2025

ASSESSMENT NIS2

REPORT DI GAP ANALYSIS e REMEDIATION PLAN

FARMACIE ITALIANE SRL

Data: 11/07/2025

TIMENTERPRISE Telsy A TIM ENTERPRISE BRAND

ASSESSMENT NIS2

REPORT DI GAP ANALYSIS
e REMEDIATION PLAN

Rif. normativi: Direttiva (UE) 2022/2555 - D.Lgs. 138 del 04/09/2024

Questo documento è firmato con Non-Fungible Tokens (NFT), cosi come previsto dal Regolamento eIDAS (Regolamento UE n. 910/2014) e inviato via PEC .

TIMENTERPRISE Telsy A TIM ENTERPRISE BRAND

Anagrafica dell'Organizzazione

Indirizzo sede legale:	Via Abruzzi 25 (RM), 00187 Roma
Indirizzo sedi secondarie:	
Soggetti coinvolti:	Elisa Celletti Daniele De Biase Filippo Malzone
Data intervista:	14/05/2025
Data emissione report:	11/07/2025
Documento elaborato da:	Nicolò Serafini
Documento revisionato e approvato da: Titolo e funzioni:	Giuseppe Izzo Legale Rappresentante UESE ITALIA S.P.A.

SOMMARIO

INTRODUZIONE

Il presente documento costituisce l'esito dettagliato dell'attività di gap analysis condotta per FARMACIE ITALIANE SRL, d'ora in avanti "FARMACIE ITALIANE" o "l'organizzazione", al termine dell'attività Assessment, finalizzato all'adeguamento alle disposizioni della Direttiva (UE) 2022/2555 del Parlamento Europeo e del Consiglio del 14 dicembre 2022, comunemente nota come Direttiva NIS2, relativa a misure per un elevato livello comune di cybersicurezza nell'Unione.

CONTESTO NORMATIVO

La Direttiva NIS2

La direttiva (UE) n. 2022/2555, nota anche come “direttiva NIS2”, del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa a misure per un livello comune elevato di cybersicurezza nell'Unione europea, modifica il regolamento (UE) n. 910/2014, la direttiva (UE) n. 2018/1972 e abroga la precedente direttiva NIS, ossia la direttiva (UE) n. 2016/1148 sulla sicurezza delle reti e dei sistemi informativi nell'Unione, che fino ad oggi ha costituito il primo strumento legislativo dell'Unione europea sulla sicurezza in ambito cibernetico volto a prevedere misure giuridiche per incrementarne il livello complessivo.

La direttiva NIS2 fa parte di un pacchetto ampio di strumenti giuridici e di iniziative a livello dell'Unione, mirato ad aumentare la resilienza di soggetti pubblici e privati alle minacce nell'ambito cibernetico.

L'adozione della direttiva NIS2 mira a garantire un aumento del livello di sicurezza cibernetica comune, grazie all'armonizzazione delle norme applicabili ai diversi operatori nei diversi Stati membri e al rafforzamento dei livelli standard di sicurezza rispetto a quelli previsti dalla disciplina vigente, incidendo, in via prioritaria sui seguenti pilastri:

capacità degli Stati membri in relazione all’architettura istituzionale, alla strategia nazionale e ai piani di gestione delle crisi cibernetiche;

gestione del rischio da parte degli operatori, prevedendo misure di sicurezza adeguate e un sistema di notifica degli incidenti efficace e reattivo;

cooperazione e condivisione delle informazioni, attraverso diverse modalità di scambio, a livello nazionale ed europeo.

Il nuovo impianto normativo, inoltre, rafforza quanto già previsto dalla precedente direttiva NIS, recepita nell'ordinamento nazionale con il d.lgs. n. 65/2018.

Gap Analysis NIS2

Obiettivi, contenuti, metodologia

Obiettivi

L'obiettivo primario dell'attività è l'individuazione e la valutazione approfondita degli eventuali scostamenti esistenti tra le pratiche e le misure di sicurezza attualmente implementate da FARMACIE ITALIANE e i requisiti normativi e tecnici stabiliti dalla Direttiva NIS2. In particolare, come emerso dall'attività di Pre–Assessment effettuata in data 27/01/2025, FARMACIE ITALIANE è soggetta agli obblighi previsti dalla Direttiva in oggetto, secondo quanto previsto dall'Articolo 2.

L'organizzazione, pertanto, è tenuta a conformarsi ai requisiti specifici delineati dalla Direttiva, in relazione alla gestione del rischio di cybersicurezza, l'adozione di misure tecniche e organizzative adeguate e proporzionate, nonché gli obblighi di segnalazione degli incidenti significativi alle autorità competenti.

In conformità al regolamento di esecuzione (UE) 2024/2690 della commissione del 17 ottobre 2024, (relativo al considerando numero 3), l'attività di gap analysis Nis 2 è stata anche indirizzata alla raccolta e all'analisi approfondita delle informazioni necessarie per l'implementazione di un Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) conforme alla norma internazionale ISO/IEC 27001:2024.

L'adozione di tale standard supporta l'organizzazione, non solo nel soddisfare i requisiti normativi, ma anche nell'aderire alle best practice internazionali in materia di sicurezza delle informazioni, garantendo un approccio sistematico e integrato nella gestione dei rischi correlati.

Contenuti

Il presente documento fornisce una sintesi delle informazioni reperite nel corso dell'attività, evidenziando le discrepanze riscontrate rispetto ai requisiti specifici della Direttiva NIS2.

Per ciascun gap identificato, sono state formulate raccomandazioni specifiche, corredate da proposte di remediation finalizzate a colmare le carenze individuate e ad analizzare le implementazioni e gli investimenti necessari al raggiungimento di una postura di sicurezza in linea con la Direttiva NIS 2.
È fondamentale sottolineare che il raggiungimento di un elevato livello di conformità alla Direttiva NIS2 non rappresenta un semplice adempimento formale, bensì costituisce un elemento essenziale per la protezione degli asset critici dell'organizzazione, la salvaguardia della continuità operativa e la tutela della reputazione aziendale.

In un contesto in cui le minacce cibernetiche sono in costante evoluzione e intensificazione, l'implementazione di misure di sicurezza adeguate e proporzionate ai rischi identificati è imprescindibile per garantire la resilienza dell'organizzazione e mantenere la fiducia dei propri stakeholder.

Metodologia 1/2

L'approccio metodologico adottato per la conduzione della presente attività di gap analysis è stato concepito per garantire un'analisi esaustiva e sistematica delle misure di sicurezza informatica attualmente implementate dall'organizzazione, in relazione ai requisiti prescritti dalla Direttiva NIS2.

In primo luogo, è stata effettuata una dettagliata disamina degli obblighi normativi delineati dalla suddetta Direttiva, con particolare riferimento all'Articolo 21, il quale stabilisce le misure di gestione del rischio di cybersicurezza che le entità essenziali e importanti sono tenute ad adottare. Sulla base di tali prescrizioni, è stato sviluppato un quadro di riferimento composto da una serie di controlli specifici, ciascuno associato a un Control ID univoco, che raggruppano le macro-categorie di misure di sicurezza su cui la Direttiva insiste. Questo framework ha permesso di strutturare l'analisi in modo organico, assicurando la copertura completa di tutti gli aspetti rilevanti previsti dalla normativa.

Successivamente, sono state condotte interviste approfondite con le funzioni aziendali pertinenti, finalizzate a reperire informazioni dettagliate sulle misure tecniche e organizzative attualmente in essere all'interno dell'organizzazione. Le informazioni raccolte sono state analizzate e confrontate con i requisiti specifici associati a ciascun controllo identificato, al fine di valutare il grado di allineamento dell'organizzazione con le disposizioni della Direttiva NIS2. Tale processo ha consentito di identificare i gap esistenti, i.e. le aree in cui le misure implementate risultano insufficienti o non conformi rispetto alle aspettative normative.

Al fine di garantire un'analisi oggettiva e misurabile, è stata sviluppata una metrica di valutazione che ha attribuito a ciascun controllo un punteggio basato sul livello di conformità riscontrato. Tali punteggi sono stati poi aggregati per determinare un indice complessivo di conformità, il quale fornisce una rappresentazione quantificata del grado di aderenza dell'organizzazione ai requisiti della Direttiva (si veda la sezione "Risultati" per una disamina dettagliata).

Metodologia 2/2

Per ogni gap individuato, sono state elaborate raccomandazioni specifiche, articolate in relazione alla macroarea di controllo corrispondente.

Tali raccomandazioni tengono conto delle peculiarità operative dell'organizzazione, dell'entità del rischio associato al gap e delle best practice riconosciute a livello internazionale. Nella sezione "Remediation", le suddette raccomandazioni sono state ulteriormente sviluppate in azioni operative concrete che l'organizzazione può intraprendere per sanare le carenze identificate.

L'intero processo metodologico è stato guidato dai principi di integrità, riservatezza e professionalità, assicurando che tutte le informazioni raccolte siano state gestite in conformità con le normative vigenti in materia di protezione dei dati e che l'analisi sia stata condotta con il massimo rigore tecnico e giuridico.

Gap Analysis NIS2

Controlli e raccomandazioni

GAP ANALYSIS

La presente sezione offre una disamina dell'analisi delle discrepanze effettuata in relazione alle macroaree di controllo identificate mediante i Control ID, elaborati secondo la metodologia precedentemente delineata. Per ciascun Control ID vengono presentate le informazioni raccolte durante l'attività e, ove pertinenti, le raccomandazioni formulate per sanare i gap o per potenziare le misure esistenti. Le raccomandazioni proposte sono state elaborate tenendo conto delle peculiarità operative dell'organizzazione e delle best practice internazionali, con l'obiettivo di fornire soluzioni efficaci e sostenibili nel medio-lungo termine.

Gli elementi caratterizzanti delle macroaree di controllo sono stati derivati dalle prescrizioni dell'Articolo 21, comma 2 della Direttiva (UE) 2022/2555, il cui testo integrale è riportato di seguito.

"Articolo 21 Misure di gestione dei rischi di cibersicurezza

[...] 2. Le misure di cui al paragrafo 1 sono basate su un approccio multirischio mirante a proteggere i sistemi informatici e di rete e il loro ambiente fisico da incidenti e comprendono almeno gli elementi seguenti: a) politiche di analisi dei rischi e di sicurezza dei sistemi informatici; b) gestione degli incidenti; c) continuità operativa, come la gestione del backup e il ripristino in caso di disastro, e gestione delle crisi; d) sicurezza della catena di approvvigionamento, compresi aspetti relativi alla sicurezza riguardanti i rapporti tra ciascun soggetto e i suoi diretti fornitori o fornitori di servizi; e) sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informatici e di rete, compresa la gestione e la divulgazione delle vulnerabilità; f) strategie e procedure per valutare l'efficacia delle misure di gestione dei rischi di cibersicurezza; g) pratiche di igiene informatica di base e formazione in materia di cibersicurezza; h) politiche e procedure relative all'uso della crittografia e, se del caso, della cifratura; i) sicurezza delle risorse umane, strategie di controllo dell'accesso e gestione degli attivi;) uso di soluzioni di autenticazione a più fattori o di autenticazione continua, di comunicazioni vocali, video e testuali protette e di sistemi di comunicazione di emergenza protetti da parte del soggetto al proprio interno, se del caso.

[...]"

Control ID 1
Politiche di analisi dei rischi e di sicurezza dei sistemi informatici

Control ID 1 - Note
Si riscontra che non è mai stata condotta una valutazione del rischio formale. L'organizzazione non ha ancora una figura formalmente nominata come responsabile della sicurezza informatica (CISO). Elisa Celletti è stata identificata come referente IT e avrà la delega al ruolo di responsabile della cybersecurity, ma questa nomina non è ancora stata formalizzata. Non esiste attualmente un budget dedicato alla cybersecurity.
Raccomandazioni
Si raccomanda di definire e implementare una politica strutturata di analisi del rischio in linea con il contesto aziendale del settore farmaceutico, con particolare attenzione alla gestione di dati sensibili relativi alla salute e alle peculiarità della rete di farmacie distribuite sul territorio.

Control ID 2
Gestione degli incidenti

Control ID 2 - Note
Si riscontra che il cliente non ha una strategia formalizzata di Incident Response. Non è presente ad oggi alcuna procedura documentata per la gestione degli incidenti di sicurezza informatica. In caso di problemi, il personale contatta informalmente il responsabile IT tramite chiamata o email, senza un processo strutturato. Non esiste un sistema di ticketing per la registrazione degli incidenti.
Raccomandazioni
Si raccomanda di definire e formalizzare un processo di gestione degli incidenti, comprensivo di una tassonomia chiara e misure di risposta coerenti, con particolare attenzione alla gestione di incidenti che potrebbero compromettere dati sanitari sensibili e alla necessità di notifica alle autorità competenti entro i termini previsti dalla normativa.

Control ID 3
Continuità operativa

Control ID 3.1: Gestione del backup - Note
Si riscontra l'implementazione di un sistema prototipo nella farmacia di Nesima, loro farmacia controllata che include: sistema di business continuity con 3 UPS + gruppo elettrogeno di emergenza, due server (uno primario e uno secondario) con NAS che fa copie degli ultimi 7 giorni. C'è l'intenzione di estendere questa configurazione a tutte le farmacie della rete ma ad oggi non risultano procedure documentate di backup e test di ripristino.
Control ID 3.2: Disaster Recovery - Note
Non esiste un piano formale di Disaster Recovery strutturato per l'intera organizzazione. È presente, come già indicato, solo il prototipo implementato nella farmacia di Nesima che deve essere ancora esteso. Non sono stati effettuati test attivi di disaster recovery.
Control ID 3.3: Gestione delle crisi - Note
Non è presente una formalizzazione di un comitato di crisi o di procedure per la gestione delle emergenze. Non risultano policy formalizzate per la gestione delle crisi di sicurezza informatica all'interno dell'organizzazione.
Raccomandazioni
• Formalizzare un processo strutturato per la gestione dei backup garantendo integrità, disponibilità e riservatezza dei dati, estendendo il modello Nesima a tutte le farmacie; • Definire e implementare un piano di Disaster Recovery e Business Continuity completo per tutta l'organizzazione; • Implementare una strategia di Crisis Management con ruoli, responsabilità e procedure ben definite.

Control ID 4
Supply chain security

Control ID 4 - Note
Si riscontra non essere presente un controllo strutturato sulla gestione contrattuale con clausole di sicurezza per i fornitori critici. Per le fidelity card ad oggi vengono fatti assessment continuativi sulla privacy. Quando non riescono a risolvere un problema legato all'IT intervengono Consalvo e CGM per manutenzione, sistemistica o in generale problemi hardware o software, due società che forniscono assistenza alle farmacie e che accedono tramite TeamViewer ai sistemi dell'organizzazione. Non esistono procedure formalizzate per la valutazione della sicurezza di questi o in generale di tutti i fornitori critici.
Raccomandazioni
Si raccomanda di definire un processo strutturato e condiviso di gestione dei fornitori con criteri di sicurezza chiari, implementando clausole contrattuali specifiche per la cybersecurity e controlli periodici sui fornitori critici che accedono ai sistemi.

Control ID 5 - Gestione dei sistemi informatici e di rete

Control ID 5.1: Acquisizione di reti e sistemi - Note
Si riscontra che il cliente stia procedendo all'aggiornamento di tutte le macchine a Windows 11 e all'implementazione di sistemi hardware/software prototipo per la gestione backup e disaster recovery. Non risultano processi formalizzati per l'acquisizione di hardware e software con criteri di sicurezza documentati.
Control ID 5.2: Manutenzione di reti e sistemi - Note
Tutte le farmacie interne dialogano in VPN. L'organizzazione sta aggiungendo switch Aruba Networking con sistema operativo centrale cloud-native basato su microservizi e database e sistemando i rack delle farmacie controllate. Il software gestionale attualmente utilizzato risale al 1980 ed è scritto in COBOL il quale presenta grande difficolta di aggiornamento anche rispetto alle esigenze normative richieste. È installato ESET versione completa ed endpoint completa (EDR) su tutte le macchine. L'organizzazione sta cambiando tutti i server delle farmacie per i quali è stata riscontrata obsolescenza.
Control ID 5.3: Sviluppo di sistemi informatici - Note
Il problema principale, come già citato, è l'applicativo scritto in COBOL (sviluppato da una società esterna) che presenta limitazioni tecniche, tra cui l'impossibilità di implementare crittografia via database non essendo relazionale. L'organizzazione sta implementando un sistema per ricevere ordini tramite web service per modernizzare l'infrastruttura.
Control ID 5.4: Gestione delle vulnerabilità - Note
Non sono mai state implementate procedure di hardening dei sistemi o disattivazione dei servizi non necessari. Il logging è poco strutturato e non è presente un sistema SIEM per il monitoraggio centralizzato.
Raccomandazioni
• Implementare politiche e procedure per standardizzare l'acquisizione di infrastrutture IT con criteri di sicurezza documentati • Strutturare un processo documentato per la manutenzione sicura di reti e sistemi • Pianificare la migrazione dal sistema COBOL legacy verso soluzioni moderne che supportino nativamente la sicurezza o valutare con i fornitori alternative valide per garantire la sicurezza informatica del sistema • Implementare un processo strutturato per l'identificazione, valutazione e mitigazione delle vulnerabilità

Control ID 6
Valutazione delle misure di sicurezza implementate

Control ID 6 - Note
Si riscontra che l'organizzazione non abbia implementato un processo formale e strutturato per la valutazione delle misure di sicurezza. Non dispone di un SIEM per il controllo e monitoraggio centralizzato dei log. Non vengono effettuati audit periodici di sicurezza.
Raccomandazioni
Si raccomanda di definire un meccanismo strutturato di audit e valutazione continua delle misure di sicurezza, implementando un sistema SIEM per il monitoraggio centralizzato e definendo metriche specifiche per misurare l'efficacia delle misure implementate.

Control ID 7
Formazione e sensibilizzazione

Control ID 7.1: Pratiche di igiene informatica - Note
Non esiste una formalizzazione delle policy di uso sicuro di dispositivi aziendali e personali (BYOD), clear desk e clean screen per l'organizzazione.
Control ID 7.2: Formazione in materia di cyber security - Note
Si riscontra che, da maggio 2024, il cliente ha iniziato un programma di formazione a moduli con CyberGuru. Il programma include: campagne di phishing simulation, whitelisting per simulazione, videopillole di awareness e rilascio di certificazioni in alcuni ambiti per il completamento del percorso formativo. La formazione è gestita per iniziare dalla sede centrale per poi estendersi a tutti gli elementi del direttivo e successivamente a tutta la rete.
Raccomandazioni
• Formalizzare le policy relative all'igiene informatica di base (BYOD, clear desk, clean screen) cfr. 7.1 • Strutturare e completare il piano di formazione cybersecurity già avviato con CyberGuru, estendendolo a tutto il personale della rete di farmacie controllate.

Control ID 8
Crittografia

Control ID 8 - Note
Si riscontra una situazione critica, come già indicato il gestionale dell'organizzazione cripta solamente il codice fiscale. I dati non sono criptati nel transito tra le farmacie e il server centrale. Il limite tecnico dell'applicativo COBOL impedisce l'implementazione di crittografia a livello database non avendo un database relazionale. Si riscontra la volontà da parte dell'organizzazione di comunicare al fornitore del software la volontà di capire dove e come il software comunica per comprendere la sua disponibilità a creare una struttura di sicurezza idonea per questi canali. Per gli endpoint si riscontra l'esistenza di un sistema di crittografia gestito nativamente dalla console ESET PROTECT. A netto di ciò si riscontra che non esiste ad oggi una politica formale di crittografia per la protezione dei dati a riposo o in transito. Questa è una carenza a cui prestare particolare attenzione considerando che possono essere trattati dati sanitari sensibili.
Raccomandazioni
Implementare con massima urgenza una politica di crittografia completa, basata sulla classificazione dei dati, con particolare attenzione ai dati sanitari sensibili. Valutare soluzioni alternative per proteggere i dati in transito in attesa dell'eventuale migrazione dal sistema COBOL.

Control ID 9
Access control

Control ID 9.1: Sicurezza delle risorse umane - Note
Si riscontra che nell'ambito risorse umane la gestione della sicurezza è informale, senza policy documentate.
Control ID 9.2: Gestione degli accessi - Note
L'accesso ai sistemi avviene tramite account con privilegi amministrativi gestiti centralmente. I client non hanno accesso di tipo Amministratore e per aggiornamenti devono chiamare la sede centrale. Non risultano implementate policy di tipo 'least privilege' né modelli Zero Trust documentati.
Control ID 9.3: Gestione delle utenze - Note
Non esiste un processo strutturato e documentato di provisioning e deprovisioning delle utenze. La gestione è operativa ma priva di regolamentazione formale.
Raccomandazioni
• Formalizzare politiche di sicurezza specifiche per la protezione delle risorse umane • Definire e implementare procedure chiare per la gestione degli accessi basate sul principio del least privilege • Implementare un sistema strutturato di Identity Access Management (IAM) con processi di provisioning e deprovisioning documentati

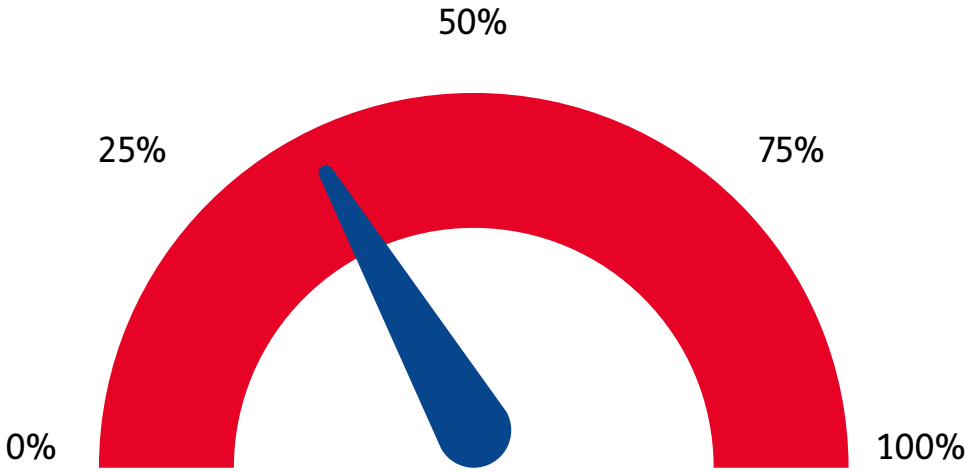
Control ID 10
Autenticazione

Control ID 10.1: Strong authentication - Note
Si riscontra l'implementazione dell'autenticazione a due fattori 2FA su posta elettronica e gestione operativa tramite i servizi di Office 365.
Control ID 10.2: Protezione dei canali di comunicazione
Si riscontra l'utilizzo di ESET PROTECT. Le farmacie interne utilizzano VPN mentre le affiliate non sono in VPN ma accedono solo tramite FTP protetto da IP protection. Stanno implementando un nuovo sistema per ricevere ordini tramite web service del quale ancora non si ha ancora conoscenza del sistema di protezione.
Raccomandazioni
• Estendere l'implementazione MFA a tutti i sistemi critici dell'organizzazione • Implementare una strategia documentata per la protezione end-to-end dei canali di comunicazione • Estendere l'utilizzo della VPN a tutte le farmacie della rete, incluse le affiliate

Gap Analysis NIS2

Risultati e remediation

RISULTATI



Alla luce delle analisi condotte, in conformità con la metodologia dettagliata nel presente documento, si rileva che FARMACIE ITALIANE SRL presenta un livello di adempimento insufficiente rispetto ai requisiti stabiliti dalla Direttiva (UE) 2022/2555 (Direttiva NIS2). L'indice di adempimento complessivo è pari al 35%, attestando, allo stato dell'arte, un'aderenza insufficiente alle prescrizioni.

Indice di adempimento
35%

REMEDIATION

Nella presente sezione sono illustrate le proposte di remediation, concepite per colmare le lacune evidenziate nella fase di analisi. Le azioni proposte derivano direttamente dalle raccomandazioni formulate in relazione ai diversi Control ID e sono finalizzate a rafforzare in maniera significativa la postura di sicurezza dell'organizzazione, promuovendo una gestione proattiva e integrata dei rischi cibernetici. Per ciascuna attività proposta, viene indicato il corrispondente Control ID (o i Control ID, qualora l'azione interessi più macroaree di controllo).

È di particolare rilevanza sottolineare che le attività evidenziate in verde nella tabella sottostante rappresentano interventi che saranno sviluppati nell'ambito della realizzazione del Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) conforme alla norma internazionale ISO/IEC 27001. L'implementazione di tale sistema costituisce lo step successivo dell'attività di Assessment e consentirà all'organizzazione di adottare un framework strutturato e riconosciuto a livello globale per la gestione della sicurezza delle informazioni.

Remediation	Controlli Associati
Formalizzare la nomina di Elisa Celletti come CISO; Implementare l'analisi del rischio strutturata con metodologia definita per il settore farmaceutico; Definire budget dedicato cybersecurity	ID 1
Creare e documentare un Incident Response Plan specifico per dati sanitari; Implementare sistema di ticketing; Definire procedura di notifica alle autorità entro i termini NIS2	ID 2
Estendere il modello Nesima a tutte le farmacie; Redigere Backup Policy aziendale; Implementare test periodici di ripristino	ID 3.1
Creare Disaster Recovery Plan completo; Definire RTO/RPO per sistemi critici; Effettuare test periodici di DR	ID 3.2
Formalizzare Crisis Management Team; Definire procedure di escalation; Organizzare simulazioni periodiche	ID 3.3
Implementare Supplier Security Policy; Inserire clausole cybersecurity nei contratti con fornitori; Controlli periodici su accessi remoti	ID 4
Formalizzare procedure acquisizione HW/SW sicura; Completare migrazione Windows 11; Pianificare migrazione da COBOL; Implementare politiche di hardening dei sistemi	ID 5.1, ID 5.2, ID 5.3
Implementare SIEM per monitoraggio centralizzato; Definire processo vulnerability management; Centralizzare logging	ID 5.4, ID 6
Formalizzare policy BYOD/clean desk; Strutturare e completare il piano di formazione cybersecurity già avviato con CyberGuru, estendendolo a tutto il personale della rete	ID 7.1, ID 7.2
Con priorità massima implementare crittografia dati in transito tra farmacie; Definire policy crittografia per dati sanitari; Valutare soluzioni temporanee pre-migrazione COBOL eventuale	ID 8
Formalizzare policy HR security; Implementare IAM con least privilege; Documentare provisioning/deprovisioning utenze	ID 9.1, ID 9.2, ID 9.3
Estendere MFA a tutti i sistemi critici; Implementare VPN per tutte le farmacie incluse affiliate; Proteggere comunicazioni end-to-end	ID 10.1, ID 10.2

Con tecnologie e servizi innovativi guidiamo la transizione digitale dell'Italia e del Brasile perché vogliamo contribuire ad accelerare la crescita sostenibile dell'economia e della società portando valore e benessere alle persone, alle aziende, alle istituzioni. Offriamo soluzioni diversificate che rispondono alle esigenze dei nostri interlocutori integrando anche obiettivi di climate strategy, economia circolare e crescita digitale. TIM offre agli individui e le famiglie servizi e prodotti di telefonia fissa e mobile per la comunicazione e l'intrattenimento, e accompagna le piccole e medie imprese verso la digitalizzazione con un portafoglio ritagliato sulle loro esigenze. Cloud, IoT e Cybersecurity sono al centro delle soluzioni End–to–End di TIM Enterprise per aziende e Pubblica Amministrazione, che realizzano la digital transformation del Paese avvalendosi della più grande rete di data center in Italia, delle competenze di società del Gruppo come Noovle, Olivetti e Telsy, e di partnership con gruppi di primaria importanza. Sviluppiamo infrastrutture di rete mobile 4G e 5G e la rete fissa in fibra a livello internazionale attraverso Sparkle.

Operando in sinergia con le altre factories del Gruppo TIM, Telsy offre servizi di Intelligence, soluzioni di sicurezza gestite (MSS), servizi erogati tramite il SOC aziendale e Cyber Professional Services mettendo a disposizione esperti, tecnologie e infrastrutture proprietarie per una sicurezza su misura dei clienti più esigenti. Telsy è sottoposta alla normativa Golden Power in qualità di società titolare di attività di rilevanza strategica per la difesa e la sicurezza nazionale. Per garantire la sicurezza di oggi bisogna anticipare le minacce di domani. Telsy lavora per sviluppare prodotti e soluzioni future-proof che siano di supporto alla protezione di dati e comunicazioni sensibili, contribuendo al rafforzamento della difesa nazionale e della sicurezza dei clienti business.

UESE ITALIA S.p.A. è leader nell'offerta di servizi di adeguamento normativo, di Consulenza e Formazione obbligatori per le Aziende pubbliche e private, affiancandole nel percorso di regolamentazione e del rispetto delle normative locali, regionali, nazionali ed europee. Aiutiamo le aziende a mantenere o aumentare la propria competitività sul mercato nei seguenti macro settori: Consulenza e formazione sicurezza ambienti di lavoro d.lgs. 81/08, al rispetto al Regolamento Europeo GDPR 679/2016 privacy, NIS2, trasformazione tecnologica industria 4.0, prevenzione crisi d'impresa nel rispetto del decreto 83/2022. Affianchiamo le aziende nel processo di certificazioni aziendali Internazionali ISO e di conformità CE di macchine, prodotti e medical device. Siamo professionisti ufficiali per la richiesta dell'attestazione SOA Argenta, Guardian Certification, IWZ International, IWZ Cert Srl e Certificato IWZ. Siamo advisor per start-up innovative supportandole nella trasformazione di un'idea di business in un'impresa di successo. UESE ITALIA è vicina allo sport con contributi reali a sostegno di realtà locali e nazionali. E' socia del Consorzio Treviso siamo noi.

TIMENTERPRISE	CONTATTI:	https://offerta.timenterprise.it/form?id=sdte060
Telsy A TIM ENTERPRISE BRAND	CONTATTI:	support-riskmanagement@telsy.com
UESE	CONTATTI:	info@uese.it


TIMENTERPRISE
Telsy
A TIM ENTERPRISE BRAND