LA GOVERNANCE DEL PIANO NAZIONALE DI RIPRESA E RESILIENZA – Decreto Legislativo n. 138 del 2024 – Capo II artt. 9-17 - Quadro Nazionale di Sicurezza Informatica

PNRR

Dossier

L'importanza della sicurezza informatica, o cybersicurezza, è oggi al centro dell'agenda europea e nazionale, dato il numero crescente di minacce che incidono sulla stabilità e l'integrità delle infrastrutture digitali e dei servizi essenziali**. In risposta alla crescente sofisticazione degli attacchi e all'aumento della dipendenza dai sistemi digitali, l'Unione Europea ha istituito un quadro normativo, rappresentato principalmente dalla direttiva NIS 2** - Network and Information Security -, approvata con la direttiva UE 2022/2555. La normativa stabilisce requisiti specifici per migliorare la resilienza dei sistemi informatici all'interno degli Stati membri, con l'obiettivo di creare una capacità di risposta europea che superi le frontiere e promuova un livello di sicurezza cibernetica omogeneo e collaborativo. **La trasposizione italiana di questa normativa avviene attraverso il Decreto Legislativo n. 138 del 2024, il quale definisce un quadro strutturato e complesso per la sicurezza informatica, con una serie di disposizioni normative volte a rafforzare la protezione delle infrastrutture critiche e dei servizi essenziali nel paese**. All'interno di questo quadro, il Capo II del decreto risulta fondamentale, poiché delinea la struttura e le responsabilità delle autorità competenti, stabilendo le strategie, le misure di risposta e i processi di cooperazione, sia a livello nazionale che internazionale. Gli articoli compresi tra il 9 e il 17 stabiliscono i principi guida della cybersicurezza nazionale, specificando ruoli chiave come quello dell'Agenzia per la Cybersicurezza Nazionale, definendo le modalità di cooperazione con altre autorità nazionali e stabilendo il CSIRT Italia come organismo di risposta agli incidenti. Questa parte del decreto, inoltre, fornisce le linee guida per la gestione delle vulnerabilità, promuovendo la condivisione delle informazioni sulle minacce cibernetiche e rafforzando la capacità del paese di reagire in modo tempestivo ed efficace agli incidenti informatici. La **Strategia Nazionale di Cybersicurezza** è un elemento fondamentale per la pianificazione e l'implementazione di misure preventive e di risposta agli incidenti informatici. **Questo documento è redatto dall'Agenzia per la Cybersicurezza Nazionale e stabilisce obiettivi, priorità settoriali, risorse e strumenti per una difesa resiliente nel tempo**. La strategia rispecchia un quadro dinamico, in quanto è soggetta a revisioni periodiche almeno ogni cinque anni, sebbene sia possibile modificarla in tempi più brevi qualora emergano nuovi fattori di rischio. Gli obiettivi della strategia comprendono la protezione delle infrastrutture critiche, la creazione di un meccanismo efficace di gestione delle crisi informatiche e il miglioramento continuo della resilienza delle infrastrutture nazionali. Gli allegati I, II, III e IV del decreto elencano i settori

considerati essenziali per la sicurezza nazionale e includono aree strategiche come l'energia, i trasporti, le infrastrutture digitali e la sanità. Il decreto delinea un quadro di governance specifico, chiarendo i ruoli e le responsabilità delle autorità di settore e delle amministrazioni pubbliche, con particolare attenzione alla cooperazione tra l'Agenzia per la Cybersicurezza Nazionale e altre autorità competenti in tema di regolamentazione e sicurezza. Oltre alla gestione tecnica delle crisi, **la Strategia Nazionale di Cybersicurezza prevede meccanismi per aumentare la consapevolezza dei cittadini, promuovendo un'educazione alla sicurezza informatica che includa anche attività di sensibilizzazione e formazione. Tale misura è di primaria importanza, poiché la sicurezza delle infrastrutture digitali nazionali dipende non solo dall'efficacia delle misure di sicurezza adottate, ma anche dalla capacità di riconoscere e affrontare i rischi informatici da parte di ogni cittadino e organizzazione.** L'articolo 10 conferisce all'Agenzia per la Cybersicurezza Nazionale ACN il ruolo di Autorità Nazionale Competente NIS e di Punto di Contatto Unico NIS. Questo implica che l'ACN non solo sovrintende all'applicazione del decreto a livello nazionale, ma agisce anche come principale organo di collegamento per la cooperazione transfrontaliera in ambito europeo. Come **Autorità Nazionale, l'ACN dispone di ampi poteri di regolamentazione, gestione e coordinamento degli obblighi di sicurezza informatica. In qualità di Punto di Contatto Unico, l'ACN facilita la collaborazione e lo scambio di informazioni sulle minacce con le autorità degli altri Stati membri e con agenzie come l'ENISA, l'Agenzia dell'Unione europea per la sicurezza informatica**. Questa cooperazione rafforza la capacità di monitoraggio e risposta del sistema di sicurezza italiano, in linea con le best practice europee. Attraverso specifici provvedimenti, l'ACN assicura che i soggetti essenziali e importanti del settore pubblico e privato rispettino i requisiti di sicurezza, fornendo raccomandazioni operative e orientamenti non vincolanti per garantire un'adeguata protezione dei dati e delle reti. Oltre al ruolo centrale dell'ACN, il decreto designa specifiche **Autorità di settore NIS**, delineate nell'articolo 11, le quali hanno la funzione di supportare l'ACN nell'implementazione della normativa NIS e di garantire che le disposizioni del decreto vengano rispettate nei vari settori economici. Le autorità designate comprendono, tra le altre, la **Presidenza del Consiglio dei Ministri per la gestione dei servizi TIC, il Ministero dell'Economia e delle Finanze per i settori bancario e finanziario, il Ministero della Salute per il settore sanitario e il Ministero dell'Ambiente per l'energia e la gestione delle risorse idriche**. Le Autorità di settore NIS collaborano con l'ACN nel monitoraggio dei soggetti critici e dei soggetti importanti, nel

supporto alla stesura dell'elenco nazionale dei soggetti essenziali e nell'individuazione delle misure di mitigazione e prevenzione dei rischi. La collaborazione tra le diverse autorità settoriali si estende anche all'ambito europeo, poiché l'attuazione della direttiva NIS 2 richiede una cooperazione coordinata a livello dell'Unione Europea, soprattutto nei settori delle infrastrutture e dei servizi che hanno un impatto transnazionale. L'articolo 12 istituisce il **Tavolo per l'attuazione della disciplina NIS**, **presieduto dal Direttore Generale dell'ACN e composto dai rappresentanti delle Autorità di settore e da rappresentanti designati da regioni e province autonome. Questo Tavolo costituisce un punto di raccordo per la condivisione delle informazioni, la formulazione di proposte normative e la preparazione di una relazione annuale sull'attuazione del decreto, offrendo un meccanismo istituzionalizzato di dialogo e coordinamento**. Il Tavolo è essenziale per l'efficace attuazione della disciplina NIS, poiché permette una discussione approfondita sulle problematiche settoriali, garantendo che le peculiarità di ciascun settore siano prese in considerazione nella formulazione di politiche e misure di sicurezza. L'articolo 13 introduce il **Quadro nazionale di gestione delle crisi informatiche**, affidando all'ACN e al Ministero della Difesa il ruolo di Autorità nazionali di gestione delle crisi informatiche, ciascuno per il proprio ambito di competenza. Questo sistema di gestione delle crisi si fonda su un piano nazionale di risposta agli incidenti e alle crisi informatiche su vasta scala, aggiornato almeno ogni tre anni e approvato tramite decreto del Presidente del Consiglio dei Ministri. Il piano stabilisce obiettivi e modalità di gestione, definendo le responsabilità delle autorità coinvolte, le procedure operative, le misure di preparazione e i portatori di interesse, pubblici e privati, che devono essere coinvolti nella gestione delle emergenze. Questo approccio sistematico alla gestione delle crisi è cruciale per garantire che il paese sia preparato ad affrontare minacce cibernetiche di ampia portata e che le procedure siano integrate nei meccanismi di gestione delle crisi nazionali. La **cooperazione tra le Autorità nazionali**, trattata nell'articolo 14, rappresenta un altro aspetto fondamentale per la sicurezza informatica nazionale. **Il decreto stabilisce un obbligo di cooperazione e condivisione delle informazioni tra l'ACN e altre autorità nazionali, come il Garante per la protezione dei dati personali, l'Autorità per le garanzie nelle comunicazioni, l'Agenzia per l'Italia Digitale (AgID), e il Ministero della Difesa.** Tale cooperazione è estesa anche alle autorità di contrasto, in particolare in relazione alle violazioni della privacy, agli incidenti di sicurezza e alla gestione degli aspetti di difesa militare. **Questa collaborazione istituzionale assicura che le competenze siano condivise in modo ottimale**

e che le minacce cibernetiche siano affrontate in un'ottica di sicurezza complessiva. L'articolo 15 riguarda il **Gruppo nazionale di risposta agli incidenti di sicurezza informatica CSIRT Italia**, che riveste un ruolo centrale nella risposta agli incidenti cibernetici. Il CSIRT Italia è incaricato di gestire gli incidenti di sicurezza informatica per tutti i settori inclusi negli allegati I, II, III e IV del decreto, garantendo un'infrastruttura informativa e di comunicazione resiliente e sicura. Tra i compiti del CSIRT vi è il monitoraggio delle minacce informatiche e delle vulnerabilità, l'emissione di preallarmi e allerte, l'assistenza ai soggetti essenziali e importanti, la raccolta di dati forensi e l'analisi dinamica dei rischi. Inoltre, il CSIRT Italia è responsabile della collaborazione con altri CSIRT europei e internazionali, facilitando lo scambio di informazioni e promuovendo l'integrazione delle pratiche di sicurezza a livello globale. La sua funzione è integrata con altri team di risposta agli incidenti di carattere nazionale, inclusi i CERT -Computer Emergency Response Team-, con cui il CSIRT collabora per rafforzare il coordinamento delle risposte agli incidenti, migliorando la capacità del paese di rispondere alle crisi cibernetiche. Un aspetto innovativo del decreto è rappresentato dalla **divulgazione coordinata delle vulnerabilità**. Il CSIRT Italia è designato come coordinatore per facilitare la segnalazione delle vulnerabilità da parte di individui o enti, agendo da intermediario di fiducia tra il segnalante e il produttore o fornitore di servizi TIC. La divulgazione coordinata rappresenta un approccio proattivo alla gestione delle vulnerabilità: tramite l'identificazione, la comunicazione e la risoluzione delle criticità informatiche prima che diventino vettori di attacco, il CSIRT assicura che le vulnerabilità siano gestite in modo sicuro, evitando potenziali danni. La possibilità di segnalazioni anonime e la cooperazione con altri CSIRT europei rende questo processo trasparente e sicuro, favorendo la fiducia tra il pubblico e gli enti di sicurezza. Infine, l'articolo 17 promuove la creazione di **accordi di condivisione delle informazioni sulla sicurezza informatica**, consentendo ai soggetti interessati di scambiarsi informazioni rilevanti per prevenire e mitigare gli incidenti di sicurezza. Questi accordi sono di natura volontaria e coinvolgono sia soggetti pubblici che privati, favorendo una cooperazione basata sulla condivisione di informazioni su minacce, vulnerabilità e tecniche di mitigazione. L'ACN e il CSIRT Italia supportano e promuovono questi accordi, incentivando l'uso di piattaforme TIC sicure e strumenti di automazione per rendere la condivisione delle informazioni più efficace. La collaborazione attraverso tali accordi offre una maggiore capacità di difesa e un migliore scambio di conoscenze tra gli attori della sicurezza cibernetica, rendendo il sistema complessivo più resiliente alle minacce

informatiche. Il Capo II del Decreto Legislativo n. 138 del 2024 rappresenta dunque un passaggio cruciale per l'implementazione di un sistema di sicurezza informatica integrato e resiliente in Italia. **Attraverso una strategia nazionale mirata, l'attribuzione di competenze specifiche alle autorità di settore, la creazione di tavoli di coordinamento, la gestione delle crisi, e la promozione della cooperazione informativa, il decreto fornisce una risposta organica e coordinata alle minacce cibernetiche. La normativa non solo adatta il paese ai requisiti della direttiva NIS 2, ma promuove anche la costruzione di un ecosistema digitale sicuro e affidabile, in cui le informazioni e le competenze sono condivise per proteggere le infrastrutture critiche e garantire la continuità dei servizi essenziali per i cittadini e le imprese. La cooperazione a livello europeo e la promozione della sensibilizzazione pubblica ampliano ulteriormente la portata di queste misure, contribuendo a creare una cultura della sicurezza informatica che sia in grado di evolversi nel tempo, rispondendo in modo tempestivo ed efficace ai nuovi rischi digitali.**

Articolo 9 del Decreto Legislativo n. 138 del 2024

L'articolo 9 del Decreto Legislativo n. 138 del 2024 introduce la Strategia Nazionale di Cybersicurezza, che rappresenta il fulcro delle politiche italiane di sicurezza informatica. La strategia è concepita per stabilire obiettivi strategici chiari, le risorse necessarie per raggiungerli e le misure strategiche e normative per mantenere un livello elevato di sicurezza informatica. Questo approccio integrato include la definizione di settori prioritari, identificati negli allegati I, II, III e IV del decreto, che vanno dai settori industriali critici ai servizi pubblici essenziali. **Uno dei principali obiettivi della strategia è garantire che il paese disponga di una governance chiara per la cybersicurezza, indicando i ruoli e le responsabilità dei principali attori coinvolti, come l'Agenzia per la Cybersicurezza Nazionale (ACN), il CSIRT Italia e le Autorità di settore NIS**. Il decreto specifica un sistema di governance che prevede una stretta collaborazione tra le autorità nazionali e le autorità dell'Unione Europea, così da facilitare lo scambio di informazioni e garantire una risposta rapida ed efficiente agli incidenti. L'articolo pone inoltre grande attenzione alla gestione delle risorse, includendo la valutazione dei rischi a livello nazionale e la creazione di misure per garantire la preparazione, la risposta e il recupero dagli incidenti. Viene anche enfatizzata la collaborazione tra pubblico

e privato, essenziale per costruire una rete resiliente che coinvolga tutti i principali portatori di interesse. **Un elemento centrale della strategia è il rafforzamento della consapevolezza pubblica in materia di cybersicurezza, con un piano mirato ad accrescere la cultura della sicurezza tra i cittadini, fondamentale per ridurre le vulnerabilità umane alle minacce cyber.** Tra le misure strategiche elencate, particolare rilevanza viene data alla sicurezza nella catena di approvvigionamento dei prodotti e servizi TIC utilizzati dai soggetti per la fornitura dei loro servizi. Viene anche introdotta l'inclusione di requisiti di sicurezza informatica negli appalti pubblici, compresi aspetti quali la certificazione di cybersicurezza e l'utilizzo di prodotti di sicurezza open source, come misure per aumentare la trasparenza e l'affidabilità delle soluzioni implementate. Un altro punto cruciale riguarda la gestione delle vulnerabilità, dove l'articolo 9 incoraggia la divulgazione coordinata delle vulnerabilità come previsto dall'articolo 16, promuovendo una cultura di prevenzione e trasparenza. La strategia include inoltre il sostegno alla sicurezza della rete internet, con misure specifiche per la protezione dei cavi sottomarini, elemento fondamentale per l'integrità delle comunicazioni globali e, di conseguenza, per la sicurezza nazionale. L'articolo 9 incoraggia lo sviluppo e l'integrazione di tecnologie avanzate, un elemento chiave per mantenere l'Italia all'avanguardia nelle tecniche di gestione dei rischi cyber. La promozione della formazione e della sensibilizzazione, così come il supporto agli istituti di ricerca e accademici, sono componenti altrettanto importanti della strategia, poiché consentono di creare una forza lavoro preparata e una solida base di conoscenza nazionale. La strategia include anche la messa a punto di procedure e strumenti per la condivisione delle informazioni sulla sicurezza informatica, incoraggiando la collaborazione volontaria tra soggetti e rispettando la normativa europea, per promuovere uno scambio rapido e sicuro di dati. L'articolo evidenzia inoltre la necessità di sostenere le piccole e medie imprese, anche quelle non direttamente incluse nell'ambito del decreto, attraverso linee guida facilmente accessibili e orientamenti pratici per rafforzare la loro resilienza e igiene informatica**. Viene anche enfatizzata la promozione di una protezione informatica attiva, un approccio che va oltre la reazione agli attacchi e si concentra su misure preventive e proattive per evitare che le minacce possano danneggiare le infrastrutture critiche e i servizi essenziali**. L'Agenzia per la Cybersicurezza Nazionale è incaricata di valutare e aggiornare periodicamente la strategia, con il contributo delle amministrazioni componenti il Nucleo per la cybersicurezza. Tale valutazione, effettuata ogni cinque anni o al bisogno, si basa su indicatori chiave di prestazione e viene proposta al Presidente del Consiglio dei ministri per l'adozione. In questo

modo, la strategia nazionale si mantiene dinamica e rispondente all'evoluzione delle minacce e delle tecnologie, assicurando che l'Italia resti pronta ad affrontare sfide sempre nuove nel panorama della cybersicurezza globale.

Articolo 10 del Decreto Legislativo n. 138 del 2024

L'articolo 10 del Decreto Legislativo n. 138 del 2024 attribuisce all'Agenzia per la Cybersicurezza Nazionale ACN il ruolo di Autorità nazionale competente NIS, in linea con quanto previsto dall'articolo 8, paragrafo 1, della direttiva UE 2022/2555 NIS 2. **In quanto Autorità nazionale competente, l'ACN è responsabile della supervisione e dell'attuazione delle disposizioni del decreto, nonché della predisposizione dei provvedimenti necessari per la sua implementazione. Questo ruolo comporta una serie di compiti che includono la regolamentazione attraverso l'adozione di linee guida, raccomandazioni e orientamenti non vincolanti, al fine di fornire direttive chiare ai soggetti regolati e supportare la conformità normativa. L'ACN è inoltre incaricata dell'identificazione dei soggetti essenziali e importanti**, come previsto dagli articoli 3 e 6 del decreto, **e della redazione dell'elenco annuale di tali soggetti** secondo l'articolo 7. Questo elenco è cruciale per monitorare le infrastrutture e i servizi critici, consentendo un intervento tempestivo e mirato in caso di incidenti. L'Agenzia rappresenta anche l'Italia nelle iniziative e nei consessi dell'Unione Europea relativi alla direttiva NIS 2, collaborando strettamente con il Gruppo di cooperazione NIS e con altre autorità europee per coordinare le misure di cybersicurezza a livello continentale. Oltre al ruolo di regolazione interna, l'ACN funge da Punto di contatto unico NIS, secondo quanto indicato all'articolo 8, paragrafo 3, della direttiva NIS 2. In questo ruolo, l'Agenzia assicura il collegamento e la cooperazione transfrontaliera tra le autorità nazionali, la Commissione Europea e l'ENISA, facilitando uno scambio continuo di informazioni e una risposta congiunta alle minacce cyber che superano le frontiere nazionali. Questo sistema di coordinamento è essenziale per garantire un alto livello di sicurezza cibernetica a livello europeo, specialmente in situazioni di emergenza o crisi che richiedono un'azione coordinata. Per sostenere queste funzioni, l'articolo 10 prevede un finanziamento annuo di 2 milioni di euro a partire dal 2025, come disposto dall'articolo 44. Questa dotazione finanziaria è destinata a coprire le spese operative e a rafforzare le capacità dell'ACN nel

perseguire i suoi obiettivi strategici, in linea con gli impegni previsti dalla direttiva NIS 2 e dalla normativa nazionale sulla cybersicurezza.

Articolo 11 del Decreto Legislativo n. 138 del 2024

L'articolo 11 del Decreto Legislativo n. 138 del 2024 istituisce le Autorità di settore NIS per garantire un'efficace attuazione del decreto nei vari ambiti settoriali. Queste autorità sono designate per supportare e collaborare con l'Autorità nazionale NIS - l'Agenzia per la Cybersicurezza Nazionale, ACN - nelle attività di regolamentazione, monitoraggio e gestione della cybersicurezza a livello settoriale, secondo le modalità stabilite. Tra le autorità designate, la Presidenza del Consiglio dei Ministri si occupa del settore dei servizi TIC, del settore dello spazio, della gestione delle pubbliche amministrazioni e delle società pubbliche; il Ministero dell'Economia e delle Finanze supervisiona i settori bancario e delle infrastrutture dei mercati finanziari, in coordinamento con la Banca d'Italia e la Consob; il Ministero delle Imprese e del Made in Italy è responsabile delle infrastrutture digitali, dei servizi postali e di corriere, della produzione di sostanze chimiche, della fabbricazione di apparecchiature tecnologiche e dei servizi digitali. Altre autorità di settore includono il Ministero dell'Agricoltura per il settore alimentare, il Ministero dell'Ambiente per il settore energetico e idrico, il Ministero delle Infrastrutture per i trasporti, il Ministero della Ricerca per il settore della ricerca, il Ministero della Cultura per le attività di interesse culturale e il Ministero della Salute per il settore sanitario e i dispositivi medici. **Queste amministrazioni, nei rispettivi ambiti, sono anche designate Autorità di settore per i soggetti individuati come essenziali o importanti, come indicato nell'articolo 3. Le Autorità di settore NIS verificano l'elenco dei soggetti critici, supportano l'ACN nell'identificazione dei soggetti essenziali e importanti, individuano i soggetti che potrebbero essere esentati dagli obblighi del decreto e contribuiscono alla stesura della relazione annuale. Esse sono inoltre responsabili dell'istituzione dei tavoli settoriali, forum di coordinamento per garantire un'applicazione coerente del decreto e monitorare le attività dei soggetti di settore**. Le Autorità di settore partecipano inoltre alle attività settoriali del Gruppo di Cooperazione NIS a livello europeo, promuovendo una collaborazione transfrontaliera e lo scambio di informazioni e best practices. **Un importante aspetto è la collaborazione con le regioni e le province autonome in caso di soggetti critici**

di carattere regionale, con modalità definite tramite la Conferenza Stato-Regioni. L'articolo autorizza ciascuna autorità di settore, tranne quella per i mercati finanziari, a reclutare personale non dirigenziale tramite procedure pubbliche, mobilità o altre modalità, per garantire l'efficienza delle operazioni di attuazione del decreto. A sostegno di questa misura, l'articolo 11 prevede un budget dedicato di 409.424 euro per il 2024 e di 925.695 euro annui a partire dal 2025, coperto attraverso le disposizioni dell'articolo 44.

Articolo 12 del Decreto Legislativo n. 138 del 2024

L'articolo 12 del Decreto Legislativo n. 138 del 2024 istituisce, presso l'Agenzia per la Cybersicurezza Nazionale ACN, il **Tavolo per l'attuazione della disciplina NIS, una struttura permanente concepita per garantire l'implementazione e l'attuazione efficace del decreto. Questo tavolo è presieduto dal direttore generale dell'ACN, o da un suo delegato, ed è composto da un rappresentante di ciascuna Autorità di settore NIS, come indicato nell'articolo 11, insieme a due rappresentanti designati dalle regioni e dalle province autonome di Trento e Bolzano, tramite la Conferenza Stato-Regioni**. I componenti del Tavolo possono essere affiancati, in funzione delle materie trattate, da ulteriori rappresentanti delle loro amministrazioni. Inoltre, **il Tavolo può coinvolgere rappresentanti di altre amministrazioni, università, enti di ricerca e operatori privati interessati dal decreto, assicurando così una collaborazione ampia e multidisciplinare.** La convocazione delle riunioni del Tavolo avviene su iniziativa del presidente o su richiesta di almeno tre componenti, con una frequenza minima di una riunione trimestrale. Le funzioni principali del Tavolo comprendono il supporto all'ACN nello svolgimento delle sue funzioni di attuazione del decreto, la formulazione di proposte e pareri per l'adozione di linee guida e atti di indirizzo, e la redazione di una relazione annuale sullo stato di attuazione del decreto. L'organizzazione e il funzionamento del Tavolo possono essere ulteriormente disciplinati secondo le modalità dell'articolo 40, comma 5. Va sottolineato che **la partecipazione al Tavolo è gratuita e non comporta compensi, gettoni di presenza o rimborsi spese, garantendo così un impegno continuativo e senza oneri aggiuntivi per i partecipanti**.

Articolo 13 del Decreto Legislativo n. 138 del 2024

L'articolo 13 del Decreto Legislativo n. 138 del 2024 istituisce un quadro nazionale per la gestione delle crisi informatiche, designando l'Agenzia per la Cybersicurezza Nazionale ACN e il Ministero della Difesa come Autorità nazionali per la gestione di tali crisi, ciascuna operante nei propri ambiti di competenza definiti nell'articolo 2, comma 1, lettera g). Questi due enti hanno il compito di identificare le capacità, risorse e procedure disponibili per affrontare potenziali crisi informatiche, fornendo una risposta strutturata e coerente a livello nazionale. Entro un anno dall'entrata in vigore del decreto, il Presidente del Consiglio dei Ministri, su proposta dell'ACN e del Ministero della Difesa e con il parere del Comitato Interministeriale per la Sicurezza della Repubblica, deve adottare uno o più decreti per stabilire un piano nazionale di risposta agli incidenti e alle crisi informatiche su vasta scala. Questo piano è aggiornato almeno ogni tre anni per garantire la sua efficacia in un panorama di minacce in continua evoluzione. Il piano nazionale stabilisce gli obiettivi di gestione delle crisi informatiche, definendo nel dettaglio i compiti e le responsabilità delle Autorità nazionali e le procedure per la gestione integrata delle crisi nel quadro nazionale di cybersicurezza. Tra i punti principali, il piano prevede anche le misure di preparazione come esercitazioni e attività formative, che assicurano una risposta coordinata tra gli enti pubblici e privati coinvolti. Inoltre, definisce le modalità di scambio di informazioni e il coinvolgimento di tutte le infrastrutture e i portatori di interesse rilevanti, garantendo una cooperazione efficace tra pubblico e privato. Questo coordinamento include anche l'adesione dell'Italia agli sforzi dell'Unione Europea nella gestione delle crisi informatiche transfrontaliere, con l'obiettivo di partecipare alla gestione unificata di incidenti a livello comunitario. I decreti che definiscono il piano nazionale di risposta sono esclusi dall'accesso pubblico e non vengono pubblicati, assicurando così il rispetto della riservatezza delle strategie e delle misure operative adottate per la sicurezza nazionale. A sostegno di queste misure, è previsto un finanziamento annuale di un milione di euro a partire dal 2025, coperto attraverso le disposizioni finanziarie dell'articolo 44 del decreto.

Articolo 14 del Decreto Legislativo n. 138 del 2024

L'articolo 14 del Decreto Legislativo n. 138 del 2024 stabilisce un quadro per la cooperazione tra l'Autorità nazionale competente NIS -ACN - e altri organi di controllo e sicurezza per garantire una risposta coordinata e integrata alle minacce e agli incidenti informatici. L'articolo sottolinea **l'importanza della collaborazione tra l'Autorità nazionale e il Punto di contatto unico NIS con enti nazionali chiave come il Ministero dell'Interno, il Garante per la protezione dei dati personali, l'ENAC (Ente Nazionale per l'Aviazione Civile), l'AgID (Agenzia per l'Italia Digitale), l'Autorità per le garanzie nelle comunicazioni (AGCOM), e il Ministero della Difesa, tra altri. Questa rete di collaborazione ha l'obiettivo di consolidare lo scambio regolare e tempestivo di informazioni riguardanti incidenti e minacce rilevanti, rafforzando la capacità nazionale di monitorare e rispondere agli eventi cyber in modo efficace.** L'articolo introduce **specifiche modalità di cooperazione con il Garante per la protezione dei dati personali**, soprattutto nei casi in cui gli incidenti includano la violazione di dati personali, come stabilito dal GDPR. Se l'Autorità nazionale NIS rileva che una violazione di sicurezza potrebbe implicare una violazione dei dati personali, è tenuta a informare il Garante senza ritardi. Nel caso in cui il Garante, o altre autorità di controllo, impongano una sanzione per violazioni legate a dati personali, l'Autorità nazionale NIS evita di imporre ulteriori sanzioni amministrative per la stessa violazione, limitandosi invece ad esercitare eventuali poteri esecutivi necessari per garantire il rispetto delle norme di sicurezza. Un'altra parte importante del quadro di cooperazione si sviluppa tra l'Autorità nazionale NIS e il Ministero della Difesa, attraverso un decreto del Presidente del Consiglio dei Ministri. Questo decreto definisce un elenco di soggetti le cui attività hanno un impatto sulla sicurezza militare dello Stato. In tali casi, l'Autorità nazionale NIS è tenuta a notificare tempestivamente al Ministero della Difesa eventuali incidenti o violazioni, facilitando così la protezione delle infrastrutture critiche per la difesa nazionale. A livello internazionale, l'Autorità nazionale competente NIS partecipa a collaborazioni strutturate con le autorità nazionali di altri Stati membri dell'Unione Europea, in conformità con il regolamento UE 2022/2554. Questo include la partecipazione nel forum di sorveglianza europea per monitorare e gestire l'impatto di fornitori critici di servizi TIC, favorendo una vigilanza armonizzata su scala europea. Inoltre, le autorità italiane cooperano attivamente con le autorità competenti di altri Stati membri per lo

scambio di informazioni su rischi e incidenti. Per rafforzare ulteriormente la risposta coordinata a minacce che possono riguardare soggetti critici, l'articolo stabilisce che le autorità competenti ai sensi del decreto che recepisce la direttiva UE 2022/2557 condividano informazioni con l'Autorità nazionale NIS. Questo scambio include dati su soggetti considerati critici, aggiornamenti su rischi e incidenti e informazioni sulle misure adottate. Le autorità del decreto UE 2022/2557 possono anche chiedere all'Autorità nazionale NIS di intervenire e adottare misure di vigilanza o esecuzione specifiche sui soggetti critici. **L'articolo 14 delinea dunque un quadro di cooperazione multisettoriale e transfrontaliera per la sicurezza informatica. Attraverso questi accordi, il sistema nazionale di cybersicurezza può rispondere più efficacemente alle minacce informatiche, rispettando al contempo le competenze degli altri enti di controllo e armonizzando le misure di sicurezza a livello europeo e nazionale.**

Articolo 15 del Decreto Legislativo n. 138 del 2024

L'articolo 15 del Decreto Legislativo n. 138 del 2024 istituisce e descrive le funzioni e i compiti del **CSIRT Italia, il Gruppo Nazionale di Risposta agli Incidenti di Sicurezza Informatica. Questo organo opera per gestire e rispondere agli incidenti di sicurezza informatica riguardanti settori e soggetti critici elencati negli allegati al decreto, come stabilito dalle modalità definite dal CSIRT stesso. Il CSIRT è dotato di una struttura di comunicazione nazionale sicura e resiliente per consentire uno scambio rapido ed efficace di informazioni con i soggetti essenziali o importanti e con altri stakeholder rilevanti.** Il CSIRT Italia collabora attivamente a livello nazionale e internazionale, inclusa la cooperazione con comunità settoriali o intersettoriali e la partecipazione alla rete europea dei CSIRT nazionali, promuovendo una risposta integrata agli incidenti di sicurezza. **Tra i suoi compiti principali rientrano la supervisione e analisi delle minacce informatiche, la fornitura di assistenza ai soggetti essenziali, l'emissione di allerte e bollettini, e l'analisi forense degli incidenti. È anche autorizzato a svolgere scansioni proattive dei sistemi informativi di soggetti essenziali e importanti, con lo scopo di identificare vulnerabilità che potrebbero compromettere la sicurezza dei loro servizi.** Questa scansione è effettuata in modo non intrusivo e senza impatti sul funzionamento delle attività dei soggetti monitorati. Per garantire

la continuità dei suoi servizi, il CSIRT dispone di sistemi ridondanti e di spazi di lavoro di backup, oltre a mantenere un alto livello di disponibilità dei canali di comunicazione, che devono essere accessibili in qualsiasi momento, e di locali e sistemi sicuri. Al CSIRT Italia è attribuito anche il compito di sviluppare strumenti sicuri per facilitare la condivisione di informazioni, rendendo la cooperazione tra le parti più efficiente e riservata. In un'ottica di collaborazione estesa, il CSIRT Italia promuove il dialogo con i pertinenti stakeholder privati, incoraggiando l'adozione di standard comuni per la gestione degli incidenti e la divulgazione coordinata delle vulnerabilità, secondo quanto stabilito dall'articolo 16. Per supportare queste attività, è stato approvato un finanziamento annuale di 2 milioni di euro a partire dal 2025, in linea con le disposizioni dell'articolo 44 del decreto. Questa struttura avanzata permette al CSIRT di fungere da nucleo operativo e di supporto tecnico per le iniziative di sicurezza informatica in Italia, sostenendo il coordinamento delle risposte agli incidenti con altre strutture pubbliche e migliorando la resilienza del sistema cyber nazionale, in particolare tramite l'adozione di buone pratiche e l'armonizzazione delle tecniche di risposta e gestione degli incidenti tra i vari attori coinvolti.

Articolo 16 del Decreto Legislativo n. 138 del 2024

L'articolo 16 del Decreto Legislativo n. 138 del 2024 disciplina **la c.d. Divulgazione coordinata delle vulnerabilità** con l'obiettivo di gestire in modo strutturato e sicuro la comunicazione e la risoluzione delle vulnerabilità nei sistemi e nei servizi TIC -Tecnologie dell'Informazione e della Comunicazione- che possano rappresentare un rischio per la sicurezza informatica nazionale e per i soggetti coinvolti. Il CSIRT Italia è incaricato di fungere da coordinatore e intermediario di fiducia tra chi segnala una vulnerabilità, come individui o entità giuridiche, e il produttore o fornitore dei servizi o prodotti potenzialmente vulnerabili. La sua funzione di coordinamento mira a facilitare la comunicazione tra le parti e ad assistere, quando richiesto, chi segnala una vulnerabilità, sia nel contatto con il fabbricante, sia nella gestione dei tempi e delle modalità di divulgazione. Inoltre, per vulnerabilità che interessano più soggetti o che presentano rilevanza transnazionale, il CSIRT Italia può estendere la cooperazione con CSIRT di altri Stati membri, promuovendo una risposta integrata e coordinata a livello europeo.

Una caratteristica fondamentale di questa procedura è la possibilità per i segnalanti di agire in forma anonima, una disposizione che tutela il contributo degli esperti di sicurezza informatica e dei ricercatori, incoraggiando la collaborazione senza rischio di esposizione personale o professionale. Il CSIRT Italia adotta tutte le misure necessarie per mantenere l'anonimato dei segnalanti e garantisce che le azioni successive siano gestite con diligenza per massimizzare la sicurezza e minimizzare il rischio di sfruttamento delle vulnerabilità. In linea con le disposizioni della direttiva UE 2022/2555, il CSIRT Italia deve anche attuare una politica nazionale di divulgazione delle vulnerabilità, conforme alle linee guida del Gruppo di cooperazione NIS. Tale politica è supportata dall'implementazione di strumenti tecnici da parte dell'Agenzia per la Cybersicurezza Nazionale, che agevolano l'attuazione delle politiche e rafforzano la capacità di risposta del sistema italiano alle vulnerabilità, promuovendo una gestione proattiva della sicurezza informatica

Articolo 17 del Decreto Legislativo n. 138 del 2024

L'articolo 17 del Decreto Legislativo n. 138 del 2024 disciplina i c.d. **Accordi di condivisione delle informazioni sulla sicurezza informatica** con l'obiettivo di incentivare la collaborazione tra i soggetti pubblici e privati, fondamentali per prevenire e rispondere in modo efficace alle minacce informatiche. I soggetti inclusi nell'ambito di applicazione del decreto, e in alcuni casi ulteriori entità, hanno la facoltà di scambiare informazioni relative alla sicurezza informatica su base volontaria. Queste informazioni possono comprendere dati rilevanti sulle minacce informatiche, vulnerabilità, tecniche di attacco e metodi di difesa, così come raccomandazioni operative per migliorare la sicurezza, ridurre i rischi e limitare l'impatto di eventuali incidenti. Tale condivisione ha una duplice finalità: da un lato, essa mira a potenziare le capacità di prevenzione, rilevazione e risposta agli incidenti, contribuendo alla resilienza complessiva del sistema; dall'altro, promuove una maggiore consapevolezza sulle minacce e un sostegno alla ricerca e sviluppo di contromisure adeguate. La condivisione delle informazioni avviene principalmente all'interno di comunità di soggetti essenziali e importanti e, quando opportuno, con i loro fornitori, mediante accordi formali che considerano la sensibilità dei dati trattati. In questo contesto, l'Agenzia per la Cybersicurezza Nazionale -ACN-, in qualità di Autorità

nazionale competente NIS e CSIRT Italia, facilita la conclusione e l'implementazione di questi accordi. La cooperazione è ulteriormente rafforzata dall'adozione delle migliori pratiche non vincolanti elaborate dall'ENISA, che l'ACN può includere per definire gli aspetti operativi degli accordi, come l'utilizzo di piattaforme digitali specifiche e strumenti di automazione. Questo approccio garantisce un coordinamento efficace tra le autorità nazionali e i soggetti privati, consentendo uno scambio di informazioni mirato e sicuro. I soggetti essenziali e importanti devono notificare la loro partecipazione a tali accordi all'Autorità NIS al momento della loro adesione e, successivamente, in caso di ritiro. Inoltre, per agevolare un'efficace cooperazione, gli Organismi di informazione per la sicurezza (artt. 4, 6 e 7 della legge n. 124 del 2007) hanno accesso agli elenchi dei soggetti essenziali e importanti, alle notifiche di sicurezza e alle vulnerabilità individuate. L'accesso a queste informazioni, inclusa la condivisione delle notifiche di incidenti e vulnerabilità, avviene attraverso una piattaforma digitale, rendendo possibile una visione integrata e coordinata delle attività di sicurezza, in linea con le intese tra gli Organismi di informazione e l'Agenzia per la Cybersicurezza Nazionale.