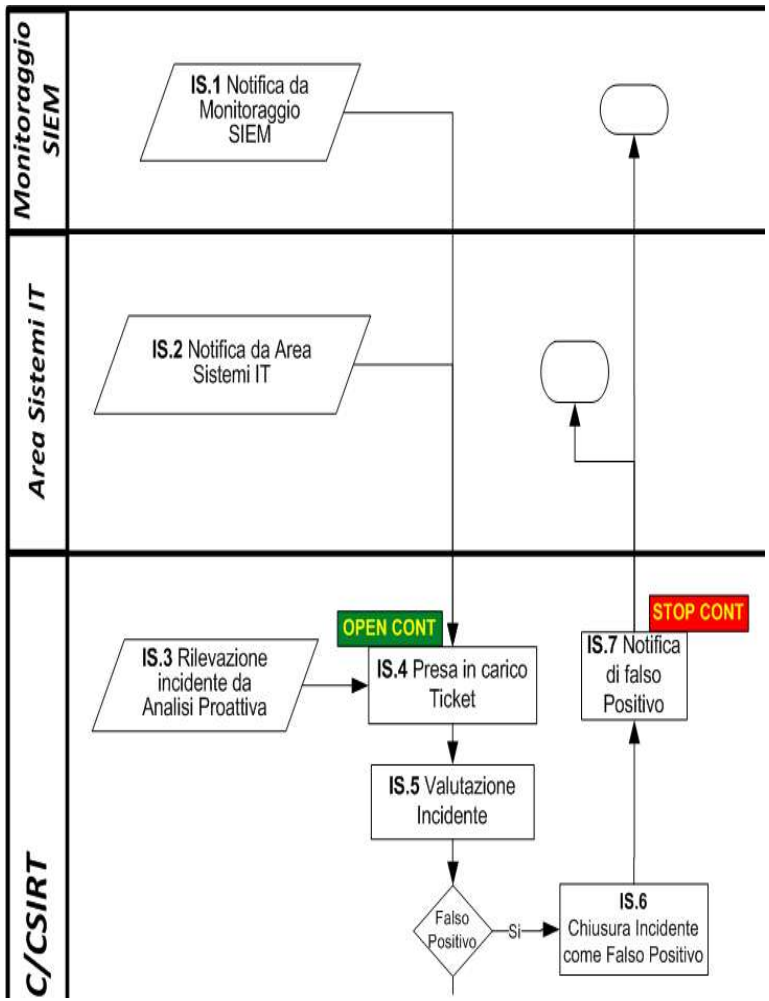
valutare la gestione dei rischi della catena di fornitura implementando misure di sicurezza adeguate a mitigare i rischi lungo tutta la catena di fornitura.

Preparare adeguatamente la segnalazione degli incidenti e gli audit, stabilendo procedure di rilevamento, analisi e segnalazione degli incidenti che soddisfino i requisiti di notifica della direttiva e assicurando che l'organizzazione sia preparata agli audit e ispezioni da parte delle autorità competenti.

DIRETTIVA NIS 2 – Riepilogo e conclusioni



DIRETTIVA NIS 2 – Riepilogo e conclusioni



ATTIVITÀ	DESCRIZIONE	RESPONSABILI
IS.1 Notifica da Monitoraggio SIEM	Nelle attività di monitoraggio il SIEM può rilevare un possibile Incidente e notificarlo al SOC/CSIRT. (ticket)	**R**: SIEM **A**: …. **I**:
IS.2 Notifica da Area Sistemi IT	L' Area Sistemi IT invia una segnalazione classificata come incidente di Sicurezza (anche solo probabile), al SOC/CSIRT, al RS e al Direttore IT.	**R**: Area Sistemi IT **A**: **I**: SOC/CSIRT, RS, Direttore IT
IS.3 Rilevazione incidente da Analisi Proattiva	Il SOC/CSIRT nell'ambito delle sue attività di analisi può rilevare la presenza di un Incidente di Sicurezza e aprire un ticket.	**R**: SOC/CSIRT **A**: **I**:
IS.4 Presa in carico Ticket ***[Open Contatore SLA]***	Il SOC/CSIRT prende in carico il Ticket della rilevazione di un potenziale Incidente	**R**: SOC/CSIRT **A**: **I**:
IS.5 Valutazione Incidente	Il SOC/CSIRT verifica la segnalazione di potenziale incidente di Sicurezza e Accerta che non sia un falso Positivo.	**R**: SOC/CSIRT **A**: **I**:
IS.6 Chiusura Incidente come Falso Positivo	Nel caso l'incidente di Sicurezza sia un falso Positivo chiude l'incidente indicandolo nel Ticket	**R**: SOC/CSIRT **A**: **I**: RS
IS.7 Notifica di falso Positivo ***[Stop Contatore per SLA]***	Il SOC/CSIRT notifica la valutazione di Falso Positivo al RS e all' Area Sistemi IT, la quale inoltrerà tale informazione alla Struttura che ha rilevato l'incidente.	**R**: SOC/CSIRT **A**: **I**: Area Sistemi IT, RS, SIEM

NIS2 Regolamento Esecutivo

Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024

ULTERIORI Riferimenti Normativi e Best Practices

Gazzetta ufficiale
dell'Unione europea

IT
Serie L

2024/2690

18.10.2024

REGOLAMENTO DI ESECUZIONE (UE) 2024/2690 DELLA COMMISSIONE

del 17 ottobre 2024

recante modalità di applicazione della direttiva (UE) 2022/2555 per quanto riguarda i requisiti tecnici e metodologici delle misure di gestione dei rischi di cibersicurezza e l'ulteriore specificazione dei casi in cui un incidente è considerato significativo per quanto riguarda i fornitori di servizi DNS, i registri dei nomi di dominio di primo livello, i fornitori di servizi di cloud computing, i fornitori di servizi di data center, i fornitori di reti di distribuzione dei contenuti, i fornitori di servizi gestiti, i fornitori di servizi di sicurezza gestiti, i fornitori di mercati online, di motori di ricerca online e di piattaforme di servizi di social network e i prestatori di servizi fiduciari

(Testo rilevante ai fini del SEE)

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R2690&qid=1732605994741

https://www.enisa.europa.eu/publications/implementation-guidance-on-nis-2-security-measures

REGOLAMENTO DI ESECUZIONE (UE) 2024/2690 DELLA COMMISSIONE

	Requisiti tecnici e metodologici di cui all'articolo 2 del presente regolamento
1	Politica di sicurezza dei sistemi informativi e di rete [articolo 21, paragrafo 2, lettera a), della direttiva (UE) 2022/2555]
2	Politica di gestione dei rischi [articolo 21, paragrafo 2, lettera a), della direttiva (UE) 2022/2555]
3	Gestione degli incidenti [articolo 21, paragrafo 2, lettera b), della direttiva (UE) 2022/2555]
4	Continuità operativa e gestione delle crisi [articolo 21, paragrafo 2, lettera c), della direttiva (UE) 2022/2555]
5	Sicurezza della catena di approvvigionamento [articolo 21, paragrafo 2, lettera d), della direttiva (UE) 2022/2555]
6	Sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informativi e di rete [articolo 21, paragrafo 2, lettera e), della direttiva (UE) 2022/2555]
7	Strategie e procedure per valutare l'efficacia delle misure di gestione dei rischi di cibersicurezza [articolo 21, paragrafo 2, lettera f), della direttiva (UE) 2022/2555]
8	Pratiche di igiene informatica di base e formazione in materia di sicurezza [articolo 21, paragrafo 2, lettera g), della direttiva (UE) 2022/2555]
9	Crittografia [articolo 21, paragrafo 2, lettera h), della direttiva (UE) 2022/2555]
10	Sicurezza delle risorse umane [articolo 21, paragrafo 2, lettera i), della direttiva (UE) 2022/2555]
11	Controllo dell'accesso [articolo 21, paragrafo 2, lettere i) e j), della direttiva (UE) 2022/2555]
12	Gestione delle risorse [articolo 21, paragrafo 2, lettera i), della direttiva (UE) 2022/2555]
13	Sicurezza ambientale e fisica [articolo 21, paragrafo 2, lettere c), e) ed i), della direttiva (UE) 2022/2555]

REGOLAMENTO DI ESECUZIONE (UE) 2024/2690 DELLA COMMISSIONE

1	**Politica di sicurezza dei sistemi informativi e di rete [articolo 21, paragrafo 2, lettera a), della direttiva (UE) 2022/2555]**	
1.1	**Politica di sicurezza dei sistemi informativi e di rete**	1.1.1 Ai fini dell'articolo 21, paragrafo 2, lettera a), della direttiva (UE) 2022/2555, la politica di sicurezza dei sistemi informativi e di rete deve: a) definire l'approccio dei soggetti pertinenti alla gestione della sicurezza dei sistemi informativi e di rete; b) essere adeguata alla strategia e agli obiettivi aziendali dei soggetti pertinenti e complementare a tale strategia e tali obiettivi; c) stabilire obiettivi di sicurezza dei sistemi informativi e di rete; d) includere un impegno al miglioramento continuo della sicurezza dei sistemi informativi e di rete; e) includere un impegno a fornire le risorse adeguate necessarie per la sua attuazione, compresi il personale, le risorse finanziarie, i processi, gli strumenti e le tecnologie necessari; f) essere comunicata ai dipendenti e alle parti esterne interessate ed essere da essi riconosciuta; g) definire i ruoli e le responsabilità a norma del punto 1.2; h) elencare la documentazione da conservare e la durata della sua conservazione; i) elencare le politiche specifiche per tematica; j) stabilire indicatori e misure volti a monitorare la sua attuazione e lo stato corrente del livello di maturità della sicurezza dei sistemi informativi e di rete dei soggetti pertinenti; k) indicare la data dell'approvazione formale da parte degli organi di gestione dei soggetti pertinenti
		1.1.2. La politica di sicurezza dei sistemi informativi e di rete deve essere riesaminata e, se opportuno, aggiornata dagli organi di gestione almeno annualmente e qualora si verifichino incidenti significativi o cambiamenti significativi delle operazioni o dei rischi. Il risultato dei riesami deve essere documentato.

REGOLAMENTO DI ESECUZIONE (UE) 2024/2690 DELLA COMMISSIONE

1	**Politica di sicurezza dei sistemi informativi e di rete [articolo 21, paragrafo 2, lettera a), della direttiva (UE) 2022/2555]**	
1.2	Ruoli, responsabilità e autorità	1.2.1. Nel contesto della loro politica di sicurezza dei sistemi informativi e di rete di cui al punto 1.1, i soggetti pertinenti devono stabilire le responsabilità e le autorità in materia di sicurezza dei sistemi informativi e di rete e assegnarle a ruoli, attribuendole in base alle esigenze dei soggetti pertinenti e comunicandole agli organi di gestione.
		1.2.2. I soggetti pertinenti devono imporre a tutto il personale e ai terzi di applicare la sicurezza dei sistemi informativi e di rete conformemente alla relativa politica, alle politiche specifiche per tematica e alle procedure dei soggetti pertinenti.
		1.2.3. Almeno una persona deve riferire direttamente agli organi di gestione in merito a questioni relative alla sicurezza dei sistemi informativi e di rete.
		1.2.4. A seconda delle dimensioni dei soggetti pertinenti, la sicurezza dei sistemi informativi e di rete deve essere trattata da ruoli o compiti specifici svolti in aggiunta ai ruoli esistenti.
		1.2.5. Le funzioni e i settori di responsabilità contrastanti devono essere separati, se applicabile.
		1.2.6. I ruoli, le responsabilità e le autorità devono essere riesaminati e, se opportuno, aggiornati dagli organi di gestione a intervalli pianificati e qualora si verifichino incidenti significativi o cambiamenti significativi delle operazioni o dei rischi.

REGOLAMENTO DI ESECUZIONE (UE) 2024/2690 DELLA COMMISSIONE

2 Politica di gestione dei rischi [articolo 21, paragrafo 2, lettera a), della direttiva (UE) 2022/2555]

2.1	Quadro di gestione dei rischi	2.1.1. Ai fini dell'articolo 21, paragrafo 2, lettera a), della direttiva (UE) 2022/2555, i soggetti pertinenti devono istituire e mantenere un quadro di gestione dei rischi adeguato al fine di individuare e affrontare i rischi per la sicurezza dei sistemi informativi e di rete. I soggetti pertinenti devono eseguire e documentare valutazioni dei rischi e, sulla base dei risultati, stabilire, attuare e monitorare un piano di trattamento dei rischi. I risultati della valutazione dei rischi e i rischi residui devono essere accettati dagli organi di gestione o, se applicabile, da persone che sono responsabili e dispongono dell'autorità per gestire i rischi, a condizione che i soggetti pertinenti garantiscano una segnalazione adeguata agli organi di gestione.
		2.1.2. Ai fini del punto 2.1.1, i soggetti pertinenti devono stabilire procedure per l'individuazione, l'analisi, la valutazione e il trattamento dei rischi. Il processo di gestione dei rischi di cibersicurezza deve essere parte integrante del processo generale di gestione dei rischi dei soggetti pertinenti, se applicabile. Nell'ambito del processo di gestione dei rischi di cibersicurezza, i soggetti pertinenti devono: a) seguire una metodologia di gestione dei rischi; b) stabilire il livello di tolleranza per i rischi conformemente alla propensione al rischio dei soggetti pertinenti; c) stabilire e mantenere criteri di rischio pertinenti; d) in linea con un approccio multirischio, individuare e documentare i rischi per la sicurezza dei sistemi informativi e di rete, in particolare in relazione a terzi, come pure i rischi che potrebbero causare perturbazioni in termini di disponibilità, integrità, autenticità e riservatezza dei sistemi informativi e di rete, e) analizzare i rischi per la sicurezza dei sistemi informativi e di rete, compresi la minaccia, la probabilità, l'impatto e il livello di rischio, tenendo conto delle informazioni di intelligence relative alle minacce informatiche e delle vulnerabilità; f) valutare i rischi individuati sulla base dei criteri di rischio; g) individuare le opzioni e le misure adeguate per il trattamento dei rischi e attribuirvi la priorità; h) monitorare costantemente l'attuazione delle misure di trattamento dei rischi; i) individuare i soggetti competenti per l'attuazione delle misure di trattamento dei rischi e la tempistica per tale attuazione; j) documentare in un piano di trattamento dei rischi, le misure di trattamento dei rischi scelte e le ragioni che giustificano l'accettazione di rischi residui.
		2.1.3. Nell'individuare le opzioni e le misure adeguate di trattamento dei rischi e nel definirne un ordine di priorità, i soggetti pertinenti devono tenere conto dei risultati della valutazione dei rischi, dei risultati della procedura volta a valutare l'efficacia delle misure di gestione dei rischi di cibersicurezza, dei costi di attuazione in relazione ai benefici attesi, della classificazione delle risorse di cui al punto 12.1 e dell'analisi dell'impatto sulle attività aziendali (business impact analysis) di cui al punto 4.1.3.
		2.1.4. I soggetti pertinenti devono riesaminare e, se opportuno, aggiornare i risultati della valutazione dei rischi e il piano di trattamento dei rischi a intervalli pianificati e almeno con cadenza annuale, nonché qualora si verifichino incidenti significativi o cambiamenti significativi delle operazioni o dei rischi.

REGOLAMENTO DI ESECUZIONE (UE) 2024/2690 DELLA COMMISSIONE

2	**Politica di gestione dei rischi [articolo 21, paragrafo 2, a), della direttiva (UE) 2022/2555]**	
2.2	Monitoraggio della conformità	2.2.1. I soggetti pertinenti devono riesaminare periodicamente il rispetto delle loro politiche di sicurezza dei sistemi informativi e di rete nonché delle loro politiche specifiche per tematica, regole e norme. Gli organi di gestione devono essere informati in merito allo stato della sicurezza dei sistemi informativi e di rete sulla base dei riesami di conformità mediante relazioni periodiche.
		2.2.2. I soggetti pertinenti devono mettere in atto un sistema efficace di comunicazione della conformità che sia adeguato alle loro strutture, ai loro ambienti operativi e al loro panorama delle minacce. Tale sistema di comunicazione della conformità deve essere in grado di fornire agli organi di gestione una visione informata dello stato corrente della gestione dei rischi da parte dei soggetti pertinenti.
		2.2.3. I soggetti pertinenti devono effettuare il monitoraggio della conformità a intervalli pianificati e qualora si verifichino incidenti significativi o cambiamenti significativi delle operazioni o dei rischi.

2	Politica di gestione dei rischi [articolo 21, paragrafo 2, lettera a), della direttiva (UE) 2022/2555]	
2.3	Riesame indipendente della sicurezza dei sistemi informativi e di rete	2.3.1. I soggetti pertinenti devono riesaminare in modo indipendente il loro approccio alla gestione della sicurezza dei sistemi informativi e di rete e alla sua attuazione, considerando anche le persone, i processi e le tecnologie.
		2.3.2. I soggetti pertinenti devono sviluppare e mantenere processi volti a effettuare riesami indipendenti che devono essere svolti da persone che dispongono di competenze adeguate in materia di audit. Se il riesame indipendente è effettuato da membri del personale del soggetto pertinente, le persone che effettuano i riesami non devono appartenere alla linea gerarchica del personale del settore oggetto del riesame. Se le loro dimensioni non consentono tale separazione nella linea gerarchica, i soggetti pertinenti devono mettere in atto misure alternative per garantire l'imparzialità dei riesami.
		2.3.3. I risultati dei riesami indipendenti, compresi i risultati del monitoraggio della conformità di cui al punto 2.2 e del monitoraggio e della misurazione di cui al punto 7, devono essere comunicati agli organi di gestione. Si devono adottare azioni correttive oppure si deve accettare il rischio residuo secondo i criteri di accettazione dei rischi dei soggetti pertinenti.
		2.3.4. I riesami indipendenti devono essere svolti a intervalli pianificati e qualora si verifichino incidenti significativi o cambiamenti significativi delle operazioni o dei rischi.

REGOLAMENTO DI ESECUZIONE (UE) 2024/2690 - SINTESI

1 Politica di sicurezza dei sistemi informativi e di rete [articolo 21, paragrafo 2, a), direttiva (UE) 2022/2555]

Definire le politiche di sicurezza
Definire e implementare la Security Governance
Designare chiaramente i Ruoli e le Responsabilità

2 Politica di gestione dei rischi [articolo 21, paragrafo 2, a), della direttiva (UE) 2022/2555]

Adottare un framework per la gestione e valutazione dei Rischi
Definire il piano dei trattamenti e mitigazione dei Rischi

3 Gestione degli incidenti [articolo 21, paragrafo 2, lettera b), della direttiva (UE) 2022/2555]

Definire le politiche e le procedure per la gestione degli incidenti di Sicurezza
Implementare sistemi per il monitoraggio delle attività (log) sui sistemi.

4 Continuità operativa e gestione delle crisi [articolo 21, paragrafo 2, lettera c), della direttiva (UE) 2022/2555]

Implementare il business continuity plan.
Garantire la gestione dei backup

5 Sicurezza della catena di approvvigionamento [articolo 21, paragrafo 2, d), della direttiva (UE) 2022/2555]

Definire le politiche per la gestione dei rischi della catena di approvvigionamento.
Gestione e monitoraggio della sicurezza nei contratti con i fornitori.

REGOLAMENTO DI ESECUZIONE (UE) 2024/2690 - SINTESI

6	**Sicurezza dell'acquisizione, sviluppo e manutenzione dei sistemi informativi e di rete [articolo 21, paragrafo 2, e), della direttiva (UE) 2022/2555]**

Garantire il ciclo di vita dello sviluppo sicuro.
Implementare sistemi per la gestione delle vulnerabilità
Implementare la gestione delle configurazioni e degli aggiornamenti (Patch).
Attuare la segmentazione delle Reti
Utilizzare sistemi di protezione e sicurezza protezione come antivirus, IPS/IDS, threat intelligence

7	**Strategie e procedure per valutare l'efficacia delle misure di gestione dei rischi di cibersicurezza [articolo 21, paragrafo 2, f), della direttiva (UE) 2022/2555]**

Definire processi e procedure per la valutazione dell'efficacia delle misure di gestione della sicurezza (audit)

8	**Pratiche di igiene informatica di base e formazione in materia di sicurezza [articolo 21, paragrafo 2, g), della direttiva (UE) 2022/2555]**

Definire piani periodici di sensibilizzazione e formazione in materia di sicurezza

9	**Crittografia [articolo 21, paragrafo 2, h), della direttiva (UE) 2022/2555]**

Definire politiche e procedure per l'utilizzo di sistemi di crittografia per la protezione delle informazioni e dei dati

REGOLAMENTO DI ESECUZIONE (UE) 2024/2690 - SINTESI

10 Sicurezza delle risorse umane [articolo 21, paragrafo 2, lettera i), della direttiva (UE) 2022/2555]

Garantire la Sicurezza delle risorse umane (Formazione, accordi di riservatezza, verifica dei precedenti)
Implementare Policy per cessazione e modifica del rapporto di lavoro
Definire e contrattare i procedimenti disciplinari

11 Controllo dell'accesso [articolo 21, paragrafo 2, lettere i) e j), della direttiva (UE) 2022/2555]

Implementare Processi e procedure per il controllo degli accessi
Gestire identificazione e autenticazione degli utenti (Profilazione accessi, privilegi e amministratori)

12 Gestione delle risorse [articolo 21, paragrafo 2, lettera i), della direttiva (UE) 2022/2555]

Implementare inventario delle risorse e degli asset
Gestire la classificazione dei dati, delle informazione e degli asset
Definire le politiche e le procedure per la gestione dei supporti removibili
Definire politiche e procedure per la gestione di risorse alla cessazione (Restituzione cancellazione)

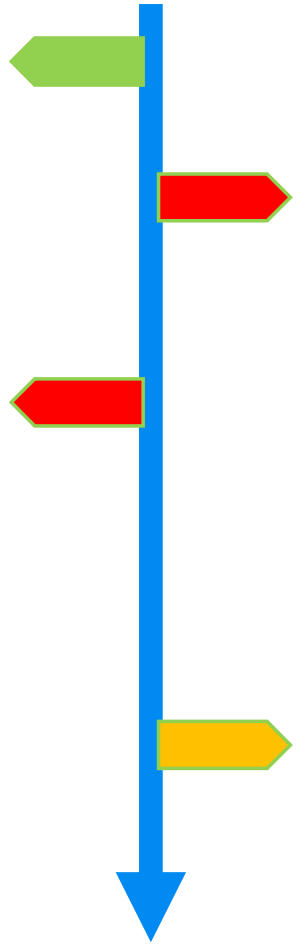
13 Sicurezza ambientale e fisica [articolo 21, paragrafo 2, lettere c), e) ed i), della direttiva (UE) 2022/2555]

Implementare un piano di continuità operativa
Garantire la protezione da minacce fisiche (Eventi naturali e accessi fisici NON autorizzati)

NIS 2 - Recepimento e attuazione

FEBBRAIO 23 - METÀ OTTOBRE 24
Recepimento
Avvio di alcuni tavoli settoriali
7 agosto 2024: adozione definitiva in CDM
1° ottobre 2024: pubblicazione in Gazzetta Ufficiale
16 ottobre 2024: entrata in vigore

METÀ APRILE 25 – METÀ APRILE 26
Seconda fase attuativa
Monitoraggio e supporto
A partire da gennaio 2026: obbligo di notifica di base
Entro aprile 2026: elaborazione e adozione del modello di categorizzazione delle attività e dei servizi
Entro aprile 2026: elaborazione e adozione degli obblighi a lungo termine
Entro settembre 2026: completa implementazione delle misure di sicurezza di base



METÀ OTTOBRE 24 – METÀ APRILE 25
Prima fase attuativa
Avvio formale di tutti i tavoli settoriali
Entro febbraio 2025: censimento e registrazione dei soggetti
Entro marzo 2025: adozione dell'elenco dei soggetti NIS
Entro aprile 2025: notifica ai soggetti NIS
Entro aprile 2025: elaborazione e adozione obblighi di base

DA METÀ APRILE 26
Terza fase attuativa
•Categorizzazione delle attività e dei servizi
•Implementazione degli obblighi a lungo termine

NIS 2 - Recepimento e attuazione

1️⃣ **Registrazione sulla piattaforma ACN**
-Entro il 17 gennaio 2025: per fornitori di servizi critici come cloud computing, data center, sicurezza gestita, mercati online, motori di ricerca e social network.
-Entro il 28 febbraio 2025: per tutti gli altri soggetti inclusi nel decreto.

2️⃣ Entro metà aprile 2025 (Autorità nazionale competente):
-Creazione dell'elenco dei soggetti NIS.
-Adozione degli obblighi di base in materia di misure di sicurezza informatica e notifica di incidenti.

3️⃣ Entro metà maggio 2025:
-Trasmissione e aggiornamento delle informazioni dei soggetti NIS, con aggiornamenti tempestivi (max 14 giorni).

4️⃣ Entro gennaio 2026:
-Adempimento degli obblighi di base in materia di notifica di incidente (entro 9 mesi dalla notifica di inclusione).

5️⃣ Entro ottobre 2026:
-Adempimento agli obblighi di base in materia di sicurezza informatica (entro 18 mesi dalla notifica di inclusione).

RIFERIMENTI e CONSIGLIATI

https://www.iso.org/standard/27001
https://www.cybersecurityframework.it/
https://www.nist.gov/cyberframework

https://www.nis-2-directive.com/
https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32022L2555

https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/digital-operational-resilience-act-dora
https://eur-lex.europa.eu/eli/reg/2022/2554/oj
https://eur-lex.europa.eu/eli/reg_impl/2024/2690/oj

ENISA

DIBATTITO SUL SEMINARIO

Grazie

fabio.pieralice@isecprof.com