Associazione Industriali Vicenza

WEBINAR GIOVEDÌ 7 MARZO 2024
11:30-12:30

“ Sicurezza e Conformità Normativa:
Navigare nel Labirinto Normativo dei nuovi Standard Europei ”

BV·TECH

AGENDA

- ✓ Panoramica delle principali normative europee in materia di sicurezza
- ✓ Analisi dei principali requisiti e obblighi per le aziende
- ✓ Strategie e best practice per la conformità normativa
- ✓ Casi ed esempi concreti
- ✓ Sessione di domande e risposte

Davide Gnesutta - Security and Compliance Senior Manager
ISO9001 LA, ISO27001 LA, ISO22301 LA, ISACA CISA, ITIL®, Master Privacy
davide.gnesutta@bvtech.com

Norme e Regolamenti - Introduzione

La differenza principale tra Direttive e Regolamenti Europei sta nella loro **applicabilità**:

Regolamenti:

- Sono atti **uniformi** e **auto-applicativi:** sono applicati **direttamente** in tutti gli Stati membri dal giorno della loro entrata in vigore.
- Hanno **obbligatorietà generale** in tutti i loro elementi.
- Prevalgono sulle leggi nazionali contrastanti.

Direttive:

- Sono atti **flessibili** che necessitano di una legge di **recepimento** nazionale
- Devono essere **recepite** da ciascun Stato membro entro un termine stabilito.
- Indicano un **obiettivo** da raggiungere, lasciando agli Stati la scelta dei mezzi per farlo.
- Possono essere impugnate dal Consiglio d'Europa se non recepite correttamente.

Norme e Regolamenti - Introduzione

Il percorso normativo europeo in materia di protezione dei dati e cybersicurezza (2000-2024)

2000-2010:

Carta dei Diritti Fondamentali dell'UE (Carta di Nizza del dicembre del 2000) da cui è derivato, per il tramite dell'Articolo 8 - Protezione dei dati di carattere personale, il Regolamento n. 2016/679 (GDPR).

2002: Direttiva 2002/58/CE sulla privacy e le comunicazioni elettroniche (ePrivacy): disciplina la privacy nel settore delle comunicazioni elettroniche; si concentra sulla conservazione dei dati, sulla fatturazione anonima, sullo SPAM e sulla gestione dei cookies.

2008: Pubblicata «decisione quadro» sulla lotta contro la criminalità informatica: armonizza le legislazioni nazionali in materia di reati informatici.

Norme e Regolamenti - Introduzione

Il percorso normativo europeo in materia di protezione dei dati e cybersicurezza (2000-2024)

2010-2020:

2016: Nuovo regolamento UE 2016/679 sulla protezione dei dati «**GDPR**»: sostituisce la Direttiva sulla protezione dei dati e rafforza la protezione dei dati personali in Europa.

2016: Direttiva UE 2016/1148 «**NIS**» - Direttiva sulla sicurezza delle reti e dei sistemi informativi per Operatori di Servizi Essenziali (OSE) e Fornitori di Servizi Digitali (FSD).

2019: Regolamento sulla sicurezza informatica **Cyber Security Act** (CSA): introduce un quadro europeo per la certificazione della sicurezza dei prodotti e dei servizi ICT[1].

2020: Proposta di Regolamento **Cyber Resilience Act** (CRA): stabilisce i requisiti di sicurezza per i prodotti dotati di elementi digitali ed immessi sul mercato europeo.

2020: Pubblicata la «***Strategia di Sicurezza Informatica dell'UE per il Decennio Digitale***»: contiene il piano d'azione per la resilienza cibernetica e delinea le azioni per rafforzare la resilienza dell'UE.

Norme e Regolamenti - Introduzione

Il percorso normativo europeo in materia di protezione dei dati e cybersicurezza (2000-2024)

2020-2024:

2022: Pubblicato Toolbox per la resilienza cibernetica: fornisce alle organizzazioni strumenti e risorse per migliorare la propria resilienza cibernetica (in particolare per le infrastrutture 5G).

2022: Regolamenti Digital Markets Act «**DMA**», che norma i mercati digitali e il Digital Services Act «**DSA**», il regolamento sui servizi digitali[1].

2022: Direttiva UE 2022/2555 «**NIS2**» - Direttiva sulle misure per un livello comune elevato di cybersicurezza nell'Unione; riprende la Direttiva NIS (che abroga), e introduce nuovi obblighi.

2022: Regolamento UE n.2022/2554 Digital Operational Resilience Act, «**DORA**»

2022: Direttiva UE 2022/2557 Critical Entity Resilience «**CER**» per l'identificazione e protezione delle infrastrutture critiche europee.

2023: Regolamento (UE) 2023/2854 **Data Act** che riguarda l'armonizzazione delle norme in materia di accesso equo ai dati e al loro utilizzo.

Norme e Regolamenti - Introduzione

Il percorso normativo europeo in materia di protezione dei dati e cybersicurezza (2000-2024)

2020-2024:

2024: Regolamento di esecuzione della **Commissione UE 2024/482** del 31/01/2024; specifica i ruoli, le norme e gli obblighi, nonché la struttura del sistema europeo di certificazione della cybersicurezza.

Norme e Regolamenti - Introduzione

La Commissione europea ha inoltre adottato una nuova strategia per la sicurezza cibernetica per il periodo 2023-2027, con l'obiettivo di rendere l'UE un leader globale nella sicurezza informatica e proteggere i cittadini europei dalle minacce informatiche.

La strategia si concentra su quattro pilastri:

1. ***Rafforzare la resilienza****: migliorare la capacità dell'UE di prevenire, rispondere e recuperare da incidenti informatici.*
2. ***Rafforzare le capacità di difesa****: sviluppare strumenti e tecnologie per proteggere le infrastrutture critiche e i cittadini europei.*
3. ***Promuovere la cooperazione****: rafforzare la collaborazione tra gli Stati membri e le diverse parti interessate in materia di sicurezza informatica.*
4. ***Promuovere la leadership globale****: affermare l'UE come leader globale nella sicurezza informatica.*

La strategia include anche una serie di azioni concrete, tra cui:

- Creare un centro europeo per la competenza in materia di sicurezza informatica.
- Investire in ricerca e sviluppo per la sicurezza informatica.
- Sviluppare un quadro europeo per la certificazione della sicurezza dei prodotti e dei servizi ICT (TIC).
- Rafforzare la cooperazione con i partner internazionali.

Norme e Regolamenti

Regolamento UE n. 2016/679 - Privacy

Il GDPR, entrato in vigore il 27 aprile 2016, è un regolamento dell'Unione Europea orientato alla protezione delle persone fisiche, e disciplina il trattamento dei loro dati personali e la loro privacy. Ha assunto piena efficacia (operativa e sanzionatoria) 25 maggio 2018. L'apparato sanzionatorio è rilevante[1].

Punti salienti:

- **Responsabilità del titolare del trattamento:** Il GDPR richiede ai titolari del trattamento di adottare misure tecniche e organizzative adeguate per proteggere i dati personali da violazioni e intrusioni, e piena responsabilità del Titolare[2].
- **Consenso:** Il GDPR richiede un consenso libero, specifico, informato e inequivocabile per il trattamento dei dati personali. Il consenso deve essere ottenuto PRIMA di raccogliere o utilizzare i dati personali.
- **Diritti degli interessati:** Il GDPR conferisce agli individui una serie di diritti sui propri dati personali, tra cui il diritto di accesso, rettifica, cancellazione (oblio), limitazione del trattamento, opposizione al trattamento e portabilità dei dati.
- **Trasferimenti di dati al di fuori dell'UE:** Il GDPR limita il trasferimento di dati personali al di fuori dell'Unione Europea a paesi che offrono un livello adeguato di protezione dei dati.

Punti critici:

- La complessità del regolamento che ha creato sfide per la sua applicazione.
- L'adeguamento al GDPR richiede un forte impegno in termini di tempo, risorse e competenze.

Norme e Regolamenti

Direttiva n. 2016/680 - Privacy delle Istituzioni

Protezione dei dati personali nell'ambito delle attività delle Istituzioni

Punti salienti:

- Disciplina il trattamento dei dati personali da parte delle autorità competenti ai fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali.
- Si applica a tutte le autorità competenti, comprese le forze dell'ordine, le autorità giudiziarie e le autorità di intelligence.
- Introduce nuovi diritti per gli interessati, come il diritto di accesso, di rettifica e di cancellazione dei dati.

Punti critici:

- La direttiva ha lasciato un certo margine di discrezionalità agli Stati membri nella sua attuazione.
- La complessità della direttiva ha reso difficile la sua applicazione coerente in tutti gli Stati membri.

Norme e Regolamenti

Regolamento UE n. 2018/1725 - Privacy Istituzioni e Organi UE

GDPR per le Istituzioni e Organi dell'UE: Proteggere i dati personali

Punti salienti:

- Disciplina il trattamento dei dati personali da parte delle Istituzioni e Organi dell'UE in modo conforme al GDPR (Regolamento Generale sulla Protezione dei Dati).
- Introduce nuovi diritti per gli interessati, come il diritto di accesso, di rettifica e di cancellazione dei dati trattati dalle istituzioni dell’Unione.
- Istituisce il Garante europeo della protezione dei dati (GEPD) per monitorare l'applicazione del regolamento.

Punti critici:

- La complessità del regolamento potrebbe creare sfide per la sua applicazione.
- La sua compatibilità con le legislazioni nazionali in materia di privacy potrebbe generare dubbi interpretativi.

Norme e Regolamenti

Regolamento UE n. 2023/2854 - Data Act

Adottata dal Consiglio europeo il 27 novembre 2023 e in vigore dal 11 gennaio 2024, è stata dotata di efficacia differita al 12 settembre 2025, e per una sezione, al 12 settembre 2027.

Punti salienti:

1. Diritto di accesso e riutilizzo dei dati: Le imprese e le persone hanno il diritto di accedere ai dati generati dai loro prodotti connessi all'IoT e di riutilizzarli a determinate condizioni.

2. Trasparenza e correttezza: Le imprese che forniscono prodotti e servizi connessi ai dati devono informare gli utenti in modo chiaro e comprensibile sulle modalità di raccolta, utilizzo e condivisione dei loro dati.

3. Interoperabilità e portabilità dei dati: I prodotti e servizi connessi all'IoT devono essere progettati per facilitare l'interoperabilità e la portabilità dei dati.

4. Accesso ai dati per enti pubblici in circostanze eccezionali: Gli enti pubblici possono accedere ai dati privati detenuti dal settore privato in circostanze eccezionali e per scopi di interesse pubblico, a determinate condizioni e con garanzie appropriate.

5. Governance dei dati: Il Data Act istituisce un nuovo organismo di governance per la supervisione dell'attuazione del regolamento e per la promozione della condivisione dei dati.

Norme e Regolamenti

Regolamento UE n. 2023/2854 - Data Act

Punti critici:

- **Complessità**: Il Data Act è un regolamento complesso che potrebbe essere difficile da applicare per le piccole e medie imprese.
- **Mancanza di armonizzazione con altre normative**: il Data Act non è completamente armonizzato con altre normative in materia di protezione dei dati, come il GDPR, il che potrebbe creare confusione e incertezza.
- **Rischi per la privacy**: alcune disposizioni del Data Act potrebbero essere considerate come un rischio per la privacy degli utenti, in particolare per quanto riguarda l'accesso ai dati da parte degli enti pubblici.
- **Costi di implementazione:** i costi di implementazione del Data Act potrebbero essere significativi per le imprese, in particolare per le piccole e medie imprese.
- **Efficacia**: non è chiaro se il Data Act sarà efficace nel raggiungere i suoi obiettivi, in particolare per quanto riguarda la promozione della condivisione dei dati.

Regolamenti UE n. 2022/2065 – Digital Services Act

Regolamento UE 2022/2065 sui servizi digitali: approvato il 5 luglio 2022 insieme al Digital Markets Act. I due provvedimenti compongono il **Digital Services Package**, che è diventato esecutivo nel 2023.

Punti salienti:

1. Combatte i contenuti illegali online: impone alle piattaforme online l'obbligo di agire contro contenuti illegali come discorsi di incitamento all'odio, terrorismo e materiale di abuso sessuale minorile.

2. Promuove la trasparenza della pubblicità: richiede alle piattaforme di rendere più trasparente la pubblicità online, identificando chiaramente chi sta pagando per gli annunci e il loro targeting.

3. Combatte la disinformazione: introduce misure per contrastare la diffusione di disinformazione online, come l'obbligo per le piattaforme di adottare codici di condotta per i fact-checker e di aumentare la trasparenza degli algoritmi di raccomandazione.

4. Protegge i diritti fondamentali degli utenti: stabilisce procedure più efficaci per gli utenti per segnalare contenuti illegali e ottenere il loro ritiro dalle piattaforme online.

Norme e Regolamenti

Regolamento UE n. 2022/1925 – Digital Markets Act «DMA»

Regolamento europeo sui mercati digitali: approvato il 5 luglio 2022 ed entrato in vigore ed è diventato esecutivo nel maggio 2023.

Punti salienti: i «gatekeeper» non potranno:

1. Promuovere eccessivamente i propri prodotti.
2. Imporre propri metodi di pagamento come unica possibilità di pagamento per i propri servizi.
3. Riutilizzare i dati personali raccolti per un servizio, ai fini di un altro servizio.
4. Preinstallare determinate applicazioni software.
5. Imporre limitazioni agli utenti.
6. Ricorrere a determinate pratiche di vendita aggregata.

Le imprese che non rispetteranno le prescrizioni del regolamento, saranno soggette ad ammende fino al 10% del loro fatturato mondiale.

Norme e Regolamenti

Regolamento UE n. 2019/881 - Cyber Security Act (CSA) – ENISA

Il Regolamento è stato recepito in GU il 7 giungo 2019 ed è entrato in vigore il 27 giugno 2019; crea un “quadro” per l’istituzione di schemi europei per la certificazione dei prodotti e servizi digitali.

Obiettivi:

- Rafforzare la sicurezza informatica in Europa.
- Promuovere la fiducia nei prodotti e servizi ICT.
- Migliorare la capacità dell'UE di rispondere alle minacce informatiche.

Misure principali:

- Creazione di un quadro europeo per la certificazione della sicurezza dei prodotti e servizi ICT.
- Istituzione di un Gruppo europeo per la certificazione della cybersicurezza (ECSG).
- Sviluppo di schemi di certificazione per diverse categorie di prodotti e servizi ICT.
- Designazione di organismi di valutazione della conformità per la verifica della conformità dei prodotti e servizi ICT agli schemi di certificazione.

Norme e Regolamenti

Regolamento UE n. 2019/881 - Cyber Security Act (CSA) - ENISA

Punti salienti:

- Istituisce formalmente l'ENISA (**E**uropean **N**etwork and **I**nformation **S**ecurity **A**gency) con poteri rafforzati.
- Assegna all'ENISA compiti di:
  - Coordinamento tra gli Stati membri.
  - Sviluppo di best practice.
  - Schemi di certificazione di prodotti e servizi di sicurezza informatica.
  - Gestione di campagne di sensibilizzazione.

Punti critici:

- Il successo dell'ENISA dipenderà dalla sua capacità di ottenere le risorse finanziarie e umane necessarie.
- La sua efficacia potrebbe essere limitata dalla mancanza di poteri coercitivi[1].

Norme e Regolamenti

Cyber Resilience Act (CRA) è una proposta di regolamento europeo che mira a rafforzare la sicurezza informatica dei prodotti digitali immessi sul mercato europeo. Infatti, è fondamentale garantire che qualunque dispositivo ‘intelligente’ e dotato di connessione alla rete”, sia sicuro da attacchi informatici. I regolamento dovrebbe entrare in vigore all'inizio del 2024. I fabbricanti dovranno applicare le norme 36 mesi dopo la loro entrata in vigore.

Il regolamento si applica a un'ampia gamma di prodotti, tra cui:

- **Hardware:** computer, smartphone, tablet, router, videocamere, i dispositivi IoT, etc.
- **Software:** sistemi operativi, applicazioni, firmware, etc.
- **Componenti e servizi ICT:** chip, schede madri, software di sicurezza, etc.

Obiettivi del Regolamento:

- ✓ Garantire che i prodotti digitali siano progettati e sviluppati con la sicurezza «by-design».
- ✓ Assicurare che i prodotti digitali siano resilienti alle minacce informatiche, tramite un quadro di sicurezza informatica coerente.
- ✓ Migliorare la trasparenza delle informazioni sulla sicurezza dei prodotti digitali.
- ✓ Promuovere la fiducia dei consumatori nei prodotti digitali, e di utilizzare prodotti con elementi digitali in modo sicuro.

Norme e Regolamenti

Cyber Resilience Act (CRA)

Il CRA prevede due classi di aggregazione che riflettono i diversi livelli di rischio associati a differenti tipi di prodotti hardware e software.

Classe I: la Classe I comprende prodotti a basso rischio, come ad esempio periferiche semplici o software di base; per questi prodotti i requisiti del CRA sono relativamente leggeri.

Classe II: la Classe II comprende prodotti ad alto rischio, come ad esempio sistemi industriali o software destinati ad essere impiegati su infrastrutture critiche; per questi prodotti, i requisiti del CRA sono più rigorosi.

La distinzione tra le due classi si basa su diversi fattori e metriche, tra cui (esempi):

- **L'impatto potenziale di un attacco:** se un prodotto viene compromesso, qual è il potenziale impatto sulla sicurezza informatica, sulla salute pubblica, sulla sicurezza economica o sul benessere sociale?
- **La dipendenza dal prodotto:** quanto è dipendente l'economia o la società da questo prodotto?
- **La complessità del prodotto:** quanto è complesso il prodotto e quanto è difficile da proteggere?

Cyber Resilience Act (CRA)

Classificazione dei dispositivi: Classe I

- Software per sistemi di gestione dell'identità e software per la gestione degli accessi privilegiati;
- Browser autonomi e incorporati;
- Gestori di password;
- Software che cerca, rimuove o mette in quarantena software dannoso;
- Prodotti con elementi digitali con funzione di rete privata virtuale (VPN);
- Sistemi di gestione della rete;
- Strumenti di gestione della configurazione di rete;
- Sistemi di monitoraggio del traffico di rete;
- Gestione delle risorse di rete;
- Sistemi di gestione delle informazioni e degli eventi di sicurezza (SIEM);
- Gestione aggiornamenti/patch, inclusi boot manager;
- Sistemi di gestione della configurazione delle applicazioni;
- Software di accesso/condivisione remota;
- Software per la gestione di dispositivi mobili;
- Interfacce di rete fisiche;
- Sistemi operativi non compresi nella classe II;
- Firewall, sistemi di rilevamento e/o prevenzione delle intrusioni non compresi nella classe II;
- Router, modem destinati alla connessione a Internet e switch, non compresi nella classe II;
- Microprocessori non compresi nella classe II;
- Microcontrollori;
- Circuiti integrati specifici per l'applicazione (ASIC) e array di porte programmabili sul campo (FPGA) destinati all'uso da parte di entità essenziali del tipo di cui all'[allegato I della direttiva XXX/XXXX (NIS2)];
- Sistemi di automazione e controllo industriale (IACS) non compresi nella classe II, come controllori logici programmabili (PLC), sistemi di controllo distribuito (DCS), controllori numerici computerizzati per macchine utensili (CNC) e sistemi di controllo di supervisione e acquisizione dati (SCADA);
- Internet delle cose (IoT) industriale non compreso nella classe II

Cyber Resilience Act (CRA)

Classificazione dei dispositivi: Classe II

- Sistemi operativi per server, desktop e dispositivi mobili;
- Hypervisor e sistemi runtime di contenitori che supportano l'esecuzione virtualizzata di sistemi operativi e ambienti simili;
- Infrastrutture a chiave pubblica ed emittenti di certificati digitali;
- Firewall, sistemi di rilevamento e/o prevenzione delle intrusioni destinati ad uso industriale;
- Microprocessori per uso generale;
- Microprocessori destinati all'integrazione in controllori logici programmabili ed elementi sicuri;
- Router, modem destinati alla connessione ad Internet e switch, destinati ad uso industriale;
- Elementi sicuri;
- Moduli di sicurezza hardware (HSM);
- Crittoprocessori sicuri;
- Smartcard, lettori di smartcard e gettoni;
- Sistemi di automazione e controllo industriale (IACS) destinati all'uso da parte di entità essenziali del tipo di cui all'[allegato I della direttiva XXX/XXXX (NIS2)], come controllori logici programmabili (PLC), sistemi di controllo distribuito (DCS) , controlli numerici computerizzati per macchine utensili (CNC) e sistemi di controllo di supervisione e acquisizione dati (SCADA);
- Dispositivi industriali dell'Internet delle cose (IoT) destinati all'uso da parte di entità essenziali, come previsto dall’allegato I della Direttiva 2022/2555 (NIS2);
- Componenti di rilevamento e attuazione di robot e controller di robot;
- Contatori intelligenti.

Norme e Regolamenti

Cyber Resilience Act (CRA)

Apparato sanzionatorio

Articolo 53, vari paragrafi:

3. L'inosservanza dei requisiti essenziali di cybersicurezza di cui all'allegato I e degli obblighi di cui agli articoli 10 e 11 è punita con sanzioni amministrative fino a **15.000.000 di euro** o, se l'autore del reato è un'impresa, **fino al 2,5% del fatturato totale annuo mondiale dell'anno finanziario precedente**, a seconda di quale sia il più elevato.

4. L'inosservanza di **qualsiasi altro** obbligo previsto dal presente regolamento è soggetta a sanzioni amministrative fino a **10 000 000 di euro** o, se l'autore del reato è un'impresa, **fino al 2% del suo fatturato annuo mondiale totale per l'esercizio finanziario precedente**, a seconda di quale dei due è più alto.

5. La fornitura di informazioni errate, incomplete o fuorvianti agli organismi notificati e alle autorità di vigilanza del mercato in risposta a una richiesta, è soggetta a sanzioni amministrative fino a **5 000 000 di euro** o, se l'autore del reato è un'impresa, **fino all'1% dell'importo totale fatturato annuo mondiale dell'anno finanziario precedente**, a seconda di quale sia il più elevato.

Norme e Regolamenti

Direttiva n. 2016/1148 – NIS

La Direttiva NIS (Direttiva 2016/1148 sulla sicurezza delle reti e dei sistemi informativi), è stata recepita nel nostro ordinamento attraverso il decreto legislativo **18 maggio 2018, n. 65** (anche detto “decreto legislativo NIS”), in vigore dal 24 giugno 2018.

Punti salienti:

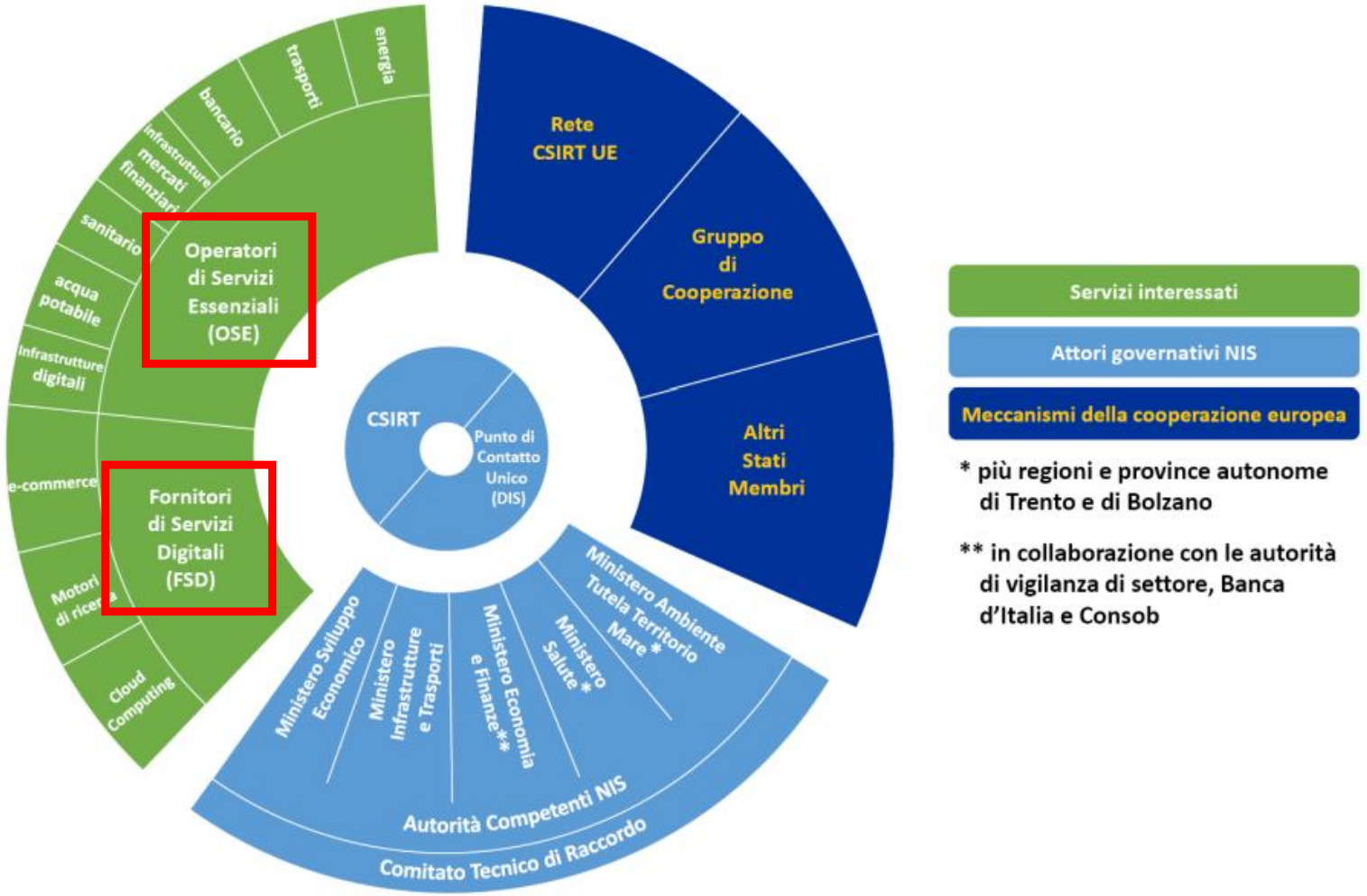
- Introduce misure per migliorare la sicurezza delle reti e dei sistemi informativi di operatori di servizi essenziali (OSE) e fornitori di servizi digitali (DSP).
- Prevede la designazione di autorità nazionali competenti per la sicurezza informatica.
- Stabilisce un quadro per la cooperazione tra gli Stati membri in materia di sicurezza informatica.

Punti critici:

- La direttiva non è vincolante per gli Stati membri, che possono scegliere di non applicarla in toto o in parte.
- La direttiva non è sufficientemente prescrittiva, lasciando ampia discrezionalità agli Stati membri nella sua implementazione.
- Nell’attuare la Direttiva NIS, il Governo ha optato per un approccio abbastanza soft, limitandosi per lo più ad incorporare nel decreto legislativo NIS quanto già stabilito dalla Direttiva.

Norme e Regolamenti

Direttiva NIS e ambiti di applicazione.



Norme e Regolamenti

Direttiva n. 2022/2555 - NIS2 - Rafforzare la sicurezza informatica in Europa

Al fine di rispondere alle nuove e crescenti minacce e rivedere la sua strategia di cybersicurezza, la Commissione EU ha ripreso la precedente normativa NIS, integrandola e sviluppandola, e a dicembre 2022 è stata formalizzata la Direttiva (UE) n.**2022/2555** del Parlamento Europeo e del Consiglio, del 14 dicembre 2022 «Network and Information Security» (di seguito, “Direttiva NIS 2” o più semplicemente «NIS2»).

Inoltre, la Direttiva NIS2 è stata introdotta in quanto:

- predominava uno stato di incertezza negli Stati membri circa l’adozione delle misure NIS;
- basso livello di resilienza delle imprese stabilite nella UE;
- sensibilità non omogenea nelle istituzioni dei Paesi membri, e concomitante recepimento diseguale nei vari settori;
- perimetro ristretto di settori individuati (restavano escluse alcune importanti infrastrutture);
- apparati sanzionatori troppo esigui rispetto al rischio e al potenziale impatto sui soggetti inadempienti.

Norme e Regolamenti

Direttiva n. 2022/2555 - NIS2 - Rafforzare la sicurezza informatica in Europa

Punti salienti: A far data dal 17 ottobre 2024 sostituisce la Direttiva NIS, rafforzando in modo significativo le misure di sicurezza per OSE e FSD (ora individuati come soggetti ESSENZIALI e IMPORTANTI).

- Introduce nuovi obblighi per i soggetti essenziali e importanti, tra cui:
  - Due diligence sulla sicurezza informatica.
  - Gestione degli incidenti di sicurezza.
  - Test di penetrazione e piani di risposta.
  - Applicazione di misure di sicurezza adeguate.
- Istituisce reti e gruppi di cooperazione europei per la sicurezza informatica (CSIRT e EU-CyCLONe) per:
  - Facilitare la cooperazione tra gli Stati membri, e sostenere la gestione coordinata a livello operativo degli incidenti e delle crisi di cybersicurezza su vasta scala;
  - Garantire il regolare scambio di informazioni pertinenti tra gli Stati membri e promuovere lo sviluppo di best practice.

Punti critici:

- Deve essere adottata mediante legge di recepimento **entro il 17 ottobre 2024**.
- La complessità potrebbe creare sfide per l'attuazione da parte dei soggetti ESSENZIALI e IMPORTANTI.

Norme e Regolamenti

Direttiva n. 2022/2555 - NIS2 - Rafforzare la sicurezza informatica in Europa

Compiti e requisiti tecnici dei CSIRT «Computer Security Incident Response Team»:

- ogni Stato membro designa o istituisce uno o più organismi CSIRT;
- è possibile designare o istituire i CSIRT all'interno di un'autorità competente (es. ACN);
- i CSIRT cooperano e scambiano informazioni con comunità settoriali ed intrasettoriali[1];
- garantiscono l'affidabilità e la sicurezza dei canali di comunicazione e la riservatezza delle informazioni;
- monitorano e analizzano le minacce informatiche, le vulnerabilità e gli incidenti a livello nazionale;
- forniscono assistenza ai soggetti essenziali e importanti interessati per quanto riguarda il monitoraggio in tempo reale o prossimo al reale dei loro sistemi informatici e di rete;
- forniscono una risposta agli incidenti e forniscono assistenza ai soggetti essenziali e importanti interessati;
- raccolgono e analizzano dati forensi e forniscono un'analisi dinamica dei rischi e degli incidenti;
- effettuano, su richiesta di un soggetto essenziale o importante, una scansione proattiva dei sistemi informatici e di rete del soggetto interessato;
- **possono effettuare, <u>in autonomia</u>, una scansione proattiva dei sistemi informatici e di rete del soggetto interessato, proattiva e non intrusiva, per individuare sistemi vulnerabili[2];**
- fungono da intermediari tra il soggetto segnalante una vulnerabilità ed il fornitore di prodotti o servizi TIC.

Norme e Regolamenti

Direttiva n. 2022/2555 - NIS2 - Rafforzare la sicurezza informatica in Europa

E’ stato ridefinito il campo di applicazione, individuando i soggetti ESSENZIALI e IMPORTANTI:

Tra i settori critici **essenziali** rientrano il settore energetico produzione e distribuzione (elettrico, oli and gas, riscaldamento, idrogeno etc.), dei trasporti (aereo, nautico, ferroviario, stradale), sanitario (produttori dispositivi medicali, laboratori R&D, farmaceutico), acque ed acque reflue; infrastrutture digitali; settore spaziale; pubblica amministrazione; settore bancario.

Tra i settori critici **importanti**, rientrano i servizi postali e delle spedizioni, la gestione e il trattamento dei rifiuti, la produzione e la distribuzione dei prodotti chimici, il settore dell’industria alimentare, le industrie tecnologiche ed ingegneristiche, i servizi di data center e DNS, la ricerca scientifica.

Inoltre la direttiva NIS2 **include non solo gli operatori privati dei settori ritenuti “essenziali”** dall’Unione europea (quelli dell’energia, dei trasporti, delle banche, delle infrastrutture dei mercati finanziari, dell’acqua potabile, della sanità e delle infrastrutture digitali) **ma altresì i fornitori di servizi digitali** (che forniscono servizi on-line di e-commerce; motori di ricerca; cloud computing; social media; gestione dei servizi ICT per i settori della pubblica amministrazione e per l’aerospazio).

Norme e Regolamenti

Direttiva n. 2022/2555 - NIS2 - Rafforzare la sicurezza informatica in Europa

Sono stati individuati nello specifico i soggetti ESSENZIALI e IMPORTANTI[1]:

a) i soggetti ESSENZIALI sono tutte le imprese, categorizzate all'allegato I, **ma che superano le 250 persone**, il cui **fatturato annuo supera i 50 milioni di EUR** oppure **il cui totale di bilancio annuo supera i 43 milioni di EUR**.
b) prestatori di servizi fiduciari qualificati e registri dei nomi di dominio di primo livello, nonché prestatori di servizi DNS, indipendentemente dalle loro dimensioni;
c) fornitori di reti pubbliche di comunicazione elettronica o di servizi di comunicazione elettronica accessibili al pubblico che si considerano medie imprese ai sensi dell'articolo 2, dell'allegato alla Raccomandazione 2003/361/CE;
d) i soggetti della pubblica amministrazione di cui all'articolo 2, paragrafo 2, lettera f), punto i);[2]
e) qualsiasi altro soggetto di cui all'allegato I o II che uno Stato membro identifica come soggetti critici
f) soggetti identificati come soggetti critici ai sensi della direttiva (UE) 2022/2557 (CER), di cui all'articolo 2, paragrafo 3 della presente direttiva;
g) se lo Stato membro lo prevede, i soggetti che tale Stato membro ha identificato prima del 16 gennaio 2023 come operatori di servizi essenziali

NOTA: *la norma si applica a tutti i soggetti individuati dalla Direttiva 2022/2557 (CER),* ***indipendentemente dalla loro dimensione economica.***

Norme e Regolamenti

Direttiva n. 2022/2555 - NIS2 - Rafforzare la sicurezza informatica in Europa

E’ stato ridefinito il campo di applicazione, individuando i soggetti ESSENZIALI e IMPORTANTI[1]:

a) **i soggetti IMPORTANTI sono tutte le imprese, categorizzate all'allegato I, ma che NON sono considerati soggetti essenziali per l’Art. 3 «Soggetti essenziali e importanti».**

Ciò comprende nei soggetti IMPORTANTI tutti i soggetti identificati dagli Stati membri come soggetti importanti ai sensi dell'articolo 2, paragrafo 2, lettere da b) a e), e cioè:

b) il soggetto sia l'unico fornitore in uno Stato membro di un servizio che è essenziale per il mantenimento di attività sociali o economiche fondamentali;

c) una perturbazione del servizio fornito dal soggetto potrebbe avere un impatto significativo sulla sicurezza pubblica, l'incolumità pubblica o la salute pubblica;

d) una perturbazione del servizio fornito dal soggetto potrebbe comportare un rischio sistemico significativo, in particolare per i settori nei quali tale perturbazione potrebbe avere un impatto transfrontaliero;

e) il soggetto sia critico in ragione della sua particolare importanza a livello nazionale regionale per quel particolare settore o tipo di servizio o per altri settori indipendenti nello Stato membro.

Norme e Regolamenti

Direttiva n. 2022/2555 - NIS2 - Rafforzare la sicurezza informatica in Europa

Per estensione normativa, la NIS2 si applica a tutti i soggetti privati che costituiscono la filiera di approvvigionamento dei soggetti ESSENZIALI e IMPORTANTI, generando così un “effetto domino” lungo tutta la filiera, che impatta anche sulle piccole e medie imprese.

Di conseguenza**, tutti i fornitori in filiera** potrebbero trovarsi ad essere obbligati a conformarsi alla nuova Direttiva sulla sicurezza delle reti e dei sistemi informatici, **pena l’esclusione dalla filiera di fornitura**.

I soggetti già vincolati dalla Direttiva NIS (e ora NIS2), sono chiamati a valutare la gestione dei rischi da parte dei loro fornitori, lungo tutta la filiera, rivalutando sistemi e reportistica periodica in materia di sicurezza informatica.

Norme e Regolamenti

Direttiva n. 2022/2555 - NIS2 - Rafforzare la sicurezza informatica in Europa

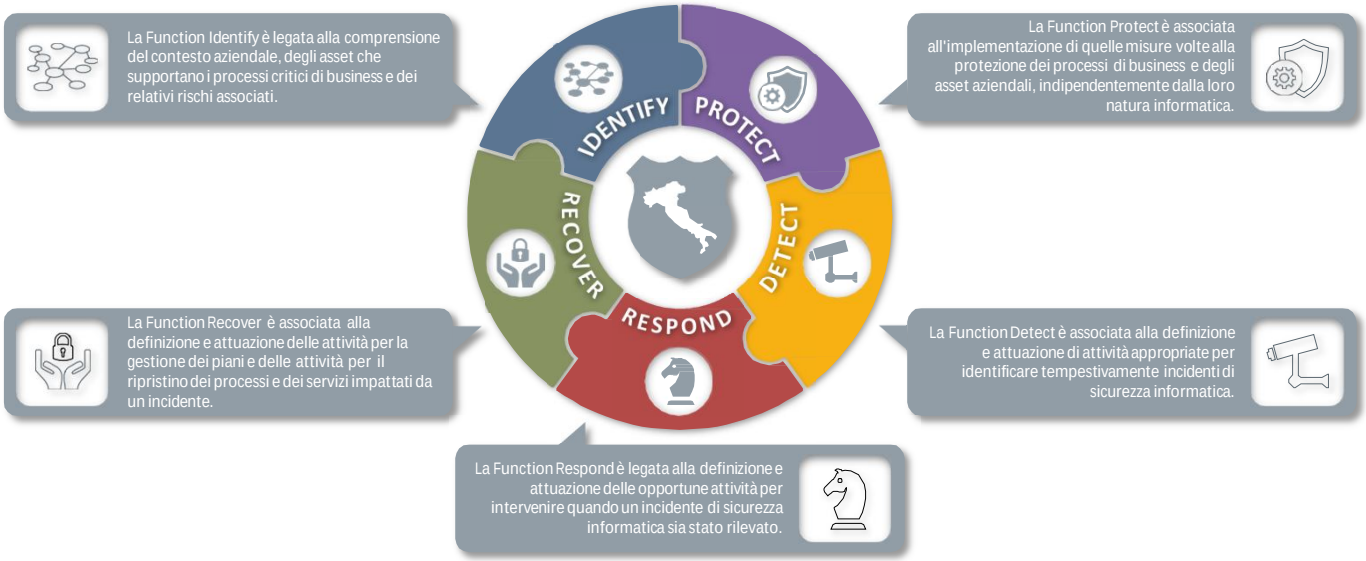
La NIS2, prevedendo un approccio di gestione del rischio olistico lungo tutta la filiera di approvvigionamento, impone ai soggetti ESSENZIALI e IMPORTANTI di **adottare una complessa attività di valutazione, gestione e mitigazione del rischio informatico** mediante misure tecniche, operative e organizzative adeguate e proporzionate, riassunte nei seguenti punti:

1. Definizione del perimetro, asset management (fisico e logico) e reportistica
2. Analisi dei rischi e della sicurezza dei sistemi (**analisi coordinata e multirischio**)
3. Gestione degli incidenti (Incident Management), e loro segnalazioni alle autorità competenti
4. Continuità Operativa (Piani di continuità operativa)
5. Sicurezza della catena di approvvigionamento, con audit attivi (propri o tramite terze parti) sui fornitori
6. Sicurezza delle manutenzioni dei servizi, compresa la gestione delle vulnerabilità
7. Politiche e procedure per valutare l'efficacia delle misure di protezione
8. Utilizzo di crittografia e cifratura
9. Sicurezza e controlli fisici e gestione opportuna delle risorse umane
10. Utilizzo di metodi di autenticazione a più fattori

Norme e Regolamenti

Direttiva n. 2022/2555 - NIS2 - Rafforzare la sicurezza informatica in Europa

Il Comitato che riunisce le Autorità NIS ha condiviso l'opportunità di utilizzare il **Framework Nazionale di Cyber Security** (abbreviato in FNSC) come base di riferimento per l'adeguamento al D.Lgs. 65/2018 (NIS) e NIS2.



Norme e Regolamenti

Direttiva n. 2022/2555 - NIS2 - Rafforzare la sicurezza informatica in Europa

Tutti i soggetti essenziali o importanti hanno l'obbligo di segnalare – senza indebito ritardo – tutti gli incidenti relativi alla cybersicurezza (sia fisica che logica), seguendo le tempistiche:

- Entro 24 ore, pre-allarme al CSIRT di incidente significativo
- Entro le 72 ore dalla scoperta, segnalazione completa al CSIRT

Inoltre, si rende necessario fornire:

- Supporto alle autorità per le investigazioni del caso
- Eventuale segnalazione dell'incidente a tutti gli interessati o potenzialmente interessati
- Entro un mese dalla scoperta, una relazione finale con dettagliata descrizione dell'incidente

Nota: *i prestatori di servizi fiduciari sono tenuti a notificare l'incidente completo entro 24 ore.*

Norme e Regolamenti

Direttiva n. 2022/2555 - NIS2 - Rafforzare la sicurezza informatica in Europa

Perimetri di applicabilità,
settori e sottosettori:

Settore	*SottoSettore*
1. Energia	Energia Elettrica
	Teleriscaldamento o Teleraffrescamento
	Petrolio
	Gas
	Idrogeno
2. Trasporti	Trasporto Aereo
	Trasporto Ferroviario
	Trasporto per via d'acqua
	Trasporto su strada
3. Settore Bancario	(Enti creditizi quali definiti all'articolo 4, punto 1), del regolamento (UE) n. 575/2013)
4. Infrastrutture dei mercati finanziari	
5. Settore Sanitario (prestatori di assistenza sanitaria e laboratori)	
6. Acqua Potabile	
7. Acque Reflue	
8. Infrastrutture Digitali (fornitori di servizi DNS, Cloud, Datacenter, nIX Internet)	
9. Gestione dei servizi TIC (B2B - Fornitori di servizi TIC gestiti e di servizi di sicurezza gestiti)	
10. Pubbliche Amministrazioni	
11. Spazio	

Norme e Regolamenti

Direttiva n. 2022/2555 - NIS2 - Rafforzare la sicurezza informatica in Europa

Sanzioni in capo ai soggetti obbligati: sono previste, laddove si rilevino violazioni all'**Art. 21** (Misure di gestione dei rischi di cybersicurezza) e **Art. 23** (Obblighi di segnalazione):

- Soggetti ESSENZIALI: sanzioni pecuniarie amministrative pari a un massimo di almeno **10.000.000 EUR** o a un massimo di **almeno il 2% del totale del fatturato mondiale annuo** per l'esercizio precedente.
- Soggetti IMPORTANTI: sanzioni pecuniarie amministrative pari a un massimo di almeno **7.000.000 EUR** o a un massimo di **almeno l'1,4% del totale del fatturato mondiale annuo** per l'esercizio precedente.

Nota1: gli stati membri possono prevedere delle **penalità di mora** al fine di imporre a un soggetto ESSENZIALE o IMPORTANTE di cessare la violazione della direttiva.

Nota2: se il soggetto viene sanzionato in pecunia per il GDPR, allora non può essere sanzionato in pecunia per la NIS2, però - in base alla NIS2 - al soggetto può essere imposto di applicare le misure di esecuzione in base all'art. 32 NIS2 (esecuzione coatta delle misure di mitigazione del rischio).

Norme e Regolamenti

Direttiva n. 2022/2557 – CER - Resilienza fisica per le entità critiche

La Direttiva (UE) 2022/2557 firmata il 14 dicembre 2022 rafforza la resilienza fisica dei soggetti critici (imprese e organizzazioni) che forniscono servizi essenziali (energia, trasporti, sanità...) contro le minacce, sia naturali che umane.

In vigore dal gennaio 2023, deve essere adottata mediante legge di recepimento **entro il 17 ottobre 2024**.

Punti salienti:

- Introduce misure per la gestione del rischio di perturbazioni fisiche per le «entità critiche» (es. fornitori di servizi sanitari, energia, trasporti), che devono essere individuati entro il 17 luglio 2026 e comunicati alle Autorità comp.
- Deve essere attuata in modo coordinato con la NIS2 e ne amplia l'ambito di applicazione alle infrastrutture fisiche.
- Stabilisce un quadro per la notifica e la gestione delle perturbazioni informatiche.

Punti critici:

- Entro il **17 gennaio 2026** ogni stato deve adottare una strategia per rafforzare la resilienza delle «entità critiche»
- La sua relazione con la Direttiva NIS2 richiama la coerenza applicativa dei controlli della NIS2.
- Il suo successo dipenderà dalla capacità degli Stati membri di identificare le entità critiche e di applicare le misure correttamente.

Norme e Regolamenti

Direttiva n. 2022/2557 – CER - Resilienza informatica per le entità critiche

Attività di mitigazione per i soggetti obbligati, nell'attesa di pubblicazione di RTS specifici:

- Evitare il verificarsi di incidenti o catastrofi, soprattutto causati da cambiamenti climatici.
- In base alle risultanze del risk assessment, assicurare un'adeguata protezione fisica alle infrastrutture
- Predisporre piani di resilenza, pronti a scattare senza preavviso, per contrastare e resistere agli impatti
- Predisporre piani di risposta efficienti per ripristinare le proprie capacità operative
- Predisporre processi e procedure per mitigare gli impatti nella filiera di fornitura, anche mediante la predisposizione di catene di approvvigionamento alternative.
- Procedere fin da subito con la predisposizione di percorsi formativi verticali.
- Assicurare la disponibilità del personale, soprattutto di quello individuato come critico dal risk assessment, in particolare, per coloro che rivestono ruoli sensibili all'interno del soggetto critico o a vantaggio di quest'ultimo.
- Predisporre adeguati processi di gestione e comunicazione degli incidenti; i tempi di notifica prevedono una notifica iniziale **entro le 24 ore**, seguita da una relazione finale dettagliata al più tardi dopo un mese.

Norme e Regolamenti

Direttiva n. 2022/2557 – CER - Resilienza informatica per le entità critiche

Il soggetto critico è autorizzato, in casi debitamente motivati e tenendo conto della valutazione del rischio dello Stato membro, a presentare richieste di controlli dei precedenti personali in particolare, per:

- coloro che rivestono ruoli sensibili all'interno del soggetto critico o a vantaggio di quest'ultimo
- coloro che sono autorizzati ad accedere — direttamente o a distanza — ai suoi siti e ai suoi sistemi informatici o di controllo,
- coloro che sono presi in considerazione per l'assunzione in ruoli che rientrano nei criteri precedenti

devono essere condotte attività di (come misure minime):

a) conferma l'identità della persona che è soggetta al controllo dei precedenti personali;

b) verifica dei **precedenti penali** di tale persona per quanto riguarda reati rilevanti ai fini di uno specifico ruolo.

Ci si può avvalere del sistema europeo di informazione sui casellari giudiziali; controlli dei precedenti personali sono proporzionati e strettamente limitati a quanto necessario e sono effettuati al solo scopo di valutare un potenziale rischio per la sicurezza.

Norme e Regolamenti

Direttiva n. 2022/2557 – CER - Resilienza informatica per le entità critiche

Perimetri di applicabilità, settori e sottosettori:

Settore	*SottoSettore*
1. Energia	Energia Elettrica Teleriscaldamento o Teleraffrescamento Petrolio Gas Idrogeno
2. Trasporti	Trasporto Aereo Trasporto Ferroviario Trasporto per via d'acqua Trasporto su strada Trasporto Pubblico
3. Settore Bancario	(Enti creditizi quali definiti all'articolo 4, punto 1), del regolamento (UE) n. 575/2013)
4. Infrastrutture dei mercati finanziari	
5. Salute (prestatori di assistenza sanitaria e laboratori)	
6. Acqua Potabile	
7. Acque Reflue	
8. Infrastrutture Digitali (fornitori di servizi DNS, Cloud, Datacenter, nIX Internet)	
9. Enti Pubblica Amministrazione	
10 Spazio	
11. Produzione, trasformazione e distribuzione di alimenti	

Norme e Regolamenti

Regolamento UE n. 2022/2554 – DORA - Resilienza digitale per il settore finanziario (#001)

Il Regolamento DORA è stato pubblicato 27 dicembre 2022 nella Gazzetta ufficiale dell'Unione Europea ed è entrato in vigore il 16 gennaio 2023. **Assumerà piena efficacia il 17 gennaio 2025**, 2 anni dopo la sua pubblicazione nella Gazzetta ufficiale dell'Unione Europea.

Punti salienti:

Introduce misure per la gestione dei rischi di tecnologie dell'informazione e della comunicazione (TIC) nel settore finanziario. La DORA punta sul concetto di ***resilienza operativa digitale***, per il settore finanziario***.***

Per **resilienza operativa digitale** si deve intendere «*la capacità dell'entità finanziaria di costruire, assicurare e riesaminare la propria integrità e affidabilità operativa, garantendo, direttamente o indirettamente tramite il ricorso ai servizi offerti da fornitori terzi di servizi TIC, l'intera gamma delle capacità connesse alle TIC, necessarie per garantire la sicurezza dei sistemi informatici e di rete utilizzati dall'entità finanziaria, su cui si fondano la costante offerta dei servizi finanziari e la loro qualità, anche in occasione di perturbazioni*»

Norme e Regolamenti

In sintesi, scrivendo il Regolamento DORA, l'obiettivo principale del legislatore europeo è stato: ***«creare un quadro normativo sulla resilienza operativa digitale, grazie a cui tutte le imprese garantiscono di poter far fronte a tutti i tipi di malfunzionamenti e minacce connesse alle TIC, al fine di prevenire e mitigare le minacce informatiche»***; pertanto:

- ✓ Garantire che le entità finanziarie siano in grado di resistere a gravi interruzioni operative digitali, come attacchi informatici o guasti ai sistemi.
- ✓ Promuovere la condivisione delle informazioni e la cooperazione tra le entità finanziarie e le autorità competenti.
- ✓ Rafforzare la fiducia dei consumatori e degli investitori nel sistema finanziario europeo.

Di conseguenza, DORA si concentra su un ampio spettro di rischi e minacce; ad esempio:

- Attacchi informatici, come malware, ransomware e attacchi di phishing.
- Guasti ai sistemi, come blackout, guasti hardware o bugs software.
- Interruzione dei servizi, dovuta a dimensionamento errato o scarsità di risorse.
- Problemi occorsi ai fornitori di servizi critici, che si ripercuotono sull’entità finanziaria.

Norme e Regolamenti

Il Regolamento si applica alle seguenti *entità finanziarie* (qui un estratto), che devono conformarsi alle prescrizioni:

- Banche
- Istituti di pagamento
- Società di intermediazione mobiliare
- Imprese di investimento
- Società di gestione del risparmio
- Compagnie di assicurazione e intermediari assicurativi
- Casse di previdenza
- Organismi di investimento collettivo
- Fondi pensione
- Fornitori di servizi di crowdfunding

(segue)

Norme e Regolamenti

Oltre alle c.d. *entità finanziarie*, nelle quali sono inclusi anche:

- prestatori di servizi di informazione sui conti;
- fornitori di servizi per le cripto-attività autorizzati;
- fornitori di servizi di comunicazione dati;

Si applica anche a:

- **fornitori terzi di servizi TIC**.

Rimangono esclusi dal Regolamento:

- gestori di fondi di investimento alternativi*;
- piccole imprese di assicurazione e di riassicurazione (esclusione dall'ambito di applicazione a causa delle dimensioni[1]);
- enti pensionistici aziendali o professionali che gestiscono schemi pensionistici che contano congiuntamente non più di 15 aderenti in totale;
- intermediari assicurativi che sono microimprese o piccole o medie imprese;
- persone fisiche o giuridiche esentate a norma degli articoli 2 e 3 della Direttiva 2014/65/UE (le autorità pubbliche di controllo, di vigilanza e di autoregolamentazione);
- alcuni uffici dei conti correnti postali.

Norme e Regolamenti

Regolamento UE n. 2022/2554 – DORA - Resilienza digitale per il settore finanziario (#002)

Punti critici:

- Il Regolamento è ancora in fase di implementazione nel settore finanziario, quindi i suoi effetti non sono ancora completamente visibili.
- La sua complessità potrebbe creare sfide per l'attuazione da parte degli enti finanziari.
- La sua implementazione richiede uno sforzo medio/alto per l’adeguamento, in termini di risorse umane, finanziarie e tecnologiche.
- Le compagnie assicurative, in particolare quelle di piccole dimensioni, potrebbero avere difficoltà ad adeguarsi alle sue disposizioni.
- Alcune disposizioni del Regolamento sono formulate in modo generico e non forniscono indicazioni sufficienti per la loro concreta implementazione; si attendono ulteriori RTS
  Le ESA hanno già emesso due lotti di consultazione congiunta in merito a svariati RTS; il riscontro per il secondo lotto scadeva il 4 marzo scorso.
- Il successo del Regolamento dipenderà dalla capacità delle autorità competenti di supervisionare e far rispettare le sue disposizioni.

Norme e Regolamenti

Regolamento UE n. 2022/2554 – DORA - Resilienza digitale per il settore finanziario (#003)

Macro-punti di attività da verificare / implementare, mediante integrazioni strutturali ed organizzative (processi / procedure):

- ✓ Policy e Procedure di IT & Risk Governance (compresi i protocolli di autorizzazione per gli accessi fisici/logici).
- ✓ Screening delle risorse umane.
- ✓ Asset Inventory & Management (fisico e logico).
- ✓ Risk assessment periodico + VA/PT.
- ✓ Incident management, con inclusi i processi di gestione escalation alle autorità competenti.
- ✓ Predisposizione Piani di BCP/DR (con BIA + Risk Assessment); esecuzione dei test di resilienza digitale (!).
- ✓ Supply Chain management (valutazione rischio fornitori – audit ai fornitori – richiesta di formazione al personale).
- ✓ Change management (manutenzioni e aggiornamenti dei sistemi).
- ✓ Adeguamento dei servizi e sistemi (crittografia, MFA, VPN, monitoraggio in real-time, sistemi IDS, IPS, sistemi di Data Loss Prevention…).
- ✓ Formazione periodica e continua a tutto il personale interno.
- ✓ Verifica dell'imposizione dell'utilizzo di determinati prodotti / servizi TIC (Tecnologie dell'Informazione e Comunicazione)
- ✓ Condivisione di dati ed informazioni in relazione alle vulnerabilità e alle minacce informatiche.

REQUISITI DEL REGOLAMENTO – GESTIONE DEI RISCHI TIC

Alcuni esempi:

1) Un'entità finanziaria che fornisce servizi di pagamento online potrebbe adottare le seguenti misure per mitigare il rischio di interruzioni operative digitali:
   - ✓ Utilizzare un'infrastruttura informatica resiliente e affidabile.
   - ✓ Avere un piano di Disaster Recovery in caso di interruzioni operative.
   - ✓ Formazione del personale sull'uso sicuro dei dati e delle informazioni.

2) Un'entità finanziaria che tratta dati personali sensibili potrebbe adottare le seguenti misure per mitigare il rischio di interruzioni operative digitali:
   - ✓ Utilizzare una soluzione di crittografia per proteggere i dati personali sensibili.
   - ✓ Avere un processo di autenticazione e autorizzazione rigoroso per accedere ai dati personali sensibili.
   - ✓ Monitorare costantemente l'accesso ai dati personali sensibili.

In generale, le entità finanziarie **devono adottare un approccio proattivo** alla gestione dei rischi TIC. Ciò significa che le entità finanziarie devono identificare e mitigare i rischi TIC prima che si verifichino.

Norme e Regolamenti - Recap

Collegamenti tra le normative - Un ecosistema normativo in evoluzione

- Le normative presentate sono interconnesse e si completano a vicenda.
- La coerenza e l'efficace attuazione di tutte le normative è fondamentale per la sicurezza informatica in Europa.
- La cooperazione tra le diverse autorità competenti è fondamentale per garantire l'applicazione coerente delle normative.
- L'istituzione della Rete Europea dei CSIRT (Computer Security Incident Response Team) è fondamentale per:
  - Promuovere la cooperazione tra i CSIRT nazionali ed europei.
  - Facilitare lo scambio di informazioni e best practice in materia di sicurezza informatica.
  - Coordinare la risposta agli incidenti informatici di rilevanza europea (attacchi su vasta scala).
- Inoltre, la rete europea euCyCLONe dovrebbe consentire:
  - Fornire un quadro per la cooperazione tra i CSIRT e le autorità competenti in materia di lotta contro la criminalità informatica, sotto il profilo tecnico.
  - Facilitare l'identificazione, la persecuzione e il deferimento alla giustizia dei perpetratori di reati informatici.
  - Rafforzare la rete di CSIRT in Europa, favorendo lo scambio di informazioni e la cooperazione a livello politico, raccordando le informazioni tra le varie entità politiche europee.

Associazione Industriali Vicenza

WEBINAR GIOVEDÌ 7 MARZO 2024

“ Sicurezza e Conformità Normativa:
Navigare nel Labirinto Normativo dei nuovi Standard Europei ”

Grazie per l’attenzione

BV TECH