Decreto legislativo 04/09/2024, n. 138

Recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148.
Pubblicato nella Gazz. Uff. 1° ottobre 2024, n. 230.

Epigrafe

Decreto legislativo 4 settembre 2024 n. 138[1]

Recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148.

Note:

[1]Pubblicato nella Gazz. Uff. 1° ottobre 2024, n. 230.

Capo IV

Obblighi in materia di gestione del rischio per la sicurezza informatica e di notifica di incidente[7]

Art. 23. Organi di amministrazione e direttivi[8]

In vigore dal 16 ottobre 2024

1. Gli organi di amministrazione e gli organi direttivi dei soggetti essenziali e dei soggetti importanti:
   a) approvano le modalità di implementazione delle misure di gestione dei rischi per la sicurezza informatica adottate da tali soggetti ai sensi dell'articolo 24;
   b) sovrintendono all'implementazione degli obblighi di cui al presente capo e di cui all'articolo 7;
   c) sono responsabili delle violazioni di cui al presente decreto.
2. Gli organi di amministrazione e gli organi direttivi dei soggetti essenziali e dei soggetti importanti:
   a) sono tenuti a seguire una formazione in materia di sicurezza informatica;
   b) promuovono l'offerta periodica di una formazione coerente a quella di cui alla lettera a) ai loro dipendenti, per favorire l'acquisizione di conoscenze e competenze sufficienti al fine di individuare i rischi e valutare le pratiche di gestione dei rischi per la sicurezza informatica e il loro impatto sulle attività del soggetto e sui servizi offerti.
3. Gli organi di amministrazione e gli organi direttivi dei soggetti essenziali e dei soggetti importanti sono informati su base periodica o, se opportuno, tempestivamente, degli incidenti e delle notifiche di cui agli articoli 25 e 26.

7Sull'applicabilità delle disposizioni del presente Capo vedi l'art. 15, comma 1, D.Lgs. 10 marzo 2025, n. 23

8Sull'applicabilità delle disposizioni del Capo IV, di cui il presente articolo è parte, vedi l'art. 15, comma 1, D.Lgs. 10 marzo 2025, n. 23.

Art. 24. Obblighi in materia di misure di gestione dei rischi per la

sicurezza informatica[9]

In vigore dal 16 ottobre 2024

1. I soggetti essenziali e i soggetti importanti adottano misure tecniche, operative e organizzative adeguate e proporzionate, secondo le modalità e i termini di cui agli articoli 30, 31 e 32, alla gestione dei rischi posti alla sicurezza dei sistemi informativi e di rete che tali soggetti utilizzano nelle loro attività o nella fornitura dei loro servizi, nonché per prevenire o ridurre al minimo l'impatto degli incidenti per i destinatari dei loro servizi e per altri servizi. Tali misure:

a) assicurano un livello di sicurezza dei sistemi informativi e di rete adeguato ai rischi esistenti, tenuto conto delle conoscenze più aggiornate e dello stato dell'arte in materia e, ove applicabile, delle pertinenti norme nazionali, europee e internazionali, nonché dei costi di attuazione;

b) sono proporzionate al grado di esposizione a rischi del soggetto, alle dimensioni del soggetto e alla probabilità che si verifichino incidenti, nonché alla loro gravità, compreso il loro impatto sociale ed economico.

2. Le misure di cui al comma 1 sono basate su un approccio multi-rischio, volto a proteggere i sistemi informativi e di rete nonché il loro ambiente fisico da incidenti, e comprendono almeno i seguenti elementi:

a) politiche di analisi dei rischi e di sicurezza dei sistemi informativi e di rete;

b) gestione degli incidenti, ivi incluse le procedure e gli strumenti per eseguire le notifiche di cui agli articoli 25 e 26;

c) continuità operativa, ivi inclusa la gestione di backup, il ripristino in caso di disastro, ove applicabile, e gestione delle crisi;

d) sicurezza della catena di approvvigionamento, ivi compresi gli aspetti relativi alla sicurezza riguardanti i rapporti tra ciascun soggetto e i suoi diretti fornitori o fornitori di servizi;

e) sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informativi e di rete, ivi comprese la gestione e la divulgazione delle vulnerabilità;

f) politiche e procedure per valutare l'efficacia delle misure di gestione dei rischi per la sicurezza informatica;

g) pratiche di igiene di base e di formazione in materia di sicurezza informatica;

h) politiche e procedure relative all'uso della crittografia e, ove opportuno, della cifratura;

i) sicurezza e affidabilità del personale, politiche di controllo dell'accesso e gestione dei beni e degli assetti;

l) uso di soluzioni di autenticazione a più fattori o di autenticazione continua, di comunicazioni vocali, video e testuali protette, e di sistemi di comunicazione di emergenza protetti da parte del soggetto al proprio interno, ove opportuno.

3. Nel valutare quali misure di cui al comma 2, lettera d), siano adeguate, i soggetti tengono conto delle vulnerabilità specifiche per ogni diretto fornitore e fornitore di servizi e della qualità complessiva dei prodotti e delle pratiche di sicurezza informatica dei propri fornitori e fornitori di servizi, comprese le loro procedure di sviluppo sicuro. Per la medesima finalità i soggetti tengono altresì conto dei risultati delle valutazioni coordinate dei rischi per la sicurezza delle catene di approvvigionamento critiche effettuate dal Gruppo di cooperazione NIS.

4. Qualora un soggetto rilevi di non essere conforme alle misure di cui al comma 2, esso adotta, senza indebito ritardo, tutte le misure appropriate e proporzionate correttive necessarie.

[9] Sull'applicabilità delle disposizioni del Capo IV, di cui il presente articolo è parte, vedi l'art. 15, comma 1, D.Lgs. 10 marzo 2025, n. 23.

Art. 25. Obblighi in materia di notifica di incidente[10]

In vigore dal 16 ottobre 2024

1. I soggetti essenziali e i soggetti importanti notificano, senza ingiustificato ritardo, al CSIRT Italia ogni incidente che, ai sensi del comma 4, ha un impatto significativo sulla fornitura dei loro servizi, secondo le modalità e i termini di cui agli articoli 30, 31 e 32.

2. Le notifiche includono le informazioni che consentono al CSIRT Italia di determinare un eventuale impatto transfrontaliero dell'incidente.

3. La notifica non espone il soggetto che la effettua a una maggiore responsabilità rispetto a quella derivante dall'incidente.

4. Un incidente è considerato significativo se:

a) ha causato o è in grado di causare una grave perturbazione operativa dei servizi o perdite finanziarie per il soggetto interessato;

b) ha avuto ripercussioni o è idoneo a provocare ripercussioni su altre persone fisiche o giuridiche causando perdite materiali o immateriali considerevoli.

5. Ai fini della notifica di cui al comma 1, i soggetti interessati trasmettono al CSIRT Italia:

a) senza ingiustificato ritardo, e comunque entro 24 ore da quando sono venuti a conoscenza dell'incidente significativo, una pre-notifica che, ove possibile, indichi se l'incidente significativo possa ritenersi il risultato di atti illegittimi o malevoli o può avere un impatto transfrontaliero;

b) senza ingiustificato ritardo, e comunque entro 72 ore da quando sono venuti a conoscenza dell'incidente significativo, una notifica dell'incidente che, ove possibile, aggiorni le informazioni di cui alla lettera a) e indichi una valutazione iniziale dell'incidente significativo, comprensiva della sua gravità e del suo impatto, nonché, ove disponibili, gli indicatori di compromissione;

c) su richiesta del CSIRT Italia, una relazione intermedia sui pertinenti aggiornamenti della situazione;

d) una relazione finale entro un mese dalla trasmissione della notifica dell'incidente di cui alla lettera b), che comprenda:

1) una descrizione dettagliata dell'incidente, ivi inclusi la sua gravità e il suo impatto;

2) il tipo di minaccia o la causa originale (root cause) che ha probabilmente innescato l'incidente;

3) le misure di attenuazione adottate e in corso;

4) ove noto, l'impatto transfrontaliero dell'incidente;

e) in caso di incidente in corso al momento della trasmissione della relazione finale di cui alla lettera d), una relazione mensile sui progressi e una relazione finale entro un mese dalla conclusione della gestione dell'incidente.

6. In deroga a quanto previsto dal comma 5, lettera b), un prestatore di servizi fiduciari, in relazione a incidenti significativi che abbiano un impatto sulla fornitura dei suoi servizi fiduciari, provvede alla notifica di cui alla medesima lettera, senza indebito ritardo e comunque entro 24 ore da quando sono venuti a conoscenza dell'incidente significativo.

7 . Fermo restando quanto previsto dall'articolo 15, comma 4, senza ingiustificato ritardo e ove possibile entro 24 ore dal ricevimento della pre-notifica di cui al comma 5, lettera a), il CSIRT Italia fornisce una risposta al soggetto notificante, comprensiva di un riscontro iniziale sull'incidente significativo e, su richiesta del soggetto, orientamenti o consulenza sull'attuazione di possibili misure tecniche di mitigazione. Su richiesta del soggetto notificante, il CSIRT Italia fornisce ulteriore supporto tecnico.

8. Qualora si sospetti che l'incidente significativo abbia carattere criminale, il CSIRT Italia fornisce al

soggetto notificante anche orientamenti sulla segnalazione dell'incidente significativo, all'organo centrale del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione, di cui all'articolo 7-bis del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155 (Autorità di contrasto).

9. Sentito il CSIRT Italia, se ritenuto opportuno e qualora possibile, i soggetti essenziali e i soggetti importanti comunicano, senza ingiustificato ritardo, ai destinatari dei loro servizi gli incidenti significativi che possono ripercuotersi negativamente sulla fornitura di tali servizi.

10. I soggetti essenziali e i soggetti importanti, se ritenuto opportuno e qualora possibile, sentito il CSIRT Italia, comunicano senza ingiustificato ritardo, ai destinatari dei loro servizi che sono potenzialmente interessati da una minaccia informatica significativa, misure o azioni correttive o di mitigazione che tali destinatari possono adottare in risposta a tale minaccia. Inoltre, sentito il CSIRT Italia, se ritenuto opportuno, i soggetti essenziali e i soggetti importanti comunicano ai medesimi destinatari anche la natura di tale minaccia informatica significativa.

11. L'Agenzia per la cybersicurezza nazionale, nello svolgimento delle funzioni di Autorità nazionale competente NIS e di CSIRT Italia, anche sentendo, se del caso, le autorità competenti e gli CSIRT nazionali degli altri Stati membri interessati, può informare il pubblico riguardo all'incidente significativo per evitare ulteriori incidenti significativi o per gestire un incidente significativo in corso, o qualora ritenga che la divulgazione dell'incidente significativo sia altrimenti nell'interesse pubblico.

12. L'Agenzia per la cybersicurezza nazionale adotta mezzi tecnici e relative procedure per semplificare le notifiche di cui al presente articolo e le notifiche volontarie di cui all'articolo 26, informando i soggetti essenziali e i soggetti importanti.

10Sull'applicabilità delle disposizioni del Capo IV, di cui il presente articolo è parte, vedi l'art. 15, comma 1, D.Lgs. 10 marzo 2025, n. 23.