2025
PRE-ASSESSMENT NIS2
REPORT DI IMPATTO

FARMACIE ITALIANE SRL

Data: 19/02/2025

TIMENTERPRISE Telsy A TIM ENTERPRISE BRAND

PRE-ASSESSMENT NIS2

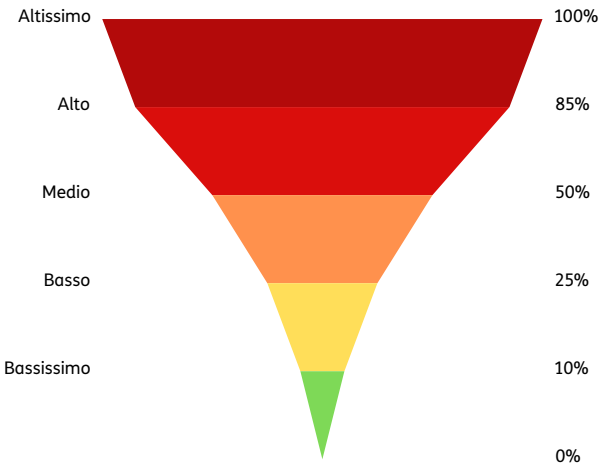
REPORT DI IMPATTO

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

Cliente: FARMACIE ITALIANE SRL

TIMENTERPRISE Telsy A TIM ENTERPRISE BRAND

NOTA PER GRAFICO (a destra): Verrà lasciata a colori solo l'area di riferimento Le altre aree verranno convertite in bianco e nero o toni di grigi.



Anagrafica dell'Organizzazione

Indirizzo sede legale:	Via San Protaso n.5, 20121 Milano (MI)
Soggetti intervenuti:	
Reparto Amministrativo:	Andrea Durante
Data intervista:	10/02/2025
Reparto IT:	Elisa Celletti
Data intervista:	27/01/2025
Reparto Risorse Umane:	Stefania Mirabelli
Data intervista:	10/02/2025
Data emissione report:	19/02/2025
Documento elaborato da:	Nicolò Serafini
Documento revisionato e approvato da:	Giuseppe Izzo
Titolo e funzioni:	Legale Rappresentante UESE ITALIA S.P.A.

SOMMARIO

RIFERIMENTI NORMATIVI

GDPR (Regolamento Generale sulla Protezione dei Dati)

- Titolo Ufficiale: Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali e alla libera circolazione di tali dati. Riferimento Normativo: OJ L 119, 4.5.2016, p. 1-88.
- Link al Testo: EUR-Lex - Regolamento (UE) 2016/679

Direttiva NIS 1 (Network and Information Systems Security Directive)

- Titolo Ufficiale: Direttiva (UE) 2016/1148 del Parlamento Europeo e del Consiglio, del 6 luglio 2016, relativa a misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione. Riferimento
- Normativo: OJ L 194, 19.7.2016, p. 1-30.
- Link al Testo: EUR-Lex - Direttiva (UE) 2016/1148

Direttiva NIS 2

- Titolo Ufficiale: Direttiva (UE) 2022/2555 del Parlamento Europeo e del Consiglio, del 14 dicembre 2022, relativa a misure per un livello comune elevato di sicurezza informatica nell'Unione (direttiva NIS 2).
- Riferimento Normativo: OJ L 333, 27.12.2022, p. 80-152.
- Link al Testo: EUR-Lex - Direttiva (UE) 2022/2555

D. Lgs. 138 del 04/09/2024

- Titolo Ufficiale: Recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148. Riferimento Normativo: (24G00155) (GU Serie Generale n.230 del 01-10-2024) Link al Testo: https://www.gazzettaufficiale.it/eli/id/2024/10/01/24G00155/SG

Codice Civile Italiano Articolo 2392 - Responsabilità degli amministratori

- Gli amministratori devono adempiere ai doveri imposti dalla legge e dallo statuto con la diligenza richiesta dalla natura dell'incarico e dalle loro specifiche competenze. In caso di inosservanza, sono solidalmente responsabili dei danni causati alla società, salvo prova di non aver concorso al fatto dannoso.

Articolo 2393 - Azione sociale di responsabilità

- L'azione sociale di responsabilità può essere promossa contro gli amministratori per chiedere il risarcimento dei danni arrecati alla società. Questa azione può essere esercitata anche dai soci che rappresentano almeno un ventesimo del capitale sociale.

Articolo 2394 - Responsabilità verso i creditori sociali

- Gli amministratori rispondono anche verso i creditori sociali quando il patrimonio della società risulta insufficiente per soddisfare i loro crediti, se il danno è stato causato dalla violazione dei doveri di conservazione dell'integrità del patrimonio sociale.

Articolo 2407 - Responsabilità dei sindaci

- Si estendono ai sindaci le disposizioni riguardanti la responsabilità degli amministratori, qualora essi non abbiano vigilato in modo adeguato sulle attività degli amministratori stessi.

Normativa Penale Gli amministratori possono anche incorrere in responsabilità penale nei seguenti casi:

Articolo 2621 - False comunicazioni sociali

- Sanziona l'amministratore che, con l'intento di ingannare i soci o il pubblico, espone fatti materiali non rispondenti al vero o omette informazioni in grado di alterare la rappresentazione della situazione economica, patrimoniale o finanziaria della società.

INTRODUZIONE ALLA NIS2

Definizione

La Direttiva NIS2, acronimo di "Network and Information Security Directive 2", rappresenta la seconda iterazione della normativa europea volta a rafforzare la resilienza informatica delle organizzazioni all'interno dell'Unione Europea (UE). Essa pone particolare enfasi sugli operatori delle infrastrutture critiche e dei servizi essenziali. Essendo una direttiva europea, NIS2 impone che ogni Stato membro recepisca e applichi le sue disposizioni entro il 17 ottobre 2024, rendendola così legalmente vincolante in tutti i paesi dell'Unione Europea.

Gli impegni degli Stati Nazionali

In primo luogo, gli Stati membri devono essere preparati a fronteggiare le minacce informatiche attraverso un'organizzazione ben formata e dotata di tutti i mezzi necessari per contrastare eventuali incidenti di sicurezza informatica. A tal fine, devono essere istituiti Team di Risposta agli Incidenti di Sicurezza Informatica (CSIRT), i quali saranno supportati da un'Autorità Nazionale dedicata alla sicurezza delle reti e dei sistemi informativi.

In tal senso, inoltre, la NIS2 sottolinea la necessità di una collaborazione tra gli Stati membri attraverso le rispettive organizzazioni nazionali e le Agenzie designate. Questa cooperazione è principalmente basata sullo scambio tempestivo e sicuro di informazioni critiche riguardanti le minacce e gli incidenti di sicurezza.

In secondo luogo, la Direttiva NIS2 pone l'accento sulla promozione e lo sviluppo di una cultura della cybersicurezza in settori critici precedentemente identificati, classificati secondo specifici livelli di rischio. Questi settori includono infrastrutture critiche che fanno uso di tecnologie dell'informazione e della comunicazione(TIC), e sono fondamentali per il funzionamento della società e dell'economia .

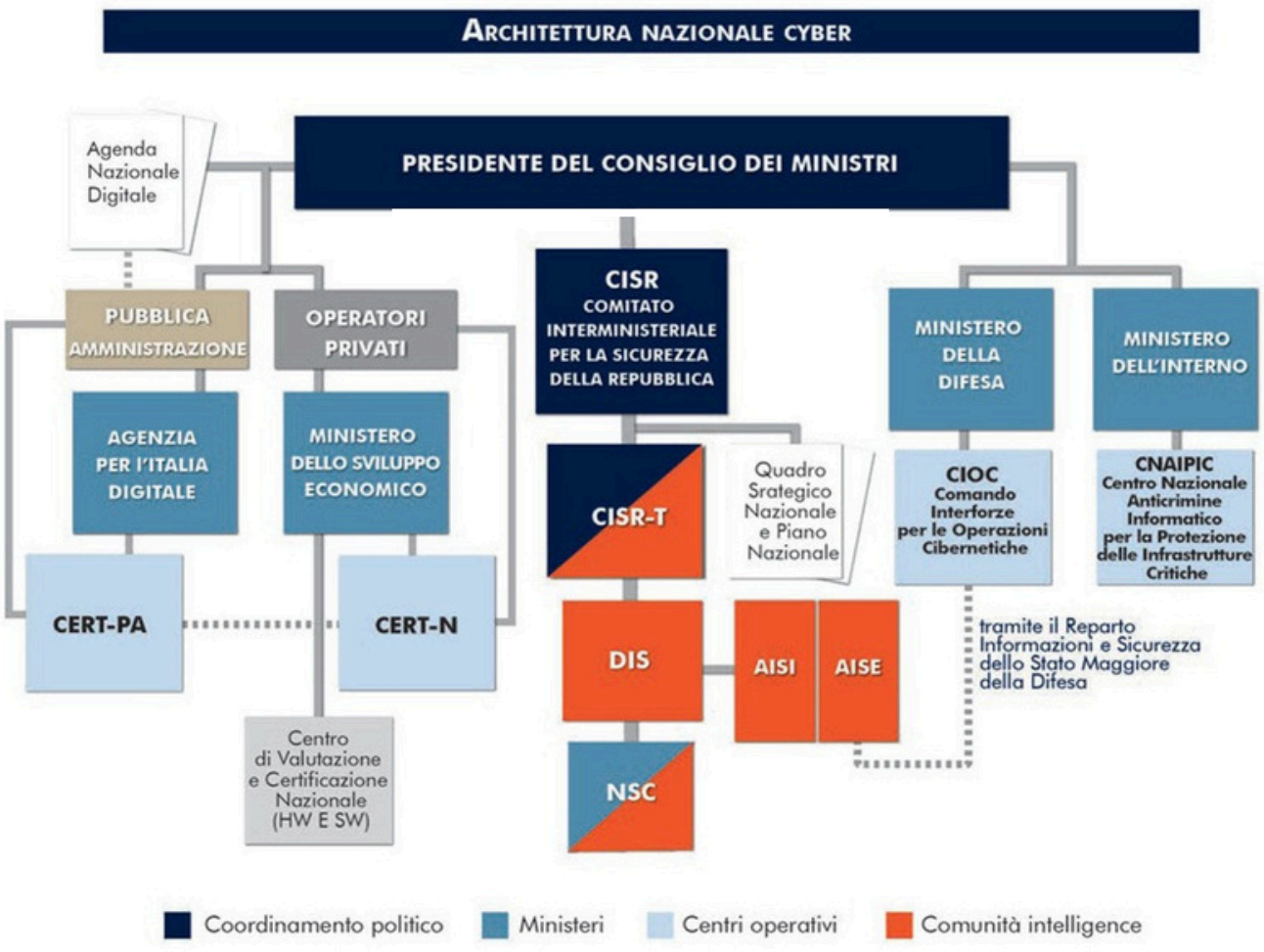
In Sintesi

La Direttiva mira a garantire che le entità operanti in questi settori siano dotate di adeguate misure di sicurezza, basate sulle migliori pratiche, sull'intelligence e sulle minacce, al fine di mitigare efficacemente i rischi.

COSA RENDE LA NIS2 COSÌ IMPORTANTE?

La Direttiva NIS2 riveste un'importanza cruciale nel panorama della sicurezza informatica europea, poiché introduce significativi vantaggi e obblighi perle organizzazioni. I principali benefici e impegni possono essere sintetizzati nei seguenti punti:

Ottimizzazione della gestione e mitigazione del rischio	T e m p i di risposta e recupero accettabili in caso di incidenti di sicurezza informatica	Monitoraggio e miglioramento continuo delle misure di sicurezza implementare a livello aziendale	Monitoraggio e rafforzamento della sicurezza in tutta la catena di fornitura (c.d. Supply chain)



IL RECEPIMENTO ITALIANO: D. Lgs. 138 del 04/09/24

Il contesto

L'Italia ha recepito la Direttiva NIS 2 mediante la formalizzazione del Decreto Legislativo n. 138 del 2024, vigente al 16/10/2024 che stabilisce le misure volte a garantire un livello elevato di sicurezza informatica su tutto il territorio nazionale. Il Decreto Legislativo 138/2024 introduce misure obbligatorie per la gestione dei rischi cibernetici in Italia, obbligando le aziende a implementare misure di sicurezza avanzate e a rispettare criteri specifici di cybersecurity, come formazione del personale e gestione della catena di approvvigionamento.

Le date importanti

Entro il 17 gennaio 2025 le aziende dovranno valutare se sono soggetti al D.lgs. che recepisce la Direttiva e registrarsi sulla piattaforma ACN.

Entro il 15 aprile 2025, ACN stabilirà se le aziende registrate sono effettivamente soggetti a cui si applica la NIS2.

Entro il primo gennaio 2026, le organizzazioni a cui si applica la NIS2 dovranno adeguarsi a quanto previsto dall'art. 25 in relazione alla notifica degli incidenti.

Entro ottobre 2026, le organizzazioni dovranno adeguarsi a quanto previsto dagli articoli 23 (obblighi degli organi di amministrazione e direttivi), 24 (gestione dei rischi e implementazione delle misure di sicurezza) e 29 (banca dati dei nomi a dominio).

L’ambito di applicazione

L’ambito di applicazione della normativa è definito dall’art. 3, che richiama gli Allegati I, II, III e IV del Decreto. Il D.lgs. 138/24 si applica nei confronti dei soggetti giuridici, pubblici o privati, indicati all’interno dei suddetti allegati e soggetti alla giurisdizione italiana, in quanto stabiliti sul territorio dello Stato. I suddetti Allegati hanno la funzione di definire i settori e le categorie di soggetti coinvolti negli obblighi di sicurezza informatica, dividendo le aree di rischio e i destinatari in categorie specifiche, con livelli di criticità variabili.

Allegato I - Settori Altamente Critici: identifica i settori considerati essenziali e particolarmente vulnerabili, per i quali l'interruzione dei servizi potrebbe avere impatti severi su scala nazionale o transfrontaliera. Tra questi settori ci sono le infrastrutture energetiche, il settore bancario e quello delle telecomunicazioni, e sono inclusi i soggetti finanziari regolati a livello europeo come le banche e le controparti centrali nei mercati finanziari. Questi soggetti devono garantire livelli di sicurezza elevati, superando standard minimi di protezione per evitare impatti su larga scala.

Allegato II - Settori Critici: riguarda altri settori importanti ma considerati meno vulnerabili rispetto a quelli dell'Allegato I. Qui rientrano settori come trasporti, sanità, distribuzione di acqua e rifiuti, e infrastrutture digitali. Anche in questo caso, sono previsti specifici requisiti di sicurezza per evitare rischi sistemici a servizi di importanza nazionale.

Allegato III - Categorie delle Pubbliche Amministrazioni: definisce le tipologie di pubbliche amministrazioni incluse nell'applicazione del decreto. In particolare, si considerano enti centrali, mentre le amministrazioni locali sono sottoposte al decreto solo se una valutazione dei rischi suggerisce un possibile impatto significativo in caso di interruzioni, basandosi su parametri come l'importanza dei servizi e la probabilità di incidenti.

Allegato IV - Altre Tipologie di Soggetti: include categorie non esplicitamente elencate nei precedenti allegati ma che, per motivi di natura strategica o rilevanza operativa (come operatori unici di servizi essenziali), sono soggette agli obblighi di sicurezza del decreto. L’obiettivo è garantire che soggetti di rilievo critico, come fornitori di servizi fiduciari o registri di domini internet, adottino misure di prevenzione per garantire la sicurezza dell'infrastruttura nazionale.

Ulteriori criteri applicativi

L'art. 3 del D. Lgs. 138/24 riporta ulteriori criteri applicativi di natura oggettiva ai fini dell'applicazione della nuova disciplina alle aziende. All'art. 3 comma 2 si precisa che il Decreto trova applicazione nei confronti dei soggetti menzionati dagli Allegati I e II, qualora questi ultimi superino le soglie dimensionali indicate al Paragrafo 2 dell'art. 2 dell'Allegato 1 alla Raccomandazione 361/2003/CE.

Il Decreto trova certa applicazione nei confronti dei soggetti operanti nei settori indicati dagli Allegati I e II che impieghino 50 o più dipendenti e abbiano un fatturato superiore ai 10 milioni di euro.

Ciò comporta una esenzione dalla disciplina in capo alle società che rientrino nella definizione di "piccola o media impresa" ai sensi dell'Allegato I alla Raccomandazione 361/2003/CE.

All'interno del comma 5 del suddetto Articolo, però, sono presenti espresse deroghe all'esonero sopra indicato, che prefigurano casi in cui il Decreto trova piena applicazione anche nei confronti delle PMI, in quanto prescindono da valutazioni di ordine dimensionale.

La distinzione tra "Soggetti essenziali" e "Soggetti importanti"

L'art. 6 del Decreto italiano introduce una distinzione definitiva tra i "Soggetti essenziali" ed i "Soggetti importanti".

Sono Soggetti Essenziali:

- tutti coloro che operano nei settori indicati all'Allegato I del D.lgs. 138/2024 (come sopra elencati) e che superino i massimali per le "medie imprese" secondo le soglie di 250 dipendenti impiegati e 50 milioni di fatturato o 43 milioni totali di bilancio; indipendentemente dalle loro dimensioni, gli enti
- identificati come soggetti critici ai sensi del Decreto Legislativo 134/2024 che recepisce la Direttiva (UE) 2022/2557; i fornitori di reti pubbliche di comunicazione elettronica e i fornitori di servizi di
- comunicazione elettronica accessibili al pubblico di cui all'articolo 3, comma 5, lettera b), che si considerano "medie imprese" ai sensi dell'articolo 2 dell'allegato alla raccomandazione 2003/361/CE; indipendentemente dalle loro dimensioni, i prestatori di servizi fiduciari qualificati e i gestori di registri
- dei nomi di dominio di primo livello, nonché i prestatori di servizi di sistema dei nomi di dominio di cui all'art. 3, comma 5, lettere c) e d); indipendentemente dalle loro dimensioni, le pubbliche amministrazioni centrali di cui all'Allegato III, comma 1, lettera a), ossia le amministrazioni centrali.

Sono Soggetti Importanti:

- tutti coloro che rientrano nell'ambito di applicazione definito dall'art. 3, ma che non soddisfano i requisiti di cui sopra per essere definiti "essenziali".

REQUISITI ED OBBLIGHI PER LE AZIENDE

La Direttiva NIS 2 e il D. Lgs. 138/24 introducono nuovi requisiti e obblighi per le organizzazioni in quattro aree principali:

Gestione del Rischio: le organizzazioni devono adottare misure per minimizzare i rischi informatici. Queste misure includono, ad esempio: la gestione degli incidenti, una maggiore sicurezza della catena di approvvigionamento, una migliore sicurezza di rete, un controllo degli accessi più efficace e la crittografia.

Responsabilità Aziendale: viene richiesto che la direzione aziendale supervisioni, approvi e sia formata e responsabile delle misure di cybersicurezza e affronti i rischi informatici. Le violazioni possono comportare sanzioni per la direzione e un potenziale divieto temporaneo di ricoprire ruoli dirigenziali.

Obblighi di Segnalazione: Le entità essenziali e importanti devono disporre di processi per la segnalazione tempestiva di incidenti di sicurezza con impatto significativo sulla fornitura del loro servizio o sui destinatari. Vengono stabilite scadenze specifiche per le notifiche: le aziende hanno 24 ore per presentare un allarme preventivo al CSIRT o all'autorità nazionale competente. La notifica ufficiale, inoltre, deve pervenire entro 72 ore dal verificarsi dell'incidente informatico.

Business Continuity: le aziende devono pianificare come intendono garantire la continuità aziendale in caso di gravi incidenti informatici. Questo piano dovrebbe includere considerazioni sul recupero dei sistemi, procedure di emergenza e la creazione di un team di risposta alle crisi.

Il servizio di Pre-Assessment NIS2

conforme al D. Lgs. 138/24

Le premesse

Questo pre-assessment si propone di analizzare in dettaglio il livello di conformità della Vostra azienda rispetto alle nuove norme di sicurezza informatica introdotte dalla direttiva NIS2 e recepite dal Decreto Legislativo 138/24. L'obiettivo è comprendere se e come vengano rispettate le disposizioni legislative, valutando sia i processi interni che le misure di sicurezza adottate per proteggere le infrastrutture critiche e i dati sensibili.

Durante il pre-assessment, sono esaminati diversi aspetti della gestione della sicurezza informatica: dai protocolli di risposta agli incidenti, alla protezione delle reti e dei sistemi, fino alla formazione del personale e alla gestione della catena di approvvigionamento. In questo modo, è possibile identificare eventuali lacune o punti di debolezza che potrebbero compromettere la resilienza aziendale in caso di cyber-attacchi.

Alla fine dell'analisi, il pre-assessment fornisce non solo una diagnosi dello stato attuale, ma anche una serie di suggerimenti e soluzioni personalizzate, studiate per aiutare l'azienda a migliorare il proprio livello di sicurezza e la capacità di rispondere a eventuali minacce informatiche. Questi interventi, che possono riguardare sia aggiornamenti tecnici sia il rafforzamento delle procedure operative, mirano a potenziare la resilienza informatica dell'azienda, allineandola ai requisiti della normativa e garantendo una maggiore protezione delle infrastrutture critiche.

Gli Obiettivi del Pre-Assessment

- Valutare il livello di conformità della vostra azienda alla direttiva NIS2 e al D. Lgs. 138/24. Identificare
- potenziali vulnerabilità e lacune nelle misure di sicurezza attualmente implementate. Fornire
- raccomandazioni dettagliate per migliorare la sicurezza delle informazioni e garantire la conformità normativa.

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.

LA METODOLOGIA ADOTTATA

Il pre-assessment è realizzato con un approccio metodologico strutturato, basato sull'analisi delle risposte raccolte tramite un form online specificamente progettato. Questo questionario, unito a quanto emerso durante le interviste sul campo, ci consente di ottenere informazioni standardizzate e dettagliate su diversi aspetti della sicurezza informatica aziendale, con l'obiettivo di fornire una valutazione del potenziale impatto della Direttiva NIS2 e del Decreto Legislativo 138/24 all'azienda.

Le principali aree esaminate sono:

- Informazioni Generali sull'Azienda: Raccolta dei dati principali sull'organizzazione, come dimensioni, settore di attività, infrastrutture digitali utilizzate, e ruolo aziendale all'interno della supply chain.
- Valutazione dei Rischi e delle Minacce: Valutazione della presenza di procedure di gestione del rischio informatico e di pratiche per identificare, monitorare e mitigare le minacce digitali.
- Misure di Sicurezza Attualmente Implementate: Raccolta di informazioni relative alla conformazione dell'infrastruttura IT dell'organizzazione e alle misure di sicurezza attualmente in atto.
- Raccomandazioni per i Miglioramenti Futuri: Vengono fornite raccomandazioni per rafforzare la sicurezza informatica dell'azienda. Queste raccomandazioni possono includere l'adozione di nuove tecnologie, l'aggiornamento delle procedure di risposta agli incidenti, e la formazione del personale per aumentare la consapevolezza sulle minacce digitali.

I risultati del Pre-Assessment NIS2

I dati riportati di seguito sono i risultati dell'analisi delle informazioni reperite in sede di intervista all'azienda dai tecnici di IWZ CERT SRL, veicolate attraverso un form digitale all'interno della piattaforma "Jotform" distribuita dall'azienda Jotform Inc.

Riepilogo

Informazioni Generali

- **Ragione sociale:** FARMACIE ITALIANE SRL
- **Partita IVA:** 10532530960
- **Indirizzo sede legale:** VIA SAN PROTRASO, 5, 20121, MILANO(MI)
- **Tipologia:** Privata
- **Forma giuridica:** Società a responsabilità limitata (S.r.l.)
- **Email:** elisa.celletti@gruppofarmacieitaliane.it
- **Numero di Telefono:** (+39) 3299077170
- **Dimensione azienda (dipendenti):** Tra 50 e 250
- **Fatturato annuo:** ≤ 10 milioni di euro
- **Totale di bilancio:** > 43 milioni di euro
- **Servizi/attività nell'UE:** Sì
- **Settori critici:** Sanitario

Informazioni specifiche

- **Reti di comunicazione elettroniche:** No
- **Fornitore di servizi di fiducia:** No
- **Gestione dei registri dei nomi di dominio:** No
- **Fornitore di servizi fiduciari non qualificati:** No
- **Fornitore di punti di interscambio internet:** No
- **Fornitore di servizi di cloud computing:** No
- **Fornitore di di servizi di data center o di di reti di distribuzione dei contenuti:** No
- **Ente della pubblica amministrazione centrale:** No
- **Ente della pubblica amministrazione a livello regionale:** No
- **Precedente identificazione come operatore di servizi essenziali (NIS):** Sì
- **Catena di fornitura di servizi critici:** No

- **Responsabile della sicurezza informatica (CISO):** No
- **Procedura documentata per la gestione degli incidenti di sicurezza informatica:** No
- **Valutazioni del rischio effettuate:** No

Eventuali Certificazioni

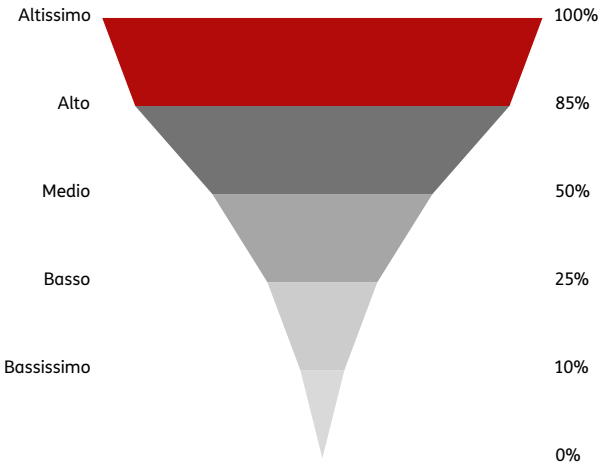
- **Certificazioni ISO:** Nessuna certificazione

Esclusioni

- **Attività legate alla sicurezza nazionale, pubblica sicurezza, difesa o forze dell'ordine:** No
- **Ente della Pubblica Amministrazione che svolge prevalentemente attività nei settori della sicurezza nazionale, della pubblica sicurezza, della difesa o delle forze dell'ordine:** No
- **Categorie esentate dal regolamento (UE) 2022/2554:** No

LIVELLO DI IMPATTO NIS2 atttribuito all'organizzazione

NOTA PER GRAFICO (a destra): Verrà lasciata a colori solo l'area di riferimento Le altre aree verranno convertite in bianco e nero o toni di grigi.



Risultati

Altissimo: Soggetto con impatto altamente critico

In base alle risposte fornite e alle informazioni raccolte, l'azienda:

- secondo quanto previsto dall'art. 3 del D. Lgs. 138/24 rientra tra i soggetti a cui essa è applicabile.
- secondo quanto previsto dall'art. 6 del D. Lgs. 138/24 è considerata un soggetto essenziale, afferente all'Allegato 1 del decreto stesso.

Pertanto, SI RENDE NECESSARIO intraprendere un percorso di allineamento alla Direttiva NIS2.

GLI IMPATTI SULL'AZIENDA

La Direttiva NIS2 segna un significativo potenziamento delle misure di sicurezza informatica, introducendo un approccio basato sul rischio ("Risk-Based") e una gestione più proattiva del monitoraggio e delle difese digitali. Questo approccio richiede alla Vostra azienda di non limitarsi a rispondere a incidenti una volta che si sono verificati, ma ad attuare una vigilanza costante sulle proprie infrastrutture IT, prevedendo e mitigando i rischi prima che si traducano in minacce concrete. Gli accessi alle reti devono essere strettamente controllati e regolati, e le procedure di risposta agli incidenti devono essere efficienti e chiare, così che possiate reagire in modo tempestivo a qualsiasi evento critico.

In Italia, con il recepimento del Decreto Legislativo 138/2024, vengono adattate e implementate le disposizioni europee alle peculiarità del contesto italiano, ampliando le categorie di soggetti e i settori considerati essenziali o importanti per la sicurezza nazionale. Il decreto stabilisce obblighi stringenti per le aziende, dai requisiti minimi di sicurezza fino alle sanzioni per chi non si adegua alle norme, con l'obiettivo di migliorare la resilienza digitale del Paese.

È stata introdotta una supervisione nazionale centralizzata tramite l'Agenzia per la Cybersicurezza Nazionale (ACN), responsabile della verifica della conformità, della registrazione dei soggetti essenziali e importanti, e del coordinamento delle risposte agli incidenti. Tra le sue funzioni principali vi sono l'aggiornamento annuale del registro delle infrastrutture critiche e il monitoraggio delle attività di mitigazione dei rischi da parte delle aziende.

OBBLIGHI DI NATURA AMMINISTRATIVA ART. 23 D. LGS. 138/24

L'art. 23 del Decreto Legislativo 138/2024 regola i doveri di carattere amministrativo che si impongono agli amministratori e ai dirigenti aziendali.

Secondo quanto stabilito dal comma I dell'art. 23, spettano agli organi direttivi e amministrativi dei soggetti essenziali o importanti i seguenti obblighi:

- approvare le modalità che l'azienda ha adottato per implementare le misure di gestione del rischio per la sicurezza informatica, come indicato nell'art. 24;
- supervisionare il processo di iscrizione alla piattaforma telematica, così come descritto;
- assumere la responsabilità in caso di violazioni delle disposizioni del Decreto 138/2024.

Inoltre, il comma II stabilisce che i medesimi organi siano anche responsabili di:

- frequentare corsi di formazione specifici in ambito di sicurezza informatica;
- incentivare una programmazione formativa periodica per i dipendenti in materia di cybersicurezza, tale da garantire loro competenze adeguate per riconoscere e valutare le pratiche di gestione dei rischi informatici e il loro impatto sui servizi offerti dall'ente.

Infine, il comma III prevede che l'organo amministrativo e direttivo sia informato prontamente, o con frequenza periodica a seconda della gravità, sugli incidenti informatici verificatisi all'interno dell'azienda.

È pertanto consigliabile che le aziende coinvolte dalla normativa istituiscano flussi informativi specifici per aggiornare puntualmente il vertice amministrativo riguardo ogni evento informatico che possa compromettere o ostacolare le normali attività operative dell'organizzazione interessata.

OBBLIGHI DI NATURA TECNICA
ART. 24 D. LGS. 138/24

L'articolo 24 stabilisce gli obblighi tecnici a carico dei soggetti essenziali e importanti, finalizzati all'implementazione di misure per la gestione e il contenimento dei rischi legati alla sicurezza informatica.
La norma prevede che i soggetti essenziali e importanti debbano adottare, entro i termini e secondo le modalità stabilite dal Decreto, misure tecniche, operative e organizzative che siano adeguate e proporzionate alla gestione dei rischi associati alla sicurezza dei sistemi informativi e delle reti utilizzati nell'ambito delle loro attività e nella fornitura dei servizi. Questo è volto a ridurre al minimo l'impatto di eventuali incidenti e il conseguente danno per i destinatari e fruitori di tali servizi.

Tali misure devono soddisfare specifici requisiti, in particolare:

- Garantire un livello di sicurezza dei sistemi informativi di rete adeguato ai rischi esistenti, considerando le conoscenze più aggiornate e lo stato dell'arte nel campo della sicurezza informatica. Quando possibile, si dovranno seguire gli standard previsti da normative nazionali, europee o internazionali, tenendo conto anche dei costi di attuazione. Si presume quindi che un risparmio ingiustificato legato a un investimento insufficiente nelle misure di sicurezza possa comportare la responsabilità del soggetto obbligato. L'investimento dovrà essere proporzionato alle risorse economiche del soggetto e al livello di rischio identificato, considerando il possibile impatto sui fruitori dei servizi. Le misure devono essere "proporzionate al grado di esposizione ai rischi del soggetto, alle dimensioni del soggetto e alla probabilità che si verifichino incidenti, nonché alla loro gravità, incluso il loro impatto sociale ed economico".

Il comma II definisce le caratteristiche minime che il sistema di prevenzione dei sistemi informativi deve avere, adottando un approccio multirischio. In particolare, le misure devono includere i seguenti elementi:

- Sviluppo di politiche per l'analisi dei rischi e la sicurezza dei sistemi informativi e di rete;
- Creazione di procedure interne per la gestione degli incidenti, con l'obiettivo di eseguire prontamente le notifiche di eventuali incidenti alle autorità competenti;
- Implementazione di procedure per garantire la continuità operativa, comprese la gestione dei backup, il ripristino in caso di disastro (disaster recovery), quando applicabile, e la gestione delle crisi;
- Verifica della sicurezza della catena di approvvigionamento, inclusi gli aspetti di sicurezza relativi ai rapporti tra ciascun soggetto e i suoi fornitori diretti o fornitori di servizi;
- Sicurezza nell'acquisizione, nello sviluppo e nella manutenzione dei sistemi informativi e di rete, comprensiva della gestione e della divulgazione delle vulnerabilità;
- Sviluppo di politiche e procedure interne per valutare periodicamente l'efficacia delle misure di gestione dei rischi per la sicurezza informatica, attraverso un sistema di audit interni;
- Implementazione di pratiche di formazione in materia di sicurezza informatica;
- Attuazione di politiche e procedure relative all'uso della crittografia e, se opportuno, della cifratura;
- Sviluppo di prassi per la sicurezza e l'affidabilità del personale, comprese politiche di controllo degli accessi e gestione dei beni e delle risorse;
- Utilizzo di soluzioni di autenticazione a più fattori o di autenticazione continua, comunicazioni vocali, video e testuali protette, e sistemi di comunicazione di emergenza protetti all'interno del soggetto, se opportuno.

Il Decreto stabilisce che, nel caso in cui il soggetto obbligato si accorga di non essere conforme all'adozione delle misure sopra menzionate, sarà tenuto ad adeguarsi e ad adottare, senza indugi, tutte le misure correttive necessarie.

OBBLIGHI DI SEGNALAZIONE
ART. 25 D. LGS. 138/24

L'articolo 25 stabilisce l'obbligo di notifica degli incidenti informatici, specificando che i soggetti essenziali e importanti devono comunicare tempestivamente al CSIRT Italia qualsiasi incidente che abbia un impatto significativo sulla fornitura dei loro servizi.

È importante notare che il Decreto offre una definizione chiara di "incidente", descrivendolo come "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".

Un incidente, come indicato al comma 4 del presente articolo, è considerato significativo se:

- ha causato o è in grado di causare una grave perturbazione operativa dei servizi o perdite finanziarie per il soggetto interessato; ha avuto ripercussioni o è idoneo a
- provocare ripercussioni su altre persone fisiche o giuridiche causando perdite materiali o immateriali considerevoli.

I soggetti interessati sono tenuti a inviare, come previsto dal comma 5 del presente Articolo, al CSIRT Italia le seguenti comunicazioni:

- Pre-notifica tempestiva: Entro 24 ore dalla scoperta di un incidente significativo. Questa comunicazione dovrebbe, se possibile, specificare se l'incidente potrebbe derivare da atti illegittimi o malevoli e se ha il potenziale per avere un impatto transfrontaliero. Notifica dettagliata: Entro 72 ore dalla scoperta
- dell'incidente significativo. I soggetti devono fornire una notifica che aggiorni le informazioni precedentemente trasmesse nella pre-notifica. Questa notifica deve includere una valutazione iniziale dell'incidente, evidenziando la sua gravità, l'impatto e, se disponibili, gli indicatori di compromissione. Relazione intermedia su richiesta: Qualora il CSIRT Italia lo richieda, è necessario presentare una relazione
- intermedia contenente aggiornamenti rilevanti sulla situazione. Relazione finale: Entro un mese dalla notifica dell'incidente. I soggetti devono trasmettere una relazione finale che includa:
-
    - Una descrizione dettagliata dell'incidente, comprensiva della gravità e dell'impatto. Il tipo di
    - minaccia o la causa originale (root cause) che ha probabilmente innescato l'incidente. Le
    - misure di attenuazione già adottate e quelle in corso. L'impatto transfrontaliero dell'incidente,
    - se noto.
- Aggiornamenti in caso di incidente in corso: Se l'incidente è ancora in corso al momento della trasmissione della relazione finale, è richiesto di fornire una relazione mensile sui progressi. Inoltre, è necessaria una relazione finale entro un mese dalla conclusione della gestione dell'incidente.

OBBLIGHI DI ELENCAZIONE
ART. 30 D. LGS. 138/24

L'articolo 30 stabilisce gli obblighi riguardanti l'elencazione, la caratterizzazione e la categorizzazione delle attività e dei servizi forniti dai soggetti essenziali e importanti.

In particolare, a partire dal 1° maggio fino al 30 giugno di ogni anno, e dopo aver ricevuto la prima comunicazione di cui all'articolo 7, comma 3, lettera a), questi soggetti sono tenuti a comunicare o aggiornare, attraverso la piattaforma digitale di cui all'articolo 7, comma 1, un elenco dettagliato delle proprie attività e dei servizi offerti. Questo elenco deve includere tutti gli elementi necessari per la loro caratterizzazione e per l'attribuzione di una categoria di rilevanza.

Dopo che l'azienda avrà effettuato la comunicazione richiesta, l'ACN avrà 90 giorni per fornire un riscontro ai soggetti essenziali e importanti, verificando la conformità di quanto comunicato rispetto alle modalità e ai criteri stabiliti.

Questo termine potrà essere prorogato una sola volta per ulteriori 60 giorni.

L'Autorità potrà richiedere integrazioni e chiarimenti all'ente riguardo alla comunicazione iniziale dell'elenco delle attività attraverso diversi poteri e facoltà, quali:

- monitoraggio, analisi e supporto ai soggetti essenziali e ai soggetti importanti (art. 35);
- svolgimento di verifiche e ispezioni (art. 36); adozione di misure di esecuzione (art. 37);
- irrogazione di sanzioni amministrative pecuniarie e accessorie (art. 38 e cfr. Par. 5).
-

SANZIONI DI NATURA AMMINISTRATIVA ART. 38 D. LGS. 138/24

Al comma 5 dell'art. 38, vengono affrontate le responsabilità delle persone fisiche che abbiano la rappresentanza degli enti soggetti alla disciplina del Decreto. La norma prevede che "qualsiasi persona fisica responsabile di un soggetto essenziale o che agisca in qualità di suo rappresentante legale con l'autorità di rappresentarlo, di prendere decisioni per suo conto o di esercitare un controllo sul soggetto stesso, assicura il rispetto delle disposizioni di cui al presente decreto. Tali persone fisiche possono essere ritenute responsabili dell'inadempimento in caso di violazione del presente Decreto da parte del soggetto di cui hanno rappresentanza". L'ACN potrà disporre l'applicazione della sanzione amministrativa accessoria della incapacità a svolgere funzioni dirigenziali all'interno del soggetto interessato, attraverso una sospensione temporanea che viene applicata fino a che il soggetto interessato non provveda a adottare le misure necessarie a porre rimedio alle carenze o a conformarsi alle diffide formulate dall'ACN stessa ai sensi all'articolo 37, commi 6 e 7.

Per le violazioni previste dal comma 8 dell'art. 38 (mancata osservanza degli artt. 23/24/25 o delle disposizioni all'art. 37 commi 3 e 4), vengono applicate, alle aziende private le seguenti sanzioni previste dal comma 9 dell'art. 38:

- per i soggetti essenziali, escluse le pubbliche amministrazioni, con sanzioni amministrative pecuniarie fino a un massimo di euro 10.000.000 o del 2% del totale del fatturato annuo; per i soggetti importanti,
- escluse le pubbliche amministrazioni, con sanzioni amministrative pecuniarie fino a un massimo di euro 7.000.000 o dell'1,4% del totale del fatturato annuo .

Le violazioni descritte dal comma 10 dell'art. 38, prevedono sanzioni amministrative fino a un massimo dello 0,1% del totale del fatturato annuo per i soggetti essenziali e dello 0,07% per i soggetti importanti, e sono le seguenti:

- mancata registrazione, comunicazione o aggiornamento delle informazioni presso la piattaforma telematica istituita dalle autorità competenti, come disciplinate ai sensi dell'articolo 7 del Decreto;
- inosservanza delle modalità stabilite dall'Autorità nazionale competente NIS per il corretto utilizzo della piattaforma telematica ai sensi dell'articolo 7;
- mancata comunicazione o aggiornamento dell'elenco delle attività e dei servizi nonché della loro categorizzazione ai sensi dell'articolo 30, comma 1;
- mancata implementazione o attuazione degli obblighi relativi all'uso di schemi di certificazione, alla banca dei dati di registrazione dei nomi di dominio nonché alle previsioni settoriali specifiche di cui agli articoli 27, 29 e 32, così come disciplinati ai sensi dell'articolo 31;
- mancata collaborazione con l'Autorità nazionale competente NIS nello svolgimento delle attività e nell'esercizio dei poteri di monitoraggio, controllo ed ispezione istituiti dal Decreto in capo alla medesima;
- mancata collaborazione con il CSIRT Italia.

Per i casi di reiterazione specifica della violazione è prevista l'applicazione della sanzione aumentata sino al doppio. Nei casi di reiterazione non specifica, invece, si applica la sanzione prevista per la violazione più grave aumentata sino al triplo.

Step successivi al Pre-Assessment NIS2

STEP SUCCESSIVI

1.Identificare - Valutare -Affrontare i propri Rischi:

Gli organi di gestione di entità essenziali e importanti devono adottare misure tecniche, operative e organizzative adeguate e proporzionate con un approccio onnicomprensivo per tutti i pericoli, in modo da gestire i rischi alla sicurezza dei sistemi informatici e di rete e dell'ambiente fisico. Tale valutazione viene supportata da una gap analysis a seguito del nostro Assessment NIS2 - D.Lgs. 138/24.

2.Valutare la propria postura di Sicurezza:

Una valutazione della sicurezza può aiutare ad identificare i punti deboli, come le password non gestite o gli account configurati in modo errato o inattivi, suscettibili di furto di credenziali.

3.Adottare misure per proteggere gli accessi privilegiati:

Gli attaccanti possono sfruttare gli account privilegiati per orchestrare gli attacchi, abbattere le infrastrutture critiche ed interrompere i servizi essenziali. La Direttiva NIS2 e il decreto italiano evidenziano la necessità, alle entità critiche, di limitare l'accesso agli account amministrativi e di ruotarne regolarmente le password.

4.Rafforzare le proprie difese anti-Ransomware:

Gli attaccanti possono sfruttare gli account privilegiati per orchestrare gli attacchi, abbattere le infrastrutture critiche ed interrompere i servizi essenziali. La Direttiva NIS2 e il decreto italiano evidenziano la necessità, alle entità critiche, di limitare l'accesso agli account amministrativi e di ruotarne regolarmente le password.

5.Passare ad un'Architettura Zero Trust:

Le architetture di sicurezza tradizionali basate sul perimetro di rete, concepite per difendere i confini della rete attendibile aziendale, non sono adatte al mondo dei servizi cloud e della forza lavoro ibrida. Adottare un approccio Zero Trust implementando diversi livelli di difesa come l'accesso con privilegio minimo, l'autenticazione continua e l'analisi delle minacce per convalidare tutti i tentativi di accesso, risulta fondamentale.

6.Monitorare la propria Supply Chain del Software:

Gli attacchi alla supply chain sono una delle principali preoccupazioni degli organi di regolamentazione dell'UE e una delle principali motivazioni alla base della Direttiva NIS2. Diventa importante dare un nuovo sguardo alla propria supply chain software e valutare l'implementazione di una soluzione digestione dei segreti per mitigare i rischi.

7.Formalizzare il proprio piano di risposta agli incidenti:

Il D.Lgs. 138/24 richiede una reportistica più rapida sugli incidenti, con una prima segnalazione da effettuare entro 24 ore dall'incidente stesso. È fondamentale verificare che la propria organizzazione sia preparata, riesaminando i processi di notifica degli eventi, raccolta di informazioni e reportistica.

8.Istruire il personale:

La formazione sulla cybersecurity e la cyber-igiene è obbligatoria secondo il D. Lgs. 138/24. Aumentare i propri sforzi per migliorare la consapevolezza informatica e promuovere una cultura incentrata sulla sicurezza.

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
UE
SE