AISIS ASSOCIAZIONE ITALIANA | SISTEMI INFORMATIVI IN SANITÀ

CHIME INTERNATIONAL ITALY CHAPTER

AIIC associazione italiana ingegneri clinici

Un primo approccio all'applicazione della Direttiva NIS2 in Sanità

In collaborazione con:

TIG THE INNOVATION GROUP

Hanno partecipato al progetto:

A-thon

Cyber Guru

Dedalus

FONDAZIONE
POLICLINICO UNIVERSITARIO
CAMPUS BIO-MEDICO

Gas.Net Group

SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Istituto Romagnolo per lo Studio dei Tumori "Dino Amadori"
Istituto di Ricovero e Cura a Carattere Scientifico

ISTITUTO ROMAGNOLO PER LO STUDIO DEI TUMORI DINO AMADORI

PIERPAOLO MAIO
AVVOCATO

REXILIENCE
#BEYOND_CYBERSECURITY

Roche

sim
società italiana di leadership e management in medicina

STEFANELLI & STEFANELLI
STUDIO LEGALE

Partecipanti al Gruppo di Lavoro

Cognome	Nome	Azienda
Amodio	Vincenzo	*AOU BO*
Assandri	Tommaso	*ASST Pavia*
Balsamo	Francesco	*Ulss6 Euganea*
Bellotti	Nicola	*Namirial*
Bitteleri	Vittorio	*Cyberguru*
Boccafogli	Luca	*AUSL Ferrara*
Brambilla	Marco	*AOU Parma - AUSL Parma*
Carbone	Gabriele	*Dedalus*
Collura	Fabio	*ISMETT*
Costi	Cesare	*AOU Parma*
D'Argenio	Marzia	*IBM*
Di Guardo	Marianna	*Hospital Consulting*
Draghetti	Michele	*AOU Bologna*
Folino	Matteo	*EY*
Gallarati	Elisa	*ASST Pavia*
Gentili	Nicola	*IRST Meldola*
Giomo	Giuseppe	*Gasnet*
Gobbo	Beatrice	*Azienda sanitaria Friuli Occidentale*
Goldoni	Roberto	*AOU Parma*
Grigioni	Mauro	*ASSD*
Guarenghi	Daniela	*AOU Parma*
Guerriero	Cinzia	*AS Universitaria Giuliano Isontina*
Latini	Maurizio	*FTMG*
Lugli	Mario	*AOU Modena*
Maio	Pierpaolo	
Mangione	Maurizio	*FTMG*
Nasi	Greta	*SDA Bocconi*
Nilo Mazza	Domenico	*IZSLER*
Pepe	Massimiliano	*Medtronic Italia*
Perrone	Massimiliano	*Rexilience*
Perselli	Greta	*FTMG*
Piaser	Paolo	*Azienda sanitaria Friuli Occidentale*
Rizzetto	Maurizio	*Azienda sanitaria Friuli Occidentale*
Romagnoli	Mattia	*ONIT*
Ronchi	Alberto	*Istituto Auxologico Italiano*
Rossetti	Jonathan	*Roche*
Solfa	Marco	*Athon*
Spagno	Cinzia	*AS Universitaria Giuliano Isontina*
Stefanelli	Silvia	*Studio Stefanelli e Stefanelli*
Vaciago	Elena	*TIG*
Vallega	Alessandro	*Rexilience*
Venditti	Marco	*Campus Biomedico*
Visentin	Fabio	*TIM*
Zaccheroni	Andrea	*IRST Meldola*

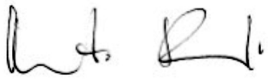
Indice

Introduzione

Ogni anno per diversi anni AISIS ha preparato un lavoro su temi rilevanti per tutta la comunità ICT della Sanità e, in particolare per i suoi associati, presentandolo poi al congresso annuale.
Il risultato era un volume frutto di uno sforzo collettivo di associati, simpatizzanti e aziende dell'offerta che portavano i loro contributi unici per creare un testo che avesse un valore pratico per la comunità delle tecnologie informatiche in sanità.
Purtroppo questa tradizione, per vari motivi, si è interrotta qualche anno fa lasciando un certo disappunto in molti nostri associati e simpatizzanti.
L'arrivo della Direttiva NIS2, delle conseguenti determine di ACN e della sempre crescente importanza della cybersicurezza, uniti alla volontà di ripartire con la tradizione di questi gruppi di lavoro, hanno fornito lo spunto necessario per la creazione del testo che vi presentiamo.
Nel primo capitolo il documento presenta l'importante apparato legislativo che ha il compito di disciplinare i temi della sicurezza e, in diversa misura, della privacy, con un bellissimo confronto tra le varie leggi e i vari decreti per capire come orientarsi in quella che si può definire una vera giungla legislativa. Nel secondo capitolo vengono affrontati i temi documentali e procedurali che hanno un'importanza fondamentale per la Direttiva NIS2 e per la determina ACN che la regolamenta. Ovviamente non possono mancare alcuni aspetti tecnici, che sono contenuti negli altri due capitoli, aspetti alcuni di natura generale altri soprattutto legati al mondo degli apparati elettromedicali e dell'ingegneria clinica.
Ringrazio AIIC per aver voluto collaborare alla stesura del testo, tutto il gruppo di lavoro per il grande contributo e per la qualità degli interventi, e in modo particolare gli ingegneri clinici, sia affiliati ad AISIS sia ad AIIC, che hanno giocato un ruolo chiave nella stesura della parte più propriamente legata alla sanità.

Come sempre auguro a tutti una buona e proficua lettura.

Il Presidente AISIS
Alberto Ronchi



Glossario

AAA	Autenticazione, Autorizzazione e Accounting
ACL	Access Control List
ACM	Alert Communication Management
ACN	Agenzia per la Cybersicurezza Nazionale
AgID	Agenzia per l'Italia Digitale
AI	Artificial Intelligence
ANAC	Autorità Nazionale Anti Corruzione
ATS	Automatic Transfer Switch
BC	Business Continuity
BCP	Business Continuity Plan
CAD	Codice per l'Amministrazione Digitale
CDA2	Clinical Document Architecture Rel 2
CERT	Computer Emergency Response Team
CIE	Carta d'Identità Elettronica
CNS	Carta Nazionale dei Servizi
CSIRT	Computer Security Incident Response Team
CVD	Coordinated Vulnerability Disclosure
CVSS	Common Vulnerability Scoring System
DEC	Device Enterprise Communication
DHCP	Dynamic Host Configuration Protocol
DPIA	Digital Pathology workflow Image Acquisition
DR	Disaster Recovery
DRP	Disaster Recovery Plan
DSE	Dossier Sanitario Elettronico
EDR	Endpoint Detection and Response
ENISA	European Network and Information Security Agency
EPSS	Exploit Prediction Scoring System
FNCDP	Framework Nazionale per la Cybersicurezza e la Data Protection

FSE	Fascicolo Sanitario Elettronico
GDPR	General Data Privacy Regulation
HA	High Availability
HL7	Health Level 7
HTTP	Hypertext Transfer Protocol Secure
IA	Intelligenza Artificiale
IAAS	Infrastructure As A Service
ICT	Information and Communication Technology
IDP	Identity Provider
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IHE	Integrating the Healthcare Enterprise
IP	Internet Protocol
IPS	Intrusion Prevention System
ISFW	Internal Segmentation Firewall
ISO	International Organization for Standardization
IT	Information Technology
IVDR	In Vitro Diagnostic medical device Regulation
LAN	Local Area Network
MAC	Media Access Control
MDR	Medical Device Regulation
MDR	Managed Detection and Response
MDS2	Manufacturer Disclosure Statement for medical device security
MFA	Multi Factor Authentication
NAC	Network Access Control
NEMA	National Electrical Manufactures Association
NIS	Network and Information Security
PA	Pubblica Amministrazione

PACS	Picture Archiving and Communication System
PDC	Patient Care Device
PDL	Postazione Di Lavoro
PHI	Personal Health Information
PT	Penetration Testing
RGPD	Regolamento Generale Protezione dei Dati
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SAAS	Software As A Service
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SPID	Sistema Pubblico di Identità Digitale
SSL	Secure Socket Layer
SSO	Single Sign On
TR	Technical Report
VA	Vulnerability Assessment
VLAN	Virtual LAN
VNA	Vendor Neutral Archive
VPC	Virtual Private Cloud
VPN	Virtual Private Network
WADO	Web Access to DICOM Objects
WLAN	Wireless LAN
XDR	eXtended Detection and Response
XDS	Cross Document Sharing
ZFP	Zero FootPrint

Analisi del contesto normativo

Prefazione

Chiunque intenda approcciarsi alla recente normativa comunitaria in materia di sicurezza informatica è destinato anche ad un primo, non facile, impatto con le molteplici intersezioni che caratterizzano la strategia digitale dell'Unione.
La NIS2, il GDPR, l'AI Act e le fonti nazionali (in particolare il CAD) sono solo alcune delle fonti di un vero e proprio ecosistema di disposizioni, non sempre omogenee, finalizzate a plasmare le caratteristiche di un ambiente digitale europeo dinamico ma sicuro, equo e sostenibile per tutti i cittadini e le imprese.
Non stupisce, quindi, la percezione degli operatori di trovarsi in un sistema "a segnali di stop" nel quale, per difficoltà interpretative o per il timore di sbagliare e di incorrere in sanzioni, la tentazione sia quella di "non fare": unica vera scelta certamente sbagliata!
Lo spirito che ha guidato la scrittura di questo capitolo è di duplice natura: la ricerca di un metodo per dare ordine al complesso di fonti di questo ecosistema e la ricerca di un linguaggio che possa risultare comprensibile a tutti gli attori: tecnico, giurista, operatore del settore pubblico o privato.
Il presente capitolo, oltre a voler fornire un supporto per orientarsi tra le diverse normative, tenta di individuare punti di contatto, adempimenti uniformi e anche disposizioni in conflitto, per progredire negli sforzi comuni verso una compliance effettiva che porti ad affrontare consapevolmente le prossime sfide che caratterizzano un mondo in continuo cambiamento.

Il confronto con il Regolamento 2016/679 (GDPR)

Il Decreto Legislativo 4 settembre 2024, n. 138, rappresenta l'attuazione italiana della Direttiva (UE) 2022/2555, meglio conosciuta come Direttiva NIS2 (Network and Information Security). Questa direttiva mira a rafforzare il livello di sicurezza cibernetica in tutta l'Unione Europea, prevedendo obblighi di protezione per una vasta gamma di settori, tra cui sanità, energia, trasporti e servizi digitali, ed estendendo, rispetto alla precedente Direttiva, la platea dei destinatari.
Sebbene il Decreto si concentri principalmente sulla sicurezza delle reti e dei sistemi informativi, esso interagisce strettamente con il Regolamento Generale sulla Protezione dei Dati (di seguito RGPD e noto anche come GDPR), che disciplina la protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.
Entrambe le normative condividono l'obiettivo di proteggere interessi fondamentali dell'individuo e della collettività nel contesto digitale, garantendo un elevato livello di sicurezza e protezione, ma si focalizzano su aspetti differenti: il RGPD garantisce il rispetto dei diritti fondamentali delle persone

fisiche attraverso la protezione dei loro dati personali mentre il D.Lgs. 138/2024 si focalizza sul rafforzamento della resilienza delle infrastrutture digitali e dei servizi essenziali mediante una maggiore sicurezza proprio delle reti e dei sistemi informativi delle organizzazioni considerate critiche, a salvaguardia dell'integrità, della disponibilità e della continuità degli stessi.
Queste discipline, sebbene abbiano differenti ratio e oggetto (RGPD si applica solo quando vi siano trattamenti di dati personali mentre il D.lgs. 138/24 prescinde da tale qualificazione), presentano significativi punti di contatto, a dimostrazione del fatto che il legislatore comunitario abbia inteso predisporre un impianto composito e integrato mediante la creazione di un sistema digitale che prende in considerazione molteplici ambiti di applicabilità che rappresentano elementi di una strategia unitaria a livello comunitario e nazionale.
Al RGPD, che ha avuto piena efficacia il 28 maggio 2018 e che contiene in sé tutti i principi cardine per la sicurezza del trattamento dei dati personali e per la loro protezione, è senza dubbio attribuibile il merito di aver introdotto novità nella protezione dei dati personali: il concetto di privacy by design e by default (anche e soprattutto per i sistemi informatici), di accountability, la necessità di individuare e mettere in atto misure di sicurezza adeguate a fronte di una valutazione preliminare dei rischi, un sistema di segnalazione delle violazioni di sicurezza e di sanzioni strutturato e diversificato a seconda della gravità della violazione.[1] Fino ad allora, la normativa non si basava sulla "responsabilizzazione" del titolare ma si prefiggeva il rispetto di prescrizioni (si veda l'abrogato allegato B del D.lgs. 196/2003 in tema di misure di sicurezza). Il titolare si limitava a soddisfare le previsioni normative e a mettere in atto le misure "sufficienti" senza essere chiamato a effettuare valutazioni critiche della propria attività di trattamento per individuare misure "adeguate".
Il cambio di paradigma è dunque tracciato: l'approccio proattivo della gestione del rischio mira, dopo l'analisi del contesto e delle finalità del trattamento nonché della probabilità e gravità dei rischi in cui l'organizzazione può incorrere, ad individuare misure di sicurezza effettivamente adeguate.
Emerge chiaramente in diversi ambiti, seppure le finalità proprie delle due normative siano quindi sostanzialmente differenti, la connessione tra loro e questo rappresenta un passaggio verso un approccio più integrato alla gestione della sicurezza informatica e alla protezione dei dati personali (senza comunque dimenticare altre normative quali ad es. AI ACT...).
Le organizzazioni soggette sia al RGPD sia al D.Lgs. 138/2024 saranno pertanto chiamate, nell'ormai breve termine di piena concretizzazione, a adottare modalità attuative che consentano la gestione della sicurezza nel suo più ampio significato. Ciò implica l'implementazione di politiche e procedure che soddisfino i requisiti di entrambe (e non solo) le normative, garantendo una protezione efficace dei dati personali nonché la sicurezza delle infrastrutture informatiche, e che prevedano una collaborazione all'interno dell'azienda di varie professionalità e competenze.
La visione unitaria del sistema di sicurezza consentirà altresì la creazione di processi integrati, anche mediante team multidisciplinari, tali da permettere, oltre il soddisfacimento dell'esigenza prioritaria di sicurezza delle infrastrutture informative e degli asset correlati, anche una miglior gestione e impiego delle risorse umane e finanziarie dell'organizzazione.

[1] Si veda anche la pubblicazione di AISIS sul GDPR [1]

COMPLEMENTARIETÀ TRA LE DUE NORMATIVE

Gestione del rischio

L'impianto normativo del RGPD è basato sulla valutazione del rischio e sulla sua gestione in maniera dinamica finalizzata alla protezione dei dati personali, laddove la NIS2 pone la sua attenzione alla continuità dei servizi essenziali in settori critici per garantire la salvaguardia delle reti e dei sistemi informativi, ma sempre in un'ottica dinamica che non sia circoscritta alla reazione a eventi bensì alla creazione di una struttura sistemica con valutazioni sistematiche e periodiche. La visione è dunque quella di manutenere il sistema in modo da assicurare la permanente valutazione dei rischi.

Misure di sicurezza

L'art. 32 del RGPD impone al titolare del trattamento l'obbligo di adottare misure tecniche e organizzative adeguate al rischio. Il D.Lgs. 138/2024, in modo analogo, richiede ai soggetti "essenziali" e "importanti" di implementare misure di gestione dei rischi relativi alla sicurezza delle reti e dei sistemi informativi che presentino i requisiti di adeguatezza e proporzionalità rispetto ai rischi. L'approccio seguito in entrambe le discipline è dunque orientato al dinamismo delle misure di sicurezza e alla loro aderenza al concreto trattamento. Conseguentemente non sono indicate misure specifiche ma, al più, macro adempimenti molti dei quali – come la cifratura, la gestione degli accessi, il controllo della supply chain – hanno riflessi diretti sia nell'ambito della sicurezza informatica sia sulla protezione dei dati personali.

Gestione della catena dei fornitori

La gestione della catena dei fornitori è un punto focale sia nel RGPD sia nella NIS2. La gestione della catena di approvvigionamento, ivi compresi gli aspetti relativi alla sicurezza riguardanti i rapporti tra ciascun soggetto e i suoi diretti fornitori o fornitori di servizi, poi, non è solo integrata nelle misure di sicurezza applicabili all'ambito ICT (art. 24, comma 2, lett. d) del D.Lgs. 138/2024) ma trova applicazione in molteplici disposizioni che hanno introdotto una serie di vincoli e requisiti. I fornitori, peraltro, che già nella disciplina del RGPD sono direttamente responsabilizzati ai fini del rispetto della normativa (cfr. su tutte le prescrizioni di cui all'art. 32, § 1 che impongono sia al Titolare sia al responsabile obblighi autonomi di attuare misure di sicurezza), diventano esplicitamente destinatari delle norme in materia di cybersicurezza (art. 3, comma 5 del Decreto) e dovranno integrare la cybersicurezza nelle proprie strategie aziendali assicurando la conformità alle normative.

Gestione attività transfrontaliere

Mentre il RGPD dedica un intero capo (capo V) alla tematica, la NIS 2 e il decreto di recepimento enfatizzano due aspetti principali: la gestione degli incidenti di sicurezza con potenziali impatti transfrontalieri (art. 23 NIS2) e la collaborazione tra Autorità nazionali e autorità pertinenti (art. 10, comma 2 del Decreto). Conformemente alla ratio del Regolamento europeo, che non impedisce la circolazione dei dati personali ma prevede che tale circolazione possa avvenire solo se in sicurezza, anche il trasferimento al di fuori dei confini dell'Unione non viene vietato ma subordinato a condizioni di

legittimazione (artt. 44 e ss. RGPD) quali la presenza di una decisione di adeguatezza da parte della commissione (art. 45 RGPD), la presenza di adeguate garanzie (art. 46 RGPD) oppure l'approvazione di norma vincolanti d'impresa (art. 47 RGPD).

Formazione e cultura della sicurezza: compliance trasversale

Entrambe le normative riconoscono un ruolo centrale alla formazione e alla consapevolezza del personale. Il RGPD lo codifica come principio cardine per ridurre il rischio di trattamenti illeciti (art. 32 par. 4 RGPD) prevedendo altresì che "il responsabile, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento" (art. 29 RGPD) e "il titolare e il responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro responsabilità".
Il D.Lgs. 138/2024 lo rende esplicito per i soggetti obbligati, richiedendo programmi strutturati di formazione continua in materia di cybersecurity sia per gli organi di amministrazione e direttivi sia per il dipendente. Inoltre, ai fini della NIS2, il personale deve presentare caratteristiche di affidabilità in termini di competenze.

Gestione degli incidenti

Una doppia soglia di segnalazione: il RGPD, all'art. 33, prescrive la notifica della violazione dei dati personali (data breach) all'autorità di controllo senza ingiustificato ritardo e comunque, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza. Qualora la notifica all'autorità non sia effettuata entro tale termine, deve essere corredata dei motivi del ritardo.
Il D.Lgs. 138/2024 prevede un ulteriore livello di segnalazione verso il CSIRT Italia per incidenti significativi che possano compromettere la fornitura dei servizi essenziali o importanti, con differenti tempistiche: una pre-notifica, senza ingiustificato ritardo, e comunque entro 24 ore, e una notifica dell'incidente, senza ingiustificato ritardo, e comunque entro 72 ore da quando sono venuti a conoscenza dell'incidente significativo. Le organizzazioni dovranno altresì redigere, una relazione intermedia, su richiesta del CSIRT Italia, sui pertinenti aggiornamenti della situazione e, da ultimo, una relazione finale entro un mese dalla trasmissione della notifica dell'incidente.
La necessità di valutare, in caso di incidente, l'attivazione di due distinti (ma spesso convergenti) canali di notifica, con tempistiche e contenuti parzialmente differenziati, deve indurre le organizzazioni a ripensare le proprie procedure al fine di agire, se l'incidente risulti significativo ai sensi della NIS2 e coinvolga dati personali ai sensi del RGPD, nelle strette tempistiche delle normative.

Gestione documentale

Sulle organizzazioni soggette alle normative RGPD e decreto NIS2 grava non solo l'obbligo di porre in essere tutti gli adempimenti necessari a garantire la conformità alla normativa ma anche di essere in grado di dimostrare tali adempimenti. Tale principio trova la sua consacrazione normativa nella cosiddetta accountability (o responsabilizzazione) di cui all'art. 24 RGPD e si ricava, deduttivamente,

dall'art. 32, comma 2, lett. g) della Direttiva, che prevede il potere, in capo alle autorità competenti, nell'esercizio dei rispettivi compiti di vigilanza nei confronti dei soggetti importanti, di sottoporre richieste di dati che dimostrino l'attuazione di politiche di cybersicurezza (quali i risultati di audit sulla sicurezza effettuati da un controllore qualificato e i relativi elementi di prova).
A tal fine le organizzazioni si dovranno dotare di procedure, percorsi multiprofessionali, istruzioni, piani, audit che dovranno trovare una corrispondente documentazione, alla quale sia possibile attribuire una data certa.

Rapporti tra ACN e Autorità Garante

L'art. 14 D.lgs. 138/2024 esplicita l'obbligo di assicurare la cooperazione e la collaborazione reciproca dell'Autorità nazionale competente NIS e del Punto di contatto unico NIS con l'Autorità Garante per la protezione dei dati personali. Tale collaborazione si esplica nell'ambito della gestione degli incidenti di sicurezza i cui profili siano rilevanti sia per la protezione dei dati personali sia per la cybersicurezza (art. 14, comma 2, lett. a), nell'ambito della notifica di violazioni di dati personali ravvisate da ACN adempiendo a compiti di vigilanza e esecutivi (comma 2, lett. b), nella fase di irrogazione di sanzioni, onde evitare che il medesimo fatto sia sanzionato da entrambe le Autorità (comma 2, lett. c).
Nell'allegato A abbiamo inserito la tabella di confronto tra i punti salienti delle due normative, divisa per articolo.

La NIS2 e la Legge 90/2024 sulla cybersicurezza a livello italiano

L'approccio giuridico europeo alla cybersecurity si caratterizza, nell'attuale momento storico, per una dimensione multilivello ovvero per la previsione di diverse forme di tutela delle medesime situazioni giuridiche nei diversi ordinamenti. La conseguenza immediata di questo approccio è il fiorire di diverse fonti normative sia comunitarie sia interne agli Stati membri, talvolta confliggenti, per disciplinare i medesimi ambiti.
Tra le fonti applicabili al contesto italiano si ricordano in particolare:

- Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativa a misure per un livello comune elevato di cybersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2).
- Decreto legislativo 4 settembre 2024, n. 138, pubblicato in Gazzetta Ufficiale del 1° ottobre e in vigore dal 16 ottobre che recepisce tale direttiva.
- Legge 28 giugno 2024, n. 90 Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici.

L'APPROCCIO ITALIANO: DALLA CYBERSECURITY

Ad una prima lettura la L. 90/2024 (fonte interna cronologicamente antecedente al decreto di recepimento 138/2024) sembra prevedere un approccio speculare a quello della NIS2 (fonte comunitaria),

al fine di precisare e contestualizzare talune delle sue disposizioni prima ancora di un pieno recepimento.
Tuttavia, ad una lettura più attenta, si potrà notare come l'oggetto di tutela sia sostanzialmente diverso nelle due fonti: la disciplina comunitaria risulta volta alla tutela del mercato interno dell'Unione, mentre la L. 90/2024 alla tutela della sicurezza nazionale. La riconduzione della materia all'ambito della sicurezza nazionale, di per sé riservato alla competenza legislativa dei singoli stati in forza dei limiti stabiliti dall'art. 4, par. 2, Trattato sull'Unione Europea (TUE), consente e consentirà al Legislatore italiano di adottare atti di portata maggiore di (o diversa da) quanto prevede la Direttiva.
Tali scelte normative, a prescindere dalla loro condivisibilità, possono comunque rischiare di vanificare l'approccio europeo, sia per la previsione di nuovi e più rigidi adempimenti in capo ai soggetti interessati, sia perché il mercato unico beneficia, come noto e come vedremo nella parte relativa al codice degli appalti, di quadri normativi uniformi e stabili tra i singoli Stati mentre rischia di essere pregiudicato da approcci e visioni autonome.
La disciplina offerta dalla L. 90/2024 prevede due distinte aree di intervento: la prima insiste specialmente sulla cybersicurezza delle amministrazioni pubbliche e sulla governance di settore (capo I); la seconda contiene misure di carattere penale (capo II) che si traducono nella previsione di nuove fattispecie di reato (in particolare l'estorsione informatica di cui all'art. 629, comma 3 c.p. sanzionata più aspramente dell'estorsione semplice) e alla ridefinizione delle cornici edittali e/o delle aggravanti di fattispecie esistenti, in termini di sostanziale ampliamento delle pene previste.
Più nel dettaglio, il Capo I, nel configurare una serie di obblighi di notifica di incidenti informatici nei dati e nei sistemi di competenza (come già inquadrati dalla NIS2) e di risoluzione delle vulnerabilità, dà immediatamente conto del carattere fortemente prescrittivo della disciplina che emerge dalla tecnica normativa utilizzata.
Gli obblighi, peraltro, si estendono ben al di là delle sole Amministrazioni centrali destinatarie delle disposizioni della NIS2, per precisa scelta del Legislatore nazionale e a fronte della possibilità concessa dall'art. 2, par. 5 della Direttiva stessa.
A parere di molti, tale estensione sarebbe dovuta andare di pari passo con un più forte e sostanziale intervento statale, diretto tanto a colmare le lacune tra le diverse pubbliche amministrazioni quanto a fornire alle stesse strumenti e risorse adeguate per far fronte agli obblighi di nuova introduzione.
Sono infatti ravvisabili e generalizzate sia carenze nelle risorse richieste sia difficoltà di applicazione in contesto organizzativi nei quali, per dimensioni e mission istituzionale, non sono disponibili competenze interne adeguate alla complessità della materia.
Il Capo II, invece, prevedendo un aumento e inasprimento delle sanzioni penali, riflette pienamente la finalità di tutela della sicurezza nazionale che non appartiene al Legislatore comunitario.
Se infatti la tutela del mercato europeo attraverso la sicurezza informatica è pienamente compatibile con una risposta più marcatamente privatistica come quella prevista dalla NIS2 (cfr. artt. 34-36 della Direttiva) e ripresa dal relativo decreto di attuazione, la finalità di garantire la sicurezza nazionale vede la sua naturale realizzazione attraverso la previsione di nuove fattispecie di reato e la riconduzione di esse a beni giuridici diversi da quelli tradizionalmente destinatari di tutela.
Si deve anche aggiungere che, per effetto della Legge 90/2024, la riconduzione dei reati informatici

alla finalità di tutela della sicurezza nazionale coincide con l'affermazione di una loro qualificazione in termini di particolare offensività: da qui le modifiche al codice di procedura penale relative, ad esempio, alla disciplina delle intercettazioni nei casi di criminalità informatica. In tali casi, l'autorizzazione all'intercettazione potrà essere concessa in presenza delle stesse condizioni che il decreto-legge 13 maggio 1991, n. 152, convertito, con modificazioni, dalla legge 12 luglio 1991, n. 203, individua nei casi di criminalità organizzata.
In ultimo si osserva che la L. 90/2024 dedica una disposizione specifica alla responsabilità amministrativa degli enti collettivi, contenuta nel decreto legislativo 8 giugno 2001, n. 231 e ss.mm.ii.
Tale disposizione (art. 20) determina l'innalzamento delle sanzioni pecuniarie applicabili all'ente in caso di accertamento della propria responsabilità nella commissione di delitti informatici e trattamento illecito di dati (art. 24-bis, D.lgs. 231/01).

... ALLA CIBERSECURITY

Il Decreto recante "Recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione...", riflette, anche nella curiosa titolazione, il duplice sforzo del Legislatore nazionale: adempiere all'obbligo di recepimento della Direttiva NIS2 ma allo stesso tempo aprire la strada a un approccio nazionale, che si riflette anche nella scelta di abbandonare il forestierismo della forma inglese cyber- sostituendola con la forma tradizionale italiana ciber.
In quest'ottica, rammentate le finalità perseguite dal Legislatore della L. 90/2024, si può avere una chiave di lettura anche di quanto previsto all'articolo 4 del Decreto Legislativo n. 138 del 2024 di recepimento della NIS2.
Con tale articolo il Legislatore nazionale coglie l'opportunità offerta dall'art. 2, par. 4 della norma comunitaria e afferma la propria visione spiccatamente orientata alla sicurezza nazionale stabilendo che il decreto stesso non intacchi la responsabilità dello Stato italiano nella tutela della sicurezza nazionale, il cui potere resta invariato nel proteggere l'integrità territoriale, l'ordine pubblico e altre funzioni essenziali.
A ben vedere, dunque, pur senza modificare sostanzialmente gli adempimenti previsti nella Direttiva, nel momento in cui il Legislatore afferma la propria prospettiva fa comunque salvi i principi disciplinati dalla L. 90/2024 e fa convivere nel medesimo atto le due anime della cybersicurezza: quella protezionistica e quella comunitaria.
Gran parte della dottrina aveva ritenuto auspicabile una armonizzazione degli obblighi e delle misure previste nella L. 90/2024 cogliendo l'occasione dell'emanazione del Decreto legislativo di recepimento della Direttiva NIS2, anche per evitare una duplicazione/sovrapposizione degli adempimenti in capo ai soggetti vigilati e favorire una interlocuzione univoca con l'Agenzia per la più efficace implementazione delle nuove norme e l'effettivo raggiungimento di un più elevato livello di cybersicurezza.
Tale armonizzazione, non essendo stata realizzata, implica necessariamente diversi approcci al medesimo adempimento. È pienamente auspicabile dunque il ruolo della Agenzia per la Cybersicurezza Nazionale che, attraverso i propri atti, si troverà a svolgere una funzione realmente "nomofilattica" a beneficio degli interpreti e dei soggetti attuatori.

Una sintesi di tre norme

A prescindere dalla ratio ispiratrice degli interventi normativi e il quadro sanzionatorio, l'interprete non può che notare una sostanziale sovrapposizione degli adempimenti previsti dalla Direttiva NIS2 e dalla L. 90/2024.
Per meglio comprendere tali punti di contatto nell'allegato B abbiamo riassunto i principali profili delle tre discipline e, in particolare, i principali adempimenti, schematizzati adottando il punto di vista dei soggetti obbligati, con contestuale confronto tra la L. 90/2024, la Direttiva e il Decreto di recepimento, suddivisi per le varie tematiche.

Il Regolamento UE n. 2017/745 (MDR) e 2017/746 (IVDR) ovvero i dispositivi medici e IVD e la NIS2

DISPOSITIVI MEDICI (E IVD) COME SISTEMI INFORMATICI

I dispositivi medici (o IVD) che si interfacciano nelle reti informatiche delle aziende sanitarie (siano essi attrezzature sanitarie completamente hardware o sistemi esclusivamente software quali i SAMD) rientrano a pieno titolo nelle competenze e tutele della NIS2.
Il D.Lgs 138/2024 governa e regola i sistemi informativi e di rete che vengono così definiti:

1) una rete di comunicazione elettronica ai sensi dell'articolo 2, comma 1, lettera vv), del decreto legislativo 1° agosto 2003, n. 259;
2) qualsiasi dispositivo o gruppo di dispositivi interconnessi o collegati, uno o più dei quali eseguono, in base ad un programma, un trattamento automatico di dati digitali;
3) i dati digitali conservati, elaborati, estratti o trasmessi per mezzo di reti o dispositivi di cui ai numeri 1) e 2), per il loro funzionamento, uso, protezione e manutenzione.

Diventa pertanto importante per una azienda sanitaria ricordare che le funzioni e le procedure di gestione dei dispositivi medici debbono essere aggiornate e riviste anche per rispettare la NIS2 e parimenti, la gestione della sicurezza informatica, dove i dispositivi medici rappresentano una percentuale molto significativa dei sistemi informativi e di rete non può prescindere dal considerare le peculiarità, anche sotto il profilo regolatorio, dei dispositivi medici e degli IVD.
Partendo dalle responsabilità già in essere per MDR e IVDR vediamo i principali ambito di approfondimento che le aziende sanitarie dovranno intraprendere.

RESPONSABILITÀ E OBBLIGHI

In riferimento agli articoli 23 e 24 D.Lgs. 138/2024 si ricordano:

- Gli organi di amministrazione e direttivi promuovono l'integrazione della governance: è importante stabilire una collaborazione formale e strutturata tra IT, Ingegneria Clinica, Ufficio Acquisti e Direzione Sanitaria per la gestione coordinata della sicurezza dei dispositivi medici.
- Gli organi di amministrazione e direttivi istituiscono la figura del referente della cybersicurezza. Sia questo anche il punto di contatto NIS2 il suo operato deve includere la sicurezza anche dei

dispositivi medici. In questo senso, stante l'esistenza di un responsabile per la dispositivovigilanza, è necessario che quest'ultimo, con il supporto del referente della cybersicurezza, armonizzi le procedure inerenti i dispositivi medici con gli obblighi derivanti dalla NIS2.
- Valutazione del rischio cyber specifica per dispositivi medici: è importante implementare un processo strutturato che analizzi le vulnerabilità specifiche dei dispositivi medici, considerando sia l'impatto sulla sicurezza informatica che sulla sicurezza del paziente.
- Inventario completo dei dispositivi medici: è obbligatorio catalogare tutti i dispositivi medici connessi alla rete, classificandoli per criticità, funzione e livello di rischio di sicurezza informatica. I dispositivi medici che rientrano nella definizione dei sistemi informativi e di rete vanno ricompresi nel più ampio catalogo dei sistemi informativi e di rete richiamato dalla NIS2.

MISURE TECNICHE

In riferimento all'articolo 24 D.Lgs. 138/2024, comma 2, si ricordano le principali misure tecniche suggerite dalla NIS2 (anche se non tutte così chiaramente esplicitate) e che si applicano anche ai DM/IVD:

- Segmentazione della rete: è importante implementare un'architettura di rete segregata per i dispositivi medici, separandoli dalle altre reti ospedaliere per limitare la propagazione di potenziali attacchi.
- Monitoraggio continuo dei dispositivi: è importante attivare sistemi di monitoraggio specifici per i dispositivi medici che rilevino comportamenti anomali, accessi non autorizzati e potenziali vulnerabilità.
- Gestione degli aggiornamenti e patch: è importante sviluppare procedure specifiche per l'aggiornamento sicuro dei dispositivi medici, verificando preventivamente la compatibilità e l'impatto degli aggiornamenti sull'operatività clinica.
- Autenticazione forte e controllo accessi: è importante implementare meccanismi di autenticazione multi-fattore per l'accesso ai dispositivi medici e sistemi di controllo puntuale delle autorizzazioni.

PROCESSI E DOCUMENTAZIONE

In riferimento agli articoli 30 e 31 D.Lgs. 138/2024, ed in continuità a quanto già richiamato in termini di responsabilità ed obblighi, sarà importante rivedere le procedure relative alla gestione dei DM o IVD. In particolare:

- Realizzare il piano di risposta agli incidenti specifico per i dispositivi medici. Definire procedure dedicate che contemplino le particolarità dei dispositivi medici, i tempi di risposta e le priorità di intervento in base all'impatto sulla sicurezza del paziente. (Art. 24.2 b) D.Lgs. 138/2024).
- Definire una procedura di notifica incidenti. Predisporre un workflow chiaro per la notifica degli incidenti al CSIRT Italia entro le tempistiche previste dalla normativa (allarme iniziale entro 24 ore, notifica completa entro 72 ore). (Art. 24.2 b), Art. 25 e 26 D.Lgs. 138/2024) (Guida alla notifica degli incidenti al CSIRT Italia). Verificare in particolare se e quando una notifica di incidente al CSIRT corrisponda anche una segnalazione in termini di dispositivovigilanza. Si ritiene ragionevole ipotizzare che se un dispositivo medico è soggetto ad un rischio di cybersicurezza diventi auto-

maticamente esposto anche ad un rischio clinico essendo il dispositivo medico esposto a manomissione.
- Realizzare piano della continuità operativa. Sviluppare piani di continuità e disaster recovery specifici per i dispositivi medici critici, considerando procedure alternative in caso di indisponibilità tecnologica. (Art. 24.2 c) D.Lgs. 138/2024).
- Manutenere documentazione tecnica di sicurezza. Mantenere aggiornata la documentazione relativa alle configurazioni di sicurezza, valutazioni di rischio e misure di mitigazione implementate per ciascun dispositivo medico.

RAPPORTI CON FORNITORI E PRODUTTORI

In riferimento agli articoli 24 (comma 2, lettera d e lettera e) e 37 del D.Lgs. 138/2024 si rende inoltre necessario considerare nelle procedure relative ai DM e IVD i seguenti aspetti.
- Verifica dei requisiti di sicurezza in fase di acquisto: integrare criteri specifici di cybersecurity nei capitolati di gara per l'acquisizione di nuovi dispositivi medici, richiedendo evidenze di conformità alla NIS2.
- Accordi di responsabilità con i fornitori: formalizzare contrattualmente le responsabilità in tema di cybersecurity, inclusi i tempi di intervento, il supporto per la gestione degli incidenti e la fornitura di aggiornamenti di sicurezza.
- Valutazione della supply chain: verificare che i produttori di dispositivi medici rispettino a loro volta gli obblighi della NIS2 e adottino prassi di secure development nella realizzazione dei dispositivi.
- Coordinamento per la gestione degli accessi remoti: definire procedure rigorose per gli accessi remoti dei fornitori ai dispositivi medici, prevedendo autenticazione forte, monitoraggio delle sessioni e revoca tempestiva degli accessi. (Art. 24.2 l) D.Lgs. 138/2024).

FORMAZIONE E SENSIBILIZZAZIONE

In riferimento all'articolo 23, comma 1, lettera c si rende inoltre necessario considerare nelle procedure relative ai DM e IVD i seguenti aspetti.
- Definire un programma di formazione specializzato (Art. 23.2 b) D.Lgs. 138/2024) (Art. 24.2 g) D.Lgs. 138/2024): implementare percorsi formativi specifici sulla sicurezza dei dispositivi medici per il personale clinico, tecnico e amministrativo, differenziati per ruolo e responsabilità.
- Sensibilizzazione del personale sanitario (Art. 23.2 b) D.Lgs. 138/2024) (Art. 24.2 g) D.Lgs. 138/2024). Sviluppare materiale informativo e sessioni periodiche di aggiornamento sulle minacce cyber specifiche per i dispositivi medici rivolte al personale sanitario.
- Realizzare simulazione di incidenti (Art. 24, comma 2, lett. f) D.Lgs. 138/2024). Organizzare esercitazioni periodiche di gestione di incidenti cyber che coinvolgano dispositivi medici per testare l'efficacia delle procedure e migliorare la preparazione del personale.

VERIFICA E MIGLIORAMENTO CONTINUO

In riferimento all'articolo 24 (comma 2, lettera f) del D.Lgs. 138/2024 si rende inoltre necessario considerare nelle procedure relative ai DM e IVD i seguenti aspetti.

- Realizzare audit periodici di conformità (Art. 41-42 D.Lgs. 138/2024). Pianificare verifiche regolari del livello di aderenza ai requisiti della NIS2 per quanto concerne i dispositivi medici.
- Realizzare Vulnerability assessment e penetration test (Art. 24, comma 2, lett. c) D.Lgs. 138/2024). Effettuare regolarmente test di sicurezza specifici sui dispositivi medici e sulle reti dedicate, utilizzando metodologie appropriate e sicure.
- Realizzare revisione della documentazione (Art. 24, comma 2, lett. a) e j) D.Lgs. 138/2024). Aggiornare periodicamente l'analisi dei rischi, i piani di risposta agli incidenti e le procedure operative in funzione dell'evoluzione delle minacce e dei cambiamenti nell'infrastruttura tecnologica.
- Realizzare dashboard di monitoraggio (Art. 24, comma 2, lett. d) D.Lgs. 138/2024). Implementare sistemi di reporting che permettano di visualizzare in tempo reale lo stato di sicurezza dei dispositivi medici e tracciare i progressi verso la piena conformità alla NIS2.

NIS2 e regolamento UE 2023/2854 (DATA ACT): accesso equo ai dati

QUADRO NORMATIVO E FINALITÀ

Il Regolamento Data Act (UE 2023/2854), entrato in vigore l'11 gennaio 2024 e applicabile dal 12 settembre 2025, mira a facilitare l'accesso e l'utilizzo dei dati, in particolare quelli generati da prodotti connessi (IoT) e servizi correlati, garantendo condizioni di equità nell'economia dei dati.
Considerando che la definizione dei sistemi informativi e di rete del DLgs 138/2024 comprende i dati digitali conservati, elaborati, estratti o trasmessi per mezzo di reti o dispositivi è evidente che i sistemi di accesso ai dati previsti dal Data Act rientrano a pieno titolo tra quelli soggiacenti la NIS2. Diventa pertanto importante analizzare entrambe le norme.

Tabella 1 - Confronto sinottico tra le normative

Caratteristica	NIS 2 (D.Lgs. 138/2024)	Data Act (Reg. UE 2023/2854)
Obiettivo primario	Elevati livelli di cybersicurezza	Accesso equo e utilizzo dei dati
Soggetti interessati	Soggetti essenziali/importanti in settori critici (incluso sanitario)	Produttori/utilizzatori di prodotti connessi, titolari e destinatari di dati
Obblighi principali	Misure di sicurezza, gestione rischi, notifica incidenti	Condivisione dati con utenti/terze parti, portabilità cloud
Autorità competenti	ACN, Ministero della Salute (settore sanitario)	Future autorità nazionali designate
Tempistiche attuative	Registrazione entro febbraio 2025, piena conformità entro ottobre 2026	Applicazione da settembre 2025

INTERSEZIONI E PUNTI DI CONTATTO CHIAVE

Sicurezza dei Dati vs. Condivisione dei Dati

La NIS2 impone misure tecniche e organizzative per proteggere sistemi e dati, mentre il Data Act promuove l'accesso e la condivisione dei dati. Questa dicotomia rappresenta una sfida: l'obbligo di condividere dati potrebbe ampliare la superficie di attacco se non gestito con adeguate misure di sicurezza.

L'interazione si manifesta in particolare nel contesto dei prodotti connessi. Un dispositivo medico connesso o un sistema industriale IoT dovrà simultaneamente:

- Garantire elevati standard di sicurezza (NIS2)
- Rendere accessibili i dati generati all'utente e a terze parti autorizzate (Data Act)

I soggetti NIS2 dovranno necessariamente integrare nella loro analisi dei rischi i nuovi scenari specificamente introdotti dagli obblighi di accesso e condivisione dei dati previsti dal Data Act. Questa valutazione dovrà abbracciare l'intero ciclo di vita del dato, inclusa la sua "esportazione" sicura verso l'esterno.

Catena di Approvvigionamento e Condivisione con Terze Parti

La NIS2 richiede la gestione dei rischi della catena di approvvigionamento, mentre il Data Act introduce obblighi di condivisione dei dati con utenti e terzi da questi designati. Si configura così un espansione del concetto tradizionale di "supply chain": ai fornitori diretti si aggiungono gli utenti che esercitano diritti di accesso ai dati e le terze parti da essi designate come destinatarie.

Nel settore sanitario, questo implica che ospedali ed enti sanitari essenziali dovranno:

- Valutare la sicurezza non solo dei propri fornitori ICT
- Gestire rischi associati alla condivisione dei dati con pazienti, altre strutture e fornitori terzi di servizi analitici

Gestione degli Incidenti e Notifiche

Il D.Lgs. 138/2024, in attuazione della NIS2, prevede l'obbligo di notificare tempestivamente gli incidenti significativi all'ACN (entro 24 ore per la notifica preliminare). Il Data Act, sebbene non stabilisca un regime analogo, contempla situazioni in cui:

- In caso di emergenze pubbliche, inclusi incidenti di cybersicurezza gravi, i titolari dei dati sono obbligati a fornire dati richiesti dalle autorità competenti
- I titolari dei dati possono rifiutare o sospendere la condivisione dei dati per motivi legittimi (es. rischi per la sicurezza), notificando tale decisione all'autorità competente

Un attacco informatico grave a danno di un gruppo ospedaliero potrebbe attivare meccanismi di condivisione dei dati previsti dal Data Act per facilitare la gestione, la risposta o la prevenzione di ulteriori incidenti.

Interoperabilità e Portabilità dei Dati

Il Data Act pone forte enfasi sull'interoperabilità e sulla portabilità dei dati, specialmente per i servizi cloud, imponendo la rimozione degli ostacoli al "cloud switching". Questo allinea i suoi obiettivi con

quelli della NIS2 in termini di continuità operativa: l'interoperabilità e la portabilità facilitano il ripristino dei servizi in caso di incidenti.
Tuttavia, l'apertura dei sistemi per garantire interoperabilità deve essere bilanciata con adeguati controlli di sicurezza per evitare nuove vulnerabilità.

IMPATTI SULLA CONFORMITÀ E RACCOMANDAZIONI OPERATIVE

La coesistenza di NIS2 e Data Act impone alle organizzazioni, particolarmente nel settore sanitario, una visione olistica della governance dei dati. I temi della condivisione, dell'accesso, dell'interoperabilità, nonché della sicurezza e protezione dei dati, devono essere affrontati in maniera coordinata.

Adeguamento dei Sistemi e delle Infrastrutture

Le organizzazioni dovranno:

- Implementare API sicure per l'accesso e la condivisione dei dati
- Aggiornare i protocolli di autenticazione e autorizzazione per gestire accessi esterni
- Applicare crittografia per dati in transito verso terzi
- Adottare un approccio di "security by design and by default" insieme a "data sharing by design"

Nel settore sanitario, questo significa progettare sistemi clinici e dispositivi medici che incorporino sia robuste misure di cybersecurity sia funzionalità di accesso ai dati.

Revisione delle Policy e Procedure

L'interazione tra NIS2 e Data Act richiederà un riesame continuo delle policy interne. Le organizzazioni dovranno aggiornare:

- Policy di sicurezza informatica
- Procedure di data governance
- Gestione degli incidenti
- Supply chain management

Particolarmente nel settore sanitario, sarà necessario:

- Sviluppare procedure specifiche per la gestione delle richieste di accesso ai dati
- Implementare criteri di valutazione del rischio per le richieste di condivisione
- Coordinare i flussi di notifica verso le diverse autorità (ACN, Garante Privacy, coordinatore dati)

Raccomandazioni Concrete per una Compliance Integrata

- Mappatura integrata di sistemi e flussi dati: identificare gli asset critici (NIS2) e i dati generati/condivisi (Data Act) attraverso un unico progetto di assessment.
- Governance unificata: istituire un team multidisciplinare che includa responsabili IT/cybersecurity, data governance, legale e privacy.
- Revisione contrattuale: aggiornare i contratti con fornitori di tecnologia e servizi includendo clausole sia di sicurezza (NIS2) sia di condivisione dati (Data Act).
- Aggiornamento dei piani di continuità e incident response: integrare scenari di data sharing con autorità e terze parti nelle procedure di gestione delle crisi.

- Formazione congiunta: sviluppare programmi formativi che coprano simultaneamente obblighi di cybersicurezza e diritti/doveri relativi alla condivisione dei dati.
- Approccio "security & data governance by design": per nuovi progetti digitali, incorporare fin dalla progettazione requisiti di entrambe le normative.

Nel settore sanitario, è particolarmente importante considerare la sensibilità dei dati e il rischio potenziale per la sicurezza dei pazienti, bilanciando apertura e protezione.

Sinergie e Opportunità

La portabilità dei dati (Data Act) può rafforzare la continuità operativa (NIS2). Se un fornitore cloud di un ospedale subisce un grave incidente, la possibilità di migrare rapidamente dati e applicazioni su un altro cloud server contribuisce a ripristinare i servizi sanitari essenziali più velocemente.

Regolamento UE 2024/1689 (AI ACT): governance dell'AI nel settore sanitario nell'era della NIS2

INQUADRAMENTO NORMATIVO

Nel settore sanitario, la sovrapposizione è particolarmente significativa poiché quasi tutti i sistemi IA utilizzati in ambito medico (diagnostica, supporto decisionale clinico, monitoraggio) rientrano nella categoria "alto rischio" ai sensi dell'AI Act, mentre ospedali, cliniche e strutture sanitarie pubbliche/private sono considerate "entità essenziali" soggette a NIS2.

Tabella 2 - Confronto sinottico tra le normative

Aspetto	Direttiva NIS2 (D.Lgs. 138/2024)	AI Act (Regolamento UE 2024/1689)
Obiettivo principale	Garantire elevato livello di cybersicurezza per reti e sistemi informativi di soggetti essenziali e importanti	Stabilire regole armonizzate per sviluppo, immissione sul mercato e utilizzo di sistemi di IA sicuri e affidabili
Approccio	Obblighi basati sul tipo di soggetto	Approccio basato sul rischio (4 categorie: minimo, limitato, alto, inaccettabile)
Soggetti obbligati	Entità essenziali e importanti in settori critici (inclusa sanità)	Fornitori, deployer e utilizzatori di sistemi IA, con obblighi differenziati
Entrata in vigore	D.Lgs. 138/2024 in vigore dal 16/10/2024; soggetti essenziali identificati entro 17/04/2025	In vigore dal 01/08/2024; applicazione scaglionata fino al 2026-2027

PRINCIPALI REQUISITI E OBBLIGHI

La NIS2 richiede un approccio "multirischio" (all-hazards) per proteggere reti e sistemi informativi, con numerose aree di intervento (Art. 24 D.Lgs. 138/2024) che includono:

- Politiche di analisi dei rischi e sicurezza dei sistemi informativi
- Gestione degli incidenti e continuità operativa
- Sicurezza della catena di approvvigionamento
- Pratiche di igiene informatica e formazione
- Sistemi di autenticazione avanzata e comunicazioni protette

L'AI Act impone per i sistemi ad alto rischio (Art. 15) requisiti specifici su:

- Accuratezza, robustezza e resilienza tecnica
- Protezione contro attacchi malevoli, data poisoning e alterazioni malevole
- Resilienza contro errori e incongruenze durante il ciclo di vita

Importante è anche analizzare le modalità con cui debbono essere notificate le segnalazioni alle autorità.

Tabella 3 - Confronto sulle segnalazioni

NIS2 (D.Lgs. 138/2024, art. 25- 26)	**AI Act (art. 73)**
Notifica incidenti significativi al CSIRT Italia/ACN	Notifica incidenti gravi/malfunzionamenti alle autorità di vigilanza
Preallarme entro 24h, notifica entro 72h, relazione finale entro 1 mese	Notifica entro 15 giorni (2 giorni per casi molto gravi)
Focus su impatto su disponibilità/continuità dei servizi	Focus su impatto su sicurezza, salute e diritti fondamentali
Entrata in vigore	In vigore dal 01/08/2024; applicazione scaglionata fino al 2026-2027

Un singolo evento potrebbe richiedere notifiche parallele a diverse autorità, rendendo necessario un coordinamento interno.

PUNTI DI CONTATTO

Entrambe le normative richiedono un approccio basato sul rischio, ma con punti di focalizzazione differenti: NIS2 si concentra sulla protezione dell'infrastruttura IT, mentre l'AI Act sui rischi specifici dei sistemi IA (bias, errori, manipolazione). Per le organizzazioni sanitarie che utilizzano sistemi IA, è necessario integrare queste dimensioni in un framework unificato, considerando:

- Come un attacco informatico può compromettere un sistema IA
- Come un sistema IA vulnerabile può rappresentare un rischio per la cybersicurezza
- Rischi combinati che impattano la sicurezza dei pazienti e la continuità del servizio

La NIS2 impone di valutare i rischi informatici legati ai fornitori, mentre l'AI Act richiede garanzie sulla conformità e sicurezza dei sistemi IA acquisiti. Per le organizzazioni sanitarie, questo significa:

- Verificare che i fornitori di sistemi IA rispettino i requisiti dell'AI Act (marcatura CE per sistemi ad alto rischio, documentazione tecnica)

- Integrare clausole di sicurezza e conformità nei contratti con fornitori
- Implementare controlli sulla sicurezza dell'intero ecosistema di fornitori

Per il D.Lgs. 138/2024: artt. 3 (comma 9), 24, 25. Per l'AI Act, ex multis: artt. 16, 25, 62, 89, 91.
Le due normative attribuiscono responsabilità a livelli dirigenziali:

- NIS2: responsabilità degli organi di amministrazione per approvazione e supervisione delle misure di sicurezza (D.Lgs. 138/2024, art. 23)
- AI Act: obblighi di alfabetizzazione AI e adeguata governance dei sistemi (AI Act, principalmente artt. 4, 9, 10)

La formazione è un elemento chiave in entrambi i contesti, con NIS2 che richiede competenze in cybersicurezza e l'AI Act che introduce il concetto di "alfabetizzazione AI".

CONFORMITÀ NEL SETTORE SANITARIO

In ambito sanitario, la conformità integrata NIS2/AI Act comporta:

- Ampliamento dell'analisi dei rischi per includere vulnerabilità specifiche dei sistemi IA clinici:
  - Attacchi malevoli che possano ingannare i sistemi diagnostici
  - Data poisoning dei modelli con conseguente compromissione della sicurezza del paziente
  - Bias algoritmici con potenziali impatti discriminatori sulle cure
- Documentazione e audit integrati:
  - Per sistemi IA ad alto rischio: documentazione tecnica, valutazione di conformità, marcatura CE
  - Possibilità di valutazione unica combinata MDR (Medical Device Regulation) + AI Act per dispositivi medici
  - Integrazione dei requisiti documentali NIS2 (policy, risk assessment, piani di continuità)
- Gestione coordinata degli incidenti:
  - Procedure unificate per incidenti che coinvolgono sistemi IA
  - Notifiche multiple a diverse autorità (CSIRT/ACN, autorità di vigilanza, eventualmente Garante Privacy)
  - Analisi post-incidente che considera entrambe le prospettive (cyber e IA)
- Competenze e risorse necessarie:
  - Figure professionali con competenze ibride (cybersicurezza + IA)
  - Task force interfunzionali o Digital Compliance Officer per coordinare gli sforzi
  - Formazione continua per personale clinico su cybersicurezza e uso sicuro/corretto dei sistemi IA

RACCOMANDAZIONI

- Governance integrata: istituire un comitato di governance digitale che includa competenze di cybersicurezza, IA, protezione dati e compliance, per supervisionare l'implementazione coordinata di NIS2 e AI Act.
- Framework di rischio unificato: adottare un approccio olistico alla gestione dei rischi che integri minacce cyber tradizionali e rischi specifici dell'IA, possibilmente basandosi su standard come il NIST AI Risk Management Framework.
- Revisione contrattualistica: aggiornare i contratti con fornitori di tecnologie/servizi IA per includere clausole su conformità, sicurezza, notifica vulnerabilità e supporto in caso di incidenti.

- Piano formativo trasversale: implementare programmi di formazione per diverse categorie di personale sanitario che coprano sia elementi di cybersicurezza che di "alfabetizzazione AI", con particolare attenzione ai clinici che utilizzano sistemi di supporto decisionale.
- Procedure di Incident Response coordinate: sviluppare procedure integrate che permettano di gestire efficacemente incidenti con dimensione cyber e IA, assicurando corretta notifica a tutte le autorità competenti.
- Monitoraggio continuo dell'evoluzione normativa: mantenere un processo di aggiornamento costante sugli sviluppi normativi (atti delegati, linee guida) relativi a entrambe le normative per adeguare tempestivamente policy e misure.

La NIS2 e il Codice dei Contratti Pubblici (D. Lgs. 36/2023)

L'approvvigionamento di beni e servizi emerge nella NIS2 come elemento fondamentale. Per le aziende sanitarie pubbliche l'applicazione della NIS2 si trova quindi a dialogare con il codice dei contratti pubblici (DLgs. 36/2023) ed al correlato DPCM del 30 aprile 2025 (Disciplina dei contratti di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici e della sicurezza nazionale).
Dalla lettura incrociata emerge come dalla NIS2 gli Stati membri nella catena di approvvigionamento dei prodotti e dei servizi ICT debbano adottare:

- misure strategiche riguardanti la cybersicurezza;
- requisiti concernenti la cybersicurezza, compresi i requisiti relativi alla certificazione, alla cifratura e la valutazione sull'utilizzo di prodotti open source.

Mentre secondo il codice degli appalti le stazioni appaltanti:

- operano secondo i principi di neutralità tecnologica, di trasparenza, nonché di protezione dei dati personali e di sicurezza informatica;
- adottano misure tecniche e organizzative a presidio della sicurezza informatica e della protezione dei dati personali;
- nella valutazione dell'elemento qualitativo di un'offerta (individuazione del miglior rapporto qualità-prezzo), tengono sempre in considerazione gli elementi di cybersicurezza e, nei casi in cui il contesto di impiego è connesso alla tutela degli interessi nazionali strategici, vi attribuiscono specifico e peculiare rilievo, stabilendo anche un tetto massimo per il punteggio economico entro il limite del 10 per cento.

Inserendo nell'analisi anche la già citata Legge 90/2024 emerge come, relativamente agli appalti pubblici il legislatore abbia voluto dare specifiche prescrizioni in materia di approvvigionamenti di elementi correlati alla cybersicurezza. In particolare demanda ad un decreto del Presidente del Consiglio dei Ministri (DPCM) - da adottare entro centoventi giorni dalla data di entrata in vigore della legge 90/2024 su proposta dell'Agenzia per la Cybersicurezza Nazionale, previo parere del Comitato interministeriale per la sicurezza della Repubblica - l'individuazione, per specifiche categorie tecnologiche di beni e servizi informatici:

- degli elementi essenziali di cybersicurezza da tenere in considerazione nelle attività di approvvigionamento di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici;
- dei casi in cui, per la tutela della sicurezza nazionale, devono essere previsti criteri di premialità per le proposte o per le offerte che contemplino l'uso di tecnologie di cybersicurezza italiane o di Paesi appartenenti all'Unione europea o di Paesi aderenti all'Alleanza atlantica (NATO) o di Paesi terzi che sono parte di accordi di collaborazione con l'Unione europea o con la NATO in materia di cybersicurezza, protezione delle informazioni classificate, ricerca e innovazione.

La norma definisce gli elementi essenziali di cybersicurezza come l'insieme di criteri e regole tecniche la conformità ai quali, da parte di beni e servizi informatici da acquisire, garantisce la confidenzialità, l'integrità e la disponibilità dei dati da trattare in misura corrispondente alle esigenze di tutela della sicurezza nazionale.

Inoltre la norma fornisce precise prescrizioni alle stazioni appaltanti:

- tengono sempre in considerazione gli elementi essenziali di cybersicurezza nella valutazione dell'elemento qualitativo, ai fini dell'individuazione del miglior rapporto qualità/prezzo per l'aggiudicazione o, nel caso in cui sia utilizzato il criterio del minor prezzo, di inserire gli elementi di cybersicurezza tra i requisiti minimi dell'offerta;
- nel caso in cui sia utilizzato il criterio dell'offerta economicamente più vantaggiosa, stabiliscono un tetto massimo per il punteggio economico entro il limite del 10 per cento;
- prevedono criteri di premialità per le proposte o per le offerte che contemplino l'uso di tecnologie di cybersicurezza italiane o di Paesi appartenenti all'Unione europea o di Paesi aderenti alla NATO o di Paesi terzi individuati tra quelli che sono parte di accordi di collaborazione con l'Unione europea o con la NATO in materia di cybersicurezza, protezione delle informazioni classificate, ricerca e innovazione, al fine di tutelare la sicurezza nazionale e di conseguire l'autonomia tecnologica e strategica nell'ambito della cybersicurezza;
- non aggiudicano l'appalto se non tiene in considerazione gli elementi essenziali di cybersicurezza (cfr. articoli 107, comma 2 - 108, comma 10 del codice dei contratti pubblici).

L'articolo 14 della Legge 90/2024 viene attuato dal decreto del Presidente del Consiglio dei Ministri del 30 Aprile 2025. Vengono così dettagliati nell'allegato 1 della norma (allegato C del presente documento) gli elementi essenziali di cybersicurezza (requisiti relativi alle proprietà dei beni e dei servizi informatici e requisiti di gestione delle vulnerabilità), nell'allegato 2 della norma (allegato D del presente documento) le categorie tecnologiche di beni e servizi informatici (elementi essenziali di cybersicurezza, sulla base dei Common Procurement Vocabulary), i criteri di premialità. Questi ultimi sono forse tra gli aspetti più complessi della fase di acquisizione. Riguardano infatti criteri di premialità per le proposte o per le offerte che contemplano l'uso di tecnologie di cybersicurezza italiane o di Paesi appartenenti all'Unione europea o di Paesi aderenti all'Alleanza atlantica (NATO) o di Paesi terzi individuati tra quelli che sono parte di accordi di collaborazione con l'Unione europea o con la NATO in materia di cybersicurezza, protezione delle informazioni classificate, ricerca e innovazione.

Si applicano previa analisi dell'elenco di tutti i componenti di fabbricazione del prodotto o delle infrastrutture impiegate per erogare un servizio (cosiddetto B.O.M. - Bill of materials) presentato in sede di

proposta o offerta dagli operatori economici. I medesimi criteri di premialità si applicano, in maniera paritaria e uniforme, alle proposte o alle offerte che contemplino l'uso di tecnologie di cybersicurezza italiane o di Paesi appartenenti all'Unione europea o di Paesi aderenti all'Alleanza atlantica (NATO) o dei Paesi terzi individuati (allegato 3 della norma e allegato E del presente documento).

Determinazioni ACN

Le determinazioni ACN rappresentano il punto di riferimento operativo per le aziende sanitarie in ambito di applicazione della NIS2. In bibliografia sono riportate le determinazioni pubblicate sino a maggio 2025 (dal [2] al [9]).
Qui di seguito si richiamano tratti di alcune determinazioni che includono definizioni, procedure e/o obblighi significativi da cui derivano procedure e istruzioni contenute nel presente testo.

DETERMINAZIONE ACN 136117 DEL 10 APRILE 2025

Articolo 4 (Punto di contatto)

1. *Il punto di contatto è una persona fisica designata dal soggetto NIS con il compito di curare l'attuazione delle disposizioni del decreto NIS per conto del soggetto stesso. In particolare, il punto di contatto accede al Portale ACN e ai Servizi NIS, effettua, per conto del soggetto, la registrazione di cui all'articolo 7 del decreto NIS, e interloquisce, per conto del soggetto NIS, con l'Autorità nazionale competente NIS.*
2. *Le funzioni di punto di contatto possono essere svolte dal rappresentante legale del soggetto NIS, da uno dei procuratori generali del soggetto NIS, censiti sul registro delle imprese di cui all'articolo 8 della legge 29 dicembre 1993, n. 580, o da un dipendente del soggetto NIS delegato dal rappresentante legale del soggetto medesimo. Laddove il punto di contatto, nell'espletamento delle proprie funzioni, si avvalga di personale esterno, restano comunque ferme le disposizioni di cui al comma 1.*
3. *Qualora il soggetto sia parte di un gruppo di imprese, le funzioni di punto di contatto possono essere svolte da un dipendente di un'altra impresa del gruppo che rientra nell'ambito di applicazione del decreto NIS, delegato dal rappresentante legale del soggetto stesso.*
4. *Qualora il soggetto NIS sia una pubblica amministrazione, le funzioni di punto di contatto possono essere svolte da personale che presta servizio o dipendente di un'altra pubblica amministrazione che rientra nell'ambito di applicazione del decreto NIS, previa autorizzazione di quest'ultima ai sensi dell'articolo 53 del decreto legislativo 30 marzo 2001, n. 165, delegato dal rappresentante legale del soggetto stesso.*
5. *Il punto di contatto riferisce direttamente al vertice gerarchico del soggetto NIS nonché agli organi di amministrazione e direttivi del soggetto medesimo ai fini di quanto previsto dal decreto NIS.*
6. *Resta ferma, in ogni caso, la responsabilità degli organi di amministrazione e direttivi del soggetto NIS ai sensi dell'articolo 23 del decreto NIS e delle persone fisiche ai sensi dell'articolo 38 del medesimo decreto.*

7. *Nel caso di avvicendamento del punto di contatto, gli organi di amministrazione e direttivi provvedono senza ingiustificato ritardo alla designazione del nuovo punto di contatto e assicurano il suo censimento sul Portale ACN.*
8. *La designazione del punto di contatto da parte dei soggetti di cui all'articolo 1, comma 1, della legge 28 giugno 2024, n. 90, che rientrano nell'ambito di applicazione del decreto NIS, può soddisfare l'obbligo di nomina e comunicazione del referente per la cybersicurezza di cui all'articolo 8, comma 2, della medesima legge.*

Con questa determinazione ACN dettaglia il ruolo, le competenze e l'afferenza del punto di contatto. Accordato, come già richiamato nell'apposita sezione che analizza la legge 90/2024, che le aziende sanitarie rispondono ad entrambe le normative e che la legge 90/2024 definisce e istituzionalizza il ruolo di referente per la cybersicurezza, è utile considerare similitudini e differenze di queste due figure.
Nelle FAQ della determinazione di ACN viene esplicitato che non necessariamente debba essere un tecnico.
Nella legge 90/2025 appare chiaro come il referente per la cybersicurezza abbia anche chiare competenze tecniche. Sempre nella legge 90/2024 viene esplicitato il fatto che il referente per la cybersicurezza svolga anche le funzioni di punto di contatto con ACN.
Sempre nella legge 90/2024 si permette l'individuazione del referente della cybersicurezza nella figura già istituita del Responsabile per la Transizione al Digitale.
Da questo disposto combinato di legge, per le aziende sanitarie pubbliche diventa pertanto ovvio applicare questa individuazione: Responsabile per la Transizione al Digitale (nominato per effetto del CAD) assume la nomina anche di referente per la cybersicurezza (nominato per effetto della legge 90/2024) che automaticamente è anche punto di contatto ACN (sempre per la medesima legge 90/2024).
Una diversa composizione tra referente cybersicurezza (e non tanto di punto di contatto che come detto è automaticamente individuato nel referente per la cybersicurezza) e RTD dovrebbe essere normata a livello di singola azienda sanitaria in considerazioni delle diverse responsabilità reciproche esistenti tra queste due figure.

Articolo 5 (Sostituto punto di contatto)
1. *Il sostituto punto di contatto è una persona fisica, distinta dal punto di contatto, designato con le medesime modalità di quest'ultimo ai sensi dell'articolo 4 a cui si applicano le previsioni del citato articolo.*
2. *Il sostituto punto di contatto supporta il punto di contatto nell'esercizio delle proprie funzioni, può interloquire direttamente con l'Autorità nazionale competente NIS e può effettuare sulla piattaforma digitale le medesime azioni del punto di contatto, ad eccezione della registrazione di cui all'articolo 7 del decreto NIS.*
3. *Il sostituto punto di contatto è designato entro il 31 maggio dell'anno in cui il soggetto NIS ha ricevuto comunicazione di inserimento nell'elenco dei soggetti NIS.*

Proseguendo quanto già analizzato relativamente alla nomina del punto di contatto è ragionevole ipotizzare che il sostituto punto di contatto venga individuato all'interno della struttura per la transizione al digitale (rispondente quindi al RTD - punto di contatto).

Articolo 16 (Elencazione degli organi di amministrazione e direttivi)

1. *Ai fini dell'articolo 15, comma 3, lettera b), tramite il Servizio NIS/Aggiornamento annuale, gli utenti elencano i codici fiscali delle persone fisiche che compongono gli organi di amministrazione e direttivi, indicandone l'indirizzo di posta elettronica certificata.*
2. *Le informazioni di cui al comma 1 sono confermate dal punto di contatto.*
3. *Ai fini dell'articolo 7, comma 4, lettera c), del decreto NIS, le persone fisiche appartenenti agli organi di amministrazione e direttivi del soggetto NIS accettano tale indicazione accedendo al Portale ACN, secondo la procedura telematica indicata nella richiesta inviata a loro indirizzo di posta elettronica certificata di cui al comma 1.*

Le persone fisiche che devono essere elencate ai sensi dell'articolo 7, comma 4, lettera c) del decreto NIS sono le persone fisiche responsabili ai sensi dell'articolo 38, comma 5, del decreto NIS. In altri termini si tratta delle persone fisiche che compongono gli organi di amministrazione e gli organi direttivi dei soggetti essenziali e dei soggetti importanti di cui all'articolo 23 del decreto NIS.
Pertanto, ai fini dell'aggiornamento annuale è richiesta la sola l'elencazione dei componenti del Consiglio di amministrazione dell'organizzazione, o strutture analoghe tenuto conto della natura giuridica e alla struttura organizzativa dell'organizzazione. Essi, infatti, ai sensi dell'articolo 23, sovrintendono all'implementazione degli obblighi di cui al decreto NIS e sono responsabili delle eventuali violazioni.
Pertanto, ai fini dell'adempimento in parola, non è attesa l'elencazione delle persone fisiche che svolgono le funzioni di punto di contatto (e sostituto), di CISO o di responsabile della sicurezza aziendale, né altre figure apicali sotto ordinate al CDA, salvo che essi siano anche componenti del CDA.
Per le aziende sanitarie pubbliche, in attesa di indicazioni dal competente Ministero della Salute, è ragionevole ipotizzare e concordare all'interno della singola amministrazione che siano almeno elencati Direttore Generale, Direttore Amministrativo e Direttore Sanitario. Tuttavia ai fini di una diffusa assunzione di responsabilità risulta compatibile anche l'inserimento dell'intero Collegio di Direzione.

DETERMINAZIONE ACN 136118 DEL 10 APRILE 2025

Articolo 2 (Oggetto, ambito di applicazione e finalità)

1. *La presente determinazione stabilisce le modalità con cui i soggetti NIS notificano all'Autorità nazionale competente NIS la loro partecipazione agli accordi di condivisione.*

Per le aziende sanitarie pubbliche o meno, in attesa di indicazioni dal competente Ministero della Salute, è ragionevole ipotizzare e concordare che siano formalizzati e indicati anche i protocolli operativi che permettono la condivisione di piattaforme tecnologiche e/o applicative o accordi di mutuo soccorso che determinano punti di intersezione delle reti di sistemi informativi esistenti.
Determinazione ACN 164179 del 14 aprile 2025 – Specifiche di base per l'adempimento agli obblighi di cui agli articoli 23, 24, 25, 29 e 32 del decreto NIS.

Le misure di sicurezza di base NIS2 per i soggetti essenziali sono delineate nell'Allegato 2 del documento ACN, strutturate in 16 categorie principali che coprono un ampio spettro della gestione della cybersecurity. Queste misure sono progettate per garantire un elevato livello comune di sicurezza delle reti e dei sistemi informativi in tutta l'Unione Europea, ponendo l'accento su un approccio basato sul rischio e sulla governance.
Nell'allegato F è riportata la tabella completa delle misure di sicurezza di base NIS2 per i soggetti essenziali. Ogni misura è identificata da un codice (es. GV.OC-04) e accompagnata dalla sua descrizione e dai requisiti specifici. La presentazione integrale di questa tabella è essenziale in quanto delinea lo standard minimo richiesto dalla nuova direttiva, permettendo di identificare chiaramente dove le misure AGID possano essere già allineate o dove siano necessarie integrazioni e rafforzamenti. Da questa tabella discendono tutte le procedure analizzate successivamente.

Il confronto tra le misure di sicurezza AGID come normate nel CAD (D.Lgs 82/2005) e la NIS2

MISURE DI SICUREZZA AGID

Le misure di sicurezza AGID, storicamente definite per guidare la Pubblica Amministrazione e derivanti dal Codice dell'Amministrazione Digitale (D.Lgs. 82/2005), hanno fornito un framework strutturato per la gestione della sicurezza informatica. Queste misure sono state un punto di riferimento per l'adozione di pratiche di sicurezza robuste, coprendo aree fondamentali come la gestione dei rischi, la protezione fisica e logica, la gestione degli incidenti e la formazione del personale.
Le aziende sanitarie pubbliche hanno pertanto potuto avere un punto di riferimento per l'adozione di tecniche di sicurezza scegliendo (più o meno liberamente) quale livello dovessero adottare. Con l'entrata in vigore della NIS2 e in particolare le precitate determinazioni ACN vengono definiti dei requisiti per i soggetti essenziali che, almeno dal punto di vista formale, si affiancano e non sostituiscono a prescindere le misure AGID. Per questo motivo è utile, per le aziende sanitarie, un'analisi comparativa delle misure AGID con i requisiti NIS2.
Nel seguito tenteremo di evidenziare le corrispondenze, le specificità e le divergenze tra i due quadri normativi, supportando le organizzazioni nella comprensione delle nuove responsabilità e nell'allineamento delle proprie strategie di cybersecurity. Il confronto sarà strutturato per aree tematiche, basandosi sulla categorizzazione delle misure NIS2, e cercherà di identificare le correlazioni dirette e indirette con le misure AGID, includendo una matrice di mappatura per facilitare la consultazione puntuale. La tabella 4 contiene l'elenco delle categorie che classificavano le misure minime di sicurezza dettate da AGID.

ANALISI COMPARATIVA ORDINATA PER CATEGORIE DELLA DETERMINA ACN

Questa sezione presenta un'analisi punto per punto delle misure, organizzandole per categorie NIS2 e identificando le corrispondenze con le misure AGID. La comprensione di queste correlazioni è fondamentale per le organizzazioni che devono navigare tra i due quadri normativi.
Nell'allegato G è contenuta una tabella riassuntiva del confronto.

Tabella 4 - Categorie delle Misure Minime di Sicurezza ICT AGID

ABSC_ID #	Descrizione
A.1	Inventario degli asset hardware e software
A.2	Configurazione di sicurezza (hardening) di hardware e software
A.3	Gestione delle vulnerabilità
A.4	Gestione degli accessi (account, privilegi, autenticazione, sessioni)
A.5	Protezione dagli attacchi malware
A.6	Backup e ripristino dei dati e della configurazione
A.7	Gestione dei log (raccolta, analisi, conservazione)
A.8	Protezione delle comunicazioni (reti, e-mail, navigazione web)
A.9	Sicurezza fisica degli ambienti e delle infrastrutture
A.10	Gestione degli incidenti di sicurezza
A.11	Formazione e consapevolezza del personale
A.12	Gestione della continuità operativa

Gestione del Rischio (GV.OC-04, GV.RM-03, ID.RA-05, ID.RA-06)

La Direttiva NIS2 pone una forte enfasi sulla gestione del rischio di cybersecurity, elevandola a un livello strategico all'interno dell'organizzazione. Richiede la definizione, l'implementazione e la documentazione di un piano di gestione del rischio informatico, che deve essere approvato dagli organi amministrativi ed esecutivi. Questo piano deve includere l'identificazione, l'analisi, la valutazione, il trattamento e il monitoraggio dei rischi. Le valutazioni del rischio devono essere eseguite a intervalli pianificati, almeno ogni due anni, e in risposta a incidenti significativi, cambiamenti organizzativi o variazioni nell'esposizione alle minacce. Tali valutazioni devono considerare minacce interne ed esterne, vulnerabilità e impatti potenziali. La direttiva richiede inoltre un piano di trattamento del rischio, che definisca le opzioni di trattamento, le priorità e le tempistiche, e che giustifichi l'accettazione di eventuali rischi residui, anch'esso soggetto all'approvazione del vertice.

Le misure AGID, in particolare la misura A.3 (Gestione delle vulnerabilità) e il requisito ABSC 4.8.1 (Definire un piano di gestione dei rischi), hanno sempre previsto un approccio basato sul rischio, con requisiti per l'analisi e la valutazione dei rischi. Tuttavia, la NIS2 formalizza ulteriormente l'approvazione del rischio a livello di vertice e la periodicità delle valutazioni. Questa richiesta di approvazione da parte degli organi amministrativi ed esecutivi implica che la cybersecurity non è più considerata un problema puramente tecnico, ma una componente integrante della strategia aziendale. Ciò comporta una maggiore consapevolezza e un'allocazione più mirata delle risorse a livello dirigenziale, influenzando direttamente la capacità dell'organizzazione di definire e implementare politiche di sicurezza efficaci (GV.PO-01). Le organizzazioni dovranno pertanto integrare i processi di gestione del

rischio cybersecurity nei loro framework di gestione del rischio aziendale complessivo, richiedendo un coinvolgimento più profondo e una maggiore responsabilità del top management.

Ruoli e Responsabilità (GV.RR-02)

La NIS2 richiede la definizione, l'approvazione da parte degli organi amministrativi ed esecutivi e la comunicazione di un'organizzazione cybersecurity chiara, con ruoli e responsabilità ben stabiliti. È necessario mantenere un elenco aggiornato del personale con ruoli specifici e comunicarlo alle unità pertinenti. Un aspetto distintivo è l'obbligo di includere un punto di contatto e almeno un sostituto per la notifica degli incidenti, in conformità con il decreto NIS. Questi ruoli e responsabilità devono essere rivisti periodicamente (almeno ogni due anni) e in caso di eventi significativi o cambiamenti.
Le misure AGID, come la misura A.X (Ruoli e Responsabilità), hanno sempre richiesto la definizione di ruoli e responsabilità, come il Responsabile della Sicurezza ICT. Tuttavia, la NIS2 specifica ulteriormente la necessità di un'organizzazione cybersecurity formale e di punti di contatto specifici per le autorità. La chiara definizione dei ruoli e la loro approvazione a livello dirigenziale sono prerequisiti per un'efficace implementazione di tutte le altre misure di sicurezza. Senza una governance chiara, le politiche e i piani rimarrebbero mere dichiarazioni d'intenti. La necessità di un punto di contatto e un sostituto è direttamente collegata alla capacità di notifica degli incidenti, garantendo che le comunicazioni con le autorità siano rapide ed efficaci. Le organizzazioni dovranno formalizzare le proprie strutture di governance della cybersecurity, potenzialmente creando o rafforzando comitati esecutivi dedicati e assicurando che i responsabili abbiano l'autorità e le risorse necessarie.

Affidabilità delle Risorse Umane (GV.RR-04)

La NIS2 integra la cybersecurity nelle pratiche delle risorse umane, richiedendo l'identificazione e la valutazione del personale autorizzato e degli amministratori di sistema in base alla loro esperienza, capacità e affidabilità, assicurando la loro piena conformità alle normative di cybersecurity. Le procedure relative a queste valutazioni devono essere adottate e documentate. Un requisito significativo è la definizione contrattuale di eventuali obblighi di cybersecurity che rimangono validi dopo la cessazione o la modifica del rapporto di lavoro, come le clausole di riservatezza, in linea con i risultati della valutazione del rischio (ID.RA-05).
Le misure AGID, come la misura A.11 (Formazione e consapevolezza del personale), coprono aspetti della gestione del personale, ma la NIS2 è più esplicita sull'affidabilità del personale e sulla gestione delle clausole contrattuali post-impiego. La valutazione dell'affidabilità del personale e la definizione di obblighi contrattuali sono direttamente correlate alla prevenzione di incidenti interni e alla protezione dei dati sensibili. Una gestione inadeguata di questo aspetto può portare a violazioni di dati o accessi non autorizzati. Le aziende dovranno rivedere le proprie politiche HR e i contratti di lavoro per includere clausole specifiche sulla cybersecurity, e implementare processi di screening e monitoraggio più rigorosi per il personale con accesso a sistemi critici.

Conformità e Audit di Sicurezza (GV.PO-01, GV.PO-02, ID.IM-01)

La NIS2 impone l'adozione e la documentazione di politiche di cybersecurity per un'ampia gamma di

aree chiave, tra cui gestione del rischio, ruoli e responsabilità, gestione degli asset, gestione delle vulnerabilità, continuità operativa, gestione degli accessi, sicurezza fisica, formazione, sicurezza dei dati, sviluppo e manutenzione dei sistemi, protezione delle reti, monitoraggio degli eventi e risposta agli incidenti. Tali politiche devono essere approvate dagli organi amministrativi ed esecutivi e riviste periodicamente (almeno annualmente) o in caso di cambiamenti normativi, incidenti significativi o variazioni nell'esposizione alle minacce. La direttiva richiede anche la definizione, implementazione e approvazione di un piano di adattamento per garantire l'implementazione delle politiche di sicurezza, e un piano per la valutazione dell'efficacia delle misure di gestione del rischio, con report periodici al vertice.
Le misure AGID, come la misura A.X (Politiche e Procedure), richiedono anch'esse politiche e procedure di sicurezza, ma la NIS2 le dettaglia ulteriormente, specificando le aree che devono essere coperte e sottolineando l'importanza della revisione periodica e dell'approvazione formale. L'enfasi sui "piani di miglioramento" e sulla "valutazione dell'efficacia" è più marcata nella NIS2. La definizione e la revisione periodica delle politiche sono fondamentali per garantire che le misure di sicurezza rimangano pertinenti ed efficaci. Se le politiche non sono aggiornate, le misure tecniche e organizzative possono diventare obsolete e inefficaci, aumentando il rischio. I piani di miglioramento sono il risultato diretto della verifica delle politiche e dell'efficacia, creando un ciclo virtuoso. Le organizzazioni dovranno implementare un robusto framework di governance della sicurezza che includa cicli di revisione regolari, meccanismi di feedback e reportistica al top management sull'efficacia delle misure e sui piani di miglioramento.

Gestione dei Rischi per la Sicurezza Informatica della Catena di Approvvigionamento (GV.SC-01, GV.SC-02, GV.SC-04, GV.SC-05, GV.SC-07)

Questa è una delle aree più significative e innovative introdotte dalla NIS2. La direttiva richiede un programma di gestione del rischio della supply chain, con il coinvolgimento dell'organizzazione cybersecurity nei processi di procurement e la definizione di requisiti di sicurezza per le forniture coerenti con le misure interne dell'entità NIS. Questi requisiti devono considerare l'affidabilità del fornitore, i ruoli e le responsabilità nella fornitura, la gestione delle vulnerabilità, la continuità operativa, la sicurezza dei dati e lo sviluppo sicuro del codice. È necessario mantenere un inventario aggiornato dei fornitori critici e integrare i requisiti di sicurezza nei contratti. La NIS2 impone anche la valutazione e il monitoraggio continuo dei rischi posti dai fornitori, inclusi il loro livello di accesso ai sistemi dell'entità NIS e l'impatto di interruzioni del servizio.
Le misure AGID, come la misura A.X (Gestione dei Fornitori), toccano la gestione dei fornitori, ma non con la stessa profondità e specificità della NIS2, che estende la responsabilità dell'ente anche ai rischi derivanti da terze parti lungo l'intera catena di approvvigionamento. Una gestione inadeguata della supply chain può introdurre vulnerabilità significative che bypassano le difese interne, portando a incidenti di sicurezza anche se le misure interne sono robuste. La valutazione del rischio sui fornitori è direttamente collegata alla valutazione del rischio complessiva dell'organizzazione. Le organizzazioni dovranno implementare programmi di gestione del rischio dei fornitori completi, che includano due diligence approfondite, clausole contrattuali stringenti, audit periodici e monitoraggio continuo dei fornitori critici. Questo avrà un impatto significativo sui processi di procurement e sulla collaborazione con i partner.

Gestione degli Asset (ID.AM-01, ID.AM-02, ID.AM-03, ID.AM-04)

La NIS2 richiede il mantenimento di inventari aggiornati e approvati internamente di tutti i dispositivi fisici (hardware), inclusi IT, IoT, OT e dispositivi mobili. Similmente, devono essere gestiti inventari aggiornati di software, servizi e applicazioni (commerciali, open-source, personalizzate, accessibili via API). La direttiva estende questo requisito ai flussi di comunicazione di rete interni ed esterni e ai servizi forniti da terzi, inclusi i servizi cloud.

Le misure AGID, in particolare la misura A.1 (Inventario degli asset hardware e software), e i requisiti ABSC 1 (Inventario dei dispositivi autorizzati e non autorizzati) e ABSC 2 (Inventario dei software autorizzati e non autorizzati) , prevedono la gestione degli asset, ma la NIS2 è più esplicita sull'inclusione di IoT, OT, dispositivi mobili e servizi cloud, riflettendo l'attuale panorama tecnologico. Un inventario degli asset accurato è la base per una gestione efficace del rischio, della vulnerabilità, della configurazione e del monitoraggio. Senza sapere cosa si possiede e dove si trova è impossibile proteggerlo efficacemente.

Le organizzazioni dovranno adottare strumenti e processi per la discovery e la gestione automatizzata degli asset, specialmente in ambienti complessi con OT/IoT e multi-cloud, per mantenere inventari precisi e aggiornati.

Gestione delle Vulnerabilità (ID.RA-01, ID.RA-08)

La NIS2 richiede l'identificazione periodica delle vulnerabilità nei sistemi informativi e di rete, anche attraverso attività come vulnerability assessment e penetration test, documentando i risultati. La direttiva impone anche l'istituzione di processi per ricevere, analizzare e rispondere alle divulgazioni di vulnerabilità, monitorando i canali di comunicazione di CSIRT Italia, CERT settoriali, ISAC e canali dei fornitori di software critici. Le vulnerabilità devono essere risolte tempestivamente tramite aggiornamenti o misure di mitigazione, o accettando il rischio in conformità con il piano di trattamento del rischio (ID.RA-06). Un piano di gestione delle vulnerabilità deve essere definito, implementato e approvato dal vertice.

Le misure AGID, in particolare la misura A.3 (Gestione delle vulnerabilità) e i requisiti di ABSC 4 (Valutazione e correzione continua della vulnerabilità), come ABSC 4.1.1, ABSC 4.1.2 (ricerca delle vulnerabilità), ABSC 4.4.2 (registrazione a servizi di informazioni sulle minacce), ABSC 4.5.1 (installazione automatica delle patch), ABSC 4.7.1 (verifica risoluzione vulnerabilità), ABSC 4.8.1 (piano di gestione dei rischi), ABSC 4.8.2 (priorità risoluzione vulnerabilità) e ABSC 4.9.1 (misure alternative), prevedono la gestione delle vulnerabilità e l'applicazione di patch. NIS2 enfatizza il monitoraggio proattivo delle fonti di informazione sulle vulnerabilità e la formalizzazione di un piano di gestione. Il monitoraggio attivo delle fonti di vulnerabilità e l'esecuzione di test sono essenziali per identificare e risolvere le vulnerabilità prima che possano essere sfruttate, riducendo la superficie di attacco e prevenendo incidenti.

La tempestiva risoluzione delle vulnerabilità è una misura di trattamento del rischio. Le organizzazioni dovranno investire in strumenti di vulnerability management, team dedicati alla sicurezza applicativa e infrastrutturale, e stabilire relazioni formali con CSIRT Italia e i fornitori per ricevere tempestivamente avvisi sulle vulnerabilità.

Continuità Operativa, Ripristino in Caso di Disastro e Gestione delle Crisi (ID.IM-04)

La NIS2 consolida i requisiti per la resilienza operativa, richiedendo piani documentati, implementati, aggiornati e approvati dagli organi amministrativi ed esecutivi per la continuità operativa, il disaster recovery e la gestione delle crisi. Questi piani devono definire scopo, ruoli, responsabilità, contatti, canali di comunicazione, condizioni di attivazione/disattivazione, risorse necessarie (inclusi backup e ridondanze), ordine di recupero e procedure specifiche. I piani devono essere rivisti periodicamente (almeno ogni due anni) e in caso di incidenti significativi o cambiamenti nelle minacce.

Le misure AGID, in particolare la misura A.6 (Backup e ripristino dei dati e della configurazione) e i requisiti di ABSC 10 (Copie di sicurezza), nonché la misura A.12 (Gestione della continuità operativa), hanno requisiti per la business continuity e il disaster recovery. NIS2 consolida questi aspetti e aggiunge esplicitamente la "gestione delle crisi", con un focus sulla comunicazione e il coordinamento con le autorità. Piani di continuità di business e di disaster recovery robusti sono direttamente collegati alla capacità di recupero da un incidente e alla minimizzazione dell'impatto sui servizi. Un piano di gestione delle crisi garantisce che la risposta a un incidente sia coordinata e che le comunicazioni siano gestite efficacemente. Le organizzazioni dovranno condurre esercitazioni regolari sui piani di continuità, disaster recovery e crisi, coinvolgendo non solo il personale tecnico ma anche la direzione e le funzioni di comunicazione, per testare l'efficacia e identificare aree di miglioramento.

Gestione dell'Autenticazione, delle Identità Digitali e del Controllo Accessi (PR.AA-01, PR.AA-03, PR.AA-05, PR.IR-01)

La NIS2 richiede che le identità e le credenziali degli utenti autorizzati, dei servizi e dell'hardware siano gestite dall'organizzazione. Questo include la registrazione e l'approvazione degli account utente (individuali ove possibile), la robustezza e l'aggiornamento delle credenziali, e la verifica periodica degli account e delle autorizzazioni. I metodi di autenticazione devono essere proporzionati al rischio, con l'impiego obbligatorio di autenticazione a più fattori (MFA) per i sistemi rilevanti. La direttiva impone l'applicazione dei principi del minimo privilegio e della separazione dei compiti nell'assegnazione dei permessi, garantendo la distinzione tra account con e senza privilegi amministrativi. Infine, le reti e gli ambienti devono essere protetti da accessi logici non autorizzati, con la definizione di attività remote consentite, il mantenimento di un elenco di sistemi accessibili da remoto e la presenza e configurazione di sistemi perimetrali come i firewall.

Le misure AGID, in particolare la misura A.4 (Gestione degli accessi) e i requisiti di ABSC 5 (Uso appropriato dei privilegi di amministratore), come ABSC 5.1.1, ABSC 5.1.2, ABSC 5.1.3 (limitazione e uso dei privilegi), ABSC 5.2.1 (inventario utenze amministrative), ABSC 5.6.1 (autenticazione a più fattori), ABSC 5.7.1, ABSC 5.7.2, ABSC 5.7.3, ABSC 5.7.4 (robustezza e gestione credenziali), ABSC 5.8.1 (accesso indiretto con utenze normali), ABSC 5.9.1 (macchine dedicate per operazioni privilegiate), ABSC 5.10.1, ABSC 5.10.2, ABSC 5.10.3 (distinzione e nominatività utenze), ABSC 5.11.1, ABSC 5.11.2 (conservazione credenziali), coprono ampiamente l'autenticazione e il controllo accessi. NIS2 rafforza l'obbligo di MFA per sistemi rilevanti e la distinzione tra account amministrativi e utente. Una gestione debole delle identità e degli accessi è una delle principali cause di violazioni. L'implementazione di MFA riduce drasticamente il rischio di compromissione degli account, mentre

il principio del minimo privilegio limita il potenziale danno in caso di compromissione. La protezione degli accessi remoti è fondamentale per prevenire accessi non autorizzati alla rete. Le organizzazioni dovranno implementare soluzioni di Identity and Access Management (IAM) robuste, condurre audit regolari sugli accessi e sui privilegi, e rafforzare la formazione del personale sull'importanza delle credenziali e delle pratiche di accesso sicuro.

Sicurezza Fisica (PR.AA-06)

La NIS2 richiede che l'accesso fisico agli asset sia gestito, monitorato e applicato in modo appropriato al rischio. Questo include la protezione dell'accesso fisico per almeno i sistemi informativi e di rete rilevanti, con procedure documentate.
Le misure AGID, in particolare la misura A.9 (Sicurezza fisica degli ambienti e delle infrastrutture), includono requisiti di sicurezza fisica. NIS2 li riafferma, sottolineando la necessità di proporzionalità al rischio. Una sicurezza fisica inadeguata può compromettere direttamente la disponibilità, integrità e riservatezza dei sistemi informativi, rendendo vane le misure di sicurezza logica. Ad esempio l'accesso non autorizzato a un server può portare alla compromissione dei dati o all'interruzione del servizio. Le organizzazioni dovranno condurre valutazioni del rischio fisico e implementare controlli (es. videosorveglianza, controllo accessi, allarmi) che siano integrati con la strategia di sicurezza informatica.

Formazione del Personale e Consapevolezza (PR.AT-01, PR.AT-02)

La NIS2 richiede la definizione, implementazione e documentazione di un piano di formazione sulla cybersecurity per tutto il personale, inclusi gli organi amministrativi ed esecutivi. Questo piano deve includere la pianificazione delle attività formative, l'indicazione dei contenuti e i metodi di verifica dell'acquisizione dei contenuti. Inoltre il piano deve prevedere una formazione dedicata per il personale in ruoli specializzati, come gli amministratori di sistema, coprendo istruzioni per la configurazione e il funzionamento sicuro dei sistemi, informazioni sulle minacce cibernetiche note e istruzioni sul comportamento in caso di eventi di sicurezza rilevanti.
Le misure AGID, in particolare la misura A.11 (Formazione e consapevolezza del personale), prevedono formazione e consapevolezza. NIS2 enfatizza l'inclusione del top management e la formazione specifica per ruoli tecnici, riconoscendo l'importanza di una cultura della sicurezza a tutti i livelli. Una formazione e consapevolezza inadeguata è una causa comune di incidenti, come attacchi di phishing o errori di configurazione. Un personale ben formato è meno propenso a cadere in trappole e più capace di reagire correttamente agli eventi di sicurezza, riducendo l'impatto degli incidenti. Le organizzazioni dovranno sviluppare programmi di formazione continua e mirata, che vadano oltre la semplice awareness per includere competenze pratiche e specifiche per i diversi ruoli, e misurare l'efficacia di tali programmi.

Sicurezza dei Dati (PR.DS-01, PR.DS-02, PR.DS-11)

La NIS2 impone la protezione della riservatezza, integrità e disponibilità dei dati. Per i dati a riposo, richiede la crittografia con protocolli e algoritmi all'avanguardia e sicuri per i dati memorizzati su dispositivi portatili e supporti rimovibili, e la disabilitazione dell'auto-esecuzione dei supporti rimovibili

con scansione per codice malevolo. Per i dati in transito, è richiesto l'uso di protocolli e algoritmi di crittografia all'avanguardia e sicuri per la trasmissione da e verso l'esterno dell'entità NIS. La direttiva sottolinea inoltre l'importanza dei backup dei dati e della configurazione, che devono essere eseguiti periodicamente, includere copie offline, garantire riservatezza e integrità (tramite protezione fisica o crittografia) e essere verificati regolarmente tramite test di ripristino.
Le misure AGID, in particolare la misura A.6 (Backup e ripristino dei dati e della configurazione) e i requisiti di ABSC 10 (Copie di sicurezza), come ABSC 10.3.1 (riservatezza delle informazioni nelle copie di sicurezza), e la misura ABSC 13 (Protezione dei dati), come ABSC 13.1.1 (analisi dei dati per individuare quelli con particolari requisiti di riservatezza) e ABSC 13.2.1 (utilizzo di sistemi di cifratura per i dispositivi portatili), coprono la protezione dei dati e i backup. NIS2 specifica l'uso di "protocolli e algoritmi all'avanguardia e sicuri" per la crittografia e l'importanza dei backup offline e dei test di ripristino. La crittografia dei dati riduce l'impatto di una violazione, proteggendo la riservatezza. I backup sono fondamentali per il ripristino in caso di disastro o incidente, garantendo la disponibilità dei dati. La verifica periodica dei backup è cruciale per assicurare che il processo di recupero sia effettivamente funzionante. Le organizzazioni dovranno rivedere le proprie politiche di crittografia, aggiornare le tecnologie utilizzate e implementare una strategia di backup robusta con test di ripristino regolari e documentati.

Sviluppo, Configurazione, Manutenzione e Dismissione dei Sistemi Informativi e di Rete (PR.PS-01, PR.PS-02, PR.PS-03, PR.PS-04, PR.PS-06)

La NIS2 richiede l'adozione e la documentazione di pratiche di gestione della configurazione, inclusa la definizione di configurazioni di riferimento sicure ("hardened") per i sistemi informativi e di rete rilevanti. Per la manutenzione del software, è richiesto di installare solo software con aggiornamenti di sicurezza garantiti e di applicare tempestivamente gli ultimi aggiornamenti rilasciati dal produttore, verificando gli aggiornamenti critici in un ambiente di test prima del deployment in produzione. Per l'hardware, sono necessarie procedure per il trasferimento fisico e la dismissione sicura dei dispositivi di archiviazione dati, e il mantenimento di log di manutenzione. La direttiva impone anche la generazione e la disponibilità di record di log per il monitoraggio continuo, con logging di tutti gli accessi remoti e degli account con privilegi amministrativi, archiviazione sicura dei log e definizione dei periodi di conservazione. Infine, la NIS2 introduce esplicitamente la necessità di adottare e documentare pratiche di sviluppo sicuro del software.
Le misure AGID, in particolare la misura A.2 (Configurazione di sicurezza - hardening) e i requisiti di ABSC 3 (Proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server), come ABSC 3.1.1, ABSC 3.1.2 (configurazioni sicure standard), ABSC 3.2.1, ABSC 3.2.2, ABSC 3.2.3 (configurazione standard e gestione modifiche), ABSC 3.5.1, ABSC 3.5.2, ABSC 3.5.3, ABSC 3.5.4 (verifica integrità file e cronologia modifiche), ABSC 3.6.1 (controllo automatico configurazioni), ABSC 3.7.1 (ripristino configurazioni standard), coprono la gestione delle configurazioni, la manutenzione e il logging. Anche la misura A.7 (Gestione dei log), con requisiti come ABSC 5.1.4, ABSC 5.4.1, ABSC 5.4.2, ABSC 5.4.3, ABSC 5.5.1 per il logging delle azioni amministrative, è correlata. NIS2 introduce esplicitamente lo sviluppo sicuro del software (Security by Design/Default) e det-

taglia i requisiti di logging e aggiornamento. Le configurazioni sicure e gli aggiornamenti tempestivi riducono le vulnerabilità sfruttabili. Il logging è essenziale per il monitoraggio degli eventi di sicurezza e per l'analisi forense in caso di incidente. Lo sviluppo sicuro del software previene l'introduzione di vulnerabilità sin dalle prime fasi del ciclo di vita. Le organizzazioni dovranno implementare pipeline di sviluppo e deployment sicure (DevSecOps), adottare strumenti di gestione delle configurazioni, e centralizzare la raccolta e l'analisi dei log per migliorare la visibilità e la capacità di rilevamento.

Protezione delle Reti e delle Comunicazioni (PR.IR-03)

La NIS2 richiede l'implementazione di meccanismi per soddisfare i requisiti di resilienza in situazioni normali e avverse, in particolare l'uso di sistemi di comunicazione di emergenza protetti, in linea con la valutazione del rischio (ID.RA-05).
Le misure AGID, in particolare la misura A.8 (Protezione delle comunicazioni) e i requisiti di ABSC 8.5.1 (Usare strumenti di filtraggio che operano sull'intero flusso del traffico di rete), ABSC 8.9.1 (Filtrare il contenuto dei messaggi di posta), ABSC 8.9.2 (Filtrare il contenuto del traffico web), ABSC 8.9.3 (Bloccare nella posta elettronica e nel traffico web i file la cui tipologia non è strettamente necessaria), e ABSC 3.4.1 (Eseguire tutte le operazioni di amministrazione remota per mezzo di connessioni protette), includono la protezione delle reti. NIS2 si concentra specificamente sulla resilienza delle comunicazioni di emergenza. La disponibilità di sistemi di comunicazione di emergenza protetti è cruciale per l'efficace gestione delle crisi e la notifica degli incidenti, specialmente in scenari in cui le comunicazioni primarie sono compromesse. Le organizzazioni dovranno identificare e implementare soluzioni di comunicazione alternative e sicure per la gestione delle crisi, testandole regolarmente nell'ambito degli esercizi di continuità operativa.

Monitoraggio degli Eventi di Sicurezza (DE.CM-01, DE.CM-09)

La NIS2 richiede la presenza di strumenti tecnici aggiornati e configurati per rilevare tempestivamente incidenti significativi. Impone la definizione di livelli di servizio (SLA) per i servizi dell'entità NIS per facilitare il rilevamento degli incidenti. Sono richiesti strumenti di analisi e filtraggio del traffico in entrata (inclusa la posta elettronica), e il monitoraggio di accessi remoti, attività dei sistemi perimetrali, eventi amministrativi significativi e accessi riusciti o falliti a risorse di rete, workstation e applicazioni. Devono essere definiti e monitorati parametri qualitativi e quantitativi per rilevare accessi non autorizzati o abusi di privilegi. Inoltre, sono richiesti sistemi di protezione delle workstation per il rilevamento di codice malevolo.
Le misure AGID, in particolare la misura A.7 (Gestione dei log) e i requisiti di ABSC 8.1.3 (Gli eventi rilevati dagli strumenti sono inviati ad un repository centrale), ABSC 8.5.1 (Usare strumenti di filtraggio che operano sull'intero flusso del traffico di rete), ABSC 8.6.1 (Monitorare, analizzare ed eventualmente bloccare gli accessi a indirizzi che abbiano una cattiva reputazione), ABSC 8.10.1 (Utilizzare strumenti anti-malware che sfruttino tecniche di rilevazione basate sulle anomalie di comportamento), e i requisiti di logging/monitoraggio delle azioni amministrative come ABSC 5.1.4, ABSC 5.4.1, ABSC 5.4.2, ABSC 5.4.3, ABSC 5.5.1, prevedono il monitoraggio.
NIS2 è più dettagliata sui tipi di eventi da monitorare, sull'uso di strumenti specifici (es. filtraggio

email) e sulla definizione di parametri qualitativi/quantitativi per il rilevamento di anomalie. Un monitoraggio efficace è il prerequisito per un rilevamento tempestivo degli incidenti, che a sua volta è essenziale per una risposta rapida e una minimizzazione del danno. La capacità di rilevare accessi non autorizzati o abusi di privilegi è direttamente collegata all'efficacia dei controlli di accesso. Le organizzazioni dovranno investire in soluzioni SIEM/SOAR, EDR/XDR, e team di Security Operations Center (SOC) per analizzare i log e gli eventi di sicurezza in tempo reale, sviluppando regole di correlazione e indicatori di compromissione.

Risposta agli Incidenti e Ripristino (RS.MA-01, RS.CO-02, RC.RP-01, RC.CO-03)

La NIS2 richiede un piano di gestione e notifica degli incidenti di cybersecurity al CSIRT Italia, che deve essere definito, implementato, aggiornato e documentato, in conformità con l'articolo 25 del decreto NIS. Questo piano deve includere fasi e procedure per la gestione e notifica degli incidenti, ruoli e responsabilità, informazioni di contatto per la segnalazione, metodi di comunicazione interni ed esterni (incluso il coinvolgimento degli organi amministrativi ed esecutivi) e modelli di reportistica. Il piano deve essere approvato dal vertice e rivisto periodicamente (almeno ogni due anni) o in caso di incidenti significativi. La direttiva impone procedure documentate per comunicare senza indebito ritardo incidenti significativi ai destinatari del servizio e, se ordinato dall'Agenzia per la Cybersicurezza Nazionale, anche al pubblico. Infine, il piano di gestione degli incidenti deve includere procedure per il ripristino delle operazioni dei sistemi informativi e di rete coinvolti, con comunicazione delle attività di recupero alle parti interessate interne.
Le misure AGID, in particolare la misura A.10 (Gestione degli incidenti di sicurezza) e il requisito ABSC 8.11.1 (Implementare una procedura di risposta agli incidenti che preveda la trasmissione al provider di sicurezza dei campioni di software sospetto), prevedono la gestione degli incident.

Conclusioni rispetto al superamento delle misure AGID rispetto alle misure proposte da ACN

In attesa di chiarimenti più formali o espliciti da parte di AGID è ragionevole ritenere che, se un'organizzazione rispetta pienamente le misure di sicurezza per i soggetti essenziali della NIS2, è molto probabile che stia già rispettando o addirittura superando le misure di sicurezza ICT di AGID.
Ecco perché:

- l'interpretazione di ACN della NIS2 è più ampia e prescrittiva: introduce requisiti più stringenti e dettagliati rispetto alle Misure Minime AGID. NIS2 non contraddice le misure AGID, ma piuttosto le integra e le espande, elevando il livello di sicurezza richiesto.
  - Ad esempio, mentre AGID A.1 (Inventario degli asset hardware e software) richiede un inventario, NIS2 con ID.AM-01, ID.AM-02, ID.AM-03, ID.AM-04 è più esplicita nel includere categorie specifiche come IoT, OT, dispositivi mobili e servizi cloud, riflettendo l'attuale panorama tecnologico.
  - Similmente, per la gestione delle vulnerabilità, AGID A.3 (Gestione delle vulnerabilità) e i suoi ABSC_ID correlati come ABSC 4.1.1 e ABSC 4.4.2 richiedono la ricerca e l'aggiornamento, ma NIS2 con ID.RA-01 e ID.RA-08 enfatizza ulteriormente il monitoraggio proattivo di fonti specifiche (come CSIRT Italia e canali dei fornitori critici) e la formalizzazione di un piano di gestione delle vulnerabilità.

- Nuove Aree di Copertura: NIS2 introduce ambiti che non erano così dettagliati o esplicitamente richiesti dalle misure AGID, come la gestione del rischio della catena di approvvigionamento.
  - La categoria NIS2 GV.SC-01, GV.SC-02, GV.SC-04, GV.SC-05, GV.SC-07 sulla "Gestione dei rischi per la sicurezza informatica della catena di approvvigionamento" è un'area significativa e nuova, con requisiti molto più stringenti sulla due diligence dei fornitori e l'estensione dei controlli di sicurezza a terze parti. Le misure AGID toccano la gestione dei fornitori, ma non con la stessa profondità e specificità.
- Maggiore Formalizzazione e Responsabilità del Vertice: NIS2 richiede una maggiore formalizzazione dei processi e un coinvolgimento esplicito degli organi amministrativi ed esecutivi.
  - Per la "Gestione del Rischio" (NIS2 GV.OC-04, GV.RM-03, ID.RA-05, ID.RA-06), NIS2 richiede che il piano di gestione del rischio e l'accettazione dei rischi residui siano approvati dagli organi amministrativi ed esecutivi. Questo eleva la cybersecurity a un livello strategico, un aspetto meno esplicitamente dettagliato nelle misure AGID, sebbene AGID richieda la definizione di un piano di gestione dei rischi (es. ABSC 4.8.1).
  - Anche per la "Formazione del Personale e Consapevolezza" (NIS2 PR.AT-01, PR.AT-02), NIS2 enfatizza l'inclusione del top management nella formazione, un dettaglio che va oltre la generica "Formazione e consapevolezza del personale" di AGID A.11.

In sintesi, le misure NIS2 sono progettate per fornire un quadro di sicurezza più robusto e completo, che include e rafforza i principi già presenti nelle misure AGID. Pertanto, un'organizzazione che si conforma alla NIS2 avrà già implementato la maggior parte, se non tutte, le misure AGID, e in molti casi con un livello di dettaglio e rigore superiore.
Tuttavia, fino al precitato chiarimento da parte del legislatore, la scelta di abbandonare le misure AGID ed adottare esclusivamente le misure NIS2 è demandata al titolare ed agli organi direttivi dell'azienda.

REGOLAMENTO (UE) 2025/327 EHDS e D.M. 31 dicembre 2024 EDS: il prossimo futuro e la NIS2

L'EUROPEAN HEALTH DATA SPACE (EHDS)

L'EHDS è entrato in vigore il 26 marzo 2025. La sua timeline di efficacia è complessa e suddivisa in quattro periodi chiave:

- 2025-2027 (Preparazione Tecnica e Normativa): La Commissione UE adotterà 13 atti implementativi critici, inclusi gli standard tecnici per l'interoperabilità e i requisiti per i sistemi EHR. L'Italia dovrà modificare il Decreto Ecosistema Dati Sanitari (EDS) per allinearlo alle specifiche EHDS, integrare l'infrastruttura nazionale con MyHealth@EU e avviare programmi di formazione per i professionisti sanitari.
- 2027-2029: Implementazione delle infrastrutture nazionali e cross-border, con testing delle piattaforme MyHealth@EU e HealthData@EU.
- 2029-2031: Entrata in vigore delle regole per l'uso primario (summary paziente, ePrescription) e secondario (dati da cartelle cliniche) dei dati.
- 2031-2034: Completa integrazione delle categorie dati complesse (imaging medico, dati genomici) e apertura a Paesi terzi.

L'European Health Data Space (EHDS) e la Direttiva NIS2 sono due normative europee che mirano a digitalizzare in modo sicuro il settore sanitario. L'EHDS si focalizza sulla creazione di uno spazio comune per i dati sanitari, mentre la NIS2 stabilisce requisiti di cybersicurezza per le infrastrutture critiche. Insieme, formano un robusto ecosistema normativo per la digitalizzazione sicura della sanità europea. La loro convergenza richiede un approccio integrato per evitare duplicazioni e massimizzare l'efficienza. Le organizzazioni sanitarie che adottano una strategia coordinata di conformità potranno beneficiare di maggiore efficienza operativa e migliore protezione dei dati.
Dall'analisi normativa emerge un solo punto di contatto inerente la gestione del rischio cyber: mentre per la NIS2 le entità essenziali e importanti devono adottare le misure previste dall'Articolo 21 di NIS2 l'EHDS richiede standard di sicurezza specifici per i sistemi EHR.

ECOSISTEMA DEI DATI SANITARI (EDS)

Il Decreto del Ministero della Salute del 31 dicembre 2024, pubblicato in Gazzetta Ufficiale il 5 marzo 2025, istituisce l'Ecosistema dei Dati Sanitari (EDS), una piattaforma innovativa che sarà pienamente operativa entro il 2026, in linea con le scadenze della Missione 6 Salute del Piano Nazionale di Ripresa e Resilienza. L'EDS rappresenta uno dei più ambiziosi progetti di digitalizzazione mai avviati dal Ministero della Salute italiano, sviluppato in collaborazione con il MEF e il Dipartimento per la trasformazione digitale, e realizzato grazie al dialogo costruttivo con il Garante per la protezione dei dati personali e l'Agenzia per la cybersicurezza nazionale.
Questa piattaforma è uno strumento strategico per la raccolta e l'analisi dei dati sanitari, con finalità che spaziano dalla prevenzione, diagnosi, cura e riabilitazione, fino alla ricerca scientifica e alla programmazione sanitaria. Il sistema, alimentato principalmente dalle informazioni del Fascicolo Sanitario Elettronico (FSE), ha l'obiettivo di garantire maggiore uniformità delle prestazioni e universalità dell'offerta assistenziale su tutto il territorio nazionale. L'architettura dell'EDS è stata progettata per garantire la separazione dei dati in chiaro, pseudonimizzati e anonimizzati, assicurando al contempo la piena interoperabilità delle diverse unità di archiviazione regionali.
Dall'analisi normativa non sono emersi particolari punti di contatto e l'implementazione delle due normative potrà proseguire simultaneamente.
L'implementazione simultanea di EDS e NIS2 crea un ecosistema normativo dove la sicurezza dei dati sanitari deve essere considerata sotto più profili. L'EDS implementa tecniche avanzate di pseudonimizzazione e anonimizzazione, mentre la NIS2 richiede l'adozione di politiche di sicurezza informatica che includono crittografia, controllo degli accessi e gestione delle vulnerabilità.

Organizzazione, processi e procedure

Premessa

Il settore sanitario si trova oggi al centro di una trasformazione digitale senza precedenti, dove la tecnologia rappresenta contemporaneamente la chiave per l'innovazione e il principale vettore di vulnerabilità.
In questo contesto la Direttiva NIS2 dell'Unione Europea non costituisce semplicemente un ulteriore adempimento normativo, ma si configura come un cambio di paradigma fondamentale per la protezione delle infrastrutture critiche europee.
Tuttavia non basta imporre normative nuove o maggiormente stringenti (specie rispetto alla prima direttiva NIS) per ottenere un ampio consenso di conformità o per coagulare un maggior numero di consapevoli al tavolo della compliance normativa. Di questo stato delle cose ve ne è dimostrazione proprio adesso, col decreto di recepimento della Direttiva ed il successivo marasma interpretativo, normativo (tra fonti primarie, secondarie e terziarie) e applicativo.
Un'eccessiva ipertrofia normativa, come sembra essere recentemente quella dell'Unione europea, se accompagnata ad un non ben chiaro quadro di competenze e di operatività (come nel caso dell'Italia) e ad un continuo gettito di normativa stratificata e sovrapponibile (vedasi gli ultimi DPCM a completamento dell'architettura della l. 90/2024, insieme a tutto il resto della produzione legislativa post NIS 2), non fa altro che complicare lo scenario per la conformità.
Da questo "canovaccio" si è volutamente lasciata fuori l'Autorità Nazionale per la Cybersicurezza per non complicare ulteriormente il quadro già complicato.
L'ambito sanitario, per sua natura depositario di dati sensibili e servizi essenziali per la collettività, è chiamato a confrontarsi con sfide di cybersecurity di complessità crescente. Attacchi ransomware, violazioni di dati personali e interruzioni dei servizi digitali hanno dimostrato quanto sia fragile l'equilibrio tra innovazione tecnologica e sicurezza informatica. La pandemia ha inoltre accelerato l'adozione di soluzioni digitali, creando nuove superfici di attacco che richiedono una protezione strutturata e sistematica.
Le piccole e medie imprese del settore sanitario si trovano in una posizione particolarmente delicata. Da un lato, devono garantire gli stessi standard di sicurezza delle grandi organizzazioni; dall'altro spesso non dispongono delle risorse economiche e delle competenze specialistiche necessarie per implementare misure di cybersecurity adeguate. Questa disparità crea un ecosistema di sicurezza disomogeneo, dove il livello di protezione dell'intera filiera è determinato dall'anello più debole.
Le grandi aziende sanitarie, pur disponendo di maggiori risorse, affrontano sfide di scala e complessità: la gestione di infrastrutture IT eterogenee, l'integrazione di sistemi legacy con tecnologie moderne e la necessità di mantenere la continuità operativa mentre si implementano nuove misure di sicurezza, rappresentano sfide organizzative e tecniche di notevole portata.

La conformità alla Direttiva NIS2 richiede pertanto un approccio olistico che vada oltre la mera implementazione di soluzioni tecniche. È necessario un cambio di rotta culturale che ponga la cybersecurity al centro della strategia aziendale, non più come costo accessorio ma come investimento strategico per la sostenibilità del business e la tutela dei pazienti.
Ci proponiamo di guidare operatori sanitari, management aziendale e professionisti IT attraverso le complessità della conformità NIS2, offrendo strumenti pratici e metodologie operative, calate in un linguaggio semplice, per trasformare gli obblighi normativi in opportunità di crescita e rafforzamento della propria postura di sicurezza.

L'importanza della Supply Chain nel contesto sanitario

INTRODUZIONE

Nel contesto sanitario i fornitori esterni di servizi ICT (ma più in generale tutti i fornitori) costituiscono un elemento strutturale nell'erogazione dei servizi digitali. Il loro coinvolgimento non si limita alla fornitura di soluzioni applicative, ma si estende all'intera filiera tecnologica, includendo infrastrutture, ambienti cloud, connettività, gestione sistemistica, assistenza tecnica e servizi operativi continuativi. In numerosi casi la responsabilità diretta su componenti critiche per la continuità assistenziale e la protezione dei dati personali è demandata a questi operatori, con implicazioni rilevanti in termini di rischio e conformità. La Direttiva NIS2 sottolinea con forza la necessità di un approccio rigoroso e sistematico alla gestione dei rischi legati alla supply chain. In particolare, richiede di presidiare con attenzione la protezione dei dati e delle informazioni, la resilienza operativa e la capacità dell'organizzazione di dimostrare accountability nei confronti dei cittadini e delle autorità.
In questo contesto, la gestione della supply chain ICT non può essere confinata all'ambito del procurement o della compliance contrattuale. Deve invece rappresentare un processo integrato, che coinvolga attivamente tutte le funzioni chiave: Sicurezza delle informazioni, Data Protection, Risk Management, Direzione Sanitaria e Governance complessiva.
L'approccio proposto si propone di supportare concretamente le organizzazioni sanitarie nell'adozione di pratiche efficaci di gestione della supply chain, in coerenza con i principi della Direttiva NIS2 anche per le casistiche che prevedano il coinvolgimento di fornitori che non sono tenuti, per la loro natura, ad essere conformi alla direttiva stessa.

OBIETTIVI DELLA GESTIONE DEI FORNITORI IN AMBITO NIS2

L'obiettivo principale è garantire che i fornitori ICT siano scelti, qualificati e monitorati in modo da assicurare la protezione dei servizi essenziali e dei dati personali, lungo tutto il ciclo di vita della fornitura. In parallelo, è essenziale che i rischi derivanti da terze parti siano compresi, valutati e mitigati in modo sistematico, e che le responsabilità in tema di cybersecurity e protezione dei dati siano chiaramente attribuite e tracciabili.
Infine, un obiettivo trasversale riguarda la promozione di una cultura della sicurezza lungo tutta la catena di fornitura. Questo significa condividere con i fornitori linee guida e requisiti chiari, stabilire

meccanismi di controllo efficaci e sviluppare con loro un rapporto di collaborazione responsabile, basato su trasparenza e impegno reciproco. Tale cultura della sicurezza dovrà estendersi anche agli eventuali subfornitori, coinvolgendo l'intera filiera nella gestione consapevole dei rischi. Per questi soggetti, sarà responsabilità del fornitore principale garantire il rispetto dei requisiti di sicurezza stabiliti, anche attraverso obblighi contrattuali e controlli equivalenti. Qualora il subfornitore sia coinvolto in attività critiche o nel trattamento di dati sensibili, l'organizzazione sanitaria potrà richiedere che venga sottoposto a una qualificazione equivalente a quella prevista per i fornitori diretti.

MODELLO OPERATIVO PROPOSTO

Il modello proposto per la gestione della supply chain ICT si articola in tre fasi integrate in una procedura aziendale formalizzata.

Qualificazione iniziale

La qualificazione iniziale rappresenta il primo livello di controllo e verifica della solidità e dell'affidabilità di un fornitore. L'obiettivo è assicurarsi che ogni fornitore, prima di essere integrato nella supply chain ICT di un'organizzazione sanitaria, possegga i requisiti minimi in termini di sicurezza, conformità normativa e capacità di gestione del rischio.

Questa fase prevede attività quali: la raccolta e analisi di certificazioni rilevanti (a titolo esemplificativo e non esaustivo: ISO 27001, ISO 9001, GDPR compliance, qualificazione ACN ove applicabile), la compilazione di questionari specifici su sicurezza, business continuity e data protection, e l'eventuale conduzione di audit. La due diligence deve includere anche aspetti etici, legali e di governance.

A supporto della qualificazione è utile impiegare griglie di valutazione ponderata, che permettono di valutare in modo strutturato i diversi aspetti della fornitura, assegnando pesi specifici ai criteri tecnici, organizzativi e normativi.

Per rafforzare la coerenza e l'efficacia del processo di qualificazione, l'organizzazione dovrebbe definire e rendere accessibili in modo trasparente i requisiti minimi di sicurezza attesi dai propri fornitori. Questi requisiti dovrebbero costituire un riferimento stabile e riconoscibile per tutti gli operatori interessati a collaborare con l'ente, indipendentemente dalla modalità di acquisizione. In funzione delle specificità di ciascuna fornitura, tali requisiti potranno poi essere integrati con vincoli aggiuntivi nei capitolati tecnici delle singole procedure di gara.

A tale scopo, può essere adottato o adattato il questionario di CLUSIT (Associazione Italiana per la Sicurezza Informatica) per la sicurezza dei fornitori[2] che rappresenta una base metodologica aperta e condivisa per esprimere le aspettative minime in materia di cybersecurity.

Nel contesto di una gara, le attività di qualificazione iniziale possono essere incluse tra i requisiti di ammissione o di capacità tecnica, oppure essere avviate dopo l'aggiudicazione, prima della stipula del contratto e dell'avvio operativo. In entrambi i casi, è fondamentale che la valutazione dell'idoneità del fornitore preceda l'erogazione del servizio e consenta di applicare un livello di controllo proporzionato al rischio.

[2] Disponibile sul sito di CLUSIT: https://clusit.it/blog/questionario-per-la-sicurezza-dei-fornitori-versione-2

È importante raccogliere già in questa fase le informazioni utili alla successiva classificazione del rischio, così da impostare da subito un livello di controllo proporzionato e un percorso coerente di monitoraggio.

Valutazione del rischio associato

Dopo la qualifica iniziale, è necessario valutare in maniera approfondita il rischio specifico che ogni fornitore comporta in relazione ai servizi offerti. La valutazione del rischio deve andare oltre la semplice verifica formale e tenere conto di fattori concreti legati al contesto operativo.
Tra gli elementi da considerare: la natura e sensibilità dei dati trattati, l'accesso a sistemi critici, il grado di dipendenza operativa, la localizzazione geografica del trattamento dei dati e l'eventuale presenza di subfornitori.
A supporto della valutazione si possono utilizzare strumenti quali:

- Scorecard di rischio, che consente di sintetizzare e rappresentare in modo strutturato il profilo di rischio operativo e cyber del fornitore, integrando informazioni provenienti da fonti interne ed esterne.
- Modelli TPRM (Third-Party Risk Management), che assicurano un approccio sistematico alla gestione dei rischi di terze parti, includendo processi di identificazione, valutazione, trattamento e monitoraggio dei rischi lungo l'intero ciclo di vita del rapporto contrattuale.
- Simulazioni tabletop, che permettono di validare congiuntamente la capacità di risposta a incidenti critici da parte del fornitore e dell'organizzazione sanitaria, attraverso l'esercizio di scenari realistici di crisi.

L'obiettivo è attuare una gestione differenziata, proporzionando obblighi, controlli e monitoraggio al livello di rischio individuato.

QUALIFICA DINAMICA (MONITORAGGIO CONTINUO)

Una gestione efficace della supply chain richiede che l'intero ciclo di vita del rapporto con i fornitori sia sottoposto a controllo dinamico. La qualifica dinamica permette di rilevare tempestivamente cambiamenti nel profilo di rischio del fornitore e di attivare azioni correttive o preventive.
Eventi quali incidenti di sicurezza, modifiche societarie, cambiamenti contrattuali, variazioni nella localizzazione del trattamento dati o l'introduzione di subfornitori devono essere considerati fattori scatenanti per la rivalutazione del rischio.
Le attività chiave includono:

- monitoraggio attivo delle notifiche e degli incidenti;
- audit periodici sui fornitori ad alto rischio;
- aggiornamento delle clausole contrattuali;
- validazione operativa attraverso esercitazioni tabletop.

L'organizzazione dovrebbe mantenere allineati i registri dei trattamenti, i registri dei rischi e i controlli documentali per assicurare tracciabilità e rendicontazione costante.
A supporto della qualifica dinamica, continuano a essere utilizzati e aggiornati gli strumenti introdotti nella fase di valutazione del rischio. La scorecard di rischio deve essere periodicamente rivista

e aggiornata sulla base delle nuove informazioni raccolte (audit, incidenti, risultati di strumenti di cybersecurity rating). Il Modello TPRM costituisce il framework metodologico di riferimento anche per la gestione continua, guidando il processo di rivalutazione e di definizione delle azioni correttive. Inoltre, le simulazioni tabletop permettono di validare periodicamente l'efficacia dei processi di gestione degli incidenti.
Questa logica di monitoraggio continuo è oggi un requisito esplicito della normativa, come ribadito dall'art. 24 del decreto di recepimento della Direttiva NIS2.
Questo approccio integrato consente di mantenere la supply chain ICT sotto controllo continuo, garantendo resilienza operativa, reattività in caso di eventi critici e piena conformità con la Direttiva NIS2.

PROCEDURA FORMALIZZATA

Il modello proposto dovrà essere tradotto in una procedura strutturata, che specifichi in modo chiaro:

- modalità operative, ruoli e responsabilità;
- frequenza e modalità di riesame;
- integrazione con registro dei trattamenti, risk register e piani di continuità operativa;
- modalità di tracciamento e reporting.

Peraltro l'articolo 24 del decreto di recepimento della Direttiva NIS2 richiama espressamente la necessità che ogni soggetto essenziale gestisca la sicurezza della propria catena di fornitura. Questo implica l'adozione obbligatoria di un processo formalizzato che, pur adattabile alle caratteristiche dell'organizzazione, deve comprendere almeno i seguenti elementi operativi:

- Definizione e documentazione del processo di gestione del rischio dei fornitori, integrato nel sistema di gestione della sicurezza aziendale.
- Coinvolgimento delle principali funzioni aziendali: Procurement, CISO, DPO, Legal, Risk Management, e per i servizi sanitari anche la Direzione Sanitaria, per una valutazione congiunta dei fornitori critici.
- Adozione di strumenti per la qualificazione, la valutazione e il monitoraggio dei fornitori, sia a livello documentale che operativo.

Oltre alle tradizionali metodologie (scorecard di rischio, griglie di valutazione ponderata, audit), è oggi possibile integrare strumenti automatici di valutazione della postura di sicurezza dei fornitori, anche per supportare la gestione di filiere complesse e di dimensioni estese.
Sul mercato esistono varie soluzioni in questo ambito: si possono ad esempio utilizzare servizi come Bitsight o Security Scorecard, che forniscono valutazioni esterne sulla sicurezza cyber dei fornitori. Un ulteriore esempio è il servizio my-score.is, sviluppato completamente in Italia, che consente una valutazione specifica della postura cyber delle PMI, spesso coinvolte nella supply chain delle organizzazioni sanitarie. Tali strumenti, classificabili come piattaforme di cybersecurity rating, supportano la valutazione iniziale e il monitoraggio dinamico, integrando il processo interno con indicatori esterni aggiornati sulla postura di sicurezza dei fornitori. Per orientarsi tra le soluzioni disponibili, può risultare utile consultare la pubblicazione Supply Chain Security promossa da CLUSIT[3] che fornisce un quadro

[3] Scaricabile gratuitamente dal sito di CLUSIT (https://supplychainsecurity.clusit.it/)

delle metodologie e degli strumenti disponibili per la gestione della sicurezza nella supply chain. L'utilizzo combinato di processi strutturati, strumenti automatizzati e una governance efficace consente di garantire un approccio sostenibile e scalabile alla gestione della supply chain ICT, in piena coerenza con le richieste di NIS2.

GESTIONE DELLA SUPPLY CHAIN ICT ATTRAVERSO UNA GRIGLIA DI VALUTAZIONE PONDERATA E SCORECARD DI RISCHIO

Nel modello di gestione della supply chain ICT in ottica NIS2, due strumenti risultano particolarmente efficaci e complementari: la Griglia di valutazione ponderata e la Scorecard di rischio.

La Griglia di valutazione ponderata è utilizzata principalmente nella fase di qualificazione iniziale. Consente di esaminare in modo strutturato la maturità e l'affidabilità del fornitore, assegnando pesi specifici a parametri come le certificazioni possedute, i livelli di business continuity, gli SLA, la sicurezza logica, l'auditabilità e lo storico relazionale. L'output è un punteggio ponderato che aiuta a determinare l'idoneità del fornitore rispetto ai requisiti aziendali.

Nella tabella 5 si può trovare un esempio di applicazione della griglia di valutazione ponderata utilizzata nella fase di qualificazione iniziale, utile per confrontare più fornitori in base a parametri definiti e pesati secondo le priorità dell'organizzazione.

La modalità di utilizzo della griglia è la seguente:

- Si assegnano dei pesi ai parametri (la somma deve essere 100%)
- Si valuta ciascun fornitore su una scala (es. 0–10)
- Si calcola la media ponderata
- Ipotizzando queste soglie di ammissione:
  - ≥ 8 → qualificato
  - 7–7,9 → qualificabile con riserva
  - < 7 → non qualificato

La Scorecard di rischio (si veda l'esempio in tabella 6) entra in gioco nella fase di valutazione del rischio associato. Questo strumento sintetizza i principali fattori di esposizione al rischio, contestualizzando rispetto ai servizi affidati. Tra i criteri tipici si considerano la natura dei dati trattati, l'accesso a sistemi critici, la continuità operativa, la localizzazione geografica del trattamento e la postura di

Tabella 5 - Griglia di Valutazione Ponderata

Criterio	Peso (%)	Punteggio Fornitore A	Punteggio Fornitore B
Conformità GDPR	30%	9	8
SLA e affidabilità	25%	8	7
Certificazioni ISO	20%	8	9
Gestione subfornitori	15%	7	6
Politiche di sicurezza	10%	9	9
Valutazione complessiva		8,25	7,55

sicurezza del fornitore. La scorecard consente di classificare il fornitore (ad esempio: basso, medio, alto rischio) e di stabilire il livello di attenzione e le misure di controllo da adottare.
Nell'esempio di seguito i punteggi positivi indicano fattori che aumentano l'esposizione al rischio, mentre i punteggi negativi riflettono la presenza di misure o controlli che lo riducono. Il totale determina il livello di rischio residuo percepito.
L'impiego integrato di questi strumenti consente di presidiare in modo coerente le diverse fasi del processo come si vede in Tabella 7.

Tabella 6 - Scorecard di Rischio

Fattore di rischio	Valore osservato	Punteggio
Trattamento di dati sanitari	Sì	3
Accesso a sistemi critici	No	0
Continuità del servizio	Essenziale	2
Trasferimento dati extra-UE	No	0
Certificazione ISO 27001	Presente	-1
Incidenti noti negli ultimi 12 mesi	No	0

Tabella 7 - Fasi del Processo di Valutazione

Fase	Strumento principale
Qualificazione iniziale	Griglia di valutazione ponderata
Valutazione rischio associato	Scorecard di rischi
Qualifica dinamica (monitoraggio)	Riesame della Scorecard + Griglia aggiornata

È fondamentale che entrambi gli strumenti siano concepiti come dinamici, ovvero aggiornabili nel tempo, così da riflettere l'evoluzione del contesto normativo, l'emergere di nuove minacce, l'introduzione di nuovi modelli di servizio e le raccomandazioni emanate dalle autorità competenti.
La loro integrazione nei processi aziendali di governance della sicurezza rappresenta un elemento chiave per rafforzare la resilienza dell'intero ecosistema sanitario.

Analisi e valutazione del rischio nel contesto sanitario

INTRODUZIONE

Nel settore sanitario, la protezione dei dati e la continuità operativa non sono solo esigenze organizzative, ma elementi fondamentali per la tutela della salute pubblica. Inoltre, la non conformità alle normative vigenti, come il GDPR, il Codice Privacy, e la Direttiva NIS2, può comportare sanzioni

amministrative significative (fino a 20 milioni di euro o al 4% del fatturato annuo globale nel caso del GDPR), configurando anche una responsabilità etica verso i pazienti in termini di tutela della riservatezza e continuità dei servizi. Un approccio risk based alla cybersecurity consente di affrontare queste sfide in modo strategico, partendo dalla consapevolezza che non tutti i rischi sono uguali, e che le risorse vanno allocate in base alla criticità degli asset e alla probabilità di accadimento delle minacce. Adottare una logica basata sul rischio significa:

- Collegare la sicurezza al valore pubblico: proteggere le informazioni sanitarie (dati clinici, referti, identità digitali) è essenziale per mantenere la fiducia dei pazienti e garantire la qualità dei servizi.
- Conformarsi alle normative vigenti, come il GDPR e la Direttiva NIS2, il Codice Privacy, la legge n. 90/2024, e il regolamento DORA, che impongono un presidio attivo e documentato dei rischi legati alla sicurezza informatica.
- Supportare la governance: la valutazione dei rischi fornisce strumenti decisionali al management, rendendo visibili le vulnerabilità e facilitando l'allocazione delle risorse per la loro mitigazione.
- Affrontare la complessità: le strutture sanitarie si basano su un ecosistema interconnesso (dispositivi IoT, software gestionali, cloud, catena dei fornitori ICT), che espone l'organizzazione a rischi sistemici e interdipendenti. La gestione del rischio aiuta a tenere conto di questa complessità.
- Prepararsi al futuro: intelligenza artificiale, telemedicina e interoperabilità pongono nuove sfide alla sicurezza. Un approccio basato sul rischio consente di accompagnare l'innovazione riducendo l'esposizione agli incidenti.

LE FASI DI UN CYBER RISK ASSESSMENT

Nel settore sanitario, un risk assessment efficace è cruciale per proteggere dati sensibili e garantire la continuità operativa. Oggi questa attività è richiesta esplicitamente dalla NIS2 (nell'Art. 23 – Valutazione del rischio, è espresso l'obbligo di "effettuare regolarmente valutazioni dei rischi relativi alla sicurezza delle reti e dei sistemi informativi").
L'analisi dei rischi è un processo che passa attraverso diverse fasi, che sintetizziamo nella tabella 8.
In sostanza, si parte da una chiara definizione del contesto, identificando gli asset critici (cartelle cliniche, dispositivi medicali, sistemi informativi) e le normative di riferimento. Segue la mappatura del-

Tabella 8 - Le fasi di un processo di risk assessment di cybersecurity in Sanità

1	Mappare gli asset critici (dati sanitari, applicazioni, dispositivi, infrastrutture) e norme di riferimento
2	Identificare le minacce e le vulnerabilità rilevanti per l'organizzazione
3	Valutare l'impatto potenziale su disponibilità, integrità e riservatezza dei servizi sanitari
4	Individuare gap di sicurezza rispetto alle best practice e agli obblighi di compliance
5	Definire un piano di mitigazione del rischio prioritizzando le azioni
6	Reporting verso il Board
7	Monitoraggio continuo e l'aggiornamento periodico di questa analisi

le minacce, che deve includere quanto meno: ransomware, attacchi ai dispositivi IoT e violazioni delle identità digitali. In questa fase si procede anche a valutare le vulnerabilità rilevanti dell'organizzazione (di persone, infrastrutture e informazioni critiche): questo viene effettuato con test di vulnerabilità (come VA/PT, vulnerability assessment e penetration test) o tramite tecnologie specifiche (Continuous Exposure Management, CEM, per la gestione continua delle vulnerabilità e l'analisi degli attacchi). Parlando di vulnerabilità, è importante in questa fase anche avere una piena comprensione di quelle legate alle terze parti, fornitori di software e apparati medicali, o IT supply chain, perché come specificato nella Direttiva NIS2, l'organizzazione risponde in prima persona anche per questi rischi.
La terza fase è la valutazione del rischio, il cui scopo è stimare l'impatto potenziale dei rischi cyber su disponibilità, integrità e riservatezza dei servizi sanitari. Questa analisi si sta spostando sempre più da approcci qualitativi ad altri maggiormente quantitativi (come sarà spiegato più avanti). Oltre alla valutazione, che combina probabilità e impatti per arrivare a una quantificazione del rischio, è necessario in questa fase posizionare i diversi accadimenti potenzialmente nocivi mappandoli in una "matrice di rischio".
In base quindi all'individuazione dei rischi legati a gap di sicurezza, oltre che di specifici obblighi di compliance, e naturalmente alla volontà dell'organizzazione di mitigare (vs accettare) determinati rischi, saranno pianificate le specifiche azioni ("piano di mitigazione del rischio prioritizzando le azioni"), dagli aggiornamenti del software alla formazione del personale alla revisione delle politiche di gestione delle identità digitali alla segmentazione delle reti e così via.
L'intero processo deve essere comprensivo della produzione di una specifica documentazione. Particolare attenzione andrà fatta al Reporting verso il Board, perché i risultati di un risk assessment aiutano a coinvolgere il vertice, a tradurre tecnicismi in business risk, a definire metriche e KPI di ausilio nel supporto decisionale.
Il ciclo si chiude con il monitoraggio continuo e l'aggiornamento periodico di questa analisi, che tipicamente rappresenta la fotografia della situazione in un determinato momento, e va quindi costantemente aggiornata nel tempo, con l'introduzione di nuovi scenari (come l'arrivo di intelligenza artificiale e telemedicina) o di nuove norme. Un esercizio di questo genere, oltre a essere oggi raccomandato dalle norme, aiuta le strutture sanitarie ad impostare un approccio strategico volto a prevenire incidenti e rafforzare la fiducia dei pazienti. Un ente sanitario deve oggi essere preparato alla creazione di un percorso di miglioramento continuo in ambito cyber risk assessment. La ciclicità di queste attività è fondamentale per raggiungere questo scopo: appare infatti difficile pensare che un ente sanitario complesso sia in grado di mitigare adeguatamente tutti i rischi individuati con le risorse economiche e umane a disposizione in un unico ciclo di assessment. Identificare un percorso di miglioramento continuo, ben tracciato e documentato, supporta gli sforzi di change management e dimostra la buona volontà e il realismo dell'ente a eventuali ispettori.

LE METODOLOGIE E GLI STRUMENTI CONSIGLIATI

Un approccio efficace alla gestione del rischio in ambito sanitario non può prescindere dall'adozione di metodologie strutturate e strumenti che supportino la raccolta di evidenze, la trasparenza del processo e il miglioramento continuo. La metodologia è una leva organizzativa che consente di collegare

la cybersecurity alla governance, al valore pubblico e alla compliance normativa, favorendo al tempo stesso la diffusione di una cultura della sicurezza all'interno dell'organizzazione, basata sulla consapevolezza, la responsabilizzazione e l'adozione di comportamenti corretti da parte di tutti gli attori coinvolti. Nel contesto sanitario, spesso caratterizzato da risorse limitate, infrastrutture eterogenee e una forte dipendenza da terze parti, una metodologia ben scelta consente di prioritizzare gli interventi, mappare le responsabilità e rendere il rischio comprensibile anche al vertice decisionale.
Tra le metodologie più consolidate, la ISO/IEC 27005 rappresenta un riferimento fondamentale per chi adotta lo standard ISO/IEC 27001 e desidera strutturare un ciclo completo di gestione del rischio informatico, dall'identificazione fino al trattamento e monitoraggio. È una metodologia flessibile, adatta anche a contesti sanitari medio-piccoli.
In ambito europeo, ENISA propone un Cybersecurity Risk Management Framework orientato alla semplicità operativa e pensato per essere implementato da pubbliche amministrazioni e imprese, anche non specialistiche. Per strutture sanitarie complesse - come aziende ospedaliere o IRCCS -può invece risultare utile il NIST Risk Management Framework (RMF), sviluppato negli Stati Uniti, che propone sei fasi iterative e integra già la logica della valutazione continua del rischio in ambienti critici.
Parallelamente, è utile integrare l'uso di strumenti di supporto digitale. Le piattaforme GRC (Governance, Risk & Compliance) permettono di automatizzare la raccolta dati, tracciare responsabilità e produrre la documentazione necessaria per audit e compliance. Per le PMI sanitarie, esistono strumenti gratuiti o accessibili, utili per avviare un primo ciclo di assessment o misurare la maturità cyber:

- Il Cybersecurity Maturity Assessment for SMEs di ENISA è uno strumento gratuito pensato proprio per piccole e medie imprese, anche sanitarie, per autovalutare le capacità di difesa e identificare le priorità di intervento.
- Il check-up sicurezza IT promosso dal Punto Impresa Digitale delle Camere di Commercio offre un'autovalutazione orientata alle imprese italiane, con particolare attenzione alla consapevolezza organizzativa.
- Per la Pubblica Amministrazione, è disponibile il tool per la gestione del rischio sviluppato dall'ACN oggi obbligatorio per Pubbliche Amministrazioni Centrali e Locali.
- Infine, in un contesto sanitario dove la dipendenza da fornitori tecnologici e dispositivi medicali è crescente, diventa centrale valutare anche il rischio esterno, attraverso strumenti che analizzano l'esposizione cyber e i rischi di terze parti (vendor risk). In questo ambito si segnalano:
- RINA Cyber, per valutare il proprio "rating" cyber secondo logiche di benchmarking
- Cyber Exposure Index, utile per stimare la vulnerabilità percepita dall'esterno
- Namirial CyberExpert, piattaforma italiana per il monitoraggio dei rischi esterni
- Security Scorecard, che consente anche un primo utilizzo gratuito per 14 giorni
- Qualys e RiskRecon, che offrono strumenti per la valutazione dell'esposizione e della postura di sicurezza, anche per analisi vendor
- UpGuard, particolarmente utile per le analisi di vendor risk e TPRM (Third Party Risk Management)

Integrare una metodologia robusta con questi strumenti consente di passare da una gestione reattiva del rischio a una strategia proattiva e misurabile, in grado di rafforzare la resilienza del sistema sanitario e di rispondere con maggiore efficacia ai requisiti di NIS2, GDPR e alle aspettative dei cittadini.

LA DOCUMENTAZIONE DA PREDISPORRE

La documentazione è un elemento essenziale di qualunque processo di risk assessment di cybersecurity, soprattutto in ottica di compliance normativa. Vediamo nel dettaglio quali documenti devono essere predisposti e quali sono i riferimenti della direttiva NIS2.
Documentazione essenziale nel processo di Risk Assessment: durante tutto il ciclo di vita dell'assessment, è fondamentale predisporre e aggiornare la seguente documentazione:

Registro dei rischi (Risk Register)

Documento comprendente l'elenco dei rischi identificati, con asset e processi coinvolti, minacce e vulnerabilità associate, valutazione di probabilità, impatto e livello di rischio, stato delle misure esistenti e pianificate, data dell'ultima valutazione, owner del rischio.

- Rapporto di Risk Assessment: documento di sintesi che include metodologia e standard utilizzati (es. ISO 27005, NIST RMF), perimetro, scopo e stakeholder coinvolti, analisi dei rischi, valutazione e classificazione, report di vulnerability scan, evidenze di test, pen test e simulazioni, risultati principali e rischi critici, raccomandazioni e priorità.
- Piano di trattamento del rischio (Risk Treatment Plan): contiene le misure tecniche e organizzative da implementare, con obiettivi specifici (riduzione, trasferimento, accettazione, ...), cronoprogramma dettagliato, risorse assegnate, metriche di verifica.
- Evidenze delle misure di sicurezza: policy aziendali e procedure operative (es. gestione delle patch, accessi, backup), audit trail, log di sistema, configurazioni, formazione del personale.
- Registro degli incidenti: aiuta a rivalutare i rischi sulla base degli eventi accaduti o sfiorati.
- Verbali e decisioni del management: documentazione formale di approvazione, accettazione del rischio residuo, priorità strategiche, budget assegnato.

Questa documentazione deve essere inoltre rivista con frequenza almeno annuale o a fronte di cambiamenti importanti (nuovi sistemi, incidenti, fusioni). La documentazione deve chiaramente indicare chi è stato coinvolto nel processo; in particolare deve esplicitare l'esistenza di un team interfunzionale composto da IT, biomedicale, risk manager, compliance, direzione medica.
Da notare che, anche se la NIS2 non elenca esplicitamente modelli di documenti, impone obblighi che rendono necessaria una documentazione strutturata, tra cui l'Art. 21 (Misure tecniche e organizzative) in cui si esplicita che gli enti devono "adottare misure tecniche, operative e organizzative appropriate e proporzionate ai rischi" e dimostrarne l'effettiva attuazione. Inoltre, nell'Art. 30 (Supervisione e controllo) si chiarisce che le autorità competenti possono chiedere qualsiasi informazione e documentazione utile a verificare la conformità, inclusi: rapporti di valutazione del rischio, evidenze di controlli e test effettuati, piani di miglioramento.

UN ESEMPIO DI GESTIONE DEL RISCHIO IN UN CONTESTO SANITARIO INTERNAZIONALE PER UNA PMI

Nel 2024 una nota multinazionale che si occupa di prodotti e servizi in ambito cybersecurity e sicurezza informatica ha ricostruito un attacco ransomware verificatosi in una piccola clinica sanitaria a gestione familiare, con meno di dieci dipendenti (un medico, un'infermiera, una receptionist e un consulente IT part-time). Come molte PMI sanitarie, la clinica disponeva di un'infrastruttura IT basilare, con dati

memorizzati su un server locale e pochi strumenti di protezione avanzata, anche a causa di budget limitati. L'attacco si è innescato tramite una mail di phishing, camuffata da fornitore di materiale medico. La receptionist ha aperto l'allegato malevolo, che ha attivato il ransomware. In pochi minuti, tutti i file – agende, cartelle cliniche, fatturazione – sono stati criptati. Un messaggio ha richiesto un riscatto di 20.000 dollari in criptovaluta, minacciando di divulgare i dati sensibili in caso di mancato pagamento. L'impatto è stato immediato e critico: le visite sono state sospese, i rimborsi assicurativi bloccati, e i pazienti preoccupati per la sicurezza dei propri dati. Oltre al danno operativo, la clinica ha affrontato un serio rischio reputazionale.
La risposta è avvenuta su più fronti:

- Coinvolgimento immediato del consulente IT, che ha isolato i sistemi e attivato i (parziali) backup disponibili.
- Denuncia alle autorità e ingaggio di una società di cybersecurity per l'analisi forense e la bonifica della rete.
- Comunicazione trasparente ai pazienti e notifica agli enti regolatori.
- Messa in sicurezza dell'infrastruttura: aggiornamento dei sistemi, introduzione di controlli di accesso, filtri email e policy di backup più frequenti.
- Attivazione di un programma di formazione del personale per prevenire nuovi casi di phishing.

Anche una struttura molto piccola può diventare bersaglio di attacchi sofisticati. Questo episodio evidenzia come la mancanza di aggiornamenti, backup coerenti e formazione di base possa esporre anche le cliniche più virtuose a rischi elevati. Ma dimostra anche che una reazione strutturata, la trasparenza e l'investimento in prevenzione permettono di superare l'incidente e trasformarlo in un'opportunità per rafforzare la resilienza organizzativa.

VALUTAZIONE DEL RISCHIO IN UNA CLINICA ODONTOIATRICA TRAMITE IL TOOL SRA

Un caso emblematico riguarda una piccola clinica odontoiatrica statunitense che ha utilizzato il Security Risk Assessment Tool messo a disposizione dal sito federale HealthIT.gov, pensato per facilitare la conformità alla normativa HIPAA. La clinica, composta da 5 persone e priva di personale IT dedicato, gestiva i dati dei pazienti (ePHI) tramite un fornitore cloud. Nonostante la buona volontà e alcune pratiche già presenti (come accessi profilati e logiche di "least privilege"), l'assessment ha fatto emergere vulnerabilità critiche: l'uso della sola autenticazione a password, l'assenza di una policy strutturata per le email contenenti ePHI, e una documentazione lacunosa.
Grazie al supporto di esperti esterni, il titolare ha completato oltre 100 delle 156 domande del tool in sei ore, identificando le azioni prioritarie per il miglioramento: introduzione della multi-factor authentication, protezione dei dispositivi fisici (es. stampanti/fax con memoria), scrittura di policy e piani di contingenza documentati, e formazione del personale. L'analisi ha inoltre evidenziato che il ricorso a fornitori cloud non elimina la necessità di svolgere due diligence e audit interni: la responsabilità sulla protezione dei dati resta condivisa.
Questo caso dimostra come anche una realtà piccola, con strumenti mirati e un approccio graduale, possa avvicinarsi agli standard di sicurezza richiesti, rafforzando la resilienza e la capacità di risposta a eventuali incidenti informatici.

LESSONS LEARNED

Questo caso evidenzia alcune lezioni per il settore sanitario:

- La documentazione va formalizzata e aggiornata, perché processi informali non sono sufficienti in caso di controlli o incidenti (soprattutto in un settore così critico e allo stesso tempo targettizzato da attacchi).
- L'autenticazione forte e il controllo degli accessi sono elementi basilari per la protezione dei dati personali.
- La formazione continua del personale rappresenta una delle difese più efficaci contro gli attacchi, riducendo il rischio collegato al fattore umano.
- La valutazione del rischio diventa quindi un'opportunità per migliorare cultura e processi di sicurezza interni, anche in realtà piccole.

L'importanza della Governance nel panorama sanitario

INTRODUZIONE

Nel panorama digitale contemporaneo, le organizzazioni sanitarie si trovano ad affrontare sfide di cybersecurity sempre più complesse e critiche. La Direttiva NIS2 non rappresenta semplicemente un adempimento normativo, ma costituisce un'opportunità strategica per rafforzare la resilienza digitale nel settore sanitario, dove la sicurezza dei sistemi informativi e di rete si intreccia direttamente con la sicurezza dei pazienti o più generalmente dell'ecosistema salute. Tali aspetti di resilienza possono essere coperti in diversi modi, non solo direttamente (per il tramite di una buona capacità di resistenza agli attacchi) ma anche indirettamente, attraverso varie misure di continuità, come piani di continuità aziendale, di ripristino in caso di disastro e anche di gestione delle crisi.

La governance della cybersecurity nel settore sanitario richiede un approccio olistico che vada oltre la mera implementazione di tecnologie di sicurezza, se si considera anche la notevole rilevanza della Supply Chain, a cui partecipano aziende pubbliche e private, di piccole, medie e grandi dimensioni. Le policy e le procedure rappresentano il tessuto connettivo che trasforma gli investimenti tecnologici in capacità operative e organizzative concrete.

L'esperienza degli ultimi anni ha dimostrato che gli attacchi informatici al settore sanitario non sono solo più frequenti, ma anche più sofisticati e mirati. Ransomware che bloccano sistemi ospedalieri, compromissione di dispositivi medici connessi, esfiltrazione di dati sanitari sensibili rappresentano minacce concrete che possono avere conseguenze dirette sulla vita dei pazienti. In questo contesto, una governance efficace della cybersecurity diventa il principale faro guida di un'attività di compliance.

Il modello di Governance deve necessariamente considerare le specificità, lo scopo e il posizionamento di enti e strutture, pubbliche o private, che offrono servizi sanitari ai cittadini, rispetto alle aziende fornitrici di strumenti informatici, dispositivi medici e di servizi. In particolare, come già menzionato in precedenza, nel contesto del sistema sanitario risulta fondamentale strutturare adeguatamente le relazioni e i processi che l'ambiente sanitario instaura con le aziende fornitrici. E' indispensabile, in questo senso garantire che le aziende sanitarie possano offrire al cittadino un servizio sicuro, in ter-

mini di protezione e privacy dei dati, e di qualità, in termini di adeguato utilizzo delle informazioni, contando anche (ma non solo) sugli strumenti che le aziende private possono mettere a disposizione. Tale rapporto tra i due ambiti non deve essere ingessato in una contrapposizione e sfiducia tra pubblico e privato, ma deve essere una fruttifera collaborazione in cui i requisiti di sicurezza richiesti dalle aziende sanitarie siano essenziali e concreti, lasciando il giusto spazio alla burocrazia. Le aziende fornitrici dal canto loro devono strutturarsi in modo da avere personale competente e nei ruoli opportuni, strumenti adeguati a garantire la sicurezza e un certo grado di flessibilità. La cybersecurity deve diventare in questo senso un dialogo proficuo che consenta di valutare, condividere e concordare le necessarie misure tecniche e organizzative da implementare, limitando l'elaborazione e scambio di documenti.

LA GOVERNANCE

Per questi motivi, il primo importante tassello non può che riguardare la Governance in generale, quindi ruoli, policy e procedure.

Le policy forniscono la direzione strategica e i principi guida che orientano le decisioni organizzative in materia di sicurezza informatica.

Tuttavia senza procedure operative dettagliate che traducano questi principi in azioni concrete, anche le policy meglio concepite rischiano di rimanere documenti teorici senza impatto reale. La governance, dal canto suo, fornisce la struttura decisionale e di responsabilità che garantisce l'implementazione efficace e il miglioramento continuo del framework di cybersecurity. Questo trittico garantisce il rispetto, almeno sulla carta, di tutta la produzione normativa in materia. La NIS2 pone però l'accento sull'accountability del top management, la responsabilità e la responsabilizzazione del organi direttivi e di amministrazione non può essere più solamente teorica.

La costruzione di un framework di compliance efficace per il settore sanitario inizia necessariamente dalla definizione di una struttura di governance chiara e robusta. Questa struttura deve rispondere alla domanda fondamentale "chi fa cosa" all'interno dell'organizzazione sanitaria, creando linee di responsabilità inequivocabili che attraversano tutti i livelli organizzativi affinchè sia sempre possibile risalire dalla base al vertice della piramide organizzativa.

Il livello strategico rappresenta il vertice decisionale dell'organizzazione, dove il Consiglio di Amministrazione o la Direzione Generale devono assumere la responsabilità formale della cybersecurity. Questo non significa che il vertice aziendale debba occuparsi degli aspetti tecnici, ma piuttosto che debba fornire la direzione strategica, allocare le risorse necessarie e richiedere reporting periodici sull'efficacia delle misure implementate.

Il livello operativo richiede la designazione di un Chief Information Security Officer (CISO) o figura equivalente (CIO) che abbia autorità decisionale reale e accesso diretto al vertice aziendale. Questa figura deve possedere competenze sia tecniche sia manageriali, essendo in grado di tradurre le esigenze strategiche in implementazioni operative e di comunicare efficacemente con il management i rischi e le opportunità legate alla cybersecurity. L'autorità decisionale è cruciale perché permette di prendere decisioni rapide in situazioni di emergenza senza dover attraversare le lungaggini burocratiche tipiche tanto di grandi organizzazioni quanto di macro organizzazioni (per problemi opposti).

Esempi di questo genere di problemi possono essere, in modo non esaustivo, un eccesso di complessità intra-organizzativa, una "non chiara" separazione o delimitazione di competenze, ma anche un'eccessiva stratificazione tra più dipartimenti o aree, od ancora una fusione senza accorpamento di staff. Sul versante delle micro-imprese il problema è rovesciato: la stratificazione di competenze e l'accentramento in un unico soggetto di più compiti fa si che si perda di vista fondamentalmente la differenza tra controllati e controllori.
Il livello tattico si concretizza nella costituzione di un team multidisciplinare che includa i rappresentanti di tutte le aree critiche dell'organizzazione sanitaria, con minime differenze tra le aziende pubbliche e private. La presenza di rappresentanti della direzione sanitaria, dell'IT, del legale, della compliance, del risk management garantisce che le decisioni sulla cybersecurity tengano conto di tutti gli aspetti organizzativi e non siano guidate esclusivamente da considerazioni tecniche. Con riferimento alle aziende private vanno considerate anche funzioni strettamente connesse al business, non solo quelle relative alla parte IT e Security. Chiaramente questa scansione di ruoli ben si sposa ad organizzazioni dotate di un numero adeguato di personale qualificato e di budget. Per le PMI tali ruoli saranno spesso condensati in un numero decisamente inferiore di soggetti(talvolta anche esternalizzati), con tutti gli aspetti positivi e negativi del caso.

LE POLICY

La definizione di ruoli e responsabilità rappresenta il secondo pilastro fondamentale della governance. Ogni policy deve essere accompagnata da una matrice (fondamentalmente la Matrice RACI, già vista anche in altri settori e per altri tipi di business, va benissimo come strumento, purché si valorizzino correttamente le aree di attività coperte) che chiarisca chi è responsabile dell'esecuzione di ogni attività, chi è responsabile per i risultati, chi deve essere consultato nelle decisioni e chi deve essere informato sui progressi. Nel settore sanitario, questa matrice deve considerare ruoli specifici tanto per gli aspetti sanitari quanto per quelli IT.
La creazione di policy efficaci richiede un approccio metodologico rigoroso che garantisca completezza, chiarezza e applicabilità pratica. Ogni policy deve seguire una struttura standardizzata che faciliti la comprensione e l'implementazione da parte di tutte le parti interessate coinvolte. Il focus non deve essere il caso eccezionale bensì il processo standard, al fine di garantire una massima applicabilità di analisi e valutazione.
L'intestazione di ogni policy deve includere informazioni fondamentali come titolo, versione, data di approvazione, prossima revisione e proprietario del documento. Questi elementi apparentemente formali sono in realtà cruciali per la gestione del ciclo di vita delle policy, permettendo di tracciare le modifiche nel tempo e di garantire che tutti utilizzino la versione più aggiornata ed anche e soprattutto quella in corso di validità.
Lo scopo e gli obiettivi della policy devono essere definiti chiaramente, spiegando cosa si vuole ottenere e perché questa è necessaria, con riferimenti specifici alla NIS2 e agli altri framework normativi applicabili.
L'ambito di applicazione deve specificare con precisione a chi si applica la policy, includendo personale interno, fornitori esterni e, dove rilevante, pazienti. Deve inoltre chiarire quali sistemi coinvolge

e quali processi regola, evitando ambiguità che potrebbero portare a lacune nell'implementazione o a conflitti di responsabilità.
La sezione delle definizioni, spesso sottovalutata, è fondamentale per garantire una comprensione uniforme dei termini tecnici e delle sigle utilizzate. Nel settore sanitario, dove convivono linguaggi tecnici informatici e medici, un glossario chiaro è sicuramente d'obbligo insieme a tutte le integrazioni specifiche tecniche.
I principi guida enunciano i valori fondamentali che orientano le decisioni organizzative, come il primato della sicurezza del paziente, la proporzionalità delle misure di sicurezza rispetto ai rischi, e la trasparenza nei processi decisionali.
Il processo di sviluppo delle policy, da intendersi come vero e proprio ciclo di vita del documento, deve essere strutturato e sistematico, iniziando con un'analisi approfondita del contesto organizzativo che mappi i processi critici, identifichi gli asset più importanti e valuti le minacce specifiche del settore sanitario. Questa fase di analisi deve essere seguita da una gap analysis che confronti lo stato attuale con i requisiti NIS2, identificando chiaramente le lacune da colmare. Il passo successivo obbligato sarà sicuramente quello di identificazione, analisi e valutazione del rischio. Il passaggio finale, che porta poi alla vigenza della policy, sarà sicuramente quello concernente l'iter formale di approvazione e riesame, con valutazioni di idoneità e adeguatezza, di solito compiuti da due soggetti ben differenti: il Top Management (Alta Direzione) e di solito il CISO (o il CIO o il Responsabile IT).

LE PROCEDURE

Il precipitato naturale delle policy è per ovvi motivi quello delle procedure operative, il quale rappresenta il momento cruciale in cui i principi strategici si traducono in azioni concrete e misurabili.
Le procedure devono fornire istruzioni dettagliate che permettano a chiunque di eseguire correttamente le attività richieste indipendentemente dal livello di esperienza tecnica.
L'identificazione dei processi richiede un'analisi granulare di ogni area coperta dalle policy, definendo i workflow operativi necessari per implementare efficacemente le disposizioni strategiche.
Le check-list operative rappresentano uno strumento particolarmente efficace nel settore sanitario, dove il personale deve bilanciare costantemente le esigenze di sicurezza informatica con l'urgenza delle cure ai pazienti. Queste liste devono essere progettate per essere utilizzate rapidamente anche in situazioni di stress, fornendo una guida affidabile che soprattutto non rallenti l'operatività clinica.
Gli escalation path (come ad esempio le call tree o il processo di segnalazione all'autorità) devono essere definiti con particolare attenzione alla criticità degli ambienti sanitari, dove i tempi di risposta possono avere implicazioni dirette sulla sicurezza dei pazienti. Le procedure devono specificare chiaramente quando e come fare escalation, fornendo criteri oggettivi che permettano al personale di prendere decisioni rapide anche in assenza del supervisore diretto.
La personalizzazione per il settore sanitario richiede che ogni procedura valuti attentamente l'impatto sulla continuità assistenziale e preveda alternative operative che garantiscano la continuità delle cure anche durante l'implementazione delle misure di sicurezza. Le procedure devono inoltre considerare le specificità dei dispositivi medici, molti dei quali non possono essere facilmente aggiornati, spenti o isolati dalla rete senza compromettere l'attività clinica e sanitaria.

Un fattore cruciale da tenere sotto controllo, per quanto riguarda la governance in senso generale (policy procedure e ruoli), è sicuramente quello del monitoraggio dell'attuale coerenza e validità delle stesse.
Il sistema di monitoraggio e miglioramento continuo deve utilizzare metriche che misurino l'efficacia delle policy attraverso indicatori di processo, risultato e compliance. Il ciclo di revisione deve includere revisioni periodiche, feedback sistematico dagli utenti finali, benchmarking con le best practice del settore, allineamento ad obiettivi ben delineati e aggiornamento continuo per riflettere l'evoluzione normativa e tecnologica.
Infine le procedure non vanno solamente monitorate, ma vanno altresì testate in contesti che siano il più possibile rappresentativi della realtà, al fine di allenare le figure responsabili a reagire a determinati scenari ed applicare correttamente quanto definito dalla procedura stessa.
Ad ogni modo gli aspetti di governance fin qui delineati non possono ignorare anche altri aspetti fondamentali come la gestione del rischio, il controllo della supply chain, la gestione degli incidenti, la continuità operativa e, molto importante, l'awareness informatico-sanitaria e la formazione del personale, che non deve essere misurata solo in termini di grado di apprendimento ma anche di efficacia, ossia di capacità di applicare concretamente quanto appreso.
L'allegato H contiene un esempio di team di lavoro per la preparazione di un modello di governance.

La gestione degli incidenti nel contesto sanitario

INTRODUZIONE

L'era digitale ha rivoluzionato il modo in cui le organizzazioni operano, rendendole sempre più dipendenti dalle reti e dai sistemi informativi. Parallelamente, la complessità e la frequenza delle minacce cyber sono cresciute esponenzialmente, rendendo la gestione degli incidenti un pilastro fondamentale della cybersicurezza. In questo contesto, la Direttiva NIS2 (Direttiva UE 2022/2555), recepita in Italia con il Decreto Legislativo n. 138/2024, introduce un quadro normativo più robusto e armonizzato a livello europeo, con implicazioni significative per un'ampia gamma di enti e settori.
Al netto di una formulazione laconica che richiede solamente l'implementazione di "misure di gestione degli incidenti" rimandando all'Autorità di riferimento (ACN) il compito di meglio approfondire il tema, il problema si pone soprattutto, all'interno del settore sanitario, per tutte quelle organizzazioni che volenti o nolenti non hanno mai preso seriamente in considerazione il management di questi aspetti.
Il problema, talvolta, può proporsi anche con riferimento alla medie e grandi organizzazioni, ma in quei casi non sempre si tratta di questioni di budget, anzi spesso di scarsa consapevolezza e di una mala-gestio dell'organizzazione interna.
Al centro della NIS2 vi è un'enfasi marcata sulla gestione del rischio cyber e sulla resilienza operativa. Le organizzazioni sanitarie coinvolte sono tenute a implementare misure tecniche e organizzative adeguate per gestire i rischi per la sicurezza delle reti e dei sistemi informativi che utilizzano per le erogare i propri servizi. Tra le misure chiave rientra la gestione degli incidenti, che assume un ruolo prioritario e con requisiti sempre più stringenti.

A questo problema deve potersi mettere mano partendo dalle base, preferendo un approccio semplice e lineare, che eviti complicazioni (al netto di quelle che già la normativa statale e quella regolamentare dell'Autorità mettono in campo). Per questi motivi, la gestione degli incidenti cyber nel settore sanitario richiede un approccio specifico che bilanci la sicurezza informativa dei sistemi e della rete con la continuità degli aspetti sanitari (da intendersi operativamente). Il "framework" deve essere costruito considerando che ogni interruzione può avere impatti diretti sulla salute dei pazienti ed indirettamente con ricadute sulla struttura, le parti interessate e l'immagine stessa (oltre a quelle di stampo economico).
Un approccio strutturato alla gestione degli incidenti si fonda su politiche chiare e processi ben definiti. In questo ambito è sempre consigliato adottare processi basati su standard, best practice o framework internazionali quali ISO 27001, ISO/IEC 27035, ITIL ma anche il nostrano Framework Nazionale per la cybersecurity e la data protection (l'FNCDP versione 2.1), basato su una variazione del NIST CSF 2.0 di recente aggiornamento.
Questo consente alle organizzazioni sanitarie di avere un quadro di riferimento chiaro e di velocizzare i tempi di implementazione delle politiche e dei processi di gestione degli incidenti informatici.

PRINCIPI

Oltre ad un impianto documentale preciso, bisogna tenere in considerazione sempre una serie di pilastri fondamentali, capaci di coniugare la dimensione della struttura con gli aspetti di incident management. Una scelta semplice e consapevole di questi potrebbe essere:

- Ogni decisione deve prioritizzare la sicurezza del paziente
- Le misure di contenimento e mitigazione devono essere proporzionate al rischio clinico
- Informazione tempestiva a tutti gli stakeholder rilevanti
- Rispetto simultaneo delle normative cogenti richieste (ad es. NIS2, GDPR e sanitarie specifiche)

Da queste quattro direttive bisogna poi costruire tutta la struttura di coordinamento e gestione degli incidenti, che sia per quanto possibile multidisciplinare (che abbia competenze sia IT ma che sia anche concretamente investita nel tessuto organizzativo sanitario).

FASE PREPARATORIA (RUOLI E CLASSIFICAZIONE)

Un'esemplificazione di queste figure potrebbe essere la presenza di una serie di soggetti di questo tipo:

- Figura con competenze tecniche e manageriali, preferibilmente con background sanitario per comprendere l'impatto clinico delle decisioni.
- Esperti IT specializzati in sistemi sanitari, dispositivi medici IoT, e infrastrutture critiche ospedaliere.
- Una figura sanitaria senior (ad es. un Direttore medico) che possa valutare l'impatto delle misure di sicurezza sui processi di cura.
- La parte legale e di compliance (che nelle piccole realtà è spesso esternalizzata).
- Il Responsabile della comunicazione interna ed esterna.

In ottica NIS2, considerando le recenti determine di ACN, in una struttura tipo quella immaginata sopra, il punto di contatto potrebbe essere la prima figura ed il sostituto l'ultima.
Le fasi di gestione degli incidenti sono (solitamente) sei: preparazione (che include tutta la fase for-

mativa e di classificazione che vedremo tra poco), identificazione (in cui si rinviene sempre la classificazione), contenimento, eradicazione, ripristino ed infine le attività di lessons learned.
Delineati gli aspetti di cui si è detto precedentemente e comprese le scansioni del processo di gestione degli incidenti, si può pensare successivamente, parallelamente al processo di gestione dei rischi, alla classificazione degli incidenti:
Utilizzando uno schema classico di probabilità per impatto, coadiuvato da alcuni criteri suppletivi di matrice "business continuity" (come ad esempio la durata dell'interruzione, il tempo massimo accettabile per il ripristino ed il tempo disponibile prima che l'incident si tramuti in crisi e diventi ingestibile), si può pervenire ad uno schema che dovrebbe ricalcare quanto qui sotto:

Rischio

- Livello 5 - Critico: Compromissione operativa totale di sistemi e infrastruttura
- Livello 4 – Alto: Compromissione parziale di sistemi e infrastruttura
- Livello 3 - Medio: Compromissione parziale di alcune parti di sistema e/o dell'infrastruttura
- Livello 2 - Basso: Nessuna compromissione grave, rallentamento di sistema o infrastrutturale
- Livello 1 - Lievi: Rallentamento di aspetti secondari non operativi

Impatto

- Impatto Catastrofico: Interruzione immediata delle infrastrutture e dei sistemi e rischio grave per la sicurezza del paziente
- Impatto Alto: Interruzione immediata delle infrastrutture e dei sistemi senza rischio grave
- Impatto Medio: Interruzione parziale delle infrastrutture e dei sistemi con rallentamenti nei presidi sanitari
- Impatto Basso: Rallentamento nella gestione operativa e nei presidi sanitari
- Nessun Impatto Clinico: Rallentamenti e malfunzionamenti amministrativi gestionali di processi secondari.

Naturalmente sono stati presi in considerazione aspetti solo sanitari e operativi, ma un'organizzazione dovrebbe pensare anche ad altri aspetti (reputazionali ad esempio).
Tenuta in considerazione la verosimiglianza di accadimento si può poi elaborare la classica matrice di prioritizzazione che vede nell'angolo in alto a destra la necessità di una risposta critica, il più efficiente, efficace e celere possibile al fine di ripristinare l'operatività e la sicurezza del paziente; laddove nell'angolo in basso a sinistra saranno contenute tutte quelle priorità secondarie da lavorare e gestire "dietro le quinte" ma con un'attenzione non secondaria, specie qualora i processi intaccati possano espandersi fino a toccare e influenzare aspetti primari.

ERADICAZIONE E CONTENIMENTO

In apertura si era accennato al fatto che la fase di mitigazione e contenimento debba essere sempre proporzionata all'organizzazione e al rischio clinico, alla luce della classificazione di cui sopra.
Tralasciando l'ipotesi catastrofica e alta, che sappiamo risulti essere una totale disconnessione dei

sistemi operativi e del loro conseguente spegnimento. Per gli impatti medi, questa fase dovrebbe prioritizzare un isolamento selettivo dei processi infrastrutturali colpiti dall'incidente al fine di poter mantenere operativi gli aspetti clinici essenziali. Quando questo non è possibile è chiaro che sia necessario procedere con soluzioni più dirette come la disattivazione totale dei sistemi compromessi, l'implementazione di backup con finestre operative brevi ed anche di protocolli di emergenza clinica che impediscano l'aggravamento della situazione.
Quando invece il tipo di incidente lo consente si può anche operare con un monitoraggio continuo a seguito di azioni correttive non impattanti sull'infrastruttura clinica, basandosi anche su soluzioni già sperimentate e che non vadano a ledere la norma operatività strutturale e sanitaria.
Le due fasi di impatto più alto dovranno prendere in considerazione anche aspetti maggiormente di accountability, decision making e comunicazione. Si tratta di definire fin da subito criteri preordinati a rispondere in modo immediato a domande come "chi fa cosa in caso di crisi?". Attraverso la predisposizione di un team come quello descritto sopra, composto in parti uguali da tecnici e sanitari, i secondi con poteri di coordinamento e decisione, tale fase può procedere in modo agile nella corretta informazione e comunicazione, tanto interna quanto esterna, della situazione di incidente all'interno dell'organizzazione. La comunicazione, per quanto spesso aspetto secondario, può fare la differenza tra una gestione lineare, efficace di una situazione critica e una gestione, caotica, infruttuosa, anche di una situazione molto meno grave.

RIPRISTINO

Successivamente alla fase di mitigazione deve poter iniziare la fase di ripristino, la quale ha un'importanza direttamente proporzionale al rischio dell'incidente e all'impatto subito.
Quindi, a fronte di impatti critici ed elevati, la fase di ripristino deve essere veloce ed efficace, al fine di poter ripristinare la disponibilità e l'integrità dei sistemi cercando di minimizzare e contenere gli eventuali rischi clinici.
Impatti medi e bassi invece dovranno (o potranno) limitarsi alla ricostruzione della normale operatività sanitaria ed infrastrutturale minimizzando le ricadute occorse in punto clinico.
Per gli aspetti lievi il ripristino spesso coincide con la soluzione proposta per la risoluzione dell'incidente, trattandosi di aspetti secondari, non operativi e routinari.
Ad ogni modo deve essere prioritizzata sempre la risposta clinica o sanitaria, che abbia al vertice i sistemi critici e di emergenza e alla base quelli standard e amministrativi.
Scopo ulteriore è anche quello di lavorare, in ottica successiva, sull'eliminazione delle root cause ed il rafforzamento delle misure di sicurezza. L'eradicazione deve infatti garantire la completa rimozione della minaccia senza compromettere l'integrità dei sistemi sanitari:
Ulteriori fasi di una gestione degli incidenti sono sicuramente gli aspetti comunicativi (specie con l'Autorità) e quelli di lessons learned.
Nel primo caso sarà necessario attenersi scrupolosamente alle procedure, ed alle tempistiche dettate dall'Autorità, ovvero:

- Entro 24 ore: pre-notifica all'ACN con informazioni preliminari sull'incidente.
- Entro 72 ore: notifica dettagliata con valutazione dell'impatto dell'incidente.

- Entro un mese (periodico): relazioni periodiche, con scansioni mensili, qualora l'incidente sia ancora in corso, per aggiornare l'Autorità sui progressi e lo stato d'implementazione delle misure.
- Entro un mese (finale): relazione finale con approfondimenti sulle misure adottate entro un mese dalla chiusura dell'incidente (se è durato più di un mese questo step sarà preceduto da una relazione mensile intermedia come si è visto immediatamente sopra).

Sarà poi necessario, con riferimento agli aspetti contenutistici, porre attenzione ad inserire tutte le informazioni necessarie per la valutazione della situazione; qualora si tratti di incidente significativo con riflessi anche sulla supply chain va fatta la notifica ai destinatari di tali servizi. Infine, qualora si tratti di incidente che comporta una violazione ai sensi del GDPR anche la scrupolosa attenzione a quanto da questo prescritto ed ai rapporti di notifica al Garante (entro 72 ore) e, se necessario (secondo quanto previsto dal Regolamento Europeo), agli interessati.

Un corretto workflow degli aspetti cogenti di comunicazione, nonché della cooperazione dell'organizzazione con l'Autorità può talvolta significare, qualora emergano lacune di compliance normativa e/o carenze organizzative ed infrastrutturali di base (come ad esempio la non implementazione di misure minime di cui alla Determina 164179 di ACN [5]) o la designazione solo sulla carte delle persone deputate a fare da raccordo con ACN, una riduzione della sanzione applicabile, qualora queste lacune siano verificate e confermate.

POST-INCIDENTE

Per questi motivi un aspetto non secondario è quello della formazione e della consapevolezza, perché se il personale non ha la bussola giusta per orientarsi e non conosce il "terreno" su cui si muove si potranno fare tutte le politiche e le procedure possibili ma il problema continuerà ad esistere e persistere, relegando ogni futura implementazione ad una impossibile stabilità operativa.

Strettamente collegata agli aspetti formativi e di awareness è la fase di lessons learned, la quale è una fase post-incidente obbligatoria per il rafforzamento anche delle misure stesse applicate e di quelle applicabili.

Le misure di più facile implementazione, oltre ad un piano formativo globale e non solo IT security oriented, riguardano:

- l'analisi sistematica di ogni incidente avvenuto e anche degli eventi di sicurezza o dei quasi-incidenti;
- l'analisi delle root causes, attraverso l'implementazione di metodologia conosciute e ben rodate;
- lo sviluppo di piani d'azione concreti, con scadenze e responsabilità definite (anche sotto forma di scenari e play books);
- la creazione di un sistema condiviso di Knowledge Management (da inserirsi all'interno di un piano formativo a più ampio respiro);
- l'identificazione di trend e pattern periodici in un'ottica di studio evolutivo delle minacce e di contenimento di eventuali incidenti futuri.

In conclusione è chiaro come la tematica di gestione degli incidenti, per quanto non secondaria, sia da sempre un punto da attenzionare in ogni organizzazione. Chiaramente in organizzazioni sanitarie alla necessità di ripristinare il servizio e le infrastrutture tecnico-operative fa da direttiva parallela la necessità di preservare e rafforzare gli aspetti clinici e sanitari.

SIMULAZIONE DI INCIDENTE

Le simulazioni di incidenti informatici sono fondamentali per la sicurezza delle nostre aziende. Prendendo spunto dalle linee guida della normativa e calandole nelle singole strutture riportiamo di seguito una sintesi dei motivi per i quali tali simulazioni sono così importanti.

- Migliorano la preparazione e la capacità di risposta. Attraverso le simulazioni, le organizzazioni possono testare e affinare la loro capacità di reagire rapidamente ed efficacemente a un attacco informatico. L'obiettivo è prevenire il peggioramento dell'incidente e garantire il ripristino dei servizi essenziali.
- Validano i piani e le procedure. Le simulazioni permettono di verificare l'efficacia dei piani di risposta agli incidenti, individuando eventuali lacune o punti deboli prima che un vero attacco si verifichi. Questi piani definiscono chiaramente i ruoli, le responsabilità e le modalità di comunicazione interna ed esterna.
- Identificano le "lezioni apprese". Dopo ogni simulazione o incidente reale, è fondamentale analizzare ciò che è andato bene e ciò che può essere migliorato. Questo processo di miglioramento continuo è essenziale per affinare costantemente le capacità di difesa cibernetica.
- Promuovono il coordinamento e la collaborazione. Le simulazioni coinvolgono diversi attori, a livello nazionale e internazionale, per migliorare la preparazione e la resilienza del Paese di fronte alle minacce informatiche.
- Adempiono agli obblighi normativi. La legge impone alle organizzazioni essenziali di implementare misure di gestione dei rischi informatici, inclusa la gestione degli incidenti e la continuità operativa, per cui le simulazioni sono uno strumento chiave.

In sintesi, le simulazioni di incidenti informatici sono molto più che semplici test; sono momenti di apprendimento e miglioramento continui che permettono ad un'organizzazione di rimanere agile e preparata di fronte alle minacce cibernetiche in continua evoluzione.

La continuità operativa nel contesto sanitario

INTRODUZIONE

In questo paragrafo analizzeremo le strategie organizzative e daremo una base tecnica di terminologie e concetti chiave per garantire la continuità operativa dei servizi in caso di incidente informatico; alla luce delle direttive NIS2 questo argomento è ripreso nell'obbligo di segnalazione di incidenti che blocchino l'attività dei soggetti e nel contesto degli allegati contenenti le misure minime di sicurezza della determina 164179/2025 emanata da ACN lo scorso aprile. Verranno approfonditi i concetti di resilienza digitale, Business Continuity Plan (BCP) o Piano di Continuità Aziendale e Disaster Recovery Plan (DRP) o Piano di Disaster Recovery, evidenziando il loro ruolo nell'assicurare la tenuta dei processi clinici e amministrativi.

L'importanza di questa disamina è volta alla sensibilizzazione degli impatti economici e operativi legati ai tempi di ripristino e ai costi del mancato ripristino, con l'obiettivo di offrire un quadro pratico e strategico per la governance della sicurezza informatica.

PERCHÉ PARLARE DI RESILIENZA IN SANITÀ OGGI

Nel contesto di una crescente digitalizzazione dei servizi sanitari, la continuità operativa non può più essere considerata solo un tema tecnico. Le minacce informatiche, insieme a guasti accidentali o malfunzionamenti, rappresentano un rischio reale per l'erogazione dei servizi sanitari e amministrativi. Questo significa che la resilienza operativa è diventata una priorità strategica cruciale per tutte le strutture sanitarie, sia pubbliche che private.

La normativa NIS2 offre un quadro regolatorio di riferimento importante, imponendo obblighi di preparazione e risposta agli incidenti informatici. Tuttavia, la vera sfida è quella di integrare questi requisiti in una governance efficace e proattiva, in grado di proteggere i pazienti e garantire la continuità delle cure.

Gli operatori sanitari si trovano ad affrontare scenari complessi, dove la componente tecnologica costituisce un fattore essenziale abilitante, ma critico in quanto vulnerabile. È fondamentale investire nella formazione del personale, nell'aggiornamento dei sistemi e nell'adozione di misure di sicurezza adeguate. Solo così potremo costruire un sistema sanitario resiliente, capace di affrontare le sfide del futuro.

CONTINUITÀ OPERATIVA: COSA SIGNIFICA IN AMBITO SANITARIO

In ambito sanitario, la continuità operativa implica la capacità di garantire i processi essenziali – dalle cure ai pazienti alla gestione delle informazioni cliniche – anche in condizioni avverse, minimizzando il rischio clinico. Questo richiede una visione olistica, che vada oltre la semplice infrastruttura IT per includere il funzionamento di team, procedure alternative anche non digitali e definizione chiara delle responsabilità. L'interruzione di un sistema critico può avere ripercussioni immediate sul rischio clinico, ovvero sulla sicurezza, l'efficacia e la tempestività dell'assistenza sanitaria, sottolineando l'importanza di strategie di prevenzione e mitigazione. Non si tratta solo di un problema tecnico, ma di una sfida che coinvolge l'intera organizzazione.

Per garantire la continuità dei servizi sanitari, i piani operativi devono considerare tutte le componenti essenziali che ne supportano l'erogazione. Questo include non solo le infrastrutture tecnologiche e informatiche (IT), ma anche le infrastrutture IoT/OT elettromedicali e i servizi tecnici a supporto dei datacenter quali continuità energetica, condizionamento, antincendio, accessibilità.

Anche il personale sanitario deve essere preparato ad affrontare situazioni di emergenza, con piani di continuità ben definiti e testati. Allo stesso tempo, è fondamentale investire nella resilienza dei sistemi informatici, adottando misure di sicurezza avanzate e piani di disaster recovery.

Solo attraverso un approccio integrato, che metta al centro la tutela dei pazienti e la qualità delle cure, le strutture sanitarie potranno garantire la continuità operativa anche di fronte a sfide impreviste. È una responsabilità cruciale, che richiede il coinvolgimento di tutti gli attori del sistema.

DALLA BUSINESS CONTINUITY ALLA RESILIENZA OPERATIVA

Avere un solido Piano di Continuità Aziendale (BCP) e un Piano di Disaster Recovery (DRP) è fondamentale, ma non è sufficiente da solo per garantire la vera resilienza operativa di un'organizzazione sanitaria. Ci vuole molto di più.

La resilienza richiede un approccio integrato, che sappia coniugare gli aspetti tecnici, come il ripristino dei sistemi informatici, con quelli organizzativi, come il coordinamento del personale, la comunicazione efficace e la capacità di reazione rapida. Le strutture sanitarie devono essere in grado di adattarsi velocemente agli imprevisti, grazie a una cultura interna orientata alla preparazione e al coinvolgimento attivo di tutti i livelli di leadership. Non basta avere un bel piano scritto, è necessario che tutto il personale sia addestrato, consapevole del proprio ruolo e pronto ad agire in caso di emergenza.
Questo richiede investimenti nella formazione, nell'esercitazione di scenari di crisi e nell'adozione di una mentalità proattiva. I responsabili devono essere in grado di prendere decisioni tempestive, comunicare in modo chiaro e coordinare le risposte, sempre con l'obiettivo di tutelare la sicurezza dei pazienti e garantire la continuità delle cure.
Solo attraverso questo approccio olistico, che integra gli aspetti tecnici e organizzativi, le strutture sanitarie potranno davvero costruire una resilienza operativa solida e affidabile. È una sfida complessa, ma essenziale per garantire l'eccellenza dell'assistenza sanitaria, anche nelle situazioni più difficili.

TEMPI E COSTI: QUANTO VALE LA RESILIENZA

Quando si parla di continuità operativa, ci sono alcune metriche chiave da tenere a mente, come il RTO (Recovery Time Objective) e l'RPO (Recovery Point Objective). Questi indicatori ci rappresentano quanto tempo possiamo permetterci di stare fermi prima che il danno diventi insostenibile, e a partire da quale punto possiamo riprendere le attività. Non esiste ovviamente una catalogazione e strutturazione universale ma vanno calati nel contesto.
Immaginiamo il caso di una clinica che si trova ad affrontare un blackout IT. Se il sistema va offline per più di 4 ore (il loro RTO), potrebbero iniziare a sorgere seri problemi. I pazienti non potrebbero essere registrati, le prescrizioni non potrebbero essere emesse, e le informazioni cliniche essenziali non sarebbero accessibili. Questo significherebbe non solo costi diretti per il fermo servizio, ma anche un grave danno all'immagine e alla fiducia dei pazienti, senza contare i rischi clinici legati all'interruzione delle cure.D'altra parte, se la clinica avesse un RPO di 1 ora, potrebbero riprendere rapidamente le attività senza perdere troppi dati. Certo, ci sarebbero comunque dei disagi, ma nulla di paragonabile a uno scenario in cui l'ultimo backup fosse di una settimana prima. Con l'evoluzione dei sistemi informatici la sfida è abbassare l'RPO fino ad azzerarlo garantendo una continuità operativa esente da interruzioni. Oggi è impossibile arrivare a tanto ma si può strutturare il sistema livelli, avvicinandosi nella maggior parte delle situazioni critiche all'azzeramento. Ecco perché la resilienza operativa non dovrebbe essere vista come un costo, ma come un investimento. Sì, richiede risorse e impegno, ma può fare la differenza tra dare continuità dei servizi e dover fermarli per giorni o settimane con le conseguenze del caso. E in un ambito come la sanità, dove la continuità delle cure è essenziale, questo può davvero significare la differenza tra la vita e la morte per i pazienti.

PIANI D'AZIONE E RACCOMANDAZIONI STRATEGICHE

Quando si tratta di costruire una solida resilienza operativa per una struttura sanitaria, è essenziale avere un piano d'azione ben definito. I piani di Business Continuity (BCP) e Disaster Recovery (DRP) sono gli strumenti chiave per affrontare questa sfida. Innanzitutto, è cruciale effettuare una valu-

tazione approfondita dei rischi a cui l'organizzazione potrebbe essere esposta, sia da un punto di vista tecnologico che organizzativo. Questo ci permetterà di identificare le aree più vulnerabili e di predisporre le contromisure adeguate. Una valutazione attenta e conforme ai controlli di framework riconosciuti è la base del documento di valutazione dei rischi e dell'impatto sottolineato come adempimento dalla NIS2 ed in genere elemento cardine quando si parla di sicurezza delle informazioni.
Inoltre, è fondamentale che i dirigenti sanitari, il reparto IT e la direzione generale lavorino in sinergia per definire una strategia efficace. Questo include la pianificazione di simulazioni periodiche per testare l'efficacia dei piani, la formazione continua del personale sulle procedure da seguire in caso di emergenza, e la gestione attenta dei rapporti con i fornitori di servizi critici.
Infine, non bisogna sottovalutare il ruolo delle partnership tecnologiche e delle assicurazioni cyber. Collaborare con provider affidabili e stipulare coperture assicurative adeguate può fornire un importante supporto aggiuntivo per affrontare eventuali incidenti e minimizzare i danni.
Insomma, costruire la resilienza operativa di una struttura sanitaria richiede un approccio olistico e strategico, che coinvolga tutti i livelli dell'organizzazione. Solo così potremo essere davvero preparati ad affrontare le sfide del futuro e garantire la continuità delle cure ai nostri pazienti.

LA RESILIENZA COME LEVA PER L'AFFIDABILITÀ DEI SERVIZI SANITARI

Possiamo affermare che la resilienza operativa rappresenta una leva fondamentale per garantire l'affidabilità e la continuità dei servizi sanitari, soprattutto in un contesto di crescente digitalizzazione e minacce informatiche.
Abbiamo visto come gli elementi chiave di un solido piano di Business Continuity e Disaster Recovery includano una valutazione approfondita dei rischi, simulazioni periodiche, formazione del personale e sinergia tra i diversi dipartimenti dell'organizzazione. Questo approccio è essenziale per prepararsi ad affrontare qualsiasi tipo di imprevisto o emergenza.
Tuttavia, il vero salto di qualità avviene quando l'organizzazione sanitaria va oltre la semplice compliance normativa (come il regolamento NIS2) e abbraccia una vera e propria "cultura della resilienza". Questo significa che la capacità di resistere e riprendersi rapidamente da eventi critici deve diventare parte integrante della mentalità e delle priorità di tutti, dai vertici aziendali al personale di prima linea. Perché in fondo, costruire la fiducia dei pazienti nei servizi sanitari significa anche dimostrarsi affidabili e in grado di mantenere la continuità delle cure anche nei momenti più difficili. È una responsabilità che va oltre il semplice adempimento normativo: è una sfida che richiede impegno, investimenti e un cambiamento culturale profondo, ma che può fare la differenza per la salute e il benessere di tutta la comunità.

VERSO UN ECOSISTEMA SANITARIO INTERCONNESSO E RESILIENTE

Come già dimostrato nel periodo post-pandemico, alla luce della trasformazione digitale in atto, la sanità non può più essere considerata un insieme di entità isolate. Ospedali, cliniche, servizi territoriali, fornitori tecnologici, enti regolatori e cittadini compongono un sistema interconnesso, dove la resilienza di ciascun attore influenza la tenuta complessiva del sistema. La NIS2 promuove la sicurezza della supply chain che al di là degli aspetti normativi va allargata anche agli attori periferici e agli utilizzatori e fruitori dei sistemi.

In questo scenario, la resilienza operativa del sistema sanitario non può limitarsi alla singola struttura ospedaliera o clinica. Deve estendersi all'intera rete sanitaria, coinvolgendo i sistemi regionali, i partner tecnologici e le autorità pubbliche. Un attacco informatico a un fornitore critico o un'interruzione della connettività può avere effetti a catena, compromettendo l'intero percorso di cura del paziente. È quindi essenziale adottare un approccio collaborativo e interdisciplinare, basato sulla condivisione delle informazioni, la standardizzazione delle interfacce e la pianificazione congiunta degli scenari di crisi. L'interoperabilità dei sistemi informatici gioca un ruolo chiave in questo contesto. Piattaforme sanitarie integrate, repository unificati e protocolli comuni non solo migliorano l'efficienza operativa, ma permettono anche una risposta più rapida e coordinata in caso di emergenza. Inoltre, è fondamentale definire ruoli, responsabilità e piani d'intervento che coinvolgano anche soggetti esterni all'organizzazione sanitaria, come fornitori di servizi IT e autorità competenti.
La resilienza dell'intero ecosistema sanitario dipenderà sempre più anche dalla capacità di gestire le nuove vulnerabilità introdotte dalle tecnologie emergenti. L'adozione di soluzioni cloud, l'utilizzo crescente di dispositivi IoT in ambito clinico e il ricorso all'intelligenza artificiale pongono nuove sfide di sicurezza, integrità e continuità dei dati. Questi elementi devono essere inclusi nei piani di resilienza con una visione evolutiva e sistemica, anticipando i possibili scenari futuri.
Infine, è cruciale promuovere una cultura della resilienza condivisa, dove ogni attore – pubblico o privato – sia consapevole del proprio ruolo all'interno dell'ecosistema sanitario. Solo così sarà possibile costruire una sanità moderna, sicura e capace di rispondere con efficacia alle crisi future, tutelando al tempo stesso i diritti dei pazienti e la qualità delle cure.

L’importanza della formazione all’interno del contesto sanitario e della NIS2

INTRODUZIONE: DALLA CONSAPEVOLEZZA ALLA PADRONANZA

La Direttiva NIS2 introduce importanti novità sulla sicurezza informatica, enfatizzando il ruolo centrale del fattore umano e della formazione. In un’epoca in cui le minacce cyber evolvono rapidamente, non basta investire in tecnologia; occorre anche coltivare e diffondere una solida cultura della sicurezza in tutti i membri dell’organizzazione. La Direttiva NIS2 riconosce che le persone – dai dirigenti ai dipendenti – possono costituire sia l’anello debole sia la prima linea di difesa dei sistemi informativi. Per questo, la normativa rende la security awareness avanzata un pilastro fondamentale della gestione del rischio informatico.
Nell’attuale panorama della cybersecurity, il fattore umano rappresenta uno dei principali punti di vulnerabilità. Gli attacchi informatici non si limitano più a violare sistemi tecnologici: mirano direttamente agli utenti, sfruttando le loro debolezze, i loro automatismi cognitivi, le abitudini digitali e le emozioni. In questo contesto, la formazione in ambito Security Awareness assume un ruolo cruciale. Tuttavia, l’obiettivo di una formazione avanzata non può più essere semplicemente quello di “sensibilizzare”. È necessario mirare a un cambiamento profondo e duraturo dei comportamenti. La conoscenza teorica deve trasformarsi in competenza operativa, fino a costituire un mindset: un insieme di atteggiamenti, prontezze e reazioni integrate nel quotidiano. Si parla così non solo di awareness,

ma di mastery – una padronanza consapevole, adattiva e reattiva nei confronti delle minacce cyber. Perché ciò avvenga, la formazione deve essere continua, metodologicamente fondata, esperienziale e personalizzata. Solo in questo modo si può costruire una cultura della sicurezza diffusa, resiliente e capace di evolversi con la velocità del cambiamento digitale.

AWARENESS: PENSIERI LENTI, PENSIERI VELOCI E BIAS COGNITIVI

La teoria dei due sistemi di pensiero di Daniel Kahneman, descritta nel suo libro Thinking, Fast and Slow [10], spiega come il nostro cervello processa le informazioni attraverso due modalità distinte:

- Sistema 1 (pensiero veloce e intuitivo) – È automatico, rapido ed emozionale. Funziona per associazioni ed esperienze pregresse, permettendoci di rispondere istintivamente agli stimoli senza sforzo cognitivo. Tuttavia, è anche soggetto a bias cognitivi ed errori, rendendoci vulnerabili a manipolazioni e inganni.
- Sistema 2 (pensiero lento e razionale) – È deliberato, analitico e richiede più tempo ed energia. Ci permette di valutare criticamente le informazioni, riflettere sulle decisioni e individuare inganni o rischi.

Nel contesto della Cybersecurity, gli attacchi informatici (in particolare il Phishing) sfruttano il Sistema 1, inducendo la vittima a reagire d'impulso a stimoli mirati (urgenza, autorità, paura). Il meccanismo "Click-to-Run" (che nell'ambito del Phishing potremmo definire "Click-to-Click") porta a cliccare su link fraudolenti o a rivelare informazioni sensibili senza attivare il Sistema 2, che richiederebbe una valutazione più attenta.

Nel corso degli ultimi anni, numerosi attacchi informatici hanno sfruttato proprio il funzionamento automatico e impulsivo del Sistema 1. Un caso emblematico è quello della campagna di phishing denominata "CEO Fraud", in cui i cybercriminali inviavano mail false, apparentemente provenienti da dirigenti aziendali, per indurre i dipendenti a effettuare bonifici urgenti. Sfruttando il senso di autorità e urgenza, questi attacchi evitano l'attivazione del Sistema 2, portando la vittima a reagire d'istinto.

Analogamente, durante la pandemia di COVID-19, molte strutture sanitarie sono state bersaglio di email fraudolente contenenti finti aggiornamenti su vaccini o su protocolli d'emergenza, che inducevano il personale a cliccare su link malevoli. Questi attacchi, oltre a compromettere dati sensibili, hanno messo a rischio la continuità dei servizi sanitari.

La direttiva NIS2, entrata in vigore per rafforzare la resilienza informatica a livello europeo, affronta direttamente queste problematiche. Tra i settori coperti dalla normativa rientra anche la sanità, incluse le attività di ricerca e sviluppo di prodotti medicinali, proprio per la loro criticità e l'elevato livello di interconnessione digitale. La NIS2 impone alle entità essenziali e importanti di attuare un approccio basato sulla gestione del rischio, che includa elementi specifici come la gestione degli incidenti, la sicurezza della supply chain, e – aspetto cruciale in relazione agli attacchi che sfruttano il Sistema 1 – programmi di formazione e sensibilizzazione del personale.

I BIAS COGNITIVI, RICONOSCERLI PER PROTEGGERSI

I bias cognitivi sono errori sistematici di pensiero che influenzano la nostra capacità di elaborare informazioni in modo oggettivo; questi bias possono influenzare la valutazione delle vulnerabilità del

sistema e la scelta delle misure di sicurezza da adottare. Nel contesto degli attacchi informatici, i bias cognitivi possono portare a giudizi errati sulla minaccia, sulla gravità dell'attacco e sulle conseguenze delle azioni intraprese per affrontarlo. È dunque importante riconoscerli per poterne mitigare gli effetti e prendere decisioni informate sulla sicurezza informatica.
I bias agiscono indifferentemente nel mondo reale e in quello virtuale e sono alla base di qualsiasi meccanismo di truffa. Nel mondo virtuale la loro influenza viene amplificata a causa della bassa percezione generale del pericolo.
Gli hacker sfruttano i bias cognitivi in modo mirato, costruendo scenari che spingono le persone a compiere azioni senza riflettere. Un esempio frequente è l'utilizzo del principio di autorità: l'attaccante si finge un superiore o un tecnico informatico e chiede con urgenza di condividere credenziali o aprire allegati. La vittima, riconoscendo una figura "credibile", tende ad obbedire senza attivare pensiero critico. Un altro meccanismo molto usato è quello della scarsità: "ultima possibilità", "tempo limitato", "accesso bloccato se non agisci ora". Questo bias induce all'azione rapida, aggirando le normali valutazioni di rischio. È lo stesso principio alla base di molte truffe bancarie o email fasulle in ambito sanitario, dove l'urgenza percepita prevale sulla cautela. Anche il bias ottimistico ha un peso significativo: la convinzione, spesso inconscia, che "tanto a noi non capiterà mai", porta a ignorare segnali d'allarme, sottovalutare la necessità di misure preventive o agire con leggerezza nell'uso degli strumenti digitali. Inoltre, c'è il principio di empatia, spesso sfruttato in attacchi che simulano raccolte fondi, emergenze umanitarie o storie toccanti. In questi casi, la leva emotiva prevale sulla verifica logica, e la vittima agisce per impulso emotivo, dimenticando ogni cautela.
Sono solo alcuni esempi di come i bias possono influenzare i comportamenti del personale delle aziende che operano in ambito sanitario. Nell'ambito della formazione finalizzata alla sicurezza, anche secondo i principi della NIS2, si pone una riflessione anche sulla potenziale enorme massa di individui (soggetti ovviamente ai bias) che potranno conferire informazioni e dati direttamente ai sistemi sanitari grazie ad una larga serie di fattori abilitanti: smartphone, mobile apps, wearables, ecosistema del Fascicolo Sanitario Elettronico, integrazione e interoperabilità con cartelle cliniche o sistemi informativi ospedalieri e sanitari. Questi soggetti sono pazienti e cittadini, per i quali è necessaria una riflessione sulla cultura più estesa sulla cultura digitale, di quella che può essere affrontata in queste pagine.

UN IMPIANTO METODOLOGICO SOLIDO E SCIENTIFICAMENTE FONDATO

Una formazione realmente efficace nel dominio della cybersecurity richiede un impianto metodologico robusto, fondato su discipline come la psicologia cognitiva, la didattica per adulti (andragogia), le neuroscienze e la comunicazione efficace.
Un elemento chiave è la gestione del carico cognitivo: apprendere significa elaborare informazioni, ma la soglia di attenzione umana è limitata. Stimoli e contenuti devono essere dosati e segmentati in unità semplici, mirate, senza sovraccaricare i discenti. Questo implica una progettazione centrata sull'utente, rispettosa dei suoi tempi e dei suoi livelli di elaborazione.
All'interno di questo impianto, la formazione deve essere anche multimodale: basata su più canali sensoriali e cognitivi, per rispondere alla varietà degli stili di apprendimento e facilitare un'elabora-

zione più profonda. Come dimostrano le ricerche di Mayer e Moreno [12], l'uso integrato di narrazione, immagine, interazione e supporto immediato può amplificare l'efficacia della formazione, indipendentemente dalle preferenze individuali.
La seguente tabella sintetizza le principali modalità e tecniche formative applicabili a contesti di cybersecurity, raggruppate per funzione didattica prevalente:
Queste modalità possono essere combinabili e modulari, creando percorsi didattici flessibili, continui e integrati con l'operatività quotidiana. L'obiettivo è allenare competenze reali, consolidare comportamenti e sviluppare una cultura organizzativa della sicurezza.

Tabella 9 - Tecniche e Modalità Formative

Finalità	Tecniche e Modalità Formative
Favorire apprendimento rapido	**Microlearning:** pillole di 4–6 minuti integrate nel flusso di lavoro quotidiano
	Time-Spaced Learning: distribuzione temporale dei contenuti per favorire memorizzazione
Facilitare comprensione profonda	**Storytelling immersivo:** narrazione coinvolgente e realistica per stimolare identificazione
	Educational Language: linguaggio accessibile, non tecnico, per semplificare la complessità
Promuovere coinvolgimento attivo	**Gamification:** dinamiche ludiche per motivazione e partecipazione
	Esercitazioni interattive: simulazioni e feedback dinamici in tempo reale
Allenare abilità e comportamenti	**Problem-Solving Learning:** scenari reali da analizzare e risolvere
	Dibattito guidato: confronto strutturato per sviluppare pensiero critico e consapevolezza
	Teatro d'impresa: simulazioni relazionali e comunicative in contesti protetti
Garantire progressione didattica	**Percorsi multilivello:** aumento graduale della complessità con rinforzo selettivo
	Formazione esperienziale: attacchi simulati, esercitazioni operative, errori protetti
Personalizzare e supportare	**Apprendimento conversazionale:** chatbot e assistenti digitali per interazione continua
	Supporto proattivo: sistemi intelligenti che offrono suggerimenti nel momento del bisogno
Adattare al singolo	**Human-Centered Design:** progettazione formativa centrata su tempi, bisogni, profilo cognitivo

FORMAZIONE CON AI GENERATIVA: VERSO PERCORSI ADATTIVI

Tra le innovazioni più promettenti emerge il Generative AI-based Learning, che sfrutta modelli linguistici avanzati per creare esperienze formative personalizzate, dinamiche e adattive. Le applicazioni includono:

- Tutor virtuali intelligenti per l'apprendimento conversazionale.
- Creazione automatica di contenuti formativi (testi, quiz, video).
- Adattamento dinamico dei percorsi in base al profilo e al progresso dell'utente.
- Feedback immediato e contestuale, in ambienti simulati o reali.

Tuttavia, la formazione basata su AI deve essere progettata e supervisionata con attenzione. Tre aspetti critici da considerare sono:

- Affidabilità dei contenuti
  - Si può mitigare con l'uso di tecnologie RAG (Retrieval-Augmented Generation) e validazione delle fonti
- Creazione automatica di contenuti formativi (testi, quiz, video)
  - Si può contrastare integrando metodi attivi per stimolare pensiero critico
- Adattamento dinamico dei percorsi in base al profilo e al progresso dell'utente
  - È necessaria l'adozione di standard etici e compliance GDPR nella gestione dei dati

Se integrata con un approccio metodologico solido e finalizzata allo sviluppo di autonomia e consapevolezza, l'intelligenza artificiale può amplificare l'efficacia e la portata della formazione, rendendola realmente inclusiva, continua e centrata sulla persona.

FORMAZIONE PERMANENTE E ADATTIVA: IMPARARE A EVOLVERSI

In un contesto in cui le minacce digitali cambiano rapidamente, è essenziale adottare una prospettiva di lifelong learning: l'apprendimento deve essere continuo, aggiornato, dinamico. Non si tratta solo di aggiungere nuovi contenuti, ma di creare un ecosistema formativo che accompagni l'individuo nel tempo, rinforzando conoscenze e abilità.

Le minacce informatiche sfruttano bias cognitivi, meccanismi automatici e vulnerabilità psicologiche (ad esempio il cosiddetto "click impulsivo"). Per contrastare questi meccanismi serve allenamento costante, che sviluppi:

- Flessibilità cognitiva: abbandonare schemi rigidi e adattarsi a situazioni nuove.
- Resilienza emotiva: gestire l'incertezza e lo stress senza perdere il controllo.
- Propensione al miglioramento: mantenere uno spirito di aggiornamento continuo.

La formazione deve diventare parte integrante della cultura organizzativa: non un evento, ma un processo. Ciò implica creare contenuti sempre attuali, offrire percorsi differenziati per ruolo e livello, e adottare sistemi capaci di monitorare il progresso individuale e proporre stimoli personalizzati.

La formazione continua non deve essere un mero adempimento normativo né costituire un costo legato all'immagine aziendale, costituisce un investimento strategico che produce ritorni tangibili quale l'aumento dell'efficienza operativa, la riduzione dei costi a lungo termine (prevenzione errori, gestione efficace delle criticità), fidelizzazione del personale (crescita professionale, soddisfazione lavorativa, riduzione del turnover).

DALLA TEORIA ALLA PRATICA: TRE LIVELLI FORMATIVI

Per essere realmente trasformativa, la formazione in ambito cybersecurity deve agire su tre livelli:

- Sapere: fornire conoscenze teoriche, comprensione delle minacce e dei concetti fondamentali della sicurezza.
- Saper fare: sviluppare abilità operative, come il riconoscimento di un attacco o la gestione sicura delle credenziali.
- Saper essere: interiorizzare un comportamento sicuro, proattivo e adattivo, che diventa parte della propria identità digitale.

Questi tre livelli devono essere trattati in sinergia. La conoscenza fine a sé stessa è sterile se non si traduce in azione. Al tempo stesso, l'azione rischia di essere inefficace se non è supportata da una comprensione adeguata. La vera padronanza nasce dall'equilibrio tra conoscenza, abilità e atteggiamento.
Per trasformare la formazione da esercizio teorico a leva di cambiamento concreto, la tabella 10 propone una declinazione delle aree tematiche maggiormente connesse alla NIS2 nei tre livelli descrivendo la conoscenza di base necessaria, le abilità operative che devono essere allenate sul campo e l'atteggiamento - il mindset, i valori, i comportamenti - che dovrebbe essere stimolato e affinato per trasformare la pratica in abitudine organizzativa.
Per rendere operativi e misurabili i tre livelli formativi – sapere, saper fare, saper essere – è utile mappare le figure organizzative coinvolte nella sicurezza informatica con le competenze attese, i contenuti formativi specifici e le modalità didattiche più efficaci per ciascun profilo. La matrice seguente integra le esigenze formative delle aree tematiche destinate a diversi target aziendali, con gli approcci cognitivi e modalità formative, con l'obiettivo di facilitare la progettazione di percorsi formativi personalizzati, coerenti con i ruoli e capaci di produrre impatti reali su comportamenti e cultura organizzativa.

CONCLUSIONI: VERSO UNA NUOVA CULTURA DELLA SICUREZZA

Il cambiamento culturale è il traguardo ultimo di una formazione avanzata. Una cultura della sicurezza informatica diffusa e condivisa si manifesta in comportamenti coerenti, attenzione quotidiana ai rischi, capacità di collaborare per la protezione collettiva. Così come è avvenuto per le cinture di sicurezza — da imposizione normativa a gesto automatico per ogni automobilista — anche la sicurezza informatica dovrà evolvere da semplice obbligo a riflesso spontaneo: bloccare lo schermo, usare l'autenticazione forte o segnalare un'e-mail sospetta dovranno diventare atti naturali, radicati nella quotidianità digitale di tutti.
Per arrivare a questo risultato serve una strategia formativa integrata che:

- Alleni la mente a gestire l'incertezza, trasformando il cambiamento in occasione di apprendimento.
- Renda l'utente protagonista, capace di riconoscere, reagire e prevenire.
- Promuova un mindset antifragile, in grado di rafforzarsi di fronte alle difficoltà.
- Utilizzi la tecnologia non solo come contenitore, ma come alleato intelligente nel processo formativo.

Una tale formazione non è statica né standardizzata: è un organismo vivo, capace di adattarsi alle esigenze individuali e organizzative, alla maturità dei discenti e alle evoluzioni dello scenario.
Costruire una formazione avanzata in ambito Security Awareness significa progettare un ecosistema in cui l'individuo non è destinatario passivo, ma agente attivo del proprio apprendimento. Significa

Tabella 10 - Conoscenze per Aree Tematiche

Aree tematiche	Sapere (conoscere)	Saper fare (applicare)	Saper essere (integrare)
Evoluzione della cybersecurity	• Breve storia della sicurezza iformatica • Triade della sicurezza • Deepweb, darkweb, ethical hacking • Etica • Framework e standard (ISO27001, NIST CSF)	• Analizzare trend e valutare impatti sul contesto specifico • Aggiornare policy	• Mentalità di apprendimento continuo • Gestione del cambiamento tecnologico
Cyber-risk & compliance	• Direttiva NIS2, GDPR, AI ACT • DPIA, FRIA • Modelli di risk management	• Conduzione risk assessment • Mappatura responsabilità e accountability • Definizione misure di mitigazione del rischio	• Cultura del rischio e trasparenza • Responsabilità verso stakeholder e autorità
Incident & crisis management	• Ciclo di vita dell'incidente (NIST 800.61) • Ruoli CSIRT, forensics di base • Best practice di crisis communication	• Contenimento, eradication, recovery • Redigere rapporti forensi e lezioni apprese	• Prontezza decisionale • Collaborazione interfunzionale
Tecniche d'attacco e prevenzione	• Phishing, ransomware, social engineering • Assets, Minacce • Attack tree • Crittografia	• Riconoscere indicatori di compromissione • Applicare misure	• Vigilanza attiva e segnalazione tempestiva • Abitudini di cyber-hygiene quotidiana
Aspetti giuridici e proprietà intellettuale	• Reati informatici e responsabilità penali • Protezione IP, copyright, segreti • Obblighi di log e conservazione prove	• Gestire dati secondo principi di liceità e minimizzazione • Garantire catena di custodia forense	• Etica professionale e rispetto della privacy • Accountability

sviluppare percorsi che combinano rigore scientifico, empatia didattica e innovazione tecnologica, con l'obiettivo di costruire una vera competenza difensiva. Questi elementi di "cultura aziendale" devono però necessariamente partire dal Board e dagli apicali delle aziende per trasmettere l'importanza e la necessità di evolvere tutti insieme verso una postura più resiliente.
Nel mondo digitale, sapere non basta. È necessario saper fare. E, soprattutto, saper essere.
La NIS2 ha sicuramente rivoluzionato non solo l'approccio alla protezione aziendale della sicurezza informatica, ma soprattutto l'organizzazione delle aziende. Ad esempio, e per tutti, gli organi di am-

Tabella 11 - Aree formative suddivise per ruoli aziendali

Target	Aree tematiche					Modalità formative consigliate
	Evoluzione della cybersecurity	Cyber-risk & compliance	Incident & crisis management	Tecniche d'attacco e prevenzione	Aspetti giuridici e proprietà intellettuale	
Direzione Generale						• Storytelling immersivo • Problem-solving • Supporto proattivo
CISO						• Percorsi multilivello • Formazione esperienziale • Apprendimento conversazionale
DPO						• Educational language • Problem-solving • Microlearning
CSIRT Interno						• Formazione esperienziale • Esercitazioni interattive • Supporto proattivo
Responsabili di funzione[4]						• Time-spaced learning • Microlearning • Apprendimento conversazionale
Personale sanitario[5] (non ICT)						• Educational language • Storytelling immersivo • Gamification

[4] ICT, Qualità, Rischi, Marketing

[5] La formazione per il personale sanitario richiede un ulteriore livello di approfondimento che possa permettere di personalizzare i contenuti in funzione dello specifico ambito operativo (emergenza-urgenza, territorio, ospedale, ...) e ruolo (medico, infermiere, tecnico, amministrativo, ...). Tale approfondimento devo poi essere poi valutato in termini di fattibilità e sostenibilità economica nel contesto di contenimento dei costi tipico del periodo attuale della sanità italiana.

Target	Aree tematiche					Modalità formative consigliate
	Evoluzione della cybersecurity	Cyber-risk & compliance	Incident & crisis management	Tecniche d'attacco e prevenzione	Aspetti giuridici e proprietà intellettuale	
Referenti NIS2 / Audit locali						• Dibattito strutturato • Problem-solving • Formazione esperienziale
Sviluppatori interni						• Percorsi multilivello • Gamification • Formazione esperienziale
Fornitori software, dispositivi medici						• Problem-solving • Apprendimento conversazionale • Supporto proattivo
Persone assistite / Cittadine e cittadini						• Microlearning • Educational language • Storytelling immersivo
Legenda		Base	Conoscenza introduttiva e orientamento al tema.			
		Avanzato	Conoscenza e applicazione operativa. *Il livello avanzato può essere necessario solo per alcuni sotto argomenti specifici all'interno dell'area tematica.*			
		Esperto	Padronanza completa, capacità di leadership e mentorship. *Il livello avanzato può essere necessario solo per alcuni sotto argomenti specifici all'interno dell'area tematica.*			

ministrazione e controllo non possono più limitarsi a delegare la cybersicurezza alle funzioni IT, ma devono assumere un ruolo attivo nella definizione delle strategie di protezione e resilienza.
In quest'ottica, può essere utile ispirarsi al framework proposto da Spitz e Desbiey [13], che sintetizza le tre capacità fondamentali per affrontare un contesto incerto e dinamico: Anticipazione, Agilità e Antifragilità. Tre direttrici che, se integrate nella formazione e nella governance, possono sostenere una postura più evoluta, adattiva e robusta – non solo per rispondere alle minacce, ma per crescere attraverso di esse.

Alcune considerazioni tecniche

Introduzione

Raccogliamo in questo capitolo alcune considerazioni prettamente tecniche che sono desumibili dalla lettura della Direttiva NIS2, la quale, in modo analogo a quanto già successo con il GDPR, non ha come scopo principale quello di dare indicazione tecniche concrete, probabilmente nella consapevolezza della velocità di cambiamento e della continua nascita di novità nel mondo delle tecnologie informatiche. La Direttiva si concentra più su processi, procedure, ruoli, formazione e così via, ovvero su come gestire in modo corretto la parte tecnica e quella non tecnica.
ACN ha voluto fornire delle linee guida che facessero da complemento alla Direttiva, pubblicando una determina che è invece ricca di indicazioni tecniche anche molto specifiche.
Questa determina è già stata analizzata nei precedenti capitoli e richiede sicuramente, allo stato delle cose, ulteriori confronti e approfondimenti.
Qui invece cerchiamo di illustrare ed analizzare quelle indicazioni tecniche più basilari e già ricavabili dalla Direttiva.

Gestione delle vulnerabilità

La gestione delle vulnerabilità è un processo strategico e continuo volto ad identificare, valutare e correggere le debolezze tecniche che compromettono la sicurezza dei sistemi informativi. Per una gestione efficace, è opportuno usare metodi di classificazione del rischio come il calcolo del CVSS (Common Vulnerability Scoring System) o dell'EPSS (Exploit Prediction Scoring System) e affidarsi a fonti di informazione affidabili come il CERT, l'ENISA, il CSIRT o gli stessi produttori di software e hardware; inoltre è fondamentale pianificare delle scansioni di vulnerabilità periodiche documentandone i risultati.
Tale processo deve essere anche integrato con una serie di altri processi: il change management, la distribuzione di patch, la valutazione dei rischi e la risposta agli incidenti.
Per ogni fase del processo devono essere chiaramente definiti ruoli e le responsabilità e, in particolare, per garantire una risposta efficace, va nominato il punto di contatto unico per la sicurezza IT, per un buon coordinamento interno ed esterno, anche con i fornitori.
Inoltre va creata una procedura per la divulgazione coordinata delle vulnerabilità (CVD) che permetta di segnalare tempestivamente le vulnerabilità.
Se le vulnerabilità sono critiche, bisogna elaborare ed attuare un piano di mitigazione. Se invece si decide di non intervenire, occorre documentare in maniera esaustiva e coerente i motivi di tale decisione.

I canali di monitoraggio delle vulnerabilità devono essere revisionati almeno ogni sei mesi e l'elenco delle fonti informative deve essere aggiornato periodicamente.
I fornitori devono essere contrattualmente vincolati a notificare eventuali vulnerabilità che riguardano servizi e prodotti finiti.
Infine è raccomandabile effettuare delle scansioni straordinarie in caso di incidenti o modifiche sostanziali ai sistemi, mantenere registri delle azioni correttive e sottoporre il processo a verifiche interne periodiche.
Una gestione delle vulnerabilità che sia efficace, contribuisce alla prevenzione e riduzione dei rischi (si veda il capitolo 6 della guida ENISA [11]).
Dal punto di vista del monitoraggio e della gestione di log si consiglia di implementare una scansione periodica delle vulnerabilità e, in particolare, di monitorare i nuovi report di vulnerabilità pubblicati per qualsiasi componente software libero e open source utilizzato dall'ente (si veda il paragrafo 3.2 della guida ENISA [11]).

Backup e DR

FINALITÀ E AMBITO DI APPLICAZIONE

Lo scopo principale di un sistema di backup e di disaster recovery è la protezione dei dati. In sostanza, crea copie di sicurezza dei dati per poterli ripristinare in caso di perdita o corruzione dei file originali.
Le sue finalità principali sono:

- il ripristino da fallimenti hardware o software,
- il ripristino da errori umani,
- la protezione da attacchi informatici,
- la continuità operativa,
- la conformità normativa.

RUOLI E RESPONSABILITÀ

Per una corretta gestione del sistema di backup e di disaster recovery occorre definire gli ordini di intervento e strutturare dei gruppi operativi che definiscano i diversi livelli che compongono la catena decisionale, in ordine gerarchico:

- Decisore: singola persona delegata o gruppo di direzionale che decide il momento nel quale attivare le procedure di ripristino al punto precedente.
- Referenti sistemistici (suddivisi in almeno due sottogruppi sistemi centrali e periferia): operatori formati e autorizzati all'attivazione pratica delle procedure.
- Referenti applicativi: operatori formati e autorizzati alla verifica del buon esito delle operazioni di cui sopra prima del rilascio in produzione.
- Referenti operativi: operatori formati e autorizzati afferenti alla linea di produzione che si configurano come interfacce con i referenti applicativi.

La catena operativa sopra indicata decide ed implementa le varie tipologie di recupero da disastro

e pertanto dovrà essere strutturata per fornire una disponibilità coerente con i livelli di servizio, ad esempio di caso di copertura 24x7 o di reperibilità.

I CONTATTI PRINCIPALI E I CANALI DI COMUNICAZIONE (INTERNI ED ESTERNI)

I quattro ruoli indicati devono essere associati a recapiti validati e condividere almeno due canali di comunicazione disgiunti, per essere resilienti al disservizio stesso (sistemi di chat/mail associati a canali standard telefonici, potenzialmente anche con telefonia tradizionale).
Occorre definire internamente al piano di recupero anche la catena comunicativa con tutti gli attori coinvolti nella procedura per mantenere un adeguato allineamento informativo sull'avanzamento del ripristino.
Si sottolinea come i canali comunicativi debbano essere scelti sulla base del criterio di indipendenza rispetto all'ambito tecnologico che è oggetto del piano di ripristino.

LE RISORSE NECESSARIE

In situazione critica occorre innanzitutto verificare la disponibilità operativa dei sistemi di backup e DR, e, di conseguenza, i referenti sistemistici propongono al "decisore" le strategie percorribili e l'ordine di ripristino dell'operatività tecnica; l'ordine dev'essere già stato analizzato e predisposto nel piano di recupero da disastro tenendo conto sia delle priorità sia dell'interoperabilità delle componenti della catena produttiva.

LE CONDIZIONI PER L'ATTIVAZIONE E LA DISATTIVAZIONE DEL PIANO

Su impianti produttivi di elevata complessità il ruolo di Decisore dovrà essere costituito da almeno due membri/gruppi; uno afferente alla Direzione ICT per le decisioni di carattere prettamente tecnico e l'altro alla Direzione Aziendale per tutti gli altri tipi di decisioni (produttive, rapporto con il personale, rapporto con i pazienti, ...).

LINEE GUIDA PER I PIANI OPERATIVI

Devono essere garantiti riservatezza, integrità, disponibilità ed RTO e RPO coerenti con i livelli di servizio e con i piani di continuità operativa.
Deve essere definito un workflow dei backup e del disaster recovery coerente con il modello ISO/OSI e che garantisca già nella fase iniziale il funzionamento dei sistemi fino al livello 3 di sessione (senza il quale tutto il resto non può funzionare).
Occorre pertanto implementare un impianto di recupero o di bypass dei sistemi che garantiscono il livello di sessione, con un backup e/o una ridondanza offline delle configurazioni dei sistemi critici come firewall, IDS, IPS, NAC, switch, eccetera.
Occorre valutare il mantenimento di almeno un telefono tradizionale in ogni unità produttiva come ad esempio i sistemi radio di emergenza dove i concetti di recupero da disastro si estendono a tutte quelle condizioni ambientali che producono gli stessi effetti: rischio idrico, incendio, terremoti, pandemie, eccetera.
Occorre valutare attentamente il prodotto utilizzato per i sistemi di backup e disaster recovery in

termini di affidabilità e sensibilità del produttore nei confronti della Cybersecurity, dismettendo e sostituendo ovviamente i sistemi fuori supporto.

RISERVATEZZA E DISPONIBILITÀ

Le seguenti caratteristiche del sistema di backup e disaster recovery sono fortemente raccomandate.

- Autenticazione MFA per soggetti autorizzati alla gestione del backup
- Sistemi di backup ad almeno due livelli disgiunti di autorizzazione
- Cifratura
- Integrità e Coerenza backup e DR
- Backup immutabile o distaccato periodicamente dalla rete - offline (Immutabilità assicura la disponibilità e Isolamento - Cassaforte)
- Test periodico backup e DR
- Log del backup
- Revisione periodica delle politiche di Backup e DR, in ragione almeno annuale.
- Implementare soluzioni per ridurre il rischio di attacchi informatici automatizzando le strategie di ripristino e continuità aziendale; alcuni strumenti possono rilevare e difendere da minacce isolando i dati critici, identificano attività sospette (accelerando il ripristino dei dati)
- Analisi dei contenuti per rilevare il danneggiamento dei dati associato all'apprendimento automatico che monitora i cambiamenti nei dati e rileva segni di corruzione indicativi di attacchi ransomware

MIGLIORAMENTO DEI PARAMETRI RTO E RPO

Si suggerisce, laddove possibile e anche sui sistemi già in uso o da inserire come prerogativa nella catena di approvvigionamento, una configurazione logica del dato da proteggere che permetta uno snellimento del sistema minimale necessario alla ripresa operativa.

- Dato statico storicizzato su sistemi con SLA meno stringenti.
- Dato dinamico, necessario a ripristino dell'operatività, con SLA più stringenti.
- Gestione dei rischi per la sicurezza informatica della catena di approvvigionamento.
- Coerenza dei piano di backup e DR per protezione da attacchi logici ai dati.

IAM, PAM, MFA

IAM - IDENTITY AND ACCESS MANAGEMENT

Un sistema di Identity e Access Management è un software o un insieme di processi e tecnologie che permette una migliore gestione delle identità digitali e un migliore controllo degli accessi alle risorse di un'organizzazione.

Svolge un ruolo cruciale nella sicurezza informatica aziendale garantendo che solo gli utenti autorizzati abbiano accesso alle risorse sensibili: aiuta a prevenire accessi non autorizzati, riduce il rischio di violazioni dei dati e assicura la conformità alle normative di sicurezza.

In pratica, serve a garantire che le persone giuste (o i sistemi giusti) abbiano l'accesso appropriato alle risorse giuste, al momento giusto e per i motivi giusti.
Le funzioni principali che deve garantire:

- gestione delle identità: creazione, modifica e cancellazione degli account utente (conformità con la misura PR.AA-01)
- autenticazione: verifica dell'identità di un utente, es. tramite password o token (conformità con la misura PR.AA-03)
- autorizzazione: definizione di cosa può fare un utente una volta autenticato, es. accesso ad applicazioni, database, ecc. (conformità con la misura PR.AA-05)
- gestione dei privilegi: assegnazione di ruoli e permessi in base alle funzioni lavorative (conformità con la misura PR.AA-05)
- audit e conformità: tracciamento delle attività degli utenti per motivi di sicurezza e rispetto delle normative (conformità con la misura PR.PS-04)

È fortemente consigliato che sia affiancato da ulteriori tecnologie come l'autenticazione a più fattori (MFA in conformità con la misura PR.AA-03 punto 2) e il monitoraggio continuo delle attività degli utenti (SIEM e sistemi MDR, vedi DE.CM-01) per rafforzare ulteriormente la sicurezza.
Integrandolo con le fonti di autenticazione è possibile implementare un meccanismo di Single Sign-On (SSO) che permetta l'accesso a più sistemi con un solo login, gestendo le abilitazioni in maniera centralizzata. Indispensabile per garantire le disabilitazioni a tutti i livelli, spesso eseguite solo a livello di fonte di autenticazione e non capillarmente sugli applicativi.

PAM - PRIVILEGED ACCESS MANAGEMENT

Un sistema PAM (Privileged Access Management) è una soluzione di sicurezza informatica progettata per gestire, controllare e monitorare gli accessi privilegiati all'interno di un'organizzazione, cioè gli account che hanno accesso elevato a sistemi critici, come amministratori di sistema, database, reti o applicazioni sensibili. Questa tipologia di utenti è spesso un obiettivo primario per attacchi informatici, date le notevoli abilitazioni di cui è in possesso.
Il suo scopo è assicurare che solo gli utenti autorizzati possano accedere e operare su risorse sensibili, veicolando accessi, implementando vincoli e registrando le sessioni.
Le funzionalità che un PAM mette a disposizione sono:

- gestione delle credenziali privilegiate: rotazione automatica delle password e password vaulting
- accessi just-in-time: accesso temporaneo e controllato
- controllo degli accessi basato su policy
- session management: monitoraggio e registrazione delle sessioni
- generazione di audit e reportistica per dimostrare la conformità a normative

Come funzionalità desiderate aggiuntive possiamo elencare:

- possibilità di impostare comandi o applicazioni proibite agli utenti
- invio di segnalazioni in caso siano rilevate azioni specifiche

Come per le soluzioni IAM, è fortemente consigliato che l'accesso sia protetto da autenticazione a più fattori (MFA in conformità con la misura PR.AA-03 punto 2). Per aumentare il livello di sicurezza

delle utenze locali dei sistemi è consigliabile che queste siano dedicate a ciascun sistema, evitando la presenza di utenze con medesima password su sistemi differenti.
Un sistema PAM si integra con la direttiva NIS2 in vari ambiti:

- permette di controllare chi ha accesso a cosa, quando e per quanto tempo (conformità con le misure PR.AA-01 e PR.AA-03)
- registra e monitora tutte le attività degli utenti privilegiati (conformità con la misura PR.PS-04)
- limita i privilegi solo al necessario, perseguendo il principio del minimo privilegio (conformità con la misura PR.AA-05)
- si integra nelle attività di monitoraggio continuo delle attività degli utenti (SIEM e sistemi MDR, vedi DE.CM-01)

Crittografia e Cifratura

Nel contesto dell'evoluzione digitale della sanità, la protezione dei dati sensibili dei pazienti rappresenta una priorità assoluta. Le informazioni sanitarie richiedono misure di sicurezza avanzate, tra cui la crittografia e la cifratura, per garantire la riservatezza, l'integrità e l'autenticità dei dati.
Nel linguaggio comune i due termini sono spesso usati come sinonimi, ma in ambito tecnico si distinguono:

- **Cifratura:** è il processo tecnico di trasformazione dei dati leggibili (plaintext) in un formato illeggibile (ciphertext), utilizzando un algoritmo e una chiave. Serve a proteggere i dati da accessi non autorizzati.
- **Crittografia:** è la disciplina più ampia che studia le tecniche di protezione delle informazioni, e include non solo la cifratura ma anche meccanismi come la firma digitale, l'autenticazione, la gestione delle chiavi, ecc.

Di seguito si riportano alcune delle principali applicazioni.

Sicurezza delle reti: proteggere il perimetro digitale

Negli ambienti sanitari, i dati transitano continuamente tra dispositivi, server, cloud e terminali utente. La sicurezza delle reti è quindi il primo baluardo contro le minacce. Le misure più efficaci includono:

- **VPN (Virtual Private Network)** per la connessione sicura tra sedi remote o tra il personale e i sistemi aziendali.
- **Firewall avanzati e sistemi IDS/IPS** per identificare e prevenire attacchi.
- **Segmentazione della rete** in modo da isolare i sistemi critici (come cartelle cliniche elettroniche) da quelli non sanitari.

Le VPN, ad esempio, creano un tunnel crittografato tra il dispositivo dell'utente e il server della rete, proteggendo i dati in transito da intercettazioni e manipolazioni. I protocolli di crittografia più utilizzati includono:

- **IPSec (Internet Protocol Security):** garantisce la cifratura dei pacchetti IP e l'autenticazione tra le parti.

- **OpenVPN:** molto usato per la sua flessibilità, utilizza TLS/SSL per stabilire connessioni sicure.
- **WireGuard:** protocollo moderno, più snello ed efficiente, che utilizza algoritmi crittografici avanzati come ChaCha20.

HTTPS: la base della comunicazione sicura

La comunicazione HTTPS (HyperText Transfer Protocol Secure) è oggi lo standard per proteggere il traffico tra client e server, in particolare su portali sanitari, telemedicina e sistemi di prenotazione. HTTPS utilizza:

- **Protocollo TLS (Transport Layer Security),** che garantisce cifratura dei dati, autenticazione del server e integrità del contenuto.
- **Certificati digitali,** rilasciati da autorità di certificazione (CA), per verificare l'identità dei soggetti coinvolti.

In ambito sanitario, l'uso di HTTPS è fondamentale per evitare intercettazioni (man-in-the-middle) e accessi non autorizzati durante la trasmissione dei dati.

Firma digitale: autenticità e non ripudio

La firma digitale è un meccanismo crittografico che permette di:

- Verificare l'identità del mittente (autenticità).
- Garantire che il documento non sia stato alterato (integrità).
- Evitare il disconoscimento della paternità del documento (non ripudio).

Nel settore sanitario italiano, la firma digitale è ampiamente usata per firmare referti medici, prescrizioni elettroniche, documenti clinici e consensi informati, anche attraverso strumenti come SPID, CIE o CNS.

Crittografia dei dati a riposo e in transito

Oltre alla cifratura dei dati in transito (es. tramite HTTPS), è essenziale proteggere i dati a riposo, ovvero quelli memorizzati su dischi rigidi, database e cloud:

- **Crittografia full-disk (FDE)** per proteggere dispositivi mobili e server.
- **Crittografia a livello di database,** per tutelare solo determinati campi sensibili (es. diagnosi).
- **Key management systems (KMS)** per una gestione sicura delle chiavi di cifratura.

Autenticazione sicura e gestione crittografica delle credenziali

Un elemento fondamentale nella sicurezza informatica sanitaria è il controllo degli accessi, che si basa su meccanismi di autenticazione robusti per garantire che solo utenti autorizzati possano accedere ai sistemi e ai dati sensibili. Le modalità di autenticazione sicura più comuni includono:

- **Autenticazione a due fattori (2FA) o a più fattori (MFA):** combina qualcosa che l'utente conosce (es. password) con qualcosa che possiede (es. token OTP, smart card) o è (es. impronta digitale). È largamente usata in contesti sanitari per l'accesso a portali di telemedicina o referti.
- **Autenticazione con certificato digitale:** il sistema verifica l'identità dell'utente tramite certificati, spesso contenuti in dispositivi come la Carta Nazionale dei Servizi (CNS) o smart card professionali per i medici.

- **Single Sign-On (SSO):** consente l'accesso a più sistemi attraverso un'unica autenticazione, semplificando l'esperienza utente e riducendo i rischi legati alla gestione di molteplici password.

Tutti questi metodi si basano su protocolli crittografici per proteggere le credenziali durante la trasmissione e l'autenticazione.

È bene tenere in considerazione i due principi generali più comunemente utilizzati:

- need-to-know: a un'entità viene concesso l'accesso solo alle informazioni necessarie per svolgere i propri compiti (compiti o ruoli diversi comportano diverse informazioni need-to-know e quindi diversi profili di accesso);
- need-to-use: a un'entità viene assegnato l'accesso all'infrastruttura informatica solo in presenza di una chiara necessità.

Si considerino i seguenti aspetti quando si specificano le regole di controllo degli accessi:

- stabilire regole basate sul presupposto del privilegio minimo ("tutto è generalmente vietato a meno che non sia espressamente consentito") piuttosto che sulla regola più debole ("tutto è generalmente consentito a meno che non sia espressamente vietato");
- modifiche alle autorizzazioni utente avviate automaticamente dalla rete e dal sistema informativo e quelle avviate da un amministratore di sistema;
- quando definire e rivedere regolarmente l'approvazione.

Valutare le modalità di implementazione del controllo degli accessi, come il controllo degli accessi obbligatorio (MAC), il controllo degli accessi discrezionale (DAC), il controllo degli accessi basato sui ruoli (RBAC) e il controllo degli accessi basato sugli attributi (ABAC), a seconda delle esigenze aziendali.

Tenere presente che le regole di controllo degli accessi possono contenere anche elementi dinamici (ad esempio una funzione che valuta gli accessi passati o specifici valori ambientali, si veda il paragrafo 11.1 della guida ENISA [11]).

Salvataggio sicuro delle password: hash e salt

Il salvataggio delle password in chiaro rappresenta un grave rischio di sicurezza. Per proteggere le credenziali archiviate, si utilizza una combinazione di hash crittografico e salt:

- **Hash:** è una funzione unidirezionale che trasforma la password in una stringa apparentemente casuale (es. con algoritmi come SHA-256). Una volta applicato l'hash, la password originale non è più recuperabile.
- **Salt:** è un valore casuale aggiunto alla password prima dell'hash, unico per ogni utente, e serve ad evitare attacchi con rainbow table, che usano dizionari precomputati di hash comuni, e a rendere unici gli hash anche per password identiche, impedendo agli attaccanti di riconoscere utenti che usano la stessa password.

La corretta implementazione di queste tecniche è un requisito fondamentale per la sicurezza degli applicativi sanitari.

La gestione operativa della crittografia deve includere delle misure che garantiscano l'accessibilità e la continuità dei sistemi crittografici. In caso di perdita delle chiavi crittografiche, l'organizzazione deve garantire la possibilità di accedere o recuperare i dati protetti, per esempio mediante l'utilizzo di sistemi

di escrow. È possibile tenere in considerazione anche l'aspetto relativo all'agilità crittografica, ovvero progettare i sistemi in modo flessibile per poter aggiornare gli algoritmi e protocolli tenendo conto di evoluzioni come la crittografia post quantistica (si veda il paragrafo 9.2 della guida ENISA [11]).
Un ulteriore aspetto riguarda la gestione della crittografia, che deve essere regolata da una politica specifica e aggiornata. Deve essere riesaminata almeno una volta l'anno oppure nel momento in cui vengono attuati dei cambiamenti significativi a livello normativo e tecnologico. Deve inoltre essere testata prima dell'introduzione di nuove misure, comunicata chiaramente al personale e anche integrata con attività formative specifiche, per accrescere la consapevolezza dei dipendenti sul corretto utilizzo degli strumenti crittografici e sull'importanza della protezione dei dati (si veda il paragrafo 9.1 della guida ENISA [11]).

Formazione obbligatoria

La Direttiva NIS2 impone obblighi formativi specifici per rafforzare la sicurezza informatica nei soggetti pubblici e privati classificati come essenziali o importanti.
Nello specifico l'articolo 20 comma 2 del capo IV sulle misure di gestione del rischi di cybersicurezza e obblighi di segnalazione, riporta che "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" al fine di acquisire "conoscenze e competenze sufficienti al fine di individuare i rischi e valutare le pratiche di gestione dei rischi di cybersicurezza e il loro impatto sui servizi offerti dal soggetto".
Di conseguenza la formazione per i membri dell'organo di gestione, che in ambito sanitario si può ricondurre alla direzione strategica, unitamente ai direttori di distretto, di presidio, di dipartimento ed eventualmente di UOC, deve fornire le conoscenze e le competenze per comprendere e valutare i rischi legati alla cybersicurezza, in modo da poter partecipare attivamente alla definizione delle strategie di sicurezza informatica dell'organizzazione, avendo ben presenti le responsabilità legali e operative in caso di incidenti.
In altre parole, i vertici aziendali non possono limitarsi a delegare completamente al servizio ICT la sicurezza informatica, ma piuttosto devono formarsi per guidare le strategie e le decisioni in materia di protezione digitale, potendo quindi comprendere i rischi e le minacce informatiche, integrando la sicurezza nelle politiche aziendali e allocando le adeguate risorse economiche, umane e tecnologiche.
In particolare, è prevista una formazione approfondita e mirata per i vertici aziendali che include non solo contenuti tecnici aggiornati, ma anche esercitazioni pratiche di risposta agli attacchi informatici.
È inoltre fondamentale tenere traccia della partecipazione, dei materiali usati e dei risultati delle valutazioni. I programmi formativi devono essere rivisiti annualmente e adattati in base a cambiamenti organizzativi e tecnologici (si veda il paragrafo 8.2 della guida ENISA [11]).
Tutto questo senza perdere di vista che la mancata formazione o l'inosservanza degli obblighi può comportare sanzioni significative per l'organo direttivo, in quanto responsabile della gestione del rischio cyber.

Per i dipendenti le finalità sono leggermente diverse. La formazione deve essere mirata a promuovere la cultura della sicurezza, responsabilizzando tutti i componenti dell'azienda affinché venga condivisa una mentalità orientata alla protezione dei dati e dei sistemi.
Di conseguenza, in questo caso, l'obiettivo è aumentare la consapevolezza dei rischi informatici, ovvero mettere i dipendenti nelle condizioni di riconoscere minacce comuni come phishing, malware, ransomware e attacchi social engineering, limitando quindi gli errori umani da cui scaturiscono l'80% degli attacchi.
Le attività formative possono svolgersi mediante webinar, moduli online o incontri in aula, supportati da strumenti comunicativi come e-mail aziendali o intranet. Al termine della formazione possono essere previsti quiz, simulazioni o test di apprendimento utili a verificarne l'efficacia (si veda il paragrafo 8.1 della guida ENISA [11]).
Avere dipendenti formati permette di essere in grado di reagire tempestivamente e correttamente in caso di incidente, contribuendo a limitare i danni e aumentare la resilienza dell'organizzazione.

OBIETTIVI E QUADRO NORMATIVO

Ci proponiamo di fornire un quadro operativo chiaro e completo per l'implementazione di programmi formativi in materia di sicurezza informatica, in linea con quanto previsto dalla Direttiva NIS2. L'intento è assicurare che tutto il personale coinvolto nella gestione e nell'utilizzo dei sistemi digitali aziendali sia adeguatamente preparato a prevenire, riconoscere e affrontare efficacemente i rischi informatici.
La Direttiva NIS2 impone agli enti essenziali e importanti di adottare misure tecniche e organizzative, tra cui la formazione continua del personale, per garantire un livello di sicurezza adeguato delle reti e dei sistemi informativi. In questo contesto, la formazione rappresenta un elemento fondamentale per rafforzare la resilienza informatica dell'organizzazione. Infatti, la carenza di consapevolezza e competenze specifiche è una delle principali vulnerabilità aziendali: errori umani, pratiche di igiene informatica insufficienti e una gestione non adeguata degli incidenti possono compromettere seriamente la sicurezza. Per questo motivo, la governance aziendale ha la responsabilità di promuovere una cultura della sicurezza, assicurandosi che i programmi formativi siano pianificati, attuati, monitorati e aggiornati regolarmente, con ruoli ben definiti e risorse dedicate.

DESTINATARI E LIVELLI DI FORMAZIONE

Per proteggere efficacemente l'organizzazione dai rischi informatici, è necessario investire in percorsi formativi differenziati, che si rivolgono a due livelli complementari: da un lato una sensibilizzazione generale rivolta a tutto il personale, personale operativo e vertici aziendali; dall'altro una formazione specialistica pensata per i ruoli tecnici e per coloro che operano in contesti a rischio elevato.
Il personale operativo composto da impiegati, amministrativi e collaboratori che utilizzano quotidianamente strumenti digitali, pur non avendo competenze tecniche specifiche, è spesso esposto a minacce comuni come phishing e malware. Per questo motivo, la formazione rivolta a questa categoria deve mirare a rafforzare la consapevolezza sui comportamenti a rischio e a fornire strumenti pratici per evitarli.
Il personale tecnico ICT, OT/SCADA e di ingegneria clinica include sistemisti, tecnici di rete, ingegn-

eri OT, operatori di infrastrutture critiche e tecnici specializzati nella gestione di dispositivi medici e sistemi sanitari. Questi professionisti richiedono una preparazione avanzata che copra aspetti quali la difesa informatica, la gestione delle vulnerabilità, la risposta agli incidenti e la sicurezza specifica dei sistemi SCADA e dei dispositivi clinici, spesso esposti ad attacchi sofisticati e persistenti. Tale formazione deve fornire competenze approfondite per garantire la protezione, la continuità operativa e l'integrità di sistemi critici sia industriali sia sanitari, riconoscendo le peculiarità e le interdipendenze di questi ambienti tecnologici.
Infine, l'alta direzione (CEO, CIO, CISO, Direttori Generali e membri del CdA) deve essere coinvolta attivamente nei programmi formativi. Solo così è possibile garantire un approccio strategico alla cybersecurity, con particolare attenzione alla governance del rischio, all'allocazione delle risorse e all'integrazione della sicurezza nelle decisioni aziendali.

MODALITÀ E CONTENUTI DELLA FORMAZIONE

La formazione di base rivolta al personale operativo ha come obiettivo principale lo sviluppo di una solida consapevolezza sui rischi digitali e la promozione di comportamenti sicuri nella quotidianità. È importante che anche i dirigenti partecipino a queste attività, in modo da diffondere un linguaggio e una cultura condivisi all'interno dell'organizzazione. I contenuti devono affrontare le minacce più comuni, come il phishing e l'uso di reti non protette, e fornire indicazioni pratiche sulle principali regole di igiene informatica: protezione delle credenziali, backup regolari, comportamenti sicuri in mobilità e nello smart working.
Per rendere la formazione efficace e accessibile, si possono utilizzare diversi strumenti, quali moduli e-learning, workshop in aula, brevi sessioni di microlearning e campagne di sensibilizzazione veicolate tramite email, intranet e newsletter aziendali. È fondamentale pianificare queste attività in modo ricorrente, includendo anche i nuovi assunti, e misurarne l'efficacia attraverso quiz, simulazioni e feedback, così da poter aggiornare costantemente i contenuti.
Per quanto riguarda il personale tecnico, la formazione deve essere più approfondita, tecnica e costantemente aggiornata. I corsi dovrebbero coprire competenze specifiche come la gestione delle vulnerabilità, l'hardening dei sistemi, il logging avanzato, la segmentazione di rete e l'adozione di architetture di sicurezza by design. Particolarmente utili sono le esercitazioni pratiche, le simulazioni in ambienti controllati, gli scenari di attacco e difesa (red/blue team) e i tabletop exercises multidisciplinari. Inoltre, la formazione deve essere obbligatoria per chi assume nuovi ruoli tecnici o partecipa a progetti che richiedono competenze in ambito sicurezza. La tracciabilità dei corsi, la conservazione dei materiali e la valutazione dei risultati sono elementi essenziali per garantire la qualità e la conformità del programma.
L'alta direzione, infine, ha un ruolo cruciale nel promuovere una cultura della sicurezza e nel definire le priorità strategiche. La formazione per questo gruppo deve fornire strumenti decisionali, una comprensione approfondita dei principali rischi ICT, nonché indicazioni su come integrare la sicurezza nei processi aziendali. È importante che gli executive sappiano valutare i rischi in termini di impatto sul business, comprendere i piani di continuità operativa e di crisis management, supervisionare le policy di sicurezza e monitorare le metriche di efficacia. Per raggiungere questi obiettivi, si suggerisce l'utiliz-

zo di formati specifici come executive briefing, workshop direzionali e tabletop exercises condivisi con le funzioni IT, OT e comunicazione. Inoltre, la formazione deve chiarire gli obblighi di accountability dei vertici e sottolineare l'importanza del loro coinvolgimento diretto, che rappresenta un esempio fondamentale per costruire una cultura della sicurezza solida e resiliente.

STRUMENTI, GOVERNANCE E MIGLIORAMENTO CONTINUO

Per assicurare l'efficacia della formazione, è fondamentale utilizzare strumenti aggiornati, contenuti riconosciuti a livello internazionale e collaborare con partner qualificati. Tra le risorse più affidabili si annoverano le linee guida di ENISA, AgID e CSIRT Italia, oltre a toolkit e manuali operativi messi a disposizione da enti pubblici. Si consiglia inoltre l'adozione di framework riconosciuti, come ISO/IEC 27001, NIST Cybersecurity Framework e CIS Controls, e l'integrazione di percorsi di certificazione professionale per il personale tecnico (ad esempio CEH, CISM, CISSP). Le aziende possono infine collaborare con università, enti di formazione accreditati, consorzi e fornitori specializzati per progettare percorsi personalizzati e sempre aggiornati.
Una governance efficace dei programmi formativi richiede una chiara definizione delle responsabilità, una pianificazione strutturata e un sistema di monitoraggio continuo. Ogni organizzazione dovrebbe nominare un responsabile o un comitato incaricato di coordinare il piano annuale di formazione in cybersecurity, che copra l'intero ciclo di vita del dipendente, dall'onboarding agli aggiornamenti periodici. Il monitoraggio deve includere la tracciatura della partecipazione, l'analisi delle performance formative e audit regolari per verificare la qualità e l'efficacia del programma. La reportistica interna consente di misurare il ritorno dell'investimento formativo e di orientare eventuali interventi correttivi.
In conclusione, una formazione diffusa, mirata e ben governata rappresenta un elemento chiave per la resilienza informatica aziendale. Differenziare i contenuti in base ai ruoli, garantire la ciclicità delle attività formative e assicurare l'impegno diretto della governance sono condizioni imprescindibili per il successo dei programmi. Si raccomanda di adottare un piano annuale strutturato, nominare responsabili dedicati, tracciare le attività e definire indicatori di performance (KPI). Coinvolgere partner esterni per aggiornamenti e benchmarking può ulteriormente rafforzare l'efficacia del percorso formativo. Infine, il programma deve essere dinamico e in continua evoluzione, adattandosi alle nuove minacce, all'esperienza maturata e alle normative vigenti, per mantenere sempre alta la qualità e la rilevanza delle attività.

Linee Guida ENISA

Nel testo abbiamo fatto più volte riferimento alle linee guida pubblicate da ENISA nel giugno del 2025 e che ambiscono, a livello dell'Unione Europea, ad essere il riferimento per la sicurezza informatica.

ENISA NIS360

La guida ENISA NIS360 offre una visione strategica e multisettoriale della resilienza digitale nell'Unione Europea, evidenziando le vulnerabilità sistemiche e le priorità di sicurezza nel contesto sanitario.

In particolare, il settore sanitario viene collocato nella fascia superiore dell'intervallo di maturità "moderata" e a un livello intermedio in tutte le classifiche di maturità. Con la direttiva NIS2, l'ambito di applicazione del settore è stato ampliato in modo significativo, aggiungendo complessità a un settore già altamente eterogeneo.
Il settore sanitario affronta sfide significative in materia di cybersicurezza a causa dell'eterogeneità delle sue entità, dispositivi e tecnologie, con molte organizzazioni che faticano ad adottare misure di sicurezza di base, per carenza di risorse e pratiche obsolete.
Potrebbe essere opportuno:

- Sviluppare delle linee guida pratiche tenendo conto delle sue sfide uniche, come la varietà di entità, dispositivi e tecnologie.
- Lanciare campagne di sensibilizzazione per rafforzare la cultura della cybersicurezza, poiché, anche quando le entità effettuano valutazioni del rischio e implementano buone pratiche, questi sforzi risultano incoerenti a livello settoriale. Molte organizzazioni non hanno una chiara comprensione dei propri asset critici, dei rischi informatici correlati e delle strategie efficaci per mitigarli.

AREE DI MIGLIORAMENTO

- Chiarire l'interazione e le sinergie tra la Direttiva NIS2 e il Regolamento sui dispositivi medici, insieme ad altre iniziative politiche come:
  - l'AI Act,
  - il Cyber Resilience Act,
  - il Cyber Solidarity Act,
  - lo Spazio europeo dei dati sanitari (EHDS).
- Sfruttare lo strumento di mappatura normativa in arrivo a cura del Gruppo di Cooperazione NIS e di ENISA (previsto per il 2025) per orientare tali sforzi.
- Sviluppare e diffondere kit di strumenti online, incluse linee guida per l'acquisto di servizi, prodotti e infrastrutture.
- Elaborare metodologie su misura per aiutare le entità a comprendere e gestire meglio i rischi informatici nei propri ambienti.
- Mantenere le risorse aggiornate
- Condurre esercitazioni settoriali specifiche, incluse simulazioni tabletop, per migliorare le capacità di risposta a livello nazionale

LINEA GUIDA ENISA "TECHNICAL IMPLEMENTATION GUIDANCE", GIUGNO 2025

La Guida tecnica di attuazione ENISA (versione 1.0, giugno 2025), è stata sviluppata per supportare l'applicazione del Regolamento di esecuzione (UE) 2024/2690 relativo alla Direttiva NIS2.
Il regolamento di esecuzione (UE) 2024/2690 è un atto dettagliato e vincolante adottato dalla Commissione Europea per specificare:

- i requisiti tecnici e metodologici delle misure di gestione del rischio (art. 21 NIS2)
- i criteri per definire un incidente significativo (art. 23 NIS2) Serve da guida pratica per l'applicazione uniforme della Direttiva NIS2 da parte delle entità coinvolte

Tra le categorie di soggetti destinatari del regolamento e della guida rientrano:

- fornitori di servizi DNS e registri di domini di primo livello
- provider di cloud computing e data center
- content delivery network (CDN)
- managed service providers e managed security service providers
- piattaforme di marketplace online, motori di ricerca e social network
- trust service providers

La guida tecnica ENISA, pur essendo molto utile come riferimento per l'implementazione del Regolamento 2024/2690, si colloca a un livello metodologico e strutturale, offrendo cornici concettuali, esempi e mappature, ma non entra nei dettagli operativi di ciascuna misura.

Aspetti propri della sanità e dei sistemi medicali

Integrazione di competenze per una corretta gestione sicura tra IC IT e OT

Sin dall'inizio della storia dell'Ingegneria Clinica (IC) e della gestione delle tecnologie biomediche (HTM: Health Technology Management) in ambito sanitario, il focus è stato posto sulla necessità di assicurare il supporto alla componente clinica, al fine di garantire la disponibilità di tali tecnologie nelle migliori condizioni di efficacia, efficienza e sicurezza.
Secondo dati OECD https://www.oecd.org/ in Italia (dati aggiornati al 2023) ci sono 179.000 posti letto in 1060 strutture ospedaliere di diverse dimensioni, da poche decine a diverse migliaia di posti letto. Se consideriamo che in letteratura si parla di circa 3-6 dispositivi medici a posto letto connessi in rete, possiamo stimare che la base di attacco cibernetico è costituita da 0,5 a 1,0 Milioni di unità.
Un tipico ospedale italiano ha in media circa 500 posti letto con 7000 apparecchiature biomediche, caratterizzate da centinaia di modelli, produttori e fornitori diversi. Di queste, circa 1000 apparecchiature sono stimabili connesse in rete.
Le conseguenze di una compromissione cibernetica per un dispositivo medico presenta alcune peculiarità, che possono variare da un errata diagnosi, con conseguenze sul trattamento sanitario, a un ritardo nella diagnosi e conseguente trattamento, fino ad una possibile perdita o diffusione illecita di

Perché i dispositivi medici sono così difficili da proteggere

Asset IT	Asset MD
Gli asset IT tradizionali hanno una vita media di 3-5 anni	Gli asset MD in alcuni casi hanno vita superiore ai 10 anni.
Minori rischi dovuti a presenza di sistemi operativi non aggiornabili	Rischi dovuti a sistemi operativi legacy o non aggiornabili.
Patching standardizzabile	Patching complesso difficilmente standardizzabile. Le azioni di Incident Response (IR) più comuni, come il distacco dalla rete informatica di un dispositivo sospetto, non sono ragionevoli. Per dispositivi come i ventilatori polmonari, le misure IR devono tener conto dell'impatto sull'assistenza clinica. I sistemi operativi legacy rendono difficile la protezione di questi dispositivi, richiedendo una micro segmentazione di livello 2. Ogni dispositivo medico connesso in rete e interoperabile con altri sistemi può essere causa di vulnerabilità cibernetica dell'intero sistema. Può, in altri termini, costituire un single point of failure (SPoF).

dati personali del paziente. Va infine considerato il caso di un danno malevolo procurato alle apparecchiature sanitarie ed alla conseguente indisponibilità improvvisa durante una procedura medica.
È inoltre necessario osservare che vi possono essere casi di compromissione di molte apparecchiature dello stesso tipo nello stesso momento (ad esempio pompe infusionali) o di gruppi più piccoli fino a singole unità che potrebbero avere impatto significativo sulla salute e sulla vita del paziente (dispositivi di supporto vitale).
In ogni caso l'approccio dell'IC/HTM si basa sulle seguenti due domande fondamentali:

- È in pericolo la salute del paziente?
- La salute del paziente e la sua sicurezza hanno la priorità?

INTEROPERABILITÀ VS CYBERSECURITY

Negli ultimi anni, il settore dei dispositivi medici ha subito significativi cambiamenti, influenzati dalla trasformazione digitale in atto..
Si evidenziano quattro aree di forte cambiamento:

- Il numero di tecnologie presenti nell'ecosistema sanitario è in continua crescita.
- Dispositivi medici sempre più dotati di funzionalità "intelligenti", anche grazie all'applicazione dell'Intelligenza Artificiale nella loro realizzazione.
- Sistemi di dispositivi con funzionalità integrate sempre più avanzate.
- Espansione del luogo di cura, dall'ospedale al domicilio, con crescente coinvolgimento del paziente nel processo di cura, anche attraverso l'uso di tecnologie digitali (dispositivi IoT, sensoristica, dispositivi indossabili) come estensori clinici.

L'evoluzione in atto delle tecnologie in ambito sanitario ha comportato, negli ultimi decenni, un aumento esponenziale dell'esposizione ai rischi di informatici, correlato anche all'esigenza di interoperabilità e integrazione dei dispostivi medici con i sistemi IT.
La mancanza di integrazioni e interoperabilità può comportare maggiori costi nell'erogazione dei servizi sanitari a causa di: eventi avversi, errori nella somministrazione di farmaci, errori diagnostici (o per mancata diagnosi), mancata prevenzione infortuni, ridondanza di esami diagnostici e di laboratorio, eccesso di tempo speso dal personale sanitario per introduzione di dati in modo manuale, prolungati tempi di ricovero, perdita di efficacia nell'applicazione della telemedicina e nell'introduzione delle cartelle cliniche elettroniche.
In altre parole la mancanza di interoperabilità può compromettere la sicurezza del paziente, minare la qualità e i risultati dell'assistenza, contribuire all'affaticamento/burnout del medico e aumentare gli sprechi.
L'interoperabilità deve bilanciare innovazione, accesso dei pazienti (patient empowerment) e sicurezza. In altre parole i miglioramenti nella condivisione dei dati richiedono di garantire ai pazienti un maggiore controllo sui propri dati e di tutelare la sicurezza degli stessi.

EVENTI DI CYBERSECURITY NEL MONDO DEI MEDICAL DEVICE

Nell'ottobre 2012 il ricercatore Barnaby Jack ha pubblicato un articolo in cui dimostrava come fosse possibile hackerare un pacemaker attraverso un trasmettitore wireless, consentendo di assumere il

controllo del pacemaker comandando l'emissione di segnali potenzialmente dannosi per la salute del paziente. Già nel 2011 Barnaby Jack aveva dimostrato, durante una conferenza, come fosse possibile, tramite un collegamento wireless, interfacciarsi con una pompa infusionale e assumerne il controllo totale.
Il 31 luglio del 2015 l'agenzia FDA ha avvisato gli ospedali di non utilizzare un particolare modello di pompa infusionale a causa della scoperta di una vulnerabilità informatica che avrebbe consentito ad un potenziale attaccante di assumere il controllo dell'apparecchiatura.
Nell'agosto del 2017 FDA ha approvato un aggiornamento firmware che ha comportato il richiamo di 745.000 pazienti a cui è stato impiantato uno specifico pacemaker vulnerabile agli attacchi informatici.
Nel settembre 2020 zdnet.com ha segnalato il primo decesso ufficiale avvenuto in Germania a causa di un attacco Ransomware ad un Ospedale.
L'Istituto ECRI pubblica annualmente una lista dei dieci rischi principali associati alle tecnologie sanitarie, basata sui dati raccolti attraverso il proprio sistema di sorveglianza degli incidenti. Dal 2018, tale lista include costantemente elementi relativi alla sicurezza informatica. In particolare nella lista del 2025, al punto 3, è presente "fornitori di tecnologie vulnerabili e minacce informatiche". In una diversa lista relativa a "Preoccupazioni per la sicurezza dei pazienti per il 2025", al punto 4 si riporta "errori medici e ritardi nelle cure derivanti da violazioni della sicurezza informatica".

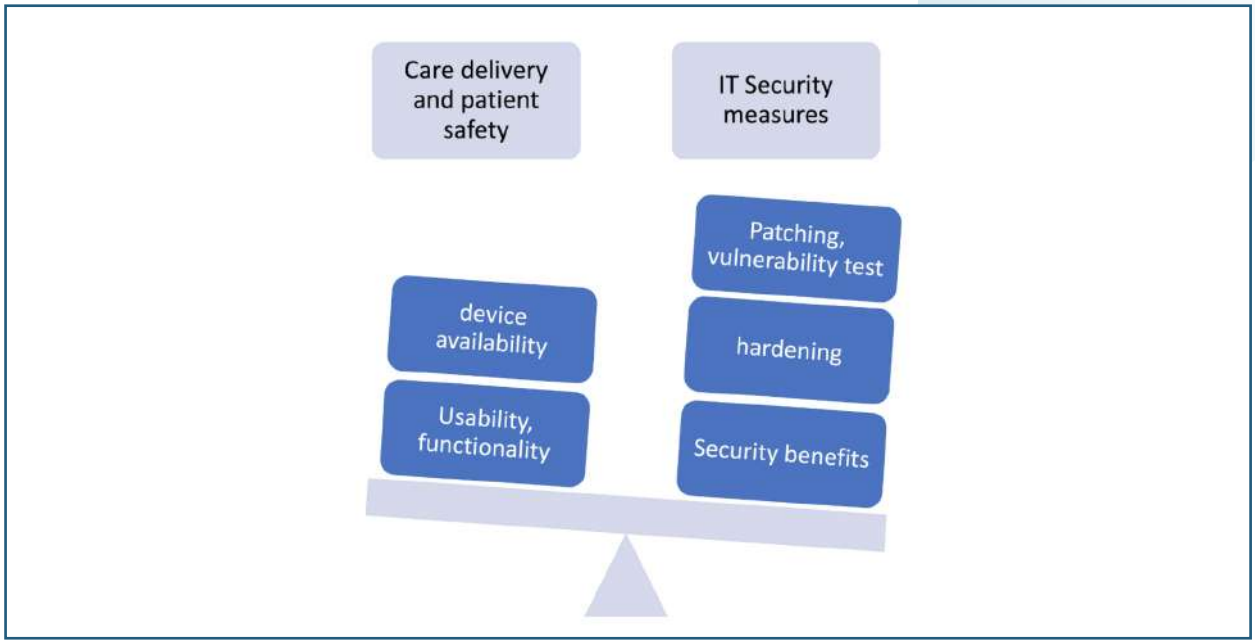
LA FORMAZIONE TECNICA DEL PERSONALE SANITARIO

La formazione del personale sanitario, tecnico e amministrativo è fondamentale. In particolare, per quanto riguarda il personale sanitario, è necessario un cambio di prospettiva: è indispensabile sviluppare una partnership sulla sicurezza informatica con tale categoria, promuovendo una maggior consapevolezza del rischio, spesso non conosciuto o non percepito. In altre parole, è necessario favorire il superamento della sicurezza IT come barriera e comprendere altresì il legame che essa ha con la sicurezza del paziente.

APPROCCIO ALLA CYBERSECURITY PER IC

I più significativi atteggiamenti nella gestione dei DM dal punto di vista della cybersicurezza possono essere così riassunti:

- Non trattare i dispositivi medici come normali endpoint IT o dispositivi IoT.
- Assicurarsi che tutte le patch, gli aggiornamenti e/o le soluzioni di sicurezza degli endpoint siano stati convalidati dal produttore prima dell'installazione.
- Richiedere istruzioni scritte, documentazione e manuali aggiornati, se necessario.
- Attivare la collaborazione tra i team di ingegneria clinica e IT/sicurezza.
- Considerare i Software as a Medical Device (SaMD) e i Software in a Medical Device (SiMD), come software critico.
- Condividere, attraverso l'analisi del rischio, che le esigenze di erogazione sicura dell'assistenza al paziente e le esigenze di applicazione delle migliori pratiche di sicurezza informatica, costituiscono due facce della stessa medaglia



GESTIONE DELLA MANUTENZIONE

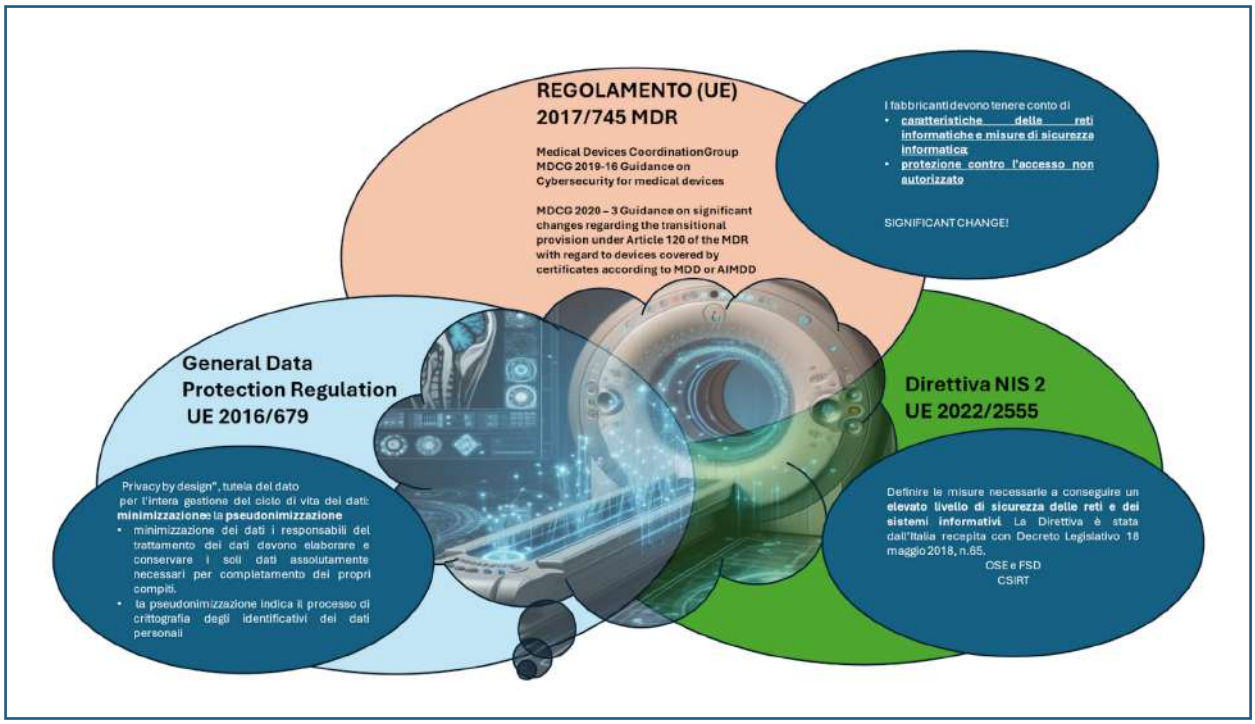
La gestione e la manutenzione dei dispositivi medici presentano differenze significative rispetto alle analoghe attività per i sistemi IT.

- La sicurezza informatica per i sistemi IT è più consolidata e l'omogeneità di tali sistemi consente la gestione delle patch, la scansione delle vulnerabilità, l'utilizzo di software antivirus e la gestione delle risorse.
- Le tradizionali attività di sicurezza informatica, come la scansione delle vulnerabilità e la gestione delle patch, risultano complesse da implementare per i dispositivi medici. Spesso, gli asset medicali non sono progettati per supportare tali operazioni. Inoltre, l'installazione di agenti potrebbe non essere possibile.
- Per i dispositivi medici IT, è difficile ottenere un inventario accurato del software. I dispositivi "legacy" più vecchi e distribuiti rappresentano una sfida per la sicurezza informatica.
- Il panorama dei dispositivi medici, caratterizzato da numerosi produttori e modelli, è complesso da monitorare.
- I produttori dovrebbero condividere informazioni sul software utilizzato nei loro prodotti (ad esempio, la versione del sistema operativo incorporato in uso). La versione più recente (2019) del Manufacturer Disclosure Statement for Medical Device Security (MDS2) rappresenta un passo avanti, ma non sempre è disponibile o completa.
- È difficile tenere traccia dei sistemi operativi, delle versioni software e di altre informazioni rilevanti per la sicurezza IT.
- I produttori dovrebbero condividere informazioni sullo stato della gestione delle patch per i loro dispositivi e, una volta testate le patch, completare il test e la raccomandazione finale in tempi ragionevoli.

- È necessario sottoporre a scansioni di vulnerabilità anche i dispositivi medici connessi in rete, al fine di identificare eventuali vulnerabilità.
- È fondamentale migliorare la gestione del software dei dispositivi medici, al fine di rispondere tempestivamente a problemi di sicurezza. Si consiglia di non collegare i dispositivi alla rete se non necessario. In caso di attacco informatico, è importante valutare la capacità di rilevamento e la tempestività di risposta.
- È necessario gestire le periferiche esterne (ad esempio, le unità USB) da utilizzi non necessari, gestire le credenziali di accesso e aggiornare il firmware (hardening).
- È consigliabile rivedere i protocolli e le procedure di sicurezza alla luce degli avvisi e degli incidenti segnalati.

IC VS IT VS OT: COME COLLABORARE PER AUMENTARE IL LIVELLO DI SICUREZZA GENERALE

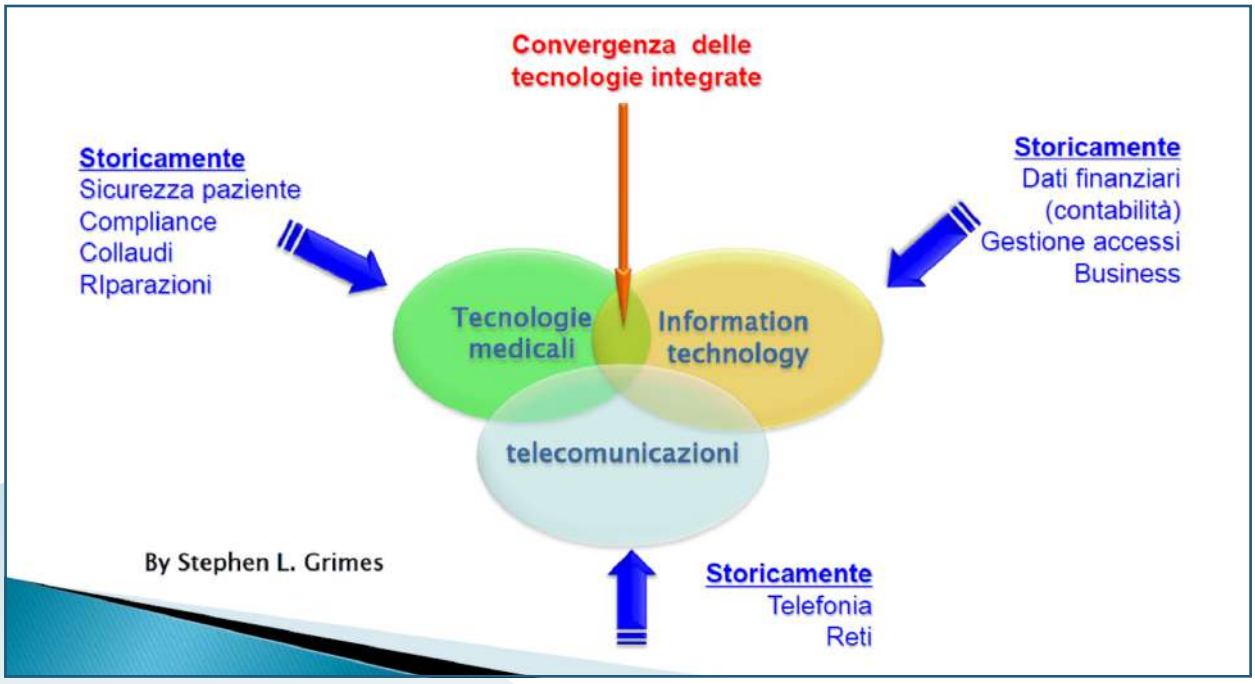
Regolamenti, leggi, linee guida nazionali ed europee



L'introduzione di normative come i requisiti AGID, la direttiva NIS (e ora NIS2) e il regolamento GDPR hanno visto inizialmente un coinvolgimento prevalente dei reparti IT e delle direzioni mediche, focalizzando l'attenzione sulla sicurezza delle reti e sulla gestione dei dati sensibili, come quelli contenuti nelle cartelle cliniche elettroniche. L'ingegneria clinica, in una fase iniziale, è stata meno coinvolta nell'applicazione di questo quadro normativo. Tuttavia, l'attuale scenario di cybersecurity richiede un cambiamento di approccio, riconoscendo che il problema della sicurezza informatica è ormai costantemente presente anche all'interno dei servizi di ingegneria clinica e non solo.

Rispetto al tema della cybersecurity applicata ai dispositivi medici, Ingegneria Clinica e Sistemi Informativi giocano ruoli cruciali, spesso interconnessi, nella gestione della sicurezza dei dati e dei dispositivi stessi. Storicamente l'Ingegneria Clinica si occupa della gestione e della manutenzione dei dispositivi medici, mentre Sistemi Informativi si concentrano sulla gestione e protezione dei dati e delle infrastrutture informatiche. Di fronte alle minacce cyber, entrambi devono collaborare per garantire la sicurezza, l'integrità e la disponibilità dei sistemi sanitari.
La situazione è cambiata e va cambiato l'approccio di chi gestisce, direttamente o indirettamente i dispositivi medici connessi in rete.
Il governo di una tecnologia non potrà più passare solo attraverso una competenza specifica, ma dovrà avvalersi di molteplici competenze.
Multidisciplinarietà del personale: il governo delle tecnologie nel settore sanitario non può più basarsi esclusivamente su competenze settoriali. È imperativo adottare un approccio multidisciplinare che coinvolga attivamente l'ingegneria clinica, i sistemi informativi, il personale che si occupa delle infrastrutture e la direzione medica per gli aspetti organizzativi. Le strutture tecniche e tecnologiche come l'Ingegneria Clinica, i Servizi Informatici e i Servizi Tecnici possiedono una visione 'allargata' del funzionamento aziendale, che li rende strategici per l'acquisizione di informazioni, per la sorveglianza e l'implementazione di aggiornamenti, rappresentando un'opportunità per stimolare azioni di miglioramento all'interno dell'organizzazione.
La crescente convergenza delle tecnologie solleva nuove e significative preoccupazioni per la sicurezza dei pazienti e delle informazioni, rendendo indispensabile una chiara definizione dei ruoli, delle

Convergenza delle tecnologie



responsabilità e delle relazioni tra il personale IT e quello di ingegneria clinica. La nuova frontiera in termini di asset non include solamente i dispositivi medici e i dispositivi IoT, ma anche le tecnologie operative (OT - Operational Technology). Questi ultimi rappresentano un ambito particolarmente complesso, in quanto, oltre a dispositivi connessi come telecamere e stampanti, comprendono un'ampia gamma di device industriali, sensori, robot e macchinari che, non avendo a bordo un sistema operativo ordinario, sono difficili da monitorare.
La compromissione di una delle tecnologie operative come gli impianti per automazione degli edifici, sensori ambientali, gruppi di continuità, sistemi HVAC e piattaforme per la distribuzione energetica, elementi invisibili, ma indispensabili per il funzionamento dell'ospedale, potrebbe interrompere il raffreddamento dei farmaci termolabili, bloccare gli ascensori o impedire il funzionamento dei sistemi antincendio.
A differenza del mondo dei dispositivi medici e dell'IT, dove le vulnerabilità possono essere individuate tramite scanner, nel mondo OT questa operazione è significativamente più difficile, poiché le scansioni potrebbero compromettere l'operatività dei dispositivi. Per questo motivo, nel mondo OT si utilizzano quasi esclusivamente sensori passivi per il monitoraggio.

MISURE IMPLEMENTABILI E UN NUOVO APPROCCIO ALLA GESTIONE: COSA È POSSIBILE FARE ADESSO?

Fase di Gara?

È possibile inserire requisiti specifici nelle gare d'appalto, come la crittografia dei dati, password di accesso robuste e multifattoriali e l'obbligo di aggiornamenti del sistema operativo, pur mantenendo un'attenzione prioritaria alla qualità clinica. Al momento, tuttavia, l'introduzione di tali requisiti come mandatori potrebbe non essere ancora pienamente attuabile, pur essendo pienamente in vigore quanto previsto da numerose leggi basate su direttive e regolamenti europei quali MDR, IVDR, AI Act, NIS2 (DLgs 138/2024) GDPR e Data Act.

In fase di collaudo?

Durante il collaudo, è fondamentale verificare e raccogliere informazioni dettagliate rispetto a quanto richiesto dalla committenza e quanto dichiarato dall'aggiudicatario della fornitura. In presenza di vulnerabilità dell'apparecchiatura, sopraggiunte tra la presentazione delle offerte e l'avvio della fornitura, è necessario implementare workaround organizzativi per mitigare i rischi, fino alla messa in sicurezza in conformità alla normativa vigente.

In fase di manutenzione?

È essenziale aggiornare e implementare un database informativo, oltre a prevedere l'applicazione di misure organizzative in caso di spostamenti o ricollocazione dell'apparecchiatura. È cruciale valutare un nuovo approccio nella gestione delle apparecchiature mediche, che vada oltre la semplice manutenzione. In particolare negli ospedali, infatti, manca una base informativa comune e integrata. Per questo nuovo approccio è indispensabile dotarsi di un database con una visione allargata, poiché la mancanza di informazioni impedisce di misurare l'entità del problema (ad esempio, per i requisiti GDPR sono necessarie informazioni diverse rispetto a quelle richieste dalla NIS2).

Da diversi anni, le associazioni che rappresentano ingegneri clinici e IT officer collaborano per affrontare congiuntamente le problematiche di sicurezza. Entrambi sono consapevoli della inderogabile necessità di lavorare in sinergia, data la sensibilità dei dati e delle informazioni in gioco e l'impatto sulla vita umana. Tuttavia, le maggiori criticità emergono a livello aziendale, dove l'efficacia della collaborazione dipende fortemente dalla relazione personale tra i Responsabili dei Servizi di Ingegneria Clinica e i Responsabili dei Servizi Informatici (presupponendo, cosa non scontata, che entrambe le figure siano presenti in azienda).

La formazione: un'arma fondamentale!

La cybersecurity per la sanità digitale ha nell'educazione la sua arma strategica. In Italia, e non solo, il settore sanitario mostra una carenza di vera e propria educazione alla cybersecurity. La scarsa consapevolezza dell'importanza della sicurezza informatica è una delle principali cause degli eventi avversi, sempre più frequenti, che si verificano ogni anno. A differenza di altri settori più orientati alla digitalizzazione, le strutture sanitarie hanno spesso investito meno risorse nella sicurezza dei dati e nella formazione del personale in materia di cybersecurity , rendendole più vulnerabili agli attacchi. Per questo, una delle misure più efficaci, benché spesso sottovalutata, è l'educazione, la formazione e l'aggiornamento regolare del personale sui rischi e le responsabilità. L'efficacia dei processi organizzativi è direttamente correlata alla coerenza con cui il personale li segue. Pertanto, le aziende dovrebbero fornire una formazione completa sulle misure di sicurezza informatica e sui rischi connessi. Il personale, ad esempio, dovrebbe essere istruito a riconoscere comunicazioni e-mail sospette e a non aprire contenuti potenzialmente pericolosi. L'importanza della crittografia è ancora troppo spesso sottovalutata. Allo stesso modo, ogni azienda sanitaria dovrebbe promuovere corsi di formazione sulla Data Governance e sul GDPR in ambito sanitario. La formazione sulla cybersecurity non deve essere percepita come un onere o un obbligo, ma come un'opportunità per migliorare le proprie capacità di proteggere sé stessi e l'azienda, riducendo l'esposizione alle minacce cyber.

Il perimetro e l'impatto della Direttiva NIS2 sul Panorama ICT e DM in Sanità

INTRODUZIONE

La Direttiva (UE) 2022/2555, nota come NIS2 (Network and Information Security 2), rappresenta l'evoluzione normativa del quadro europeo in materia di cybersicurezza, in termini di un significativo rafforzamento normativo europeo sulla sicurezza informatica rispetto alla precedente NIS del 2016. Entrata in vigore il 16 gennaio 2023, è stata recepita negli ordinamenti nazionali con il DLgs 138/2024. Il settore sanitario è identificato tra i settori "essenziali" per la resilienza dell'Unione Europea, e perciò rientra pienamente nel campo di applicazione della NIS2. Essa mira a elevare il livello di sicurezza, resilienza e gestione del rischio delle reti e dei sistemi informativi in tutti i settori critici, tra cui la sanità, settore particolarmente sensibile per la natura dei dati trattati e la criticità dei servizi erogati.

Nel contesto ICT medicale, la NIS2 impone obblighi stringenti a strutture sanitarie, produttori di dis-

positivi medici, fornitori di servizi digitali e altri stakeholder, con l'obiettivo di tutelare la riservatezza, integrità e disponibilità dei dati sanitari e garantire la continuità operativa dei servizi essenziali.
Sono rilevanti le misure di mitigazione dei rischi quali ad esempio:

- sicurezza by design: dispositivi progettati con protocolli di sicurezza integrati;
- crittografia avanzata: per proteggere i dati durante la trasmissione e l'archiviazione;
- audit indipendenti: verifiche periodiche sulla sicurezza e conformità normativa;
- sensibilizzazione degli utenti: programmi di educazione per aumentare la consapevolezza sui rischi e sui diritti digitali.

In aggiunta, è fondamentale promuovere la collaborazione tra governi, aziende e organismi di regolamentazione per sviluppare standard globali che garantiscano l'interoperabilità e la sicurezza dei dispositivi medici.
Sul mercato dell'UE ci sono oltre 500 mila tipi di dispositivi medici e dispositivi medico-diagnostici in vitro. Alcuni esempi di dispositivi medici sono i cerotti, le lenti a contatto, le apparecchiature a raggi X, i pacemaker, le protesi mammarie, le applicazioni software e le protesi dell'anca. I dispositivi medico-diagnostici in vitro sono utilizzati per effettuare analisi su campioni. Alcuni esempi comprendono i test ematici per l'HIV, i test di gravidanza e i sistemi per il controllo della glicemia per i pazienti diabetici. Molti di questi dispositivi sono associati o sono prodotti con equipaggiamenti digitali, e quindi software con varie funzionalità dall'analisi alla capacità di ricevere e trasmettere informazioni.
La connettività caratterizza la trasformazione digitale così come anche la produzione di dispositivi e servizi di varia complessità che utilizzano Software e Hardware che elaborano le informazioni scambiate in modalità digitalizzata. Le opportunità della connettività di questa diversificata disponibilità di prodotti e servizi digitali sono bilanciate dalla possibilità di inserimento di soggetti diversi da quelli previsti con conseguente attività fraudolenta (hacking) o dal conflitto o vulnerabilità informatica tra dispositivi connessi in rete, con conseguente malfunzionamento o distruzione delle informazioni o manifesta violazione della privacy/proprietà delle informazioni stesse.
In questo documento si analizza l'impatto della NIS2 sull'ecosistema ICT in ambito medicale, con particolare riguardo ai dispositivi connessi, software medicali, telemedicina, cartella clinica elettronica, interoperabilità, EHDS, intelligenza artificiale e Internet of Medical Things (IoMT).

DISPOSITIVI CONNESSI IN RETE E IOMT

I dispositivi medici connessi, inclusi quelli appartenenti all'Internet of Medical Things (IoMT), rappresentano una superficie di attacco crescente per la cybersecurity. La diffusione di dispositivi medici connessi in rete, inclusi sensori, monitor e dispositivi impiantabili, rende il settore sanitario particolarmente vulnerabile a minacce informatiche. La NIS2 richiede ai produttori e agli operatori sanitari di adottare una gestione basata sul rischio che consideri la sicurezza fin dalla progettazione e durante l'intero ciclo di vita del dispositivo.
In particolare il Rapporto Clusit descrive IoT (Internet of Things) e IoB (Internet of Bodies) come due categorie separate.
L'IoT si riferisce a un ecosistema di dispositivi interconnessi che raccolgono dati ambientali o personali e li elaborano per migliorare servizi e applicazioni. L'IoB, come sottoinsieme dell'IoT, è costituito da

dispositivi progettati per monitorare, migliorare o modificare le funzionalità del corpo umano. Esempi includono pacemaker intelligenti, interfacce cervello-computer e wearable per il monitoraggio della salute.

I principali contesti di applicazione dell'IoB spaziano dalla medicina (è in questo caso si parla di IoMT, quali dispositivi per il monitoraggio di malattie croniche o interventi chirurgici assistiti) al consumo (smartwatch, abiti con sensori), fino all'ambito militare e industriale (esoscheletri, monitoraggio dei lavoratori in contesti pericolosi). Si deve far notare che gli esoscheletri sono anche dispositivi medici quando usati nella riabilitazione.

In ambito sanitario, i dispositivi IoMT permettono diagnosi più rapide e terapie personalizzate. Nel settore industriale, gli IoB migliorano la sicurezza sul lavoro grazie a sensori che monitorano costantemente le condizioni fisiche dei lavoratori. Per quanto riguarda il consumo, strumenti come i fitness tracker stanno trasformando il modo in cui le persone si prendono cura della propria salute.

La NIS2 impone requisiti rigorosi per la gestione del rischio, la sicurezza del ciclo di vita dei dispositivi, la risposta agli incidenti e la tracciabilità. In esplicito:

- Redazione di una Analisi dei rischi specifica per i dispositivi connessi, valutando le vulnerabilità hardware e software e le potenziali conseguenze di un attacco. (Vedi normative come la serie ISO/IEC 80001)
- Gestione degli asset IT e dei flussi informativi, con inventari dettagliati che includano versioni software, firmware, stato operativo e dipendenze, per garantire una segmentazione di rete efficace e limitare i flussi non autorizzati.
- Notifica obbligatoria e tempestiva degli incidenti di sicurezza che coinvolgono dispositivi connessi, per permettere una risposta coordinata e mitigare l'impatto su pazienti e servizi.

Gli Stakeholder sanitari (organizzazioni/istituzioni pubbliche e private) dovranno:

- Integrare strategie di sicurezza "by design" e "by default" nella gestione dei dispositivi.
- Richiedere ai fabbricanti l'aggiornamento regolare dei firmware e delle patch di sicurezza.
- Monitorare le minacce in tempo reale, con sistemi di sicurezza attivi e resilienti.

Questi requisiti si applicano anche all'ecosistema IoMT, dove la molteplicità di dispositivi e la loro interconnessione richiedono un controllo rigoroso per prevenire compromissioni che potrebbero minare la sicurezza clinica e la privacy dei pazienti.

Le vulnerabilità specifiche associate alla sensoristica IoMT includono:

- Intercettazione dei dati sensibili: i sensori trasmettono costantemente dati biometrici o clinici che, se non cifrati adeguatamente, possono essere intercettati da attori malevoli.
- Accesso non autorizzato: dispositivi con autenticazione debole possono essere compromessi, permettendo manipolazioni da remoto.
- Firmware vulnerabile: l'assenza di controlli sulla filiera e di aggiornamenti tempestivi espone i dispositivi a exploit noti.
- Attacchi di tipo man-in-the-middle: in reti ospedaliere complesse, i dati trasmessi tra sensori, gateway e server possono essere alterati se i canali non sono autenticati e protetti.
- Risorse computazionali limitate: molti sensori hanno capacità limitate, che ostacolano l'implementazione di protocolli di sicurezza avanzati.

SOFTWARE MEDICAL DEVICE (MDSW)

I software dei servizi sanitari, compresi quelli dispositivo medico (MDSW), classificati secondo il Regolamento MDR 2017/745, sono particolarmente esposti ai rischi informatici. Un MDSW (vedi definizione di DM) è un SW integrato in dispositivi medici o un SW autonomo utilizzato in modalità Stand Alone o connesso in rete per diagnosi, monitoraggio e terapia. La direttiva NIS2, in linea con i regolamenti MDR e IVDR, impone che anche il software sia soggetto a rigorose analisi di rischio e misure di sicurezza informatica sin dalla fase di progettazione.

NIS2 impone:

- Valutazione continua della sicurezza informatica lungo l'intero ciclo di vita del software (misure tecniche e organizzative per garantire la sicurezza, l'integrità e la disponibilità del software).
- Adozione di politiche di vulnerability disclosure per prevenire exploit.
- Tracciabilità e gestione delle versioni per assicurare la conformità.
- Notifica obbligatoria e tempestiva di incidenti gravi (entro 24 ore).
- Nello specifico ad esempio i produttori dovranno implementare misure di sicurezza avanzate, come crittografia, autenticazione multifattoriale e aggiornamenti regolari per prevenire vulnerabilità.
- Anche le strutture sanitarie devono adottare piani di gestione del rischio specifici per i dispositivi IoMT, monitorandone costantemente il funzionamento e rilevando tempestivamente anomalie o attacchi informatici.
- Protezione della supply chain per i dispositivi che dipendono anche da fornitori esterni, per evitare che diventino punti di ingresso per attacchi.

I produttori di MDSW (in Europa è la definizione corrente del MDCG 2019/11 e 2021/24, il SaMD non è necessariamente la stessa cosa come da IMDRF) possono fare riferimento per la certificazione dei prodotti a standard tecnici (es. ISO/IEC 27001, IEC 81001-5-1, ISO/IEC 62304) per documentare le misure adottate. La crescente diffusione di MDSW, spesso integrato con algoritmi realizzati utilizzando sistemi di intelligenza artificiale, rende cruciale un approccio sistematico alla sicurezza, in modo da evitare rischi per la salute derivanti da malfunzionamenti o attacchi informatici, declinando norme e regolamenti specifici concorrenti.

Alcune indicazioni devono essere applicate anche a SW quali le App per il benessere, che, pur non dovendo rispondere ai criteri del regolamento MDR 2017/745, sono l'oggetto di una TS 82324-2, che prevede anche la verifica di requisiti quali quelli relativi al GDPR, alla interoperabilità e usabilità, al fine di non essere una porta possibile per entrare nei profili socio-sanitari dei cittadini (anche pazienti).

INTEROPERABILITÀ E EHDS (EUROPEAN HEALTH DATA SPACE)

L'interoperabilità tra sistemi è essenziale per il funzionamento del EHDS, ma crea anche nuovi rischi di sicurezza legati alla condivisione e al trasferimento di dati sensibili. Il G7 Health ha visto esperti dei ministeri della salute di 7 paesi (Italia, Francia, Germania, Inghilterra, Canada, Giappone e USA) definire codifiche e standard adeguati per la condivisione transfrontaliera (ICD e FHIR). La NIS2 richiede una gestione rigorosa dei flussi informativi e la protezione delle infrastrutture di rete che supportano l'interoperabilità, ad esempio che le interfacce tra sistemi siano protette da misure tecniche e organizzative adeguate. Inoltre, la condivisione sicura dei dati sanitari richiederà:

- In particolare: La direttiva richiede standard comuni di cybersecurity per tutti gli operatori che accedono o gestiscono dati nell'ambito EHDS
- È obbligatorio garantire l'integrità e la riservatezza dei dati durante la trasmissione e l'archiviazione (Cifratura end-to-end).
- Devono essere implementate misure di autenticazione e autorizzazione per limitare l'accesso ai soli operatori autorizzati (Sistemi di audit e tracciamento degli accessi, identità digitale e autenticazione forte).
- La segmentazione delle reti e il monitoraggio continuo dei flussi dati sono essenziali per prevenire accessi non autorizzati e fughe di dati.

Lo EHDS sarà soggetto a requisiti elevati in termini di governance, sicurezza e resilienza, con audit periodici e interoperabilità sicura tra i Paesi.
Una trattazione più esaustiva su questo tema sarà proposta nel paragrafo "Contesto legislativo e normativo".

TELEMEDICINA E CARTELLA CLINICA ELETTRONICA

La telemedicina espande i confini dell'assistenza sanitaria, ma introduce nuove vulnerabilità. La telemedicina, che consente la fornitura di servizi sanitari a distanza, si basa su infrastrutture ICT complesse e interconnesse. La NIS2 impone che tali servizi siano protetti da rischi informatici che potrebbero compromettere la continuità assistenziale o la sicurezza dei dati personali.
I fornitori/operatori di servizi dovranno:

- Garantire la protezione dei dati trasmessi in tempo reale
- Applicare criteri di protezione end-to-end nelle comunicazioni medico-paziente.
- Prevedere sistemi di backup e continuità operativa (piani di continuità operativa per garantire la disponibilità dei servizi anche in caso di attacchi informatici).
- Effettuare valutazioni periodiche dei rischi e aggiornare le misure di sicurezza in base alle evoluzioni tecnologiche e alle minacce emergenti.
- È fondamentale garantire la protezione della privacy e la conformità al GDPR, integrando la sicurezza tecnica con la governance dei dati.

La telemedicina, essendo un servizio essenziale, rientra tra le infrastrutture critiche tutelate dalla direttiva, con obblighi specifici di notifica e gestione degli incidenti.
La cartella clinica elettronica (EHR) sarà considerata infrastruttura critica specialmente nella declinazione di servizi con AI (Vedi MDCG 2025/1).
Le autorità sanitarie dovranno:

- Implementare piani di risposta agli incidenti.
- Effettuare regolarmente test di penetrazione e valutazioni dei rischi.

INTELLIGENZA ARTIFICIALE IN MEDICINA

L'uso dell'AI in medicina comporta l'elaborazione di grandi volumi di dati e decisioni cliniche automatizzate. L'AI Act declina nel caso sanitario, la maggior parte dei SW con AI classificandoli come a maggior rischio, tenendo conto oltre che dei classici rischi per i MDSW anche della governance dei

dati e della security e privacy. Robustezza e esplicabilità sono parole chiave del Risk Management. La NIS2 impone:

- Protezione dei dati usati per addestrare gli algoritmi.
- Auditabilità e tracciabilità dei processi decisionali per garantire la sicurezza clinica e la fiducia degli operatori (trasparenza).
- Sicurezza dei modelli contro attacchi di tipo adversarial (robustezza).

Sistemi AI che influenzano diagnosi o trattamenti rientrano tra le tecnologie ad alto impatto e dovranno dimostrare robustezza e resilienza. L'integrazione della cybersecurity con le normative emergenti sull'AI rappresenta una sfida e un'opportunità per migliorare la sicurezza complessiva del settore sanitario.

RACCOMANDAZIONI CONCLUSIVE GENERALI

L'impatto della NIS2 sul panorama ICT in sanità sarà significativo. Le organizzazioni sanitarie pubbliche e private dovranno adottare una cultura della sicurezza pervasiva e multidimensionale per la sicurezza delle reti, dei sistemi informativi e dei dispositivi medici.
Alcune raccomandazioni:

- Definire una governance chiara della cybersecurity, che per le strutture sanitarie significa predisporre piani di continuità e risposta rapida agli incidenti informatici, per evitare interruzioni che possano compromettere le cure a distanza, e piani di back up per il pronto ripristino dopo attacco.
- Formare il personale sanitario e tecnico (Cultura organizzativa e formazione continua per riconoscere e gestire i rischi informatici).
- Collaborare con enti certificatori e organismi notificati.
- Adottare tecnologie di sicurezza avanzate (SIEM, EDR, IAM).

La NIS2 rappresenta un'opportunità per rafforzare la fiducia nella sanità digitale europea, ponendo la sicurezza al centro dell'innovazione in medicina, ma anche una sfida complessa, di tipo culturale per proteggere i dati sensibili dei pazienti e garantire la continuità delle cure essenziali. La NIS2 spinge verso un modello di gestione della sicurezza più integrato, proattivo e strutturato, che coinvolge tecnologie, processi e persone.

Considerazioni relative all'implementazione dei sistemi digitali con Dispositivi Medici e conformità alla NIS2

Si deve tener conto, alla luce degli incidenti menzionati in questo capitolo, che tutta la catena che concorre alla realizzazione di un servizio sanitario digitale, stante la connessione informatica di più elementi SW ed HW, dovrà essere sottoposta alla valutazione e gestione dei rischi a partire dalla sua progettazione (almeno da parte del fabbricante dei sistemi componenti e della direzione sanitaria che vuole realizzare il servizio con quei componenti) fino alla sua implementazione gestita dall'ente che produrrà il servizio e che sarà anche responsabile della conseguente attività di Risk Management. I DM potranno essere il terminale della catena di sistemi componenti come ad esempio un Dispositivo Diagnostico, che essere uno dei sistemi componenti come ad esempio un modulo acquisizione

dati da DM di un sistema di cartella clinica (che è, per definizione nell'MDR, un DM); infine più DM potranno essere tra i componenti della catena (un modulo di acquisizione dati di una cartella clinica elettronica, collegato ad un DM e magari servita da un SW costruito utilizzando AI).
La vulnerabilità rispetto ad un attacco Cyber potrebbe risiedere sia in un DM (SW o HW con SW e connessione) sia in un componente della parte amministrativa in linea con tutti gli altri. Come si riscontra in molti incidenti (anche quelli riportati dal Clusit) la backdoor può essere una errata gestione delle password di una macchina con funzioni SW di tipo amministrativo, che permette l'ingresso nella catena dove per necessità di funzionalità dei servizi eseguiti da più dispositivi sono non anonimizzate alcune informazioni relative al paziente in trattamento per garantire le funzionalità necessarie, creando danni di vario genere a seconda delle intenzioni dell'esecutore del crimine. Le violazioni sono quindi a carico dei dati sensibili, delle funzionalità specifiche sia amministrative che cliniche. Nel prosieguo si esemplificano alcune richieste della normativa NIS2 in relazione agli oggetti appena descritti, ed in particolare DM.

GESTIONE DELLA SUPPLY CHAIN E DEI FORNITORI CRITICI

La direttiva NIS2 impone un rafforzamento del controllo sull'intera catena di fornitura, inclusi produttori di componenti, software e fornitori di servizi di manutenzione per dispositivi medici e infrastrutture ICT sanitarie; qui, come si accennava pocanzi è coinvolta anche la Direzione Sanitaria che ha inteso proporre ed implementare il servizio digitale. La Direzione Sanitaria è coinvolta nell'esercizio della valutazione del rischio e, una volta che il servizio è in linea, nel Risk Management del servizio e di tutte le componenti che fanno parte dell'ecosistema di connettività dello stesso, come previsto dalla NIS2,. Il fabbricante dei DM deve fornire alla direzione sanitaria tutte le informazioni iniziali necessarie, in base anche alla propria valutazione del rischio, e continuare a farlo nel tempo, tenendo conto del complesso dei requisiti dell'MDR e della NIS2.
In particolare è necessario:

- Condurre valutazioni di sicurezza dei fornitori, con audit periodici e criteri di qualificazione basati sulla conformità a standard internazionali, conformità che dovranno essere richieste in sede di gara per poi applicarle in sede di verifica (es. ISO/IEC 27001, IEC 81001-5-1).
- Inserire nei contratti clausole vincolanti per la gestione degli incidenti di sicurezza, la notifica tempestiva e l'aggiornamento dei prodotti.
- Monitorare costantemente i fornitori critici, implementando sistemi di tracciabilità delle componenti hardware e software per ridurre il rischio di compromissione lungo la supply chain.

TEST DI RESILIENZA E SIMULAZIONI DI ATTACCO

Oltre alle misure preventive, la NIS2 richiede la verifica periodica dell'efficacia delle difese. Le strutture sanitarie e i produttori di dispositivi medici dovranno:

- Programmare audit che valutino lo stato di maturità e di resilienza dei sistemi supportati.
- Realizzare test di penetrazione e attività di red teaming mirate ai sistemi clinici e ai DM connessi. (Anche red team penetration test; RT è un processo che mette alla prova l'attuale sicurezza del sistema di un'organizzazione cercando di violarla come un hacker del mondo reale).

- Simulare scenari di indisponibilità prolungata di dispositivi critici, valutando l'impatto sulla continuità assistenziale e definendo misure di mitigazione.

Si possono trovare diverse opportunità di test per i SW DM. In particolare per le App sia DM che per wellness, che rappresentano un caso con perimetro molto vasto e difficile da controllare anche per l'alta volatilità delle proposte e versioni, è stata messa alla prova con progetti di valutazione europei la Specifica Tecnica ISO/TS 82304-2:2021 per la creazione di un'etichetta simile a quelle utilizzate per il consumo di energia degli elettrodomestici, nella quale ogni produttore deve rispondere a circa 80 domande comprese interoperabilità e security. Inoltre esistono diverse opportunità di eseguire serie di test di vulnerabilità come ad esempio quelle proposte da organismi internazionali come OWASP (Open Worldwide Application Security Project), che offre servizi come MASVS (Mobile Application Security Verification Standard) e MASTG (Mobile Application Security Testing Guide), utili per applicazioni, siti web, IoT.

INTEGRAZIONE TRA CYBERSECURITY E SICUREZZA CLINICA

Ai sensi dell'articolo 21(e), la sicurezza informatica deve essere integrata fin dalla fase di sviluppo e manutenzione dei sistemi.In questo senso si può dedurre che la gestione del rischio "cyber" va correttamente integrata nella gestione del "rischio clinico". Una indicazione base è quindi quella di avere un processo attivo che sia in grado di tradurre ogni vulnerabilità dei DM utilizzati in condizioni di rischio per il paziente. Per esempio, una vulnerabilità che si riferisca alla perdita di integrità dei dati gestiti andrà tradotta nel rischio di diagnosi errata con conseguente valutazione del danno verso il paziente. Tra le misure le misure tecniche/organizzative nella gestione dei DM con impatto nella sicurezza clinica, ricordiamo:

- Secure SDLC per software e firmware dei DM
- Gestione delle vulnerabilità end-to-end
- Hardening e configurazioni sicure dell'ambiente IT richiesto dai DM
- Monitoraggio continuo e rilevamento anomalie
- Gestione degli incidenti cyber integrata con i processi clinici

Anche qui si comprende come il Risk Management richiesto dalla Nis2 tutte le componenti che interagiscono nel processo clinico, con le relative responsabilità degli stakeholder coinvolti nella catena del servizio nel quale sono utilizzati i DM.

TRATTAMENTO DEI DATI E (PSEUDO) ANONIMIZZAZIONE

Sebbene la Direttiva NIS 2 non specifichi il trattamento dei dati personali, l'articolo 21 richiede misure organizzative globali di protezione. Nei contesti trattanti dati sanitari soggetti a GDPR, si richiede l'adozione di tecniche di anonimizzazione o pseudonimizzazione per flussi EHDS o IoMT, al fine di mitigare i rischi in caso di violazione.

Poiché alcuni DM (per la diagnosi o la terapia) saranno i terminali della catena o saranno guidati, per l'automazione del processo clinico, da parte ad esempio di altro DM (ad esempio un modulo acquisizione dati di un sistema di cartella clinica elettronica) che gestisca le informazioni sensibili necessarie allo svolgimento della funzione del DM terminale, è possibile che l'anonimizzazione o pseudonimizzazione non possano avvenire all'interno di questo perimetro. In tal caso si dovrà disaccoppiare ques-

ta parte funzionale dal resto del sistema con implementazioni appropriate per difendere la qualità e tutelare la privacy dei dati necessari alla funzione da svolgere, mentre sarà cura degli implementatori soddisfare il requisito della minimizzazione dei dati (vedi GDPR) necessari in questo stretto perimetro. In questo modo si rende sicura tutta la catena per quanto possibile, non danneggiando le funzionalità del DM terminale.
In ogni caso anche lo stato dell'arte della progettazione (da parte del fabbricante per il DM, nonché della Direzione Sanitaria e dei servizi coinvolti nell'implementazione di un servizio digitale) dovrà negli anni migliorare e permettere il disaccoppiamento tecnico tra parti differenziate degli elementi del sistema per garantire il soddisfacimento dei requisiti di Security delle normative coinvolte (al minimo MDR, NIS2 e GDPR).

INDICATORI DI PRESTAZIONE E REPORTING INTERNO

Per garantire un miglioramento continuo delle misure di sicurezza, le strutture sanitarie dovranno adottare indicatori di prestazione quali:

- Tempo medio di rilevazione di un attacco (Mean Time to Detect).
- Tempo medio di risposta e mitigazione (Mean Time to Respond).
- Percentuale di dispositivi aggiornati entro i tempi definiti dalle policy interne.
- Numero di incidenti evitati grazie a misure preventive.

Tali KPI dovranno essere oggetto di revisione periodica e inclusi nei report di sicurezza destinati alla direzione e agli organismi di controllo.
La governance deve garantire l'approvazione di tali indicatori e la formazione richiesta per i vertici delle organizzazioni.

GESTIONE DEI DISPOSITIVI LEGACY

Molte strutture ospedaliere utilizzano ancora dispositivi medici datati, privi di aggiornamenti di sicurezza o non conformi agli standard più recenti. In questi casi, è necessario condurre una approfondita analisi del rischio e implementare dei "controlli di compensazione", quali:

- Isolamento di rete e segmentazione dedicata.
- Monitoraggio continuo del traffico dati associato ai dispositivi legacy.
- Procedure operative che limitino l'uso dei dispositivi in contesti ad alto rischio.

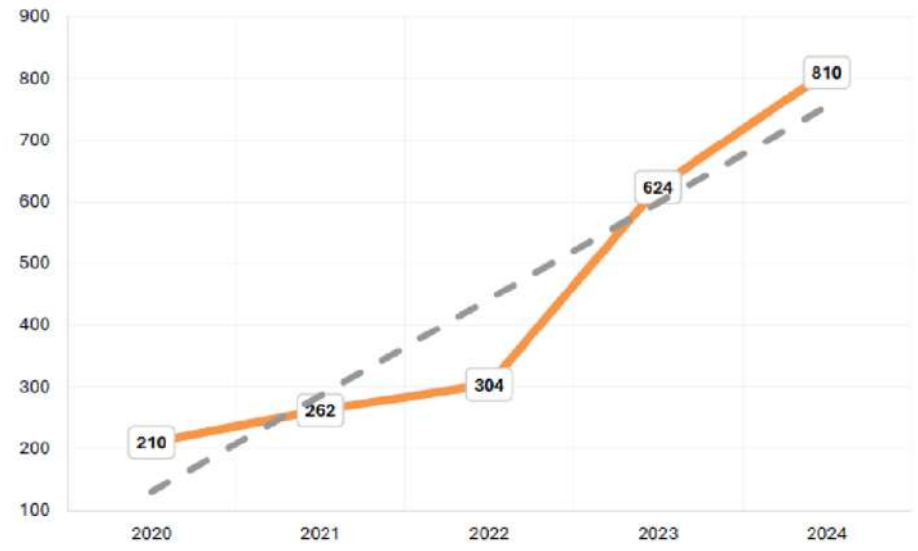
Queste misure devono essere documentate nei piani di gestione del rischio e aggiornate regolarmente in base all'evoluzione delle minacce.

Esperienze di cui tener conto per comprendere gli attacchi in ambito medicale: incidenti di Cyber Security in ambito medicale

DATI DAI RAPPORTI CLUSIT

Gli ultimi rapporti Clusit confermano una crescita significativa degli incidenti cyber che coinvolgono il settore sanitario e, in particolare, i dispositivi medici connessi. Questi dispositivi giocano un ruolo

Incidenti healthcare per anno 2020/24



© Hackmanac Global Cyber Attacks Report 2025

sempre più centrale nei flussi ospedalieri ma rappresentano un vettore di rischio critico per la sicurezza informatica delle strutture sanitarie, dei pazienti e dei dati sensibili.
I rischi ai quali è maggiormente sottoposto l'ambiente sanitario sono classificati nel rapporto 2025 come:

- Violazione dei dati: le violazioni dei dati possono portare alla perdita o al furto di informazioni personali dei pazienti, come i dettagli delle assicurazioni sanitarie, i numeri di previdenza sociale, i risultati dei test medici e altre informazioni sensibili.
- Ransomware: gli attacchi ransomware sono diventati sempre più comuni nel settore sanitario. I cybercriminali criptano i dati dei pazienti chiedendo un riscatto per sbloccarli, causando interruzioni nei servizi sanitari e mettendo a rischio la sicurezza delle persone malate.
- Accesso non autorizzato: gli hacker possono tentare di ottenere accesso non autorizzato ai sistemi informatici della sanità per rubare informazioni.
- Dispositivi medici connessi: con l'aumento dei dispositivi medici connessi alla rete, come monitor cardiaci e pompe per insulina, cresce il rischio di attacchi informatici che potrebbero compromettere la sicurezza dei pazienti.

Il settore sanitario a livello globale ha registrato 810 cyber incidenti divenuti di pubblico dominio nel 2024, il 30% in più rispetto all'anno precedente e il quadruplo rispetto al 2020 e 2021, con un trend in forte crescita che non accenna a diminuire. La media arriva a 68 incidenti al mese.
L'Healthcare è il terzo settore più colpito al mondo da incidenti informatici e Gartner prevede che, nel 2025, il 45% delle organizzazioni a livello mondiale subirà attacchi attraverso le vulnerabilità del software dei loro fornitori, un valore triplicato rispetto al 2021.

TIPOLOGIE DI INCIDENTI CYBER

Dai dati Clusit e da altre fonti del web che analizzano lo scenario, la classificazione degli incidenti più frequenti in ambito medicale riportata è la seguente:

Tipo di Incidente	Descrizione	Esempi/Casi segnalati
Ransomware	Blocca il funzionamento delle infrastrutture IT e dei dispositivi, spesso rendendo inoperativi anche monitor paziente, pompe infusionali e strumenti di diagnostica.	Attacco a Synlab Italia: servizi diagnostici sospesi.
Data Breach / Esfiltrazione Dati	Furto o pubblicazione di dati sensibili dei pazienti, compresi dati prelevati da dispositivi collegati alle cartelle cliniche.	Violazione della Croce Rossa Italiana: leak di 29GB di dati.
Interruzione/Ma-nipolazione di Servizi	Attacchi che portano all'arresto dei dispositivi critici per monitoraggio/terapia o alla modifica remota dei parametri di funzionamento con potenziali rischi clinici.	Interruzioni all'ASST Rhodense (chirurgia, terapia intensiva).
Accesso Non Autorizzato e Manipolazione	Ingresso nei sistemi di gestione dei dispositivi tramite vulnerabilità o credenziali deboli, con possibilità di alterazione delle configurazioni.	Casi di manipolazione su pompe infusionali e monitor cardiaci.
Attacchi Supply Chain	Compromissione dei fornitori o delle componenti software utilizzate nei dispositivi, sfruttando vulnerabilità in firmware o aggiornamenti. (Sono state scoperte in una libreria TCP/IP sviluppata da Treck Inc., che è stata ampiamente utilizzata in milioni di dispositivi in vari settori, anche dispositivi IoT di diverse marche. Le vulnerabilità sono state individuate da JSOF e sono state denominate "Ripple20" per indicare l'effetto a catena della loro diffusione.	Vulnerabilità Ripple20 che hanno colpito dispositivi vitali.
Compromissione dell'Integrità dei Dati	Alterazione dei dati clinici generati dai dispositivi, esponendo a diagnosi o terapie errate.	Episodi di alterazione esiti di laboratorio.

SINTESI DEGLI INCIDENTI RECENTI (2023-2024) IN ITALIA

- **Numero incidenti noti (2024):** 13 incidenti pubblici nel settore sanitario, di cui una quota rilevante ha coinvolto anche dispositivi medici connessi.

- **Tipologia e gravità:** Il 100% degli incidenti sanitari segnalati ha avuto impatti gravi o gravissimi (62% gravi, 38% gravissimi). In numerosi casi, i dispositivi medici sono stati direttamente interessati da blocchi o alterazioni, con impatti sia sull'operatività clinica sia sulla sicurezza dei pazienti.
- **Esempi rilevanti:**
  - Sanità lucana (Potenza): blocco a catena di strutture ospedaliere.
  - Synlab Italia: interruzione diagnostica per attacco ransomware.
  - ASST Rhodense: sospensione dei servizi chirurgici per compromissione di sistemi medici.
  - Croce Rossa Italiana: fuga massiva di dati anche da dispositivi in rete.

IMPATTI E RISCHI SPECIFICI

- **Blocchi operativi:** Arresto di terapie o procedure salvavita legate ai dispositivi colpiti.
- **Compromissione privacy:** Esposizione di dati clinici e biometrici scambiati dai dispositivi.
- **Manipolazione parametri:** Rischio clinico in caso di alterazione di dosaggi o settaggi sui dispositivi.
- **Effetti reputazionali ed economici:** Danni ingenti alla fiducia degli utenti e costi di ripristino elevati.

PRINCIPALI VULNERABILITÀ

Le principali vulnerabilità dei dispositivi medici evidenziate dai rapporti Clusit riguardano una combinazione di debolezze tecniche, scarsa gestione degli aggiornamenti e lacune nei processi di sicurezza. Queste vulnerabilità possono essere ricondotte a diverse categorie chiave:

1. **Sistemi Operativi Obsoleti o Non Supportati**
   Molti dispositivi medici utilizzano sistemi operativi non più supportati dai produttori, il che li rende particolarmente esposti a nuove minacce. Il rapporto Claroty (citato e ripreso da Clusit) evidenzia che l'85% dei dispositivi chirurgici dotati di sistemi non supportati mostra un'elevata probabilità di compromissione.
2. **Software non Aggiornabile e Patch Non Applicabili**
   Spesso i firmware dei dispositivi medici non possono essere aggiornati facilmente o non sono progettati per ricevere patch di sicurezza. Questo lascia le vulnerabilità note esposte per lunghi periodi, facilitando lo sfruttamento da parte dei cybercriminali.
3. **Password di Default o Credenziali Deboli**
   Molti dispositivi vengono distribuiti con password predefinite, facilmente reperibili o non modificate dagli amministratori. Questa pratica consente accessi non autorizzati e rappresenta una minaccia costante all'integrità dei sistemi.
4. **Comunicazioni non Cifrate**
   Una percentuale significativa di dispositivi medicali utilizza protocolli di comunicazione insicuri, talvolta senza cifratura, esponendo così i dati sensibili trasmessi a intercettazione o manomissione.
5. **Accessibilità Remota Non Sicura**
   Alcuni dispositivi, come sistemi di imaging, defibrillatori e robot chirurgici, sono accessibili da remoto senza adeguati controlli d'accesso, ampliando la superficie di attacco e i rischi di manipolazione.
6. **Vulnerabilità nella Supply Chain**
   Numerose vulnerabilità derivano da componenti software o hardware forniti da terze parti, come

evidenziato dagli incidenti legati a "Ripple20" che hanno coinvolto stack di rete impiegati in centinaia di dispositivi medicali.

7. **Mancanza di Segmentazione di Rete**
   L'assenza di isolamento tra dispositivi medici e altre reti ospedaliere permette una propagazione laterale rapida in caso di infezione o compromissione.
8. **Rischio di Manipolazione del Funzionamento**
   Vi sono casi documentati in cui attaccanti hanno simulato modifica di parametri vitali o di dosaggi di pompe per infusione, o persino alterazione di immagini mediche per trarre in inganno i clinici, con rischi diretti per la salute del paziente.

"Molti dispositivi hanno software non aggiornabili, password di default o comunicazioni non cifrate. [...] Un caso emblematico è quello della FDA statunitense che dovette ordinare il richiamo di 465.000 pacemaker per una falla che avrebbe permesso ai malintenzionati di alterarne il funzionamento con rischi potenzialmente letali."

Queste vulnerabilità intermittenti e persistenti rendono il parco dispositivi medici particolarmente esposto alle tipiche minacce del settore.

CYNERIO
(https://www.cynerio.com/)

Cynerio è una piattaforma di servizi per monitorare dispositivi esposti, problemi di rete e servizi correlati con la detezione e e mitigazione delle vulnerabilità.

Un importante report di Cynerio, basato sull'analisi di oltre 10 milioni di dispositivi medici connessi (IoT e IoMT) in più di 300 ospedali nel mondo, ha evidenziato che circa la metà di questi dispositivi non è adeguatamente protetta e quindi vulnerabile ad attacchi hacker.

In ambito sanitario più in generale, le violazioni della sicurezza informatica sono in forte aumento: dal 2018 al 2023 c'è stato un incremento del 102% delle violazioni nel settore sanitario, con oltre 167 milioni di persone colpite da gravi incidenti di cybersecurity.

Un caso emblematico in Italia è l'attacco ransomware al laboratorio SynLab Italia nel 2024, che ha causato l'interruzione di 380 laboratori e la compromissione di 1,5 terabyte di dati medici sensibili, dimostrando l'impatto rilevante e sistemico di questi attacchi sui dispositivi e dati medici.

Inoltre, nel 2023 i paesi UE hanno segnalato 309 incidenti significativi di cybersecurity nel settore sanitario.

Questi dati mostrano chiaramente quanto critiche siano le vulnerabilità dei dispositivi medici connessi e quanto frequenti e gravi siano gli attacchi informatici in questo ambito, con costi elevati e impatti su servizi essenziali.

OSSERVATORIO CYBER4HEALTH
(https://web.uniroma2.it/contenuto/cyber4health-tor-vergata-presenta-losservatorio-su-cybersicurezza-e-dispositivi-medici)

Dal 2000 a oggi sono stati segnalati diversi incidenti e vulnerabilità di cybersecurity riguardanti dispositivi medici di aziende come Medtronic e Abbott (ex St Jude Medical).

Negli ultimi 5 anni sono riportati circa 150-200 attacchi informatici registrati a dispositivi medici,

inclusi pacemaker e pompe di insulina, spesso fatti per estorcere denaro o danneggiare la salute di persone (anche personalità politiche).
Già Dick Cheney quando era vice presidente degli Usa (2001-2009) chiese ai suoi cardiologi di rimuovere la funzione wireless dal proprio defibrillatore per paura di poter subire un attacco terroristico; certamente una decisione eccessiva, ma in mancanza di una trasparente policy di cyber protezione il distacco dalla rete appare una opzione, che tuttavia significa non avere a disposizione molte caratteristiche e servizi oggi disponibili dalla trasformazione digitale.
Nel 2008, un team di ricercatori di università statunitensi ha dimostrato che è possibile un accesso remoto a defibrillatori cardiaci via segnali radio, con la possibilità di manipolare il dispositivo a distanza e causare danni anche fatali. A seguito di questo, sono stati fatti tentativi per migliorare la sicurezza di tali dispositivi.
Nel 2017 la FDA ha approvato un aggiornamento firmware correttivo per ridurre i rischi di sfruttamento di vulnerabilità di pacemaker Abbott (ex St Jude Medical).
Nel 2019 Medtronic ha pubblicato un avviso di sicurezza riguardante i sistemi di connessione wireless nei propri dispositivi.
Recentemente, nel 2023 il Garante privacy italiano ha sanzionato Medtronic di 300.000 euro per due incidenti di violazione dei dati personali che hanno coinvolto utenti della loro app per la misurazione del glucosio: invio errato via email di indirizzi in chiaro e mancanza di un'informativa completa.
Nel 2023-2025 continuano a emergere casi di vulnerabilità e attacchi a dispositivi medici, con piattaforme di monitoraggio e ricerca dedicate, come l'Osservatorio Cyber4health (presentata mercoledì 17 maggio 2025 a Tor Vergata). Viene confermato il rischio reale per la salute dovuto a manipolazioni maligne attraverso tecnologie wireless presenti nei dispositivi.

CONSIDERAZIONI FINALI

Gli incidenti cyber che colpiscono i dispositivi medici si suppone possano crescere con lo sviluppo dei dispositivi digitali, come SW di gestione e controllo dei DM aggiunti ai dispositivi tradizionali già connessi, nel loro sviluppo digitale, così come nuovi MDSW aumentando la superficie di attacco possibile.
La molteplicità e la diversità dei DM (più o meno complessi, con possibilità limitate o meno di inserire SW di mitigazione delle vulnerabilità), come ad esempio gli smartwatch, i pacemaker, i defibrillatori, le pompe di insulina, i neuro-stimolatori, possono avere effetti trasversali su tutto il sistema ospedaliero, dalla continuità operativa alla tutela del dato sanitario. L'adozione di misure organizzative, anche preventive, il monitoraggio continuo e la formazione per la gestione dei comportamenti degli operatori, insieme alle direttive NIS2, sono elementi cruciali per contrastare questa minaccia in evoluzione.
Esistono documenti specifici della Commissione Europea nell'ambito dei regolamenti e linee guida per i Dispositivi Medici (ad es MDCG 2019-16) che debbono essere presi in considerazione da parte dei produttori o gestori dei sistemi connessi (network), documenti che debbono essere coerenti tra i diversi contesti (dati, piattaforme, dispositivi Medici, IoT, SW sia MDSW che quelli per il wellness).
Le classificazioni qui riportate sono sintetizzate a partire dai dati e dagli episodi raccolti nei più recenti rapporti Clusit e analisi correlate sul 2023-2024, con dettagli su molteplici incidenti di pubblico dominio relativi a dispositivi medici in Italia e nel mondo.

Nei rapporti Clusit si sottolinea che il 100% degli incidenti cyber in sanità ha avuto impatti gravi o gravissimi, e i dispositivi medici sono tra gli asset più esposti e meno protetti.
In sintesi, secondo i rapporti Clusit e le fonti associate, le principali vulnerabilità dei dispositivi medici sono: sistemi operativi obsoleti, software non aggiornabile, password deboli, comunicazioni non cifrate, accesso remoto insicuro, debolezze nella supply chain, mancanza di segmentazione di rete e possibilità di manipolazione funzionamento.

CONCLUSIONE

I dispositivi medici rappresentano un punto di attacco sempre più sfruttato dalla criminalità informatica. Secondo i rapporti Clusit, tra il 2023 e il 2024 si sono verificati numerosi incidenti pubblici che hanno riguardato direttamente o indirettamente questi dispositivi, con conseguenze che vanno dal blocco operativo al furto e all'alterazione di dati sensibili, sottolineando l'importanza di un approccio integrato e proattivo alla sicurezza in ambito sanitario digitale.

Contesto legislativo e normativo

INTRODUZIONE

Il presente paragrafo si pone l'obiettivo di illustrare il contesto di applicazione delle direttive e normative comunitarie che regolano la gestione completa dei dispositivi medici nel ciclo di vita: dalle fasi di progettazione fino alla messa in uso, e in particolare di evidenziare gli aspetti legati alla sicurezza dei dispositivi medici in rete e delle reti IT medicali.
I regolamenti e le direttive comunitarie, queste ultime unitamente ai relativi recepimenti nazionali, rappresentano un obbligo per i soggetti coinvolti, principalmente i fabbricanti di soluzioni medicali e le organizzazioni responsabili che si dotano e utilizzano tali tecnologie. Le normative e regole tecniche, invece, non hanno carattere di cogenza; tuttavia, conferiscono strumento di conformità alle direttive e regolamenti, per cui vengono generalmente adottate, se ritenute valide come stato dell'arte (processo di armonizzazione).
Gli attacchi informatici e le violazioni dei dati, utilizzando principalmente agenti malevoli quali malware e/o ransomware, hanno un impatto negativo crescente sulle organizzazioni e sulle imprese in tutta l'UE. Con l'aumento delle minacce cyber, le strutture sanitarie devono adottare misure più rafforzate per la gestione del rischio, per garantire continuità operativa e resilienza dei sistemi IT, inclusi i medical device con le peculiarità che li caratterizzano rispetto agli asset IoT.
I dispositivi medici connessi in rete rappresentano una componente fondamentale per la diagnosi, il trattamento e il monitoraggio dei pazienti.
L'interconnessione di questi dispositivi in rete e l'utilizzo delle risorse e servizi informatici intra ed extra aziendali li rende vulnerabili e maggiormente esposti ad attacchi, rendendo così necessaria una regolamentazione specifica che garantisca la loro sicurezza e integrità.
Come noto agli addetti ai lavori i medical devices rappresentano spesso un asset critico all'interno delle organizzazioni sanitarie per due principali motivi:

- la peculiarità di gestione che richiedono in considerazione dello scopo e destinazione d'uso;
- la difficoltà nel garantire l'aggiornamento continuo delle varie componenti al fine di non inficiare le caratteristiche che hanno garantito il processo di certificazione.

L'applicazione di NIS2 al contesto dei dispositivi medici richiede un approccio integrato con le le altre direttive recepite e i regolamenti europei vigenti, senza tralasciare le diverse norme tecniche di riferimento e le diverse linee guida pubblicate (es. da MDCG).
La sicurezza informatica è sempre più rilevante e pertanto deve essere parte integrante degli elementi di riferimento durante la progettazione, l'implementazione e la gestione di un dispositivo medico.
Grazie ad una governance integrata, un risk management unificato e una conformità tecnica che tenga conto di MDR, NIS2, GDPR, AI Act, Data Act e delle norme ISO e CEI, sarà possibile affrontare le sfide sempre più complesse in ambito di cybersicurezza applicata ai dispositivi medici e alla protezione dei dati dei pazienti.
L'implementazione di sistemi di gestione multi-compliance e di strumenti di compliance automation può facilitare questo percorso, riducendo i costi operativi e rafforzando la sicurezza dell'intero ecosistema digitale sanitario. Investire in cybersecurity, sviluppo AI responsabile, sostenibilità e test approfonditi non è solo una necessità normativa, ma un'opportunità per costruire un futuro digitale più sicuro, efficiente e resiliente per la sanità.
Di seguito saranno trattate le principali leggi/regolamenti e le norme di settore inerenti al settore dei dispositivi medici e alla NIS2.

REGOLAMENTO MDR 2017/745

Il regolamento (UE) 2017/745 (MDR) richiede ai produttori di dispositivi medici di considerare lo stato dell'arte nella progettazione, nello sviluppo e nell'aggiornamento dei DM durante il loro intero ciclo di vita, stabilendo requisiti di sicurezza e prestazionali. Analoga richiesta riguarda i produttori di dispositivi diagnostici in vitro (IVD), la cui immissione in commercio è oggetto del regolamento (UE) 2017/746 (IVDR).
I produttori hanno obblighi sulla tracciabilità, la valutazione tecnica, la sorveglianza post-market e i requisiti che devono garantire per i software e i device medicali. Devono poter evidenziare le loro decisioni in ambito di innovazione (sulla base di standard applicabili, linee guida, conoscenze proprietarie e informazioni scientifiche/tecniche pubblicamente disponibili), dimostrando al contempo l'idoneità ad affrontare in modo proporzionato i rischi per la sicurezza.
In ambito di sicurezza, tra NIS2 e MDR/IVDR vi è una stretta correlazione, essendo evidente la necessità di garantire che i dispositivi medici siano mantenuti sicuri durante tutto il loro ciclo di vita, sia dal punto di vista della sicurezza funzionale (safety) sia di quella informatica (security). I fabbricanti e le organizzazioni responsabili sono tenute al mantenimento di tali caratteristiche nel tempo e nel contesto di applicazione specifico sulla base della destinazione d'uso.
La direttiva NIS2 ed i regolamenti MDR(IVDR trovano una sovrapposizione nei rispettivi campi di applicazione sul tema della gestione degli incidenti: da un lato vi sono l'MDR/IVDR che richiedono di notificare all'autorità competente l'avvenimento di incidenti significativi, ossia qualsiasi incidente che, direttamente o indirettamente, ha causato, può aver causato o può causare il decesso o un deterio-

ramento importante delle condizioni di una persona oppure una importante minaccia per la salute pubblica.
Dall'altro lato, un incidente grave ai sensi dell'MDR causato da un problema di cybersicurezza compreso nell'ambito della NIS2, deve essere segnalato ad ACN.

LINEE GUIDA MDCG

Le linee guida MDCG (Medical Device Coordination Group) sono responsabili della applicazione dei due nuovi regolamenti 745/2017 (MDR) e 746/2017 (IVDR). I due regolamenti hanno l'obiettivo di rafforzare la sicurezza dei dispositivi medici.
Il documento MDCG 2019-11 (Qualification and classification of software) fornisce linee guida destinate ai fabbricanti di software medicali per la qualificazione e la classificazione del software come dispositivo medico (MDSW).
Definisce i criteri per la qualificazione dei software che rientrano nell'ambito di applicazione della nuova normativa sui dispositivi medici e fornisce indicazioni sull'applicazione dei criteri di classificazione per il software ai sensi del regolamento (UE) 2017/745 – MDR e del regolamento (UE) 2017/746 – IVDR.
L'MDCG 2019-16 (Guidance on Cybersecurity for medical devices) ha invece l'obiettivo di dare indicazioni ai fabbricanti in materia di sicurezza informatica, per fornire una guida su come soddisfare i requisiti essenziali. Si applica ad ambiti di gestione e riduzione del rischio e degli eventuali effetti collaterali indesiderati, oltre che all'integrazione del software in un ambiente IT e della relativa interoperabilità tra sistemi.
Inoltre, considerando la complessità della catena di fornitura e il ruolo giocato dai differenti operatori per assicurare che il dispositivo sia protetto da minacce cyber, sono presenti nel documento considerazioni aggiuntive per altri attori diversi dal fabbricante che rientrano nella cosiddetta supply chain.
La guida pone anche l'attenzione sui requisiti relativi alla protezione e riservatezza dei dati personali associati all'uso di dispositivi medici.
Nel contesto della sicurezza informatica e nell'ambito del Regolamento sui dispositivi medici (MDR), il fabbricante deve essere particolarmente consapevole delle seguenti prescrizioni e indicazioni:

- Privacy e protezione dei dati;
- Procedure di valutazione della conformità;
- Sistema di sorveglianza post-commercializzazione del fabbricante composta da un piano di attività con rapporti periodici oggetto di riesame ed eventuale interventi correttivi sui DM.
- Segnalazione di incidenti gravi e azioni correttive di sicurezza, derivanti da guasti e problemi;
- Analisi di incidenti gravi e azioni correttive di sicurezza;
- Documentazione tecnica sul dispositivo e sulla sorveglianza post-commercializzazione;
- Valutazione clinica e follow-up post-commercializzazione.

Inoltre, la direttiva NIS2 impone che anche gli assets informatici, oltre che essere in linea con l'MDCG 2019-16, siano progettati con accortezze rivolte alla sicurezza informatica, garantendo cybersecurity by design e by default, per assicurare la protezione dei dati e la resilienza contro gli attacchi informatici.

La linea guida identifica delle misure indicative, consigliate per tutte le applicazioni. Tra queste sono identificati ad esempio i controlli per l'accesso e i sistemi di autorizzazione e autenticazione del personale; è importante che vi sia un logoff automatico o comunque un blocco temporizzato per l'accesso all'applicazione, che eviti che un utente possa utilizzare impropriamente l'account personale di un altro.
Si rende necessario delineare al meglio le configurazioni delle caratteristiche di sicurezza dei sistemi, sia per garantire integrità e autenticità delle informazioni ivi contenute sia per evitare di identificare i soggetti coinvolti e mantenere la confidenzialità dei dati anche dopo l'archiviazione. Integrità e confidenzialità vanno mantenute anche durante la trasmissione dei dati mediante protezioni quale la cifratura degli stessi.
La cybersecurity va garantita durante tutto il ciclo di vita del dispositivo medico, affinché il prodotto sia costantemente up-to-date. Inoltre, per evitare la compromissione, il deterioramento o la perdita dei dati in caso di incidenti e attacchi malware, è necessario prevedere delle misure sia attive che passive adottando un data backup and disaster recovery plan.
L'MDCG riporta anche una sezione più strutturata con le misure di sicurezza da adottare per la gestione degli asset IoMT e delle reti IT medicali (IT security requirements for the operating environment). Tra queste è di rilevante importanza condurre una valutazione del rischio, riesaminata ad ogni introduzione di un nuovo dispositivo in rete, insieme alla definizione di un insieme di policy di sicurezza IT di base, oltre che un monitoraggio continuo.

NORMA ISO 80001

La norma ISO 80001, in particolare la 80001-1, si applica a dispositivi medici designati ad essere incorporati in reti IT (rete IT medicale), per una gestione del rischio durante l'intero ciclo di vita.
Una rete IT medicale è una rete IT in cui vi è incorporato almeno un device medico
È fondamentale definire un quadro preciso che identifichi ruoli e responsabilità, questo aspetto viene ripreso e approfondito da NIS2 sottolineando anche il tema dell'affidabilità delle risorse umane dall'assunzione alla cessazione del rapporto. In questi termini, è necessario distinguere gli obblighi della figura del fabbricante, ovvero colui che si occupa della progettazione, dello sviluppo e della immissione sul mercato del dispositivo medico, e quelli dell'organizzazione responsabile, l'ente responsabile dell'uso e della manutenzione della rete IT-medicale.
È importante per assicurare una raccolta, analisi, valutazione e archiviazione delle informazioni conforme ed efficace alla gestione del rischio, tale da garantire safety, effectiveness (efficienza che deve perseguire l'organizzazione responsabile) e data and system security.
La convergenza tra dispositivi medici e sistemi di gestione delle informazioni comporta la necessità di un cambiamento nel modo in cui vengono preservate sicurezza ed efficacia. Mentre la responsabilità del fabbricante del DM nella commercializzazione non subisce variazioni, l'ambiente in cui è inserito il dispositivo, ovvero la rete IT, muta costantemente.
Prima che un dispositivo venga collegato a rete dati, è necessaria una valutazione dei rischi aggiornata periodicamente e riesaminata per ogni cambiamento introdotto nella rete, in modo da garantire un livello del rischio accettabile per la safety del paziente.

Il risk manager IT è la figura espressamente dedicata a garantire il controllo del rischio per la rete IT medicale.
La valutazione del rischio può essere affrontata con due logiche: top down e bottom up. La prima si sviluppa da una visione di insieme della rete IT e va a valutare via via un dettaglio maggiore, la seconda va a costruire, partendo dai particolari della rete, una visione più ampia.
Oltre a questa valutazione, la norma esplicita anche il fatto che dovrebbe essere prodotta una apposita documentazione contenente tutte le istruzioni riguardanti:

- le procedure di inserimento di DM nella rete IT-medicale
- le modalità di trasferimento dati dei DM attraverso la rete
- le caratteristiche di base dei DM che l'utente abilitato dovrebbe conoscere per utilizzare al meglio e responsabilmente il dispositivo

Inoltre, nella fase di approvvigionamento di un medical device da collegare alla rete dati, la normativa propone di redigere un accordo di responsabilità contenente un riepilogo delle responsabilità tra chi acquista e chi fornisce un bene.
La norma ISO 80001 si concentra sulla gestione della sicurezza dei DM e dei sistemi in cui sono interconnessi; pertanto, vi dovrà essere conformità con NIS2 per garantire un framework che assicuri la cybersecurity in ambito ospedaliero.
Sebbene la 80001 tratti già la data e system security tra le proprietà chiave per l'analisi dei rischi, la NIS2 impone delle misure specifiche su tale aspetto, in modo tale che la riservatezza, l'integrità e la disponibilità dei dati siano garantiti sia a riposo sia in transito.
La cifratura dei dati è necessaria al fine di assicurare tali caratteristiche, in aggiunta devono essere progettati dei sistemi di backup con adeguata sicurezza fisica e informatica e devono esservi test periodici per valutare la conformità dei sistemi.
Sono rilevanti sistemi perimetrali, quali firewall, e sistemi di emergenza protetti da usare in caso di necessità.

NORMA CEI EN 62304 E 62237 (NORME ITALIANE)

Le norme CEI EN 62304 e 62237 definiscono le prescrizioni relative al ciclo di vita del software per dispositivi medici, promuovendo una classificazione finalizzata alla corretta gestione dei SW stessi
Si tratta di documenti utili per i produttori di dispositivi medici che incorporano software, in quanto forniscono linee guida e requisiti per lo sviluppo sicuro, la gestione delle modifiche comprendente le fasi di verifica e validazione, la manutenzione e la gestione dei rischi del software utilizzato nei dispositivi medici nell'ottica del change release management.
La norma CEI EN 62237 sottolinea quanto sia fondamentale procedere con l'identificazione del software, processo delicato che inizia con il comprendere se il software sotto esame sia o meno dispositivo medico, di cui poi il fabbricante valuterà la destinazione d'uso e il contesto di destinazione. L'organizzazione responsabile andrà poi a definire l'uso effettivo e il contesto d'uso, facendo riferimento al contesto di utilizzo del prodotto nella situazione reale.
Il secondo aspetto importante da considerare è la distinzione tra software integrato in un dispositivo medico, software accessorio e software "standalone".

Nel primo caso dovrà seguire delle prescrizioni normative del dispositivo in cui è incorporato e dovrà essere classificato secondo la medesima classe di appartenenza. Nel caso di software accessorio, anch'esso dovrà seguire le prescrizioni normative dei dispositivi medici, mentre nell'ultimo caso di standalone è da considerarsi dispositivo medico attivo.
La norma IEC 62304 richiede determinate precauzioni sull'utilizzo del software. Contribuisce alla resilienza del software medicale, in linea con obiettivi NIS2, per garantire la sicurezza di dispositivi medici e prevede un'attività di "Software Risk Management", per la quale vi sono alcuni requisiti:

- Analisi del software per monitorare situazioni avverse
- Misure di controllo del rischio
- Misure di verifica del controllo del rischio
- Gestione del rischio successivamente a cambiamenti nel software

Il fabbricante assegnerà a ciascun sistema software una classe di sicurezza del software (A, B o C) in base ai possibili effetti sul paziente, sull'operatore o su altre persone, derivanti da un pericolo a cui il sistema software può contribuire.
Le classi di sicurezza del software saranno inizialmente assegnate in base alla gravità, come segue:

- Classe A: Non è possibile causare alcuna lesione o danno alla salute
- Classe B: è possibile indurre una lesione non grave
- Classe C: è possibile apportare una lesione grave al paziente

Se il pericolo potrebbe derivare da un mancato funzionamento del sistema software come specificato, la probabilità di tale guasto si presume pari al 100%.
Le principali differenze rispetto al software tradizionale sono le indicazioni relative alla descrizione di: matrice di tracciabilità, gestione dei rischi (analisi, mitigazione), piano di test, esecuzione dei test e registrazione dei risultati, documentazione (progettazione, manuale utente, manutenzione). Tutte queste attività richiedono di essere evidenziate tramite procedure, documenti, report, ecc.

NORMA ISO 27799

Lo standard ISO 27799, "Information security management in health using ISO/IEC 27002", fornisce linee guida e le best practices per la gestione della sicurezza delle informazioni, inclusa la selezione, l'implementazione e la gestione dei controlli nei vari contesti organizzativi, tenendo conto anche di quelli più a rischio. La ISO di riferimento è la ISO/IEC 27002 che viene integrata al fine di una applicazione più efficace nella gestione della sicurezza delle informazioni sanitarie per garantire riservatezza, integrità e disponibilità.
La riservatezza è essenziale per il mantenimento della privacy dei soggetti, l'integrità dei dati deve essere protetta per garantire la sicurezza dei pazienti e la disponibilità è fondamentale per permettere un'efficace erogazione delle prestazioni sanitarie.
La direttiva NIS2 e lo standard ISO 27799 sono due quadri normativi che si occupano di sicurezza informatica, ma con ambiti e obiettivi diversi, specialmente nel settore sanitario.
La NIS2 è una direttiva europea, recepita con D.Lgs. 138/2024, che mira a rafforzare sicurezza cibernetica delle infrastrutture critiche e dei settori essenziali, mentre la ISO 27799 è una norma tecnico internazionale che fornisce linee guida specifiche per la protezione dei dati sanitari.

La norma può essere considerata funzionale alla attuazione della NIS2, aggiungendo misure di sicurezza quali il controllo dell'accesso e la protezione di dati sensibili anche tramite configurazioni specifiche della rete dati come la segmentazione.
L'obiettivo principale della segmentazione è ridurre il rischio di attacchi e adattare le misure di sicurezza alle esigenze di utilizzo. La microsegmentazione è un approccio più moderno per fornire alle reti una maggiore sicurezza, pienamente in linea con gli ambienti IT dinamici e funzionali in relazione alle specifiche tipologie e esigenze di gestione degli asset connessi.
La microsegmentazione si discosta notevolmente dalle misure di sicurezza tradizionali, che si concentrano spesso solo sulla difesa del perimetro, proteggendo i confini della rete, ma conservando delle vulnerabilità all'interno. A tal fine, è molto rilevante la segmentazione per proteggere aree con differente funzionalità nella rete, creando di fatto un ambiente "zero trust". Questo riduce drasticamente la portata dei potenziali attacchi, sebbene vadano considerate le attività di gestione e manutenzione delle configurazioni che introduce.
Prevede la suddivisione di una rete in parti sicure e gestibili, note come segmenti: ogni segmento è isolato e dispone di un unico set di criteri di sicurezza. Ciò consente un maggiore controllo sul flusso di traffico, assicurando che sia consentito solo quello legittimo. Se una minaccia si infiltra nel sistema, la segmentazione impedisce che si sposti lateralmente attraverso la rete, evitando un single "point of failure" che determini l'interruzione dell'intero sistema.

MISURE ACN

L'agenzia per la Cybersicurezza Nazionale (ACN) opera come punto di riferimento nazionale in ambiti di prevenzione, monitoraggio e risposta alle minacce informatiche, coordinando varie attività tra cui vi è la gestione degli incidenti informatici, lo sviluppo e aggiornamento del PNSC (Perimetro Nazionale di Sicurezza Cibernetica), oltre che il coordinamento dell'attuazione della NIS2.
Il D.Lgs. 138/2024, che recepisce la direttiva europea NIS2 2022/2555, ha ampliato significativamente il perimetro di applicazione rispetto alla precedente normativa, includendo nuovi settori. Con le proprie determinazioni che hanno valore di legge, l'ACN fornisce maggior chiarezza sulle misure concrete che devono essere adottate per garantire la sicurezza dei propri sistemi informativi.
L'agenzia per la Cybersicurezza Nazionale (ACN) ha pubblicato delle misure minime e alcune raccomandazioni per la sicurezza informatica volte a definire e fare chiarezza sulle specifiche tecniche che devono essere implementate per adempiere agli obblighi imposti dalla direttiva NIS2 nel contesto italiano.
Ogni struttura sanitaria è chiamata ad adottare le misure pubblicate da ACN sulla protezione dei dispositivi medici, che partecipano alle azioni per raggiungere la conformità alla NIS2.
Tra le misure principali per ridurre il rischio di attacchi e indisponibilità dei dati introdotte da NIS2 e riportate negli articoli 32 e 33, rispettivamente per soggetti essenziali e per soggetti importanti, vi sono:

- Ispezioni in loco e vigilanza a distanza, compresi controlli casuali, effettuati da professionisti formati;
- Audit sulla sicurezza periodici e mirati effettuati da un organismo indipendente o da un'autorità competente;

- Audit ad hoc, ivi incluso in casi giustificati da un incidente significativo o da una violazione della direttiva NIS 2 da parte del soggetto essenziale;
- Scansioni di sicurezza basate su criteri di valutazione dei rischi obiettivi, non discriminatori, equi e trasparenti, se necessario in cooperazione con il soggetto interessato;
- Richieste di informazioni necessarie a valutare le misure di gestione dei rischi di cybersicurezza adottate dal soggetto interessato, comprese le politiche di cybersicurezza documentate, nonché il rispetto dell'obbligo di trasmettere informazioni alle autorità competenti;
- Controllo e monitoraggio dell'accesso ai dati, documenti e altre informazioni;
- Richieste di dati che dimostrino l'attuazione di politiche di cybersicurezza, quali i risultati di audit sulla sicurezza effettuati da un controllore qualificato e i relativi elementi di prova;
- Notifica degli incidenti e di violazioni dei dati o di minacce significative per la sicurezza.

Le misure di sicurezza introdotte non fanno esplicito riferimento ai medical device o a categorie specifiche di assets IoMT, sebbene come evidenziato nel presente documento sia assolutamente necessario un approccio specifico per tali assets nell'ambito del piano di gestione del rischio. Le figure dell'IT manager e dell'ingegnere clinico dovranno sicuramente individuare delle strategie idonee di mitigazione dei rischi, introducendo delle misure di sicurezza adeguate al contesto dei dispositivi medici che tengano conto della criticità degli stessi ma anche della differente gestione e del ruolo del fabbricante oltre che dell'organizzazione responsabile. In tal senso anche gli strumenti e le modalità di analisi devono essere ponderati in maniera adeguata e in conformità alle normative e regole tecniche di settore, in particolare per le reti IT medicali vanno tenute in considerazione le ISO 80001, per evitare di compromettere il corretto funzionamento dei sistemi o comunque di alterarne le caratteristiche principali a discapito di quanto previsto nei requisiti di certificazione.
Inoltre, per tutte le misure richieste in merito all'obbligo di notifica degli incidenti, andranno gestite in maniera armonizzata con le segnalazioni relative al monitoraggio dei dispositivi medici.

DECRETO EHDS

Il Regolamento sullo spazio europeo dei dati sanitari EHDS (European Health Data Space) punta ad istituire un quadro comune per l'uso e lo scambio di dati sanitari elettronici in tutta l'UE.
Intende migliorare l'accesso delle persone fisiche ai propri dati sanitari elettronici e il loro controllo sugli stessi, consentendo allo stesso tempo il riutilizzo di determinati dati ai fini di interesse pubblico, sostegno delle politiche e della ricerca scientifica.
Il regolamento promuove un ambiente di dati correlati in modo specifico alla salute, a sostegno di un mercato unico per i servizi e prodotti sanitari digitali. Inoltre, istituisce un quadro giuridico e tecnico armonizzato per i sistemi di cartelle cliniche elettroniche, promuovendo l'interoperabilità, la condivisione sicura dei dati sanitari, l'innovazione e il buon funzionamento del mercato interno.
Lo spazio europeo dei dati sanitari intende:

- consentire alle persone di accedere, controllare e condividere i loro dati sanitari elettronici a livello transnazionale per agevolare la prestazione di assistenza sanitaria (uso primario dei dati)
- consentire il riutilizzo sicuro e affidabile dei dati sanitari in ambiti quali la ricerca, l'innovazione, l'elaborazione delle politiche e le attività regolatorie (uso secondario dei dati)

- promuovere un mercato unico per i sistemi di cartelle cliniche elettroniche, a sostegno dell'uso sia primario che secondario.

Questo consentirà all'UE di sfruttare più efficacemente le potenzialità offerte da uno scambio, utilizzo e riutilizzo sicuro dei dati sanitari a vantaggio dei pazienti, degli operatori sanitari, dei ricercatori, degli enti regolatori e degli innovatori.
EHDS e NIS2 hanno l'obiettivo comune di proteggere i dati sanitari, oltre che garantirne la disponibilità per la continuità operativa.
Entrambi richiedono una gestione rigorosa dei flussi informativi e la protezione delle infrastrutture di rete che supportano l'interoperabilità, per ottenere una condivisione sicura dei dati sanitari.
La direttiva NIS2 impone standard comuni di cybersecurity per tutti gli operatori che accedono o gestiscono dati nell'ambito EHDS, in modo da garantire integrità e riservatezza dei dati durante la trasmissione e l'archiviazione, utilizzando strumenti come la cifratura end-to-end. Devono essere assicurate misure di autenticazione e di autorizzazione per limitarne l'accesso.
Lo EHDS sarà soggetto a requisiti elevati in termini di governance, sicurezza e resilienza, con audit periodici e interoperabilità sicura tra i Paesi.
L'EHDS introduce una serie di prescrizioni per i fabbricanti e gli organismi di vigilanza in termini di interoperabilità e di segnalazione di incidenti sui SW di cartella clinica (EHR). Queste prescrizioni vanno messe in relazione a quanto previsto dal regolamento dispositivi medici (MDR) e NIS2, per trovarne la giusta applicabilità e le corrette modalità di gestione.
Di particolare rilevanza è l'articolo 27, che specifica come i fabbricanti di dispositivi medici, anche quelli in vitro, devono dimostrare la conformità alle prescrizioni essenziali relative al componente software europeo di interoperabilità dei sistemi di EHR in modo tale che il tutto sia interconnesso nei sistemi e reso interoperabile, in maniera conforme.
L'art.27 prevede infatti che *"i fabbricanti di dispositivi medici o dispositivi medico-diagnostici in vitro, che dichiarano l'interoperabilità di tali dispositivi medici o dispositivi medico-diagnostici in vitro con i componenti software armonizzati dei sistemi di cartelle cliniche elettroniche dimostrano la conformità alle prescrizioni essenziali relative al componente software europeo di interoperabilità dei sistemi di cartelle cliniche elettroniche e al componente software europeo di registrazione dei sistemi di cartelle cliniche elettroniche di cui all'allegato II, sezione 2, del regolamento EHDS.*
A tali dispositivi medici e dispositivi medico-diagnostici in vitro si applica l'articolo 36 del presente regolamento. I commi principali dell'articolo 36 sono il 5 e il 6 indicati di seguito:
5. Qualora le specifiche comuni relative alle prescrizioni in materia di interoperabilità e sicurezza dei sistemi di cartelle cliniche elettroniche riguardino dispositivi medici, dispositivi medico-diagnostici in vitro o sistemi di IA ad alto rischio che rientrano nell'ambito di altri atti giuridici, come il regolamento (UE) 2017/745, (UE) 2017/746 o (UE) 2024/1689, l'adozione di tali specifiche comuni può essere preceduta, a seconda dei casi, da una consultazione con il gruppo di coordinamento per i dispositivi medici (MDCG) istituito dall'articolo 103 del regolamento (UE) 2017/745 o con il comitato europeo per l'intelligenza artificiale istituito dall'articolo 65 del regolamento (UE) 2024/1689 e il comitato europeo per la protezione dei dati (European Data Protection Board - EDPB)
6. Qualora le specifiche comuni relative alle prescrizioni in materia di interoperabilità e sicurezza

dei dispositivi medici, dei dispositivi medico-diagnostici in vitro o dei sistemi di IA ad alto rischio che rientrano nell'ambito di altri atti giuridici, come il regolamento (UE) 2017/745, (UE) 2017/746 o (UE) 2024/1689, incidano sui sistemi di cartelle cliniche elettroniche, la Commissione garantisce che l'adozione di tali specifiche comuni sia preceduta, a seconda dei casi, da una consultazione con il comitato EHDS e con l'EDPB."

REGOLAMENTO CLOUD ITALIA

Il regolamento Cloud Italia è un quadro unico che definisce requisiti per i fornitori Cloud qualificati per le pubbliche amministrazioni. Chiarisce aspetti riguardanti la localizzazione dei dati, le certificazioni di sicurezza e la continuità operativa.

Il Regolamento per le infrastrutture e i servizi cloud per la PA chiarisce:

- le modalità per la classificazione, per la migrazione e per la qualificazione dei servizi cloud, di cui la PA può approvvigionarsi ricorrendo al libero mercato;
- le misure e i requisiti per il raggiungimento dei livelli minimi di sicurezza, capacità elaborativa, risparmio energetico e affidabilità delle infrastrutture digitali per la PA;
- le caratteristiche di qualità, sicurezza, performance, scalabilità e portabilità dei servizi cloud per la PA.

I dispositivi medici che utilizzano servizi Cloud dovranno essere fare riferimento anche a tale regolamento.

AI ACT APPLICATO AI MDSW (MEDICAL DEVICE SW)

Il Regolamento UE 2024/1689 sull'Intelligenza Artificiale ("AI Act"), pubblicato sulla Gazzetta Ufficiale europea il 12 luglio 2024, ha aperto una nuova era per i software basati su sistemi di intelligenza artificiale (AI). Il Regolamento prevede una serie di regole per la progettazione, realizzazione e immissione sul mercato dei sistemi di AI, che troveranno applicazione non solo nei confronti dei fornitori stabiliti nella UE, ma anche nei confronti di quelli extra UE (articolo 2, lett. a. AI Act).

L'art. 3 dell'AI Act definisce sistema di AI: "un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsione, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali".

Si tratta di una definizione molto ampia, che ricomprende qualsiasi software che, per finalità determinate dall'uomo, sia in grado di generare output in grado di influenzare gli ambienti – quindi anche le persone – con cui interagiscono.

Secondo l'Explanatory Memorandum of the updated Oecd definition of an AI system, pubblicato nel marzo 2024 dall'OEDC.AI, un software rientra nella nozione di AI qualora vi siano:

- autonomie variabili (cioè, delle diverse capacità di apprendimento in diverse aree – come computer vision, elaborazione del linguaggio naturale, riconoscimento vocale, sistemi intelligenti di supporto alle decisioni, i sistemi robotici intelligenti);
- capacità di adattamento (cioè, la capacità di continuare ad evolversi attraverso l'interazione diretta (con input e dati) anche dopo l'immissione sul mercato;
- obiettivi espliciti (cioè definiti esplicitamente dall'uomo), impliciti, che possono derivare dalle rego-

le specificate dall'uomo o dai dati di addestramento (in quest'ultimo caso, l'obiettivo finale non è programmato esplicitamente, ma è incorporato attraverso i dati di addestramento e un'architettura di sistemi che impara a emulare quei dati), o non completamente conosciuti in anticipo (sistemi di raccomandazione che usano apprendimento per rinforzo per restringere gradualmente il modello delle preferenze dei singoli utenti);

- capacità di generare output, che possono essere raccomandazioni, previsioni e decisioni.

Se dunque un MDSW presenta le funzionalità di cui sopra, esso rientra nella definizione di "intelligenza artificiale" e deve quindi conformarsi anche all'AI Act.

Tuttavia, l'applicazione armonizzata dell'MDR e dell'AI ACT non è ancora ben definita in termini di contemporanea applicabilità allo stesso SW, considerando la natura "dinamica" dei modelli AI e quella più "statica" della certificazione MDR, che prevede la ripetibilità del risultato a parità di input. Il tema sarà sicuramente oggetto di analisi nei prossimi anni per valutare l'opportunità di un approccio modulare, cioè basato sulle diverse componenti che possono caratterizzare un SW, nei processi di certificazione MDR/AI ACT.

Al momento si può affermare che i fabbricanti di MDSW che utilizzano per lo sviluppo del prodotto sistemi di AI, devono attenersi certamente, oltre che al MDR/IVDR, anche all'AI Act.

L'AI Act distingue tra tre categorie di software di intelligenza artificiale:

- i sistemi di AI vietati (art. 5 AI Act);
- i sistemi di AI considerati ad alto rischio (artt. 6 e ss. AI Act);
- i sistemi di AI per finalità generati (artt. 51 e ss. AI Act).

I MDSW, che presentano le funzionalità della AI, rientrano per lo più nella categoria dei software ad alto rischio in quanto sono presenti i seguenti presupposti:

- il sistema di AI è stato progettato per essere un componente di sicurezza di altro prodotto oppure è esso stesso un prodotto autonomo;
- il prodotto che contiene il componente di sicurezza o il prodotto autonomo è soggetto a una valutazione della conformità da parte di un organismo notificato ai fini dell'immissione sul mercato o messa in servizio, ai sensi della normativa di armonizzazione dell'Unione Europea (in cui vi è indicato anche l'MDR).

Alla luce di quanto sopra, sono soggetti all'AI Act e rientrano nella nozione di "AI ad alto rischio" i MDSW di Classe IIa, IIb, III (sottoposti alla valutazione di conformità di un ente), mentre i MDSW di Classe I rientrano nei software non ad alto rischio.

Per i MDSW classificati ad alto rischio, l'AI Act prevede una serie di obblighi, che entreranno in vigore a partire dal 2 agosto 2027, Tali obblighi riguardano tutti gli operatori del settore, ovvero produttori, distributori, rivenditori e deployer.

Si designa chiunque utilizzi un sistema di AI a conformarsi alle specifiche dell'AI Act che riguardano la produzione e l'impiego di MDSW ad alto rischio, come alcune delle misure riportate di seguito:

- obbligo di adozione di un sistema di gestione del rischio;
- garantire elevati standard di qualità dei dati impiegati per addestrare il MDSW;
- obblighi di trasparenza e trasmissione delle informazioni concernenti il MDSW, al fine di limitare i rischi connessi alla sua potenziale opacità;

- adottare misure di sorveglianza umana del funzionamento del MDSW, nonché garantire idonei livelli di accuratezza, robustezza e cybersicurezza.

DATA ACT

Il Data Act europeo (Regolamento UE 2023/2854), in vigore dall'11 gennaio 2024 e pienamente applicabile dal 12 settembre 2025, introduce obblighi specifici per i dispositivi medici connessi, con l'obiettivo di garantire accesso, trasparenza e interoperabilità dei dati generati.
I dispositivi devono consentire l'accesso ai dati in modo semplice, sicuro e gratuito, utilizzando formati standard leggibili automaticamente e compatibili con i sistemi sanitari. Già in fase pre-contrattuale, è necessario fornire informazioni dettagliate su tipologia, formato, frequenza e modalità di accesso. Se l'accesso diretto non è tecnicamente possibile, il produttore deve garantire una trasmissione continua e tempestiva, mantenendo la qualità. I dispositivi devono essere progettati fin dall'origine per favorire la condivisione, con API dedicate e interfacce intuitive. Gli utenti hanno diritto a consultare e trasferire i dati a terzi.
Le aziende devono verificare se i propri prodotti rientrano tra quelli regolati, adottare strategie di conformità che includano revisione tecnologica, contratti, sicurezza e formazione, e prepararsi a controlli e sanzioni da parte dell'autorità nazionale, attesa entro settembre 2025.
Gli articoli chiave del regolamento (2, 3, 4, 5, 23–36) definiscono i prodotti connessi, regolano l'accesso e la condivisione dei dati, e impongono requisiti di interoperabilità. Questi obblighi pongono le basi per una gestione più aperta, sicura e innovativa dei dati sanitari, a beneficio della sanità digitale e degli utenti.

Acquisti di dispositivi medici nell'era della NIS2

INTRODUZIONE

La fase di approvvigionamento di beni e soluzioni IT medicali che devono essere parzialmente o completamente integrate nell'infrastruttura di rete e sistemistica aziendale rappresenta per l'azienda un momento cruciale per definire il perimetro di responsabilità del fornitore.
Oltre a questo, le indicazioni contenute nella documentazione tecnica di gara, consentono all'azienda sanitaria la definizione della postura relativamente alla sicurezza all'ingresso della soluzione, di conseguenza il livello di rischio minimo accettabile dall'azienda stessa.
Di seguito verrà dunque presentato un elenco di informazioni/richieste che dovranno essere corrisposte dal fornitore in fase di presentazione dell'offerta. Per rendere efficace la trasmissione di tali richieste/specifiche potrebbe essere opportuno inserirle in un documento, ad esempio "allegato IT" da allegare alla documentazione di gara. Per rendere valido il documento nella sua interezza, è opportuno richiederlo restituito e firmato per attestazione di quanto dichiarato.
Questo documento dovrà essere indicato nel disciplinare di gara o nel capitolato speciale d'appalto come l'unico riferimento valido per quanto riguarda la gestione per la parte IT medicale relativa alla procedura di affidamento, per evitare che eventuali indicazioni contrastanti contenute nel capitolato tecnico vengano prese come riferimento.

Nei paragrafi successivi verrà riportato un esempio di come strutturare questo documento, e quali argomenti toccare.
La prima parte tratterà aspetti di carattere generale che si prestano ad essere utilizzabili in qualsiasi percorso di acquisto, nella seconda parte verranno fatti espliciti riferimenti a caratteristiche e indicazioni che la soluzione proposta dovrà rispettare in due situazioni specifiche:

- soluzione stand alone;
- soluzione integrata con i sistemi informativi dell'azienda.

In aggiunta nel documento sopra citato, allegato IT, è possibile fornire una indicazione di quale sia l'architettura della infrastruttura di rete aziendale e come questa viene gestita. Inoltre è possibile descrivere come è configurata l'area sistemistica (ad esempio, quanto gestito in azienda, servizi IaaS privati o della in-house regionale su cui potenzialmente appoggiare i nuovi sistemi) e come questa sia organizzata e gestita anche in considerazione di sviluppi futuri aderenti alle indicazioni del Piano Triennale dell'informatica nella PA.

REQUISITI NORMATIVI DI ORDINE GENERALE PER LA PARTE IT

Di seguito si riportano delle considerazioni di carattere generale dell'area IT alle quali il fornitore deve rispondere, ove applicabili:

- dal Regolamento Europeo sulla Protezione dei Dati – GDPR del 14.04.2016 (https://eur-lex.europa.eu/) e al D. Lgs. 196/2003 s.m.i., cosiddetto Codice Privacy, così come novellato dal D.Lgs. 101/2018; l'aggiudicatario verrà designato responsabile ex art.28 del GDPR e dovrà produrre ed attuare tutto quanto richiesto in capitolato e suoi allegati, fornire supporto alla stesura della DPIA, prima del collaudo e per tutta la durata del contratto;
- dalla Circolare AGID 18 aprile 2017, n. 2/2017, recante "Misure minime di sicurezza ICT per le pubbliche amministrazioni";
- il rispetto di quanto prescritto nelle "linee guida di sicurezza nello sviluppo delle applicazioni" AgID, anche dette "linee guida AgID per lo sviluppo sicuro del software";
- la conformità alle regole sull'interoperabilità prescritte dalle linee guida emanate in attuazione dell'articolo 73 del CAD (d.lgs 82/2005);
- conformità della soluzione a quanto indicato nelle linee guida n.8 di ANAC, al fine di scongiurare il lock-in, per tutte le componenti di fornitura.

REQUISITI NORMATIVI SPECIFICI PER LA PARTE MEDICALE

Qualora il prodotto dovesse rientrare nella definizione di dispositivo medico, anche in relazione alla destinazione d'uso identificata, dovrà trovare piena rispondenza a quanto previsto dalla normativa sui dispositivi medici, MDR oppure IVDR.
I sistemi IT oggetto di fornitura, integrati nella rete aziendale, e di conseguenza inseriti in una rete che ospita al suo interno dispositivi medici (ad esempio software medicali, ecotomografi, elettrocardiografi, colonne per endoscopia, ...) dovranno rispettare quanto indicato nella ISO 80001-1, ovvero la norma che definisce obiettivi e perimetri di responsabilità nella gestione delle reti IT medicali. In conformità alla normativa vigente, prima della messa in produzione di qualsiasi soluzione è forte-

mente consigliata la sottoscrizione di un accordo di responsabilità, volto a definire le competenze in relazione ai rispettivi ambiti di intervento.
Se l'oggetto di fornitura include dispositivi medici, il fornitore dovrà compilare, sottoscrivere e allegare all'offerta tecnica il modulo Manufacturer Disclosure Statement for Medical Device Security (MDS2) nella sua versione più aggiornata (attualmente 2019, sito NEMA), in modo da permettere all'azienda sanitaria una più agevole valutazione delle eventuali criticità della messa in uso dei sistemi offerti anche secondo EC/TR 80001-2-2.
La fornitura, nel caso di integrazione con altri dispositivi medici già presenti in azienda, oppure verso applicativi trasversali o verticali, dovrà essere conforme ai profili di integrazione definiti da IHE per lo specifico ambito di utilizzo. Quindi dovranno essere riconoscibili e identificabili i singoli attori e le transazioni, i quali dovranno essere aderenti a quanto definito nei technical framework di pertinenza per la specifica applicazione. Ad esempio, per la gestione di soluzioni di digital pathology, dovranno essere rispettati attori e transazioni previsti nel profilo IHE DPIA. Nel caso in cui l'oggetto di fornitura sia una verticale di reparto è necessario che la produzione dei referti avvenga secondo le specifiche indicate da HL7 Italia, ovvero che sia conforme allo standard CDA2 per la corretta alimentazione della nuova versione del FSE 2.0.

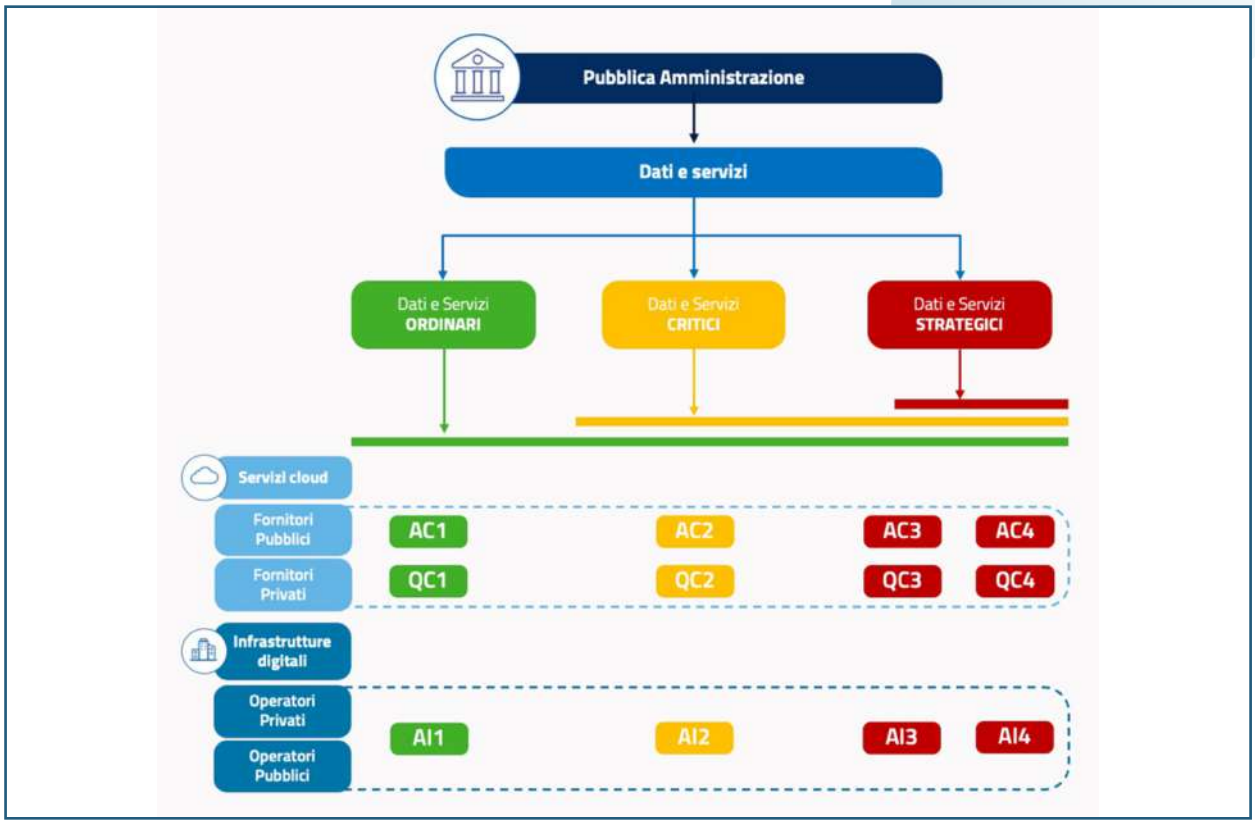
REQUISITI NORMATIVI PER LE SOLUZIONI SAAS

In coerenza con quanto stabilito dal Piano Triennale AgID, che suggerisce un approccio "Cloud First", i servizi oggetto di fornitura potranno essere erogati in modalità SaaS, i quali dovranno essere pubblicati sul Cloud Marketplace di ACN, la piattaforma che espone i servizi e le infrastrutture qualificate da ACN secondo quanto previsto dal Regolamento Cloud per la PA, adottato con Decreto di ACN n. 21007 del 27.06.2024.
I servizi SaaS forniti dovranno avere caratteristiche tecniche compatibili con tale modalità di erogazione in maniera nativa, ovvero dovranno essere SaaS by design.
La scelta della tipologia del servizio cloud si basa su una preliminare definizione dei dati e servizi che verranno trattati ed erogati per il suo tramite. Infatti i servizi cloud si differenziano su vari livelli, ognuno con caratteristiche opportune per particolari tipologie di dati e servizi.
Di seguito si riporta la classificazione dei dati e servizi definita da AgID (futura revisione da parte di ACN):

- strategico: dati e servizi la cui compromissione può avere un impatto sulla sicurezza nazionale;
- critico: dati e servizi la cui compromissione potrebbe determinare un pregiudizio al mantenimento di funzioni rilevanti per la società, la salute, la sicurezza e il benessere economico e sociale del paese;
- ordinario: dati e servizi la cui compromissione non provochi l'interruzione di servizi dello Stato o, comunque, un pregiudizio per il benessere economico e sociale del paese.

In considerazione della tipologia di dati trattati in ambito sanitario è evidente che la corretta classificazione risulti essere di livello critico, per tutte quelle applicazioni che gestiscono dati sanitari. Invece una soluzione in SaaS per gestire il magazzino, non trattando dati relativi allo stato di salute, è riconducibile alla categoria di dati e servizi ordinari.

Il Regolamento Cloud per la PA individua i livelli di servizio cloud adatti alla gestione delle varie tipologie di dati e servizi indicati in precedenza secondo il seguente schema:



In considerazione di ciò, in linea con quanto indicato nel Regolamento Cloud per la PA, il livello minimo di servizio SaaS utilizzabile per dati e servizi di livello critico risulta essere il secondo. Pertanto il fornitore che parteciperà alla procedura dovrà dare evidenza di possedere una valida qualificazione della propria soluzione, riscontrabile sul portale di ACN.
Nella situazione in cui il fornitore non fosse in grado di fornire una soluzione SaaS qualificata, è possibile per l'azienda sanitaria scegliere di posizionare la componente applicativa su una infrastruttura IaaS di livello adeguato già nelle disponibilità dell'ente.
I servizi SaaS offerti dovranno essere fruibili tramite collegamento Internet e tramite i web browser supportati dai principali vendor mondiali e senza alcuna componente aggiuntiva; la sicurezza delle connessioni tra browser e servizi SaaS remoti dovrà essere adeguata alla tipologia di dati trattati, per esempio tramite opportuna implementazione del protocollo HTTPS, ovvero i servizi dovranno sempre essere fruibili in maniera efficace e sicura tramite Internet.
È opportuno che venga richiesto che i server che contengono i dati trattati di titolarità dell'azienda sanitaria siano residenti all'interno della UE e che per nessuna ragione dovranno essere effettuate copie di tali dati al di fuori del perimetro della UE, neppure per motivi di continuità di servizio e disaster recovery.

Una ulteriore accortezza per soluzioni in SaaS, al fine di migliorare la definizione dei perimetri di responsabilità, è l'auspicabilità che il sistema fornito venga configurato per gestire sistemi di autenticazione federata, in modo tale da sfruttare l'IdP aziendale svincolandosi completamente da politiche di dominio infrastrutturale attive dell'ente. Questo a tutela del paradigma SaaS, dove la gestione della soluzione è completamente a carico del fornitore.
La fruizione delle componenti applicative offerte in SaaS dovrà essere il più aderente possibile al paradigma ZFP, tramite interfacce web messe a disposizione dall'ambiente SaaS per la fruizione del servizio. In caso di carenze architetturali o prodotti non ancora ZFP è consentito l'utilizzo di soluzioni di virtualizzazione applicativa o del desktop, nel rispetto della marcatura CE del software DM.

RESPONSABILITÀ PROPRIE DELL'AGGIUDICATARIO

In generale l'aggiudicatario si assume la piena responsabilità della sicurezza informatica e del trattamento dei dati, in particolare in merito all'integrità, disponibilità e riservatezza dei dati e dei sistemi. Pertanto, anche nei casi in cui la sicurezza dei dati gestiti da sistemi oggetto di fornitura è legata ad hardware e software in gestione di altro soggetto, l'aggiudicatario rimane responsabile del monitoraggio di tali elementi segnalando eventuali inadeguatezze.
A tale scopo è opportuno che l'aggiudicatario richieda gli strumenti opportuni per fare audit e monitoraggio, per eseguire le ricerche di anomalie e comunicare formalmente proposte percorribili per il raggiungimento degli obiettivi di sicurezza.
In base alla natura del servizio/prodotto verranno richiesti al fornitore certificazioni e requisiti di competenza specifici. In aggiunta a ciò, in caso di contratti di lunga durata (come ad esempio l'acquisto di una soluzione software dispositivo medico con manutenzione/supporto per più anni), il fornitore è tenuto a sostenere sessioni di aggiornamento per tutta la durata contrattuale.
Nel caso di progetti complessi è onere del fornitore la configurazione di un ambiente di test dove verranno implementate in prima istanza tutte le funzioni per certificare il funzionamento prima della messa in produzione della soluzione completa.
Qualora ci sia la necessità, l'aggiudicatario dovrà essere disponibile a fornire l'adeguata formazione e manuali necessari alla gestione in autonomia da parte dell'azienda sanitaria del software oggetto di fornitura.
Per tutta la durata contrattuale il fornitore dovrà garantire:

- il servizio di manutenzione per ogni componente della fornitura oggetto di gara, includendo a costo zero eventuali adeguamenti normativi che dovessero realizzarsi durante la fase contrattuale;
- gli aggiornamenti applicativi delle componenti per evoluzione tecnologica, major e minor release, inclusi quelli per i sistemi operativi oggetto di fornitura;
- gli aggiornamenti volti a risolvere vulnerabilità sia dei sistemi operativi che della parte applicativa della fornitura;
- l'implementazione di tutte le misure di mitigazione disponibili volte a ridurre il rischio di sfruttamento della vulnerabilità fino al rilascio dell'aggiornamento ufficiale;
- il mantenimento di un registro degli aggiornamenti, sia applicativi che di sicurezza;
- eseguire verifiche e controlli in conformità con quanto indicato dal produttore della soluzione;

- un dialogo costante per la gestione delle abilitazioni ai sistemi/soluzioni fornite;
- la comunicazione tempestiva di quanto in essere che potrebbe determinare un rischio per la salute o per la tutela dei diritti del personale dell'azienda sanitaria o dei suoi utenti.

DEFINIZIONE DEL PERIMETRO ARCHITETTURALE AZIENDALE

Di seguito verranno indicati due scenari che aiuteranno a definire i profili di responsabilità e pertinenza della fornitura, individuando nello specifico quanto di competenza del fornitore e quanto dell'azienda. Verranno presentate delle indicazioni basate su normativa di settore, linee guida e best practice da utilizzare direttamente come base per la stesura dell'allegato IT.

Scenario 1: sistemi isolati

Nel primo scenario, gli host oggetto di fornitura saranno integrati nella sola infrastruttura di rete aziendale e saranno oggetto di policy di segmentazione e segregazione del traffico. La segmentazione del traffico verrà effettuata assegnando agli host stessi una specifica classe di indirizzi IP e verranno inseriti in una VLAN dedicata, dalla quale potranno effettuare solo il traffico necessario per svolgere le funzioni richieste in capitolato e il traffico relativo all'assistenza remota da parte del fornitore. La segmentazione della rete verrà garantita tramite opportune ACL (Access Control List) o configurazioni sui firewall aziendali (ISFW – Internal Segmentation Firewall), stilate per rete IP (anche per singolo host dove possibile) e per porta, sulla base delle sole effettive necessità di traffico per svolgere le funzioni richieste in capitolato. Il fornitore dovrà garantire piena collaborazione nella redazione di tali ACL e/o regole sul firewall di segmentazione. In ogni caso il traffico sarà consentito solo dalla periferia al centro e non da periferia a periferia, in particolare la rete IP/VLAN assegnata non avrà in alcun caso visibilità sulle reti delle PDL aziendali a meno di specifica necessità.
Al fine di garantire un accesso sicuro alla LAN aziendale, dovrà essere possibile gestire per i dispositivi oggetto di fornitura un metodo di autenticazione di rete conforme con i sistemi di gestione di accesso alla rete aziendali. Il livello minimo richiesto è la MAC-authentication.
Per le eventuali attività di assistenza remota, effettuate nel corso della durata del contratto dal personale tecnico dell'aggiudicatario, la connettività agli host oggetto di assistenza sarà garantita esclusivamente per mezzo dei sistemi VPN aziendali a cui sarà dato accesso solo a seguito di richiesta scritta. La connessione VPN è opportuno che sia di tipo client-to-site ed effettuata per mezzo di credenziali personali. Nel presente scenario, a valle dell'instaurazione della connessione VPN, il collegamento ai singoli host oggetto di assistenza potrà avvenire con gli strumenti scelti dall'aggiudicatario, sempre e comunque con modalità rispondenti al quadro legislativo e normativo vigente.
Per il telemonitoraggio degli host integrati nella rete aziendale verranno effettuate specifiche eccezioni sui sistemi di sicurezza perimetrali e comunque mantenendo il minimo livello di visibilità. L'aggiudicatario dovrà fornire la massima collaborazione per la definizione delle suddette eccezioni.
Nel presente scenario, l'aggiudicatario sarà responsabile in toto delle prescrizioni di ambito sicurezza informatica e privacy, secondo quanto previsto dal quadro legislativo e normativo vigente. In particolare, il fornitore sarà responsabile per quanto riguarda le politiche:

- di autenticazione, autorizzazione e accounting (AAA);

- di backup e disaster recovery (definite in collaborazione con l'azienda);
- di aggiornamento di sicurezza di tutti i software installati sugli host oggetto di assistenza;
- di protezione antivirus e altri sistemi per garantire la cyber-resilienza degli host oggetto di fornitura (per la parte antivirus con l'obbligo per il fornitore di mantenerlo aggiornato per tutta la durata contrattuale).

Resta inteso che sarà l'ente sanitario a definire le politiche di audit e verifica dell'ottemperanza di quanto richiesto in capitolato da parte del fornitore, come ad esempio la verifica dell'aggiornamento dell'antivirus messo a disposizione del fornitore stesso.
Per quanto riguarda la componente server eventualmente presente in fornitura dovranno essere previste caratteristiche di alta affidabilità della connettività sia elettrica che di rete, nel caso di server forniti e gestiti in toto dall'aggiudicatario.
Per soluzioni virtualizzate, in coerenza con il Piano Triennale, è preferibile dedicare uno spazio sullo IaaS aziendale ed eventualmente nel sistema di virtualizzazione gestito dall'ente sanitario, nel caso in cui non siano disponibili IaaS di livello adeguato alla tipologia di dati e servizi erogati. Resta inteso che una volta fornito lo IaaS all'aggiudicatario, l'azienda sanitaria è responsabile solo del servizio IaaS e non della gestione di quanto installato su di esso da parte del fornitore. E' auspicabile che l'azienda sanitaria possa dare in gestione porzioni del proprio IaaS direttamente all'aggiudicatario della gara. Come per la parte client, anche per la parte server il fornitore è responsabile di tutte le prescrizioni di sicurezza indicate in precedenza.
Per l'intera durata contrattuale l'operatore economico dovrà gestire il ciclo di vita dei sistemi forniti in modo che siano sempre compatibili con le versioni più aggiornate dei sistemi operativi (sia build client che server), nonché con i web browser, i database e altri software con cui l'applicativo fornito dovesse avere delle dipendenze e/o interagire (es. librerie Java, Adobe Reader, ecc). Il fornitore dovrà quindi rendere disponibile la release compatibile dei software forniti che non dovranno in alcun caso costituire un vincolo per l'azienda sanitaria in relazione all'aggiornamento tecnologico obbligatorio dei sistemi in essere.

Scenario 2: sistemi integrati

Nel secondo scenario si prevede che l'aggiudicatario dovrà integrare i sistemi oggetto di fornitura anche con l'infrastruttura sistemistica dell'azienda sanitaria.
Come nel caso precedente resta in carico al fornitore la gestione del ciclo di vita dei sistemi forniti, fatto salvo quanto gestito effettivamente dall'azienda.
I profili di responsabilità condivisa, in questo caso d'uso in cui la soluzione risulta integrata e comunicante con i sistemi aziendali, secondo quanto previsto dalla ISO IEC 80001, sono definiti nel documento redatto al momento della messa in produzione del sistema (responsibility agreement).
Nel presente scenario, gli eventuali server forniti potranno essere:

- virtualizzati preferibilmente nel sistema IaaS aziendale, eventualmente nel sistema di virtualizzazione aziendale e come per lo scenario 1 saranno gestiti direttamente dall'aggiudicatario;
- fisici ed installati presso il datacenter aziendale oppure in uno indicato dall'ente stesso in completa gestione del fornitore, dove verranno garantiti solo alimentazione elettrica e raffrescamento;

- forniti in SaaS, dove verranno fatte valere le indicazioni definite in precedenza per lo specifico ambito cloud e verranno richiesti i livelli di servizio indicati nella documentazione tecnica.

In ogni caso si dovranno seguire le politiche di gestione, comprese quelle di indirizzamento IP, di aggiornamento, di backup e di disaster recovery definite dall'azienda in collaborazione con il fornitore.
In caso di housing nei datacenter individuati dall'azienda le macchine dovranno essere compatibili almeno con il sistema operativo in uso nei server aziendali e inserite nel dominio aziendale. In caso di hosting (su IaaS qualificato dell'azienda o altra soluzione validata nelle disponibilità dell'azienda sanitaria) verranno garantiti i requisiti tecnologici previsti per il livello di servizio atteso e per la tipologia di dati trattati e in linea con il livello di rischio minimo accettabile da parte dell'azienda. Sarà comunque onere del fornitore, nel caso in cui non sia nelle disponibilità dell'azienda una soluzione qualificata al momento della fornitura, il servizio di migrazione ad infrastruttura qualificata quando disponibile.
Allo scopo di uniformare i sistemi forniti agli standard dell'azienda, i server dovranno essere dotati di sistema operativo validato dall'azienda. Qualora vengano aggiunti nel dominio aziendale i nuovi server verranno inseriti in apposite unità organizzative ed è richiesta la massima collaborazione nella scelta delle regole applicabili a tale unità organizzativa. Restano di completa responsabilità del fornitore, gli aggiornamenti di tutta quanto di propria gestione secondo il documento dei profili di responsabilità.
In caso di hosting, resta in carico all'azienda la scelta dell'infrastruttura di virtualizzazione da utilizzare e le modalità con cui vengono gestite le macchine, in ottemperanza alle indicazioni per i requisiti minimi del fornitore.
Ai server verrà in ogni caso assegnata una opportuna classe di indirizzi IP fissi, in VLAN con visibilità gestita attraverso ACL e/o ISFW redatti con la collaborazione del fornitore.
Sarà esclusivo onere dell'aggiudicatario, nel caso intenda utilizzare motori di database diversi da quelli forniti dall'azienda, comunicare le necessarie politiche di manutenzione e controllo, nonché le politiche di backup e disaster recovery, anche a livello sistemistico, allo scopo di garantire i necessari standard di performance e sicurezza.
In base alle specifiche scelte, progettuali e di infrastruttura, l'aggiudicatario dovrà usufruire della struttura di backup dell'azienda sanitaria per i sistemi operativi di tutti i server e per la configurazione dei database. Dovrà essere fornito all'azienda sanitaria supporto per il loro inserimento nel proprio sistema di backup, nonché per la redazione delle procedure di backup e disaster recovery.
Ogni attività di tipo change lato server, inteso come intervento o aggiornamento sui sistemi oggetto di fornitura, non dovrà in ogni caso causare disservizio per un tempo superiore a quanto ritenuto accettabile dall'azienda sanitaria che considererà anche l'eventuale presenza di soluzioni di business continuity. In ogni caso le attività di change dovranno essere anticipatamente comunicate e concordate con l'azienda sanitaria, nonché documentate e dovrà essere previsto un sistema di rollback.
Nel presente scenario, lato utente, ovvero lato PDL, gli applicativi eventualmente forniti potranno essere basati su tecnologia preferibilmente web (ZFP) oppure client/server. Non saranno considerati compatibili con l'infrastruttura IT sistemi basati sul paradigma client/database.
Gli applicativi client forniti, necessari all'espletamento di una o più funzionalità richieste, verranno resi disponibili sulle PDL (link web o applicativo client), senza limitazioni in termini di numero di postazi-

oni, e dovranno essere adeguati alle caratteristiche software e hardware delle postazioni stesse, in particolare alle policy del dominio aziendale applicate a tutte le PDL.
Gli applicativi web forniti dovranno essere compatibili con almeno due dei browser installati su ciascuna PDL. Nel presente scenario non saranno considerati accettabili eventuali PC forniti, se non identici ad uno dei modelli standard già in produzione presso l'azienda sanitaria, che in tal caso potranno essere inseriti nel dominio aziendale a seguito di clonazione e hardening standard dell'azienda sanitaria, a condizione di seguire le policy e caratteristiche dei PC dell'azienda.
Nel presente scenario, tutte le funzionalità dei sistemi forniti dovranno essere garantite con il sistema di indirizzamento IP dinamico (DHCP) attivo sulle PDL dell'azienda e non verranno in alcun caso create sul servizio DHCP configurazioni di tipo reservation ed exclusion.
Tutte le funzionalità dei sistemi forniti dovranno essere garantite con l'antivirus in uso nelle PDL aziendali, in considerazione del fatto che verranno applicate le politiche di aggiornamento/scansione standard dell'azienda, a meno di eccezioni concordate. Inoltre, saranno attivati sui client anche dei servizi di host intrusion prevention system e di local firewall. In tal senso l'aggiudicatario dovrà garantire piena collaborazione nella redazione di tali eccezioni sul client.
Eventuali host (di tipologia non server) oggetto di fornitura che non siano dotati di client in dominio e che necessitano di connettività con la rete dati aziendale, verranno connessi alla stessa e saranno oggetto di policy di segmentazione e segregazione del traffico. La segmentazione del traffico, analogamente al primo scenario, verrà garantita tramite opportune ACL (Access Control List) o configurazioni sui firewall aziendali (ISFW – Internal Segmentation Firewall), stilate per rete IP (anche singolo host) e per porta, sulla base delle sole effettive necessità di traffico per svolgere le funzioni richieste in capitolato. In ogni caso il traffico sarà consentito solo dalla periferia al centro e non da periferia a periferia, in particolare la rete IP/VLAN assegnata non avrà in alcun caso visibilità di rete sulle reti delle PDL aziendali a meno di specifica necessità.
L'azienda sanitaria si riserva di assegnare una o più reti IP/VLAN all'aggiudicatario in base alla specifica architettura proposta.
Nel presente scenario, in generale, sia lato server che lato client, dovranno essere installate tutte le patch necessarie. Potranno essere segnalate all'azienda patch contrassegnate come "non applicabili", solo se di natura non critica o se incidenti sulla marcatura CE di una delle componenti di fornitura. In tal caso l'aggiudicatario dovrà comunque risolvere nel minor tempo possibile il problema di compatibilità. In ogni caso la veicolazione degli aggiornamenti avverrà tramite il sistema di distribuzione dei software presente in azienda, pertanto resta onere dell'aggiudicatario fornire un pacchetto di distribuzione delle proprie componenti utilizzabile con il sistema aziendale di software distribution. Questo sistema di distribuzione sarà utilizzato per tutta la durata contrattuale.
Al fine di garantire un accesso sicuro alla LAN aziendale, dovrà essere possibile gestire per i dispositivi oggetto di fornitura un sistema di autenticazione di rete conforme con i sistemi di gestione di accesso alla rete aziendali. L'autenticazione si basa, a seconda delle caratteristiche dell'host, su uno dei seguenti criteri (ordinati per livello di sicurezza e quindi per preferenza di implementazione):

- tramite certificato o account macchina per gli host in dominio;
- tramite nome utente e password o di MAC address per tutti gli host non in dominio.

Per le eventuali attività di assistenza remota, effettuate nel corso della durata del contratto dal personale tecnico dell'aggiudicatario, la connettività agli host oggetto di assistenza sarà garantita esclusivamente per mezzo dei sistemi VPN definita dall'azienda sanitaria, alla quale sarà dato accesso solo a seguito di richiesta scritta. La connessione VPN è opportuno sia di tipo client-to-site ed effettuata per mezzo di credenziali. A valle dell'instaurazione della connessione VPN, il collegamento ai singoli host oggetto di assistenza:

- dovrà avvenire esclusivamente con gli strumenti in uso presso l'azienda sanitaria nel caso di host dotati di client in dominio;
- potrà avvenire con gli strumenti scelti dall'aggiudicatario, sempre e comunque con modalità rispondenti al quadro legislativo e normativo vigente, solo a valle di validazione degli strumenti stessi e della loro configurazione da parte dell'azienda sanitaria nel caso di host non dotati di client in dominio.

Per quanto riguarda le eventuali attività di telemonitoraggio continuo degli strumenti e in generale degli host oggetto di fornitura, potranno essere usati strumenti messi a disposizione dall'azienda sanitaria come ad esempio proxy di navigazione autenticata. Nel caso in cui sia effettivamente in uso il proxy gli host forniti dovranno essere tali da consentire la configurazione del proxy Internet, tramite il quale, su specifiche porte di navigazione (80, 443, ecc.), potranno raggiungere specifici IP pubblici.
I dispositivi oggetto di fornitura è opportuno che siano coerenti e integrati con la soluzione di single sign-on (SSO) in essere presso l'azienda sanitaria; che siano utilizzate credenziali del tipo "nome utente" e "password" oppure sistemi basati su certificati aziendali, in base alla soluzione utilizzata dall'azienda. Nel caso di utilizzo di password è consigliabile l'uso di password complesse di almeno 12 caratteri, con password history a 24 e cambio password obbligatorio ogni 90 giorni, così come suggerito dalle più importanti linee guida nazionali e internazionali.
Le modalità operative di accesso agli applicativi ed ai sistemi forniti da parte degli operatori è buona norma che siano basate su credenziali nominali; a queste potranno inoltre essere associati uno o più ruoli.
Tutte le credenziali impersonali, eventualmente presenti negli applicativi e nei sistemi forniti, dovranno essere opportunamente create e configurate nel dominio aziendale senza funzione di logon interattivo; gli account di dominio associati a credenziali impersonali si autenticheranno in maniera automatica (e trasparente agli operatori) a tali applicativi/servizi in base al proprio livello di autorizzazione minimo necessario e a seguito di auto logon (in ogni caso senza l'immissione delle credenziali impersonali da parte degli operatori).
L'autorizzazione (authorization) è intesa in questo contesto come profilatura dell'account e gestione dei ruoli e delle abilitazioni ad esso associati. In particolare, gli applicativi/servizi forniti importeranno gli account da abilitare dal repository del dominio aziendale sulla base di un gruppo di dominio specifico che verrà realizzato ad hoc, e circoscriveranno la profilatura e l'attribuzione dei ruoli all'interno degli applicativi/servizi stessi solo per gli account appartenenti a quello specifico gruppo. In via propedeutica al collaudo dei sistemi forniti, l'aggiudicatario installerà la consolle amministrativa su un client dell'azienda sanitaria e garantirà adeguata formazione relativamente alla profilatura degli account nei sistemi forniti, in modo da rendere l'azienda sanitaria autonoma nelle procedure di abilitazione e successiva reinstallazione della console amministrativa.

È bene che non sia possibile creare, configurare e profilare altri account non appartenenti al dominio dell'azienda, ad eccezione di specifiche situazioni opportunamente motivate ed in ogni caso concordate con l'azienda sanitaria. La profilatura e l'attribuzione dei ruoli degli applicativi/servizi forniti garantirà il massimo livello di dettaglio di configurazione.

SPECIFICHE TECNICHE DI SICUREZZA INFORMATICA

Di seguito vengono riportate le specifiche da richiedere in fase di gara che i sistemi forniti dovranno rispettare, sia nel caso di non collegamento in rete, sia nello Scenario 1 che nello Scenario 2, relativamente ad aspetti generali della sfera dell'IT con particolare riferimento alla sicurezza informatica.
Vale in ogni caso il principio generale per cui la sicurezza informatica è un fattore intrinseco dell'architettura dei sistemi che sono in approvvigionamento e dovranno trovare corrispondenza anche nelle caratteristiche tecniche degli elementi che li compongono; perciò in fase di acquisto si dovrà richiedere all'aggiudicatario di garantire che, sia l'architettura che gli elementi, siano progettati, implementati e mantenuti nel tempo in modo da minimizzare il rischio informatico residuo (sia considerando il sistema come veicolo che oggetto di potenziali attacchi) e comunque in osservanza delle normative e best practice già riportate nel presente documento e sempre in coerenza con il paradigma "Zero Trust".
È fondamentale richiedere che tutti gli elementi al momento della consegna non siano fuori supporto tecnico del fabbricante o a fine ciclo di vita (end-of-life) e comunque non dovranno trovarsi in tale stato ad un anno dal collaudo o nell'arco di durata della manutenzione/servizio oggetto di fornitura.
Inoltre è opportuno richiedere che per le componenti hardware fornite il guasto entro 4 mesi dalla data di collaudo sia prevista la sostituzione per "mortalità infantile".
Di seguito si riporta un elenco generale di caratteristiche a cui dovrebbero rispondere eventuali software presenti nella fornitura:

- coerenti con il paradigma privacy by design e by default, e costruiti per proteggere i dati trattati per impostazione predefinita;
- intuitivi e di facile utilizzo, ad ogni livello di accesso ed in ogni configurazione, per tutti gli operatori (a prescindere dal ruolo);
- dotati di impostazioni internazionali di Microsoft Windows (se presente) IT standard, comprese le tastiere, allo scopo di non incorrere in nessun caso in errori nelle date, nei dati numerici e nei dati personali locali;
- stabili, in particolare che siano in grado di gestire le eccezioni;
- sicuri, sia dal punto di vista della sicurezza informatica che della qualità delle funzioni svolte;
- ottimizzati, in termini di rapporto tra uso delle risorse e prestazioni;
- sviluppati tenendo conto dei principi del ciclo di vita del software e dell'analisi del rischio, secondo le norme tecniche (o principi e metodologie almeno equivalenti) e le best practice internazionali; in ogni caso non dovranno utilizzare librerie deprecate e/o obsolete, né dovranno essere scritti e sviluppati con versioni del linguaggio di programmazione fuori supporto tecnico del fabbricante o a fine ciclo di vita (end-of-life) e comunque non dovranno trovarsi in tale stato ad un anno dal collaudo definitivo dei sistemi;

- pensati, progettati e realizzati nel rispetto del quadro legislativo vigente, nonché in modo da non mettere in alcun caso gli operatori in condizione di violare il quadro legislativo stesso nell'espletamento del normale utilizzo dei sistemi;
- installati e configurati per essere utilizzati, in condizioni di massima sicurezza e funzionalità;
- manutenuti e gestiti in modo da conservare e mantenere stabili nel tempo tutte le caratteristiche possedute al momento del collaudo definitivo.

In particolare, tutti i software in acquisizione che potrebbero essere installati su dispositivi collegati alla LAN dell'ente e inseriti nel dominio, dovrebbero essere configurati per essere eseguiti:

- in un contesto user space per i client;
- come servizio per tutti i server;
- come servizio per i client se non è richiesta interazione con l'operatore;

senza modifiche sui permessi d'azione degli utenti sul file system, oppure alterazione del registro di sistema.

Per quanto concerne gli eventuali "account amministrativi" (ovvero ogni account a cui è associato un ruolo Amministratore o che è dotato di privilegi amministrativi o che consenta di svolgere funzioni di amministratore su qualunque macchina, sistema o applicativo fornito) è opportuno inserire nell'allegato IT queste indicazioni relative all'operatività di questi utenti:

- potranno, nel caso di account amministrativi locali di default (a titolo di esempio non esaustivo: "admin", "administrator", "root", ecc.), essere impersonali e dovranno essere tutti comunicati all'azienda sanitaria, che potrà modificarne le password e che li conserverà secondo le proprie procedure standard di sicurezza;
- dovranno, nel caso di account amministrativi non locali che consentano l'accesso interattivo a macchine/sistemi/applicativi collegati alla LAN aziendale, essere sempre personali e sottostare al sistema di autenticazione presente nell'ente;
- potranno, nel caso di account digitali amministrativi, essere configurati dall'aggiudicatario solo in accordo con l'azienda sanitaria e dovranno essere nominali e nelle disponibilità dell'ente;
- dovranno, nel caso di tutti gli account di sistemi non in LAN, essere gestiti a cura e responsabilità dell'aggiudicatario;
- potranno, nel caso di account amministrativi di macchine/sistemi/applicativi non collegati alla LAN aziendale, essere impersonali e dovranno essere tutti comunicati all'azienda, che potrà modificarne le password e che li conserverà secondo le proprie procedure standard di sicurezza;
- gli account amministrativi impersonali di sistemi non collegati alla LAN dovranno essere configurati in modo tale da:
  - non consentire modifiche di configurazioni, impostazioni e settaggi di macchine/sistemi/applicativi;
  - non consentire un trattamento dati eccedente al minimo rispetto alla tipologia di account utilizzato.

Considerando eventuali attività manutentive o necessità che comportino l'uso di periferiche di storage è utile indicare nel documento che:

- sono considerati e ammessi solo come archivi provvisori/di transito;
- i dati personali dei pazienti vi devono risiedere il minor tempo possibile e comunque non superare le 24 ore, implementando procedure di cancellazione automatica che garantiscano il non recupero dei dati eliminati.

In linea generale nell'allegato IT è opportuno ricondurre la gestione degli storage, anche provvisori, solo a utenti nominali, in modo da referenziare ogni azione condotta sui dati, fornendo opportuni permessi agli utenti (il minimo privilegio necessario) e accedendo ai dati attraverso l'applicativo e non direttamente all'eventuale file system.
Va inserito anche che non è possibile archiviare dati temporaneamente, anche in forma anonima, su dispositivi situati al di fuori del perimetro dell'azienda sanitaria, salvo diversi accordi con l'ente per attività descritte, contrattualizzate e validate dall'ente.

Applicazioni pratiche di soluzioni di integrazione di dispositivi medici in congruenza ai requisiti NIS 2

Sulla base delle considerazioni fatte finora, verranno presentate di seguito due applicazioni pratiche dell'utilizzo della normativa di settore per l'implementazione sicura di soluzioni software o hardware, categorizzate come dispositivo medico, in un contesto ospedaliero. Successivamente si svilupperanno delle considerazioni generali legate all'implementazione di soluzioni marcate dispositivo medico in reti aziendali, e di come le azioni indicate nei due casi d'uso vadano a rispondere ad alcuni requisiti previsti per i soggetti essenziali, come nel caso di un'azienda sanitaria.
Le due situazioni faranno riferimento all'analisi e implementazione di una centrale di monitoraggio e di una verticale di reparto classificata come dispositivo medico.
L'analisi propone un approccio orientato alla mitigazione del rischio, sotto vari aspetti:

- rischio clinico;
- rischio cybersecurity;
- rischio legato al corretto trattamento dei dati;
- rischio infrastrutturale;
- ...

Di seguito verranno presentati per i due casi d'uso affrontati implementando diversi approcci, basati sull'utilizzo di normativa, linee guida, best practice e standard di settore con un occhio di riguardo alle integrazioni, associati all'uso di soluzioni tecnologiche per la cybersecurity.

CASO D'USO NUMERO 1: CENTRALE DI MONITORAGGIO PER TERAPIA INTENSIVA

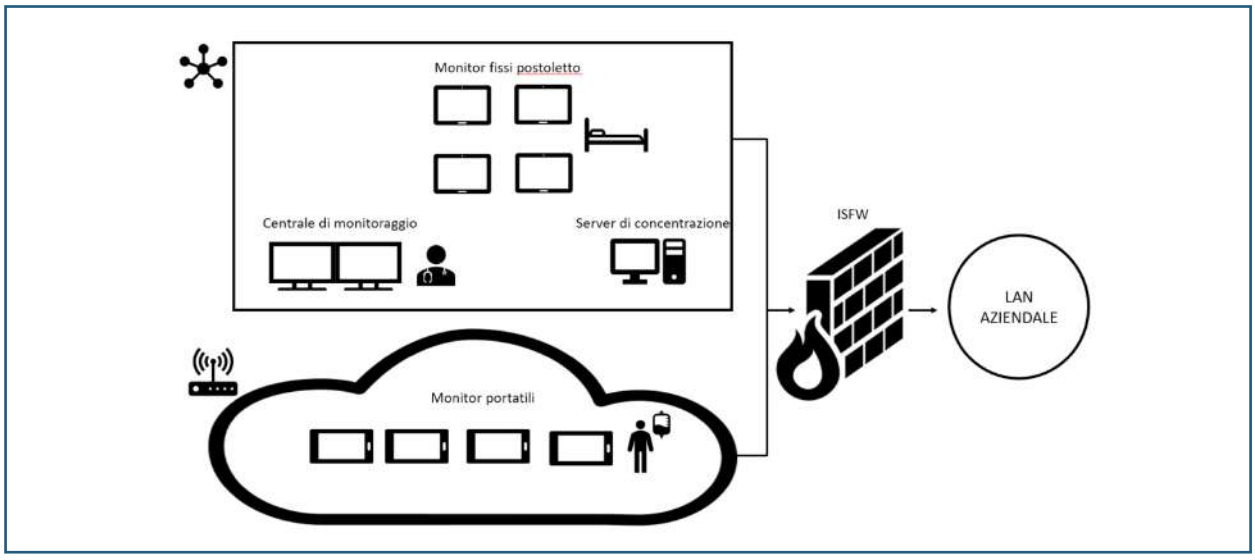
Il primo caso d'uso prende in considerazione la progettazione e messa in opera di una centrale di monitoraggio, quindi una soluzione particolarmente normata da un punto di vista di certificazione lato dispositivo medico e di conseguenza una soluzione in cui il personale aziendale deve operare scelte strategiche a livello architetturale e di policy organizzative/implementative.
Una tipica centrale di monitoraggio è costituita essenzialmente da due aree, una di core e una di edge:

- EDGE: il monitoraggio posto letto, direttamente a contatto con il paziente. Può essere modulare, e quindi potenzialmente composto di un monitor principale, spesso ancorato ad uno dei pensili o al testa-letto del paziente, e una parte più piccola, trasportabile che consente il monitoraggio del paziente all'interno della struttura in caso si dovessero rendere necessarie attività ulteriori, ad

esempio l'esecuzione di esami diagnostici di radiologia oppure interventi specifici all'interno del blocco operatorio;
- CORE: la centrale e il server che di fatto rappresentano il punto di concentrazione dei segnali ricevuti dai monitor e presentano i dati al personale sanitario coinvolto nel processo di cura.

Schema infrastrutturale

Così come presentata la soluzione necessita di una architettura progettata a garantire la sicurezza delle comunicazioni ma anche la sicurezza dell'ecosistema IT che di fatto abbraccia la centrale di monitoraggio. L'approccio nella soluzione architetturale che verrà presentata di fatto ha come intento sia la protezione della rete del monitoraggio da eventuali pericoli esterni che della rete aziendale da eventuali minacce legate ad una implementazione non sicura della soluzione.
Così come strutturata per garantire una corretta gestione dell'infrastruttura del monitoraggio è opportuno suddividere la connettività in due sottoreti, una che gestirà le comunicazioni tra i monitor principali (in questo caso collegati con cavo) e la centrale di monitoraggio/server di concentrazione, e l'altra che gestirà i moduli portatili (su infrastruttura wireless con visibilità sulla centrale/server) che consentirà al personale sanitario di seguire lo stato di salute del paziente anche fuori dal reparto. Questo in ottemperanza a quanto indicato nella ISO 27799 (famiglia delle norme 27000) che suggerisce la segmentazione in VLAN dedicate per la protezione delle PHI, isolando di fatto i dispositivi "sensibili" al fine di garantire confidenzialità, integrità e disponibilità dei dati sanitari.



Server, centrale e monitor principali

La rete che fornisce connettività a questa parte della infrastruttura è cablata.
Il server centrale è, ubicato all'interno del datacenter aziendale, con doppio collegamento agli apparati attivi, possibilmente in fibra su una infrastruttura dimensionata per garantire i requisiti minimi di performance definita dal produttore che ha certificato la soluzione. Le due linee di collegamento

dovranno essere attestate su due apparati di rete differenti aggregati. Questo per garantire continuità operativa in caso di primo guasto di uno dei due apparati, oppure per interruzioni accidentali di uno dei due collegamenti, o di guasto di una delle schede di rete del server.
Il server dovrà essere dotato di doppia alimentazione con fornitura differenziata, in modo da garantire la continuità di servizio in caso di guasto alla rete elettrica. Nel caso il server non fosse provvisto della seconda alimentazione si suggerisce l'utilizzo di un ATS, strumento utilizzato per fornire una doppia tipologia di alimentazione per quei dispositivi provvisti di un unico collegamento alla rete elettrica.
I monitor principali, saranno collegati alla rete attraverso dei punti isolati galvanicamente, per ridurre il rischio di correnti di dispersione verso il paziente derivanti dal collegamento di rete del dispositivo.
Gli switch di attestazione, come quelli per la parte server, dovranno essere provvisti di doppia alimentazione e collegati al nodo gerarchicamente successivo tramite un collegamento in alta affidabilità.
Occorre porre particolare attenzione per la parte di attestazione dei monitor e della centrale in quanto anche i tempi di avvio degli apparati di rete direttamente collegati ad essi potrebbero presentare risvolti negativi durante le manutenzioni. Pertanto è consigliabile scegliere apparati che garantiscono ridotti tempi di avvio.
Tutti e tre gli elementi saranno ubicati logicamente all'interno della VLAN del monitoraggio, opportunamente terminata sul firewall e collegata a strumenti di monitoraggio passivo come SIEM o sistemi di analisi del traffico tramite sonde inserite in rete.

Moduli Portatili

Per la parte di moduli portatili la soluzione più indicata è quella di utilizzare l'infrastruttura di rete wifi, in questo caso d'uso gestita dall'IT aziendale, distribuita all'interno dell'azienda con SSID nascosto e configurato sui monitor portatili al momento del collaudo e relativi test.
La WLAN dedicata ai monitor portatili dev'essere anch'essa terminata su firewall, sempre richiamando le indicazioni della ISO 27799, e distribuita sugli access point dedicati dai sistemi controller della parte wireless.

SICUREZZA APPLICATIVA

Server di concentrazione

In questo caso, sulla base di quanto detto in precedenza, lo scopo è quello di garantire il più elevato livello di sicurezza possibile, garantendo un corretto trattamento dei dati.
Il server dovrà essere accessibile soltanto a personale autorizzato e che sia provvisto di credenziali nominali, in modo da tracciare la responsabilità almeno per quanto riguarda gli accessi, se in aggiunta si è provvisti di un sistema di gestione dei log, il server, con l'accordo del produttore/fornitore, sarà configurato per inviare i log citati al sistema di gestione aziendale. È preferibile poi configurare la porta di management del server stesso, su VLAN dedicata, per gestire la macchina in caso di malfunzionamenti che impediscano l'accesso al sistema operativo. Se possibile va implementata una politica di backup il più aderente possibile al paradigma 3-2-1-1-0,,di conseguenza: 3 copie del dato/sistema (esclusa quella di produzione), su due supporti tecnologici diversi, di cui uno in un altro presidio e uno in modalità offline (ad esempio storage immutabile) con una verifica di assenza di errori. Questa

implementazione per ridurre al minimo il rischio di perdita dei dati di produzione a causa di guasti o altri pericoli. Le aperture sul firewall dovranno essere solamente quelle previste per le normali funzionalità (ricezione dei parametri dai dispositivi di monitoraggio e eventuale invio dei dati alla verticale di reparto specifica) e le eventuali attività manutentive. Considerando la delicatezza della soluzione tecnologica è auspicabile attivare profili/policy di sicurezza commisurate al valore dei dati che vi transitano, ad esempio attivando IPS, SSL inspection e log delle sessioni.
L'accesso per la manutenzione da remoto va gestito con collegamenti VPN dedicati ed accessi limitati al solo personale autorizzato, possibilmente interponendo un livello di controllo ulteriore una volta stabilita la connessione in VPN, ad esempio assegnando staticamente gli indirizzi per le VPN dei tecnici che eseguono la manutenzione per operare l'opportuno filtraggio degli accessi alle reti del monitoraggio.

Centrale di monitoraggio

Per la centrale di monitoraggio vanno definite, come per il server, autenticazioni basate sui ruoli con credenziali nominali. Le credenziali di service della centrale devono rimanere ad appannaggio del manutentore e del solo personale autorizzato e competente, riducendone l'uso in favore di credenziali nominali con profilo amministrativo dove possibile.
Dev'essere implementata una policy di autenticazione alla rete, gestita tramite un NAC, poiché la centrale, come gli altri oggetti diversi dal server che compongono il sistema, accederà alla rete per il tramite di switch di accesso. In considerazione di quanto dichiarato dal fornitore va implementato il sistema di autenticazione per gli asset dispositivo medico di livello più alto possibile. Anche per questi dispositivi, in considerazione della delicatezza della soluzione tecnologica è auspicabile attivare profili di sicurezza aderenti al valore dei dati che vi transitano, ad esempio attivando IPS, SSL inspection e log delle sessioni.

Monitor fissi posto letto

Per i monitor, deve essere interdetto l'accesso al pannello di configurazione e vanno modificati in fase di collaudo i codici di accesso all'area di service del monitor in accordo con l'installatore e dovranno essere comunicati al personale addetto alla manutenzione. Come per la centrale l'accesso alla rete aziendale dovrà essere intermediato da un sistema NAC, anche in questo caso implementando il più alto livello possibile di autenticazione. Considerando la delicatezza della soluzione tecnologica è auspicabile anche in questo caso attivare profili di sicurezza aderenti al valore dei dati che vi transitano, ad esempio attivando IPS, SSL inspection e log delle sessioni.

Monitor portatili

Come per i monitor fissi, solamente che il sistema di autenticazione dovrà essere reso disponibile ai sistemi di gestione dell'infrastruttura wifi, opportunamente configurati in modo da veicolare la WLAN dedicata una volta avvenuta l'autenticazione, ad esempio sfruttando attribuiti specifici durante l'autenticazione. È consigliato nei ISFW attivare profili di sicurezza aderenti al valore dei dati che vi transitano, ad esempio attivando IPS, SSL inspection e log delle sessioni.

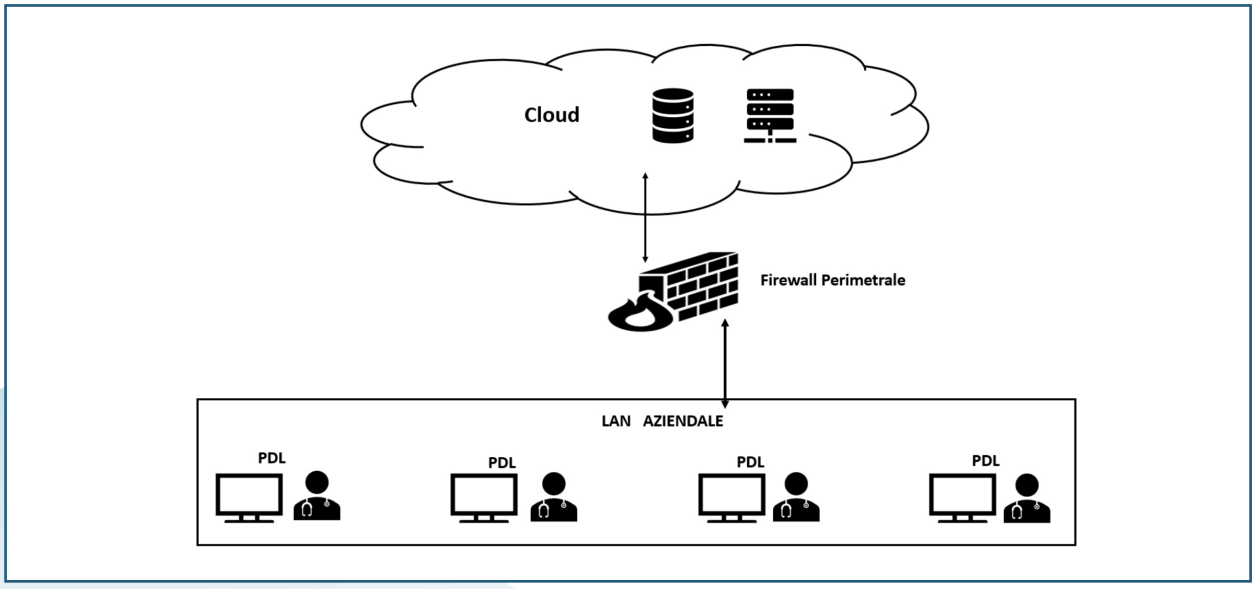
Nel caso in cui la soluzione di monitoraggio, debba interfacciarsi con applicativi in uso e distribuiti nella LAN aziendale è opportuno che ciò avvenga seguendo le specifiche definite nei technical framework dei profili IHE PCD (patient care device). Nei profili vengono identificati attori e transazioni che comunicano in formato standard le informazioni sul paziente o altri eventi, come ad esempio definito nei profili ACM (alert communication management) e DEC (device enterprise communication). Per agevolare il lavoro dei clinici e ridurre quindi gli errori legati ad inserimenti manuali di dati paziente, dovranno essere considerate e attivate integrazioni della soluzione stand alone con il sistema ADT, in modo da popolare in automatico i dati paziente sulla centrale di monitoraggio, associando il nuovo paziente ad una etichetta indicante univocamente il posto letto e di conseguenza il monitor a cui verrà collegato. Altra integrazione auspicabile è l'invio dei dati del monitoraggio, in formato standard HL7, verso la verticale di reparto, in modo da fruire dei dati in real time anche nell'applicativo di reparto.

CASO D'USO NUMERO 2: VERTICALE DI REPARTO DI GASTROENTEROLOGIA IN SAAS

Nel secondo caso, la situazione affrontata è diversa. Se nel primo caso ci si muoveva in un contesto più chiuso, molto legato a quanto definito dal produttore a livello di scelte, sia software che hardware, in questo secondo caso d'uso vi è una profonda commistione nella gestione della soluzione tecnologica scelta.

Schema Infrastrutturale

Negli ultimi anni, anche in considerazione delle indicazioni contenute nelle varie edizioni del Piano Triennale per l'informatica nella PA (prima significativa edizione in questo senso quella del triennio 2019-2021) per le soluzioni applicative (ove non rientranti tra le eccezioni contenute nella delibera AgID n.2 del 2018) si applica il paradigma del Cloud First.



Nel caso specifico, definito dalla realizzazione di una verticale di reparto per la gastroenterologia che si basa su un servizio in cloud, concorrono molteplici aspetti per definire il perimetro di realizzazione della soluzione tecnologica.
Nel caso in esame, fornitura di una verticale di reparto per mezzo di servizio SaaS, e quindi una soluzione applicativa in un cloud al quale devono accedere le PDL, vanno verificate le seguenti caratteristiche:

- qualificazione del prodotto SaaS sulla base del regolamento Cloud emanato da ACN nel luglio 2024;
- tipologia di servizio scelto per la definizione delle modalità di collegamento più appropriate, sia in rapporto alle SLA desiderate che alla resilienza del sistema;
- tipologia dei dati trattati secondo la classificazione dei dati e servizi stabilita da AgID e di prossima revisione da parte di ACN.

Servizio in cloud

Nel caso d'uso proposto, i desiderata a livello di performance, e quindi riconducibili a SLA ben determinate (ad esempio RPO e RTO, politiche di backup, piani di BC e DR), la soluzione suggerita prevede l'acquisto di un servizio che sia qualificato per trattare dati di livello critico.
L'infrastruttura cloud dovrà essere tra quelle qualificate\adeguate di livello pertinente alla tipologia di dati e servizi che vengono trattati su tale infrastruttura secondo quanto indicato nel nuovo Regolamento Cloud di ACN, "Regolamento per le infrastrutture digitali e per i servizi cloud per la pubblica amministrazione".
Spesso capita che i fornitori in sede di gara indichino il livello di qualificazione AI2. Questa determina la qualificazione della sola infrastruttura su cui poggia la soluzione e non la soluzione applicativa stessa. Pertanto nell'eventualità si dovesse presentare un fornitore che dichiara questa tipologia di qualificazione per un servizio in Saas, tale qualifica non è pertinente alla tipologia di servizio offerto.
Una volta appurata la corretta qualificazione e validità del servizio sul portale di ACN, la scelta si sposta sulla tipologia di collegamento per raggiungere il servizio in cloud.
Abbiamo diverse tipologie di connessione, che garantiscono performance diverse e quindi vanno scelte in base alle specifiche necessità della soluzione (ad esempio VPN site to site, connessioni dirette, gateway Internet).
Ad esempio in una verticale di reparto che tra le evidenze prodotte conta immagini, video, registrazioni di sonde specifiche, le performance giocano un ruolo importante per rendere il sistema fluido e fruibile efficacemente. Pertanto in considerazione di ciò la soluzione più pertinente è una connessione diretta, oppure, nel caso di linee presenti già performanti si può optare per la versione in collegamento VPN.
La tipologia di connessione dev'essere comunque in grado di sopportare una condizione di guasto della linea, affrontabile in due modalità:

- doppia linea per il collegamento al servizio in cloud;
- server fornito come edge computing nel datacenter aziendale ma visto e gestito come un elemento del servizio in Saas.

In relazione alla politica di backup, è opportuno richiedere una soluzione che sia riferita al paradigma 3-2-1-1-0 e conforme alle esigenze di recupero dei dati.
Per la quantificazione di RPO e RTO, si deve considerare la tipologia del servizio e la variabilità delle informazioni che insistono sulla verticale di reparto, per definire i valori opportuni.

Soluzione sulle PDL aziendali

Le postazioni di lavoro, ad eccezione dei sistemi di produzione di immagini, ad esempio le colonne, sono completamente gestite dall'IT aziendale e pertanto soggette alle regole definite a livello di dominio, e di altri strumenti come EDR/XDR, inclusi sistemi di VA.
In aggiunta dovranno essere eseguite le opportune valutazioni e test per garantire la coesistenza degli applicativi, compresi EDR/XDR e le eventuali funzioni/moduli che si dovessero rendere necessari come componenti installate localmente. Pertanto le PDL, in un contesto di questo tipo potranno seguire il profilo di hardening distribuito anche sugli altri pc aziendali.
A livello di fruizione del sistema, essendo un servizio in Saas è opportuno che l'applicativo sia di tipo web, ZFP e accessibile a tutti i browser di navigazione validati in azienda, mantenuti e aggiornati con soluzioni di software distribution.
Per gli eventuali moduli aggiuntivi che si rendessero necessari al completo funzionamento della nuova verticale, ad esempio moduli di integrazione con i dispositivi medici collegati al sistema, è opportuno che sia presente un certificato di validazione del software da parte di un ente terzo e una indicazione da parte del produttore dell'aderenza alle linee guida per lo sviluppo sicuro del software di AgID.

Sicurezza Applicativa

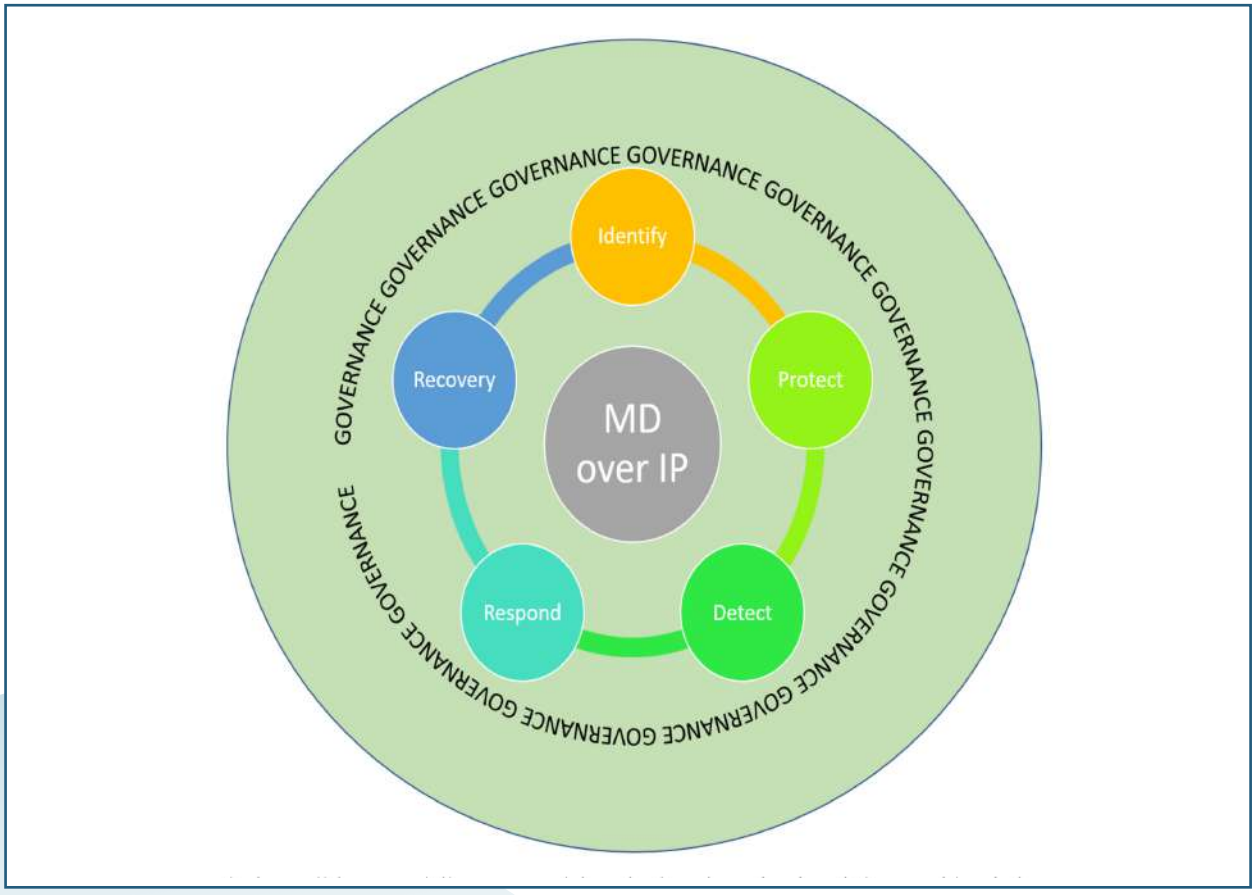
La soluzione fornita, in totale gestione a carico del fornitore, anche per la eventuale componente di edge computing, non verrà inserita nel dominio dell'azienda.
Di conseguenza sarà necessario provvedere ad implementare una tipologia di autenticazione federata, che abbia come IDP il dominio dell'azienda ad esempio basata su Open Id Connect e OAuth 2.0. Dovrà essere utilizzato un portale in https, con gestione del certificato a carico del fornitore del servizio SaaS, per garantire la sicurezza delle comunicazioni tra la parte edge (PDL) e la parte in cloud della verticale.
In generale tutte le tipologie di connessione dovranno poggiare su canali cifrati in relazione alla tipologia di dati e informazioni veicolate.
Gli aggiornamenti della verticale, anche quelli di sicurezza, sono a completo carico del fornitore del servizio, invece quelli delle PDL resteranno in carico all'azienda sanitaria.
Le transazioni attive, da e verso il sistema in cloud, dovranno rispettare standard e regole definite nei profili IHE di pertinenza, come la chiamata per il recupero delle immagini eventualmente salvate nel PACS/VNA aziendale (utilizzando il WADO su https per l'accesso alle immagini)consultabili con viewer dedicato, piuttosto che la generazione del referto secondo le linee guida definite da HL7 Italia nel formato CDA2 e conforme al flusso definito per l'alimentazione del FSE 2.0.
È fondamentale per la buona riuscita del progetto, attivare da subito alcune serie di integrazioni per la gestione informatizzata del paziente con il nuovo software. Si rende opportuno quindi attivare le integrazioni con l'anagrafica aziendale, con il sistema ADT, con il sistema CUP e con l'order entry

usato in azienda. Risulta decisiva anche l'integrazione per l'alimentazione del registry e del repository aziendale con le specifiche indicate in precedenza in aderenza al profilo IHE XDS.b per la parte documentale e XDS-I.b per la parte relativa all'imaging. Si potranno poi prevedere integrazioni con la piattaforma regionale per lo screening e con altre verticali di reparto che contribuiscono al completamento delle prestazioni erogate in gastroenterologia.
La gestione delle eventuali componenti aggiuntive necessarie dovrà essere conforme alle modalità di installazione del software dell'azienda sanitaria, ad esempio tramite l'utilizzo di un sistema di software distribution.
Il firewall dovrà essere opportunamente configurato per garantire solo le transazioni dichiarate e ammesse da e per la soluzione cloud. La visibilità tra le componenti della verticale e i dispositivi medici che alimenteranno la stessa sarà garantita attraverso opportune regole nei ISFW per ridurre al minimo la possibilità di aperture sfruttabili da eventuali minacce, preservando di fatto la riservatezza, integrità e disponibilità delle PHI.
Periodicamente sulle PDL dovranno essere eseguite attività di VA e PT, per validare la resilienza delle postazioni. Medesime valutazioni vanno eseguite per la componente web, preferibilmente in ambiente di test, per valutare la postura in sicurezza della soluzione fornita.

Considerazioni finali

Come anticipato all'inizio del paragrafo, i casi d'uso sopra descritti e le politiche adottate, sono volte a una riduzione del rischio, che rappresenta di fatto il cardine su cui si basa la NIS 2.
L'assunzione di responsabilità del livello di rischio accettabile è influenzata da diversi fattori, non per ultimo ad esempio il fattore organizzativo. Molto spesso le scelte e le politiche adottate per la gestione di sistemi eterogenei non collimano con le effettive azioni che possono essere intraprese.
Di fatto molto spesso ci si trova in situazioni in cui è di rilevante importanza, sia per la sicurezza che per la riuscita della messa in funzione di una nuova tecnologia, la politica di integrazione e gestione adottata.
È necessario trovare un bilanciamento tra quanto è attuabile come azienda, e di questo definire in anticipo le attività che sono sostenibili, e di quanto è necessario responsabilizzare il fornitore in fase di acquisto e implementazione della nuova soluzione tecnologica.
Il tutto ha come traguardo il raggiungimento di un determinato livello di controllo e di rischio che sia sostenibile, coerente con il valore dei dati trattati e dei servizi che vengono erogati.
Pertanto risulta di fondamentale importanza un approccio orientato alla identificazione di profili di responsabilità, dove è chiaro chi è competente per ciascuna parte del sistema, come definito nella ISO IEC 80001 (responsibility agreement).
Nei casi d'uso si evidenziano diverse tipologie di approccio differenziate sulla base della soluzione tecnologica implementata, ma gli obiettivi di sicurezza restano invariati, come quelli di mantenimento dell'ambiente di lavoro conforme al rispetto della certificazione dei dispositivi medici che vi insistono.
Ad esempio è di fondamentale importanza definire un sistema che consenta una valutazione del rischio cibernetico basato sull'analisi degli asset collegati alla rete e la loro inventariazione (anche degli apparati di rete e dei servizi collegati come la componente in cloud), sia monitorando il traffico

che le attività svolte direttamente sulla apparecchiatura stessa, come nel caso delle PDL(VA e PT).
Questi strumenti, anche di diversa estrazione, dovrebbero essere integrati in una piattaforma di gestione del rischio, che consenta valutazione, monitoraggio e gestione delle vulnerabilità insite nei sistemi collegati alla rete e che faccia correlazione di queste informazioni con anche tutti gli altri strumenti che generano contenuto informativo sul comportamento dei dispositivi collegati. Il tutto per evidenziare criticità oppure vulnerabilità al fine di adottare un piano di remediation (delle PDL o della componente core del sistema) o di mitigazione (apparecchiature e software marcati dispositivo medico), che sia sostenibile e attuabile dall'azienda. L'integrazione di queste informazioni dovrebbe rappresentare un dataset importante per la produzione delle segnalazioni relative agli incidenti, inserite in un percorso di gestione degli incidenti cyber così come definito nella NIS 2.
È utile già in fase di acquisizione una definizione chiara delle politiche di backup e disaster recovery e che queste vengano condivise tra tutti gli attori coinvolti (fornitore, IT, ingegneria clinica, clinici) in modo che risultino chiari il percorso e i tempi per il ripristino dei sistemi.
In relazione all'impatto della NIS 2 e dei suoi adempimenti nei casi d'uso evidenziati vediamo di seguito come le scelte/azioni indicate in precedenza ci consentono di rispondere già ad alcuni requisiti previsti per i soggetti essenziali.



Ad esempio tra le misure identificate per i soggetti essenziali, nella funzione di governance, sono ricompresi i seguenti obiettivi:

- definizione di ruoli e responsabilità;
- continuità operativa e ripristino in caso di disastro;
- gestione vulnerabilità;
- sviluppo, configurazione, manutenzione e dismissione dei sistemi informativi e di rete;
- protezione delle reti e delle comunicazioni;
- monitoraggio degli eventi di sicurezza;
- coinvolgimento dell'organizzazione per la sicurezza informatica nella definizione ed esecuzione dei processi di approvvigionamento a partire dalla fase di identificazione e progettazione della fornitura;
- sicurezza dei dati.

Tra le misure appartenenti alla funzione identify nei casi d'uso possiamo riscontrare la gestione delle vulnerabilità.

Nella sezione relativa alla funzione protect possiamo evidenziare l'attuazione nei casi d'uso delle seguenti attività:

- commisurazione delle modalità di autenticazione legate al rischio;
- gestione delle credenziali amministrative con policy dedicate;
- assegnazioni dei permessi sulla base del ruolo, nel rispetto del minimo privilegio necessario a svolgere le operazioni di competenza e pertinenza.

Relativamente alla funzione di detect possiamo evidenziare:

- presenza e gestione di strumenti per l'identificazione di incidenti significativi;
- l'utilizzo di strumenti di analisi e filtraggio sul traffico di rete;
- rilevamento di codice malevolo sulle PDL.

Le funzioni di response e recovery sono riscontrabili nelle seguenti azioni sopra descritte:

- procedure per il ripristino dei sistemi informatici e di rete condivise con gli attori coinvolti;
- segnalazione degli incidenti.

Allegato A - Confronto tra GDPR e NIS2

Articolo GDPR	Contenuto	Articolo NIS2	Contenuto
Art. 1 – Oggetto e finalità.	Tutelare i diritti e le libertà fondamentali delle persone fisiche con riguardo al trattamento dei dati personali e di agevolare la libera circolazione di tali dati.	Art. 1 – Oggetto.	Assicurare un livello comune elevato di cybersicurezza nazionale (e quindi comunitaria).
Art. 1, 2, 4.	Applicabilità solo se vi siano trattamenti di dati personali che riguardano persona fisica.	Art. 2.	Reti e sistemi informativi indipendentemente che siano trattati dati personali.
Art. 2 e 3 – Ambito di applicazione.	Soggetti tenuti: tutti i titolari di qualunque settore. Applicazione materiale e territoriale.	Art. 3 – Ambito di applicazione e All. I, II, III, IV.	Soggetti tenuti: soggetti essenziali e importanti (attività in settori critici e strategici). Applicazione a vari soggetti (ampliamento rispetto alla nis) ma resta ferma la disciplina in materia di protezione dei dati personali di cui al regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, e al decreto legislativo 30 giugno 2003, n. 196, nonché in materia di lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile di cui al decreto legislativo 4 marzo 2014, n. 39.
Art. 4, 12 – Definizione violazione.	12) «violazione dei dati personali»: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati; (C85).	Art. 2 – c. 1 lett.	t) «Incidente»: un evento che compromette la disponibilità, l'autenticità, l'integrità o la riservatezza di dati conservati, trasmessi o elaborati o dei servizi offerti dai sistemi informativi e di rete o accessibili attraverso di essi; u) «quasi-incidente»: cd. near-miss, un evento che avrebbe potuto configurare un incidente senza che quest'ultimo si sia tuttavia verificato, ivi incluso il caso in cui l'incidente sia stato efficacemente evitato; v) «incidente di sicurezza informatica su vasta scala»: un incidente che causa un livello di perturbazione superiore alla capacità di uno Stato membro di rispondervi o che ha un impatto significativo su almeno due Stati membri; z) «gestione degli incidenti»: le azioni e le procedure volte a prevenire, rilevare, analizzare e contenere un incidente o a rispondervi e recuperare da esso.

Articolo GDPR	Contenuto	Articolo NIS2	Contenuto
Art. 5 – Principi applicabili al trattamento di dati personali. Art.6 – Liceità del trattamento. Art. 9 – Trattamento di categorie particolari di dati personali.	Circolazione dei dati personali come oggetto della normativa e principi come fondamento dei trattamenti di dati personali.	Art. 8 – Protezione dei dati personali.	Trattamento dei dati personali come conseguenza dell'applicazione della normativa (necessità di rispettare i principi della data protection). "Protezione dei dati personali 1. L'Agenzia per la cybersicurezza nazionale, le Autorità di settore NIS e i soggetti di cui all'articolo 3 trattano i dati personali nella misura necessaria ai fini del presente decreto e conformemente al decreto legislativo 30 giugno 2003, n. 196 e al regolamento (UE) 2016/679. 2. Il trattamento dei dati personali ai sensi del presente decreto da parte dei fornitori di reti pubbliche di comunicazione elettronica o dei fornitori di servizi di comunicazione elettronica accessibili al pubblico viene effettuato in conformità della legislazione dell'Unione europea in materia di protezione dei dati e della legislazione dell'Unione europea in materia di tutela della vita privata, ai sensi della direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002".
Art. 4, 7 e 9 e Art. 28.	Titolari e responsabili.	Art. 23 e Art. 24.	Organi amministrativi e direttivi (soggetti obbligati); fornitori (destinatari di norme).
Art. 28 – Responsabili.	Il Titolare ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato.	Art. 21.	Le misure di sicurezza ricomprendono anche la sicurezza della catena di approvvigionamento, ivi compresi gli aspetti relativi alla sicurezza riguardanti i rapporti tra ciascun soggetto e i suoi diretti fornitori o fornitori di servizi.
Art. 29 – Istruzione.	Chiunque agisca sotto la responsabilità del Titolare e abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.	Art. 23 – Misure di sicurezza (formazione).	Formazione degli organi di amministrazione e di governo; Offerta periodica di una formazione ai dipendenti (da parte degli organi di amministrazione e degli organi direttivi), per favorire l'acquisizione di conoscenze e competenze sufficienti al fine di individuare i rischi e valutare le pratiche di gestione dei rischi per la sicurezza informatica e il loro impatto sulle attività del soggetto e sui servizi offerti.

Articolo GDPR	Contenuto	Articolo NIS2	Contenuto
Art. 32 – Sicurezza del trattamento.	Obbligo per titolari e responsabili del trattamento di adottare misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio. Approccio multirischio finalizzato alla tutela dei diritti e delle libertà delle persone fisiche. Rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati	Art. 24 – Misure di gestione dei rischi per la sicurezza informatica.	Obbligo per i soggetti essenziali e importanti di adottare misure tecniche, operative e organizzative adeguate e proporzionate alla gestione dei rischi posti alla sicurezza dei sistemi informativi e di rete. Approccio multirischio finalizzato alla sicurezza delle infrastrutture. Le misure assicurano un livello di sicurezza dei sistemi informativi e di rete adeguato ai rischi esistenti, individuazione misure 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; proporzionalità 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.
Art. 33 – Notifica di una violazione dei dati personali all'autorità di controllo.	Adempimenti in capo ai Titolari e ai Responsabili (per quanto di competenza). Segnalazione [su piattaforma dedicata dell'Autorità Garante per la protezione dei dati personali (Autenticazione - Notifica di una violazione dei dati personali (data breach) (gpdp.it)] senza ingiustificato ritardo e, ove possibile, entro 72 ore. Riguarda la violazione dei dati personali che presenti un rischio per i diritti e le libertà delle persone fisiche	Art. 25 – Notifica degli incidenti significativi.	Adempimento in capo ai soggetti essenziali e importanti. Pre notifica entro 24 ore (poi definitiva entro 72 ore). Riguarda incidenti significativi (se ha causato o è in grado di causare una grave perturbazione operativa dei servizi o perdite finanziarie per il soggetto interessato e se ha avuto ripercussioni o è idoneo a provocare ripercussioni su altre persone fisiche o giuridiche causando perdite materiali o immateriali considerevoli).
Art. 34 – Comunicazione di una violazione dei dati personali all'interessato.	Comunicazione all'interessato quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche.		Non prevista la comunicazione all'interessato salvo che questa non sia legata ad adempimenti ulteriori individuati da ACN.
Art. 35 – Valutazione d'impatto sulla protezione dei dati.	Descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento; valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità; valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1; le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.	Art. 37 – Misure di esecuzione e art. 35, comma 3, lett. c).	Facoltà di ACN di richiedere ai soggetti, dichiarandone la finalità, di fornire i dati che dimostrino l'attuazione di politiche di sicurezza informatica. Facoltà di ACN di richiedere l'esecuzione di scansioni di sicurezza basate su criteri di valutazione dei rischi obiettivi, non discriminatori, equi e trasparenti, se necessario in cooperazione con il soggetto interessato.

Articolo GDPR	Contenuto	Articolo NIS2	Contenuto
Art. 50, 55 – Competenza (C122, C123, C128), art. 56.	Fatta salva la competenza, l'Autorità di controllo garantisce la cooperazione con le autorità di altri stati membri e a livello internazionale, per facilitare l'applicazione efficace della legislazione sulla protezione dei dati personali.	Art. 14 – Cooperazione tra Autorità nazionali.	1. Sono assicurate la cooperazione e la collaborazione reciproca dell'Autorità nazionale competente NIS e del Punto di contatto unico NIS con l'organo centrale del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione, di cui all'articolo 7-bis del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155 (Autorità di contrasto), con il Garante per la protezione dei dati personali quale autorità di controllo di cui all'articolo 55 o 56 del regolamento (UE) 2016/679, ... ivi incluso lo scambio periodico di informazioni pertinenti, anche per quanto riguarda gli incidenti e le minacce informatiche rilevanti. 2. Ai fini della cooperazione e della collaborazione di cui al comma 1: a) l'Autorità nazionale competente NIS coopera con il Garante per la protezione dei dati personali, ai sensi dell'articolo 7, comma 5, del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, nei casi di incidenti che comportano violazioni di dati personali, ai sensi del regolamento (UE) 2016/679, senza pregiudicare la competenza e i compiti di controllo di cui al citato regolamento; b) qualora l'Autorità nazionale competente NIS, in sede di vigilanza o di esecuzione, venga a conoscenza del fatto che la violazione degli obblighi di cui all'articolo 24 da parte di un soggetto essenziale o importante possa comportare una violazione dei dati personali, quale definita all'articolo 4, punto 12), del regolamento (UE) 2016/679, che deve essere notificata ai sensi dell'articolo 33 del medesimo regolamento, ne informa senza indebito ritardo il Garante per la protezione dei dati personali ai sensi dell'articolo 55 o 56 di tale regolamento; c) qualora il Garante per la protezione dei dati personali o le autorità di controllo di altri Stati membri di cui all'articolo 55 o 56 del regolamento (UE) 2016/679 impongano una sanzione amministrativa pecuniaria ai sensi dell'articolo 58, paragrafo 2, lettera i), del medesimo regolamento, l'Autorità nazionale competente NIS non procede all'irrogazione delle sanzioni amministrative pecuniarie ai sensi dell'articolo 38 per una violazione di cui alla lettera b) del presente comma, imputabile al medesimo comportamento. L'Autorità nazionale competente NIS può tuttavia esercitare i poteri di esecuzione di cui all'articolo 37.

Articolo GDPR	Contenuto	Articolo NIS2	Contenuto
Art. 57 – Compiti (C122, C129, C132).	1. Fatti salvi gli altri compiti indicati nel presente regolamento, sul proprio territorio ogni autorità di controllo: ... h) svolge indagini sull'applicazione del presente regolamento, anche sulla base di informazioni ricevute da un'altra autorità di controllo o da un'altra autorità pubblica; i) sorveglia gli sviluppi che presentano un interesse, se e in quanto incidenti sulla protezione dei dati personali, in particolare l'evoluzione delle tecnologie dell'informazione e della comunicazione e le prassi commerciali.		
Art. 58 – Poteri (C122, C129).	1. Ogni autorità di controllo ha tutti i poteri di indagine seguenti: ... b) condurre indagini sotto forma di attività di revisione sulla protezione dei dati; ... d) notificare al titolare del trattamento o al responsabile del trattamento le presunte violazioni del presente regolamento; ... 2. Ogni autorità di controllo ha tutti i poteri correttivi seguenti: a) rivolgere avvertimenti al titolare del trattamento o al responsabile del trattamento sul fatto che i trattamenti previsti possono verosimilmente violare le disposizioni del presente regolamento; b) rivolgere ammonimenti al titolare e del trattamento o al responsabile del trattamento ove i trattamenti abbiano violato le disposizioni del presente regolamento; c) ingiungere al titolare del trattamento o al responsabile del trattamento di soddisfare le richieste dell'interessato di esercitare i diritti loro derivanti dal presente regolamento; d) ingiungere al titolare del trattamento o al responsabile del trattamento di conformare i trattamenti alle disposizioni del presente regolamento, se del caso, in una determinata maniera ed entro un determinato termine; e) ingiungere al titolare del trattamento di comunicare all'interessato una violazione dei dati personali; f) imporre una limitazione provvisoria o definitiva al trattamento, incluso il divieto di trattamento; g) ordinare la rettifica, la cancellazione di dati personali o la limitazione del trattamento a norma degli articoli 16, 17 e 18 e la notificazione di tali misure ai destinatari cui sono stati comunicati i dati personali ai sensi dell'articolo 17, paragrafo 2, e dell'articolo 19; h) ...; i) infliggere una sanzione amministrativa pecuniaria ai sensi dell'articolo 83, in aggiunta alle misure di cui al presente paragrafo, o in luogo di tali misure, in funzione delle circostanze di ogni singolo caso.	Art. 37 – Misure di esecuzione. Art. 38 – Sanzioni amministrative e Art. 14, C. 2 LETT. C).	Art. 38: identificazione delle casistiche che determinano sanzioni amministrative e loro individuazione tuttavia Art. 14. C- 2 LETT. c) qualora il Garante per la protezione dei dati personali o le autorità di controllo di altri Stati membri di cui all'articolo 55 o 56 del regolamento (UE) 2016/679 impongano una sanzione amministrativa pecuniaria ai sensi dell'articolo 58, paragrafo 2, lettera i), del medesimo regolamento, l'Autorità nazionale competente NIS non procede all'irrogazione delle sanzioni amministrative pecuniarie ai sensi dell'articolo 38 per una violazione di cui alla lettera b) del presente comma, imputabile al medesimo comportamento. L'Autorità nazionale competente NIS può tuttavia esercitare i poteri di esecuzione di cui all'articolo 37.

Articolo GDPR	Contenuto	Articolo NIS2	Contenuto
Art. 58 – Poteri delle autorità di controllo.	Poteri di indagine (Art. 58, par. 1). Poteri ispettivi (Art. 58, par. 2). Poteri autorizzativi e consultivi (Art. 58, par. 3). Poteri ulteriori attribuiti per legge.	Art. 34.	Monitoraggio, l'analisi e il supporto ai soggetti essenziali e ai soggetti importanti; verifica e le ispezioni; adozione di misure di esecuzione; irrogazione di sanzioni amministrative pecuniarie e accessorie.

Allegato B - Confronto tra Legge 90, Direttiva NIS2 e suo recepimento nel DLGS 138

SOGGETTI INTERESSATI

L. 90/2024		Direttiva (UE) 2022/2555		D.lgs. 138/2024	
Art. 1.	PA Centrali (elenco ISTAT); Regioni; Province autonome; Comuni capoluogo di regione; Comuni > 100.000 abitanti; ASL; Società in House; Città metropolitane; Società di trasporto pubblico extraurbano operanti nell'ambito delle città metropolitane; Società in House che forniscono servizi di raccolta, smaltimento o trattamento di acque reflue (urbane, domestiche o industriali) e di gestione dei rifiuti.	Artt. 1-3. Allegati I e II.	Soggetti critici tra cui si distinguono. Soggetto Essenziali (soggetti critici di cui all'art. 3, comma 1, lett. a e altri soggetti non critici di cui alle lettere seguenti). Soggetti Importanti (soggetti critici esclusi dalla definizione di cui sopra).	Art. 3.	Soggetti individuati negli allegati I, II, III e IV, che includono rispettivamente settori altamente critici, settori critici, categorie di Pubbliche Amministrazioni e ulteriori tipologie di soggetti sensibili.

ADEMPIMENTI: GESTIONE DEI RISCHI PER LA SICUREZZA INFORMATICA

L. 90/2024		Direttiva (UE) 2022/2555		D.lgs. 138/2024	
Art. 8, comma 1, lett. b.	I soggetti interessati alla produzione e all'aggiornamento di sistemi di analisi preventiva di rilevamento e di un piano per la gestione del rischio informatico.	Art. 21.	Gli Stati membri provvedono affinché i soggetti essenziali e importanti adottino misure tecniche, operative e organizzative adeguate e proporzionate per gestire i rischi posti alla sicurezza dei sistemi informatici 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.	Art. 24, comma 1.	Gestione dei rischi posti alla sicurezza dei sistemi informativi e di rete utilizzate nelle attività o nella fornitura dei servizi.

ADEMPIMENTI: GOVERNANCE E GESTIONE DEGLI INCIDENTI

L. 90/2024		Direttiva (UE) 2022/2555		D.lgs. 138/2024	
Art. 8, comma 1, lett. a.	Governance e piano di gestione degli incidenti (soggetti tenuti).	Art. 20 e Art. 21 § 2, lett. b.	Governance (Stati tenuti a vigilare sull'attuazione da parte degli organi di gestione dei soggetti essenziali e importanti) e piano di gestione degli incidenti (Stati tenuti a vigilare sull'attuazione da parte dei soggetti essenziali e importanti).	Art. 9.	Nell'ambito della strategia nazionale di cybersicurezza (sistema Paese) individuate misure strategiche e normative al fine di raggiungere e mantenere un livello elevato di cybersicurezza.

ADEMPIMENTI: RESPONSABILITÀ DEL MANAGEMENT

L. 90/2024		Direttiva (UE) 2022/2555		D.lgs. 138/2024	
Art. 1, comma 6.	Responsabilità disciplinare e amministrativo-contabile per i funzionari e i dirigenti responsabili.	Considerando 137 e Art. 20	Responsabilità nelle violazioni da parte dell'organo di gestione.	Art. 29.	Responsabilità degli organi di amministrazione e gli organi direttivi.

ADEMPIMENTI: POLITICHE DI NOTIFICA DEGLI INCIDENTI

L. 90/2024		Direttiva (UE) 2022/2555		D.lgs. 138/2024	
Art. 1.	Notifica senza ritardo e comunque entro il termine massimo di ventiquattro ore dal momento in cui ne sono venuti a conoscenza a seguito delle evidenze comunque ottenute, qualunque incidente riconducibile a una delle tipologie individuate nella tassonomia di cui al comma 1 ed effettuano, entro settantadue ore a decorrere dal medesimo momento, la notifica completa di tutti gli elementi informativi disponibili + notifiche volontarie.	Art. 23. Art 30.	Politica di notifica 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 (preavviso 24h; definitivo 72h) + notifiche volontarie.	Art. 25.	Politica di notifica 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 (preavviso 24h; definitivo 72h) + notifiche volontarie + aggiornamenti (relazione) e adempimenti indicati da CSIRT.

ADEMPIMENTI: MISURE DI SICUREZZA

L. 90/2024		Direttiva (UE) 2022/2555		D.lgs. 138/2024	
Art. 8, comma 1, lett. f). Art. 9.	Misure tecniche (richiamo dinamico).	Art. 21, § 2.	Misure tecniche (proporzionalità, tenuto conto delle conoscenze più aggiornate in materia e, se del caso, delle pertinenti norme europee e internazionali, nonché dei costi di attuazione.	Art. 24.	Misure di gestione dei rischi per la sicurezza informatica (tecniche, operative e organizzative adeguate e proporzionate).

ADEMPIMENTI: CRITTOGRAFIA

L. 90/2024		Direttiva (UE) 2022/2555		D.lgs. 138/2024	
Art. 9.	Crittografia.	Art. 21, § 2, lett. h.	Crittografia.	Art. 24, comma 2, lett. h.	Politiche e procedure relative all'uso della crittografia e, ove opportuno, della cifratura.

ADEMPIMENTI: FORMAZIONE E COMPETENZE

L. 90/2024		Direttiva (UE) 2022/2555		D.lgs. 138/2024	
Art. 8, comma 1, lett. e).	Nei termini di potenziamento delle capacità per la gestione dei rischi informatici.	Art. 20, § 2.	Formazione continua (promozione) affinché i dipendenti dei soggetti essenziali e importanti acquisiscano conoscenze e competenze sufficienti al fine di individuare i rischi e valutare le pratiche di gestione dei rischi di cybersicurezza e il loro impatto sui servizi offerti dal soggetto.	Art. 23, comma 2.	Formazione continua (politica dell'offerta) nei termini della NIS2.

ADEMPIMENTI: CATENA DEI FORNITORI

L. 90/2024		Direttiva (UE) 2022/2555		D.lgs. 138/2024	
Art. 14.	Disciplina del procurement.	Art. 21, § 2, lett. d; § 3.	Sicurezza della catena di approvvigionamento, ivi compresi gli aspetti relativi alla sicurezza riguardanti i rapporti tra ciascun soggetto e i suoi diretti fornitori o fornitori di servizi e compliance dei fornitori rispetto al rischio e focus su vulnerabilità specifiche.	Art. 24, comma 2, lett. d; comma 3.	Analogo a NIS2.

ADEMPIMENTI: VIGILANZA DA PARTE DELL'AUTORITÀ

L. 90/2024		Direttiva (UE) 2022/2555		D.lgs. 138/2024	
Art. 2.	Reazione al mancato o ritardato adeguamento a segnalazioni dell'Agenzia per la cybersicurezza nazionale.	Art. 32-33.	Misure di vigilanza e esecuzione (da parte delle Autorità nazionali) e adempimenti.	Art. 34.	Misure di vigilanza e esecuzione (ACN).

FIGURE FISICHE INVESTITE DI PARTICOLARI FUNZIONI

L. 90/2024		Direttiva (UE) 2022/2555		D.lgs. 138/2024	
Art. 8, comma 2.	Referente con funzioni di punto di contatto (in Aziende/Enti).	Art. 8.	Punto di contatto (negli Stati).	Art. 1, comma 2, lett. b). Art. 10	Punto di contatto nazionale ACN.

SANZIONI AMMINISTRATIVE

L. 90/2024		Direttiva (UE) 2022/2555		D.lgs. 138/2024	
Art. 11 e singole disposizioni specifiche (Art. 1, comma 6; art. 3).	Es. sanzione amministrativa pecuniaria da euro 25.000 a euro 125.000 nei casi di cui all'art. 1, comma 6.	Art. 34.	Fino a 10 000 000 EUR o al 2% del fatturato annuo mondiale per le entità essenziali, fino a un massimo di almeno 7 000 000 EUR o all'1,4% per le entità importanti.	Art. 38.	Fino a 10 000 000 EUR o al 2% del fatturato annuo mondiale per le entità essenziali, fino a un massimo di almeno 7 000 000 EUR o all'1,4% per le entità importanti. Comminate da ACN.

SANZIONI PENALI

L. 90/2024		Direttiva (UE) 2022/2555		D.lgs. 138/2024	
Art. 16.	Sanzioni penali per il contrasto dei reati informatici.	Cons. 128, 131, 132.	Sanzioni effettive, proporzionate e dissuasive anche di natura penale ma non obbligatorie nei confronti di chi deve garantire l'attuazione della direttiva.		N/A.

Allegato C - Elementi essenziali di cybersicurezza dei beni e dei servizi informatici

PARTE I. REQUISITI RELATIVI ALLE PROPRIETÀ DEI BENI E DEI SERVIZI INFORMATICI

1) I beni e i servizi informatici sono progettati, sviluppati, prodotti e forniti in modo da garantire un livello adeguato di cybersicurezza in base ai rischi.
2) Sulla base della valutazione dei rischi di cybersicurezza, i beni e i servizi informatici:
   a) sono forniti senza vulnerabilità sfruttabili note;
   b) sono forniti con una configurazione sicura per impostazione predefinita, con la possibilità di ripristinare il bene o servizio informatico allo stato originale;
   c) garantiscono che le vulnerabilità possano essere trattate mediante aggiornamenti di sicurezza, anche, se del caso, mediante aggiornamenti di sicurezza automatici installati entro e per un periodo di tempo adeguato, abilitato come impostazione predefinita, con un meccanismo di disattivazione chiaro e di facile utilizzo, attraverso la notifica agli utilizzatori degli aggiornamenti disponibili e la possibilità di rinviarli temporaneamente;
   d) garantiscono la protezione dall'accesso non autorizzato mediante adeguati meccanismi di controllo, tra cui, e in ogni caso, sistemi di autenticazione e di gestione dell'identità o dell'accesso, e che segnalano eventuali accessi non autorizzati;
   e) proteggono la riservatezza dei dati, personali o di altro tipo, conservati, trasmessi o altrimenti trattati, mediante l'uso di tecnologie allo stato dell'arte, tra cui sistemi per la cifratura dei pertinenti dati a riposo o in transito;
   f) proteggono l'integrità dei dati, personali o di altro tipo conservati, trasmessi o altrimenti trattati, dei comandi, dei programmi e della configurazione da qualsiasi manipolazione o modifica non autorizzata da parte dell'utilizzatore, e segnalano le corruzioni;
   g) trattano solo dati, personali o di altro tipo, adeguati, pertinenti e limitati a quanto necessario in relazione alla finalità prevista («minimizzazione dei dati»);
   h proteggono la disponibilità delle funzioni essenziali e di base, anche dopo un incidente, anche attraverso misure di resilienza e di mitigazione contro gli attacchi di negazione del servizio (denial of service);
   i) riducono al minimo il loro impatto negativo sulla disponibilità dei servizi forniti da altri dispositivi o reti;
   l) sono progettati, sviluppati, prodotti e forniti per limitare le superfici di attacco, comprese le interfacce esterne;
   m) sono progettati, sviluppati, prodotti e forniti per ridurre l'impatto degli incidenti utilizzando meccanismi e tecniche di mitigazione adeguati;
   n) forniscono informazioni sulla sicurezza registrando e monitorando le attività interne pertinenti, compresi l'accesso a dati, servizi o funzioni o la modifica degli stessi, con un meccanismo di disattivazione per l'utilizzatore;

o) offrono agli utenti la possibilità di rimuovere in modo sicuro e agevole, su base permanente, tutti i dati e tutte le impostazioni e, qualora tali dati possano essere trasferiti ad altri beni e servizi informatici, garantiscono che ciò avvenga in modo sicuro.

PARTE II. REQUISITI DI GESTIONE DELLE VULNERABILITÀ

1. La fornitura di beni e servizi informatici deve prevedere:
   a) l'identificazione e la documentazione delle vulnerabilità e dei componenti contenuti nel bene o servizio informatico, e la redazione di una distinta base del software in un formato di uso comune e leggibile da un dispositivo automatico, che includa almeno le dipendenze di primo livello del bene o servizio;
   b) in relazione ai rischi posti dai beni e servizi informatici, l'indirizzamento e la correzione tempestiva delle vulnerabilità, anche fornendo aggiornamenti di sicurezza; ove tecnicamente fattibile, nuovi aggiornamenti di sicurezza sono forniti separatamente dagli aggiornamenti della funzionalità;
   c) l'esecuzione di test e riesami efficaci e periodici della sicurezza dei beni e servizi informatici;
   d) una volta reso disponibile un aggiornamento di sicurezza, la condivisione e divulgazione agli utilizzatori delle informazioni sulle vulnerabilità risolte, comprendenti una descrizione delle vulnerabilità, informazioni che consentano agli utilizzatori di identificare il bene o servizio informatico interessato, l'impatto delle vulnerabilità, la loro gravità e informazioni chiare e accessibili che aiutino gli utilizzatori a correggere le vulnerabilità; in casi debitamente giustificati, qualora ritenuto che i rischi di sicurezza legati alla divulgazione siano superiori ai benefici in termini di sicurezza, è possibile ritardare la divulgazione di informazioni su una vulnerabilità risolta fino a quando gli utilizzatori non abbiano avuto la possibilità di applicare la pertinente patch , in coerenza con quanto previsto dall'art. 16 del decreto legislativo 4 settembre 2024, n. 138;
   e) l'adozione di misure per facilitare la condivisione di informazioni sulle potenziali vulnerabilità del bene o servizio informatico e dei componenti di terzi ivi contenuti, fornendo anche un indirizzo di contatto per la segnalazione delle vulnerabilità individuate;
   f) l'adozione di meccanismi per distribuire in modo sicuro gli aggiornamenti dei beni e servizi informatici al fine di garantire che le vulnerabilità siano corrette o mitigate in modo tempestivo e, ove applicabile per gli aggiornamenti di sicurezza, in modo automatico;
   g) l'identificazione dei fornitori e dei partner terzi di sistemi informatici, componenti e servizi, la loro prioritizzazione e valutazione, utilizzando, allo scopo, un processo di valutazione del rischio inerente alla catena di approvvigionamento cyber;
   h) l'adozione di meccanismi per garantire che, qualora disponibili, siano diffusi tempestivamente e gratuitamente, aggiornamenti di sicurezza al fine di risolvere i problemi di sicurezza individuati, accompagnati da messaggi di avviso che forniscano agli utilizzatori le informazioni pertinenti, comprese le potenziali misure da adottare.

Allegato D - Elenco delle categorie tecnologiche di beni e servizi informatici per le quali sono necessari elementi essenziali di cybersicurezza

1. Sistemi di gestione dell'identita' e software e hardware per la gestione degli accessi privilegiati, compresi i lettori di autenticazione e controllo degli accessi, tra cui i lettori biometrici
   30233300-4 Lettori di smart card
   30233310-7 Lettori di impronte digitali
   30233320-0 Lettori combinati di smart card e di impronte digitali
   48730000-4 Pacchetti software di sicurezza
   48731000-1 Pacchetti software di sicurezza dei file
   48732000-8 Pacchetti software di sicurezza dei dati

2. Software che cercano, rimuovono o mettono in quarantena i software maligni
   48731000-1 Pacchetti software di sicurezza dei file
   48732000-8 Pacchetti software di sicurezza dei dati
   48760000-3 Pacchetti software di protezione dai virus
   48761000-0 Pacchetti software antivirus

3. Prodotti con elementi digitali con funzione di rete privata virtuale (VPN)
   48200000-0 Pacchetti software per reti, Internet e intranet
   48211000-0 Pacchetti software per l'interconnettivita' di piattaforme
   48220000-6 Pacchetti software per Internet e intranet
   48510000-6 Pacchetti software di comunicazione
   48730000-4 Pacchetti software di sicurezza
   48821000-9 Server di rete
   48517000-5 Pacchetti software IT
   48219100-7 Pacchetti software gateway

4. Sistemi di gestione della rete
   48517000-5 Pacchetti software IT
   48219000-6 Pacchetti software vari per reti
   48210000-3 Pacchetti software per reti
   48200000-0 Pacchetti software per reti, Internet e intranet
   48219500-1 Pacchetti software per switch o router
   48219700-3 Pacchetti software per server di comunicazione
   48781000-6 Pacchetti software di gestione di sistemi
   48151000-1 Sistema di controllo informatico

5. Sistemi di gestione delle informazioni e degli eventi di sicurezza (sistemi SIEM)
   48517000-5 Pacchetti software IT
   48730000-4 Pacchetti software di sicurezza

6. Infrastrutture a chiave pubblica e software per il rilascio di certificati digitali
   48730000-4 Pacchetti software di sicurezza
   48732000-8 Pacchetti software di sicurezza dei dati
   48800000-6 Sistemi e server di informazione
   48810000-9 Sistemi di informazione
   48151000-1 Sistema di controllo informatico

7. Router, modem, anche di tipo satellitare, per la connessione a internet e switch
   30200000-1 Apparecchiature informatiche e forniture
   32400000-7 Network
   32410000-0 Rete locale
   32412000-4 Rete di comunicazioni
   32412100-5 Rete di telecomunicazioni
   32412120-1 Intranet
   32415000-5 Rete Ethernet
   32420000-3 Apparecchiature di rete
   32422000-7 Componenti di rete
   32424000-1 Infrastruttura di rete
   32427000-2 Sistema di rete
   32552410-4 Modem
   32413100-2 Router di rete
   32500000-8 Materiali per |telecomunicazioni
   32260000-3 Apparecchiature per la trasmissione di dati

8. Microprocessori con funzionalita' legate alla sicurezza
   31712116-6 Microprocessori
   31712200-2 Microsistemi

9. Microcontrollori con funzionalita' legate alla sicurezza
   31712116-6 Microprocessori
   31712200-2 Microsistemi

10. Circuiti integrati per applicazioni specifiche (ASIC), sistemi integrati su singolo |chip (SOC) e reti di porte |programmabili dall'utilizzatore |(FPGA) con funzionalita' legate alla sicurezza
    31712116-6 Microprocessori
    31712200-2 Microsistemi

11. Firewall, sistemi di rilevamento e prevenzione delle intrusioni
    31712110-4 Circuiti elettronici integrati e microassemblaggi
    31712113-5 Schede a circuiti integrati
    31712114-2 Circuiti elettronici integrati
    31712117-3 Pacchetti di circuiti integrati

12. Dispositivi hardware con cassette di sicurezza
    30210000-4 Macchine per l'elaborazione di dati (hardware)
    30211300-4 Piattaforme informatiche

13. Gateway per contatori intelligenti nell'ambito di sistemi di misurazione intelligenti quali definiti all'articolo 2, punto 23, della direttiva (UE) 2019/944 del Parlamento europeo e del Consiglio, e altri dispositivi a |fini di sicurezza avanzati, compreso il trattamento crittografico sicuro;
    38800000-3 Attrezzature di controllo dei processi industriali e attrezzature di controllo a distanza
    38820000-9 Attrezzatura per controllo a distanza

14. Carte intelligenti o dispositivi analoghi, compresi gli elementi sicuri
    30162000-2 Carte intelligenti

15. Sistemi di storage di rete (Network Attached Storage, Storage Area Network)
    32400000-7 Network
    30234500-3 Strumenti di stoccaggio di memoria
    30233000-1 Dispositivi di stoccaggio e lettura di dati

16. Sistemi e servizi di back-up
    48710000-8 Pacchetti software di back-up o recupero
    72910000-2 Servizi di back-up informatico

17. Sistemi di videosorveglianza per controllo accessi e sicurezza fisica, nonche' sistemi di acquisizione immagini per finalita' di controllo, |compresi gli scanner
    32323500-8 Sistema di videosorveglianza
    38582000-8 / 38581000-1 Scanner per controllo bagagli e merci

18. Servizi di consulenza, sviluppo e manutenzione di piattaforme software afferenti alle categorie 1, 2, 3, 4, 5, 6, 11, 15, 16 e 17
    72200000-7 Programmazione di software e servizi di consulenza
    72230000-6 Servizi di sviluppo di software personalizzati
    72210000-0 Servizi di programmazione di prodotti software in pacchetti
    72240000-9 Servizi di analisi e programmazione di sistemi
    72260000-5 Servizi connessi al software

72530000-9 Servizi per rete informatica
72550000-5 Servizi di audit informatico
72570000-1 Servizi di back-up informatico
72250000-2 Servizi di manutenzione e assistenza sistemi

19. Servizi cloud
    72300000-8 Servizi di elaborazione dati
    72310000-1 Servizi di trattamento dati
    72400000-4 Servizi di Internet
    72410000-7 Servizi di provider
    72416000-9 Fornitori di servizi di applicazioni
    72500000-0 Servizi informatici

20. Sistemi di sicurezza gestiti (Managed Security Services)
    72300000-8 Servizi di elaborazione dati
    72314000-9 Servizi di raccolta e di collazione dati
    72315000-6 Servizi di gestione e supporto di reti di trasmissione dati
    72315100-7 Servizi di assistenza per una rete di trasmissione dati
    72315200-8 Servizi di gestione di reti di trasmissione dati
    72316000-3 Servizi analisi di dati

21. Componenti hardware e |software per acquisizione dati, monitoraggio, supervisione controllo, attuazione e automazione di reti di telecomunicazione e sistemi industriali e infrastrutturali
    42961200-2 Sistemi SCADA (Supervisory Control And Data Acquisition)

22. Software di controllo droni
    34711200-6 Aeromobili senza pilota

Allegato E

Elenco alfabetico dei Paesi terzi tra quelli che sono parte di accordi di collaborazione sia con l'Unione europea sia con la NATO in materia di cybersicurezza, protezione delle informazioni classificate, ricerca e innovazione.

1. Australia
2. Corea del Sud
3. Giappone
4. Israele
5. Nuova Zelanda
6. Svizzera

Allegato F - Copia dell'allegato 2 di ACN

Misure di sicurezza di base per i soggetti essenziali

1 GOVERNO (GOVERN)

1.1 Contesto organizzativo (GV.OC): Il contesto – missione, aspettative degli stakeholder, dipendenze e requisiti legali, normativi e contrattuali – che influisce sulle decisioni di gestione del rischio di cybersecurity dell'organizzazione è compreso.

1.1.1 GV.OC-4: Gli obiettivi, le capacità e i servizi critici dai quali gli stakeholder dipendono o che si aspettano dall'organizzazione sono compresi e comunicati.

1 È mantenuto un elenco aggiornato dei sistemi informativi e di rete rilevanti.

1.2 Strategia di gestione del rischio (GV.RM): Le priorità, i vincoli, le dichiarazioni sulla tolleranza e la propensione al rischio, e le assunzioni dell'organizzazione sono stabilite, comunicate e utilizzate per supportare le decisioni sul rischio operativo.

1.2.1 GV.RM-03: Le attività e gli esiti della gestione del rischio di cybersecurity sono parte integrante dei processi di gestione del rischio dell'organizzazione.

1 Nell'ambito dei processi di gestione del rischio del soggetto NIS e nel rispetto delle politiche di cui alla misura GV.PO-01, è definito, attuato, aggiornato e documentato un piano di gestione dei rischi per la sicurezza informatica per identificare, analizzare, valutare, trattare e monitorare i rischi.

1.3 Ruoli, responsabilità e correlati poteri (GV.RR): I ruoli, le responsabilità e i correlati poteri in materia di cybersecurity per promuovere l'accountability, la valutazione delle prestazioni e il miglioramento continuo sono stabiliti e comunicati.

1.3.1 GV.RR-02: I ruoli, le responsabilità e i correlati poteri relativi alla gestione del rischio di cybersecurity sono stabiliti, comunicati, compresi e applicati.

1 È definita, approvata dagli organi di amministrazione e direttivi, e resa nota alle articolazioni competenti del soggetto NIS, l'organizzazione per la sicurezza informatica e ne sono stabiliti ruoli e responsabilità.

2 È mantenuto un elenco aggiornato del personale dell'organizzazione di cui al punto 1 avente specifici ruoli e responsabilità ed è reso noto alle articolazioni competenti del soggetto NIS.

3 All'interno dell'organizzazione per la sicurezza informatica di cui al punto 1, sono inclusi il punto di contatto, e almeno un suo sostituto, di cui alla determina adottata ai sensi dell'articolo 7, comma 6 del decreto NIS.

4 I ruoli e le responsabilità di cui al punto 1 sono riesaminati e, se opportuno, aggiornati periodicamente e comunque almeno ogni due anni, nonché qualora si verifichino incidenti significativi, variazioni organizzative o mutamenti dell'esposizione alle minacce e ai relativi rischi.

1.3.2 GV.RR-04: La cybersecurity è inclusa nelle pratiche delle risorse umane.
1 Per almeno i sistemi informativi e di rete rilevanti, il personale autorizzato ad accedervi è individuato previa valutazione dell'esperienza, capacità e affidabilità e deve fornire idonea garanzia del pieno rispetto della normativa in materia di sicurezza informatica.
2 Gli amministratori di sistema dei sistemi informativi e di rete sono individuati previa valutazione dell'esperienza, capacità e affidabilità e devono fornire idonea garanzia del pieno rispetto della normativa in materia di sicurezza informatica.
3 Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e documentate le procedure in relazione ai punti 1 e 2.
4 In accordo agli esiti della valutazione del rischio di cui alla misura ID.RA-05, sono definiti a livello contrattuale gli eventuali obblighi, in materia di sicurezza informatica, che rimangono validi dopo la cessazione o la modifica del rapporto di lavoro dei dipendenti del soggetto NIS (ad esempio prevedendo clausole in materia di riservatezza).
5 Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e documentate le procedure in relazione al punto 4.

1.4 Politica (GV.PO): La politica di cybersecurity dell'organizzazione è stabilita, comunicata e applicata.
1.4.1 GV.PO-01: La politica per la gestione del rischio di cybersecurity è stabilita in base al contesto organizzativo, alla strategia di cybersecurity e alle priorità, ed è comunicata e applicata.
1 Sono adottate e documentate politiche di sicurezza informatica per almeno i seguenti ambiti:
a) gestione del rischio;
b) ruoli e responsabilità;
c) affidabilità delle risorse umane;
d) conformità e audit di sicurezza;
e) gestione dei rischi per la sicurezza informatica della catena di approvvigionamento;
f) gestione degli asset;
g) gestione delle vulnerabilità;
h) continuità operativa, ripristino in caso di disastro e gestione delle crisi;
i) gestione dell'autenticazione, delle identità digitali e del controllo accessi;
j) sicurezza fisica;
k) formazione del personale e consapevolezza;
l) sicurezza dei dati;
m) sviluppo, configurazione, manutenzione e dismissione dei sistemi informativi e di rete;
n) protezione delle reti e delle comunicazioni;
o) monitoraggio degli eventi di sicurezza;
p) risposta agli incidenti e ripristino.
2 Per gli ambiti di cui al punto 1 sono incluse almeno le politiche in relazione ai requisiti indicati nella tabella 1 in appendice al presente allegato.
3 Le politiche di cui al punto 1 sono approvate dagli organi di amministrazione e direttivi.

1.4.2 GV.PO-02: La politica per la gestione del rischio di cybersecurity è revisionata, aggiornata, comunicata e applicata per riflettere i cambiamenti nei requisiti, nelle minacce, nella tecnologia e nella missione dell'organizzazione.

1 Le politiche di cui alla misura GV.PO-01 sono riesaminate e, se opportuno, aggiornate periodicamente e comunque almeno con cadenza annuale, nonché qualora si verifichino evoluzioni del contesto normativo in materia di sicurezza informatica, incidenti significativi, variazioni organizzative o mutamenti dell'esposizione alle minacce e ai relativi rischi.

2 Ai fini del riesame di cui al punto 1, è verificata almeno la conformità delle politiche di cui alla misura GV.PO-01 alla normativa in materia di sicurezza informatica.

3 È mantenuto un registro aggiornato contenente gli esiti del riesame di cui al punto 1.

1.5 Gestione del rischio di cybersecurity della catena di approvvigionamento (GV.SC): I processi di gestione del rischio di cybersecurity della catena di approvvigionamento sono identificati, stabiliti, gestiti, monitorati e migliorati dagli stakeholder dell'organizzazione.

1.5.1 GV.SC-01: Sono stabiliti e accettati dagli stakeholder dell'organizzazione il programma, la strategia, obiettivi, politiche e processi di gestione del rischio di cybersecurity della catena di approvvigionamento.

1 In merito all'affidamento di forniture con potenziali impatti sulla sicurezza dei sistemi informativi e di rete, anche mediante ricorso agli strumenti delle centrali di committenza di cui all'allegato I.1, articolo 1, comma 1, lettera i), del decreto legislativo 31 marzo 2023, n. 36, sono previsti:

a) il coinvolgimento dell'organizzazione per la sicurezza informatica di cui alla misura GV.RR-02 nella definizione ed esecuzione dei processi di approvvigionamento a partire dalla fase di identificazione e progettazione della fornitura;

b) in accordo agli esiti della valutazione del rischio associato alla fornitura di cui alla misura GV.SC-07, la definizione di requisiti di sicurezza sulla fornitura coerenti con le misure di sicurezza applicate dal soggetto NIS ai sistemi informativi e di rete.

2 Per i requisiti di sicurezza di cui al punto 1, lettera b), sono considerati, ove applicabile, almeno i seguenti ambiti:

a) affidabilità dei fornitori, tenendo conto almeno delle loro eventuali vulnerabilità specifiche, della qualità complessiva dei loro prodotti e delle pratiche di sicurezza informatica, specie con riguardo all'oggetto della fornitura, della capacità di garantire l'approvvigionamento, l'assistenza e la manutenzione nel tempo, nonché, ove applicabile, dei risultati delle valutazioni coordinate dei rischi per la sicurezza delle catene di approvvigionamento critiche effettuate dal Gruppo di cooperazione NIS;

b) ruoli e responsabilità nell'ambito della fornitura;

c) affidabilità delle risorse umane;

d) conformità e audit di sicurezza;

e) gestione delle vulnerabilità;

f) continuità operativa e ripristino in caso di disastro;

g) gestione dell'autenticazione, delle identità digitali e del controllo accessi;
h) sicurezza fisica;
i) formazione del personale e consapevolezza;
j) sicurezza dei dati;
k) protezione delle reti e delle comunicazioni;
l) monitoraggio degli eventi di sicurezza ivi inclusi gli accessi e le attività effettuate;
m) gestione e segnalazione degli incidenti;
n) sviluppo sicuro del codice e sicurezza fin dalla progettazione e per impostazione predefinita;
o) manutenzione ordinaria ed evolutiva ivi inclusi gli aggiornamenti di sicurezza;
p) dismissione della fornitura ivi compresa la restituzione e la cancellazione dei dati;
q) subappalto, subfornitura o relativi potenziali requisiti di sicurezza lungo la catena di fornitura.

1.5.2 GV.SC-02: I ruoli e le responsabilità in materia di cybersecurity per fornitori, clienti e partner sono stabiliti, comunicati e coordinati internamente ed esternamente.
1 Nell'ambito dell'organizzazione per la sicurezza informatica di cui alla misura GV.RR-02, sono definiti e resi noti alle articolazioni competenti del soggetto NIS gli eventuali ruoli e responsabilità in materia di sicurezza informatica assegnati al personale delle terze parti.
2 Il personale di cui al punto 1 avente specifici ruoli e responsabilità è incluso nell'elenco di cui al punto 2 della misura GV.RR-02.

1.5.3 GV.SC-04: I fornitori sono noti e prioritizzati in base alla criticità.
1 È mantenuto un inventario aggiornato dei fornitori, le cui forniture hanno un potenziale impatto sulla sicurezza dei sistemi informativi e di rete, che comprende almeno:
a) gli estremi di contatto del referente della fornitura;
b) la tipologia di fornitura.

1.5.4 GV.SC-05: I requisiti per affrontare i rischi di cybersecurity nella catena di approvvigionamento sono stabiliti, prioritizzati e integrati nei contratti e in altri tipi di accordi con i fornitori e altre terze parti rilevanti.
1 Fatte salve motivate e documentate ragioni normative o tecniche, i requisiti di sicurezza di cui alla misura GV.SC-01, punto 1, lettera b) sono inseriti nelle richieste di offerta, bandi di gara, contratti, accordi e convenzioni relativi alle forniture con potenziali impatto sulla sicurezza dei sistemi informativi e di rete.

1.5.5 GV.SC-07: I rischi posti da un fornitore, dai suoi prodotti e servizi e da altre terze parti sono compresi, registrati, prioritizzati, valutati, trattati e monitorati nel corso della relazione.
1 Nell'ambito della valutazione del rischio di cui alla misura ID.RA-05, è valutato e documentato il rischio associato alle forniture. A tal fine, sono valutati almeno:
a) il livello di accesso del fornitore ai sistemi informativi e di rete del soggetto NIS;
b) l'accesso del fornitore alla proprietà intellettuale e ai dati anche sulla base della loro criticità;
c) l'impatto di una grave interruzione della fornitura;

d) i tempi e i costi di ripristino in caso di indisponibilità dei servizi;
e) i ruoli e le responsabilità del fornitore nel governo dei sistemi informativi e di rete.

2 È verificata periodicamente e documentata la conformità delle forniture ai requisiti di cui alla misura GV.SC-05.

2 IDENTIFICAZIONE (IDENTIFY)

2.1 Gestione degli asset (ID.AM): Gli asset (ad esempio, dati, hardware, software, sistemi, infrastrutture, servizi, persone) che consentono all'organizzazione di raggiungere gli obiettivi di business sono identificati e gestiti in coerenza con la loro importanza rispetto agli obiettivi organizzativi e alla strategia sul rischio dell'organizzazione.

2.1.1 ID.AM-01: Sono mantenuti gli inventari dell'hardware gestito dall'organizzazione.

1 È mantenuto un inventario aggiornato degli apparati fisici (hardware) che compongono i sistemi informativi e di rete, ivi inclusi i dispositivi IT, IoT, OT e mobili, approvati da attori interni al soggetto NIS.

2.1.2 ID.AM-02: Sono mantenuti gli inventari del software, dei servizi e dei sistemi gestiti dall'organizzazione.

1 È mantenuto un inventario aggiornato dei servizi, dei sistemi e delle applicazioni software che compongono i sistemi informativi e di rete, ivi incluse le applicazioni commerciali, open-source e custom, anche accessibili tramite API, approvati da attori interni al soggetto NIS.

2.1.3 ID.AM-03: Sono mantenute le rappresentazioni delle comunicazioni di rete, dei flussi di dati di rete interni ed esterni, autorizzati dall'organizzazione.

1 È mantenuto un inventario aggiornato dei flussi di rete tra i sistemi informativi e di rete del soggetto NIS e l'esterno, approvati da attori interni al soggetto NIS.

2.1.4 ID.AM-04: Sono mantenuti gli inventari dei servizi erogati dai fornitori.

1 È mantenuto un inventario aggiornato dei servizi informatici erogati dai fornitori, ivi inclusi i servizi cloud.

2.2 Valutazione del rischio (Risk Assessment) (ID.RA): È compreso il rischio di cybersecurity al quale l'organizzazione, gli asset e le persone sono esposti.

2.2.1 ID.RA-01. Le vulnerabilità negli asset sono identificate, confermate e registrate.

1 Le informazioni di cui al punto 1 della misura ID.RA-08 sono utilizzate per identificare eventuali vulnerabilità sui i sistemi informativi e di rete.

2 Per almeno i sistemi informativi e di rete rilevanti, in accordo al piano di gestione delle vulnerabilità di cui alla misura ID.RA-08, fatte salve motivate e documentate ragioni normative o tecniche, sono eseguite periodicamente e comunque prima della loro messa in esercizio, attività per l'identificazione delle vulnerabilità che comprendano almeno vulnerability assessment e/o penetration test.

3 Le attività di cui al punto 2 sono documentate tramite apposite relazioni che contengono almeno:
a) la descrizione generale delle attività effettuate e gli esiti delle stesse;

b) la descrizione delle vulnerabilità rilevate e il relativo livello di impatto sulla sicurezza.

2.2.2 ID.RA-05: Minacce, vulnerabilità, probabilità e impatti sono utilizzati per comprendere il rischio inerente e per informare la prioritizzazione della risposta al rischio.

1 In accordo al piano di gestione dei rischi per la sicurezza informatica di cui alla misura GV.RM-03, è eseguita e documentata la valutazione del rischio posto alla sicurezza dei sistemi informativi e di rete, anche con riferimento alle eventuali dipendenze da fornitori e partner terzi, che comprende almeno:
   a) l'identificazione del rischio;
   b) l'analisi del rischio;
   c) la ponderazione del rischio.

2 La valutazione del rischio di cui al punto 1 è eseguita a intervalli pianificati e comunque almeno ogni due anni, nonché qualora si verifichino incidenti significativi, variazioni organizzative o mutamenti dell'esposizione alle minacce e ai relativi rischi.

3 La valutazione del rischio cui al punto 1 è approvata dagli organi di amministrazione e direttivi.

4 La valutazione del rischio di cui al punto 1 è effettuata considerando almeno le minacce interne ed esterne, le vulnerabilità non risolte e gli impatti conseguenti ad eventuali incidenti.

2.2.3 ID.RA-06: Le risposte al rischio sono scelte, prioritizzate, pianificate, monitorate e comunicate.

1 È definito, documentato, eseguito e monitorato un piano di trattamento del rischio che comprende almeno:
   a) le opzioni di trattamento e le misure da attuare in merito al trattamento di ciascun rischio individuato e le relative priorità;
   b) le articolazioni competenti per l'attuazione delle misure di trattamento dei rischi e le tempistiche per tale attuazione;
   c) la descrizione e le ragioni che giustificano l'accettazione di eventuali rischi residui al trattamento.

2 Qualora per motivate e documentate ragioni normative o tecniche non siano attuati i requisiti di cui alla tabella 2 in appendice al presente allegato, sono adottate, ove applicabile, misure di mitigazione compensative e il piano di cui al punto 1 include la descrizione di tali misure e dell'eventuale rischio residuo.

3 Il piano di cui al punto 1, ivi compresa l'accettazione di eventuali rischi residui, è approvato dagli organi di amministrazione e direttivi.

2.2.4 ID.RA-08: Sono stabiliti processi per la ricezione, l'analisi e la risposta alle divulgazioni di vulnerabilità.

1 Sono monitorati almeno i canali di comunicazione del CSIRT Italia, nonché di eventuali CERT e Information Sharing & Analysis Centre (ISAC) settoriali, al fine di acquisire, analizzare e rispondere alle informazioni sulle vulnerabilità.

2 Le vulnerabilità, ivi comprese quelle identificate ai sensi della misura ID.RA-01, sono

prontamente risolte attraverso aggiornamenti di sicurezza o misure di mitigazione, ove disponibili, ovvero accettando e documentando il rischio in accordo al piano di trattamento del rischio informatico di cui alla misura ID.RA-06.

3 È definito, attuato, aggiornato e documentato un piano di gestione delle vulnerabilità che comprende almeno:
   a) le modalità per l'identificazione delle vulnerabilità di cui alla misura ID.RA-01 e la relativa pianificazione delle attività;
   b) le modalità per monitorare, ricevere, analizzare e rispondere alle informazioni sulle vulnerabilità;
   c) le procedure, i ruoli, le responsabilità per lo svolgimento delle attività di cui alle lettere a) e b).

4 Il piano di cui al punto 3 è approvato dagli organi di amministrazione e direttivi.

5 Ai fini di cui al punto 1, sono monitorati anche i canali dei fornitori del software ritenuto critico.

2.3 Miglioramento (ID.IM): I miglioramenti ai processi, alle procedure e alle attività di gestione del rischio di cybersecurity dell'organizzazione sono identificati in tutte le funzioni del framework.

2.3.1 ID.IM-01: Sono identificati miglioramenti in esito alle valutazioni.

1. In accordo agli esiti del riesame di cui al punto 1 della misura GV.PO-02, è definito, attuato, documentato e approvato dagli organi di amministrazioni e direttivi un piano di adeguamento che identifichi gli interventi necessari ad assicurare l'attuazione delle politiche di sicurezza.
2. Gli organi di amministrazione e direttivi sono informati mediante apposite relazioni periodiche sugli esiti dei piani di cui al punto 1.
3. È definito, attuato, aggiornato e documentato un piano per la valutazione dell'efficacia delle misure di gestione del rischio per la sicurezza informatica che comprenda l'indicazione delle misure da valutare e i relativi metodi di valutazione.
4. Gli organi di amministrazione e direttivi sono informati mediante apposite relazioni periodiche sul piano di valutazione dell'efficacia di cui al punto 3.

2.3.2 ID.IM-04: I piani di risposta agli incidenti e gli altri piani di cybersecurity che impattano le operazioni sono stabiliti, comunicati, mantenuti e migliorati.

1 Per almeno i sistemi informativi e di rete rilevanti è definito, attuato, aggiornato e documentato un piano di continuità operativa, che comprende almeno:
   a) le finalità e l'ambito di applicazione;
   b) i ruoli e le responsabilità;
   c) i contatti principali e i canali di comunicazione (interni ed esterni);
   d) le condizioni per l'attivazione e la disattivazione del piano;
   e) le risorse necessarie, ivi compresi i backup e le ridondanze.

2 Per almeno i sistemi informativi e di rete rilevanti è definito, attuato, aggiornato e documentato un piano di ripristino in caso di disastro, che comprende almeno:
   a) le finalità e l'ambito di applicazione;

b) i ruoli e le responsabilità;
c) i contatti principali e i canali di comunicazione (interni ed esterni);
d) le condizioni per l'attivazione e la disattivazione del piano;
e) le risorse necessarie, ivi compresi i backup e le ridondanze;
f) l'ordine di ripristino delle operazioni;
g) le procedure di ripristino per operazioni specifiche, compresi gli obiettivi di ripristino.

3 Per almeno i sistemi informativi e di rete rilevanti è definito, attuato, aggiornato e documentato un piano per la gestione delle crisi che comprende almeno:
a) i ruoli e responsabilità del personale e, se opportuno, dei fornitori, specificando l'assegnazione dei ruoli in situazioni di crisi, comprese le procedure specifiche da seguire;
b) le modalità di comunicazione tra i soggetti e le autorità competenti.

4 I piani di cui ai punti 1, 2 e 3 sono approvati dagli organi di amministrazione e direttivi.

5 I piani di cui ai punti 1, 2 e 3 sono riesaminati e, se opportuno, aggiornati periodicamente e comunque almeno ogni due anni, nonché qualora si verifichino incidenti significativi o mutamenti dell'esposizione alle minacce e ai relativi rischi.

3 PROTEZIONE (PROTECT)

3.1 Gestione delle identità, autenticazione e controllo degli accessi (PR.AA): L'accesso agli asset fisici e logici è limitato agli utenti, ai servizi e all'hardware autorizzati, e gestito in misura appropriata alla valutazione del rischio di accesso non autorizzato.

3.1.1 PR.AA-01: Le identità e le credenziali degli utenti, dei servizi e dell'hardware autorizzati sono gestite dall'organizzazione.

1 Tutte le utenze, ivi incluse quelle con privilegi amministrativi e quelle utilizzate per l'accesso remoto, sono censite, approvate da attori interni al soggetto NIS e, fatte salve motivate e documentate ragioni tecniche, in accordo agli esiti della valutazione del rischio di cui alla misura ID.RA-05, sono individuali per gli utenti.

2 Le credenziali (ad esempio nome utente e password) relative alle utenze sono robuste e aggiornate in accordo agli esiti della valutazione del rischio di cui alla misura ID.RA-05.

3 Per almeno i sistemi informativi e di rete rilevanti, sono verificate periodicamente le utenze e le relative autorizzazioni, aggiornandole/revocandole in caso di variazioni (ad esempio trasferimento o cessazione di personale).

4 Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e documentate le procedure in relazione ai punti 1, 2 e 3.

3.1.2 PR.AA-03: Utenti, servizi e hardware sono autenticati.

1 Le modalità di autenticazione delle utenze per accedere ai sistemi informativi e di rete sono commisurate al rischio. A tal fine sono valutati almeno i rischi connessi:
a) ai privilegi delle utenze;
b) alla criticità dei sistemi informativi e di rete;
c) alla tipologia di operazioni che le utenze possono effettuare sui sistemi informativi e di rete.

2 Per almeno i sistemi informativi e di rete rilevanti e in accordo agli esiti della valutazione del rischio di cui alla misura ID.RA-05, sono impiegate modalità di autenticazione multi fattore.
3 Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e documentate le procedure in relazione ai punti 1 e 2.

3.1.3 PR.AA-05: I permessi, i diritti e le autorizzazioni di accesso sono definiti in una politica, gestiti, applicati e rivisti e incorporano i principi del minimo privilegio e della separazione dei compiti.
1 I permessi sono assegnati alle utenze in accordo ai principi del minimo privilegio e della separazione delle funzioni, tenuto anche conto della necessità di conoscere (need to know).
2 È assicurata la completa distinzione tra utenze con e senza privilegi amministrativi degli amministratori di sistema alle quali debbono corrispondere credenziali diverse.
3 Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e documentate le procedure in relazione ai punti 1e 2.

3.1.4 PR.AA-06: L'accesso fisico agli asset è gestito, monitorato e applicato in misura appropriata al rischio.
1 Per almeno i sistemi informativi e di rete rilevanti, l'accesso fisico è protetto.
2 Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e documentate le procedure in relazione al punto 1.

3.2 Consapevolezza e formazione (PR.AT): Il personale dell'organizzazione è sensibilizzato e formato sulla cybersecurity in modo da poter svolgere i propri compiti inerenti alla cybersecurity.

3.2.1 PR.AT-01: Il personale è sensibilizzato e formato in modo da possedere le conoscenze e le competenze per svolgere compiti di carattere generale tenendo conto dei rischi di cybersecurity.
1 È definito, attuato, aggiornato e documentato un piano di formazione in materia di sicurezza informatica del personale, ivi inclusi gli organi di amministrazione e direttivi, che comprende almeno:
a) la pianificazione delle attività di formazione previste con l'indicazione dei contenuti della formazione fornita;
b) le eventuali modalità di verifica dell'acquisizione dei contenuti.
2 Il piano di formazione di cui al punto 1 è approvato dagli organi di amministrazione e direttivi.
3 È mantenuto un registro aggiornato recante l'elenco dei dipendenti che hanno ricevuto la formazione di cui al punto 1, i relativi contenuti e l'elenco delle verifiche svolte laddove previste.

3.2.2 PR.AT-02. Gli individui che ricoprono ruoli specializzati sono sensibilizzati e formati in modo da possedere le conoscenze e le competenze per svolgere i pertinenti compiti tenendo conto dei rischi di cybersecurity.
1 Il piano di cui alla misura PR.AT-01 prevede una formazione dedicata al personale con

ruoli specializzati, ossia che richiedono una serie di capacità e competenze attinenti alla sicurezza, ivi compresi gli amministratori di sistema, che comprende almeno:
a) le istruzioni relative alla configurazione e al funzionamento sicuri dei sistemi informativi e di rete;
b) le informazioni sulle minacce informatiche note;
c) le istruzioni sul comportamento da tenere in caso di eventi rilevanti per la sicurezza.

2 È mantenuto un registro aggiornato recante l'elenco dei dipendenti che hanno ricevuto la formazione di cui al punto 1, i relativi contenuti e l'elenco delle verifiche svolte laddove previste.

3.3 Sicurezza dei dati (PR.DS): I dati sono gestiti in modo coerente con la strategia sul rischio dell'organizzazione per proteggere la riservatezza, l'integrità e la disponibilità delle informazioni.

3.3.1 PR.DS-01: La riservatezza, l'integrità e la disponibilità dei dati a riposo (data-at-rest) sono protette.

1 Per almeno i sistemi informativi e di rete rilevanti e in accordo agli esiti della valutazione del rischio di cui alla misura ID.RA-05, fatte salve motivate e documentate ragioni normative o tecniche, i dati memorizzati sui dispositivi portatili, ivi inclusi laptop, smartphone e tablet, e sui supporti removibili, sono cifrati con protocolli e algoritmi allo stato dell'arte e considerati sicuri.

2 Fatte salve e documentate ragioni normative o tecniche, è disabilitata l'auto esecuzione dei supporti rimovibili ed è effettuata la loro scansione al fine di rilevare codici malevoli prima che siano utilizzati nei sistemi informativi e di rete.

3 Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e documentate le procedure in relazione ai punti 1 e 2.

3.3.2 PR.DS-02: La riservatezza, l'integrità e la disponibilità dei dati in transito (data-in-transit) sono protette.

1 Per almeno i sistemi informativi e di rete rilevanti, ivi inclusi quelli di comunicazione vocale, video e testuale, e in accordo agli esiti della valutazione del rischio di cui alla misura ID.RA-05 fatte salve motivate e documentate ragioni normative o tecniche, sono utilizzati, per la trasmissione dei dati da e verso l'esterno del soggetto NIS, protocolli e algoritmi di cifratura allo stato dell'arte e considerati sicuri.

2 Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e documentate le procedure in relazione al punto 1.

3.3.3 PR.DS-11: I backup dei dati sono creati, protetti, mantenuti e verificati.

1 In accordo alle esigenze di continuità operativa e di ripristino in caso di disastro individuate nei piani di cui alla misura ID.IM-04, sono effettuati periodicamente i backup dei dati e delle configurazioni e, per almeno i sistemi informativi e di rete rilevanti, sono anche conservate copie di backup offline.

2 Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e documentate le procedure in relazione al punto 1.

3 Per almeno i sistemi informativi e di rete rilevanti, è assicurata la riservatezza e l'integrità

delle informazioni contenute nei backup mediante adeguata protezione fisica dei supporti ovvero mediante cifratura.

4 Per almeno i sistemi informativi e di rete rilevanti, è verificata periodicamente l'utilizzabilità dei backup effettuati mediante test di ripristino.

5 Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e documentate le procedure in relazione ai punti 3 e 4.

3.4 Sicurezza delle piattaforme (PR.PS): L'hardware, il software (ad esempio firmware, sistemi operativi, applicazioni) e i servizi delle piattaforme fisiche e virtuali sono gestiti in modo coerente con la strategia sul rischio dell'organizzazione per proteggere la loro riservatezza, integrità e disponibilità.

3.4.1 PR.PS-01: Sono stabilite e applicate pratiche di gestione della configurazione.

1 Per almeno i sistemi informativi e di rete rilevanti, sono definite, e documentate in un elenco aggiornato, le loro configurazioni di riferimento sicure (hardened).

2 Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e documentate le procedure in relazione al punto 1.

3.4.2 PR.PS-02: Il software è mantenuto, sostituito e rimosso in base al rischio.

1 Fatte salve motivate e documentate ragioni normative o tecniche, è installato esclusivamente software, ivi compresi i sistemi operativi, per il quale è garantita la disponibilità di aggiornamenti di sicurezza.

2 Fatte salve motivate e documentate ragioni normative o tecniche, sono installati, senza ingiustificato ritardo, gli ultimi aggiornamenti di sicurezza rilasciati dal produttore in coerenza con il piano di gestione delle vulnerabilità di cui alla misura ID.RA-08.

3 Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e documentate le procedure in relazione ai punti 1e 2.

4 Fatte salve motivate e documentate ragioni normative o tecniche e in accordo agli esiti della valutazione del rischio di cui alla misura ID.RA-05, l'aggiornamento del software ritenuto critico è verificato in ambiente di test prima dell'effettivo impiego in ambiente operativo.

5 Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e documentate le procedure in relazione al punto 4.

3.4.3 PR.PS-03: L'hardware è mantenuto, sostituito e rimosso in base al rischio.

1 Per almeno i sistemi informativi e di rete rilevanti, sono adottate e documentate procedure per il trasferimento fisico e la dismissione di dispositivi atti alla memorizzazione di dati in modo sicuro.

2 Per almeno i sistemi informativi e di rete rilevanti, sono mantenuti uno o più registri delle manutenzioni effettuate sull'hardware.

3.4.4 PR.PS-04: I registri di log sono generati e resi disponibili per il monitoraggio continuo.

1 Tutti gli accessi eseguiti da remoto e quelli effettuati con utenze con privilegi amministrativi sono registrati.

2 Per almeno i sistemi informativi e di rete rilevanti, sono conservati in modo sicuro, e possibilmente centralizzato, almeno i log necessari ai fini del monitoraggio degli eventi di sicurezza, ivi compresi quelli relativi agli accessi di cui al punto 1.

3 In accordo agli esiti della valutazione rischio di cui alla misura ID.RA-05, sono definite e documentate le tempistiche di conservazione dei log di cui al punto 2.
4 Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e documentate le procedure in relazione ai punti 1 e 2.

3.4.5 PR.PS-06: Le pratiche di sviluppo sicuro del software sono integrate e le loro prestazioni sono monitorate durante l'intero ciclo di vita del software.
1 Sono adottate e documentate pratiche di sviluppo sicuro del codice nello sviluppo del software.

3.5 Resilienza dell'infrastruttura tecnologica (PR.IR): Le architetture di sicurezza sono gestite in accordo con la strategia sul rischio dell'organizzazione per proteggere la riservatezza, l'integrità e la disponibilità degli asset e la resilienza organizzativa.

3.5.1 PR.IR-01: Le reti e gli ambienti sono protetti dall'accesso logico e dall'uso non autorizzati.
1 Per almeno i sistemi informativi e di rete rilevanti, sono definite e documentate le eventuali attività consentite da remoto e implementate adeguate misure di sicurezza per l'accesso.
2 È mantenuto un elenco aggiornato dei sistemi informativi e di rete ai quali è possibile accedere da remoto con la descrizione delle relative modalità di accesso.
3 Sono presenti, aggiornati, mantenuti e configurati i sistemi perimetrali, quali firewall.
4 Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e documentate le procedure in relazione ai punti 1, 2 e 3.

3.5.2 PR.IR-03: Sono implementati meccanismi per soddisfare i requisiti di resilienza in situazioni normali e avverse.
1 In accordo agli esiti della valutazione del rischio di cui alla misura ID.RA-05, sono utilizzati sistemi di comunicazione di emergenza protetti.
2 Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e documentate le procedure in relazione al punto 1.

4 ILEVAMENTO (DETECT)

4.1 Monitoraggio continuo (DE.CM): Gli asset sono monitorati per individuare anomalie, indicatori di compromissione e altri eventi potenzialmente avversi.

4.1.1 DE.CM-01: Le reti e i servizi di rete sono monitorati per individuare eventi potenzialmente avversi.
1 Per almeno i sistemi informativi e di rete rilevanti, sono presenti, aggiornati, mantenuti e configurati in modo adeguato strumenti tecnici per rilevare tempestivamente gli incidenti significativi.
2 Sono definiti e documentati i livelli di servizio attesi (SL) dei servizi e delle attività del soggetto NIS anche ai fini di rilevare tempestivamente gli incidenti significativi.
3 Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e documentate le procedure in relazione ai punti 1 e 2.
4 Per almeno i sistemi informativi e di rete rilevanti, sono utilizzati strumenti di analisi e filtraggio sul flusso di traffico in ingresso (ivi inclusa la posta elettronica).

5 Per almeno i sistemi informativi e di rete rilevanti, ai fini di cui al punto 1, sono monitorati gli accessi da remoto, le attività dei sistemi perimetrali (ad esempio router e firewall), gli eventi amministrativi di rilievo, nonché gli accessi eseguiti o falliti alle risorse di rete, alle postazioni terminali e agli applicativi al fine di rilevare gli eventi di sicurezza informatica.

6 Per almeno i sistemi informativi e di rete rilevanti, ai fini di cui al punto 1, sono definiti, monitorati e documentati parametri quali-quantitativi per rilevare gli accessi non autorizzati o con abuso dei privilegi concessi.

7 Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e documentate le procedure in relazione ai punti 4, 5 e 6.

4.1.2 DE.CM-09: L'hardware e il software di elaborazione, gli ambienti di runtime e i loro dati sono monitorati per individuare eventi potenzialmente avversi.

1 Fatte salve motivate e documentate ragioni normative o tecniche, sono presenti, aggiornati, mantenuti e configurati in modo adeguato, sistemi di protezione delle postazioni terminali per il rilevamento del codice malevolo.

2 Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e documentate le procedure in relazione al punto 1.

5 RISPOSTA (RESPOND)

5.1 Gestione degli incidenti (RS.MA): Le risposte agli incidenti di cybersecurity rilevati sono gestite.

5.1.1 RS.MA-01: Il piano di risposta agli incidenti è eseguito in coordinamento con le terze parti interessate una volta dichiarato un incidente.

1 È definito, attuato, aggiornato e documentato un piano per la gestione degli incidenti di sicurezza informatica e la notifica al CSIRT Italia, in accordo a quanto previsto dall'articolo 25 del decreto NIS, che comprende almeno:

a) le fasi e le procedure di gestione e notifica degli incidenti con l'indicazione dei relativi ruoli e delle responsabilità;

b) le procedure per la predisposizione e la trasmissione delle relazioni di cui all'articolo 25, comma 5, lettere c), d) ed e) del decreto NIS;

c) le informazioni di contatto per la segnalazione degli incidenti;

d) le modalità di comunicazione interna, anche con riguardo al coinvolgimento degli organi di amministrazione e direttivi, ed esterna;

e) la reportistica da utilizzare per la documentazione dell'incidente.

2 Il piano di cui al punto 1 è approvato dagli organi di amministrazione e direttivi.

3 Il piano di cui al punto 1 è riesaminato e, se opportuno, aggiornato periodicamente e comunque almeno ogni due anni, nonché qualora si verifichino incidenti significativi, integrando le relative lezioni apprese, o mutamenti dell'esposizione alle minacce e ai relativi rischi.

5.2 Segnalazione e comunicazione della risposta agli incidenti (RS.CO): Le attività di risposta sono coordinate con gli stakeholder interni ed esterni come richiesto da leggi, regolamenti o politiche.

5.2.1 RS.CO-02: Gli stakeholder interni ed esterni sono informati degli incidenti.

1 In accordo al piano per la gestione degli incidenti di cui alla misura RS.MA-01, sono documentate e adottate procedure per comunicare senza ingiustificato ritardo, se ritenuto opportuno e qualora possibile, sentito il CSIRT Italia, ovvero qualora intimato dall'Agenzia per la cybersicurezza nazionale ai sensi dell'articolo 37, comma 3, lettere g) e h), del decreto NIS:
   a) ai destinatari dei loro servizi, gli incidenti significativi che possono ripercuotersi negativamente sulla fornitura di tali servizi;
   b) ai destinatari dei servizi che sono potenzialmente interessati da una minaccia informatica significativa, le misure o azioni correttive o di mitigazione che tali destinatari possono adottare in risposta a tale minaccia e la natura di tale minaccia.

2 Sono documentate e adottate procedure per informare il pubblico sugli incidenti occorsi, qualora intimato dall'Agenzia per la cybersicurezza nazionale ai sensi dell'art. 37, comma 3, lettera i) del decreto NIS.

6 RIPRISTINO (RECOVERY)

6.1 Esecuzione del piano di ripristino dagli incidenti (RC.RP): Le attività di ripristino sono eseguite per garantire la disponibilità operativa dei sistemi e dei servizi interessati da incidenti di cybersecurity.

6.1.1 RC.RP-01: La parte del piano di risposta agli incidenti relativa al ripristino viene eseguita una volta avviata dal processo di risposta agli incidenti.

1 Nell'ambito del piano per la gestione degli incidenti di cui alla misura RS.MA-01, sono adottate e documentate procedure per il ripristino con riguardo almeno al ripristino del normale funzionamento dei sistemi informativi e di rete coinvolti da incidenti di sicurezza informatica, ivi compresi quelli di cui all'articolo 25 del decreto NIS.

6.2 Comunicazione sul ripristino dagli incidenti (RC.CO): Le attività di ripristino sono coordinate con le parti interne ed esterne.

6.2.1 RC.CO-03: Le attività di ripristino e i progressi nel ripristino delle capacità operative sono comunicati agli stakeholder interni ed esterni designati.

1 Sono adottate e documentate procedure per comunicare alle parti interne interessate, ivi incluse le articolazioni competenti del soggetto NIS, le attività di ripristino a seguito di un incidente.

Tabella 1 - Requisiti di cui al punto 2 della misura GV.PO-01

Ambiti Politiche	Requisiti
a) Gestione del rischio.	GV.OC-04: punto 1. GV.RM-03: punto 1. ID.RA-05: punti 1, 2, 3 e 4. ID.RA-06: punti 1, 2 e 3.
b) Ruoli e responsabilità.	GV.RR-02: punti 1, 2, 3 e 4.
c) Affidabilità delle risorse umane.	GV.RR-04: punti 1, 2 e 4.

Ambiti Politiche	Requisiti
d) Conformità e audit di sicurezza.	GV.PO-01: punti 1, 2 e 3. GV.PO-02: punti 1, 2, 3. ID.IM-01: punti 1, 2, 3 e 4.
e) Gestione dei rischi per la sicurezza informatica della catena di approvvigionamento.	GV.SC-01: punti 1 e 2. GV.SC-02: punto 1. GV.SC-04: punto 1. GV.SC-05: punto 1. GV.SC-07: punti 1 e 2.
f) Gestione degli asset.	ID.AM-01: punto 1. ID.AM-02: punto 1. ID.AM-03: punto 1. ID.AM-04: punto 1.
g) Gestione delle vulnerabilità.	ID.RA-01: punti 1, 2 e 3. ID.RA-08: punti 1, 2, 3, 4 e 5.
h) Continuità operativa, ripristino in caso di disastro e gestione delle crisi	ID.IM-04: punti 1, 2, 3, 4 e 5.
i) Gestione dell'autenticazione, delle identità digitali e del controllo accessi.	PR.AA-01: punti 1, 2 e 3. PR.AA-03: punti 1 e 2. PR.AA-05: punti 1 e 2. PR.IR-01: punti 1 e 2.
j) Sicurezza fisica.	PR.AA-06: punto 1.
k) Formazione del personale e consapevolezza.	PR.AT-01: punti 1, 2 e 3. PR.AT-02: punti 1 e 2.
l) Sicurezza dei dati.	PR.DS-01: punti 1 e 2. PR.DS-02: punto 1. PR.DS-11: punti 1, 3 e 4.
m) Sviluppo, configurazione, manutenzione e dismissione dei sistemi informativi e di rete.	PR.PS-01: punto 1. PR.PS-02: punti 1, 2 e 4. PR.PS-03: punti 1 e 2. PR.PS-04: punti 1, 2 e 3. PR.PS-06: punto 1.
n) Protezione delle reti e delle comunicazioni.	PR.IR-01: punto 3. PR.IR-03: punto 1.
o) Monitoraggio degli eventi di sicurezza.	DE.CM-01: punti 1, 2, 4, 5 e 6. DE.CM-09: punto 1.
p) Risposta agli incidenti e ripristino.	RS.MA-01: punti 1, 2 e 3. RS.CO-02: punti 1 e 2. RC.RP-01: punto 1. RC.CO-03: punto 1.

Tabella 2 - Requisiti di cui al punto 2 della misura ID.RA-06

GV.SC-05: punto 1
ID.RA-01: punto 2
PR.AA-01: punto
PR.DS-01: punti 1 e 2
PR.DS-02: punto 1
PR.PS-02: punti 1, 2 e 4
DE.CM-09: punto 1

Allegato G - Tabella comparativa AGID NIS2

Obblighi di base	ID Misura ACN	Descrizione	Misure AGID Correlate	Note sul Confronto
Gestione del Rischio	GV.OC-04, GV.RM-03, ID.RA-05, ID.RA-06	Definizione e gestione del piano di rischio cybersecurity, valutazione periodica, trattamento e accettazione dei rischi, approvazione del vertice.	AGID A.3 (Gestione delle vulnerabilità), ABSC 4.8.1 (Definire un piano di gestione dei rischi).	NIS2 formalizza l'approvazione del rischio a livello di vertice e la periodicità delle valutazioni, con maggiore dettaglio sui contenuti del piano di trattamento.
Ruoli e Responsabilità	GV.RR-02	Definizione, approvazione e comunicazione dell'organizzazione cybersecurity, inclusi punti di contatto e sostituti.	AGID A.X (Ruoli e Responsabilità).	NIS2 specifica maggiormente la necessità di un'organizzazione formale di cybersecurity e di punti di contatto per le autorità.
Affidabilità Risorse Umane	GV.RR-04	Valutazione dell'affidabilità del personale autorizzato e degli amministratori di sistema, obblighi contrattuali post-impiego.	AGID A.11 (Formazione e consapevolezza del personale).	NIS2 è più esplicita sull'affidabilità del personale e sulla gestione delle clausole contrattuali post-impiego.
Conformità e Audit	GV.PO-01, GV.PO-02, ID.IM-01	Adozione e revisione di politiche di cybersecurity per tutte le aree, piani di miglioramento e valutazione dell'efficacia.	AGID A.X (Politiche e Procedure).	NIS2 dettaglia le aree di copertura delle politiche, enfatizza la revisione annuale, l'approvazione formale e la valutazione dell'efficacia con piani di adattamento.
Supply Chain Risk Mngt.	GV.SC-01, GV.SC-02, GV.SC-04, GV.SC-05, GV.SC-07	Programma di gestione del rischio della supply chain, requisiti di sicurezza per i fornitori nei contratti, inventario e valutazione continua dei fornitori critici.	AGID A.X (Gestione dei Fornitori).	Nuova area significativa per NIS2, con requisiti molto più stringenti e dettagliati sulla due diligence dei fornitori e l'estensione dei controlli.
Gestione degli Asset	ID.AM-01, ID.AM-02, ID.AM-03, ID.AM-04	Inventari aggiornati di hardware (IT, IoT, OT, mobile), software, flussi di rete e servizi di terzi (cloud).	AGID A.1 (Inventario degli asset hardware e software), ABSC 1 (Inventario dei dispositivi autorizzati e non autorizzati), ABSC 2 (Inventario dei software autorizzati e non autorizzati).	NIS2 è più esplicita nell'includere IoT, OT, dispositivi mobili e servizi cloud, riflettendo l'attuale panorama tecnologico.
Gestione Vulnerabilità	ID.RA-01, ID.RA-08	Identificazione periodica delle vulnerabilità (VA/PT), pronta risoluzione, monitoraggio fonti di informazione (CSIRT, fornitori).	AGID A.3 (Gestione delle vulnerabilità), ABSC 4 (Valutazione e correzione continua della vulnerabilità) , in particolare ABSC 4.1.1, ABSC 4.1.2, ABSC 4.4.2, ABSC 4.5.1, ABSC 4.7.1, ABSC 4.8.1, ABSC 4.8.2, ABSC 4.9.1	NIS2 enfatizza il monitoraggio proattivo delle fonti di informazione sulle vulnerabilità e la formalizzazione di un piano di gestione.

Obblighi di base	ID Misura ACN	Descrizione	Misure AGID Correlate	Note sul Confronto
Continuità Operativa, DR, Crisi	ID.IM-04	Piani documentati e approvati per continuità operativa, disaster recovery e gestione delle crisi, con ruoli, risorse, procedure chiare e revisione periodica.	AGID A.6 (Backup e ripristino dei dati e della configurazione), ABSC 10 (Copie di sicurezza) , AGID A.12 (Gestione della continuità operativa).	NIS2 consolida questi aspetti e aggiunge esplicitamente la "gestione delle crisi" con focus sulla comunicazione e coordinamento con le autorità.
Autenticazione, Identità, Accessi	PR.AA-01, PR.AA-03, PR.AA-05, PR.IR-01	Gestione identità/ credenziali (individuali, robuste, verificate), MFA proporzionata al rischio, minimo privilegio, separazione dei compiti, protezione accessi logici (firewall, remoto).	AGID A.4 (Gestione degli accessi), ABSC 5 (Uso appropriato dei privilegi di amministratore), in particolare ABSC 5.1.1, ABSC 5.1.2, ABSC 5.1.3, ABSC 5.2.1, ABSC 5.6.1, ABSC 5.7.1, ABSC 5.7.2, ABSC 5.7.3, ABSC 5.7.4, ABSC 5.8.1, ABSC 5.9.1, ABSC 5.10.1, ABSC 5.10.2, ABSC 5.10.3, ABSC 5.11.1, ABSC 5.11.2.	NIS2 rafforza l'obbligo di MFA per sistemi rilevanti e la distinzione tra account amministrativi/utente, con maggiore dettaglio sui principi di accesso.
Sicurezza Fisica	PR.AA-06	Protezione dell'accesso fisico agli asset, gestita, monitorata e applicata in modo appropriato al rischio.	AGID A.9 (Sicurezza fisica degli ambienti e delle infrastrutture)	NIS2 riafferma l'importanza della sicurezza fisica, sottolineando la proporzionalità al rischio.
Formazione e Consapevolezza	PR.AT-01, PR.AT-02	Piano di formazione cybersecurity per tutto il personale (inclusi vertici) e formazione dedicata per ruoli specializzati.	AGID A.11 (Formazione e consapevolezza del personale).	NIS2 enfatizza l'inclusione del top management e la formazione specifica per ruoli tecnici, riconoscendo l'importanza di una cultura della sicurezza a tutti i livelli.
Sicurezza dei Dati	PR.DS-01, PR.DS-02, PR.DS-11	Protezione riservatezza/ integrità/disponibilità dati a riposo (crittografia portatili/ removibili) e in transito (crittografia comunicazioni esterne); backup periodici (anche offline), protetti e verificati.	AGID A.6 (Backup e ripristino dei dati e della configurazione), ABSC 10 (Copie di sicurezza), ABSC 13 (Protezione dei dati), in particolare ABSC 10.3.1, ABSC 13.1.1, ABSC 13.2.1.	NIS2 specifica l'uso di "protocolli e algoritmi all'avanguardia e sicuri" per la crittografia e l'importanza dei backup offline e dei test di ripristino.
Sviluppo, Configurazione, Maint., Dismissione Sistemi	PR.PS-01, PR.PS-02, PR.PS-03, PR.PS-04, PR.PS-06	Configurazioni sicure, aggiornamenti tempestivi (con test), gestione sicura dismissione hardware/dati, logging accessi (remoti/ privilegiati), sviluppo software sicuro.	AGID A.2 (Configurazione di sicurezza - hardening), ABSC 3 (Proteggere le configurazioni di hardware e software), in particolare ABSC 3.1.1, ABSC 3.1.2, ABSC 3.2.1, ABSC 3.2.2, ABSC 3.2.3, ABSC 3.5.1, ABSC 3.5.2, ABSC 3.5.3, ABSC 3.5.4, ABSC 3.6.1, ABSC 3.7.1. Anche AGID A.7 (Gestione dei log), con ABSC 5.1.4, ABSC 5.4.1, ABSC 5.4.2, ABSC 5.4.3, ABSC 5.5.1 per il logging.	NIS2 introduce esplicitamente lo sviluppo sicuro del software (Security by Design/Default) e dettaglia i requisiti di logging e aggiornamento.

Obblighi di base	ID Misura ACN	Descrizione	Misure AGID Correlate	Note sul Confronto
Protezione Reti e Comunicazioni	PR.IR-03	Meccanismi per soddisfare requisiti di resilienza in situazioni normali e avverse, uso di sistemi di comunicazione di emergenza protetti.	AGID A.8 (Protezione delle comunicazioni), ABSC 8.5.1 (Usare strumenti di filtraggio del traffico di rete), ABSC 8.9.1 (Filtrare il contenuto dei messaggi di posta), ABSC 8.9.2 (Filtrare il contenuto del traffico web), ABSC 8.9.3 (Bloccare file potenzialmente pericolosi). Anche ABSC 3.4.1 (amministrazione remota con connessioni protette).	NIS2 si concentra specificamente sulla resilienza delle comunicazioni di emergenza, un aspetto cruciale per la gestione delle crisi.
Monitoraggio Eventi di Sicurezza	DE.CM-01, DE.CM-09	Strumenti tecnici per rilevamento incidenti, SL per servizi, analisi/ filtraggio traffico (email), monitoraggio accessi remoti/ privilegiati/perimetrali, protezione endpoint.	AGID A.7 (Gestione dei log), ABSC 8.1.3 (eventi rilevati inviati a repository centrale) , ABSC 8.5.1 (strumenti di filtraggio), ABSC 8.6.1 (monitorare, analizzare e bloccare accessi a indirizzi con cattiva reputazione), ABSC 8.10.1 (strumenti anti-malware basati sulle anomalie di comportamento). Anche ABSC 5.1.4, ABSC 5.4.1, ABSC 5.4.2, ABSC 5.4.3, ABSC 5.5.1 per il logging/ monitoraggio delle azioni amministrative.	NIS2 è più dettagliata sui tipi di eventi da monitorare, sull'uso di strumenti specifici (es. filtraggio email) e sulla definizione di parametri qualitativi/quantitativi per il rilevamento di anomalie.
Risposta Incidenti e Ripristino	RS.MA-01, RS.CO-02, RC.RP-01, RC.CO-03	Piano gestione/notifica incidenti (CSIRT Italia), procedure comunicazione utenti/pubblico, procedure ripristino operazioni, approvazione e revisione periodica.	AGID A.10 (Gestione degli incidenti di sicurezza), ABSC 8.11.1 (procedura di risposta agli incidenti che preveda la trasmissione al provider di sicurezza dei campioni di software sospetto).	NIS2 è estremamente dettagliata sulla notifica (tempi, contenuti, destinatari) e sulla comunicazione esterna, riflettendo la maggiore enfasi sulla trasparenza e sulla collaborazione con le autorità.

Allegato H - Modello di Governance

Presentiamo un esempio di modello di governance per una azienda fornitrice di strumenti informatici, dispositivi medici e servizi al settore sanitario. Chiaramente si tratta di un esempio lineare non particolareggiato ma che sicuramente fa capire già il molteplice ventaglio di competenze richieste per un adeguato e funzionale modello di Governance.
È necessario prevedere un gruppo di lavoro operativo multifunzione che possa adeguatamente analizzare e valutare le attività dell'azienda che hanno ricadute in termini di normativa NIS2, e allo stesso tempo possa relazionarsi in "orizzontale" e in "verticale" all'interno dell'azienda stessa, così come esternamente, con i destinatari della propria fornitura, ossia le aziende sanitarie.
Una possibile composizione del gruppo di lavoro è come segue:

- Referente Sistemi Informativi/IT "interni": l'azienda ha dei sistemi informativi interni, come minima configurazione, ma può anche sviluppare alcuni servizi per il cliente (azienda sanitaria), di conseguenza questa figura ha un ruolo essenziale, se si considera inoltre la competenza tecnica che può portare nel gruppo di lavoro e grazie alla quale può contribuire alla comprensioni di certi aspetti da parte di tutto il team.
- Referente Funzione Compliance: figura indispensabile, forse quella di principale rilevanza in quanto di fatto, la maggior parte se non tutti gli adempimenti relativi alla NIS2 "si trasformano" infine in Procedure aziendali che sanciscono ruoli, responsabilità, processi, modalità di comunicazione. Tale figura può probabilmente essere identificata anche come la Team Leader, con compito in esclusivo di riportare agli organi direttivi.
- Referente Marketing: è forse il professionista con cui l'azienda fornitrice si differenzia maggiormente dall'azienda sanitaria, in termini di Governance e ruoli. Il referente di Marketing è di fatto l'interfaccia tecnica "ma non troppo" (non meramente IT) che l'azienda mette a disposizione del cliente, ossia dell'azienda sanitaria, al fine di dialogare sul tema cyber-security, elaborare la documentazione necessaria, sviluppare specifiche funzionalità (laddove possibile) per quei dispositivi medici, strumenti e servizi che l'azienda privata offre al sistema sanitario ma che di fatto non produce direttamente. In questo senso il referente non risulta quindi essere il tecnico informatico o lo sviluppatore, ma colui che all'interno dell'azienda privata dialoga e collabora con gli sviluppatori, i quali sono collocati a livello internazionali. Questo è il caso di molte medie e grandi imprese, multinazionali, in cui i dispositivi medici sono sviluppati a livello "corporate" per tutti i Paesi, e la singola affiliata è quindi il tramite con cui vengono distribuiti messi a disposizione. In questo senso la figura di Marketing deve "localizzare" il più possibile il prodotto al fine di soddisfare i requisiti dei regolamenti nazionali e delle aziende sanitarie. Nel caso di azienda produttrice oltre che fornitrice, la figura può coincidere con il tecnico/sviluppatore informatico. Sul lato "interno" all'azienda, il referente di MKTG è responsabile anche di guidare o direttamente organizzare gli eventi informativi e formativi per il personale, a seconda del livello di coinvolgimento e il ruolo in ambito di Cybersecurity.

- Referente Commerciale: con questa figura non si fa tanto riferimento all'informatore o comunque colui che gestisce il puro rapporto commerciale (che comunque deve essere considerato e formato), ma si intende il professionista che in diretto rapporto con il cliente, installa, implementa e attiva il sistema/dispositivo medico che l'azienda fornisce al sistema sanitario, mette quindi in pratica quanto concordato, ad esempio dal tecnico informatico e dal DPO dell'azienda sanitaria con il referente di marketing, il legale e il referente commerciale stesso.
- Referente Team Legale: il team legale ha forse una quota di responsabilità inferiore rispetto alle altre funzioni, almeno laddove non coincide con la funzione di Compliance, quindi in aziende molto strutturate e di dimensioni medio grandi. Il ruolo è principalmente di supervisione delle attività del gruppo di lavoro e di supporto nell'interpretazione della normativa e degli aggiornamenti.

Bibliografia

[1] Privacy e Sicurezza a Supporto Dell'innovazione Digitale In Sanità: Il Nuovo GDPR, disponibile ai soci sul sito www.aisis.it

[2] Composizione del Tavolo per l'attuazione della disciplina NIS - Copia del documento con gli estremi del protocollo.

[3] Determinazione ACN 38564 del 26 novembre 2024 - Organizzazione e per il funzionamento del Tavolo per l'attuazione della disciplina NIS.

[4] Determinazione ACN 136117 del 10 aprile 2025 - Piattaforma, Punto di contatto e sostituto, aggiornamento delle informazioni e rappresentante NIS di cui all'articolo 7 del decreto NIS.

[5] Determinazione ACN 164179 del 14 aprile 2025 – Specifiche di base per l'adempimento agli obblighi di cui agli articoli 23, 24, 25, 29 e 32 del decreto NIS.

[6] Allegato recante le specifiche di base per l'adempimento agli obblighi di cui agli articoli 23 e 24 per i soggetti importanti.

[7] Allegato recante le specifiche di base per l'adempimento agli obblighi di cui agli articoli 23 e 24 per i soggetti essenziali.

[8] Allegato recante le specifiche di base per l'adempimento agli obblighi di cui all'articolo 25 per i soggetti importanti.

[9] Allegato recante le specifiche di base per l'adempimento agli obblighi di cui all'articolo 25 per i soggetti essenziali.

[10] Daniel Kahneman Thinking, Fast and Slow, London, Allen Lane, 2011, ISBN 9781846140556.

[11] NIS2 Technical Implementation Guidance, Versione 1.0, Giugno 2025, scaricabile dal sito www.enisa.europa.eu

[12] Moreno, R., & Mayer, R. E. (1999). Cognitive principles of multimedia learning: The role of modality and contiguity. Journal of educational psychology, 91(2), 358.

[13] Roger Spitz & Olivier Desbiey (2025) "The future of risk and insurability in the era of systemic disruption, unpredictability and artificial intelligence," Journal of Operational Risk, Journal of Operational Risk.