LA GOVERNANCE DEL PIANO NAZIONALE DI RIPRESA E RESILIENZA – Decreto Legislativo n. 138 del 2024 – Capo IV artt. 23-33 - Obblighi in materia di gestione del rischio per la sicurezza informatica e di notifica di incidente

PNRR

Dossier

Il Capo IV del Decreto Legislativo 4 settembre 2024, n. 138, recepisce la direttiva UE 2022/2555, nota come NIS 2, e rappresenta un rafforzamento cruciale della resilienza cibernetica degli Stati membri attraverso un quadro armonizzato di obblighi per la gestione del rischio della sicurezza informatica e per la notifica degli incidenti. **Questo decreto si integra con normative chiave come il GDPR e il Regolamento UE 2019/881, il c.d. Cybersecurity Act e con la disciplina nazionale sul perimetro di sicurezza cibernetica, contenuta nel decreto-legge 21 settembre 2019, n. 105**. L'Articolo 23 assegna agli organi di amministrazione e direttivi dei soggetti essenziali e importanti un ruolo di guida strategica, imponendo loro la responsabilità di approvare e monitorare le misure di sicurezza informatica e le notifiche di incidente. Tali obblighi riflettono quanto richiesto dalla NIS 2 e dalle pratiche di *governance* sancite dagli standard internazionali ISO/IEC 27001 e 27005, che promuovono l'importanza di un coinvolgimento attivo della leadership. Gli organi direttivi devono inoltre ricevere formazione specifica, evidenziando l'importanza della competenza per l'efficace prevenzione e risposta agli incidenti. L'Articolo 24 impone ai soggetti essenziali e importanti l'adozione di misure basate su un approccio multi-rischio per proteggere i sistemi informativi, le reti e l'ambiente fisico, in linea con le *best practice* internazionali come le norme ISO/IEC 27002 e il Regolamento UE 2019/881. L'attenzione alla sicurezza della catena di approvvigionamento risponde alle raccomandazioni dell'ENISA, che enfatizzano la protezione estesa anche ai fornitori e partner esterni per mitigare le vulnerabilità lungo l'intero ecosistema tecnologico. L'Articolo 25 stabilisce la procedura di notifica degli incidenti al CSIRT Italia, in coerenza con la NIS 2 e con le norme GDPR in materia di segnalazione di violazioni dei dati. L'obbligo di pre-notifica entro 24 ore e di una notifica completa entro 72 ore consente una rapida valutazione dell'incidente e una risposta coordinata, seguendo le linee guida ISO/IEC 27035 per la gestione degli incidenti. La trasmissione di aggiornamenti intermedi e relazioni finali assicura una gestione trasparente e proattiva delle crisi. L'Articolo 26 introduce le notifiche volontarie di incidenti, minacce e quasi-incidenti, incentivando una collaborazione che migliora la capacità collettiva di risposta alle minacce informatiche e rinforza l'analisi delle tendenze, in linea con le raccomandazioni ENISA e il *framework* della NIS 2. L'Articolo 27 impone l'uso di prodotti, servizi e processi TIC certificati per dimostrare la conformità alle misure di sicurezza, con un richiamo diretto al Regolamento UE 2019/881, che istituisce l'ENISA come ente centrale per la certificazione della cybersicurezza. La norma permette anche l'adozione temporanea di

schemi di certificazione nazionali, confermando la flessibilità del quadro normativo. L'Articolo 28 promuove l'adozione di specifiche tecniche aggiornate e riconosciute a livello internazionale, in conformità al Regolamento UE 1025/2012 sulla normazione europea e alle norme ISO/IEC per assicurare coerenza e aggiornamento tecnologico. L'Articolo 29 richiede la gestione accurata dei dati di registrazione dei nomi di dominio, garantendo che i dati siano completi e trasparenti e conformi al GDPR per la protezione dei dati personali. Questa norma facilita la tracciabilità e la sicurezza, migliorando la gestione delle minacce attraverso una raccolta dati strutturata e accessibile. L'Articolo 30 impone ai soggetti di comunicare annualmente un elenco aggiornato delle attività e servizi tramite una piattaforma digitale, un obbligo che aiuta l'Autorità a monitorare e analizzare le vulnerabilità in modo efficace, supportato dalle linee guida ENISA e dalle norme ISO/IEC 31000 per la gestione del rischio. L'Articolo 31 introduce la proporzionalità e la gradualità degli obblighi, un principio cardine della NIS 2, garantendo che i requisiti siano adattati alla maturità e alle dimensioni dei soggetti, soprattutto per le PMI, assicurando che non siano gravati da obblighi eccessivi. L'Articolo 32 specifica obblighi particolari per i fornitori di servizi alla pubblica amministrazione, riflettendo il decreto-legge n. 105/2019 sul perimetro di sicurezza nazionale cibernetica, che stabilisce misure di sicurezza rigorose per le infrastrutture critiche. L'articolo permette l'esclusione di determinati soggetti dagli obblighi di notifica, mantenendo comunque un livello minimo di sicurezza per i servizi di registrazione dei nomi di dominio. L'Articolo 33 integra il presente decreto con la disciplina del perimetro di sicurezza nazionale cibernetica, coordinando gli obblighi e garantendo che le reti e i sistemi già inseriti nel perimetro siano regolati coerentemente, evitando sovrapposizioni normative e mantenendo la sicurezza nazionale come priorità. Questa armonizzazione assicura che le informazioni sensibili siano gestite con la massima riservatezza, consolidando la cooperazione tra le istituzioni e la resilienza cibernetica a livello nazionale ed europeo. **L'approccio complessivo del Capo IV, connesso alle normative correlate e alle pratiche migliori del settore, riflette un impegno verso una maggiore sicurezza e interoperabilità delle misure cibernetiche, posizionando l'Italia come parte attiva in un sistema di difesa cibernetica collettivo e coeso, in linea con le direttive europee e gli standard globali per la protezione delle infrastrutture critiche**.

Articolo 23 del Decreto Legislativo 4 settembre 2024, n. 138

L'Articolo 23 del Decreto Legislativo 4 settembre 2024, n. 138, riguarda le responsabilità e gli obblighi degli organi di amministrazione e direttivi dei soggetti essenziali e importanti in relazione alla gestione della sicurezza informatica, in conformità con la direttiva UE 2022/2555 NIS 2. Tali soggetti, essendo critici per la sicurezza e la continuità dei servizi essenziali, sono tenuti a implementare e supervisionare misure rigorose di gestione dei rischi per proteggere le loro infrastrutture digitali. Il primo comma specifica che **gli organi di amministrazione e direttivi devono approvare le modalità di implementazione delle misure di gestione dei rischi per la sicurezza informatica e sovrintendere all'adempimento degli obblighi previsti dal decreto, incluso l'articolo 7, che riguarda l'identificazione dei soggetti essenziali e importanti e la gestione della sicurezza**. **Inoltre, questi organi sono ritenuti responsabili per eventuali violazioni delle disposizioni del decreto, sottolineando la loro responsabilità personale e diretta nel garantire la conformità alle normative sulla cybersicurezza. Il secondo comma stabilisce che i membri degli organi di amministrazione e direttivi devono seguire una formazione in materia di sicurezza informatica per acquisire le competenze necessarie a comprendere e gestire i rischi. Inoltre, essi devono promuovere e garantire che i dipendenti ricevano una formazione periodica in linea con le pratiche di sicurezza adottate, con l'obiettivo di rafforzare le competenze interne nell'individuare i rischi e valutare le pratiche di gestione della sicurezza informatica. Questa formazione è essenziale per mantenere un elevato livello di consapevolezza e prontezza operativa in tutta l'organizzazione.** Il terzo comma impone agli organi di amministrazione e direttivi di essere informati periodicamente, o tempestivamente quando necessario, in merito agli incidenti di sicurezza e alle notifiche previste dagli articoli 25 e 26. Questi articoli trattano la notifica obbligatoria di incidenti significativi e la gestione delle minacce informatiche. Tale obbligo assicura che i dirigenti abbiano una visione chiara e aggiornata della situazione della sicurezza informatica, permettendo una reazione adeguata e tempestiva alle minacce e incidenti che potrebbero compromettere la continuità e la sicurezza dei servizi offerti. **L'Articolo 23 attribuisce dunque agli organi di amministrazione e direttivi dei soggetti essenziali e importanti un ruolo centrale e attivo nella supervisione e gestione della sicurezza informatica, promuovendo una cultura di consapevolezza e prontezza operativa e**

sottolineando la loro responsabilità nel garantire la protezione delle infrastrutture critiche e la continuità dei servizi.

Articolo 24 del Decreto Legislativo 4 settembre 2024, n. 138

L'Articolo 24 del Decreto Legislativo 4 settembre 2024, n. 138, stabilisce gli obblighi in materia di adozione di misure di gestione dei rischi per la sicurezza informatica da parte dei soggetti essenziali e importanti, in conformità con la direttiva UE 2022/2555 c.d. NIS 2. I soggetti interessati devono implementare misure tecniche, operative e organizzative adeguate e proporzionate per gestire i rischi alla sicurezza dei loro sistemi informativi e di rete. Queste misure devono mirare non solo a proteggere i propri sistemi, ma anche a prevenire o minimizzare l'impatto degli incidenti sui destinatari dei servizi offerti e su altri servizi correlati. Le misure adottate devono garantire un livello di sicurezza proporzionato ai rischi esistenti, basandosi sulle più recenti conoscenze e lo stato dell'arte, e devono tenere conto dei costi di attuazione e delle normative rilevanti. Devono essere proporzionate al grado di esposizione ai rischi e alle dimensioni del soggetto, considerando la probabilità e la gravità degli incidenti, compreso il loro impatto sociale ed economico. Le misure devono seguire un approccio multi-rischio per proteggere sia i sistemi informativi e di rete che l'ambiente fisico circostante e includere una serie di elementi essenziali: politiche di analisi dei rischi e sicurezza dei sistemi, gestione degli incidenti e procedure per le notifiche obbligatorie, continuità operativa e gestione delle crisi, sicurezza della catena di approvvigionamento, sicurezza nell'acquisizione e manutenzione dei sistemi, valutazioni di efficacia delle misure, pratiche di igiene informatica e formazione, uso di crittografia, politiche di controllo dell'accesso e affidabilità del personale, e soluzioni di autenticazione avanzate. **In particolare, per quanto riguarda la sicurezza della catena di approvvigionamento, i soggetti devono considerare le vulnerabilità specifiche dei propri fornitori e dei servizi offerti, valutando la qualità complessiva delle pratiche di sicurezza adottate da questi ultimi, incluse le procedure di sviluppo sicuro. Devono inoltre considerare i risultati delle valutazioni dei rischi coordinati effettuati dal Gruppo di cooperazione NIS**. Se un soggetto rileva di non essere conforme alle misure stabilite, è

obbligato ad adottare senza indebito ritardo le misure correttive necessarie per allinearsi ai requisiti. Questo obbligo assicura una risposta rapida e adeguata per colmare le lacune nella sicurezza e mantenere un alto livello di protezione dei servizi critici e delle infrastrutture cibernetiche.

Articolo 25 del Decreto Legislativo 4 settembre 2024, n. 138

L'Articolo 25 del Decreto Legislativo 4 settembre 2024, n. 138, stabilisce gli obblighi di notifica degli incidenti significativi da parte dei soggetti essenziali e importanti, in linea con la direttiva UE 2022/2555 c.d. NIS 2. Questi soggetti sono tenuti a notificare senza ingiustificato ritardo al CSIRT Italia qualsiasi incidente che abbia un impatto significativo sulla fornitura dei loro servizi. La notifica deve comprendere informazioni sufficienti per permettere al CSIRT Italia di valutare un possibile impatto transfrontaliero dell'incidente, ma non implica per il soggetto notificante un aumento della responsabilità derivante dall'incidente. **Un incidente è considerato significativo se provoca o può provocare una grave perturbazione operativa o perdite finanziarie per il soggetto, o se ha ripercussioni su altre persone fisiche o giuridiche causando perdite materiali o immateriali considerevoli. I soggetti interessati devono inviare una pre-notifica entro 24 ore dalla scoperta dell'incidente, specificando, ove possibile, se l'incidente è frutto di atti malevoli e se può avere un impatto transfrontaliero. Entro 72 ore dalla scoperta, deve seguire una notifica aggiornata con una valutazione iniziale della gravità e dell'impatto, comprendendo eventuali indicatori di compromissione. La relazione finale, da inviare entro un mese dalla notifica dell'incidente, deve includere una descrizione dettagliata dell'evento, la gravità, l'impatto, la probabile causa originaria e le misure adottate per attenuare le conseguenze, insieme a un'eventuale valutazione dell'impatto transfrontaliero. Se l'incidente è ancora in corso al momento della relazione finale, devono essere fornite relazioni mensili sui progressi fino alla sua risoluzione definitiva**. In casi particolari, come per i prestatori di servizi fiduciari, la notifica di incidenti significativi deve essere effettuata entro 24 ore dalla scoperta. Il CSIRT Italia, entro 24 ore dal ricevimento della pre-notifica, fornisce un riscontro iniziale e, su

richiesta, orientamenti tecnici per la mitigazione. Se l'incidente ha carattere criminale, il CSIRT Italia fornisce anche indicazioni per la segnalazione alle autorità di contrasto competenti. I soggetti essenziali e importanti devono, ove opportuno e in consultazione con il CSIRT Italia, comunicare tempestivamente ai destinatari dei loro servizi gli incidenti significativi e le azioni di mitigazione che possono adottare. L'Agenzia per la cybersicurezza nazionale, in qualità di Autorità nazionale competente NIS, può informare il pubblico sull'incidente per prevenire ulteriori danni o se la divulgazione è nell'interesse pubblico. Infine, l'Agenzia adotta mezzi e procedure per semplificare il processo di notifica degli incidenti e delle notifiche volontarie, mantenendo informati i soggetti essenziali e importanti su tali procedure.

Articolo 26 del Decreto Legislativo 4 settembre 2024, n. 138

L'Articolo 26 del Decreto Legislativo 4 settembre 2024, n. 138, prevede la possibilità di inviare notifiche volontarie al CSIRT Italia in aggiunta agli obblighi di notifica formale degli incidenti significativi stabiliti dall'Articolo 25. Questa misura consente ai soggetti di contribuire proattivamente alla gestione della sicurezza informatica, anche quando gli incidenti, le minacce informatiche o i quasi-incidenti non rientrano tra quelli obbligatoriamente notificabili ai sensi dell'articolo precedente. In particolare, possono trasmettere notifiche volontarie sia i soggetti essenziali e importanti, per incidenti minori o eventi rilevanti per la sicurezza non coperti dall'obbligo formale, sia altri soggetti non inclusi tra quelli indicati, indipendentemente dal fatto che rientrino o meno nell'ambito di applicazione del decreto. **Questo permette di segnalare eventi significativi che potrebbero comunque avere un impatto sulla fornitura dei servizi o sulla sicurezza collettiva.** Il CSIRT Italia gestisce queste notifiche volontarie applicando la stessa procedura stabilita per le notifiche obbligatorie descritte all'Articolo 25, ma dà priorità alle notifiche obbligatorie rispetto a quelle volontarie. Tuttavia, le notifiche volontarie vengono gestite solo se il loro trattamento non comporta un onere sproporzionato o eccessivo per il CSIRT Italia. Infine, il terzo comma specifica che, fatta salva la necessità di indagini e l'eventuale perseguimento di reati, l'invio di una notifica volontaria non implica per il soggetto notificante l'imposizione di obblighi che non avrebbe avuto in assenza di tale notifica. Questo

incoraggia la trasparenza e la condivisione di informazioni senza penalizzare i soggetti che scelgono di segnalare eventi potenzialmente rilevanti.

Articolo 27 del Decreto Legislativo 4 settembre 2024, n. 138

L'Articolo 27 del Decreto Legislativo 4 settembre 2024, n. 138, stabilisce che l'Autorità nazionale competente NIS può imporre l'uso di prodotti, servizi e processi TIC - Tecnologie dell'Informazione e della Comunicazione - certificati per dimostrare il rispetto degli obblighi relativi alla gestione della sicurezza informatica definiti nell'Articolo 24. Questa misura mira a garantire che i soggetti essenziali e importanti utilizzino tecnologie conformi agli standard di sicurezza elevati riconosciuti nell'ambito dei sistemi europei di certificazione della cybersicurezza, come previsto dall'Articolo 49 del regolamento UE 2019/881 - Regolamento sulla cibersicurezza-. L'Autorità può imporre l'uso di prodotti TIC, servizi TIC e processi TIC certificati sia che siano sviluppati internamente dai soggetti interessati sia che siano acquistati da terze parti, assicurando che essi rispondano ai requisiti di cybersicurezza stabiliti a livello europeo. Oltre a questo, l'Autorità promuove l'adozione di servizi fiduciari qualificati per rafforzare ulteriormente la sicurezza delle operazioni dei soggetti essenziali e importanti. Nel periodo di transizione in attesa dell'adozione completa dei pertinenti sistemi europei di certificazione, l'Autorità ha la facoltà di imporre l'uso di tecnologie certificate secondo schemi riconosciuti a livello nazionale o europeo. Questa disposizione garantisce che i soggetti essenziali e importanti siano pronti e protetti mediante l'adozione di pratiche e tecnologie certificate, mantenendo un elevato standard di sicurezza anche in assenza di una completa armonizzazione europea. Queste misure permettono di consolidare la fiducia nell'infrastruttura TIC utilizzata e di ridurre i rischi legati alla sicurezza informatica, assicurando la conformità ai requisiti stabiliti dal decreto e promuovendo una cultura di protezione e resilienza informatica condivisa tra i principali operatori di servizi critici.

Articolo 28 del Decreto Legislativo 4 settembre 2024, n. 138

L'Articolo 28 del Decreto Legislativo 4 settembre 2024, n. 138, riguarda la promozione dell'uso di specifiche tecniche per garantire un'attuazione efficace e armonizzata delle misure di gestione dei rischi per la sicurezza informatica, come previsto dall'Articolo 24. L'Autorità nazionale competente NIS è incaricata di incoraggiare l'adozione di specifiche tecniche europee e internazionali, senza favorire o imporre l'uso di un particolare tipo di tecnologia. Tali specifiche possono includere standard adottati da organismi di normazione riconosciuti secondo il regolamento UE 1025/2012, che disciplina la normazione europea. Per supportare questa iniziativa, l'Autorità prende in considerazione le linee guida e gli orientamenti non vincolanti elaborati dall'ENISA - Agenzia dell'Unione europea per la cibersicurezza - come previsto dalla direttiva UE 2022/2555. Inoltre, può redigere e aggiornare un elenco delle categorie di tecnologie più idonee per l'implementazione delle misure di gestione dei rischi per la sicurezza informatica. Questo elenco, pur non essendo vincolante o esaustivo, serve come strumento di orientamento per i soggetti interessati. L'elenco aggiornato è pubblicato sul sito dell'Agenzia per la cybersicurezza nazionale e fornisce una guida sulle specifiche tecniche e sulle norme di settore nazionali ed europee applicabili. Tale elenco è destinato ai soggetti classificati negli allegati I, II, III e IV del decreto, offrendo loro indicazioni utili per migliorare la conformità e l'efficacia delle loro misure di gestione dei rischi per la sicurezza informatica. Questa disposizione mira a garantire un quadro armonizzato e basato sulle migliori pratiche internazionali per la protezione dei sistemi informativi e di rete, contribuendo così a un livello comune elevato di cibersicurezza nell'Unione.

Articolo 29 del Decreto Legislativo 4 settembre 2024, n. 138

L'Articolo 29 del Decreto Legislativo 4 settembre 2024, n. 138, stabilisce le disposizioni per la gestione dei dati di registrazione dei nomi di dominio, con l'obiettivo di rafforzare la sicurezza,

la stabilità e la resilienza dei sistemi di nomi di dominio. I gestori di registri dei nomi di dominio di primo livello –TLD- e i fornitori di servizi di registrazione devono raccogliere e mantenere accurati e completi i dati di registrazione in una banca dati apposita, rispettando le normative dell'Unione Europea sulla protezione dei dati personali. La banca dati deve includere le informazioni necessarie per identificare e contattare i titolari dei nomi di dominio e i punti di contatto amministrativi. Tra le informazioni minime richieste vi sono: il nome di dominio, la data di registrazione, i dati di contatto del registrante (nome, e-mail e numero di telefono), e i dati di contatto amministrativi, se diversi. I gestori devono implementare e rendere pubbliche politiche e procedure, comprese le procedure di verifica, per garantire l'accuratezza e la completezza delle informazioni contenute nelle banche dati. Inoltre, i gestori di registri e i fornitori di servizi di registrazione devono rendere pubblicamente disponibili i dati di registrazione non personali senza ritardi ingiustificati dopo la registrazione di un nome di dominio. **Per quanto riguarda l'accesso ai dati, su richiesta motivata di soggetti legittimati, i gestori e i fornitori devono fornire accesso ai dati specifici nel rispetto della normativa europea sulla protezione dei dati. Devono rispondere alle richieste entro 72 ore dalla ricezione, fornendo i dati richiesti o spiegando perché la richiesta non è stata ritenuta legittima o debitamente motivata. Le politiche di divulgazione dei dati devono essere pubblicamente disponibili. L'Agenzia per la cybersicurezza nazionale ha la facoltà di richiedere l'accesso ai dati di registrazione e può stipulare protocolli con i gestori e i fornitori per facilitare l'accesso**. Infine, per evitare duplicazioni nella raccolta dei dati, i gestori e i fornitori sono tenuti a collaborare e a stabilire procedure congiunte per la raccolta e la manutenzione dei dati di registrazione. **Queste disposizioni mirano a garantire un sistema di gestione dei dati di registrazione efficace e trasparente, proteggendo al contempo la riservatezza dei dati personali e favorendo la sicurezza e l'affidabilità dei sistemi di nomi di dominio.**

Articolo 30 del Decreto Legislativo 4 settembre 2024, n. 138

L'Articolo 30 del Decreto Legislativo 4 settembre 2024, n. 138, disciplina il processo di elencazione, caratterizzazione e categorizzazione delle attività e dei servizi dei soggetti essenziali e importanti, in relazione agli obblighi di gestione dei rischi per la sicurezza informatica previsti dall'Articolo 24. **Dal 1° maggio al 30 giugno di ogni anno, a partire dalla ricezione della prima comunicazione iniziale, i soggetti interessati devono comunicare e aggiornare un elenco dettagliato delle proprie attività e servizi tramite la piattaforma digitale designata. Questo elenco deve includere tutti gli elementi necessari per la caratterizzazione delle attività e l'attribuzione di una categoria di rilevanza. L'Autorità nazionale competente NIS è responsabile della definizione delle categorie di rilevanza e del processo, dei criteri e delle modalità per la compilazione, caratterizzazione e categorizzazione delle attività e dei servizi.** Entro novanta giorni dalla comunicazione tramite la piattaforma, l'Autorità fornisce riscontro ai soggetti interessati circa la conformità delle informazioni trasmesse. Questo termine può essere prorogato una sola volta, fino a un massimo di sessanta giorni, se sono necessari ulteriori approfondimenti. Se l'Autorità richiede integrazioni o informazioni aggiuntive, il termine è sospeso fino alla ricezione delle stesse, che devono essere fornite dai soggetti entro trenta giorni. Nel caso in cui l'Autorità non fornisca riscontro entro i termini stabiliti, la conformità delle informazioni comunicate si intende automaticamente convalidata. Per eseguire le attività previste, l'Autorità può avvalersi dei tavoli settoriali, strutture collaborative previste per facilitare il coordinamento e il confronto tra i diversi attori coinvolti. **Questa procedura garantisce che i soggetti essenziali e importanti mantengano aggiornate le loro informazioni e rispettino i criteri di gestione dei rischi, contribuendo alla sicurezza complessiva delle infrastrutture critiche**.

Articolo 31 del Decreto Legislativo 4 settembre 2024, n. 138

L'Articolo 31 del Decreto Legislativo 4 settembre 2024, n. 138, disciplina l'applicazione proporzionata e graduale degli obblighi relativi alla gestione della sicurezza informatica per i soggetti essenziali e importanti. Questi obblighi riguardano vari aspetti delineati negli articoli 23, 24, 25, 27, 28 e 29, e sono stabiliti dall'Autorità nazionale competente NIS in modo da tenere conto del grado di esposizione ai rischi, delle dimensioni dei soggetti interessati e della probabilità e gravità degli incidenti, inclusi gli impatti sociali ed economici. L'Autorità definisce termini, modalità, specifiche e tempi di implementazione che possono variare in base alle categorie di rilevanza delle attività e servizi come definite dall'Articolo 30, al settore e alla tipologia di soggetto, considerando anche il livello di maturità iniziale in ambito di sicurezza informatica e se il soggetto è classificato come essenziale o importante. Questi criteri permettono di adattare gli obblighi alle caratteristiche specifiche di ciascun soggetto, promuovendo un approccio differenziato e calibrato. L'Autorità può anche individuare le circostanze che portano alla sospensione dei termini per l'implementazione degli obblighi e può emanare linee guida vincolanti per agevolare l'attuazione delle disposizioni. Inoltre, l'Autorità ha il potere di emettere raccomandazioni per supportare i soggetti nel conformarsi agli obblighi, garantendo un'implementazione più agevole e consapevole. Per facilitare l'interazione e il coordinamento, l'Autorità può utilizzare i tavoli settoriali previsti dall'Articolo 11, che servono come piattaforme di confronto tra le parti coinvolte. Le comunicazioni tra i soggetti e l'Autorità avvengono principalmente attraverso una piattaforma digitale dedicata, come stabilito all'Articolo 7, per assicurare una gestione efficiente e centralizzata delle informazioni. Questa struttura garantisce un approccio flessibile e pratico all'implementazione degli obblighi, tenendo conto delle peculiarità di ciascun soggetto e delle dinamiche settoriali.

Articolo 32 del Decreto Legislativo 4 settembre 2024, n. 138

L'Articolo 32 del Decreto Legislativo 4 settembre 2024, n. 138, prevede disposizioni specifiche per settori particolari, con particolare attenzione ai servizi forniti alla pubblica amministrazione. **L'Autorità nazionale competente NIS, tenendo conto degli impatti sociali ed economici di un eventuale incidente significativo nella catena di approvvigionamento, può imporre obblighi specifici, proporzionati e graduali ai soggetti essenziali e importanti che forniscono servizi, inclusi quelli digitali, alla pubblica amministrazione. Questi obblighi mirano a garantire un livello adeguato di sicurezza informatica, adattato alla criticità dei servizi forniti al settore pubblico. L'Autorità può anche identificare, seguendo procedure specifiche, obblighi del capo in questione che non si applicano a determinate amministrazioni pubbliche o a specifici soggetti elencati nell'Allegato III e all'Articolo 3, commi 8, 9 (lettera f) e 10). Ciò consente una certa flessibilità normativa per adattare gli obblighi alle esigenze di specifici settori o tipologie di soggetti**. Gli articoli 24 e 25, che trattano della gestione dei rischi e della notifica degli incidenti, non si applicano ai soggetti che forniscono esclusivamente servizi di registrazione dei nomi di dominio. Tuttavia, tali soggetti devono comunque mantenere un livello di sicurezza informatica coerente con gli obblighi di gestione dei rischi e notifica degli incidenti previsti da questi articoli, garantendo così una protezione di base anche se esonerati formalmente dagli obblighi specifici. Infine, l'articolo chiarisce che la designazione o la mancata designazione di un rappresentante, come indicato all'Articolo 5, comma 3, non influisce sull'applicabilità degli obblighi previsti dal capo in questione. Questo assicura che gli obblighi di sicurezza informatica rimangano in vigore indipendentemente da dettagli specifici relativi alla rappresentanza legale o istituzionale dei soggetti coinvolti.

Articolo 33 del Decreto Legislativo 4 settembre 2024, n. 138

L'Articolo 33 del Decreto Legislativo 4 settembre 2024, n. 138, stabilisce il coordinamento tra le disposizioni del presente decreto e la normativa sul perimetro di sicurezza nazionale cibernetica, delineata dal decreto-legge 21 settembre 2019, n. 105, convertito dalla legge 18 novembre 2019, n. 133. Questo coordinamento è necessario per armonizzare le misure di gestione della sicurezza informatica e le procedure di notifica degli incidenti tra le normative esistenti, evitando duplicazioni e sovrapposizioni. In primo luogo, l'articolo specifica che gli obblighi di gestione del rischio e notifica di incidente previsti dal decreto-legge n. 105/2019 sono considerati equivalenti a quelli indicati nel presente decreto. Ciò significa che i soggetti già conformi alle normative del perimetro di sicurezza nazionale cibernetica soddisfano anche i requisiti del nuovo decreto. Le reti, i sistemi informativi e i servizi informatici inclusi nell'elenco del perimetro di sicurezza nazionale non sono soggetti alle disposizioni del presente decreto, ad eccezione dei sistemi informativi e di rete non inclusi in tale elenco, per i quali rimangono validi gli obblighi del nuovo decreto. I soggetti individuati dal decreto-legge n. 105/2019 non sono tenuti a notificare incidenti ai sensi dell'Articolo 25 del presente decreto se tali incidenti sono già stati segnalati secondo le norme del decreto-legge n. 105/2019. Inoltre, le informazioni relative a questi soggetti o fornite da essi all'Agenzia per la cybersicurezza nazionale possono essere esentate dagli obblighi di comunicazione previsti dall'Articolo 22 del presente decreto. **Queste disposizioni mirano a garantire un'integrazione efficace tra le normative esistenti in materia di sicurezza cibernetica, evitando duplicazioni di obblighi per i soggetti interessati e assicurando che le norme si applichino in modo coerente e armonizzato, mantenendo comunque alti standard di protezione per la sicurezza nazionale e la resilienza informatica.**