LA GOVERNANCE DEL PIANO NAZIONALE DI RIPRESA E RESILIENZA – Decreto Legislativo n. 138 del 2024 – Capo III artt. 18-22 - Cooperazione a livello dell'Unione europea e internazionale

PNRR

Dossier

Il Capo III del Decreto Legislativo 4 settembre 2024, n. 138, inerente la cooperazione a livello dell'Unione europea e internazionale, stabilisce un quadro di regole e pratiche volte a favorire l'integrazione e la collaborazione tra gli Stati membri per la sicurezza informatica. **Il recepimento della direttiva UE 2022/2555 c.d. NIS 2 riflette la necessità di un approccio coordinato per affrontare le crescenti minacce cibernetiche.** L'Articolo 18 disciplina la partecipazione dell'Autorità nazionale competente NIS al Gruppo di cooperazione NIS, evidenziando l'importanza di una collaborazione strutturata tra gli Stati membri per l'attuazione e il recepimento della direttiva. **Il Gruppo di cooperazione, introdotto per la prima volta dalla direttiva UE 2016/1148 c.d. NIS 1 e rafforzato nella NIS 2, funge da piattaforma per lo scambio di informazioni e buone pratiche. La partecipazione dell'Autorità nazionale e delle autorità di settore NIS alle iniziative di questo gruppo permette di integrare l'esperienza settoriale e di migliorare la risposta comune alle minacce**. L'Autorità nazionale è incaricata di considerare gli orientamenti non vincolanti del gruppo riguardo all'attuazione della direttiva e allo sviluppo di politiche di divulgazione coordinata delle vulnerabilità, in linea con il principio di prevenzione e mitigazione dei rischi cibernetici. La cooperazione estesa include anche la condivisione di esperienze, l'analisi delle migliori prassi e la partecipazione a programmi di sviluppo delle capacità e di esercitazioni di sicurezza informatica promosse dall'ENISA. Tali pratiche sono supportate dal regolamento UE 2019/881 -Cybersecurity Act-, che assegna all'ENISA un ruolo centrale nel consolidamento della sicurezza informatica nell'UE. L'Articolo 19 si concentra sulla Rete delle organizzazioni di collegamento per le crisi informatiche - EU-CyCLONe -, sottolineando l'importanza della gestione coordinata degli incidenti su vasta scala. L'Autorità nazionale di gestione delle crisi informatiche partecipa a questa rete per aumentare la preparazione e sviluppare una conoscenza situazionale comune. **EU-CyCLONe è stata istituita per rispondere in modo efficiente alle crisi cibernetiche che richiedono un coordinamento oltre i confini nazionali, facilitando il processo decisionale a livello politico e tecnico. La cooperazione con la Rete di CSIRT nazionali e il supporto al Gruppo di cooperazione NIS garantiscono che gli Stati membri possano condividere informazioni tempestive e mitigare l'impatto degli incidenti**. Si prevede inoltre che l'Autorità nazionale possa discutere i piani nazionali di risposta con altri Stati membri, rafforzando la trasparenza e la coesione strategica all'interno dell'UE. L'Articolo 20 si occupa della **partecipazione del CSIRT Italia alla Rete di CSIRT nazionali, un elemento cruciale**

per il coordinamento operativo in caso di incidenti cibernetici. Il CSIRT Italia è tenuto a facilitare lo scambio di informazioni, la condivisione di tecnologie e pratiche di sicurezza, e a cooperare per risposte coordinate a incidenti che coinvolgono più Stati membri. La struttura della Rete di CSIRT si basa su principi di interoperabilità e fiducia, supportati dal regolamento (UE) 2019/881, che promuove la collaborazione tra i team di risposta e l'adozione di protocolli standardizzati. L'articolo prevede anche lo scambio di informazioni riguardanti incidenti, minacce e vulnerabilità, essenziale per mantenere un alto livello di prontezza operativa e garantire una risposta tempestiva. L'Articolo 21 introduce la procedura di revisione tra pari, un meccanismo volto a monitorare e valutare l'attuazione della direttiva NIS 2 a livello nazionale. L'Autorità nazionale competente NIS può richiedere o partecipare a tali revisioni, che prevedono la valutazione di specifici aspetti come l'efficacia delle capacità operative del CSIRT, le risorse disponibili e l'implementazione delle misure di gestione del rischio. Questo processo permette di rafforzare la fiducia reciproca e migliorare la cooperazione tra gli Stati membri. La revisione tra pari si ispira alle pratiche di revisione previste dal GDPR e da altre normative dell'UE per garantire un'armonizzazione delle politiche. Gli esperti designati per le revisioni devono operare con imparzialità, e l'Autorità può decidere di rendere pubblici i risultati delle valutazioni per aumentare la trasparenza e la responsabilità. L'Articolo 22 stabilisce le comunicazioni all'Unione europea, ribadendo l'obbligo della Presidenza del Consiglio dei ministri e dell'Autorità nazionale competente NIS di notificare tempestivamente alla Commissione europea informazioni rilevanti, come la designazione delle autorità competenti e le modifiche agli obblighi. Questo processo include la trasmissione della Strategia nazionale di cybersicurezza e la comunicazione delle misure sanzionatorie previste. Inoltre, l'articolo evidenzia la necessità di mantenere aggiornate le informazioni sul numero di soggetti essenziali e importanti, un requisito fondamentale per la Commissione e il Gruppo di cooperazione NIS per monitorare l'attuazione della direttiva e fornire raccomandazioni strategiche. L'Autorità di gestione delle crisi informatiche deve anche condividere informazioni pertinenti con la Rete EU-CyCLONe, rafforzando così la capacità collettiva dell'UE di rispondere alle crisi. **Da questa introduzione al Capo III del Decreto Legislativo 4 settembre 2024, n. 138 si rileva l'impegno dell'Italia a integrare e coordinare le proprie pratiche di sicurezza informatica con quelle dell'UE. Il decreto rafforza la capacità di collaborazione e scambio di informazioni, promuove la trasparenza e la coesione operativa, e assicura**

che le risposte agli incidenti e alle crisi cibernetiche siano efficaci e tempestive. La cooperazione con enti europei come l'ENISA e le reti di CSIRT, nonché la partecipazione ai meccanismi di revisione tra pari, sottolineano l'importanza di una strategia unitaria per affrontare le sfide cibernetiche globali e proteggere le infrastrutture critiche e i servizi essenziali. La normativa recepisce e amplia il concetto di sicurezza collaborativa e resilienza, elementi fondamentali per mantenere la stabilità e la fiducia nella società digitale contemporanea.

Articolo 18 del Decreto Legislativo 4 settembre 2024, n. 138

L'Articolo 18 del Decreto Legislativo 4 settembre 2024, n. 138, affronta in dettaglio le responsabilità e il funzionamento del Gruppo di Cooperazione NIS, il cui obiettivo primario è facilitare la cooperazione tra gli Stati membri dell'Unione Europea per rafforzare la sicurezza informatica, in conformità alla direttiva UE 2022/2555, nota come NIS 2. Questa direttiva aggiorna la normativa precedente per affrontare in modo più efficiente le crescenti sfide poste dalla digitalizzazione e dalle minacce informatiche. L'articolo sottolinea che l'Autorità nazionale competente NIS partecipa al Gruppo di Cooperazione NIS e specifica che le autorità di settore possono partecipare su richiesta, in base alla rilevanza delle iniziative per i rispettivi ambiti. Tra i compiti principali dell'Autorità nazionale vi è la considerazione degli orientamenti non vincolanti emessi dal Gruppo per garantire un'implementazione uniforme della direttiva e la formulazione di politiche coordinate per la divulgazione delle vulnerabilità. **L'articolo enfatizza l'importanza dello scambio di migliori prassi e informazioni riguardanti minacce, incidenti, esercitazioni, formazione e sviluppo di competenze. Questo rafforza il tessuto comune di resilienza cibernetica tra gli Stati membri. L'Autorità è inoltre coinvolta nei confronti sulle revisioni tra pari e può richiedere l'elaborazione di raccomandazioni e conclusioni, assicurando un miglioramento costante delle pratiche di sicurezza**. Il testo prevede anche che l'Autorità discuta richieste di assistenza reciproca e casi di vigilanza congiunta transfrontaliera, promuovendo una collaborazione approfondita per affrontare incidenti complessi e coordinare le risposte. Un altro punto chiave riguarda la discussione di misure di mitigazione per prevenire

e gestire incidenti di larga scala, basandosi sulle esperienze tratte da EU-CyCLONe e dalla rete dei CSIRT nazionali. L'Autorità deve partecipare ai programmi di sviluppo delle capacità e può organizzare scambi di personale con altre autorità europee per potenziare le competenze condivise. **L'articolo descrive anche il contributo dell'Autorità alla definizione di linee guida e pareri non vincolanti, oltre alla collaborazione con l'ENISA e la Commissione europea per la redazione della relazione biennale sullo stato della sicurezza informatica nell'Unione.** Questa relazione è fondamentale per monitorare l'evoluzione delle minacce e valutare l'efficacia delle strategie implementate. Inoltre, l'Autorità deve organizzare riunioni con i rappresentanti del settore privato per affrontare le sfide emergenti e raccogliere feedback utili al perfezionamento delle politiche di sicurezza. **La valutazione periodica delle minacce e degli incidenti, inclusi i ransomware, è essenziale per mantenere aggiornate le misure di risposta e prevenzione.** L'Articolo 18, quindi, consolida il ruolo dell'Autorità nazionale competente come punto focale nella partecipazione alle iniziative di cooperazione europea per la sicurezza informatica, promuovendo un approccio integrato e dinamico che risponde alle sfide attuali e rafforza la resilienza collettiva dell'Unione.

Articolo 19 del Decreto Legislativo 4 settembre 2024, n. 138

L'Articolo 19 del Decreto Legislativo 4 settembre 2024, n. 138, stabilisce la partecipazione e i compiti dell'Autorità nazionale di gestione delle crisi informatiche all'interno della Rete delle organizzazioni di collegamento per le crisi informatiche - EU-CyCLONe - , in linea con le disposizioni della direttiva UE 2022/2555. **EU-CyCLONe è una rete creata per sostenere il coordinamento tra gli Stati membri nella gestione degli incidenti e delle crisi informatiche su vasta scala, con l'obiettivo di assicurare una risposta coesa e tempestiva a minacce significative per la sicurezza informatica.** L'articolo afferma che l'Autorità nazionale di gestione delle crisi informatiche è un partecipante attivo di EU-CyCLONe e descrive i suoi contributi principali per migliorare la preparazione alla gestione di incidenti gravi, sviluppare una conoscenza situazionale condivisa e valutare le conseguenze degli incidenti, proponendo misure di mitigazione. Tra le funzioni fondamentali vi è il coordinamento della gestione delle crisi e il supporto ai processi decisionali a livello politico, assicurando che la risposta a incidenti

su vasta scala sia efficace e concertata. L'Autorità ha il compito di discutere i piani nazionali di risposta agli incidenti, quando richiesto da uno Stato membro, contribuendo a una visione collettiva che abbraccia sia le specificità nazionali che il contesto europeo. Un elemento importante del suo mandato è il supporto alla collaborazione con il Gruppo di cooperazione NIS, informandolo sugli sviluppi nella gestione delle crisi e sulle tendenze emergenti, con particolare attenzione all'impatto sugli operatori ritenuti essenziali e importanti. L'Autorità collabora inoltre strettamente con la Rete di CSIRT nazionali per favorire una cooperazione tecnica efficace e una rapida condivisione delle informazioni necessarie alla risposta coordinata. L'articolo prevede anche che l'Autorità sia coinvolta nell'elaborazione della relazione destinata al Parlamento europeo e al Consiglio, che valuta il lavoro svolto da EU-CyCLONe, come indicato nell'articolo 16, paragrafo 7, della direttiva NIS 2. Questo rapporto è cruciale per evidenziare l'efficacia della cooperazione tra gli Stati membri e individuare eventuali aree di miglioramento nella gestione delle crisi informatiche su vasta scala. Infine, l'Autorità ha la facoltà di richiedere discussioni sui piani nazionali di risposta agli incidenti, garantendo così un approccio proattivo e adattabile nella gestione delle emergenze informatiche. **L'Articolo 19 evidenzia la necessità di una collaborazione coordinata a livello europeo per proteggere l'infrastruttura critica e mantenere la continuità delle operazioni essenziali in caso di gravi minacce cibernetiche.**

Articolo 20 del Decreto Legislativo 4 settembre 2024

L'Articolo 20 del Decreto Legislativo 4 settembre 2024, n. 138, regola la partecipazione del CSIRT Italia - Computer Security Incident Response Team - alla Rete di CSIRT nazionali e delinea i compiti e le modalità di cooperazione tra i vari CSIRT degli Stati membri dell'Unione Europea. Il CSIRT Italia è tenuto a contribuire a un'efficace collaborazione e scambio di informazioni nell'ambito della sicurezza informatica per garantire una risposta coordinata e tempestiva a incidenti e minacce cibernetiche. L'articolo descrive i vari aspetti della cooperazione e le responsabilità del CSIRT Italia, tra cui lo scambio di informazioni sulle capacità operative dei CSIRT nazionali e la facilitazione del trasferimento di tecnologie,

strumenti, processi e migliori pratiche per potenziare la capacità collettiva di risposta. Un compito cruciale è rappresentato dalla condivisione di informazioni relative a incidenti e minacce, su richiesta di un altro CSIRT nazionale potenzialmente coinvolto. Il CSIRT Italia deve garantire l'interoperabilità nei protocolli e nelle specifiche per lo scambio di informazioni, permettendo così una comunicazione fluida e coerente tra i team di risposta. **In casi di incidenti significativi, su richiesta di un altro CSIRT, il CSIRT Italia è tenuto a discutere e, se possibile, coordinare una risposta operativa, fornendo assistenza a più Stati membri coinvolti**. La cooperazione include anche il supporto ai CSIRT che agiscono come coordinatori secondo l'articolo 12 della direttiva UE 2022/2555 e l'assistenza nella gestione della divulgazione di vulnerabilità che possono avere un impatto su più Stati membri. L'articolo specifica la necessità di scambiare informazioni in merito a minacce, preallarmi e assistenza reciproca, nonché di contribuire ai piani di risposta nazionale alle crisi informatiche su richiesta. **Il CSIRT Italia deve anche collaborare con centri operativi di sicurezza sia regionali che a livello dell'Unione per migliorare la consapevolezza collettiva sugli incidenti e le minacce**. Inoltre, è previsto che il CSIRT discuta le relazioni sulle revisioni tra pari e fornisca al Gruppo di cooperazione NIS aggiornamenti sulle proprie attività e sulle forme di cooperazione operative individuate, richiedendo, se necessario, orientamenti non vincolanti. Infine, l'articolo sottolinea l'importanza di fare il punto sui risultati delle esercitazioni di sicurezza informatica, inclusi gli eventi organizzati dall'ENISA, e di fornire orientamenti non vincolanti per facilitare la convergenza delle pratiche operative tra i CSIRT nazionali. **Queste disposizioni mirano a costruire una rete coordinata e resiliente per affrontare congiuntamente le sfide della sicurezza informatica a livello europeo.**

Articolo 21 del Decreto Legislativo 4 settembre 2024, n. 138

L'Articolo 21 del Decreto Legislativo 4 settembre 2024, n. 138, regola la procedura di revisione tra pari - **peer review** - per l'Autorità nazionale competente NIS, in linea con quanto previsto dall'articolo 19 della direttiva UE 2022/2555 c.d. NIS 2. **Questa procedura è finalizzata a garantire che gli Stati membri attuino in modo efficace e omogeneo le misure di sicurezza informatica previste dalla direttiva**. L'Autorità nazionale competente NIS può partecipare a

tali revisioni richiedendo di essere sottoposta a revisione riguardo all'attuazione della direttiva NIS 2 a livello nazionale. Inoltre, può indicare rappresentanti esperti dell'Agenzia per la cybersicurezza nazionale o delle autorità di settore per partecipare come revisori in procedure presso altri Stati membri, nel rispetto dei codici di condotta e assicurando la trasparenza sui possibili conflitti di interesse, condivisi con Stati membri, il Gruppo di cooperazione NIS, la Commissione europea e l'ENISA. **Per attivare la procedura di revisione, l'Autorità deve identificare almeno un aspetto da esaminare, come il livello di attuazione delle misure di gestione del rischio e di notifica degli incidenti, le risorse e capacità operative del CSIRT Italia, lo stato di attuazione dell'assistenza reciproca e degli accordi di condivisione delle informazioni, o questioni transfrontaliere o intersettoriali**. L'Autorità è tenuta a notificare l'ambito della revisione agli Stati membri partecipanti e può effettuare un'autovalutazione degli aspetti oggetto di revisione. In questa fase, è anche responsabile della selezione degli esperti da designare per la revisione e, se necessario, può opporsi alla loro designazione giustificando i motivi. Durante la revisione, l'Autorità fornisce agli esperti le informazioni necessarie e facilita visite in loco o scambi a distanza, mentre può formulare osservazioni sulla relazione finale e decidere se renderla pubblica, allegando in tutto o in parte le proprie osservazioni. Gli esperti designati dall'Autorità sono vincolati a non divulgare informazioni sensibili ottenute durante le revisioni e contribuiscono all'elaborazione delle relazioni finali, mantenendo la riservatezza delle informazioni secondo la normativa europea e nazionale sulla protezione di informazioni classificate e sulla sicurezza dello Stato.

Articolo 22 del Decreto Legislativo 4 settembre 2024, n. 138

L'Articolo 22 del Decreto Legislativo 4 settembre 2024, n. 138, stabilisce le modalità e le tempistiche con cui le autorità italiane devono comunicare informazioni e designazioni alla Commissione europea e ad altri enti dell'Unione europea in merito all'attuazione della direttiva UE 2022/2555 c.d. NIS 2. Tale direttiva mira a migliorare la cibersicurezza garantendo un livello comune di protezione attraverso l'Unione. L'articolo specifica che, dopo l'entrata in vigore del decreto, la Presidenza del Consiglio dei ministri deve notificare tempestivamente

alla Commissione europea la conferma dell'Agenzia per la cybersicurezza nazionale quale Autorità nazionale competente NIS e Punto di contatto unico NIS, insieme al Ministero della difesa, come Autorità nazionale di gestione delle crisi informatiche. Ogni modifica successiva a queste designazioni o ai relativi compiti deve essere notificata senza ritardi ingiustificati, garantendo adeguata pubblicità a tali designazioni. **L'Autorità nazionale competente NIS ha il compito di trasmettere alla Commissione la Strategia nazionale di cybersicurezza entro tre mesi dalla sua adozione o aggiornamento, salvo eventuali esclusioni per motivi di sicurezza nazionale. Entro il 17 gennaio 2025, l'Autorità deve comunicare alla Commissione le misure sanzionatorie previste per i soggetti essenziali e importanti, informando anche sulle modifiche successive.** Entro il 17 aprile 2025 e ogni due anni successivi, l'Autorità deve inviare alla Commissione e al Gruppo di cooperazione NIS il numero di soggetti essenziali e importanti per ciascun settore, fornendo ulteriori dettagli sui criteri e sulle specifiche dei servizi forniti. L'Autorità può, su richiesta della Commissione, notificare i nomi dei soggetti essenziali e importanti e trasmettere all'ENISA le informazioni necessarie per l'inserimento nel registro pertinente. Il Punto di contatto unico NIS comunica alla Commissione la designazione dell'Agenzia per la cybersicurezza nazionale quale CSIRT nazionale -CSIRT Italia- e ogni modifica successiva, oltre a trasmettere all'ENISA, trimestralmente a partire dal 2026, relazioni di sintesi sui dati relativi a incidenti significativi e minacce informatiche. Il Punto di contatto è inoltre responsabile di notificare le segnalazioni di incidenti transfrontalieri agli altri Stati membri e all'ENISA senza ritardo. L'Autorità nazionale di gestione delle crisi informatiche deve comunicare alla Commissione e al EU-CyCLONe le informazioni sui piani nazionali di risposta agli incidenti e alle crisi su vasta scala entro tre mesi dall'adozione o aggiornamento, garantendo il rispetto della normativa sulla protezione delle informazioni classificate e la sicurezza nazionale.