

CYBERSECURITY E SICUREZZA DEL DATO: IMPATTO PER IL SETTORE DEI DISPOSITIVI MEDICI

Milano, 17 marzo 2025 - Sede UNIDI

Relatori:

Avv. Giuseppe Strano - A.L.I. & Partners

Avv. Rita Crobe - A.L.I. & Partners

Dr.ssa Silvia Tamarri - Complife Group

Programma

- ▶ 14:00 - 14:15 | Apertura e Introduzione al Corso
- ▶ 14:15 - 14:45 | Modulo 1: Nuove proposte e loro impatto per il settore healthcare
- ▶ 14:45 - 15:15 | Modulo 2: Dalla Direttiva NIS alla NIS 2
- ▶ 15:15 - 15:45 | Modulo 3: Direttiva NIS 2 - Novità e adempimenti richiesti per il settore dei dispositivi medici
- ▶ ☕ 15:45 - 16:00 | Pausa Caffè ☕
- ▶ 16:00 - 16:30 | Modulo 4: Gestione del rischio e compliance alla NIS 2 in ambito industriale
- ▶ 16:30 - 16:50 | Modulo 5: Sanzioni per mancata conformità alla NIS 2
- ▶ 16:50 - 17:10 | Modulo 6: Regolamentazione della cybersecurity dei dispositivi medici
- ▶ 17:10 - 17:30 | Modulo 7: Valutazione dei Rischi e Gestione delle Vulnerabilità
- ▶ 17:30 - 17:50 | Modulo 8: L'interazione tra NIS 2 e Regolamento MDR
- ▶ 17:50 - 18:00 | Chiusura e Q&A



MODULO 1 NUOVE PROPOSTE E LORO IMPATTO

► PER IL SETTORE HEALTHCARE

Dott.ssa Tamarri Silvia
Complife Group

Nuove proposte e loro impatto per il settore healthcare

Evoluzione della regolamentazione sulla cybersicurezza nel settore sanitario

- ▶ Aumento delle connessioni delle infrastrutture sanitarie (MD, IVD, LIS, HIS)
- ▶ La manipolazione di dati potrebbe portare ad una diagnosi errata e terapia incorretta

☞ Danno al paziente!

- ▶ Attacchi informatici potrebbero impedire diagnosi in tempi brevi

☞ Danno al paziente!



Cybersecurity: obiettivi

Garantire safety,
security e
performance



Prevenire attacchi
informatici,
problemi o eventi

Minimizzare rischi di danno al paziente

Cybersecurity: definizioni

“A state where information and systems are protected from unauthorized activities, such as access, use, disclosure, disruption, modification, or destruction to a degree that the related risks to confidentiality, integrity, and availability are maintained at an acceptable level throughout the life cycle”

(IMDRF/CYBER WG/N70)

"La protezione offerta a un sistema informativo per conseguire gli obbiettivi applicabili per preservare l'integrità, la disponibilità e la riservatezza delle risorse del sistema(hardware, software, firmware, informazioni/dati e telecomunicazioni)"

(NIST- National Institute of Standard and Technology)

Cybersecurity: principi fondamentali

- ▶ Integrity
- ▶ Confidentiality
- ▶ Availability



Nuove proposte e loro impatto per il settore healthcare

Cybersecurity: cyber threat





MODULO 2

DALLA DIRETTIVA NIS ALLA DIRETTIVA NIS 2



Avv. Rita Crobe
A.L.I. & Partners

Con la Direttiva NIS - Direttiva UE 2016/1148 il legislatore europeo aveva l'obiettivo di raggiungere un elevato livello comune di cybersicurezza tra gli Stati membri, prevedendo che gli stessi:

- ➔ adottassero una strategia nazionale in materia di sicurezza cibernetica che definisse obiettivi strategici e priorità, politiche adeguate e misure di regolamentazione a livello nazionale
- ➔ assicurassero la cooperazione internazionale e la collaborazione con l'ENISA (*European Union for Network and Information Security Agency*) attraverso meccanismi individuati
- ➔ designassero autorità nazionali competenti, punti di contatto e il CSIRT (*Computer Security Incident Response Team*), responsabili della sicurezza e del monitoraggio degli incidenti a livello nazionale

Dalla Direttiva NIS alla Direttiva NIS 2

Nel dicembre 2020 la Commissione Europea ha proposto la revisione programmata dell'efficacia della norma (Direttiva NIS) e della sua implementazione e i risultati hanno rivelato delle carenze intrinseche, in particolare:

Importanti divergenze nell'attuazione della Direttiva NIS anche per quanto riguarda il suo ambito di applicazione, la cui delimitazione è stata lasciata, in larga misura, alla discrezione degli Stati membri

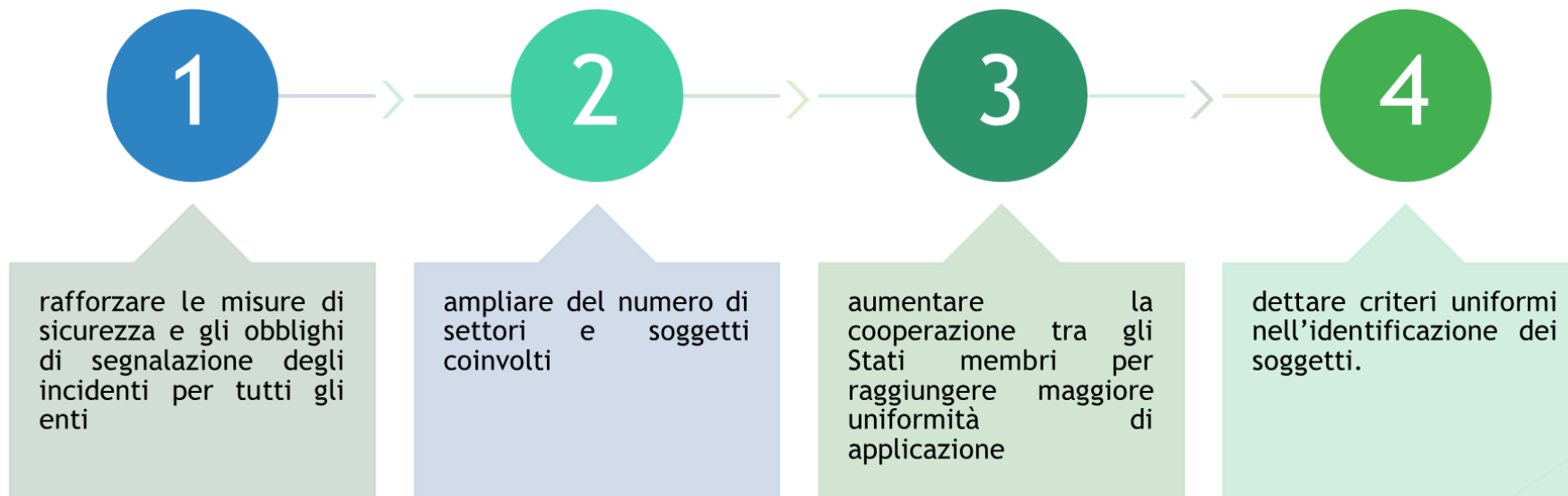
Identificazione dei soggetti che soddisfacevano i criteri per essere considerati operatori dei servizi essenziali direttamente da parte dagli Stati membri

Libertà per gli Stati di ampliare i settori / le categorie di soggetti a cui gli obblighi in materia cyber dovevano applicarsi

La rapida evoluzione delle minacce cibernetiche ha evidenziato la necessità di aggiornare e rafforzare la direttiva per mantenere un alto livello di sicurezza

Necessità di revisione del primigenio impianto normativo per raggiungere un livello comune di cybersicurezza tra gli Stati membri

Direttiva NIS 2 (Direttiva UE 2022/2555 del 14 dicembre 2022), entrata in vigore il 16 gennaio 2023 e che abroga la precedente Direttiva NIS, nasce con i seguenti obiettivi



Termine di recepimento per gli Stati Membri



Entro il 17 ottobre 2024, gli Stati membri adottano e pubblicano le misure necessarie per conformarsi alla Direttiva NIS 2



Gli Stati membri applicano tali misure a decorrere dal 18 ottobre 2024



COOPERAZIONE A LIVELLO
DELL'UNIONE E
INTERNAZIONALE



ISTITUZIONE DI UN GRUPPO DI
COOPERAZIONE



COMPOSIZIONE DEL GRUPPO
DI COOPERAZIONE:
RAPPRESENTANTI DEGLI STATI
MEMBRI, DELLA COMMISSIONE
E DELL'ENISA

Sistemi europei di certificazione della cibersecurity

Articolo 24 Direttiva NIS 2



Al fine di dimostrare il rispetto di determinate prescrizioni di cui all'articolo 21, gli Stati membri possono imporre ai soggetti essenziali e importanti di utilizzare determinati prodotti TIC, servizi TIC e processi TIC, sviluppati dal soggetto essenziale o importante o acquistati da terze parti, che siano certificati nell'ambito dei sistemi europei di certificazione della cibersecurity adottati a norma dell'articolo 49 del regolamento (UE) 2019/881. Inoltre, gli Stati membri incoraggiano i soggetti essenziali e importanti a utilizzare servizi fiduciari qualificati

Dalla Direttiva NIS alla Direttiva NIS 2

Il contenuto dell'articolo 24 della Direttiva NIS 2 è stato trasposto nell'art. 27 del D.Lgs. 138/2024 e impone l'adozione di schemi di certificazione della cybersicurezza come mezzo per garantire la conformità agli obblighi in materia di sicurezza. Esempi di schemi di certificazione:



ISO/IEC 27001 - gestione della sicurezza delle informazioni



Common Criteria (ISO/IEC 15408) - norma internazionale che consente la valutazione di sicurezza e garantisce che i prodotti TIC soddisfino requisiti specifici



EUCS (European Cybersecurity Certification Scheme) - certifica servizi di cloud computing

CSIRT *Computer Security Incident Response Team*

Ogni Stato membro deve designare o istituire uno o più CSIRT il quali si occupano almeno dei settori, dei sottosettori e dei tipi di soggetto di cui agli allegati I e II e sono responsabili della gestione degli incidenti conformemente a una procedura ben definita

Dalla NIS alla NIS2



SVILUPPARE LE CAPACITÀ DI CIBERSICUREZZA DEGLI STATI MEMBRI PER AFFRONTARE MINACCE NUOVE E EMERGENTI.



MIGLIORARE LA COOPERAZIONE TRANSFRONTALIERA TRA GLI STATI MEMBRI PER GARANTIRE UNA RISPOSTA COORDINATA AGLI INCIDENTI DI SICUREZZA.



ASSICURARE LA CONTINUITÀ E LA SICUREZZA DEI SERVIZI ESSENZIALI IN SETTORI CHIAVE COME ENERGIA, TRASPORTI, SALUTE E DIGITALE.

NIS 2 - AMBITO DI APPLICAZIONE



Tra le principali differenze che contraddistinguono la Direttiva NIS2 rispetto alla precedente è l'ambito di applicazione. Infatti, la Direttiva NIS2 si applica a **maggiori settori**, tutti considerati critici per il funzionamento della società e dell'economia: un maggiore numero di aziende di medie e grandi dimensioni dovrà conformarsi alla direttiva, oltre ad aziende anche di piccole dimensioni che, tuttavia, rientrino nella definizione di alto rischio di sicurezza.



Identificazione dei soggetti

Sotto altro aspetto, invece, scompare la distinzione precedentemente adottata tra operatori di servizi essenziali e fornitori di servizi digitali, in favore della nuova distinzione tra soggetti essenziali e soggetti importanti. Tale nuova divisione, focus di questa nuova normativa, consente di armonizzare l'applicazione delle misure di cybersicurezza, distribuendo gli oneri in base alla capacità e al potenziale di ciascuna entità, prevedendo un'equa distribuzione degli obblighi normativi, consentendo così una protezione informativa adeguata e mirata.

La Direttiva NIS2 è stata recepita mediante il **Decreto Legislativo 4 settembre 2024, n. 138** entrato in vigore il 16 ottobre 2024

Art. 1: 'Il presente Decreto stabilisce misure volte a garantire un livello elevato di sicurezza informatica in ambito nazionale, contribuendo ad incrementare il livello comune di sicurezza nell'Unione Europea in modo da migliorare il funzionamento del mercato interno'

ciò mediante la gestione dei rischi legati ai rischi e alle crisi informatiche al fine di rispondere a un'esigenza di proteggere le infrastrutture informatiche e i dati sensibili, cruciali non solo per il settore privato, ma anche per l'integrità della pubblica amministrazione e delle istituzioni italiane

Dalla Direttiva NIS alla Direttiva NIS 2

Soggetti Essenziali	Soggetti Importanti
Allegato I - realtà che per dimensione superano i massimali delle medie imprese Indipendentemente dalle dimensioni, le entità che operano nei settori definiti critici dal D.lgs.134/2024 (attuativo della Direttiva 2022/2557) Fornitori di reti pubbliche di comunicazione elettronica Prestatori di servizi fiduciari qualificati Gestori di nomi di dominio di primo livello Allegato III - le PA Allegato IV - ulteriori soggetti da individuare (PA, soggetti che forniscono servizi di trasporto pubblico locale, Istituti di istruzione che svolgono attività di ricerca, etc)	Soggetti di cui all'art. 3 che non sono considerati essenziali

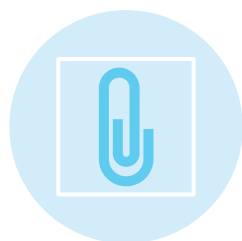
Ambito di applicazione

- Art. 3
D.Lgs.
138/2024

soggetti sottoposti alla giurisdizione italiana

che rientrano nelle tipologie di cui agli allegati
I, II, III e IV*

che superano i massimali per le piccole imprese
ai sensi dell'art. 2, par. 2 dell'allegato alla
Raccomandazione 2003/361/CE



Allegati I e II: settori critici ed altamente critici



Allegati III e IV PA e ulteriori tipologie di soggetti cui si applica il D.Lgs. 138/2024

Allegato II, punto 5 a) D.Lgs. 138/2024 «altri settori critici»

Settore	Sottosettore	Tipologia di soggetto
Fabbricazione	Fabbricazione di dispositivi medici e di dispositivi medico-diagnostici in vitro	Soggetti che fabbricano dispositivi medici quale definiti dall'articolo 2, punto 1) del regolamento (UE) 2017/745 del Parlamento europeo e del Consiglio e soggetti che fabbricano dispositivi medico-diagnostici in vitro quali definiti all'articolo 2, punto 2) del regolamento (UE) 2017/746 del Parlamento europeo e del Consiglio ad eccezione dei soggetti che fabbricano dispositivi medici di cui all'allegato I, punto 5), quinto trattino della presente direttiva

Art. 5 D.Lgs. 138/2024

Sottoposizione alla giurisdizione italiana



Sono sottoposti alla giurisdizione italiana i soggetti stabiliti sul territorio nazionale



FAQ 2.8 pubblicate sul sito dell'ACN:



Rientrano nell'ambito di applicazione del D.Lgs. 138/2024 anche le organizzazioni di diritto di altri Stati membri che sono stabilite in Italia (art. 2508 c.c. - Società estere con sede secondaria nel territorio dello Stato)



Inoltre, qualora una organizzazione sia stabilita in più Stati membri, è possibile che sia soggetta alla giurisdizione di più Stati membri.



Quali organizzazioni estere (EU ed Extra EU) rientrano nel campo di applicazione del D.Lgs. 138/2024?

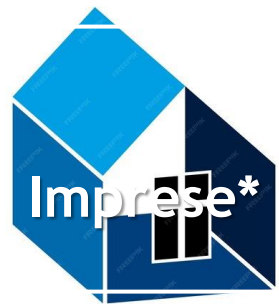


FAQ 2.8 pubblicata sul sito dell'ACN

FAQ 2.8

La direttiva e il decreto NIS si applicano alle singole persone giuridiche (*legal entities*). Conseguentemente, salvo specifiche eccezioni, rientrano nell'ambito di applicazione del decreto NIS le persone giuridiche (*legal entities*) che sono stabilite in Italia e non le eventuali persone giuridiche collegate stabilite in altri Stati membri. Con particolare riferimento ai gruppi di imprese multinazionali stabiliti anche in Italia (ovvero gruppi europei con filiali in Italia o gruppi italiani con filiali all'estero), salvo eccezioni, il decreto NIS si applica solo alle persone giuridiche del gruppo (*legal entities* / filiali) stabilite in Italia.

Art. 3, comma 2 D.Lgs. 138/2024: criteri dimensionali



Se sono medie o grandi imprese

Numero di dipendenti pari o superiore a 50

Fatturato annuo superiore a 10 mln o totale di bilancio superiore a 10 mln

Se appartengono a settori critici o altamente critici (Allegati I e II)

Art. 3 D.Lgs. 138/2024 - Definizione di impresa

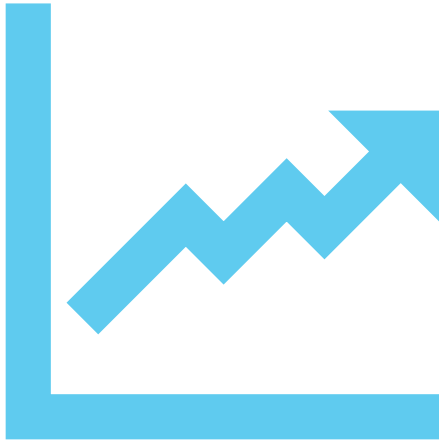
Art. 2, par. 2
Raccomandazione
2003/361/CE della
Commissione (6 maggio 2003)

Nella categoria delle PMI si
definisce piccola impresa
un'impresa che occupa meno
di 50 persone e realizza un
fatturato annuo o un totale
di bilancio annuo non
superiori a 10 milioni di EUR.

Requisito dimensionale (numero di dipendenti)

Numero di dipendenti: il calcolo del numero dei dipendenti si basa sulle Unità Lavorative-Anno (ULA) dove ciascuna ULA rappresenta un'unità lavorativa a tempo pieno per l'intero anno (lavoratori a tempo parziale o su base stagionale sono conteggiati come frazioni di ULA)

Fatturato



Fatturato annuo

totale dei ricavi derivanti dalla vendita di beni o prestazione di servizi

Totale di bilancio

somma delle attività patrimoniali -
totale dell'attivo patrimoniale -tutti
i beni e i diritti che un'azienda
possiede



FAQ 2.3 pubblicata sul sito dell'ACN

devono essere sempre presenti sia il criterio del numero di effettivi sia almeno uno dei due parametri contabili (fatturato o bilancio tra loro alternativi).

Il D.Lgs. 138/2024 semplifica la procedura di identificazione dei soggetti destinatari consentendo di classificare un'impresa secondo criteri dimensionali «puri» ossia senza considerare eventuali legami societari o influenze esercitate da soggetti collegati o controllanti

Riferimento all'articolo 6, paragrafo 2,
dell'allegato alla raccomandazione
2003/361/CE per le organizzazioni che
hanno imprese collegate o associate o che
fanno parte di gruppi di imprese

→ il calcolo dei parametri per determinare la
riconducibilità di un'organizzazione alla
categoria delle medie e grandi imprese nel
contesto dei gruppi di imprese (imprese
collegate e/o associate) prevede una forma di
consolidamento.

Art. 3, comma 4
D.Lgs. 138/2024

Clausola di salvaguardia - Art. 3, comma 4 D.Lgs. 138/2024

La clausola di salvaguardia consente di disapplicare la forma di consolidamento di cui all'articolo 6, paragrafo 2, dell'allegato alla Raccomandazione 2003/361 determinando un potenziale declassamento dell'organizzazione da grande impresa a media impresa (con conseguenti potenziali impatti sulla qualifica di soggetto essenziale o importante), ovvero da media impresa a piccola impresa (con conseguenti potenziali impatti sulla riconducibilità dell'organizzazione all'ambito di applicazione)

L'inclusione tra i destinatari del D.Lgs. 138/2024 non è determinata solo da criteri numerici (numero di dipendenti o fatturato) ma può essere estesa alle imprese formalmente più piccole che risultano, però, integrate in un'organizzazione più ampia dalla quale dipendono per l'implementazione delle misure di sicurezza e per la gestione delle infrastrutture informatiche

DPCM 9 dicembre 2024 n. 221
(pubblicato in GU il 10.02.2025)

Definizione dei criteri per l'applicazione della clausola di salvaguardia (art. 3, commi 4 e 12 del D.Lgs. 138/2024) che consente di derogare all'applicazione dell'articolo 6, paragrafo 2, dell'allegato alla raccomandazione 2003/361/CE, e definisce il relativo procedimento per la sua applicazione

Il soggetto che chiede l'applicazione della clausola di salvaguardia deve dimostrare

1. indipendenza dei sistemi informativi e di rete NIS da quelli delle imprese collegate

indipendenza deve riguardare

a) componenti hardware e software,

b) flussi di dati e le interconnessioni

evitando qualsiasi forma di interdipendenza tecnologica che potrebbe compromettere la segregazione operativa

Il soggetto che chiede l'applicazione della clausola di salvaguardia deve inoltre dimostrare

2. indipendenza delle proprie attività e servizi NIS da quelli delle imprese collegate

Le attività e i servizi che rientrano nell'ambito di applicazione del D.Lgs. 138/2024 non devono essere in alcun modo influenzati da altre realtà societarie appartenenti allo stesso gruppo. La segregazione deve essere assoluta, senza alcuna condivisione di risorse operative, tecniche o di personale

Art. 3 comma 5 D.Lgs. 138/2024

Indipendentemente dalle dimensioni il criterio applicativo del D.Lgs. 138/2024 è dato dall'importanza strategica dell'impresa



Soggetti identificati come critici ai sensi del D.Lgs. 134/2024 che recepisce la Direttiva (UE) 2022/2557 (14.12.2002)

Soggetti critici



D.lgs. 134/2024 (Attuazione della Direttiva CER): soggetto pubblico o privato individuato, entro il 17.01.2026, dalle Autorità Settoriali Competenti (ASC) nell'ambito delle categorie di soggetti che operano nei settori e sottosettori di cui all'Allegato A del D.Lgs. 134/2024 - tra cui al punto 5 sono indicati i **fabbricanti di dispositivi medici** considerati critici durante un'emergenza di sanità pubblica ai sensi dell'art. 22 Regolamento UE 2022/123 (elenco adottato, dopo il riconoscimento di un'emergenza di sanità pubblica, da parte del MDSSG - *Medical Devices Shorteges Steering Group*)

Art. 3,
comma 10
D.Lgs.
138/2024

indipendentemente dalle dimensioni il D.Lgs. 138/2024 si applica alle aziende **collegate a un soggetto essenziale o importante** se soddisfa uno dei seguenti criteri:

Gestisce o detiene sistemi informativi e di rete da cui dipende la fornitura dei servizi del soggetto essenziale o importante

Adotta decisioni o esercita un'influenza dominante sulle decisioni relative alla gestione del rischio

Fornisce servizi TIC o di sicurezza

Effettua operazioni di sicurezza informatica

La clausola di salvaguardia (art. 3, comma 4) non può essere richiesta



dal soggetto a cui si applica l' 3, comma 10 D.Lgs. 138/2024

MODULO 3
NOVITA' E ADEMPIMENTI
RICHIESTI PER IL SETTORE DEI
► DISPOSITIVI MEDICI

Avv. Giuseppe Strano
A.L.I. & Partners

Art. 7 -

Obbligo di registrazione e di aggiornamento delle informazioni

1 gennaio – 28 febbraio (dal 2025 in poi)

Una volta completato positivamente il processo di autovalutazione, le organizzazioni che si riconoscono in uno o più tipologie di soggetto cui si applica il D.Lgs. 138/2024 (per il settore dei dispositivi medici e dei dispositivi medico diagnostici tutti i fabbricanti se ed in quanto siano soddisfatti i requisiti di giurisdizione e dimensionali/economici) devono manifestarsi all'Autorità nazionale competente NIS (ACN - Agenzia per la Cybersicurezza Nazionale <https://www.acn.gov.it>) mediante registrazione o aggiornamento della propria registrazione sulla piattaforma digitale dell'ACN ovvero sul Portale dei Servizi (<https://portale.acn.gov.it/login>).

- ▶ Tale adempimento è funzionale a consentire ad ACN di censire i soggetti operanti nei settori vigilati, anche al fine di fornire loro supporto in fase di implementazione degli obblighi, attraverso le articolate attività di monitoraggio e ausilio nel loro percorso condiviso di crescita, disciplinate dall'articolo 35 del Decreto NIS.
- ▶ La mancata registrazione è una violazione assistita da una sanzione amministrativa pecuniaria con un importo fino al 0.1% del fatturato annuo su scala mondiale del soggetto.
- ▶ La registrazione è composta da tre fasi: 1. il censimento del punto di contatto 2. la sua associazione al soggetto e 3. la compilazione della dichiarazione NIS.

- ▶ Prima di avviare la registrazione, il soggetto deve designare **il Punto di contatto**, di cui all'articolo 7, comma 1, lettera c) del decreto NIS.
- ▶ Il Punto di contatto ha il compito di curare l'attuazione delle disposizioni del decreto NIS per conto del soggetto stesso, a partire dalla registrazione, e interloquisce, per conto del soggetto NIS, con l'ACN.
- ▶ Il Punto di contatto è il **rappresentante legale** o un suo **procuratore generale** oppure un **dipendente delegato** del soggetto. In quest'ultimo caso, nel corso della registrazione, il punto di contatto dovrà allegare la delega (resa in forma di dichiarazione sostitutiva di atto di notorietà) ad operare per conto del soggetto nel contesto NIS.
- ▶ Il processo di censimento del punto di contatto e associazione al soggetto NIS si conclude con l'invio di un link di richiesta di convalida al domicilio digitale del soggetto stesso. L'accesso al Portale può avvenire a mezzo SPID o credenziali.

La dichiarazione che il punto di contatto dovrà compilare è suddivisa in 4 sezioni:

- ▶ A) ragione sociale
- ▶ B) indirizzo e recapiti aggiornati, compreso gli indirizzi e-mail e i numeri di telefono
- ▶ C) designazione di un punto di contatto, indicando il ruolo presso il soggetto e i recapiti aggiornati (anche e-mail e numeri di telefono)
- ▶ D) ove applicabile, i pertinenti settori, sottosettori e tipologie di soggetto di cui agli allegati I, II, III e IVA
- ▶ Dopo aver compilato la dichiarazione, il Punto di contatto dovrà prendere visione del riepilogo delle informazioni fornite, accettare le clausole di responsabilità e trasmettere la dichiarazione all'Agenzia. Una copia della dichiarazione è inviata al domicilio digitale del soggetto.

Valutazione da parte dell'ACN e dell'Autorità competente



Entro 31 marzo 2025 e di ogni anno successivo

ACN e Ministero della Salute valutano le dichiarazioni per costituire l'elenco dei soggetti NIS

**Entro il 31
marzo** di ogni
anno successivo
all'entrata in
vigore del
Decreto NIS

l'ACN redige, sulla base delle registrazioni effettuate, l'elenco dei soggetti essenziali e dei soggetti importanti. Per il tramite della piattaforma digitale, l'Autorità competente NIS comunica ai soggetti registrati:

- a) l'inserimento tra i soggetti essenziali o importanti
- b) la permanenza nell'elenco dei soggetti essenziali o importanti
- c) l'espunzione dall'elenco dei soggetti

Dal 2026 e tra il 15 aprile e il 31 maggio di ogni anno i soggetti che avranno ricevuto la comunicazione da parte dell'Autorità competente NIS dovranno fornire o aggiornare:

- a) lo spazio di indirizzamento IP pubblico e i nomi di dominio in uso o nella disponibilità del soggetto
- b) ove applicabile, l'elenco degli Stati membri in cui forniscono servizi che rientrano nell'ambito di applicazione
- c) i responsabili di cui all'articolo 38, comma 5*, indicando il ruolo presso il soggetto e i loro recapiti aggiornati, compresi gli indirizzi e-mail e i numeri di telefono
- d) un sostituto del punto di contatto indicando il ruolo presso il soggetto e i recapiti aggiornati, compresi gli indirizzi e-mail e i numeri di telefono

RESPONSABILE

Art. 38,
comma 5

qualsiasi persona fisica
responsabile di un soggetto
essenziale o che agisca in
qualità di suo rappresentante
legale con l'autorità di
rappresentarlo, di prendere
decisioni per suo conto o di
esercitare un controllo sul
soggetto stesso

Ministero della Salute (quale Autorità competente NIS)



può indicare ulteriori informazioni che i soggetti devono fornire nonché i termini e le modalità e i procedimenti di designazione dei rappresentanti

Elencazione, caratterizzazione e categorizzazione delle attività e dei servizi

Al fine di assicurare un livello di sicurezza dei sistemi informativi e di rete adeguato ai rischi esistenti

DAL 1 GENNAIO 2026

Dal 1 maggio al 30 giugno di ogni anno a partire dalla ricezione della prima comunicazione dell'Autorità Nazionale competente NIS, i soggetti essenziali e i soggetti importanti COMUNICANO e AGGIORNANO, tramite la piattaforma resa disponibile dall'ACN, un elenco delle proprie attività e dei propri servizi, comprensivo di tutti gli elementi necessari alla loro caratterizzazione e della relativa attribuzione di una categoria di rilevanza

Nuove misure di sicurezza imposte dalla NIS 2

Novità e adempimenti richiesti per il settore dei dispositivi medici

La Direttiva NIS 2 fornisce un elenco di sicurezza minima di base che le aziende dovranno implementare, imponendo altresì un approccio di gestione del rischio. Le misure sono basate su un approccio multirischio allo scopo di proteggere i sistemi informatici e di rete e il loro ambiente fisico da incidenti.

Adottare
politiche di
Cybersicurezza

- **Politiche di analisi dei rischi e di sicurezza dei sistemi informatici**

Obblighi di
segnalazione

- **Gestione degli incidenti (con obblighi di notifica)**

Soggetti tenuti
all'adozione delle
misure di gestione
dei rischi per la
sicurezza
informatica

**Soggetti essenziali e soggetti
importanti**

Adozione delle misure

**Organi di amministrazione e
organi direttivi**

Approvazione delle modalità di
implementazione

Controllo sull'implementazione
delle misure

Novità e adempimenti richiesti per il settore dei dispositivi medici

Art. 24 del D.lgs. 138/2024 impone l'adozione di misure di sicurezza adeguate, aggiornate e proporzionate al livello di rischio, con un approccio che combina la precisione tecnica alla responsabilità gestionale.



Si richiede che ogni misura implementata rispecchi il massimo grado di avanzamento tecnologico, in costante armonia con le best practice e i regolamenti nazionali, europei ed internazionali.



Questo requisito evidenzia l'importanza di un continuo aggiornamento e miglioramento delle politiche di sicurezza, affinché siano adeguate a fronteggiare le minacce in continua evoluzione.

1 OTTOBRE 2026

18 mesi dalla ricezione della
comunicazione dell'Autorità
competente (da farsi entro il 31
marzo 2025)

Timeline per
l'adozione delle
misure di sicurezza

Art. 24 comma 3

- ▶ Sicurezza della catena di approvvigionamento, inclusi gli aspetti relativi alla sicurezza sui rapporti tra ciascun soggetto e i suoi diretti fornitori o fornitori di servizi.
- ▶ Il legislatore definisce uno specifico criterio di adeguatezza delle misure: vulnerabilità specifiche per ogni diretto fornitore e fornitore di servizi e qualità complessiva dei prodotti e delle pratiche di sicurezza informatica dei propri fornitori e fornitori di servizi, comprese le loro procedure di sviluppo sicuro, tenendo anche conto dei risultati delle valutazioni coordinate dei rischi per la sicurezza delle catene di approvvigionamento critiche effettuate dal Gruppo di cooperazione NIS.

Nell'ambito del primo censimento di un nuovo fornitore ovvero nella valutazione periodica dei fornitori esistenti è necessario effettuare una **valutazione completa dei rischi** per comprendere i potenziali rischi per la sicurezza, con un focus sulle policy, sulle pratiche e sulla cronologia delle violazioni di sicurezza informatica dei fornitori potenziali ed attuali - ad esempio mediante la revisione delle certificazioni dei fornitori (ad esempio, ISO 27001 - Standard di Sicurezza Informatica) e la conformità a qualsiasi altro standard di sicurezza pertinente.



Art 25 obblighi di segnalazione

Novità e adempimenti richiesti per il settore dei dispositivi medici



I soggetti «essenziali» e i soggetti «importanti» notificano, **senza ingiustificato ritardo**, al CSIRT (*Computer Security Incident Response Team*)* Italia ogni incidente che, ai sensi dell'art. 24, comma 4 del D.Lgs. 138/2024, ha un **impatto significativo sulla fornitura dei loro servizi**, secondo le modalità e i termini di cui agli articoli 30, 31 e 32 del D.Lgs. 138/2024.



Il CSIRT Italia è istituito presso l'Agenzia per la cybersicurezza nazionale. I compiti del CSIRT sono definiti dal D. Lgs. 65/2018 e dal D.M. dell'8 agosto 2019 art. 4, tra cui: monitoraggio degli incidenti a livello nazionale; emissione di preallarmi, allerte, annunci e divulgazione di informazioni alle parti interessate in merito a rischi e incidenti; l'intervento in caso di incidente; l'analisi dinamica dei rischi e degli incidenti; la sensibilizzazione situazionale; la partecipazione alla rete dei CSIRT.



I soggetti essenziali e i soggetti importanti notificano, senza ingiustificato ritardo, al CSIRT (*Computer Security Incident Response Team*) Italia ogni incidente che, ai sensi dell'art. 25, comma 4 D.Lgs. 138/2024, ha un impatto significativo sulla fornitura dei loro servizi, secondo le modalità e i termini di cui agli articoli 30, 31 e 32 del D.Lgs. 138/2024.

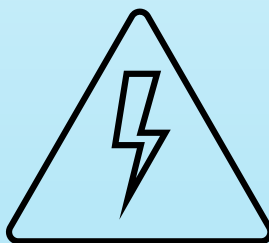


Il CSIRT Italia è istituito presso l'Agenzia per la cybersicurezza nazionale. I compiti del CSIRT sono definiti dal D. Lgs. 65/2018 e dal D.M. dell'8 agosto 2019 art. 4, tra cui:
monitoraggio degli incidenti a livello nazionale;
emissione di preallarmi, allerte, annunci e divulgazione di informazioni alle parti interessate in merito a rischi e incidenti;
l'intervento in caso di incidente; l'analisi dinamica dei rischi e degli incidenti;
la sensibilizzazione situazionale; la partecipazione alla rete dei CSIRT.

Perimetro delle notifiche obbligatorie

Ai fini della notifica, si intende un ‘incidente significativo’ un incidente che abbia un impatto rilevante sulla sicurezza delle reti e dei sistemi informatici utilizzati per la fornitura di servizi essenziali e importanti

l’impatto è valutato sulla base di criteri quali la durata dell’incidente, il numero di utenti potenzialmente interessati, la gravità delle conseguenze e l’estensione geografica dell’incidente



Segnalazione

Ingiustificato ritardo

I soggetti interessati devono effettuare una pre-notifica entro 24 ore dal rilevamento dell'incidente, o dal momento in cui si ritiene probabile che l'incidente possa avere un impatto significativo. Entro 72 ore, un'altra notifica deve aggiornare le informazioni, fornendo una valutazione iniziale dell'incidente, indicandone gravità, impatto e indicatori di compromissione, presenti.

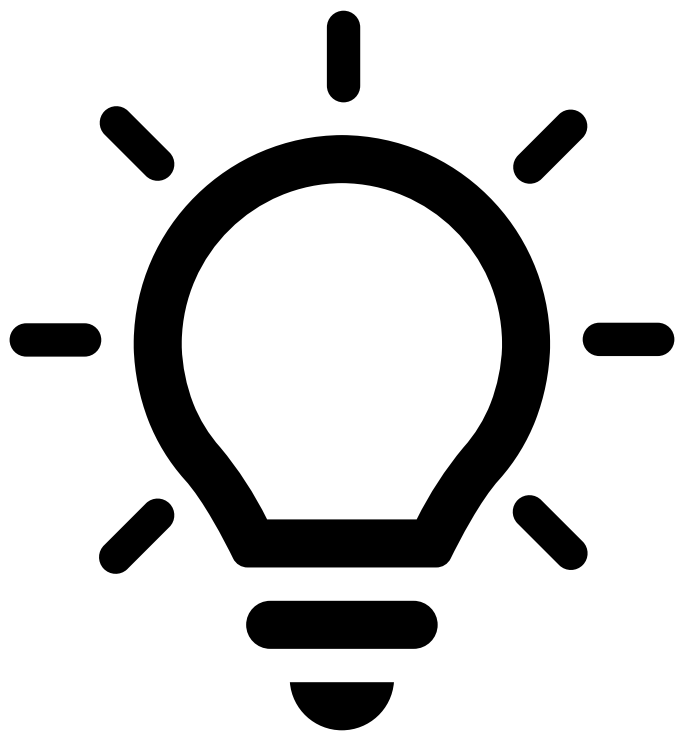
Impatto significativo

Le notifiche devono includere informazioni dettagliate riguardanti l'incidente, quali la natura dell'attacco, l'origine, le vulnerabilità sfruttate, l'entità dell'impatto sui servizi, e le misure adottate per mitigare l'incidente.

Relazione

La notifica deve essere seguita da una relazione intermedia dettagliata entro una settimana dall'incidente, contenente una valutazione più approfondita delle cause e delle misure correttive adottate.

Deve seguire poi, entro un mese, una relazione finale che comprenda la descrizione dell'incidente e delle minacce causate, nonché le misure adottate e l'impatto transfrontaliero dell'incidente.



L'ACN ha pubblicato sul suo sito una «*Guida alla notifica degli incidenti*», che costituisce il modello per adempiere a questo obbligo essenziale.

I soggetti essenziali e importanti sono tenuti a fornire tutte le informazioni utili al CSIRT Italia per analizzare l'incidente e a collaborare attivamente per individuare le misure di mitigazione più appropriate. Questo obbligo di cooperazione è esteso anche i fornitori di servizi digitali, che sono invitati a condividere informazioni rilevanti con gli altri operatori del settore al fine di prevenire di propagarsi delle minacce

Obbligo di
cooperazione

Novità e adempimenti richiesti per il settore dei dispositivi medici

In caso di incidenti che possano comportare un impatto diretto sulla sicurezza pubblica o sui diritti degli utenti, si prevede la possibilità per il CSIRT di informare il pubblico e i soggetti potenzialmente interessati, qualora si ritenga necessario per prevenire danni ulteriori.

Requisiti specifici per i fornitori di servizi digitali (piattaforme online, motori di ricerca e servizi di cloud computing:

questi soggetti sono tenuti a notificare qualsiasi incidente che possa compromettere la continuità o la sicurezza dei servizi offerti, con particolare attenzione alle minacce transfrontaliere.

È previsto un meccanismo di monitoraggio da parte delle autorità competenti per garantire il rispetto degli obblighi di notifica, in caso di mancata segnalazione o di ritardo ingiustificato, sono previste sanzioni amministrative proporzionate alla gravità dell'incidente e alla recidiva del soggetto interessato.

Ruolo del Ministero

Ministero della salute
è competente per

Il settore sanitario

Il sottosettore di
fabbricazione di DM e
DM diagnostici in vitro.

Novità e adempimenti richiesti per il settore dei dispositivi medici

L'art. 11 designa le Autorità di settore NIS, individuandole come entità essenziali per l'efficace attuazione della disciplina NIS a livello settoriale e dispone che debbano strettamente collaborare con l'ACN, secondo le modalità che saranno specificamente stabilite da apposito decreto (art. 40, comma 2, lettera c).

verifica e
aggiornamento
dell'elenco dei
soggetti essenziali e
importanti che si
sono iscritti in
piattaforma.

supporto ad ACN nella
individuazione di quali
soggetti iscritti in
piattaforma devono
considerarsi soggetti
Essenziali e quali
invece soggetti
Importanti.

partecipazione alle
attività settoriali del
Gruppo di
Cooperazione NIS
nonché dei consessi e
delle iniziative a
livello di Unione
europea relativi
all'attuazione della
NIS 2.

istituzione e
coordinamento dei tavoli
settoriali, al fine di
contribuire all'efficace e
coerente attuazione
settoriale del decreto
nonché al relativo
monitoraggio.

elaborazione dei
contributi per la
relazione annuale
di cui all'articolo
12, comma 5,
lettera c).

supporto per le
funzioni e per le
attività di
regolamentazione
che verranno
stabilite nel decreto
di cui all'art. 40

Definizione, con l'ACN, delle
deroghe e esenzioni
applicabili a particolari
categorie di soggetti,
contribuendo così alla
personalizzazione delle
misure di sicurezza.

Attività di rilievo



Di rilievo è il compito dell'Autorità di settore di istituire e coordinare i tavoli settoriali, luoghi di confronto tecnico e di monitoraggio in cui si sviluppano politiche mirate alla resilienza del settore di competenza.



L'art. 11 sottolinea la necessità di una cooperazione a livello europeo, prevedendo la partecipazione delle Autorità di settore al Gruppo di Cooperazione NIS e ad altre iniziative dell'UE per l'attuazione della direttiva.

In questo modo, il sistema di cybersicurezza viene allineato alle normative europee, rafforzando la dimensione internazionale.

Novità e adempimenti richiesti per il settore dei dispositivi medici



Ministero della Salute

Nota del Ministero della Salute del 14/02/2025

Direttore Dipartimento Dispositivi Medici del Ministero ha inviato una nota a tutte le associazioni del settore sanitario affinché sollecitino i loro soci a procedere alla iscrizione nella piattaforma sul portale dell'ACN, ossia:

- prestatori di assistenza sanitaria
- laboratori di riferimento dell'UE
- soggetti che svolgono attività di ricerca e sviluppo relative ai medicinali
- soggetti che fabbricano prodotti farmaceutici
- soggetti che fabbricano dispositivi medici considerati critici
- soggetti che fabbricano DM quali i dispositivi ex MDR ed i diagnostici in vitro ex IVDR



Tavolo settoriale

Con D.M. del 14 gennaio 2025 (G.U. n. 45 del 24.02.2025) è istituito presso il Ministero della salute il tavolo settoriale per l'attuazione della direttiva NIS 2, con lo scopo di contribuire all'efficace e coerente attuazione settoriale della direttiva NIS 2 in ambito sanitario, nel rispetto della vigente normativa europea e nazionale in materia di cybersicurezza e in coordinamento con l'ACN nella qualità di Autorità nazionale competente in materia, nonché al monitoraggio dell'attuazione del D.Lgs. 138/2024

MODULO 4
GESTIONE DEL RISCHIO E
COMPLIANCE ALLA NIS 2 IN
▶ **AMBITO INDUSTRIALE**

Dr.ssa Silvia Tamarri
Complife

Registrazione dei soggetti NIS2 sul portale ACN

Chi deve registrarsi?

- ▶ **Soggetti essenziali e importanti:** imprese che operano nei settori critici definiti negli allegati del D.Lgs. 138/2024.
- ▶ **Imprese collegate:** aziende che influenzano o supportano direttamente la sicurezza cibernetica dei soggetti essenziali e importanti.
- ▶ **Pubbliche amministrazioni:** incluse quelle di grandi dimensioni o strategiche (e.g., comuni con oltre 100.000 abitanti).



Registrazione dei soggetti NIS2 sul portale ACN

Dove effettuare la registrazione?

<https://portale.acn.gov.it/login>

Chi?

PUNTO DI CONTATTO>>PERSONA FISICA O DELEGATO

- ▶ una persona fisica con adeguati poteri di rappresentanza (legale rappresentante o altro procuratore generale coerentemente con quanto risulti dall'iscrizione nel registro delle imprese)
- ▶ è possibile **delegare** un altro soggetto, caricando nel portale la relativa delega (ecco il Modello suggerito di Delega del Punto di contatto) opportunamente compilata.



Registrazione dei soggetti NIS2 sul portale ACN

I STEP

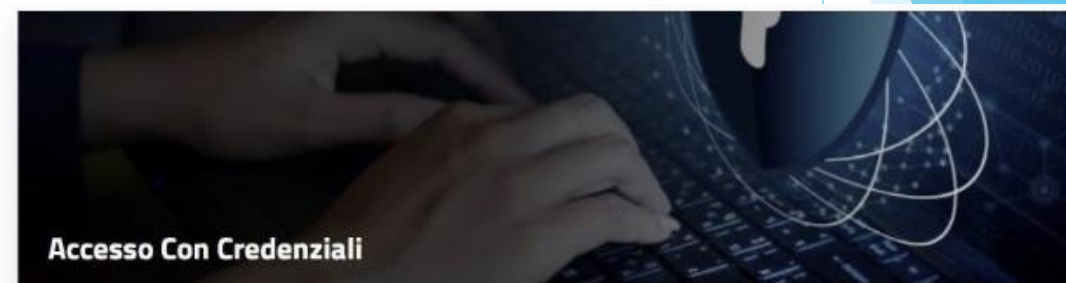
<https://portale.acn.gov.it/login>



Accesso Con SPID

Da qui potrai accedere al portale tramite **SPID**

Accedi con SPID



Accesso Con Credenziali

Da qui potrai accedere con le tue **credenziali**

Inserisci username e password per accedere al portale

Accedi con credenziali

Registrazione dei soggetti NIS2 sul portale ACN

I passaggi della procedura:

- ▶ **Iscrizione Iniziale:** Censimento e associazione all'organizzazione inserendo codice fiscale o IPA
- ▶ **Conferma:** organizzazione riceverà dall'agenzia nazionale per la cybersicurezza una PEC per convalidare il censimento
- ▶ Il punto di contatto deve **compilare** i dati dell'organizzazione relativi al contesto, caratterizzazione e tipologie di soggetto
- ▶ Il punto di contatto deve effettuare l'**autovalutazione** dell'organizzazione come soggetto essenziale importante o fuori ambito
- ▶ Il punto di contatto deve verificare e confermare tutte le informazioni inserite

ATTENZIONE!!!

- non interrompere a metà la registrazione alla NIS 2
- monitorate sempre la casella email inserita



Registrazione dei soggetti NIS2 sul portale ACN

Chiarimenti sulle Normative EU:

- ▶ Durante la registrazione, il portale richiede di indicare l'applicazione di ulteriori normative europee, spesso identificate solo dai riferimenti legislativi. Sono normative molto specifiche, è molto frequente la non applicabilità

Ambito	Normative
Mercato interno dell'energia elettrica	• Dir. (UE) 2019/944 • Reg. (UE) 2019/943
Promozione dell'uso dell'energia da fonti rinnovabili	• Dir. (UE) 2018/2001
Livello minimo di scorte di petrolio greggio e/o di prodotti petroliferi	• Dir. 2009/119/CE
Sicurezza dell'aviazione civile	• Reg. (CE) 300/2008
Diritti aeroportuali	• Dir. 2009/12/CE
Rete transeuropea dei trasporti	• Reg. (UE) 315/2013
Principi generali per l'istituzione del cielo unico europeo	• Reg. (CE) 549/2004
Spazio ferroviario europeo unico	• Dir. 2012/34/UE



Registrazione dei soggetti NIS2 sul portale ACN

Cosa si intende per società collegate?

- ▶ Indicare se l'azienda fa parte di un gruppo e fornire il codice fiscale della CapoGruppo
- ▶ Indicare le società collegate.

Sono “imprese collegate” le imprese tra cui esiste una delle seguenti relazioni:

- ▶ un'impresa detiene la maggioranza dei diritti di voto degli azionisti o soci di un'altra impresa
- ▶ un'impresa ha il diritto di nominare o revocare la maggioranza dei membri del Consiglio di amministrazione, direzione o sorveglianza di un'altra impresa
- ▶ un'impresa ha il diritto di esercitare un'influenza dominante su un'altra impresa in virtù di un contratto concluso con quest'ultima oppure in virtù di una clausola dello statuto di quest'ultima
- ▶ un'impresa azionista o socia di un'altra impresa controlla da sola, in virtù di un accordo stipulato con altri azionisti o soci dell'altra impresa, la maggioranza dei diritti di voto degli azionisti o soci di quest'ultima.



Registrazione dei soggetti NIS2 sul portale ACN

Cos'è la clausola di salvaguardia?

richiedere una deroga al calcolo delle dimensioni aziendali (dipendenti, fatturato e bilancio) tenendo conto del grado di indipendenza dai sistemi informativi e di rete delle imprese collegata

[CRT.4] Clausola di salvaguardia

L'organizzazione ritiene sproporzionata l'applicazione dell'articolo 6, paragrafo 2, dell'allegato alla Raccomandazione 2003/361/CE e vuole richiedere la clausola di salvaguardia di cui all'articolo 3, comma 4, del decreto NIS?

☐ Sì ☒ No



Registrazione dei soggetti NIS2 sul portale ACN

Settori e sottosettori economici

Durante la registrazione dell'azienda, bisognerà selezionare uno o più settori di attività, corrispondenti all'elenco di settori critici citati nel Decreto. Si consideri che in questa fase, la procedura terrà conto dei codici ATECO già inseriti per “suggerire” le probabili attività svolte, segnalando possibili dimenticanze o incoerenze nella compilazione.

Il principale suggerimento pratico per l'individuazione delle attività svolte, è quello di consultare anticipatamente e con attenzione direttamente l'allegato I e l'allegato II della norma, dove risultano chiaramente schematizzati e di immediata lettura.



Registrazione dei soggetti NIS2 sul portale ACN

Entro Aprile 2025

- ▶ Autorità NIS comunicherà se l'organizzazione rientra nell'ELENCO dei soggetti NIS



Strategie per la gestione del rischio cibernetico

I soggetti essenziali e i soggetti importanti adottano misure tecniche, operative e organizzative adeguate e proporzionate, secondo le modalità e i termini di cui agli articoli 30, 31 e 32, alla gestione dei rischi posti alla sicurezza dei sistemi informativi e di rete che tali soggetti utilizzano nelle loro attività o nella fornitura dei loro servizi, nonché per prevenire o ridurre al minimo l'impatto degli incidenti per i destinatari dei loro servizi e per altri servizi.

- ▶ Misure tecniche;
- ▶ Operative;
- ▶ Organizzative;
- ▶ Adeguate e proporzionate

Caratteristica delle misure

- ▶ Assicurano un livello di sicurezza dei sistemi informativi di rete adeguato ai rischi esistenti, tenuto conto delle conoscenze più aggiornate e dello stato dell'arte in materia e, ove applicabile, delle pertinenti norme nazionali, europee e internazionali, nonché dei costi di attuazione;
- ▶ Sono proporzionate al grado di esposizione a rischi del soggetto, alle dimensioni del soggetto e alla probabilità che si verifichino incidenti, nonché alla loro gravità, compreso il loro impatto sociale ed economico.

Costante
Aggiornamento

Tenendo conto
delle
conoscenze più
aggiornate e dello
stato dell'arte

Tenendo conto
delle pertinenti
norme nazioni
europee e
internazioni

Il management del rischio



Le misure di cui al comma 1 sono basate su un approccio multi-rischio, volto a proteggere i sistemi informativi e di rete nonché il loro ambiente fisico da incidenti

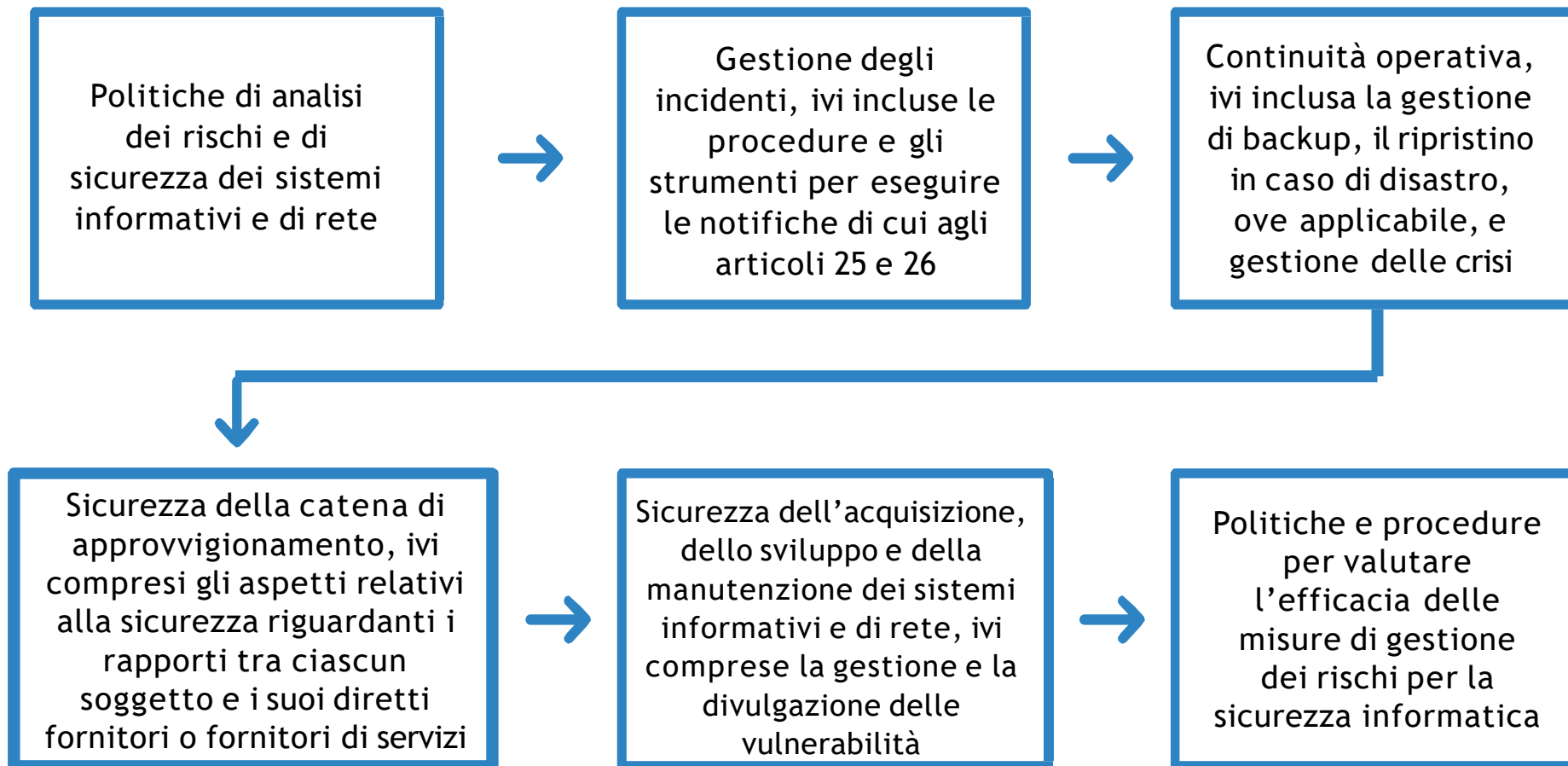


Per approccio multirischio si intende una strategia di protezione e gestione che prende in considerazione la molteplicità dei rischi che possono minacciare un sistema



Nell'approccio multirischio occorre tenere in considerazione tutti i potenziali fattori di rischio, compresi quelli fisici e digitali, prevedendo misure di sicurezza integrate e sinergiche

Il management del rischio



Il management del rischio

Pratiche di igiene di base e di formazione in materia di sicurezza informatica;

Politiche e procedure relative all'uso della crittografia e, ove opportuno, della cifratura;

Sicurezza e affidabilità del personale, politiche di controllo dell'accesso e gestione dei beni e degli assetti;

L'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, ove opportuno.

Modalità

Nel valutare quali misure siano adeguate, i soggetti tengono conto delle vulnerabilità specifiche per ogni diretto fornitore e fornitore di servizi e della qualità complessiva dei prodotti e delle pratiche di sicurezza informatica dei propri fornitori e fornitori di servizi, comprese le loro procedure di sviluppo sicuro. Per la medesima finalità i soggetti tengono altresì conto dei risultati delle valutazioni coordinate dei rischi per la sicurezza delle catene di approvvigionamento critiche effettuate dal Gruppo di cooperazione NIS.



Analisi sartoriale
dei fornitori

Modalità

Esempi di best practice in relazione agli obblighi di cui all'art. 24 del D. Lgs. 138/2024

Società	Best practices
DIESEC GmbH	➤ Conduct a clear risk analysis to decide on adequate cybersecurity measures ➤ Tackle risks using an all-hazards approach ➤ Improve supply chain security ➤ Plan and practice incident response ➤ Recognize that cybersecurity has board-level accountability ➤ Use certifications to benefit your NIS2 compliance
Esprinet S.p.A.	➤ Network Security ➤ End Point Protection ➤ Secure Identity and Access Management Solutions per Cyber Security ➤ Security and Vulnerability Management ➤ Advanced Threat Protection ➤ Content Security ➤ Automated Security and Monitoring Solutions

Verifiche e ispezioni

Ai fini del monitoraggio le autorità competenti possono richiedere

► DOCUMENTAZIONE:

- Politiche e procedure di sicurezza: Dettagli sui controlli di sicurezza implementati.
- Valutazione dei rischi: Rapporti sulle analisi dei rischi effettuate.
- Piani di gestione degli incidenti: Documenti che descrivono le procedure da seguire in caso di incidente informatico.
- Piano di continuità operativa e disaster recovery: Strategie per garantire la continuità dei servizi critici.
- Registro degli incidenti: Un elenco degli incidenti di sicurezza gestiti, con dettagli su come sono stati risolti.

Verifiche e ispezioni

Ai fini del monitoraggio le autorità competenti possono richiedere

► **Rapporti di monitoraggio:**

- Rapporti periodici: Informazioni sull'implementazione delle misure di sicurezza.
- Report sugli incidenti: Dettagli sugli incidenti segnalati, incluse cause e azioni correttive adottate.
- Metriche di sicurezza: Indicatori che mostrano lo stato della sicurezza, come numero di tentativi di accesso non autorizzato o vulnerabilità risolte.

► **Accesso a sistemi e infrastrutture**

- Ispezioni tecniche: Accesso ai sistemi IT per verificare configurazioni, log e sicurezza.
- Test di penetrazione: Possibilità di eseguire test di sicurezza (anche da parte di terzi autorizzati).
- Audit: Verifiche dettagliate sui controlli di sicurezza e la loro efficacia.

Verifiche e ispezioni

Ai fini del monitoraggio le autorità competenti possono richiedere

► Prove di conformità

- Certificazioni di sicurezza: Dimostrazione che l'organizzazione ha ottenuto certificazioni come ISO 27001 o altre equivalenti.
- Prove di formazione: Evidenze che i dipendenti hanno ricevuto formazione sulla sicurezza informatica.

► Segnalazione obbligatoria di incidenti

- Notifica di incidenti rilevanti: L'organizzazione deve segnalare alle autorità qualsiasi incidente che possa avere un impatto significativo sui suoi servizi essenziali.
- Dettagli sull'incidente: Descrizione dell'accaduto, analisi delle cause, e azioni intraprese per mitigarlo.

Verifiche e ispezioni

Ai fini del monitoraggio le autorità competenti possono richiedere

► Piani di miglioramento

- Azioni correttive: Le autorità possono richiedere un piano per colmare eventuali lacune di conformità riscontrate.
- Tempistiche: Scadenze per implementare le misure necessarie.

► Collaborazione con altre parti

- Partecipazione a esercitazioni: Le autorità possono richiedere la partecipazione a simulazioni o esercitazioni di crisi informatiche.
- Condivisione di informazioni: Contributo a reti di condivisione delle informazioni (ISACs o simili).

Verifiche e ispezioni

- ▶ Verifiche della documentazione e delle informazioni trasmesse
- ▶ Ispezioni in loco e a distanza, compresi controlli casuali
- ▶ Richieste di accesso a dati, documenti e altre informazioni necessari allo svolgimento dei poteri dichiarando la finalità della richiesta e specificando le informazioni richieste ai soggetti.

D'ufficio

Casuali
(non necessario
disastro)

Accesso ai dati
previa
motivazione



MODULO 5 SANZIONI PER MANCATA CONFORMITA' ALLA NIS 2



**Avv. Giuseppe Strano
A.L.I. & Partners**

Art 38 -Sanzioni

Art. 38 del D.Lgs. 138/2024

Disciplina le sanzioni amministrative nell'ambito della sicurezza informatica, conferendo all'Autorità nazionale competente NIS ampi poteri per monitorare e sanzionare le violazioni da parte dei soggetti obbligati, secondo i principi di:

effettività

proporzionalità

dissuasività

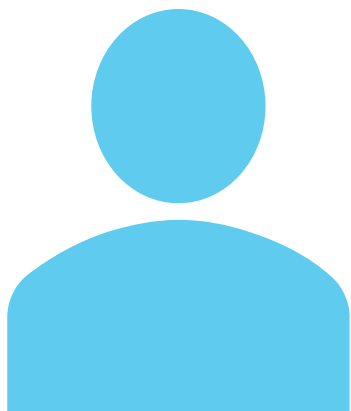
Valutazione

L'Autorità nazionale competente NIS, ai fini dell'esercizio dei suoi poteri sanzionatori, tiene anche conto degli esiti delle attività di monitoraggio, supporto e analisi, delle risultanze dell'esercizio dei poteri di verifica e ispettivi, nonché dell'esercizio dei poteri di esecuzione.

Correttezza degli
adempimenti

Grado di collaborazione

Regime di responsabilità



- ▶ Qualsiasi persona fisica responsabile di un soggetto essenziale o che agisca in qualità di suo rappresentante legale con l'autorità di rappresentarlo, di prendere decisioni per suo conto o di esercitare un controllo sul soggetto stesso, assicura il rispetto delle disposizioni di cui al presente decreto. **Tali persone fisiche possono essere ritenute responsabili dell'inadempimento in caso di violazione del presente decreto da parte del soggetto di cui hanno rappresentanza.**
- ▶ Qualora il soggetto non adempia nei termini stabiliti dalla diffida di cui all'art. 37 l'ACN NIS può disporre nei confronti delle persone fisiche, ivi inclusi gli organi di amministrazione e gli organi direttivi dei soggetti essenziali e dei soggetti importanti, nonché di quelle che svolgono funzioni dirigenziali a livello di amministratore delegato o rappresentante legale di un soggetto essenziale o importante, **l'applicazione della sanzione amministrativa accessoria della incapacità a svolgere funzioni dirigenziali all'interno del medesimo soggetto.** Tale sospensione temporanea è applicata finché il soggetto interessato non adotta le misure necessarie a porre rimedio alle carenze o a conformarsi alle diffide di cui all'articolo 37, commi 6 e 7 del D.Lgs. 138/2024

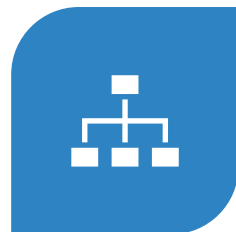
Violazioni Sanzionate



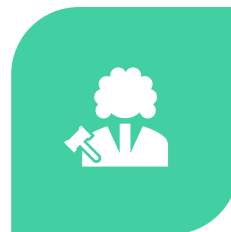
Mancata osservanza degli obblighi imposti dall'articolo 23 agli organi di amministrazione e agli organi direttivi, nonché degli obblighi relativi alla gestione del rischio per la sicurezza informatica e alla notifica di incidente, di cui agli articoli 24 e 25.



L'inottemperanza alle disposizioni adottate dall'Autorità nazionale competente NIS (art. 37, commi 3 e 4) e alle relative diffide (esecuzione di audit sulla sicurezza, esecuzione di scansioni di sicurezza, osservanza di istruzioni vincolanti date dall'Autorità competente NIS).



**SOGGETTI
ESSENZIALI:** FINO
AD EURO 10 MIO O
AL 2% DEL
FATTURATO
GLOBALE ANNUO, A
SECONDA DI QUALE
SIA PIÙ ALTO



**SOGGETTI
IMPORTANTI:** FINO AD
EURO 7 MIO O
ALL'1,4% DEL
FATTURATO GLOBALE
ANNUO, SE
SUPERIORE



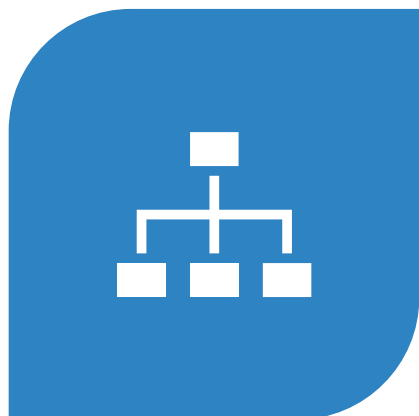
**PUBBLICHE
AMMINISTRAZIONI:**
DA 25.000 A 125.000
DI EURO PER
SOGGETTI
ESSENZIALI, MENTRE
TALI IMPORTI SONO
RIDOTTI DI UN TERZO
PER I SOGGETTI
IMPORTANTI

Ammontare delle sanzioni

Altre Violazioni Sanzionate

- ▶ mancata registrazione, aggiornamento e comunicazione delle informazioni previste dall'art. 7 (registrazione sul portale reso disponibile dall'ACN)
- ▶ inosservanza delle modalità e degli standard prescritti dall'Autorità NIS per le comunicazioni
- ▶ mancata comunicazione o aggiornamento dell'elenco delle attività e dei servizi e della loro categorizzazione ai sensi dell'art. 30, comma 1
- ▶ violazione degli obblighi settoriali specifici, stabiliti dagli artt. 27, 29 e 32
- ▶ inadempimento degli obblighi di collaborazione con l'Autorità NIS e con il CSIRT

Sanzioni per mancata conformità alla NIS 2



SOGGETTI ESSENZIALI: FINO ALLO
0,1% DEL FATTURATO GLOBALE
ANNUO.



SOGGETTI IMPORTANTI: FINO ALLO
0,07% DEL FATTURATO GLOBALE ANNUO.



PUBBLICHE AMMINISTRAZIONI: DA 10.000 A
50.000 € PER SOGGETTI ESSENZIALI, MENTRE
TALI IMPORTI SONO RIDOTTI DI UN TERZO PER I
SOGGETTI IMPORTANTI.

Ammontare delle sanzioni

Sanzioni per mancata conformità alla NIS 2

Invito a conformarsi: l'Autorità che rileva la possibile frazione, offre al soggetto la possibilità di sanare, entro congruo termine, l'inadempienza senza incorrere immediatamente in una sanzione.

Pagamento in misura ridotta: entro 60gg dalla notifica della violazione, il soggetto può optare per l'estinzione anticipata della sanzione con il pagamento pari a un terzo del massimo della sanzione o, se più favorevole, al doppio del minimo edittale previsto.

Esenzione dalla pubblicità delle sanzioni, nei casi in cui la pubblicità delle sanzioni risulti non necessaria o sproporzionata.

Sistemi deflattivi e meccanismi di riduzione della sanzione

Convergenza tra Regolamenti 2017/745 e 2017/746 e NIS2

La NIS2 e i Regolamenti (UE) 2017/745 e 2017/746 perseguono finalità diverse: il primo è relativo alla cybersecurity, mentre il secondo alla sicurezza del prodotto e, quindi, dei pazienti e degli individui.

Vi è astrattamente un piano di sovrapposizione in quanto l'applicazione dei Regolamenti sui DM si basa anche su una serie di requisiti per la sicurezza informatica dei DM stessi.



MODULO 6

REGOLAMENTAZIONE DELLA CYBERSECURITY DEI ▶ DISPOSITIVI MEDICI

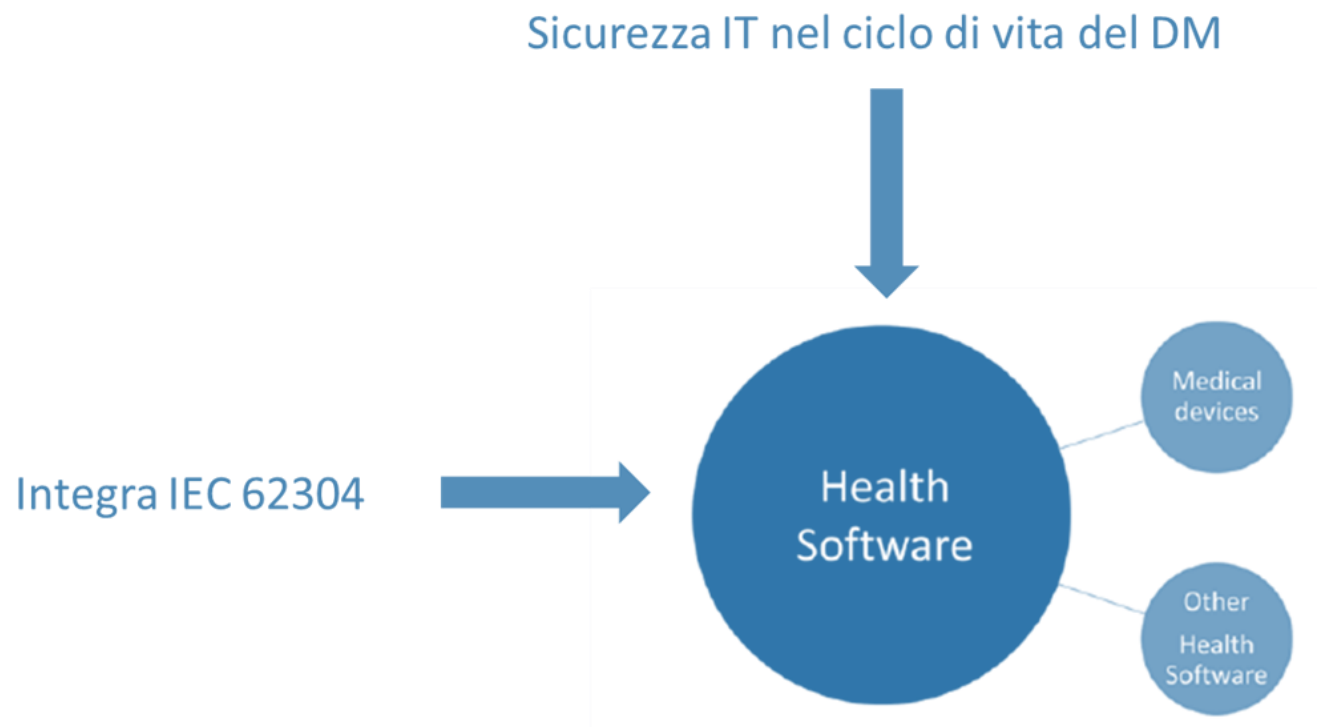
Dr.ssa Silvia Tamarri
Complife

Cybersecurity: regolamenti, norme e linee guida

- ▶ **MDR** - Regolamento Dispositivi Medici (UE) 2017/745
- ▶ **EN ISO 14971** Dispositivi medici — Applicazione della gestione dei rischi ai dispositivi medici
- ▶ **IEC 62304** - Medical device software - Software life cycle processes
- ▶ **IEC 81001-5-1** Health software and health IT systems safety, effectiveness and security — Part 5-1: Security — Activities in the product life cycle
- ▶ **IEC 82304-1:2016** Health software Part 1: General requirements for product safety
- ▶ **IEC/TR 60601-4-5** Medical Electrical Equipment - Part 4-5: Safety related technical security specifications for medical devices
- ▶ **IEC/TR 80002-1** Medical device software - Part 1: Guidance on the application of ISO 14971 to medical device software
- ▶ **MDCG 2019-16** Guidance on Cybersecurity for medical devices

Cybersecurity: IEC 81001-5-1:2021

Health software and health IT systems safety, effectiveness and security –
Part 5-1: Security – Activities in the product life cycle



Cybersecurity: IEC 81001-5-1:2021

Health software and health IT systems safety, effectiveness and security –
Part 5-1: Security – Activities in the product life cycle

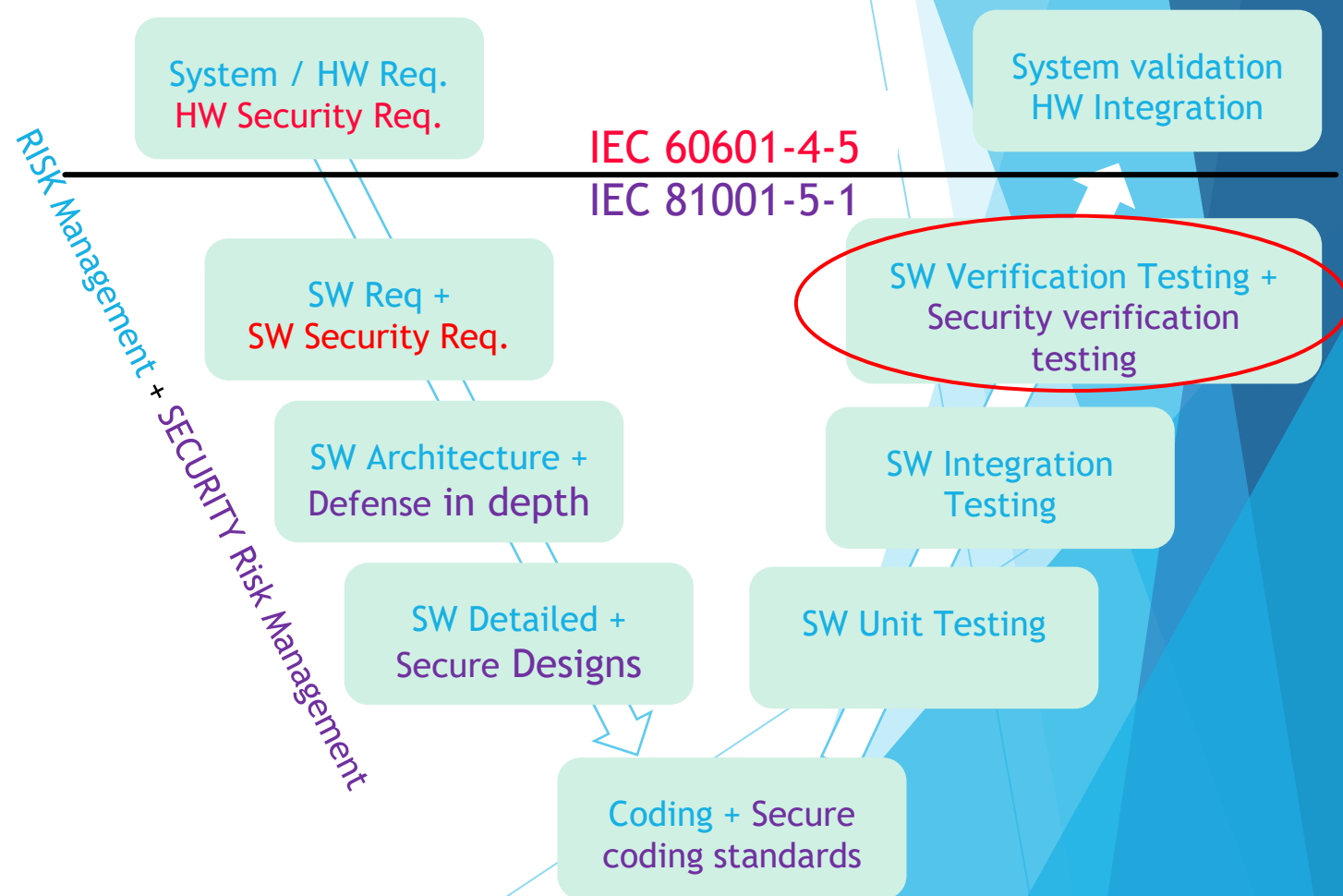


NOTA BENE: tutti i requisiti della IEC 81001-5-1 sono applicabili a qualsiasi software a prescindere dalla classe: A,B,C

Regolamentazione della cybersecurity dei dispositivi medici

EN 81001-5-1 e IEC/TR 60601-4-5

- ▶ **HOW:** IEC 81001-5-1: requisiti complementari di cybersecurity da integrare all'interno del **processo** descritto da EN 62304
- ▶ **WHAT:** IEC - TR 60601-4-5 definisce una lista di requisiti di sicurezza che possono essere implementati all'interno di un dispositivo medico (req. sia hardware che software)



Cybersecurity: MDCG 2019-16

Scopo: fornire ai fabbricanti indicazioni su come soddisfare tutti i requisiti generali pertinenti dell'**Allegato I** del Regolamento Dispositivi Medici (UE) 2017/745 per quanto riguarda la sicurezza informatica

Medical Device

Medical Device Coordination Group Document

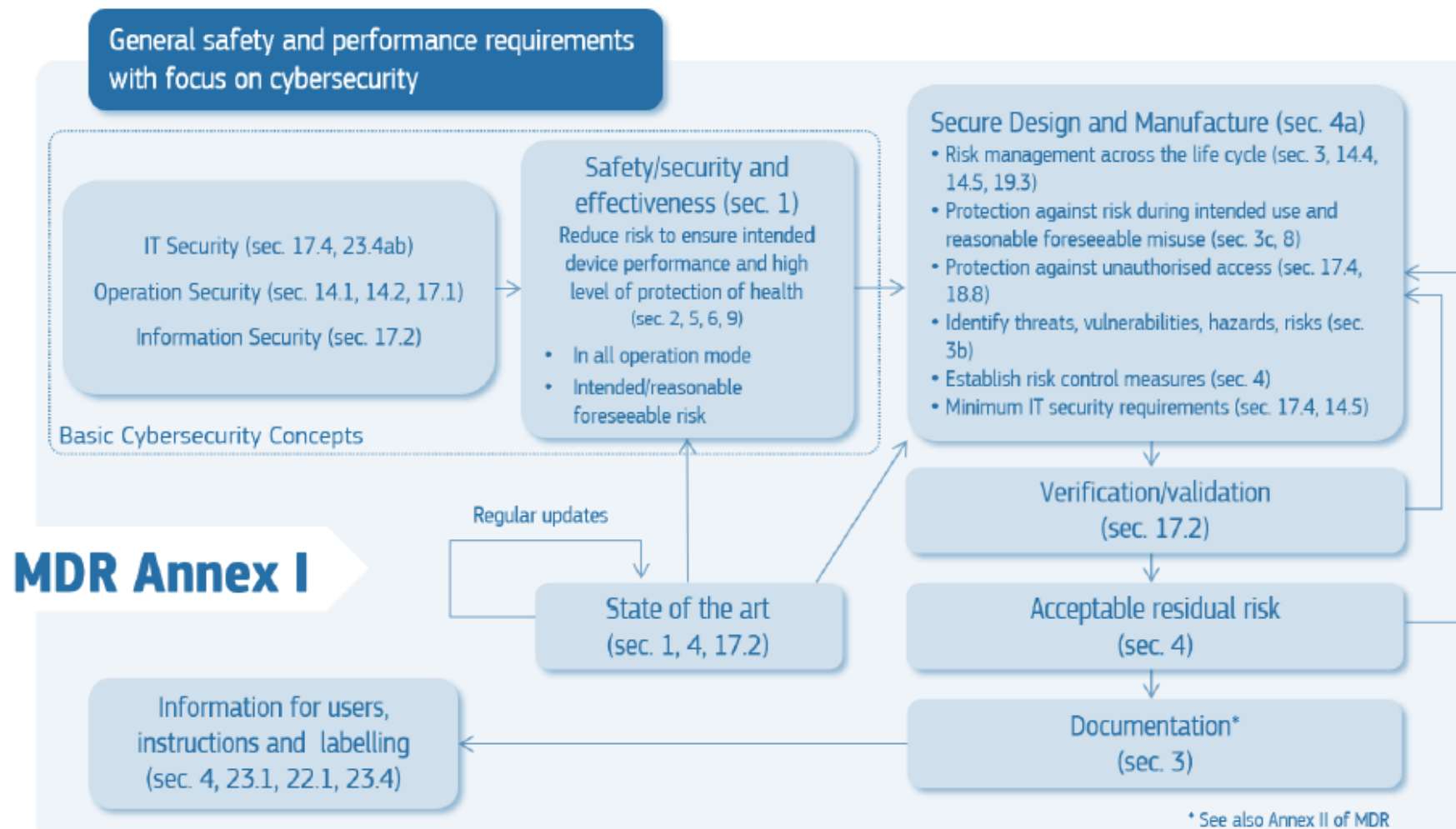
MDCG 2019-16

MDCG 2019-16 Guidance on Cybersecurity for medical devices

December 2019

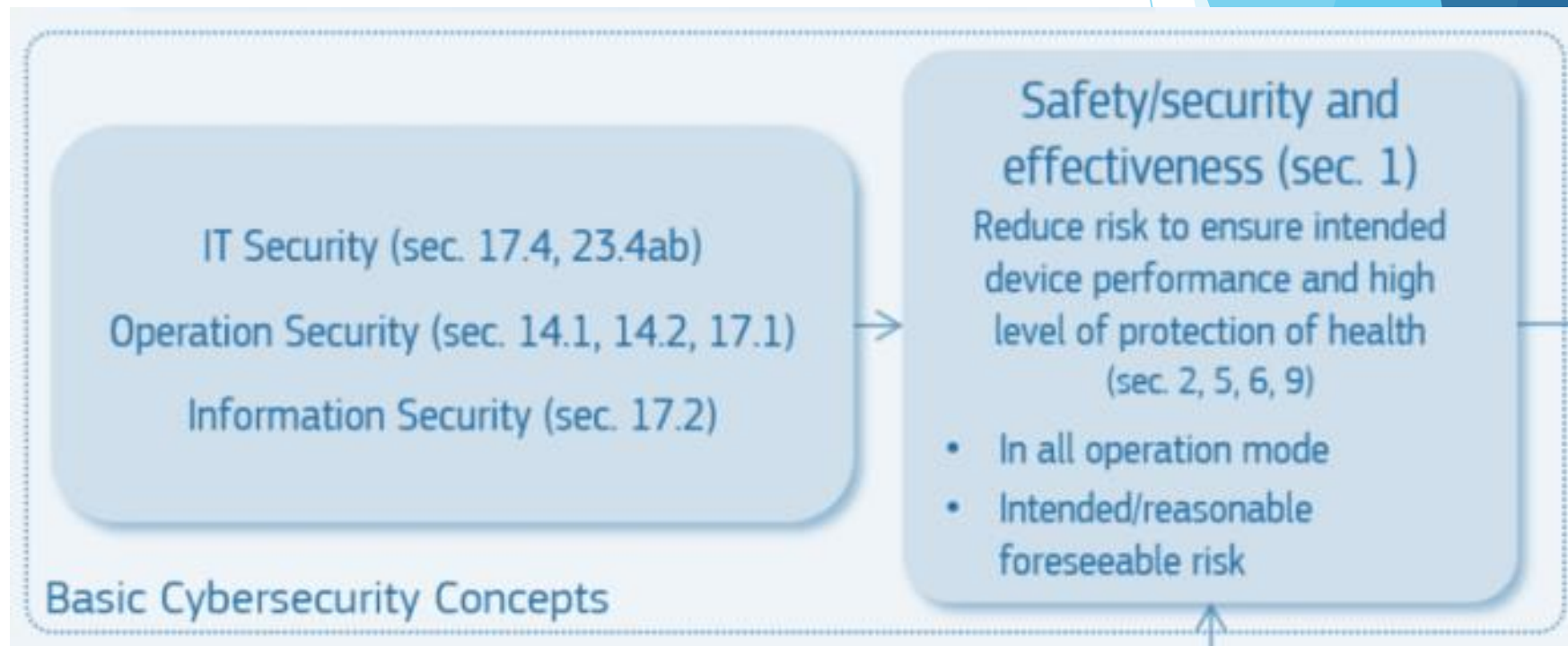
This document has been endorsed by the Medical Device Coordination Group (MDCG) established by Article 103 of Regulation (EU) 2017/745. The MDCG is composed of representatives of all Member States and it is chaired by a representative of the European Commission. The document is not a European Commission document and it cannot be regarded as reflecting the official position of the European Commission. Any views expressed in this document are not legally binding and only the Court of Justice of the European Union can give binding interpretations of Union law.

MDCG 2019-16: Requisiti di Cybersecurity in MDR



Cybersecurity: concetti base

- ▶ IT Security
- ▶ Operation Security
- ▶ Information Security



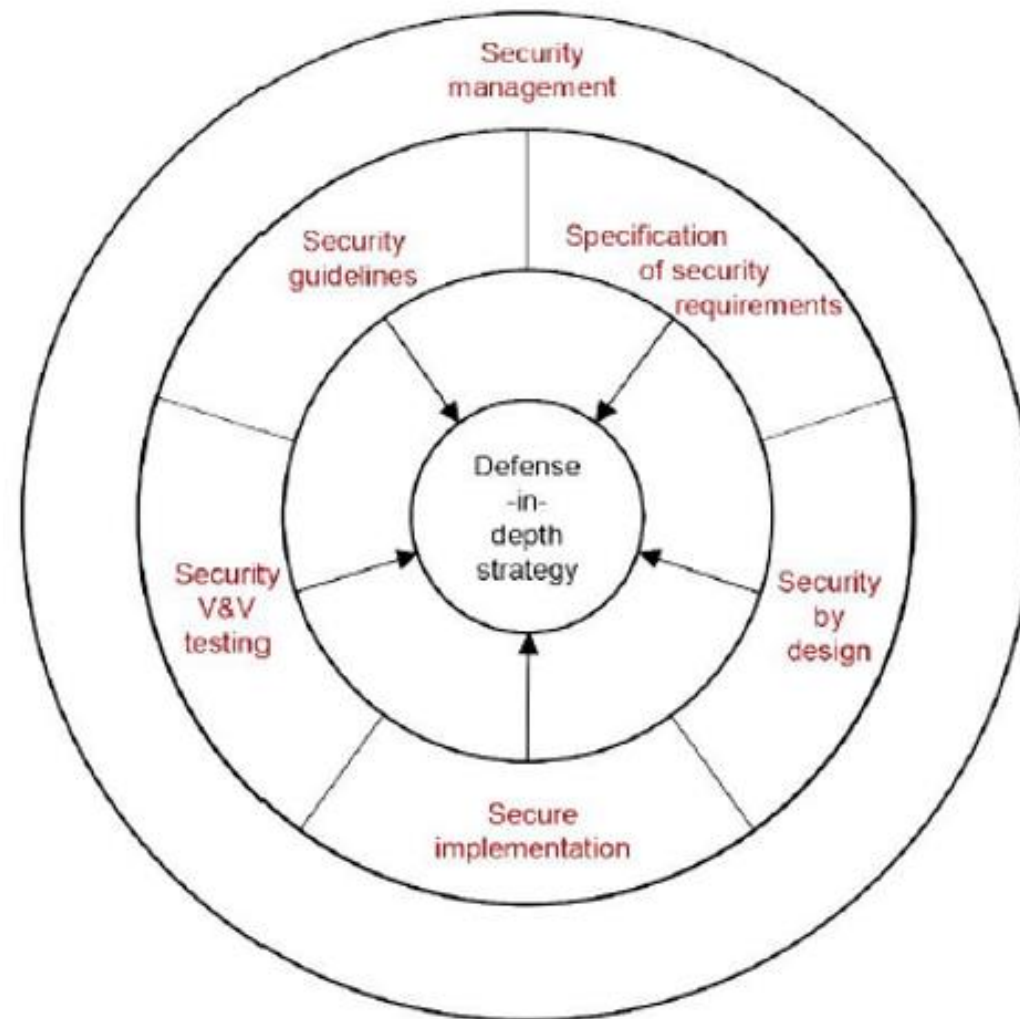
Regolamentazione della cybersecurity dei dispositivi medici

Cybersecurity: progettazione e fabbricazione sicura

Strategia di “difesa in profondità” (Defense-in-Depth)

Secure Design and Manufacture (sec. 4a)

- Risk management across the life cycle (sec. 3, 14.4, 14.5, 19.3)
- Protection against risk during intended use and reasonable foreseeable misuse (sec. 3c, 8)
- Protection against unauthorised access (sec. 17.4, 18.8)
- Identify threats, vulnerabilities, hazards, risks (sec. 3b)
- Establish risk control measures (sec. 4)
- Minimum IT security requirements (sec. 17.4, 14.5)



Regolamentazione della cybersecurity dei dispositivi medici

Cybersecurity: progettazione e fabbricazione sicura

Strategia di “difesa in profondità” (Defense-in-Depth)

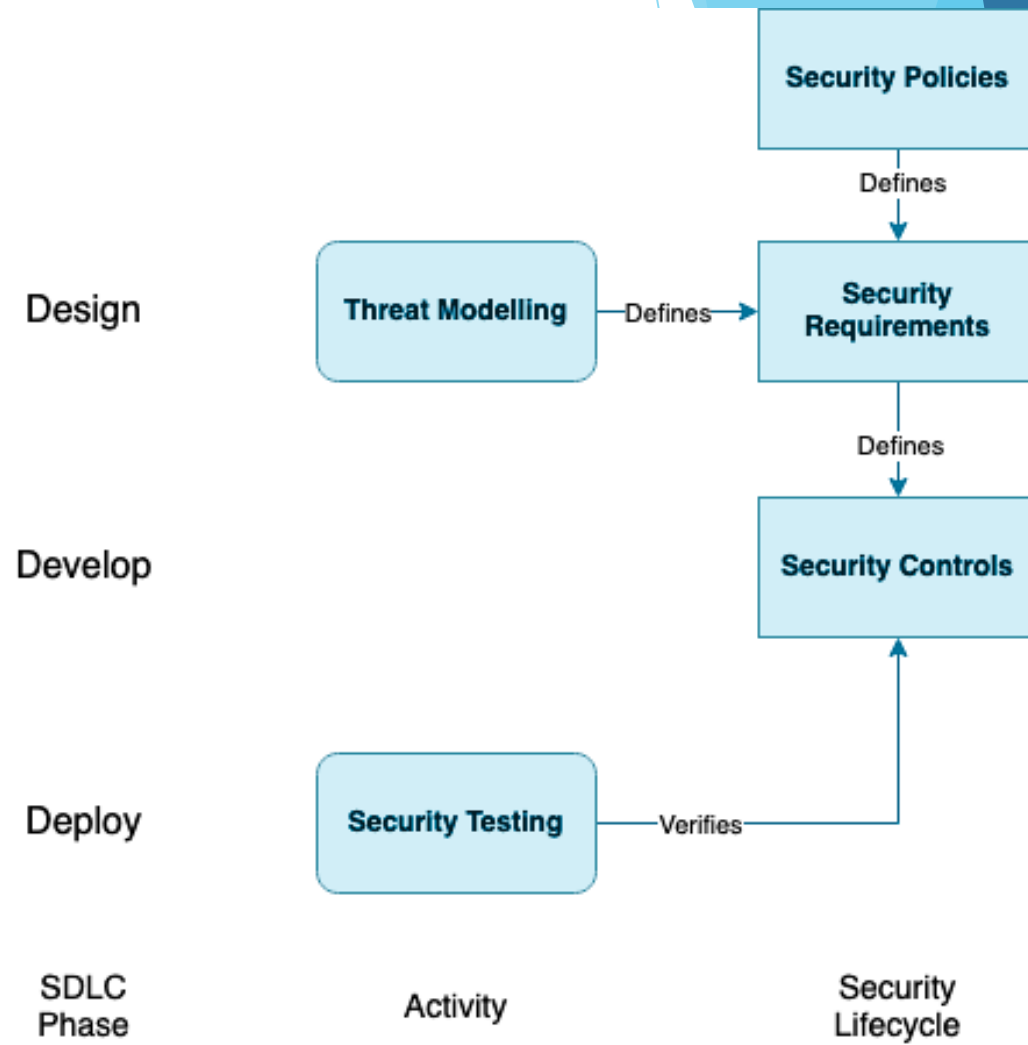
Corrispondenza tra le pratiche di
«difesa in profondità» MDCG 2019-16
e i processi di IEC 81001-5-1

MDCG 2019-16	IEC 81001-5-1
1. Security Management	4.1 Quality Management 5.1 Software Development Planning
2. Specification of security requirements	5.2 Health Software Requirement Analysis
3. Secure by design	5.3 Software Architectural Design 5.4 Software Design
4. Secure implementation	5.1 Software Development Planning 5.5 Software Unit Implementation and Verification
5. Security verification and validation testing	5.5 Software Unit Implementation and Verification 5.6 Software Integration Testing 5.7 Software System Testing 5.8 Software Release
6. Management of security-related issues	4.1 Quality Management 5.1 Software Development Planning 6 Software Maintenance Process 7 Security Risk Management Process 8 Software Configuration Management Process 9 Software Problem Resolution Process
7. Security update management	6.1 Establish Software Maintenance Plan 6.2 Problem and modification analysis 6.3 Modification implementation
8. Security guidelines	4.1.9 Accompanying documentation review 5.8.2 Release documentation 5.8.7 Secure decommissioning guidelines for Health Software 6.3.1 Supported Software Security update documentation

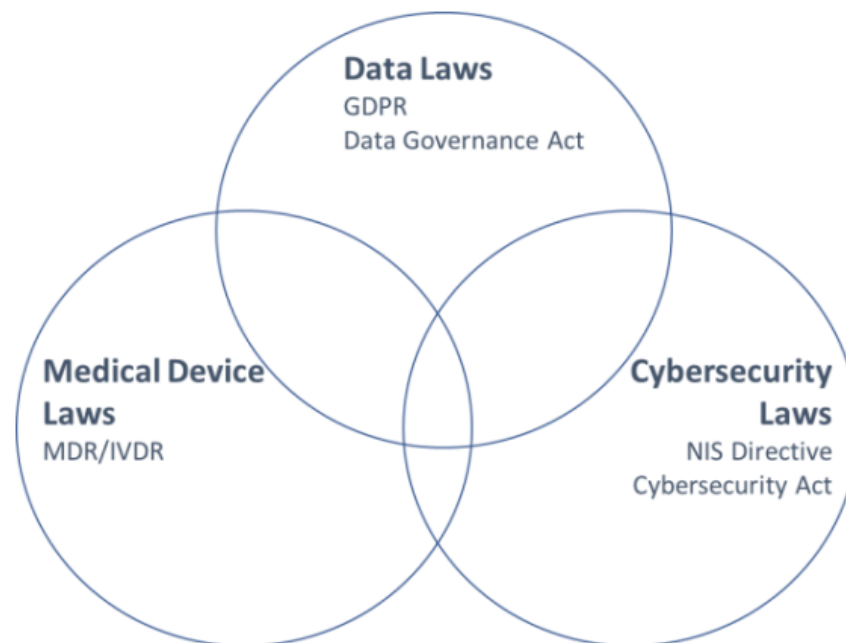
Progettazione sicura e modellazione della minacce

La progettazione sicura passa per la **modellazione delle minacce** che è un processo **strutturato e ripetibile** utilizzato per ottenere informazioni utili sulle caratteristiche di sicurezza di un particolare sistema.

- ▶ Modellazione di un sistema
- ▶ Identificazione delle minacce (es. STRIDE)
- ▶ Determinazione delle contromisure



Cybersecurity: altri requisiti





MODULO 7: VALUTAZIONE DEI RISCHI E GESTIONE DELLA VULNERABILITA'



Dr.ssa Silvia Tamarri
Complife

Security del prodotto

Il fabbricante di un dispositivo medico deve operare secondo le disposizioni nazionali e/o europee e deve fornire un prodotto cyber-resiliente



Minimizzazione dei rischi di security

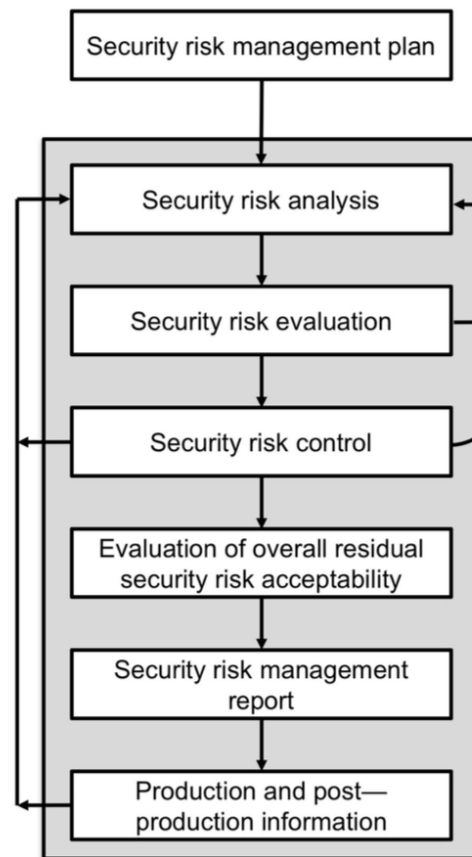
*SECURITY - A state where information and systems are protected from unauthorized activities, such as access, use, disclosure, disruption, modification, or destruction to a degree that the related risks to **confidentiality, integrity, and availability** are maintained at an acceptable level throughout the life cycle (ISO 81001-1).*

Valutazione dei rischi e gestione della vulnerabilità

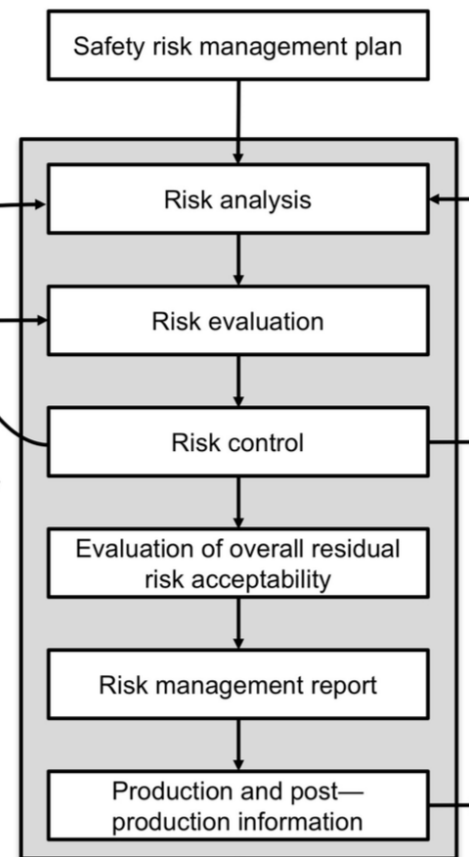
Cybersecurity: gestione del rischio



Security Risk Management Process



Safety Risk Management Process



----- Complaint/vigilance data for security expertise assessment -----

MDCG 2019-16

ALLEGATO II - Esempi di incidenti di cybersecurity

Serious incident (Yes/No)	Risk relationship	Device	Security Harm	Safety Harm
			Security Control	Safety Control
Yes	Security risk with a safety impact.	Anaesthesia device	An unauthorized user with physical access to the device guesses the weak password for the service account and manipulates the configuration settings.	The anaesthesia device supplies a wrong anesthetic concentration.
			Access control without password complexity enforcement.	Not Applicable.

MDCG 2019-16

ALLEGATO II - Esempi di incidenti di cybersecurity

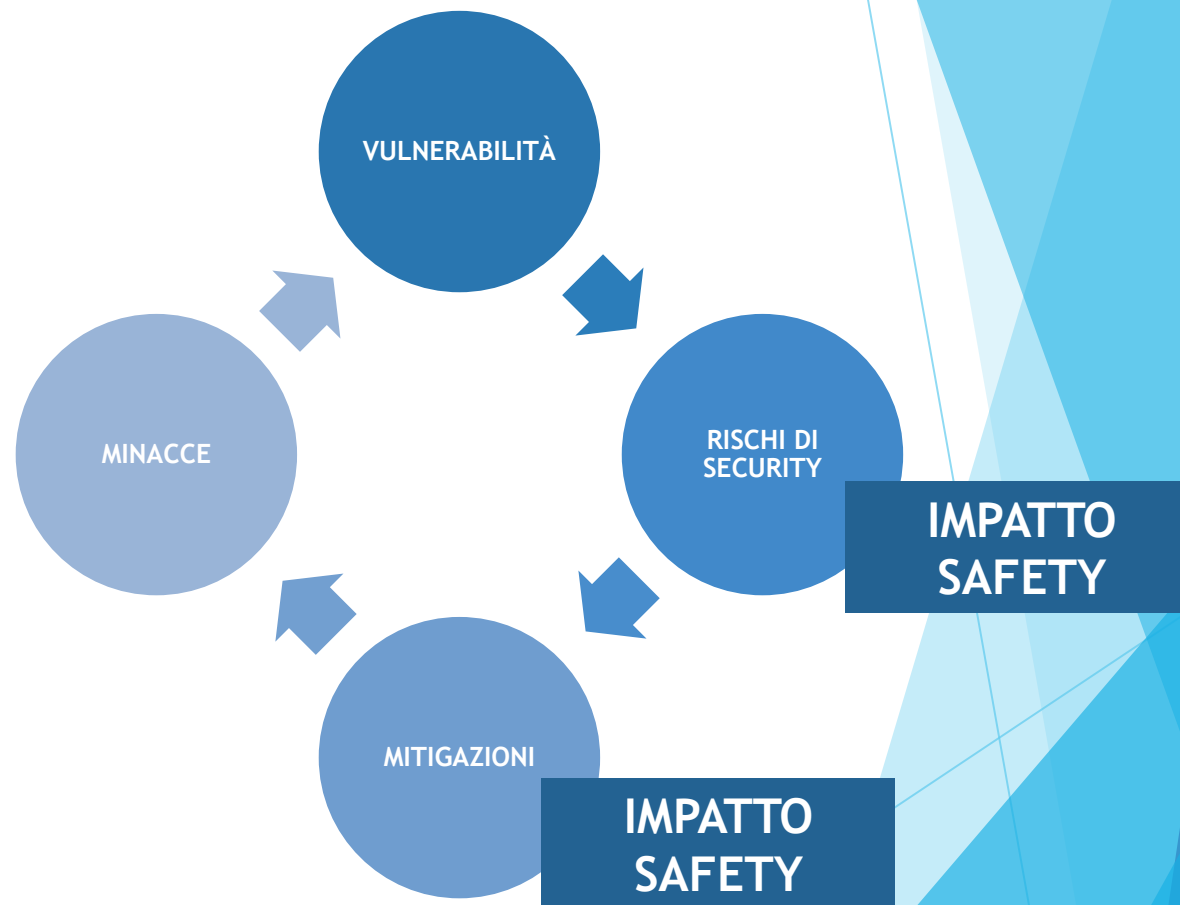
Serious incident (Yes/No)	Risk relationship	Device	Security Harm	Safety Harm
			Security Control	Safety Control
No	Security risk only.	Warming therapy device for premature babies	An unauthorized user with physical access to the device guesses the weak password for the service account and exports therapy and patient data via the USB interface.	None.
			Access control without password complexity enforcement.	Not Applicable.

Security Risk Assessment

La modellazione delle minacce aiuta a identificare le vulnerabilità nel dispositivo medico e nei suoi componenti

Ciò permette di valutare i rischi di security e determinare l'impatto delle vulnerabilità note o dei potenziali rischi di sicurezza informatica sulla sicurezza del paziente

È un processo iterativo e ripetibile fin al raggiungimento di un livello accettabile di rischio



Modellazione delle minacce

È fondamentale identificare le potenziali minacce che possono compromettere la sicurezza del dispositivo medico. Esistono diverse metodologie per valutare i rischi.

Tra queste, STRIDE è una delle più utilizzate per un'analisi rapida dei rischi di cybersicurezza. Questo approccio sistematico aiuta i team di sviluppo a pensare come un potenziale aggressore, consentendo di proteggere i sistemi in modo proattivo prima che si verifichino violazioni.

- ▶ Spoofing: impersonare un'altra persona o processo
- ▶ Tampering: effettuare modifiche non autorizzate
- ▶ Repudiation: negare azioni fatte
- ▶ Information Disclosure: esporre dati in modo non autorizzato
- ▶ Denial of Service: rendere indisponibile un processo/servizio
- ▶ Elevation of privileges: incrementare il livello di accesso non autorizzato

Risk Management process

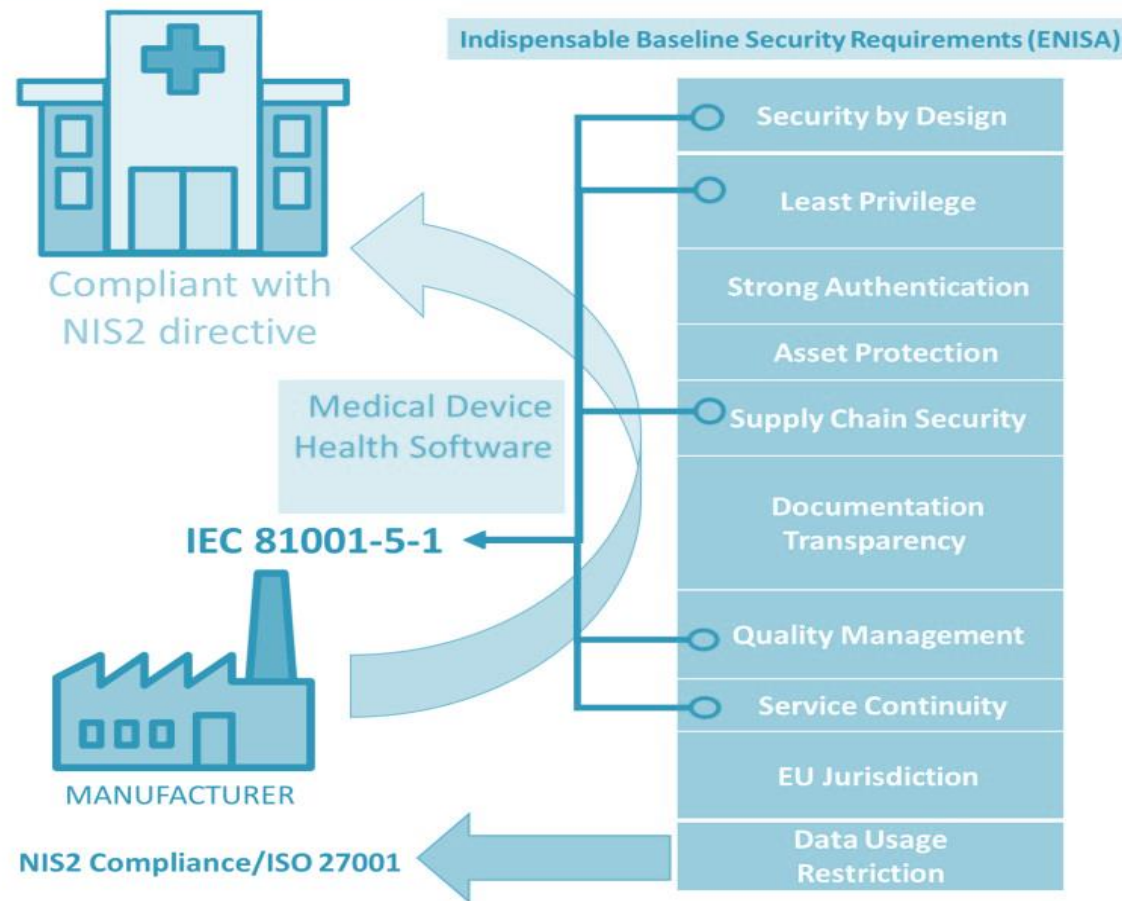
RISK Management process: Parallelismo tra safety e security	
Safety risk management	Security risk management / threat management
Risk identification process to identify safety risks	Threat Modeling to identify software vulnerabilities
Risk Severity assignation	Vulnerability scoring Ex: Common Vulnerability Scoring System (CVSS)
Risk mitigation Ex: Risk control measures	Threat mitigation Ex: Defense in depth
Evaluation of safety risk mitigation effectiveness Ex: Safety testing (IEC 60601-1)	Evaluation of security risk mitigation effectiveness Ex: Penetration testing

MODULO 8: L'INTERAZIONE TRA NIS 2 E REGOLAMENTO MDR'



Dr.ssa Silvia Tamarri
Complife

NIS2 vs Medical device



MDR vs NIS2 - Sovrapposizioni

MDR

- Design sicuro
- Gestione del rischio
- Stabilire misure di controllo del rischio
- Verifica e validazione
- Documentazione tecnica
- Valutazione della conformità
- Attività di PMS
- Valutazione clinica

NIS2

- Gestione del rischio
- Stabilire misure di controllo del rischio
- Segnalazione

Considerando 10 NIS2: Criterio di specialità

‘Qualora le disposizioni di atti giuridici settoriali dell’Unione impongano ai soggetti critici di adottare misure per rafforzare la propria resilienza o di notificare gli incidenti, e qualora tali requisiti siano riconosciuti dagli Stati membri come almeno equivalenti ai corrispondenti obblighi stabiliti dalla presente direttiva, le pertinenti disposizioni della presente direttiva non dovrebbero applicarsi, in modo da evitare duplicazioni e oneri non necessari. In tal caso dovrebbero applicarsi le pertinenti disposizioni di tali atti giuridici dell’Unione. Qualora non si applichino le pertinenti disposizioni della presente direttiva, non dovrebbero applicarsi nemmeno le disposizioni di cui alla presente direttiva in materia di vigilanza ed esecuzione’

L'interazione tra MDR e NIS2

- ▶ Il considerando 12 della direttiva >>dovrebbero applicarsi tali **disposizioni settoriali**".
- ▶ **MDR come lex specialis**
- ▶ **alcuni Stati considereranno l'MDR come lex specialis:** alcuni richiederanno la notifica di entrambi gli incidenti, mentre altri no.
- ▶ disposizioni in materia di notifica di incidenti potranno subire dei cambiamenti
- ▶ **IEC/TR 60601-4-5** Medical Electrical Equipment - Part 4-5: Safety related technical security specifications for medical devices
- ▶ **MDCG 2019-16** Guidance on Cybersecurity for medical devices

Q&A



Grazie per l'attenzione