Consiglio
dell'Unione europea

Bruxelles, 13 marzo 2024
(OR. en)

7721/24

ENER 134
ENV 295
CLIMA 114
COMPET 320
CONSOM 104
FISC 51
CYBER 88
DELACT 55

NOTA DI TRASMISSIONE

Origine:	Segretaria generale della Commissione europea, firmato da Martine DEPREZ, direttrice
Data:	11 marzo 2024
Destinatario:	Thérèse BLANCHET, segretaria generale del Consiglio dell'Unione europea
n. doc. Comm.:	C(2024) 1383 final
Oggetto:	REGOLAMENTO DELEGATO (UE) …/... DELLA COMMISSIONE del 11.3.2024 che integra il regolamento (UE) 2019/943 del Parlamento europeo e del Consiglio istituendo un codice di rete relativo a disposizioni settoriali per gli aspetti di cibersicurezza dei flussi transfrontalieri di energia elettrica

Si trasmette in allegato, per le delegazioni, il documento C(2024) 1383 final.

All.: C(2024) 1383 final

COMMISSIONE
EUROPEA

Bruxelles, 11.3.2024
C(2024) 1383 final

REGOLAMENTO DELEGATO (UE) …/... DELLA COMMISSIONE

del 11.3.2024

che integra il regolamento (UE) 2019/943 del Parlamento europeo e del Consiglio istituendo un codice di rete relativo a disposizioni settoriali per gli aspetti di cibersicurezza dei flussi transfrontalieri di energia elettrica

(Testo rilevante ai fini del SEE)

RELAZIONE

1. CONTESTO DELL'ATTO DELEGATO

La presente iniziativa è stata identificata quale importante misura per migliorare la resilienza delle infrastrutture e dei servizi energetici critici nelle comunicazioni della Commissione sull'integrazione del sistema energetico[1], sulla strategia per l'Unione della sicurezza[2] e sulla strategia per la cibersicurezza[3]. Essa si basa sui poteri che il Parlamento europeo e il Consiglio hanno conferito alla Commissione nel regolamento (UE) 2019/943[4] (regolamento sull'energia elettrica) per elaborare norme settoriali specifiche ("codice di rete") per gli aspetti relativi alla cibersicurezza dei flussi transfrontalieri di energia elettrica. Si tratterà soprattutto di norme relative ai requisiti minimi comuni, alla pianificazione, al monitoraggio, alla rendicontazione e alla gestione delle crisi.

Il codice di rete sugli aspetti di cibersicurezza dei flussi transfrontalieri di energia elettrica includerà norme su vari aspetti legati alla cibersicurezza dell'energia elettrica, quali:

- un processo completo di gestione del rischio transfrontaliero;
- ruoli e competenze chiari;
- controlli minimi e avanzati di cibersicurezza (mappati in riferimento a norme europee e internazionali selezionate);
- flussi di condivisione delle informazioni sulla cibersicurezza per garantire informazioni tempestive e una risposta rapida e coordinata da parte dei pertinenti portatori di interessi;
- norme sulla gestione degli attacchi informatici e delle crisi;
- un quadro di esercitazioni in materia di cibersicurezza per rafforzare la preparazione di tutti gli operatori;
- norme per la protezione dello scambio di informazioni;
- un quadro di riferimento per il monitoraggio, la comparazione e la rendicontazione.

Il codice di rete mira a stabilire un processo ricorrente di valutazione del rischio per la cibersicurezza nel settore dell'energia elettrica. Le valutazioni mireranno a individuare sistematicamente i soggetti che eseguono processi digitalizzati con un impatto critico o elevato nei flussi transfrontalieri di energia elettrica, i loro rischi per la cibersicurezza e le necessarie misure di mitigazione che devono attuare. Oggi nel settore della cibersicurezza esistono diverse metodologie e norme. Si tratta inoltre di un campo di conoscenza in rapida evoluzione. Con l'obiettivo di armonizzare e garantire una base comune rispettando il più possibile le pratiche e gli investimenti esistenti, il codice di rete stabilisce quindi un modello di governance per sviluppare, seguire e rivedere regolarmente le metodologie dei diversi portatori di interessi. Questo modello di governance e di contributo dei portatori di interessi tiene conto degli attuali mandati dei diversi organismi dei sistemi di regolamentazione della cibersicurezza e dell'energia elettrica.

---

1 COM(2020) 299 final.
2 COM(2020) 605 final.
3 Nuova strategia dell'UE per la cibersicurezza.
4 Regolamento (UE) 2019/943 del Parlamento europeo e del Consiglio, del 5 giugno 2019, sul mercato interno dell'energia elettrica (rifusione) (GU L 158 del 14.6.2019, pag. 54).

Dal momento che la tecnologia è in continua evoluzione e il settore dell'energia elettrica è in rapida digitalizzazione, il codice di rete evita di pregiudicare l'innovazione e di costituire un ostacolo all'accesso di nuovi soggetti al mercato dell'energia elettrica e al conseguente utilizzo di soluzioni innovative che possano contribuire a rendere più efficiente il sistema elettrico. Nell'ambito di tale obiettivo, tutti i nuovi sistemi, processi e procedure devono rispettare i requisiti di cibersicurezza. Al fine di individuare le nuove tendenze e i possibili rischi futuri per la cibersicurezza, si procederà a una rendicontazione periodica con una relazione completa di valutazione del rischio per la cibersicurezza dell'energia elettrica a livello transfrontaliero, prevista dal codice di rete ed effettuata almeno a cadenza triennale.

Le misure previste dal codice di rete sono importanti per migliorare la sicurezza dell'approvvigionamento di energia elettrica nell'UE. Il presente regolamento delegato definirà norme armonizzate applicabili a tutti gli operatori del settore in tutti gli Stati membri. Esso mirerà a raggiungere gli obiettivi garantendo parità di condizioni. Contribuirà inoltre a integrare il mercato dell'energia elettrica dell'UE in modo non discriminatorio e a garantire un'effettiva concorrenza.

Gli obiettivi della presente iniziativa non possono essere raggiunti a livello nazionale, perché si concentra sui flussi transfrontalieri di energia elettrica e si riferisce alle reti energetiche interconnesse in tutta Europa.

Il presente regolamento intende:

- stabilire norme relative alla governance degli aspetti di cibersicurezza dei flussi transfrontalieri di energia elettrica per garantire l'affidabilità del sistema elettrico e la stretta collaborazione con le strutture di governance esistenti per la cibersicurezza;
- determinare criteri comuni per l'esecuzione di valutazioni del rischio per la cibersicurezza per l'affidabilità operativa del sistema elettrico in relazione ai flussi transfrontalieri di energia elettrica;
- promuovere un quadro comune di cibersicurezza dell'energia elettrica e, di conseguenza, favorire un livello minimo comune di cibersicurezza dell'energia elettrica in tutta l'Unione;
- definire meccanismi per valutare l'applicazione dei controlli minimi e avanzati di cibersicurezza sui sistemi che possono influire sui flussi transfrontalieri di energia elettrica;
- stabilire i flussi di informazioni attraverso la definizione di norme per la raccolta e la condivisione di informazioni in relazione ai flussi transfrontalieri di energia elettrica, compatibili con le altre legislazioni nazionali e dell'UE;
- stabilire processi efficaci per identificare, classificare e rispondere agli attacchi informatici che hanno un impatto sui flussi transfrontalieri di energia elettrica;
- istituire processi efficaci per la gestione delle crisi transfrontaliere dell'energia elettrica legate agli attacchi informatici;
- definire principi comuni per le esercitazioni di cibersicurezza dell'energia elettrica per aumentare la resilienza e migliorare la preparazione ai rischi del settore dell'energia elettrica;
- proteggere le informazioni scambiate ai sensi del presente regolamento;

- definire un processo per il monitoraggio dell'attuazione del presente regolamento, al fine di valutare l'efficacia degli investimenti nella protezione della cibersicurezza e di riferire sui progressi della protezione della cibersicurezza in tutta l'Unione; nonché
- garantire che le raccomandazioni sulle specifiche relative alla cibersicurezza negli appalti pubblici rilevanti per i flussi transfrontalieri di energia elettrica non pregiudichino l'innovazione e nuovi sistemi, processi e procedure.

2. CONSULTAZIONI PRECEDENTI L'ADOZIONE DELL'ATTO

Gli articoli 59 e 61 del regolamento (UE) 2019/943 stabiliscono norme dettagliate sull'elaborazione dei codici di rete, assegnando ruoli specifici all'Agenzia per la cooperazione fra i regolatori nazionali dell'energia (ACER), alla Rete europea di gestori di sistemi di trasmissione dell'energia elettrica (ENTSO per l'energia elettrica) e all'ente europeo dei gestori dei sistemi di distribuzione di energia elettrica dell'UE (EU DSO). Il regolamento include inoltre norme specifiche sulle consultazioni dettagliate di tutti i pertinenti portatori di interessi. Gli articoli 31 e 56 prevedono l'obbligo di un'ampia consultazione dei portatori di interessi durante l'elaborazione del codice di rete.

Il codice di rete è il primo codice elaborato sulla base delle nuove norme stabilite dal regolamento (UE) 2019/943, con particolare riguardo al disposto dell'articolo 59. Le responsabilità nell'ambito del processo formale di elaborazione del codice di rete sono assegnate all'ENTSO per l'energia elettrica, all'EU DSO e ad ACER. Il codice di rete sarà il primo ad essere (co)redatto dall'ENTSO per l'energia elettrica e dall'EU DSO.

Prima dell'avvio del processo ufficiale di elaborazione del codice di rete, all'inizio del 2020 ha preso il via un lavoro informale sotto la guida della direzione generale dell'Energia, che si è conclusa con una relazione tecnica all'inizio del 2021.

L'ACER ha poi elaborato orientamenti quadro nel periodo marzo-luglio 2021. Nel marzo 2021 i gestori dei sistemi di trasmissione e i gestori dei sistemi di distribuzione, con il supporto dell'ACER, della Commissione e dell'Agenzia dell'Unione europea per la cibersicurezza, hanno istituito diversi sottogruppi congiunti per sviluppare il contenuto tecnico delle principali aree che dovevano essere coperte dagli orientamenti quadro dell'ACER e successivamente dal codice di rete. Nell'aprile 2021 l'ACER ha condotto una consultazione pubblica di 2 mesi sul progetto di orientamenti quadro, invitando i portatori di interessi a condividere le loro opinioni. Sono pervenute 42 risposte, la maggior parte delle quali da parte di aziende o associazioni del settore energetico con sede negli Stati membri dell'UE. Secondo l'ACER, è emerso dai contributi il favore dei partecipanti per il progetto di orientamenti quadro; l'88 % ritiene che gli orientamenti contribuiscano a proteggere ulteriormente i flussi transfrontalieri di energia elettrica; il 65 % afferma che esistono ancora lacune nella cibersicurezza dei flussi transfrontalieri di energia elettrica, che il progetto di orientamenti dovrebbe colmare. A seguito del riscontro ricevuto, l'ACER ha riesaminato il contenuto del progetto di orientamenti in consultazione con i portatori di interessi, in particolare con l'ENTSO per l'energia elettrica e l'EU DSO, presentandoli alla Commissione il 27 luglio 2021.

Il processo di sviluppo della rete, come stabilito dall'articolo 59 del regolamento (UE) 2019/943, prevede un ampio coinvolgimento dei portatori di interessi e un comitato di redazione specifico per aiutare l'ENTSO per l'energia elettrica e l'EU DSO a redigere il codice di rete. Ai sensi dell'articolo 59, paragrafo 10, del regolamento (UE) 2019/943, l'8 settembre 2021 l'ENTSO per l'energia elettrica ha istituito il comitato di redazione per avviare il processo formale di redazione. Tenendo conto dei suggerimenti dei portatori di interessi di cui

all'articolo 59 e della lettera della Commissione all'ENTSO per l'energia elettrica del 23 luglio 2021, quest'ultima ha chiesto formalmente ai pertinenti portatori di interessi di nominare un rappresentante nel comitato di redazione per partecipare attivamente alle riunioni mensili ed esaminare i progressi.

L'ENTSO per l'energia elettrica e l'EU DSO hanno condotto una consultazione pubblica[5] della durata di un mese, dal 12 novembre al 10 dicembre 2021, sul progetto di codice di rete. Il 19 novembre e l'8 dicembre 2021 si sono tenuti due seminari pubblici per i portatori di interessi. Quando necessario, l'ENTSO per l'energia elettrica e l'EU DSO hanno inoltre tenuto riunioni ad hoc e scambiato opinioni con le parti interessate. Ciò è avvenuto prima che la proposta finale del codice di rete fosse presentata all'ACER per il riesame il 14 gennaio 2022.

Nel periodo gennaio-luglio 2022, l'ACER ha riesaminato il codice di rete proposto per garantire che fosse conforme ai pertinenti orientamenti quadro e che contribuisse all'integrazione del mercato, alla non discriminazione, all'effettiva concorrenza e al funzionamento efficace del mercato. Durante il riesame, l'ACER ha condotto ampie consultazioni con i pertinenti portatori di interessi[6] in audizioni specifiche e ha tenuto conto delle opinioni fornite da tutte le parti coinvolte nella redazione della proposta, coordinate dall'ENTSO per l'energia elettrica e dall'EU DSO

La Commissione ha tenuto conto delle osservazioni ricevute e ha riesaminato il regolamento delegato rispetto al progetto presentato dall'ACER. Nel fare ciò, la Commissione ha anche cercato assistenza dal 23 maggio al 20 giugno 2023 attraverso opportune e tempestive consultazioni a livello di esperti con il gruppo di coordinamento per l'energia elettrica. Ciò è previsto dalla procedura della delega per l'adozione di misure di applicazione generale che integrano o modificano alcuni elementi non essenziali del regolamento (UE) 2019/943. Non era previsto alcun voto o parere formale da parte del gruppo. Parallelamente, il Parlamento europeo e il Consiglio sono stati informati contemporaneamente agli esperti degli Stati membri, in linea con l'accordo interistituzionale "Legiferare meglio" del 2016 e la convenzione d'intesa sugli atti delegati ad esso allegata[7]. Oltre al gruppo di coordinamento per l'energia elettrica, la DG ENER, in collaborazione con la DG CONNECT e l'Agenzia dell'Unione europea per la cibersicurezza, ha consultato anche il gruppo di cooperazione sui sistemi informatici e di rete (NIS) (flusso di lavoro sull'energia). La Commissione ha completato la fase successiva della procedura di adozione, dopo le consultazioni a livello di esperti con il gruppo di coordinamento per l'energia elettrica. La consultazione interservizi è stata utilizzata per richiedere e ottenere il parere formale di altri servizi con un interesse legittimo in un progetto di testo. La Commissione ha pubblicato il progetto di regolamento delegato sul sito web della Commissione "Di' la tua" dove per quattro settimane, dal 20 ottobre al 17 novembre, tutti i portatori di interessi hanno potuto esprimere il loro parere. Tutti i contributi ricevuti sono pubblicamente disponibili sul sito web e la Commissione ha integrato nel testo i riscontri pertinenti.

---

5 Consultazione pubblica: https://www.entsoe.eu/news/2021/11/12/entso-e-and-eu-dso-entity-launch-a-public-consultation-on-the-network-code-on-cybersecurity/

6 T&D Europe, rete CSIRT, EU DSO, SmartEn, Flusso di lavoro NIS sull'energia, ENTSO per l'energia elettrica, NEMOS.

7 Accordo interistituzionale "Legiferare meglio" tra il Parlamento europeo, il Consiglio dell'Unione europea e la Commissione europea (GU L 123 del 12.5.2016, pag. 1).

3. ELEMENTI GIURIDICI DELL'ATTO DELEGATO

L'articolo 59, paragrafo 2, del regolamento (UE) 2019/943 conferisce alla Commissione il potere di adottare atti delegati, conformemente all'articolo 68 e ad integrazione di tale regolamento, concernenti l'istituzione di codici di rete in determinati settori.

Per quanto riguarda la cibersicurezza, l'articolo 59, paragrafo 2, lettera e), prevede norme settoriali specifiche per gli aspetti relativi alla cibersicurezza dei flussi transfrontalieri di energia elettrica, comprese le norme sui requisiti minimi, la pianificazione, il monitoraggio, la comunicazione e la gestione delle crisi.

Con la decisione di esecuzione (UE) 2020/1479 della Commissione[8] è stato inoltre stabilito un elenco di priorità per l'elaborazione di codici di rete e orientamenti per l'energia elettrica per il periodo dal 2020 al 2023. L'articolo 1 di tale decisione dispone l'elaborazione di norme settoriali specifiche per gli aspetti relativi alla cibersicurezza dei flussi transfrontalieri di energia elettrica.

Il regolamento (UE) 2019/941[9] sulla preparazione ai rischi nel settore dell'energia elettrica è di estrema importanza anche per il codice di rete, in quanto prevede la messa in atto di strumenti adeguati per la prevenzione, la preparazione e la gestione di eventuali crisi dell'energia elettrica in uno spirito di solidarietà e trasparenza. Un attacco informatico potrebbe causare una crisi dell'energia elettrica, come definita all'articolo 2, punto 9, del regolamento (UE) 2019/941, contribuirvi o coincidere con essa, con un impatto sui flussi transfrontalieri di energia elettrica. Il codice di rete si baserà sugli obblighi di legge vigenti in materia di cibersicurezza e baderà a integrarli per aumentare la cibersicurezza del settore dell'energia elettrica nell'UE. In particolare, il codice di rete integra le norme generali sulla sicurezza dei sistemi informatici e di rete stabilite dalla direttiva (UE) 2022/2555[10] (direttiva NIS 2). In tal modo si garantisce che gli attacchi informatici siano adeguatamente identificati come un rischio e che le misure adottate per risolverli siano adeguatamente riprese nei piani di preparazione ai rischi.

Inoltre il codice di rete è stato parzialmente redatto mentre era in corso il riesame di alcune delle principali normative in materia di cibersicurezza (in particolare: la direttiva (UE) 2016/1148, la direttiva NIS). Tutti coloro che hanno contribuito alla stesura del testo si sono adoperati per garantire la massima coerenza e compatibilità con le modifiche legislative discusse in parallelo.

Infine il 14 dicembre 2022 è stata adottata la direttiva (UE) 2022/2555 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione (direttiva NIS 2), che abroga la precedente direttiva (UE) 2016/1148 (direttiva NIS). La direttiva (UE) 2022/2555 mira a migliorare ulteriormente la resilienza e le capacità di risposta agli incidenti del settore pubblico e privato e dell'UE nel suo complesso. Il codice di rete è stato quindi allineato alla nuova direttiva adottata.

---

8 Decisione di esecuzione (UE) 2020/1479 della Commissione del 14 ottobre 2020 che stabilisce gli elenchi di priorità per l'elaborazione di codici di rete e orientamenti per l'energia elettrica per il periodo dal 2020 al 2023 e per il gas nel 2020 (GU L 338 del 15.10.2020, pag. 10).

9 Regolamento (UE) 2019/941 del Parlamento europeo e del Consiglio, del 5 giugno 2019, sulla preparazione ai rischi nel settore dell'energia elettrica e che abroga la direttiva 2005/89/CE (GU L 158 del 14.6.2019, pag. 1).

10 Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, 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 (direttiva NIS 2) (GU L 333 del 27.12.2022, pag. 80).

REGOLAMENTO DELEGATO (UE) …/... DELLA COMMISSIONE

del 11.3.2024

che integra il regolamento (UE) 2019/943 del Parlamento europeo e del Consiglio istituendo un codice di rete relativo a disposizioni settoriali per gli aspetti di cibersicurezza dei flussi transfrontalieri di energia elettrica

(Testo rilevante ai fini del SEE)

LA COMMISSIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea,

visto il regolamento (UE) 2019/943 del Parlamento europeo e del Consiglio, del 5 giugno 2019, sul mercato interno dell'energia elettrica[11], in particolare l'articolo 59, paragrafo 2, lettera e),

considerando quanto segue:

(1) La gestione dei rischi per la cibersicurezza è fondamentale per mantenere la sicurezza dell'approvvigionamento di energia elettrica e garantire un alto livello di cibersicurezza nel settore dell'energia elettrica.

(2) La digitalizzazione e la cibersicurezza sono decisive per la fornitura di servizi essenziali e hanno pertanto rilevanza strategica per le infrastrutture energetiche critiche.

(3) La direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio[12] dispone misure per un livello comune elevato di cibersicurezza nell'Unione. Il regolamento (UE) 2019/941 del Parlamento europeo e del Consiglio[13] integra la direttiva (UE) 2022/2555 garantendo che gli incidenti di cibersicurezza nel settore dell'energia elettrica siano adeguatamente identificati come rischio e che le misure adottate per risolverli siano adeguatamente riprese nei piani di preparazione ai rischi. Il regolamento (UE) 2019/943 integra la direttiva (UE) 2022/2555 e il regolamento (UE) 2019/941 stabilendo disposizioni specifiche per il settore dell'energia elettrica a livello dell'Unione. Il presente regolamento delegato a sua volta integra le disposizioni della direttiva (UE) 2022/2555 relative al settore dell'energia elettrica per tutti i casi che riguardano flussi transfrontalieri di energia elettrica.

(4) In un contesto di interconnessione dei sistemi digitalizzati dell'energia elettrica, la prevenzione e la gestione delle crisi dell'energia elettrica connesse agli attacchi informatici non possono essere considerate un compito esclusivamente nazionale. È opportuno sviluppare al massimo il potenziale che risiede nell'adozione di misure più efficienti e meno costose attraverso la cooperazione a livello regionale e dell'Unione. È

---

11 GU L 158 del 14.6.2019, pag. 54.

12 Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, 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 (direttiva NIS 2) (GU L 333 del 27.12.2022, pag. 80).

13 Regolamento (UE) 2019/941 del Parlamento europeo e del Consiglio, del 5 giugno 2019, sulla preparazione ai rischi nel settore dell'energia elettrica e che abroga la direttiva 2005/89/CE (GU L 158 del 14.6.2019, pag. 1).

pertanto necessario dotarsi di un quadro comune di regole e procedure meglio coordinate per garantire che gli Stati membri e altri soggetti possano collaborare efficacemente attraverso le frontiere in uno spirito di maggiore trasparenza, fiducia e solidarietà tra Stati membri e autorità competenti per l'energia elettrica e la cibersicurezza.

(5) La gestione dei rischi per la cibersicurezza nell'ambito di applicazione del presente regolamento richiede un processo strutturato che comprenda, tra l'altro, l'individuazione dei rischi per i flussi transfrontalieri di energia elettrica derivanti da attacchi informatici, i relativi processi operativi e perimetri e i corrispondenti controlli e meccanismi di verifica della cibersicurezza. Il calendario dell'intero processo copre diversi anni e tutte le sue fasi dovrebbero contribuire a un elevato livello comune di cibersicurezza nel settore e all'attenuazione dei rischi per la cibersicurezza. Tutti i partecipanti al processo dovrebbero adoperarsi al massimo per sviluppare e concordare il prima possibile le metodologie, senza indebito ritardo e in ogni caso entro i termini definiti nel presente regolamento.

(6) Le valutazioni dei rischi per la cibersicurezza a livello di Unione, di Stati membri, di regioni e di soggetti di cui al presente regolamento possono essere limitate a quelle derivanti da attacchi informatici quali definiti nel regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio[14], escludendo così, ad esempio, gli attacchi fisici, le catastrofi naturali e le indisponibilità dovute alla perdita di strutture o di risorse umane. I rischi a livello dell'Unione e regionale connessi ad attacchi fisici o a catastrofi naturali nel settore dell'energia elettrica sono già disciplinati da altre normative vigenti dell'Unione, tra cui l'articolo 5 del regolamento (UE) 2019/941 o il regolamento (UE) 2017/1485 della Commissione, del 2 agosto 2017, che stabilisce orientamenti in materia di gestione del sistema di trasmissione dell'energia elettrica. Analogamente, la direttiva (UE) 2022/2557, del 14 dicembre 2022, relativa alla resilienza dei soggetti critici mira a ridurre le vulnerabilità e a rafforzare la resilienza fisica dei soggetti critici e copre tutti i pertinenti rischi naturali e di origine umana che possono incidere sulla fornitura di servizi essenziali, fra cui gli incidenti, le catastrofi naturali, le emergenze di sanità pubblica come pandemie, minacce ibride o altre minacce antagoniste, compresi i reati di terrorismo, le infiltrazioni criminali e il sabotaggio.

(7) La nozione di "soggetti ad alto impatto e a impatto critico" di cui al presente regolamento è fondamentale per circoscrivere l'ambito dei soggetti interessati dagli obblighi ivi descritti. L'approccio basato sul rischio delineato nelle diverse disposizioni mira a individuare i processi, gli asset di supporto e i soggetti che li gestiscono che incidono sui flussi transfrontalieri di energia elettrica. A seconda del grado di impatto dei possibili attacchi informatici sulle loro operazioni di flussi transfrontalieri di energia elettrica, tali soggetti possono essere considerati "ad alto impatto" o "a impatto critico". L'articolo 3 della direttiva (UE) 2022/2555 stabilisce le nozioni di soggetti essenziali e importanti e i criteri per individuare i soggetti appartenenti a tali categorie. Sebbene molti di essi siano considerati e identificati simultaneamente come "essenziali" ai sensi dell'articolo 3 della direttiva (UE) 2022/2555 e ad alto impatto o a impatto critico ai sensi dell'articolo 24 del presente regolamento, i criteri stabiliti nel presente regolamento si riferiscono unicamente al loro ruolo e al loro impatto nei processi dell'energia elettrica

[14] Regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n. 909/2014 e (UE) 2016/1011 (GU L 333 del 27.12.2022, pag. 1).

che incidono sui flussi transfrontalieri e non tengono conto dei criteri definiti all'articolo 3 della direttiva (UE) 2022/2555.

(8) I soggetti che rientrano nell'ambito di applicazione del presente regolamento, considerati ad alto impatto o a impatto critico a norma dell'articolo 24 e tenuti al rispetto degli obblighi ivi stabiliti, sono principalmente quelli che hanno un impatto diretto sui flussi transfrontalieri di energia elettrica nell'UE.

(9) Il presente regolamento si avvale di meccanismi e strumenti esistenti, già stabiliti in altre normative, onde garantire l'efficienza ed evitare duplicazioni nel conseguimento degli obiettivi.

(10) Nell'applicazione del presente regolamento, gli Stati membri, le autorità competenti e i gestori di sistema dovrebbero tenere conto delle norme europee e delle specifiche tecniche degli organismi europei di normazione e agire in linea con la legislazione dell'Unione relativa all'immissione sul mercato o alla messa in servizio dei prodotti in essa contemplati.

(11) Per attenuare i rischi per la cibersicurezza, è necessario stabilire un insieme dettagliato di regole che disciplini gli interventi e la cooperazione dei portatori di interessi pertinenti, le cui attività riguardano aspetti di cibersicurezza dei flussi transfrontalieri di energia elettrica, al fine di garantire la sicurezza del sistema. Tali regole organizzative e tecniche dovrebbero garantire che la maggior parte degli incidenti elettrici derivanti da problemi di cibersicurezza sia affrontata efficacemente a livello operativo. È necessario stabilire gli interventi che i portatori di interessi pertinenti dovrebbero intraprendere per prevenire queste crisi e quali misure possono adottare qualora le regole di gestione del sistema si rivelino insufficienti. È pertanto necessario stabilire un quadro comune di disposizioni per la prevenzione, la preparazione e la gestione delle crisi simultanee dell'energia elettrica derivanti da problemi di cibersicurezza. Si aumenta così la trasparenza nella fase di preparazione e nello svolgimento di una crisi simultanea dell'energia elettrica e si garantisce che le misure siano adottate in modo coordinato ed efficace insieme alle autorità competenti per la cibersicurezza negli Stati membri. Gli Stati membri e i soggetti interessati dovrebbero avere l'obbligo di cooperare a livello regionale e, se del caso, a livello bilaterale, in uno spirito di solidarietà. La cooperazione e le regole sono intese a conseguire una migliore preparazione ai rischi per la cibersicurezza a costi minori, anche in linea con gli obiettivi della direttiva (UE) 2022/2555. Appare inoltre necessario rafforzare il mercato interno dell'energia elettrica incrementando il livello di fiducia in tutti gli Stati membri, in particolare attenuando il rischio di un'indebita riduzione dei flussi transfrontalieri di energia elettrica e riducendo così il rischio di effetti di ricaduta negativi sugli Stati membri confinanti.

(12) La sicurezza dell'approvvigionamento di energia elettrica comporta un'efficace cooperazione tra Stati membri, istituzioni, organi, uffici e agenzie dell'Unione nonché pertinenti portatori di interessi. I gestori dei sistemi di distribuzione e i gestori dei sistemi di trasmissione svolgono un ruolo fondamentale nel garantire la sicurezza, l'affidabilità e l'efficienza del sistema elettrico, conformemente agli articoli 31 e 40 della direttiva (UE) 2019/944 del Parlamento europeo e del Consiglio[15]. Le varie autorità di regolazione e altre autorità nazionali competenti svolgono altresì un ruolo importante nell'assicurare e monitorare la cibersicurezza nell'ambito

[15] Direttiva (UE) 2019/944 del Parlamento europeo e del Consiglio, del 5 giugno 2019, relativa a norme comuni per il mercato interno dell'energia elettrica e che modifica la direttiva 2012/27/UE (rifusione) (GU L 158 del 14.6.2019, pag. 125).

dell'approvvigionamento di energia elettrica, nel quadro dei compiti loro attribuiti dalle direttive (UE) 2019/944 e (UE) 2022/2555. Gli Stati membri dovrebbero designare un'entità esistente o nuova quale autorità nazionale competente per l'attuazione del presente regolamento, al fine di garantire la partecipazione trasparente e inclusiva di tutti gli attori coinvolti, la preparazione efficiente e la corretta attuazione delle disposizioni, la cooperazione fra i diversi portatori di interessi e le autorità competenti per l'energia elettrica e la cibersicurezza, nonché al fine di agevolare la prevenzione e la valutazione ex-post sia delle crisi dell'energia elettrica derivanti da problemi di cibersicurezza sia degli scambi di informazioni al riguardo.

(13) Qualora un soggetto ad alto impatto o a impatto critico fornisca servizi in più di uno Stato membro, o abbia la propria sede o un altro stabilimento o un rappresentante in uno Stato membro e i suoi sistemi informatici e di rete in uno o più altri Stati membri, gli Stati membri interessati dovrebbero incoraggiare le rispettive autorità competenti a compiere ogni sforzo per cooperare e assistersi reciprocamente per quanto necessario.

(14) Gli Stati membri dovrebbero garantire che le autorità competenti dispongano dei poteri necessari, in relazione ai soggetti ad alto impatto e a impatto critico, per promuovere il rispetto del presente regolamento. Tali poteri dovrebbero consentire alle autorità competenti di effettuare ispezioni in loco e vigilanza a distanza. Ciò può includere controlli casuali, lo svolgimento di audit periodici, audit mirati sulla sicurezza basati su valutazioni del rischio o su informazioni disponibili relative al rischio e scansioni di sicurezza basate su criteri di valutazione del rischio oggettivi, non discriminatori, equi e trasparenti e che includano la richiesta delle informazioni necessarie per valutare le misure di cibersicurezza adottate dal soggetto. Tali informazioni dovrebbero includere politiche di cibersicurezza documentate, dati, documenti o qualsiasi informazione necessaria per lo svolgimento dei loro compiti di vigilanza, nonché prove dell'attuazione delle politiche di cibersicurezza, quali i risultati degli audit di sicurezza effettuati da un revisore qualificato e le rispettive prove sottostanti.

(15) Al fine di evitare lacune o duplicazioni per quanto riguarda gli obblighi di gestione dei rischi per la cibersicurezza imposti ai soggetti ad alto impatto e a impatto critico, le autorità nazionali designate a norma della direttiva (UE) 2022/2555 e le autorità competenti a norma del presente regolamento dovrebbero cooperare all'attuazione delle misure di gestione dei rischi per la cibersicurezza e alla vigilanza della conformità con tali misure a livello nazionale. Le autorità competenti a norma della direttiva (UE) 2022/2555 potrebbero considerare la conformità di un soggetto ai requisiti di gestione dei rischi per la cibersicurezza di cui al presente regolamento come garanzia della conformità ai corrispondenti requisiti stabiliti in tale direttiva, o viceversa.

(16) Per un approccio comune alla prevenzione e alla gestione delle crisi simultanee dell'energia elettrica occorre che gli Stati membri condividano una nozione comune di quanto costituisce una crisi simultanea dell'energia elettrica e di quando un attacco importante ne è un fattore rilevante. In particolare, si dovrebbe agevolare il coordinamento fra Stati membri e soggetti interessati al fine di affrontare una situazione in cui sia presente o imminente il rischio potenziale di significativa carenza di energia elettrica o di impossibilità di fornire energia elettrica ai clienti in conseguenza di un attacco informatico.

(17) Il considerando 1 del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio[16] riconosce il ruolo essenziale delle reti e dei sistemi informativi e delle reti e dei servizi di comunicazione elettronica nel mantenere il buon funzionamento dell'economia in settori chiave come l'energia, mentre il considerando 44 afferma che l'Agenzia dell'Unione europea per la cibersicurezza ("ENISA") dovrebbe instaurare rapporti con l'Agenzia dell'Unione europea per la cooperazione fra i regolatori nazionali dell'energia ("ACER").

(18) Il regolamento (UE) 2019/943 attribuisce responsabilità specifiche in materia di cibersicurezza ai gestori dei sistemi di trasmissione ("TSO") e ai gestori dei sistemi di distribuzione ("DSO"). Le loro associazioni europee, vale a dire la rete europea dei TSO per l'energia elettrica ("ENTSO per l'energia elettrica") e l'ente europeo dei gestori dei sistemi di distribuzione ("EU DSO") promuovono, a norma rispettivamente degli articoli 30 e 55 di quel regolamento, la cibersicurezza in cooperazione con le autorità competenti e le entità regolamentate.

(19) Un approccio comune alla prevenzione e alla gestione delle crisi simultanee dell'energia elettrica derivanti da problemi di cibersicurezza richiede che tutti i portatori di interessi utilizzino metodi e definizioni armonizzati per individuare i rischi per la cibersicurezza nell'approvvigionamento di energia elettrica. È inoltre necessario che siano in grado di confrontare efficacemente il loro livello di prestazioni con quello dei paesi vicini. Occorre pertanto stabilire i processi, i ruoli e le responsabilità per elaborare e aggiornare le metodologie di gestione dei rischi, le scale di classificazione degli incidenti e le misure di cibersicurezza adattate ai rischi per la cibersicurezza che incidono sui flussi transfrontalieri di energia elettrica.

(20) Agli Stati membri spetta individuare, tramite l'autorità competente designata per il presente regolamento, i soggetti che soddisfano i criteri per essere designati soggetti ad alto impatto e a impatto critico. Al fine di eliminare le divergenze tra gli Stati membri a tale riguardo e garantire la certezza del diritto per quanto riguarda le misure di gestione dei rischi per la cibersicurezza e gli obblighi di segnalazione per tutti i soggetti pertinenti, è opportuno stabilire un insieme di criteri che determini quali soggetti rientrano nell'ambito di applicazione del presente regolamento. Tale insieme di criteri dovrebbe essere definito e regolarmente aggiornato attraverso il processo di elaborazione e adozione dei termini, delle condizioni e delle metodologie stabilito nel presente regolamento.

(21) Le disposizioni del presente regolamento dovrebbero lasciare impregiudicate le norme specifiche previste nel diritto dell'Unione sulla certificazione dei prodotti delle tecnologie dell'informazione e della comunicazione ("TIC"), dei servizi TIC e dei processi TIC, in particolare il regolamento (UE) 2019/881 per quanto riguarda il quadro per l'istituzione di sistemi europei di certificazione della cibersicurezza. Nel contesto del presente regolamento, i prodotti TIC dovrebbero includere anche dispositivi tecnici e software che consentano l'interazione diretta con la rete elettrotecnica, in particolare i sistemi di controllo industriale che possono essere utilizzati per la trasmissione, la distribuzione e la produzione di energia, nonché per la raccolta e trasmissione delle relative informazioni. Le disposizioni dovrebbero

[16] Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 (regolamento sulla cibersicurezza) (GU L 151 del 7.6.2019, pag. 15).

garantire che i prodotti TIC, i servizi TIC e i processi TIC da appaltare soddisfino i pertinenti obiettivi di sicurezza di cui all'articolo 51 del regolamento (UE) 2019/881.

(22) Gli attacchi informatici recenti dimostrano che i soggetti sono sempre più bersaglio di attacchi alla catena di approvvigionamento. Questi attacchi non solo hanno un impatto sui singoli soggetti che rientrano nell'ambito di applicazione, ma possono anche avere un effetto a cascata e risultare in attacchi di maggiore portata nei confronti di altri soggetti collegati mediante la rete elettrica. Sono state pertanto aggiunte disposizioni e raccomandazioni per contribuire ad attenuare i rischi per la cibersicurezza associati ai processi della catena di approvvigionamento, in particolare gli appalti, che hanno un impatto sui flussi transfrontalieri di energia elettrica.

(23) Poiché lo sfruttamento delle vulnerabilità dei sistemi informatici e di rete può causare gravi interruzioni dell'approvvigionamento energetico e danni all'economia e ai consumatori, tali vulnerabilità dovrebbero essere individuate e corrette rapidamente in modo da ridurre i rischi. Al fine di agevolare l'efficace attuazione del presente regolamento, i soggetti interessati e le autorità competenti dovrebbero cooperare per esercitare e sperimentare attività ritenute adeguate a tale scopo, compresi lo scambio di informazioni su minacce informatiche, attacchi informatici, vulnerabilità, strumenti e metodi, tattiche, tecniche e procedure, preparazione alla gestione delle crisi di cibersicurezza e altre esercitazioni. Considerando la costante evoluzione della tecnologia e i rapidi progressi della digitalizzazione del settore dell'energia elettrica, l'attuazione delle disposizioni adottate non dovrebbe pregiudicare l'innovazione o costituire un ostacolo all'accesso al mercato dell'energia elettrica e al successivo utilizzo di soluzioni innovative che contribuiscano all'efficienza e alla sostenibilità del sistema elettrico.

(24) Le informazioni raccolte ai fini del controllo dell'attuazione del presente regolamento dovrebbero essere ragionevolmente limitate sulla base del principio della necessità di conoscere. I portatori di interessi dovrebbero poter presentare queste informazioni entro termini temporali realizzabili ed efficaci. È opportuno evitare la doppia notifica.

(25) La protezione della cibersicurezza non si ferma alle frontiere dell'Unione. Un sistema sicuro esige il coinvolgimento dei paesi terzi vicini. L'Unione e i suoi Stati membri dovrebbero adoperarsi per sostenere i paesi terzi limitrofi la cui infrastruttura elettrica è collegata alla rete europea nell'applicazione di disposizioni in materia di cibersicurezza analoghe a quelle del presente regolamento.

(26) Al fine di migliorare il coordinamento della sicurezza fin dalle prime fasi e sperimentare futuri termini, condizioni e metodologie vincolanti, l'ENTSO per l'energia elettrica, l'EU DSO e le autorità competenti dovrebbero iniziare a elaborare orientamenti non vincolanti immediatamente dopo l'entrata in vigore del presente regolamento. Gli orientamenti fungeranno da base per lo sviluppo dei termini, delle condizioni e delle metodologie futuri. Parallelamente, le autorità competenti dovrebbero individuare i soggetti candidati alla designazione come soggetti ad alto impatto e a impatto critico per avviare l'adempimento degli obblighi su base volontaria.

(27) Il presente regolamento è stato elaborato in stretta collaborazione con l'ACER, l'ENISA, l'ENTSO per l'energia elettrica, l'EU DSO e altri portatori di interessi, al fine di adottare regole efficaci, equilibrate e proporzionate in modo trasparente e partecipativo.

(28) Il presente regolamento integra e potenzia le misure di gestione delle crisi stabilite nel quadro di risposta alle crisi di cibersicurezza dell'UE di cui alla raccomandazione (UE) 2017/1584 della Commissione[17]. Un attacco informatico potrebbe anche causare una crisi dell'energia elettrica quale definita all'articolo 2, punto 9), del regolamento (UE) 2019/941, contribuirvi o coincidere con essa, con ripercussioni sui flussi transfrontalieri di energia elettrica. Ne potrebbe risultare una crisi simultanea dell'energia elettrica quale definita all'articolo 2, punto 10), del regolamento (UE) 2019/941. Un siffatto incidente potrebbe avere ripercussioni anche su altri settori dipendenti dalla sicurezza dell'approvvigionamento di energia elettrica. Qualora ciò si traduca in un incidente di cibersicurezza su vasta scala ai sensi dell'articolo 16 della direttiva (UE) 2022/2555, dovrebbero applicarsi le disposizioni del medesimo articolo che istituiscono la rete europea delle organizzazioni di collegamento per le crisi informatiche ("EU-CyCLONe"). Per la gestione delle crisi a livello dell'Unione, le parti interessate dovrebbero affidarsi ai dispositivi integrati dell'UE per la risposta politica alle crisi ("dispositivi IPCR") nel quadro della decisione di esecuzione (UE) 2018/1993 del Consiglio[18].

(29) Il presente regolamento dovrebbe lasciare impregiudicata la competenza degli Stati membri di adottare le misure necessarie per assicurare la tutela degli interessi essenziali della loro sicurezza, salvaguardare l'ordine pubblico e la pubblica sicurezza e consentire la ricerca, l'individuazione e il perseguimento dei reati, nel rispetto del diritto dell'Unione. Conformemente all'articolo 346 del TFUE, nessuno Stato membro è tenuto a fornire informazioni la cui divulgazione sia dallo stesso considerata contraria agli interessi essenziali della propria sicurezza.

(30) Sebbene il presente regolamento si applichi, in via di principio, ai soggetti che svolgono attività di produzione di energia elettrica da centrali nucleari, alcune di tali attività possono essere collegate alla sicurezza nazionale.

(31) A qualsiasi trattamento di dati personali ai sensi del presente regolamento dovrebbe applicarsi il diritto dell'Unione in materia di protezione dei dati personali e della vita privata. Il presente regolamento non pregiudica in particolare il regolamento (UE) 2016/679[19], la direttiva 2002/58/CE[20] e il regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio[21]. Il presente regolamento non dovrebbe pertanto pregiudicare, tra l'altro, i compiti e i poteri delle autorità competenti di monitorare il rispetto del diritto dell'Unione in vigore in materia di protezione dei dati personali e della vita privata.

(32) Data l'importanza della cooperazione internazionale in materia di cibersicurezza, le autorità competenti per l'esecuzione dei compiti loro assegnati a norma del presente regolamento e designate dagli Stati membri dovrebbero poter partecipare alle reti di cooperazione internazionale. Pertanto, ai fini dello svolgimento dei loro compiti, le autorità competenti dovrebbero poter scambiare informazioni, compresi i dati personali, con autorità competenti di paesi terzi, purché siano soddisfatte le condizioni previste dal diritto dell'Unione in materia di protezione dei dati per i trasferimenti di dati personali verso paesi terzi, tra cui quelle dell'articolo 49 del regolamento (UE) 2016/679.

---

17 Raccomandazione (UE) 2017/1584 della Commissione, del 13 settembre 2017, relativa alla risposta coordinata agli incidenti e alle crisi di cibersicurezza su vasta scala (GU L 239 del 19.9.2017, pag. 36).

18 Decisione di esecuzione (UE) 2018/1993 del Consiglio.

19 Regolamento (UE) 2016/679.

20 Direttiva 2002/58/CE.

21 Regolamento (UE) 2018/1725.

(33) Il trattamento dei dati personali, nella misura necessaria e proporzionata a garantire la sicurezza degli asset da parte di soggetti ad alto impatto o a impatto critico, potrebbe essere considerato lecito in virtù del fatto che è conforme a un obbligo legale cui è soggetto il titolare del trattamento, conformemente ai requisiti di cui all'articolo 6, paragrafo 1, lettera c), e all'articolo 6, paragrafo 3, del regolamento (UE) 2016/679. Il trattamento dei dati personali potrebbe essere necessario anche per i legittimi interessi perseguiti dai soggetti ad alto impatto o a impatto critico, nonché dai fornitori di tecnologie e servizi di sicurezza che agiscono per conto di tali soggetti, a norma dell'articolo 6, paragrafo 1, lettera f), del regolamento (UE) 2016/679, anche qualora sia necessario per accordi di condivisione delle informazioni in materia di cibersicurezza o per la notifica volontaria di informazioni pertinenti a norma del presente regolamento. Le misure relative alla prevenzione, al rilevamento, all'individuazione, al contenimento e all'analisi degli attacchi informatici e alla risposta agli stessi, le misure di sensibilizzazione in relazione a specifiche minacce informatiche, lo scambio di informazioni nel contesto della risoluzione e della divulgazione coordinata delle vulnerabilità, lo scambio volontario di informazioni su tali attacchi informatici, sulle minacce informatiche e sulle vulnerabilità, sugli indicatori di compromissione, sulle tattiche, sulle tecniche e le procedure, sugli allarmi di cibersicurezza e sugli strumenti di configurazione potrebbero richiedere il trattamento di talune categorie di dati personali, quali indirizzi IP, localizzatori uniformi di risorse (URL), nomi di dominio, indirizzi di posta elettronica e, laddove rivelino dati personali, marcature temporali. Il trattamento dei dati personali da parte delle autorità competenti, dei punti di contatto unici e dei CSIRT potrebbe costituire un obbligo legale o essere considerato necessario per svolgere un compito di interesse pubblico o connesso all'esercizio dei pubblici poteri di cui è investito il titolare del trattamento ai sensi dell'articolo 6, paragrafo 1, lettera c) o e), e dell'articolo 6, paragrafo 3, del regolamento (UE) 2016/679, o per perseguire un interesse legittimo dei soggetti ad alto impatto e a impatto critico di cui all'articolo 6, paragrafo 1, lettera f), di tale regolamento. Inoltre, il diritto nazionale potrebbe stabilire norme che consentano alle autorità competenti, ai punti di contatto unici e ai CSIRT, nella misura necessaria e proporzionata al fine di garantire la sicurezza dei sistemi informatici e di rete dei soggetti ad alto impatto o a impatto critico, di trattare categorie particolari di dati personali conformemente all'articolo 9 del regolamento (UE) 2016/679, in particolare prevedendo misure adeguate e specifiche per tutelare i diritti e gli interessi fondamentali delle persone fisiche, comprese limitazioni tecniche al riutilizzo di tali dati e l'uso di misure all'avanguardia in materia di sicurezza e di tutela della vita privata, quali la pseudonimizzazione o la cifratura qualora l'anonimizzazione possa incidere significativamente sulla finalità perseguita.

(34) In molti casi gli attacchi informatici compromettono i dati personali. In tale contesto, le autorità competenti dovrebbero cooperare e scambiarsi informazioni su tutte le questioni pertinenti con le autorità di cui al regolamento (UE) 2016/679 e alla direttiva 2002/58/CE.

(35) Conformemente all'articolo 42, paragrafo 1, del regolamento (UE) 2018/1725, il Garante europeo della protezione dei dati è stato consultato e ha formulato il suo parere il 17 novembre 2023,

HA ADOTTATO IL PRESENTE REGOLAMENTO:

Capo I

DISPOSIZIONI GENERALI

Articolo 1

Oggetto

Il presente regolamento istituisce un codice di rete che dispone regole settoriali specifiche per gli aspetti di cibersicurezza dei flussi transfrontalieri di energia elettrica, anche su requisiti minimi comuni, pianificazione, monitoraggio, comunicazione e gestione delle crisi.

Articolo 2

Ambito di applicazione

1. Il presente regolamento si applica agli aspetti di cibersicurezza dei flussi transfrontalieri di energia elettrica nelle attività dei seguenti soggetti, se sono individuati come soggetti ad alto impatto o a impatto critico a norma dell'articolo 24:

   (a) le imprese elettriche quali definite all'articolo 2, punto 57), della direttiva (UE) 2019/944;

   (b) i gestori del mercato elettrico designati quali definiti all'articolo 2, punto 8), della direttiva (UE) 2019/943;

   (c) i mercati organizzati quali definiti all'articolo 2, punto 4), del regolamento di esecuzione (UE) n. 1348/2014 della Commissione[22] che gestiscono operazioni su prodotti pertinenti ai flussi transfrontalieri di energia elettrica;

   (d) i prestatori di servizi TIC critici di cui all'articolo 3, punto 9), del presente regolamento;

   (e) l'ENTSO per l'energia elettrica istituita a norma dell'articolo 28 del regolamento (UE) 2019/943;

   (f) l'EU DSO istituito a norma dell'articolo 52 del regolamento (UE) 2019/943;

   (g) i responsabili del bilanciamento quali definiti all'articolo 2, punto 14), del regolamento (UE) 2019/943;

   (h) i gestori di punti di ricarica quali definiti nell'allegato I della direttiva (UE) 2022/2555;

   (i) i centri di coordinamento regionali (RCC) istituiti a norma dell'articolo 35 del regolamento (UE) 2019/943;

   (j) i prestatori di servizi di sicurezza gestiti (MSSP) quali definiti all'articolo 6, punto 40), della direttiva (UE) 2022/2555;

[22] Regolamento di esecuzione (UE) n. 1348/2014 della Commissione, del 17 dicembre 2014, relativo alla segnalazione dei dati in applicazione dell'articolo 8, paragrafi 2 e 6, del regolamento (UE) n. 1227/2011 del Parlamento europeo e del Consiglio concernente l'integrità e la trasparenza del mercato dell'energia all'ingrosso (GU L 363 del 18.12.2014, pag. 121).

(k) ogni altro soggetto o terzo cui sono state delegate o attribuite responsabilità a norma del presente regolamento.

2. Le autorità seguenti sono responsabili, nell'ambito dei loro attuali mandati, dell'esecuzione dei compiti assegnati dal presente regolamento:

(a) l'Agenzia dell'Unione europea per la cooperazione fra i regolatori nazionali dell'energia (ACER) istituita dal regolamento (UE) 2019/942;

(b) le autorità nazionali competenti per l'esecuzione dei compiti loro assegnati a norma del presente regolamento e designate dagli Stati membri a norma dell'articolo 4 ("autorità competente");

(c) le autorità nazionali di regolazione designate da ciascuno Stato membro ai sensi dell'articolo 57, paragrafo 1, della direttiva (UE) 2019/944;

(d) le autorità competenti per la preparazione ai rischi istituite a norma dell'articolo 3 del regolamento (UE) 2019/941;

(e) i team di risposta agli incidenti di sicurezza informatica ("CSIRT") quali designati o istituiti a norma dell'articolo 10 della direttiva (UE) 2022/2555;

(f) le autorità competenti per la cibersicurezza quali designate o istituite a norma dell'articolo 8 della direttiva (UE) 2022/2555;

(g) l'Agenzia dell'Unione europea per la cibersicurezza, istituita a norma del regolamento (UE) 2019/881;

(h) ogni altra autorità o terzo cui sono state delegate o attribuite responsabilità a norma dell'articolo 4, paragrafo 3.

3. Il presente regolamento si applica anche a tutti i soggetti che non sono stabiliti nell'Unione ma prestano servizi a soggetti nell'Unione, a condizione che le autorità competenti li abbiano individuati come soggetti ad alto impatto o a impatto critico a norma dell'articolo 24, paragrafo 2.

4. Il presente regolamento lascia impregiudicata la responsabilità degli Stati membri di tutelare la sicurezza nazionale e il loro potere di salvaguardare altre funzioni essenziali dello Stato, tra cui la garanzia della sua integrità territoriale e il mantenimento dell'ordine pubblico.

5. Il presente regolamento lascia impregiudicata la responsabilità degli Stati membri di salvaguardare la sicurezza nazionale relativamente alle attività di produzione di energia elettrica da centrali nucleari, comprese le attività all'interno della catena del valore nucleare, conformemente ai trattati.

6. I soggetti, le autorità competenti, i punti di contatto unici a livello di soggetto e i CSIRT trattano i dati personali nella misura necessaria ai fini del presente regolamento e conformemente al regolamento (UE) 2016/679, in particolare trattandoli in base all'articolo 6 dello stesso.

Articolo 3

Definizioni

Si applicano le definizioni seguenti:

(1) "asset": un'informazione, software o hardware nei sistemi informatici e di rete, materiale o immateriale, che ha valore per un singolo, un'organizzazione o un governo;

(2) "autorità competente per la preparazione ai rischi": l'autorità competente designata a norma dell'articolo 3 del regolamento (UE) 2019/941;

(3) "team di risposta agli incidenti di sicurezza informatica": il gruppo responsabile del trattamento dei rischi e degli incidenti conformemente all'articolo 10 della direttiva (UE) 2022/2555;

(4) "asset a impatto critico": l'asset necessario per eseguire un processo a impatto critico;

(5) "soggetto a impatto critico": il soggetto che svolge un processo a impatto critico e è individuato dalle autorità competenti conformemente all'articolo 24;

(6) "perimetro di impatto critico": il perimetro definito da un soggetto di cui all'articolo 2, paragrafo 1, che contiene tutti gli asset a impatto critico, in cui l'accesso agli asset può essere controllato e che definisce l'ambito di applicazione dei controlli avanzati di cibersicurezza;

(7) "processo a impatto critico": il processo operativo effettuato da un soggetto per il quale gli indici di impatto sulla cibersicurezza dell'energia elettrica sono superiori alla soglia di impatto critico;

(8) "soglia di impatto critico": i valori degli indici di impatto sulla cibersicurezza dell'energia elettrica di cui all'articolo 19, paragrafo 3, lettera b), al di sopra dei quali un attacco informatico a un processo operativo causa perturbazioni critiche dei flussi transfrontalieri di energia elettrica;

(9) "prestatore di servizi TIC critici": l'entità che fornisce un servizio TIC o un processo TIC necessari per un processo a impatto critico o ad alto impatto che incide sugli aspetti di cibersicurezza dei flussi transfrontalieri di energia elettrica e che, se compromesso, può determinare un attacco informatico con un impatto superiore alla soglia di impatto critico o di alto impatto;

(10) "flusso transfrontaliero di energia elettrica": il flusso transfrontaliero quale definito all'articolo 2, punto 3), del regolamento (UE) 2019/943;

(11) "attacco informatico": l'incidente quale definito all'articolo 3, punto 14), del regolamento (UE) 2022/2554;

(12) "cibersicurezza": la cibersicurezza quale definita all'articolo 2, punto 1), del regolamento (UE) 2019/881;

(13) "controllo della cibersicurezza": le azioni o le procedure svolte al fine di evitare, identificare, contrastare o ridurre al minimo i rischi per la cibersicurezza;

(14) "incidente di cibersicurezza": l'incidente quale definito all'articolo 6, punto 6), della direttiva (UE) 2022/2555;

(15) "sistema di gestione della cibersicurezza": le politiche, le procedure, gli orientamenti e le risorse e attività associate, gestite collettivamente da un soggetto nell'intento di proteggere i suoi asset informatici dalle minacce informatiche, istituendo, attuando, gestendo, monitorando, riesaminando, mantenendo e migliorando sistematicamente la sicurezza dei sistemi informatici e di rete di un'organizzazione;

(16) "centro operativo per la cibersicurezza": il centro apposito in cui una squadra tecnica composta da uno o più esperti, coadiuvata da sistemi informatici di cibersicurezza,

esegue compiti connessi alla sicurezza (servizi del centro operativo per la cibersicurezza, "CSOC"), quali la gestione degli attacchi informatici e degli errori di configurazione della sicurezza, il monitoraggio della sicurezza, l'analisi dei log e l'identificazione degli attacchi informatici;

(17) "minaccia informatica": la minaccia informatica quale definita all'articolo 2, punto 8), del regolamento (UE) 2019/881;

(18) "gestione delle vulnerabilità di cibersicurezza": la pratica di individuare e affrontare le vulnerabilità;

(19) "soggetto": il soggetto quale definito all'articolo 6, punto 38), della direttiva (UE) 2022/2555;

(20) "preallarme": le informazioni necessarie per indicare il sospetto che l'incidente significativo sia stato causato da atti illeciti o dolosi o potrebbe avere un impatto transfrontaliero;

(21) "indice di impatto sulla cibersicurezza dell'energia elettrica" ("ECII"): l'indice o la scala che classifica le possibili conseguenze degli attacchi informatici per i processi operativi connessi ai flussi transfrontalieri di energia elettrica;

(22) "sistema europeo di certificazione della cibersicurezza": il sistema quale definito all'articolo 2, punto 9), del regolamento (UE) 2019/881;

(23) "soggetto ad alto impatto": il soggetto che svolge un processo ad alto impatto e è individuato dalle autorità competenti conformemente all'articolo 24;

(24) "processo ad alto impatto": il processo operativo effettuato da un soggetto per il quale gli indici di impatto sulla cibersicurezza dell'energia elettrica sono superiori alla soglia di alto impatto;

(25) "asset ad alto impatto": l'asset necessario per eseguire un processo ad alto impatto;

(26) "soglia di alto impatto": i valori degli indici di impatto sulla cibersicurezza dell'energia elettrica di cui all'articolo 19, paragrafo 3, lettera b), al di sopra dei quali un attacco informatico riuscito a un processo causa gravi perturbazioni dei flussi transfrontalieri di energia elettrica;

(27) "perimetro di alto impatto": il perimetro definito da un soggetto elencato all'articolo 2, paragrafo 1, che contiene tutti gli asset ad alto impatto, nel quale l'accesso agli risorse può essere controllato e che definisce l'ambito di applicazione dei controlli minimi di cibersicurezza;

(28) "prodotto TIC": il prodotto TIC quale definito all'articolo 2, punto 12), del regolamento (UE) 2019/881;

(29) "servizio TIC": il servizio TIC quale definito all'articolo 2, punto 13), del regolamento (UE) 2019/881;

(30) "processo TIC": il processo TIC quale definito all'articolo 2, punto 14), del regolamento (UE) 2019/881;

(31) "sistema legacy": il sistema legacy di TIC quale definito all'articolo 3, punto 3), del regolamento (UE) 2022/2554;

(32) "punto di contatto unico nazionale": il punto di contatto unico designato o istituito da ciascuno Stato membro a norma dell'articolo 8, paragrafo 3, della direttiva (UE) 2022/2555;

(33) "autorità nazionali di gestione delle crisi informatiche nei sistemi informatici e di rete": le autorità designate o istituite a norma dell'articolo 9, paragrafo 1, della direttiva (UE) 2022/2555;

(34) "originatore": il soggetto che avvia uno scambio di informazioni, una condivisione di informazioni o un'archiviazione di informazioni;

(35) "capitolato di appalto": le specifiche che i soggetti definiscono per l'appalto di prodotti TIC, processi TIC o servizi TIC nuovi o aggiornati;

(36) "rappresentante": la persona fisica o giuridica stabilita nell'Unione la quale è esplicitamente designata ad agire per conto di un soggetto ad impatto critico o ad alto impatto non stabilito nell'Unione ma che fornisce servizi a soggetti nell'Unione e alla quale l'autorità competente o il CSIRT può rivolgersi anziché rivolgersi al soggetto riguardo agli obblighi che a questi incombono a norma del presente regolamento;

(37) "rischio": il rischio quale definito all'articolo 6, punto 9), della direttiva (UE) 2022/2555;

(38) "matrice dell'impatto del rischio": la matrice utilizzata durante la valutazione del rischio per determinare il livello di impatto del rischio risultante per ciascun rischio valutato;

(39) "crisi simultanea dell'energia elettrica": la crisi dell'energia elettrica quale definita all'articolo 2, punto 10), del regolamento (UE) 2019/941;

(40) "punto di contatto unico a livello di soggetto": il punto di contatto unico a livello di soggetto designato a norma dell'articolo 38, paragrafo 1, lettera c);

(41) "portatore di interessi": la parte avente un interesse nel successo e nella continuità del funzionamento di un'organizzazione o di un processo, quali dipendenti, amministratori, azionisti, autorità di regolazione, associazioni, fornitori e clienti;

(42) "norma": la norma quale definita all'articolo 2, punto 1), del regolamento (UE) n. 1025/2012;

(43) "regione di gestione del sistema": una delle regioni di gestione del sistema quali definite nell'allegato I della decisione ACER 05-2022 sulla definizione di regioni di gestione del sistema, istituite a norma dell'articolo 36 del regolamento (UE) 2019/943;

(44) "gestori di sistema": il "gestore del sistema di distribuzione" (DSO) e il "gestore del sistema di trasmissione" (TSO) quali definiti all'articolo 2, punti 29) e 35), della direttiva (UE) 2019/944;

(45) "processo a impatto critico a livello dell'Unione": il processo del settore dell'energia elettrica, che può coinvolgere più soggetti, per il quale il possibile impatto di un attacco informatico può essere considerato critico in sede di valutazione del rischio per la cibersicurezza a livello dell'Unione;

(46) "processo ad alto impatto a livello dell'Unione": il processo del settore dell'energia elettrica, che può coinvolgere più soggetti, per il quale il possibile impatto di un attacco informatico può essere considerato alto in sede di valutazione del rischio per la cibersicurezza a livello dell'Unione;

(47) "vulnerabilità sfruttata attivamente non risolta": la vulnerabilità non ancora resa pubblica né ancora risolta e per la quale valide prove consentono di ritenere che un attore abbia eseguito un codice malevolo su un sistema senza l'autorizzazione del proprietario del sistema;

(48) "vulnerabilità": la vulnerabilità quale definita all'articolo 6, punto 15), della direttiva (UE) 2022/2555;

Articolo 4

Autorità competente

1. Quanto prima e in ogni caso entro [*OP: inserire la data corrispondente a sei mesi dall'entrata in vigore del presente regolamento*], ciascuno Stato membro designa un'autorità nazionale governativa o di regolazione responsabile dell'esecuzione dei compiti assegnati dal presente regolamento ("autorità competente"). Fino a quando non siano stati assegnati all'autorità competente, i compiti previsti dal presente regolamento sono eseguiti dall'autorità di regolazione designata da ciascuno Stato membro a norma dell'articolo 57, paragrafo 1, della direttiva (UE) 2019/944.
2. Gli Stati membri notificano senza indugio alla Commissione, all'ACER, all'ENISA, al gruppo di cooperazione NIS istituito a norma dell'articolo 14 della direttiva (UE) 2022/2555 e al gruppo di coordinamento per l'energia elettrica istituito a norma dell'articolo 1 della decisione della Commissione del 15 novembre 2012[23] la loro autorità competente designata a norma del paragrafo 1 del presente articolo, con comunicazione del nome e dei recapiti, e ogni successiva modifica.
3. Gli Stati membri possono autorizzare la loro autorità competente a delegare i compiti assegnatile dal presente regolamento ad altre autorità nazionali, ad eccezione dei compiti elencati all'articolo 5. Ciascuna autorità competente controlla l'applicazione del presente regolamento da parte delle autorità cui ha delegato compiti. L'autorità competente comunica alla Commissione, all'ACER, al gruppo di coordinamento per l'energia elettrica, all'ENISA e al gruppo di cooperazione NIS il nome, i recapiti, i compiti assegnati, e le eventuali successive modifiche, delle autorità cui è stato delegato un compito.

Articolo 5

Cooperazione tra le autorità e gli organismi competenti a livello nazionale

Le autorità competenti coordinano e garantiscono un'adeguata cooperazione tra le autorità competenti per la cibersicurezza, le autorità di gestione delle crisi informatiche, le autorità nazionali di regolazione, le autorità competenti per la preparazione ai rischi e i CSIRT ai fini dell'adempimento dei pertinenti obblighi di cui al presente regolamento. Le autorità competenti si coordinano inoltre con altri organismi o autorità stabiliti da ciascuno Stato membro al fine di garantire procedure efficaci ed evitare duplicazioni di compiti e obblighi. Le autorità competenti possono incaricare le rispettive autorità nazionali di regolazione di chiedere all'ACER un parere a norma dell'articolo 8, paragrafo 3.

[23] Decisione della Commissione, del 15 novembre 2012, che istituisce il gruppo di coordinamento per l'energia elettrica (GU C 353 del 17.11.2012, pag. 2).

Articolo 6

Termini e condizioni o metodologie o piani

1. I TSO elaborano, in cooperazione con l'EU DSO, proposte di termini e condizioni o metodologie a norma del paragrafo 2, o di piani a norma del paragrafo 3.

2. I termini e condizioni o le metodologie elencati di seguito, nonché eventuali modifiche, sono subordinati all'approvazione di tutte le autorità competenti:

   (a) le metodologie di valutazione del rischio per la cibersicurezza di cui all'articolo 18, paragrafo 1;

   (b) la relazione globale di valutazione transfrontaliera del rischio per la cibersicurezza dell'energia elettrica a norma dell'articolo 23;

   (c) i controlli minimi e avanzati di cibersicurezza a norma dell'articolo 29, la mappatura dei controlli sulla cibersicurezza dell'energia elettrica in riferimento alle norme di cui all'articolo 34, compresi i controlli minimi e avanzati di cibersicurezza nella catena di approvvigionamento conformemente all'articolo 33;

   (d) una raccomandazione per gli appalti riguardo alla cibersicurezza a norma dell'articolo 35;

   (e) la metodologia della scala di classificazione degli attacchi informatici a norma dell'articolo 37, paragrafo 8.

3. Le proposte di piani di attenuazione dei rischi per la cibersicurezza a livello regionale a norma dell'articolo 22 sono soggette all'approvazione di tutte le autorità competenti della regione di gestione del sistema interessata.

4. Le proposte di termini e condizioni e di metodologie di cui al paragrafo 2 o di piani di cui al paragrafo 3 includono una proposta di calendario attuativo e una descrizione dell'impatto previsto sugli obiettivi del presente regolamento.

5. L'EU DSO può fornire un parere motivato ai TSO interessati fino a 3 settimane prima del termine per la presentazione alle autorità competenti della proposta di termini e condizioni o di metodologie o di piani. I TSO responsabili della proposta di termini e condizioni o di metodologie o di piani tengono conto del parere motivato dell'EU DSO prima di presentarla alle autorità competenti per approvazione. I TSO motivano l'eventuale decisione di non prendere in considerazione il parere dell'EU DSO.

6. Se elaborano congiuntamente i termini e le condizioni, le metodologie e i piani, i TSO partecipanti cooperano strettamente. I TSO, con l'assistenza dell'ENTSO per l'energia elettrica e in cooperazione con l'EU DSO, informano regolarmente le autorità competenti e l'ACER in merito ai progressi compiuti nell'elaborazione dei termini e delle condizioni o delle metodologie o dei piani.

Articolo 7

Regole di voto dei gestori dei sistemi di trasmissione (TSO)

1. Se non sono in grado di raggiungere un accordo, i TSO che decidono in merito alle proposte di termini e condizioni o di metodologie decidono a maggioranza qualificata. La maggioranza qualificata per tali proposte è calcolata come segue:

   (a) TSO rappresentanti almeno il 55 % degli Stati membri; e

(b) TSO rappresentanti Stati membri che totalizzano almeno il 65 % della popolazione dell'Unione.

2. La minoranza di blocco per le decisioni riguardanti le proposte di termini e condizioni o di metodologie di cui all'articolo 6, paragrafo 2, comprende TSO che rappresentino almeno quattro Stati membri; in caso contrario si ritiene raggiunta la maggioranza qualificata.

3. Se non sono in grado di raggiungere un accordo in una regione composta da più di cinque Stati membri, i TSO che decidono in merito alle proposte di piani di cui all'articolo 6, paragrafo 2, deliberano a maggioranza qualificata. La maggioranza qualificata per le proposte di cui all'articolo 6, paragrafo 2, esige una maggioranza di:

(a) TSO rappresentanti almeno il 72 % degli Stati membri interessati; e

(b) TSO rappresentanti Stati membri che totalizzano almeno il 65 % della popolazione dell'area interessata.

4. La minoranza di blocco per le decisioni in merito a proposte di piani include almeno il numero minimo di TSO che rappresentano oltre il 35 % della popolazione degli Stati membri partecipanti, più i TSO che rappresentano almeno un altro Stato membro interessato; in caso contrario si ritiene raggiunta la maggioranza qualificata.

5. Per le decisioni dei TSO riguardanti proposte di termini e condizioni o di metodologie in applicazione dell'articolo 6, paragrafo 2, a ogni Stato membro è attribuito un voto. Se sul territorio di uno Stato membro esistono più TSO, lo Stato membro assegna i diritti di voto fra i TSO.

6. Se i TSO, in cooperazione con l'EU DSO, non presentano alle autorità competenti interessate una proposta iniziale o modificata di termini e condizioni o di metodologie, o di piani, entro i termini stabiliti nel presente regolamento, essi trasmettono alle autorità competenti interessate e all'ACER i progetti dei termini e delle condizioni o delle metodologie o dei piani. I TSO motivano il mancato raggiungimento di un accordo. Le autorità competenti prendono congiuntamente i provvedimenti opportuni per l'adozione dei termini e delle condizioni o delle metodologie necessari, o dei piani necessari. Può trattarsi, ad esempio, di chiedere modifiche dei progetti a norma del presente paragrafo, di rivederli e completarli o, se non sono stati trasmessi progetti, di definire e approvare i termini e le condizioni o le metodologie necessari, o i piani necessari.

Articolo 8

Presentazione delle proposte alle autorità competenti

1. I TSO presentano le proposte di termini e condizioni o di metodologie, o di piani, per approvazione, alle autorità competenti interessate entro i rispettivi termini di cui agli articoli 18, 23, 29, 33, 34, 35 e 37. Le autorità competenti possono prorogare congiuntamente tali termini in circostanze eccezionali, in particolare nei casi in cui un termine non possa essere rispettato per motivi fuori del controllo dei TSO o dell'EU DSO.

2. Le proposte di termini e condizioni, di metodologie o di piani a norma del paragrafo 1 sono trasmesse per informazione all'ACER contemporaneamente alla presentazione alle autorità competenti.

3. Su richiesta congiunta delle autorità nazionali di regolazione, l'ACER formula un parere sulla proposta di termini e condizioni o di metodologie, o di piani, entro sei mesi dall'averla ricevuta, e lo trasmette alle autorità nazionali di regolazione e alle autorità competenti. Le autorità nazionali di regolazione, le autorità competenti per la cibersicurezza e ogni altra autorità designata come autorità competente si coordinano prima che le autorità di regolazione richiedano un parere all'ACER. L'ACER può includere nel parere le proprie raccomandazioni. Prima di emettere un parere sulle proposte di cui all'articolo 6, paragrafo 2, l'ACER consulta l'ENISA.

4. Le autorità competenti si consultano fra loro e mettono in atto una stretta cooperazione e coordinazione al fine di raggiungere un accordo sui termini e sulle condizioni, sulle metodologie o sui piani proposti. Prima di approvare i termini e le condizioni o le metodologie, o i piani, esse rivedono e completano le proposte, se necessario, previa consultazione dell'ENTSO per l'energia elettrica e dell'EU DSO, al fine di garantire che le proposte siano in linea con il presente regolamento e contribuiscano a un alto livello comune di cibersicurezza in tutta l'Unione.

5. Le autorità competenti decidono in merito ai termini e alle condizioni o alle metodologie o ai piani entro sei mesi dalla data in cui li hanno ricevuti o, se del caso, dalla data in cui li ha ricevuti l'ultima autorità competente interessata.

6. Qualora l'ACER emetta un parere, le autorità competenti interessate ne tengono conto e adottano le loro decisioni entro sei mesi dal suo ricevimento.

7. Qualora le autorità competenti richiedano congiuntamente una modifica dei termini e delle condizioni o delle metodologie o dei piani proposti, al fine di approvarli, i TSO elaborano, in collaborazione con l'EU DSO, una proposta di modifica. I TSO presentano la proposta modificata per approvazione entro due mesi dalla richiesta delle autorità competenti. Le autorità competenti decidono in merito ai termini e alle condizioni o alle metodologie o ai piani modificati entro due mesi dalla loro presentazione.

8. Qualora le autorità competenti non abbiano raggiunto un accordo entro il termine di cui al paragrafo 5 o 7, ne informano la Commissione. La Commissione può prendere i provvedimenti opportuni per rendere possibile l'adozione dei termini e condizioni o delle metodologie, o dei piani, necessari.

9. I TSO, con l'assistenza dell'ENTSO per l'energia elettrica e dell'EU DSO, pubblicano i termini e le condizioni o le metodologie, o i piani, sui loro siti web, previa approvazione delle autorità competenti interessate, salvo nei casi in cui tali informazioni sono considerate riservate a norma dell'articolo 47.

10. Le autorità competenti possono richiedere congiuntamente ai TSO e all'EU DSO proposte di modifica dei termini e delle condizioni o delle metodologie, o dei piani, da presentare entro un termine da esse stabilito. I TSO, in cooperazione con l'EU DSO, possono proporre modifiche alle autorità competenti anche di propria iniziativa. Le proposte di modifica dei termini e condizioni o delle metodologie, o dei piani, sono elaborate e approvate secondo la procedura di cui al presente articolo.

11. Almeno ogni tre anni dopo la prima adozione dei rispettivi termini e condizioni o metodologie, o dei rispettivi piani adottati, i TSO, in cooperazione con l'EU DSO, svolgono un riesame dell'efficacia dei termini e delle condizioni o delle metodologie, o dei piani adottati, e ne comunicano senza indebito ritardo i risultati alle autorità competenti e all'ACER.

Articolo 9

Consultazione

1. I TSO, con l'assistenza dell'ENTSO per l'energia elettrica e in cooperazione con l'EU DSO, consultano i portatori di interessi, tra cui l'ACER, l'ENISA e l'autorità competente di ciascuno Stato membro, in merito ai progetti di proposte di termini e condizioni o di metodologie elencati all'articolo 6, paragrafo 2, e di piani di cui all'articolo 6, paragrafo 3. La consultazione ha una durata di almeno un mese.

2. Le proposte di termini e condizioni o di metodologie di cui all'articolo 6, paragrafo 2, presentate dai TSO, in cooperazione con l'EU DSO, sono pubblicate e sottoposte a consultazione a livello dell'Unione. Le proposte di piani di cui all'articolo 6, paragrafo 3, presentate a livello regionale dai TSO interessati, in cooperazione con l'EU DSO, sono pubblicate e sottoposte a consultazione almeno a livello regionale.

3. I TSO, con l'assistenza dell'ENTSO per l'energia elettrica, e dell'EU DSO responsabile della proposta di termini e condizioni o di metodologie, o di piani, tengono debitamente conto dei pareri dei portatori di interessi emersi dalle consultazioni svolte a norma del paragrafo 1, prima di presentarla per approvazione regolamentare. In ogni caso, insieme alla proposta è presentata una motivazione valida che giustifichi l'inclusione o l'esclusione dei punti di vista emersi dalla consultazione ed è pubblicata tempestivamente prima della proposta di termini e condizioni o di metodologie o contemporaneamente ad essa.

Articolo 10

Partecipazione dei portatori di interessi

L'ACER, in stretta cooperazione con l'ENTSO per l'energia elettrica e con l'EU DSO, organizza la partecipazione dei portatori di interessi, anche mediante riunioni periodiche per individuare i problemi e proporre miglioramenti dell'attuazione del presente regolamento.

Articolo 11

Recupero dei costi

1. I costi sostenuti dai TSO e dai DSO soggetti alla regolamentazione delle tariffe di rete e derivanti dagli obblighi stabiliti dal presente regolamento, compresi i costi sostenuti dall'ENTSO per l'energia elettrica e dall'EU DSO, sono valutati dall'autorità nazionale di regolazione competente di ciascuno Stato membro.

2. I costi ritenuti ragionevoli, efficienti e proporzionati sono recuperati mediante tariffe di rete o altri meccanismi appropriati, secondo quanto stabilito dall'autorità nazionale di regolazione competente.

3. Su richiesta delle autorità nazionali di regolazione competenti, i TSO e i DSO di cui al paragrafo 1 trasmettono, entro un termine ragionevole stabilito dall'autorità nazionale di regolazione, le informazioni necessarie per facilitare la valutazione dei costi sostenuti.

Articolo 12

Controllo

1. L'ACER controlla l'attuazione del presente regolamento conformemente all'articolo 32, paragrafo 1, del regolamento (UE) 2019/943 e all'articolo 4, paragrafo 2, del regolamento (UE) 2019/942. Nell'effettuare tale controllo, l'ACER può cooperare con l'ENISA e chiedere il sostegno dell'ENTSO per l'energia elettrica e dell'EU DSO. L'ACER informa periodicamente il gruppo di coordinamento per l'energia elettrica e il gruppo di cooperazione NIS in merito all'attuazione del presente regolamento.

2. L'ACER pubblica una relazione almeno ogni tre anni dopo l'entrata in vigore del presente regolamento per:

   (a) riesaminare lo stato di attuazione delle misure di gestione dei rischi per la cibersicurezza applicabili per quanto riguarda i soggetti ad alto impatto e a impatto critico;

   (b) individuare l'eventuale necessità di ulteriori disposizioni in materia di requisiti comuni, pianificazione, controllo, comunicazione e gestione delle crisi per prevenire i rischi nel settore dell'energia elettrica; e

   (c) individuare margini di miglioramento per la revisione del presente regolamento o determinare gli ambiti non disciplinati e le nuove priorità che possono emergere in funzione degli sviluppi tecnologici.

3. Entro il [*OP: inserire la data corrispondente a 12 mesi dall'entrata in vigore del presente regolamento*], l'ACER, in cooperazione con l'ENISA e previa consultazione dell'ENTSO per l'energia elettrica e dell'EU DSO, può emanare orientamenti sulle informazioni pertinenti che devono esserle comunicate ai fini del controllo, nonché sul processo e sulla frequenza della raccolta, sulla base degli indicatori di prestazione definiti conformemente al paragrafo 5.

4. Le autorità competenti possono avere accesso alle informazioni pertinenti detenute dall'ACER, raccolte a norma del presente articolo.

5. L'ACER, in cooperazione con l'ENISA e con il sostegno dell'ENTSO per l'energia elettrica e dell'EU DSO, pubblica indicatori di prestazione non vincolanti per valutare l'affidabilità operativa, in termini di cibersicurezza, dei flussi transfrontalieri di energia elettrica.

6. I soggetti elencati all'articolo 2, paragrafo 1, trasmettono all'ACER le informazioni di cui necessita per svolgere i compiti di cui al paragrafo 2.

Articolo 13

Analisi comparativa

1. Entro il [*OP: inserire la data corrispondente a 12 mesi dall'entrata in vigore del presente regolamento*], l'ACER, in cooperazione con l'ENISA, emana una guida non vincolante per l'analisi comparativa della cibersicurezza. La guida illustra alle autorità nazionali di regolazione i principi dell'analisi comparativa dei controlli di cibersicurezza attuati a norma del paragrafo 2, tenendo conto dei costi di attuazione dei controlli e dell'efficacia della funzione svolta da processi, prodotti, servizi, sistemi e soluzioni utilizzati per attuarli. Per l'elaborazione della guida non vincolante per

l'analisi comparativa della cibersicurezza, l'ACER tiene conto delle relazioni di analisi comparativa esistenti. L'ACER trasmette alle autorità nazionali di regolazione, per informazione, la guida non vincolante per l'analisi comparativa della cibersicurezza.

2. Entro 12 mesi dall'emanazione della guida per l'analisi comparativa di cui al paragrafo 1, le autorità nazionali di regolazione effettuano un'analisi comparativa per valutare se gli attuali investimenti nella cibersicurezza:

   (a) attenuano i rischi che hanno un impatto sui flussi transfrontalieri di energia elettrica;

   (b) ottengono i risultati auspicati e aumentano i guadagni di efficienza per lo sviluppo dei sistemi elettrici;

   (c) sono efficienti e bene integrati nei processi di acquisizione di asset e servizi.

3. Per l'analisi comparativa, le autorità nazionali di regolazione possono tenere conto della guida non vincolante per l'analisi comparativa della cibersicurezza elaborata dall'ACER e valutano in particolare:

   (a) la spesa media per la cibersicurezza volta ad attenuare i rischi che hanno un impatto sui flussi transfrontalieri di energia elettrica, in particolare per quanto riguarda i soggetti ad alto impatto e a impatto critico;

   (b) in cooperazione con l'ENTSO per l'energia elettrica e con l'EU DSO, i prezzi medi dei servizi, dei sistemi e dei prodotti di cibersicurezza che contribuiscono in larga misura al miglioramento e alla manutenzione delle misure di gestione dei rischi per la cibersicurezza nelle diverse regioni di gestione del sistema;

   (c) l'esistenza e il livello di comparabilità di costi e funzioni dei servizi, dei sistemi e delle soluzioni di cibersicurezza idonei all'attuazione del presente regolamento, individuando possibili misure necessarie per promuovere l'efficienza della spesa, in particolare ove possano essere necessari investimenti tecnologici in cibersicurezza.

4. Tutte le informazioni relative all'analisi comparativa sono gestite e trattate conformemente alle prescrizioni di classificazione dei dati di cui al presente regolamento, ai controlli minimi di cibersicurezza e alla relazione di valutazione transfrontaliera del rischio per la cibersicurezza dell'energia elettrica. L'analisi comparativa di cui ai paragrafi 2 e 3 non è resa pubblica.

5. Fatti salvi gli obblighi di riservatezza di cui all'articolo 47 e la necessità di proteggere la sicurezza dei soggetti cui si applicano le disposizioni del presente regolamento, l'analisi comparativa di cui ai paragrafi 2 e 3 del presente articolo è condivisa con tutte le autorità nazionali di regolazione, tutte le autorità competenti, l'ACER, l'ENISA e la Commissione.

Articolo 14

Accordi con TSO di paesi terzi

1. Entro 18 mesi dall'entrata in vigore del presente regolamento, i TSO di una regione di gestione del sistema confinante con un paese terzo si adoperano per concludere accordi con i TSO del paese terzo confinante che siano conformi al pertinente diritto dell'Unione e definiscano la base per la cooperazione in materia di protezione della cibersicurezza e gli accordi di cooperazione in materia di cibersicurezza con detti TSO.

2. I TSO informano l'autorità competente in merito agli accordi conclusi a norma del paragrafo 1.

Articolo 15

Rappresentanti legali

1. I soggetti che non sono stabiliti nell'Unione ma forniscono servizi a soggetti nell'Unione e a cui è stato notificato di essere soggetti ad alto impatto o ad impatto critico a norma dell'articolo 24, paragrafo 6, designano per iscritto, entro tre mesi dalla notifica, un rappresentante nell'Unione e ne informano l'autorità competente notificante.
2. Il rappresentante di cui al paragrafo 1 è incaricato di fungere da punto di contatto cui un'autorità competente o CSIRT nell'Unione può rivolgersi in aggiunta o in sostituzione del soggetto ad alto impatto o a impatto critico riguardo agli obblighi di quest'ultimo a norma del presente regolamento. Il soggetto ad alto impatto o a impatto critico conferisce al proprio rappresentante legale le deleghe necessarie e risorse sufficienti per consentire la sua cooperazione efficiente e tempestiva con le autorità competenti o i CSIRT.
3. Il rappresentante è stabilito in uno degli Stati membri in cui il soggetto offre i propri servizi. Il soggetto è considerato soggiacente alla giurisdizione dello Stato membro in cui è stabilito il suo rappresentante. I soggetti ad alto impatto e a impatto critico notificano il nome, l'indirizzo postale, l'indirizzo di posta elettronica e il numero di telefono del loro rappresentante legale all'autorità competente nello Stato membro in cui il rappresentante legale risiede o è stabilito.
4. Il rappresentante legale designato può essere ritenuto responsabile del mancato rispetto degli obblighi derivanti dal presente regolamento, fatte salve le responsabilità e le azioni legali che potrebbero essere avviate nei confronti del soggetto ad alto impatto o a impatto critico.
5. Nell'assenza di un rappresentante nell'Unione designato a norma del presente articolo, qualsiasi Stato membro in cui il soggetto fornisce servizi può avviare un'azione legale nei suoi confronti per mancato rispetto degli obblighi di cui al presente regolamento.
6. La designazione di un rappresentante legale all'interno dell'Unione a norma del paragrafo 1 non equivale a uno stabilimento nell'Unione.

Articolo 16

Cooperazione tra l'ENTSO per l'energia elettrica e l'EU DSO

1. L'ENTSO per l'energia elettrica e l'EU DSO cooperano nello svolgimento delle valutazioni dei rischi per la cibersicurezza a norma degli articoli 19 e 21, in particolare per quanto riguarda i seguenti compiti:
   (a) elaborazione delle metodologie di valutazione dei rischi per la cibersicurezza di cui all'articolo 18, paragrafo 1;
   (b) elaborazione della relazione globale di valutazione transfrontaliera del rischio per la cibersicurezza dell'energia elettrica a norma dell'articolo 23;

(c) elaborazione del quadro comune per la cibersicurezza dell'energia elettrica a norma del capo III;

(d) formulazione della raccomandazione per gli appalti riguardo alla cibersicurezza a norma dell'articolo 35;

(e) elaborazione della metodologia della scala di classificazione degli attacchi informatici a norma dell'articolo 37, paragrafo 8;

(f) elaborazione dell'indice provvisorio di impatto sulla cibersicurezza dell'energia elettrica (ECII) a norma dell'articolo 48, paragrafo 1, lettera a);

(g) stesura dell'elenco provvisorio consolidato dei soggetti ad alto impatto e a impatto critico a norma dell'articolo 48, paragrafo 3;

(h) stesura dell'elenco provvisorio dei processi ad alto impatto e a impatto critico a livello dell'Unione a norma dell'articolo 48, paragrafo 4;

(i) stesura dell'elenco provvisorio delle norme e dei controlli europei e internazionali a norma dell'articolo 48, paragrafo 6;

(j) esecuzione della valutazione dei rischi per la cibersicurezza a livello dell'Unione a norma dell'articolo 19;

(k) esecuzione delle valutazioni dei rischi per la cibersicurezza a livello regionale a norma dell'articolo 21;

(l) definizione dei piani di attenuazione dei rischi per la cibersicurezza a livello regionale a norma dell'articolo 22;

(m) elaborazione di orientamenti su sistemi europei di certificazione della cibersicurezza per prodotti TIC, servizi TIC e processi TIC conformemente all'articolo 36;

(n) elaborazione di orientamenti per l'attuazione del presente regolamento in consultazione con l'ACER e l'ENISA.

2. La cooperazione tra l'ENTSO per l'energia elettrica e l'EU DSO può prendere la forma di un gruppo di lavoro sui rischi per la cibersicurezza.

3. L'ENTSO per l'energia elettrica e l'EU DSO informano regolarmente l'ACER, l'ENISA, il gruppo di cooperazione NIS e il gruppo di coordinamento per l'energia elettrica in merito ai progressi compiuti nell'attuazione delle valutazioni del rischio per la cibersicurezza a livello dell'Unione e regionale a norma degli articoli 19 e 21.

Articolo 17

Cooperazione tra l'ACER e le autorità competenti

L'ACER, in cooperazione con ciascuna autorità competente:

(1) controlla l'attuazione delle misure di gestione dei rischi per la cibersicurezza a norma dell'articolo 12, paragrafo 2, lettera a), e degli obblighi di rendicontazione a norma dell'articolo 27 e di segnalazione a norma dell'articolo 39; e

(2) controlla il processo di adozione e l'attuazione dei termini e condizioni, delle metodologie o dei piani a norma dell'articolo 6, paragrafi 2 e 3. La cooperazione tra l'ACER, l'ENISA e ciascuna autorità competente può prendere la forma di un organismo di monitoraggio dei rischi per la cibersicurezza.

CAPO II

VALUTAZIONE DEI RISCHI E INDIVIDUAZIONE DEI RISCHI DI CIBERSICUREZZA

Articolo 18

Metodologie di valutazione del rischio per la cibersicurezza

1. Entro il [*OP: inserire la data corrispondente a nove mesi dall'entrata in vigore del presente regolamento*], i TSO, con l'assistenza dell'ENTSO per l'energia elettrica, in cooperazione con l'EU DSO e previa consultazione del gruppo di cooperazione NIS, presentano una proposta di metodologie di valutazione del rischio per la cibersicurezza a livello dell'Unione, a livello regionale e a livello di Stato membro.

2. Le metodologie di valutazione del rischio per la cibersicurezza a livello dell'Unione, a livello regionale e a livello di Stato membro comprendono:

   (a) un elenco delle minacce informatiche da considerare, comprendente almeno le seguenti minacce alla catena di approvvigionamento:

      i) un deterioramento grave e imprevisto della catena di approvvigionamento;

      ii) l'indisponibilità di prodotti TIC, servizi TIC o processi TIC nella catena di approvvigionamento;

      iii) attacchi informatici avviati attraverso attori della catena di approvvigionamento;

      iv) la fuga di informazioni sensibili attraverso la catena di approvvigionamento, anche attraverso il tracciamento della catena di approvvigionamento;

      v) l'introduzione di punti deboli o di backdoor nei prodotti TIC, nei servizi TIC o nei processi TIC attraverso gli attori della catena di approvvigionamento;

   (b) i criteri per valutare l'impatto del rischio per la cibersicurezza come alto o critico, utilizzando soglie definite per le conseguenze e per la probabilità;

   (c) un approccio per analizzare il rischio per la cibersicurezza derivante da sistemi legacy, da effetti a cascata degli attacchi informatici e dal funzionamento in tempo reale dei sistemi che gestiscono la rete;

   (d) un approccio per analizzare il rischio per la cibersicurezza derivante dalla dipendenza da un unico fornitore di prodotti TIC, servizi TIC o processi TIC.

3. Le metodologie di valutazione del rischio per la cibersicurezza a livello dell'Unione, a livello regionale e a livello di Stato membro fanno uso di un'unica matrice dell'impatto del rischio. La matrice dell'impatto del rischio:

   (a) misura le conseguenze degli attacchi informatici sulla base dei criteri seguenti:

      i) perdita di carico;

      ii) riduzione della produzione di energia;

      iii) perdita di capacità della riserva di regolazione primaria della frequenza;

iv) perdita di capacità di ripristino del funzionamento della rete elettrica senza utilizzare una rete di trasmissione esterna per il riavvio dopo un arresto totale o parziale (detta anche "capacità di black start");

v) durata prevista di un'interruzione dell'energia elettrica che si ripercuote sui clienti in combinazione con l'entità dell'indisponibilità in numero di clienti; e

vi) ogni altro criterio quantitativo o qualitativo che possa ragionevolmente fungere da indicatore dell'effetto di un attacco informatico sui flussi transfrontalieri di energia elettrica;

(b) misura la probabilità di un incidente in termini di frequenza annuale di attacchi informatici.

4. Le metodologie di valutazione del rischio per la cibersicurezza a livello di Unione descrivono il modo in cui saranno definiti i valori ECII per le soglie di alto impatto e di impatto critico. L'ECII consente ai soggetti di stimare, valendosi dei criteri di cui al paragrafo 2, lettera b), l'impatto dei rischi sui loro processi operativi durante le valutazioni dell'impatto operativo svolte a norma dell'articolo 26, paragrafo 4, lettera c), punto i).

5. L'ENTSO per l'energia elettrica, in coordinamento con l'EU DSO, informa il gruppo di coordinamento per l'energia elettrica in merito alle proposte di metodologie di valutazione del rischio per la cibersicurezza elaborate a norma del paragrafo 1.

Articolo 19

Valutazione del rischio per la cibersicurezza a livello dell'Unione

1. Entro 9 mesi dall'approvazione delle metodologie di valutazione del rischio per la cibersicurezza a norma dell'articolo 8 e successivamente ogni tre anni, l'ENTSO per l'energia elettrica, in cooperazione con l'EU DSO e in consultazione con il gruppo di cooperazione NIS, effettua, fatto salvo l'articolo 22 della direttiva (UE) 2022/2555, una valutazione del rischio per la cibersicurezza a livello dell'Unione ed elabora un progetto di relazione sulla valutazione del rischio per la cibersicurezza a livello dell'Unione. A tal fine saranno utilizzate le metodologie sviluppate a norma dell'articolo 18 e approvate a norma dell'articolo 8 per individuare, analizzare e valutare le possibili conseguenze degli attacchi informatici che incidono sulla sicurezza operativa del sistema elettrico e perturbano i flussi transfrontalieri di energia elettrica. La valutazione del rischio per la cibersicurezza a livello dell'Unione non tiene conto dei danni di natura giuridica o finanziaria o dei danni alla reputazione causati da attacchi informatici.

2. La relazione di valutazione del rischio per la cibersicurezza a livello dell'Unione comprende i seguenti elementi:

(a) i processi ad alto impatto e a impatto critico a livello dell'Unione;

(b) una matrice dell'impatto del rischio che i soggetti e le autorità competenti utilizzano per valutare il rischio per la cibersicurezza individuato nella valutazione del rischio per la cibersicurezza a livello di Stato membro effettuata a norma dell'articolo 20 e nella valutazione del rischio per la cibersicurezza a livello di soggetto a norma dell'articolo 26, paragrafo 2, lettera b).

3. Per quanto riguarda i processi ad alto impatto e a impatto critico a livello dell'Unione, la relazione di valutazione del rischio per la cibersicurezza a livello dell'Unione comprende:

   (a) una valutazione delle possibili conseguenze di un attacco informatico utilizzando i parametri definiti nella metodologia di valutazione del rischio per la cibersicurezza elaborata a norma dell'articolo 18, paragrafi 2, 3 e 4, e approvata a norma dell'articolo 8;

   (b) l'ECII e le soglie di alto impatto e di impatto critico che le autorità competenti utilizzano a norma dell'articolo 24, paragrafi 1 e 2, per individuare i soggetti ad alto impatto e a impatto critico coinvolti nei processi ad alto impatto e a impatto critico a livello dell'Unione.

4. L'ENTSO per l'energia elettrica, in cooperazione con l'EU DSO, presenta all'ACER, per parere, il progetto di relazione di valutazione del rischio per la cibersicurezza a livello dell'Unione con i relativi risultati. L'ACER formula un parere sul progetto di relazione entro tre mesi dal ricevimento. L'ENTSO per l'energia elettrica e l'EU DSO ultimano la relazione tenendo nella massima considerazione il parere dell'ACER.

5. Entro tre mesi dal ricevimento del parere dell'ACER, l'ENTSO per l'energia elettrica, in cooperazione con l'EU DSO, notifica la relazione finale di valutazione del rischio per la cibersicurezza a livello dell'Unione all'ACER, alla Commissione, all'ENISA e alle autorità competenti.

Articolo 20

Valutazione del rischio per la cibersicurezza a livello di Stato membro

1. L'autorità competente effettua una valutazione del rischio per la cibersicurezza dello Stato membro valutando tutti i soggetti ad alto impatto e a impatto critico nello Stato membro con le metodologie elaborate a norma dell'articolo 18 e approvate a norma dell'articolo 8. La valutazione del rischio per la cibersicurezza a livello di Stato membro individua e analizza i rischi di attacchi informatici che incidono sulla sicurezza operativa del sistema elettrico e perturbano i flussi transfrontalieri di energia elettrica. La valutazione del rischio per la cibersicurezza a livello di Stato membro non tiene conto dei danni di natura giuridica o finanziaria o dei danni alla reputazione causati da attacchi informatici.

2. Entro 21 mesi dalla notifica dei soggetti ad alto impatto e a impatto critico a norma dell'articolo 24, paragrafo 6, e ogni tre anni dopo tale data, e previa consultazione dell'autorità competente per la cibersicurezza dell'energia elettrica, l'autorità competente, con il sostegno del CSIRT, presenta all'ENTSO per l'energia elettrica e all'EU DSO una relazione di valutazione del rischio per la cibersicurezza a livello di Stato membro contenente le seguenti informazioni per ciascun processo operativo ad alto impatto e a impatto critico:

   (a) lo stato di attuazione dei controlli minimi e avanzati di cibersicurezza a norma dell'articolo 29;

   (b) un elenco di tutti gli attacchi informatici segnalati nei tre anni precedenti a norma dell'articolo 38, paragrafo 3;

   (c) una sintesi di tutte le minacce informatiche segnalate nei tre anni precedenti a norma dell'articolo 38, paragrafo 6;

(d) per ciascun processo ad alto impatto o a impatto critico a livello dell'Unione, una stima del rischio di compromissione della riservatezza, dell'integrità e della disponibilità delle informazioni e degli asset corrispondenti;

(e) se necessario, un elenco di altri soggetti individuati come ad alto impatto o a impatto critico a norma dell'articolo 24, paragrafi 1, 2, 3 e 5.

3. La relazione di valutazione del rischio per la cibersicurezza a livello di Stato membro tiene conto del piano di preparazione ai rischi dello Stato membro elaborato a norma dell'articolo 10 del regolamento (UE) 2019/941.

4. Le informazioni contenute nella relazione di valutazione del rischio per la cibersicurezza a livello di Stato membro a norma del paragrafo 2, lettere da a) a d), non sono collegate a soggetti o asset specifici. La relazione di valutazione del rischio per la cibersicurezza a livello di Stato membro include anche una valutazione del rischio delle deroghe temporanee rilasciate dalle autorità competenti degli Stati membri a norma dell'articolo 30.

5. L'ENTSO per l'energia elettrica e l'EU DSO possono richiedere informazioni supplementari alle autorità competenti in relazione ai compiti di cui al paragrafo 2, lettere a) e c).

6. Le autorità competenti garantiscono che le informazioni da esse fornite sono esatte e corrette.

Articolo 21

Valutazioni del rischio per la cibersicurezza a livello regionale

1. L'ENTSO per l'energia elettrica, in collaborazione con l'EU DSO e in consultazione con il pertinente centro di coordinamento regionale, effettua una valutazione del rischio per la cibersicurezza a livello regionale per ciascuna regione di gestione del sistema, utilizzando le metodologie elaborate a norma dell'articolo 19 e approvate a norma dell'articolo 8, al fine di individuare, analizzare e valutare i rischi di attacchi informatici che incidono sulla sicurezza operativa del sistema elettrico e perturbano i flussi transfrontalieri di energia elettrica. Le valutazioni del rischio per la cibersicurezza a livello regionale non tengono conto dei danni di natura giuridica o finanziaria o dei danni alla reputazione causati da attacchi informatici.

2. Entro 30 mesi dalla notifica dei soggetti ad alto impatto e a impatto critico a norma dell'articolo 24, paragrafo 6, e successivamente ogni tre anni, l'ENTSO per l'energia elettrica, in cooperazione con l'EU DSO e in consultazione con il gruppo di cooperazione NIS, redige una relazione di valutazione del rischio per la cibersicurezza a livello regionale per ciascuna regione di gestione del sistema.

3. La relazione di valutazione del rischio per la cibersicurezza a livello regionale tiene conto delle informazioni pertinenti contenute nelle relazioni di valutazione del rischio per la cibersicurezza a livello dell'Unione e nelle relazioni di valutazione del rischio per la cibersicurezza a livello di Stati membri.

4. La valutazione del rischio per la cibersicurezza a livello regionale tiene conto degli scenari regionali di crisi dell'energia elettrica connessi alla cibersicurezza individuati a norma dell'articolo 6 del regolamento (UE) 2019/941.

Articolo 22

Piani di attenuazione dei rischi per la cibersicurezza a livello regionale

1. Entro 36 mesi dalla notifica dei soggetti ad alto impatto e a impatto critico a norma dell'articolo 24, paragrafo 6, e non oltre il [*OP: inserire la data corrispondente a 84 mesi dopo l'entrata in vigore*], e successivamente ogni tre anni, i TSO, con l'ausilio dell'ENTSO per l'energia elettrica, in cooperazione con l'EU DSO e in consultazione con il gruppo di cooperazione NIS, elabora un piano di attenuazione dei rischi per la cibersicurezza a livello regionale per ciascuna regione di gestione del sistema.

2. I piani di attenuazione dei rischi per la cibersicurezza a livello regionale comprendono:

   (a) i controlli minimi e avanzati di cibersicurezza che i soggetti ad alto impatto e a impatto critico devono applicare nella regione di gestione del sistema;

   (b) i rischi residui di cibersicurezza nelle regioni di gestione del sistema dopo l'applicazione dei controlli di cui alla lettera a).

3. L'ENTSO per l'energia elettrica trasmette i piani di attenuazione dei rischi a livello regionale ai pertinenti gestori dei sistemi di trasmissione, alle autorità competenti e al gruppo di coordinamento per l'energia elettrica. Il gruppo di coordinamento per l'energia elettrica può raccomandare modifiche.

4. I TSO, con l'assistenza dell'ENTSO per l'energia elettrica, in collaborazione con l'EU DSO e in consultazione con il gruppo di cooperazione NIS, aggiornano i piani di attenuazione dei rischi a livello regionale ogni tre anni, a meno che le circostanze giustifichino aggiornamenti più frequenti.

Articolo 23

Relazione globale di valutazione transfrontaliera del rischio per la cibersicurezza dell'energia elettrica

1. Entro 40 mesi dalla notifica dei soggetti ad alto impatto e a impatto critico a norma dell'articolo 24, paragrafo 6, e successivamente ogni tre anni, i TSO, con l'assistenza dell'ENTSO per l'energia elettrica, in cooperazione con l'EU DSO e in consultazione con il gruppo di cooperazione NIS, trasmettono al gruppo di coordinamento per l'energia elettrica una relazione sull'esito della valutazione del rischio per la cibersicurezza in relazione ai flussi transfrontalieri di energia elettrica ("relazione globale di valutazione transfrontaliera del rischio per la cibersicurezza dell'energia elettrica").

2. La relazione globale di valutazione transfrontaliera del rischio per la cibersicurezza dell'energia elettrica si basa sulle relazioni di valutazione del rischio per la cibersicurezza a livello dell'Unione, di Stati membri e di regioni e comprende le seguenti informazioni:

   (a) l'elenco dei processi a livello dell'Unione ad alto impatto e a impatto critico individuati nella relazione di valutazione del rischio per la cibersicurezza a livello dell'Unione conformemente all'articolo 19, paragrafo 2, lettera a), compresa la stima della probabilità e dell'impatto dei rischi per la cibersicurezza valutati nelle relazioni di valutazione del rischio per la

cibersicurezza a livello regionale a norma dell'articolo 21, paragrafo 2, e dell'articolo 19, paragrafo 3, lettera a);

(b) le minacce informatiche attuali, con particolare attenzione alle minacce e ai rischi emergenti per il sistema elettrico;

(c) gli attacchi informatici del periodo precedente a livello dell'Unione, con una sintesi critica di come tali attacchi informatici possono aver avuto un impatto sui flussi transfrontalieri di energia elettrica;

(d) la situazione generale dell'attuazione delle misure di cibersicurezza;

(e) la situazione dei flussi di informazioni a norma degli articoli 37 e 38;

(f) l'elenco delle informazioni o i criteri specifici per la classificazione delle informazioni a norma dell'articolo 46;

(g) i rischi individuati ed evidenziati che possono derivare da una gestione non sicura della catena di approvvigionamento;

(h) i risultati e le esperienze acquisiti con le esercitazioni di cibersicurezza regionali e transregionali organizzate a norma dell'articolo 44;

(i) un'analisi dello sviluppo dei rischi transfrontalieri complessivi per la cibersicurezza nel settore dell'energia elettrica dopo le ultime valutazioni del rischio per la cibersicurezza a livello regionale;

(j) ogni altra informazione che possa essere utile per individuare eventuali perfezionamenti del presente regolamento o la necessità di una revisione del presente regolamento o di uno dei suoi strumenti; e

(k) informazioni aggregate e anonimizzate sulle deroghe concesse a norma dell'articolo 30, paragrafo 3.

3. I soggetti elencati all'articolo 2, paragrafo 1, possono contribuire all'elaborazione della relazione globale di valutazione transfrontaliera del rischio per la cibersicurezza dell'energia elettrica, nel rispetto della riservatezza delle informazioni conformemente all'articolo 47. I TSO, con l'assistenza dell'ENTSO per l'energia elettrica e in collaborazione con l'EU DSO, consultano questi soggetti sin dalle prime fasi.

4. La relazione globale di valutazione transfrontaliera del rischio per la cibersicurezza dell'energia elettrica è soggetta alle disposizioni sulla protezione dello scambio di informazioni a norma dell'articolo 46. Fatti salvi l'articolo 10, paragrafo 4, e l'articolo 47, paragrafo 4, l'ENTSO per l'energia elettrica e l'EU DSO divulgano una versione pubblica della relazione che non contiene informazioni suscettibili di arrecare danni ai soggetti elencati all'articolo 2, paragrafo 1. La versione pubblica della relazione non è divulgata senza l'accordo del gruppo di cooperazione NIS e del gruppo di coordinamento per l'energia elettrica. L'ENTSO per l'energia elettrica, in coordinamento con l'EU DSO, è responsabile della compilazione e della divulgazione della versione pubblica della relazione.

Articolo 24

Individuazione dei soggetti ad alto impatto e a impatto critico

1. L'autorità competente individua, utilizzando l'ECII e le soglie di alto impatto e di impatto critico inclusi nella relazione di valutazione del rischio per la cibersicurezza

a livello dell'Unione di cui all'articolo 19, paragrafo 3, lettera b), i soggetti ad alto impatto e a impatto critico nel proprio Stato membro che sono coinvolti nei processi ad alto impatto e a impatto critico a livello dell'Unione. Le autorità competenti possono richiedere informazioni a un soggetto nel loro Stato membro per determinarne i valori ECII. Se l'ECII determinato di un soggetto è superiore alla soglia di alto impatto o di impatto critico, il soggetto individuato è elencato nella relazione di valutazione del rischio per la cibersicurezza dello Stato membro di cui all'articolo 20, paragrafo 2.

2. L'autorità competente individua, utilizzando l'ECII e le soglie di alto impatto e di impatto critico inclusi nella relazione di valutazione del rischio per la cibersicurezza a livello dell'Unione di cui all'articolo 19, paragrafo 3, lettera b), i soggetti ad alto impatto e a impatto critico non stabiliti nell'Unione che sono attivi nell'Unione. L'autorità competente può richiedere informazioni a un soggetto non stabilito nell'Unione per determinarne i valori ECII.

3. L'autorità competente può individuare altri soggetti nel proprio Stato membro come soggetti ad alto impatto o a impatto critico se sono soddisfatti i seguenti criteri:

   (a) il soggetto fa parte di un gruppo di soggetti esposti a un rischio significativo di subire simultaneamente un attacco informatico;

   (b) l'ECII aggregato per il gruppo di soggetti è superiore alla soglia di alto impatto o di impatto critico.

4. Se l'autorità competente individua altri soggetti conformemente al paragrafo 3, tutti i processi presso tali soggetti per i quali l'ECII aggregato del gruppo è superiore alla soglia di alto impatto sono considerati processi ad alto impatto e tutti i processi presso tali soggetti per i quali l'ECII aggregato del gruppo supera le soglie di impatto critico sono considerati processi a impatto critico.

5. Se l'autorità competente individua soggetti di cui al paragrafo 3, lettera a), in più Stati membri, ne informa le rispettive autorità competenti, l'ENTSO per l'energia elettrica e l'EU DSO. L'ENTSO per l'energia elettrica, in cooperazione con l'EU DSO, sulla base delle informazioni ricevute da tutte le autorità competenti, fornisce alle autorità competenti un'analisi dell'aggregazione di soggetti in più di uno Stato membro che può creare un disturbo distribuito ai flussi transfrontalieri di energia elettrica ed eventualmente risultare in un attacco informatico. Se un gruppo di soggetti in più Stati membri è individuato come un'aggregazione il cui ECII è superiore alla soglia di alto impatto o di impatto critico, tutte le autorità competenti interessate individuano i soggetti che vi appartengono come soggetti ad alto impatto o a impatto critico per il rispettivo Stato membro, sulla base dell'ECII aggregato per il gruppo di soggetti, e i soggetti così individuati sono elencati nella relazione di valutazione del rischio per la cibersicurezza a livello dell'Unione.

6. Entro nove mesi dalla notifica da parte dell'ENTSO per l'energia elettrica e dell'EU DSO della relazione di valutazione del rischio per la cibersicurezza a livello dell'Unione a norma dell'articolo 19, paragrafo 5, e in ogni caso entro il [*OP: inserire la data corrispondente a 48 mesi dopo l'entrata in vigore*], l'autorità competente notifica ai soggetti figuranti nell'elenco che sono stati individuati come soggetti ad alto impatto o a impatto critico nello Stato membro.

7. Quando un prestatore di servizi è segnalato all'autorità competente come prestatore di servizi TIC critico a norma dell'articolo 27, lettera c), l'autorità lo notifica alle autorità competenti degli Stati membri in cui ha sede il prestatore o il suo

rappresentante. Quest'ultima autorità competente notifica al prestatore di servizi che è stato identificato come prestatore di servizi critici.

Articolo 25

Sistemi nazionali di verifica

1. Le autorità competenti possono istituire un sistema nazionale di verifica per accertare che i soggetti a impatto critico individuati a norma dell'articolo 24, paragrafo 1, abbiano attuato il quadro legislativo nazionale incluso nella matrice di mappatura di cui all'articolo 34. Il sistema nazionale di verifica può basarsi su un'ispezione effettuata dall'autorità competente, su audit di sicurezza indipendenti o su valutazioni reciproche inter pares effettuate da soggetti a impatto critico dello stesso Stato membro sotto la supervisione dell'autorità competente.

2. L'autorità competente che decide di istituire un sistema nazionale di verifica garantisce che la verifica sia effettuata conformemente ai seguenti requisiti:

   (a) qualsiasi soggetto che effettua la valutazione inter pares, l'audit o l'ispezione è indipendente dal soggetto a impatto critico sottoposto a verifica e non ha conflitti di interesse;

   (b) il personale che effettua la valutazione inter pares, l'audit o l'ispezione ha una conoscenza dimostrabile di:

      i) cibersicurezza nel settore dell'energia elettrica;

      ii) sistemi di gestione della cibersicurezza;

      iii) principi di auditing;

      iv) valutazione del rischio per la cibersicurezza;

      v) il quadro comune per la cibersicurezza dell'energia elettrica;

      vi) il quadro legislativo e regolamentare nazionale e le norme europee e internazionali applicabili all'ambito della verifica;

      vii) i processi a impatto critico nell'ambito della verifica;

   (c) al soggetto che effettua la valutazione inter pares, l'audit o l'ispezione è concesso un periodo di tempo sufficiente per svolgere tali attività;

   (d) il soggetto che effettua la verifica inter pares, l'audit o l'ispezione adotta le misure appropriate per proteggere le informazioni raccolte durante la verifica, in linea con il loro livello di riservatezza; e

   (e) le verifiche inter pares, gli audit o le ispezioni sono effettuati almeno una volta all'anno e coprono l'intero ambito della verifica almeno ogni tre anni.

3. L'autorità competente che decide di istituire un sistema nazionale di verifica comunica annualmente all'ACER la frequenza con cui ha effettuato le ispezioni nell'ambito del sistema.

Articolo 26

Gestione del rischio per la cibersicurezza a livello di soggetto

1. Il soggetto ad alto impatto e a impatto critico individuato dalle autorità competenti a norma dell'articolo 24, paragrafo 1, gestisce il rischio per la cibersicurezza di tutti gli asset nei suoi perimetri ad alto impatto e a impatto critico. Il soggetto ad alto impatto e a impatto critico effettua ogni tre anni la gestione del rischio secondo le fasi di cui al paragrafo 2.

2. Il soggetto ad alto impatto e a impatto critico fonda la propria gestione del rischio per la cibersicurezza su un approccio che mira a proteggere i propri sistemi informatici e di rete e comprende le seguenti fasi:

   (a) definizione del contesto;

   (b) valutazione del rischio per la cibersicurezza a livello di soggetto;

   (c) trattamento del rischio per la cibersicurezza;

   (d) accettazione del rischio per la cibersicurezza.

3. Durante la fase di definizione del contesto, il soggetto ad alto impatto e a impatto critico:

   (a) definisce l'ambito di applicazione della valutazione del rischio per la cibersicurezza, compresi i processi ad alto impatto e a impatto critico individuati dall'ENTSO per l'energia elettrica e dall'EU DSO e altri processi suscettibili di subire attacchi informatici ad alto impatto o a impatto critico sui flussi transfrontalieri di energia elettrica; e

   (b) definisce i criteri per la valutazione e l'accettazione del rischio conformemente alla matrice di impatto del rischio che i soggetti e le autorità competenti utilizzano nelle metodologie di valutazione del rischio per la cibersicurezza a livello dell'Unione, a livello regionale e a livello di Stato membro elaborate dall'ENTSO per l'energia elettrica e dall'EU DSO conformemente all'articolo 19, paragrafo 2.

4. Durante la fase di valutazione del rischio per la cibersicurezza il soggetto ad alto impatto e a impatto critico:

   (a) individua i rischi per la cibersicurezza tenendo conto:

      i) di tutti gli asset che intervengono nei processi ad alto impatto e a impatto critico a livello dell'Unione, con una valutazione del possibile impatto sui flussi transfrontalieri di energia elettrica in caso di compromissione dell'asset;

      ii) delle possibili minacce informatiche considerando quelle individuate nell'ultima relazione di valutazione globale del rischio per la cibersicurezza transfrontaliera dell'energia elettrica di cui all'articolo 23 e delle minacce alla catena di approvvigionamento;

      iii) delle vulnerabilità, comprese le vulnerabilità nei sistemi legacy;

      iv) dei possibili scenari di attacco informatico, compresi gli attacchi informatici che incidono sulla sicurezza operativa del sistema elettrico e interrompono i flussi transfrontalieri di energia elettrica;

v) delle pertinenti valutazioni del rischio effettuate a livello dell'Unione, comprese le valutazioni coordinate del rischio per le catene di approvvigionamento critiche conformemente all'articolo 22 della direttiva (UE) 2022/2555, e

vi) dei controlli già attuati;

(b) analizza la probabilità e le conseguenze dei rischi per la cibersicurezza individuati alla lettera a) e determina il livello del rischio per la cibersicurezza mediante la matrice di impatto utilizzata nelle metodologie di valutazione del rischio per la cibersicurezza a livello dell'Unione, a livello regionale e a livello di Stato membro elaborate dai TSO con l'assistenza dell'ENTSO per l'energia elettrica e in collaborazione con l'EU DSO conformemente all'articolo 19, paragrafo 2;

(c) classifica gli asset in base alle possibili conseguenze della compromissione della cibersicurezza e determina il perimetro ad alto impatto e a impatto critico procedendo come segue:

i) valuta, per tutti i processi oggetto della valutazione del rischio per la cibersicurezza, l'impatto operativo mediante l'ECII;

ii) classifica un processo come ad alto impatto critico o a impatto critico se il suo ECII supera le rispettive soglie;

iii) determina tutti gli asset ad alto impatto e a impatto critico necessari per i rispettivi processi;

iv) definisce i perimetri ad alto impatto e a impatto critico contenenti, rispettivamente, tutti gli asset ad alto impatto e a impatto critico, in modo da poterne controllare l'accesso;

(d) valuta il grado di priorità dei rischi per la cibersicurezza in base ai criteri di valutazione e di accettazione di cui al paragrafo 3, lettera b).

5. Durante la fase di trattamento del rischio per la cibersicurezza il soggetto ad alto impatto e a impatto critico stabilisce un piano di attenuazione dei rischi a livello di soggetto selezionando opzioni di trattamento del rischio adeguate per gestire i rischi e individuare quelli residui.

6. Durante la fase di accettazione del rischio per la cibersicurezza, il soggetto ad alto impatto e a impatto critico decide se accettare il rischio residuo sulla base dei criteri di accettazione di cui al paragrafo 3, lettera b).

7. Il soggetto ad alto impatto e a impatto critico registra in un inventario gli asset individuati al paragrafo 1. L'inventario di asset non fa parte della relazione di valutazione del rischio.

8. L'autorità competente può ispezionare gli asset dell'inventario durante le ispezioni.

Articolo 27

Rendicontazione del rischio a livello di soggetto

Entro 12 mesi dalla notifica dei soggetti ad alto impatto e a impatto critico a norma dell'articolo 24, paragrafo 6, e successivamente ogni tre anni, il soggetto ad alto impatto e a

impatto critico trasmette all'autorità competente una relazione contenente le informazioni seguenti:

(1) un elenco dei controlli selezionati per il piano di attenuazione dei rischi a livello di soggetto a norma dell'articolo 26, paragrafo 5, con l'attuale stato di attuazione di ciascun controllo;

(2) per ciascun processo ad alto impatto o a impatto critico a livello dell'Unione, una stima del rischio di compromissione della riservatezza, dell'integrità e della disponibilità delle informazioni e degli asset corrispondenti. La stima di tale rischio è ottenuta conformemente alla matrice di impatto del rischio di cui all'articolo 19, paragrafo 2;

(3) un elenco dei prestatori di servizi TIC critici per i processi a impatto critico del soggetto.

CAPO III

QUADRO COMUNE PER LA CIBERSICUREZZA DELL'ENERGIA ELETTRICA

Articolo 28

Composizione, funzionamento e riesame del quadro comune per la cibersicurezza dell'energia elettrica

1. Il quadro comune per la cibersicurezza dell'energia elettrica si compone dei seguenti controlli e del sistema di gestione della cibersicurezza:

   (a) i controlli minimi di cibersicurezza, elaborati conformemente all'articolo 29;

   (b) i controlli avanzati di cibersicurezza, elaborati conformemente all'articolo 29;

   (c) la matrice di mappatura, elaborata conformemente all'articolo 34, che rileva i controlli di cui alle lettere a) e b) in riferimento a norme europee e internazionali e quadri legislativi o regolamentari nazionali selezionati;

   (d) il sistema di gestione della cibersicurezza istituito in applicazione dell'articolo 32.

2. Tutti i soggetti ad alto impatto applicano i controlli minimi di cibersicurezza di cui al paragrafo 1, lettera a), all'interno del loro perimetro di alto impatto.

3. Tutti i soggetti a impatto critico applicano i controlli avanzati di cibersicurezza di cui al paragrafo 1, lettera b), all'interno del loro perimetro di impatto critico.

4. Entro 7 mesi dalla presentazione del primo progetto di relazione di valutazione del rischio per la cibersicurezza a livello dell'Unione a norma dell'articolo 19, paragrafo 4, il quadro comune per la cibersicurezza dell'energia elettrica di cui al paragrafo 1 è integrato dai controlli minimi e avanzati di cibersicurezza nella catena di approvvigionamento, elaborati a norma dell'articolo 33.

Articolo 29

Controlli minimi e avanzati di cibersicurezza

1. Entro 7 mesi dalla presentazione del primo progetto di relazione di valutazione del rischio per la cibersicurezza a livello dell'Unione a norma dell'articolo 19, paragrafo 4, i TSO, con l'assistenza dell'ENTSO per l'energia elettrica e in cooperazione con l'EU DSO, elaborano una proposta di controlli minimi e avanzati di cibersicurezza.

2. Entro 6 mesi dalla stesura della relazione di valutazione del rischio per la cibersicurezza a livello regionale a norma dell'articolo 21, paragrafo 2, i TSO, con l'assistenza dell'ENTSO per l'energia elettrica e in cooperazione con l'EU DSO, propongono all'autorità competente una modifica dei controlli minimi e avanzati di cibersicurezza. La proposta sarà conforme all'articolo 8, paragrafo 10, e terrà conto dei rischi individuati nella valutazione del rischio a livello regionale.

3. I controlli minimi e avanzati di cibersicurezza sono verificabili attraverso la partecipazione a un sistema nazionale di verifica secondo la procedura di cui all'articolo 31 o per mezzo di audit di sicurezza condotti da terzi indipendenti conformemente alle prescrizioni di cui all'articolo 25, paragrafo 2.

4. I controlli minimi e avanzati di cibersicurezza iniziali elaborati a norma del paragrafo 1 si basano sui rischi individuati nella relazione di valutazione del rischio per la cibersicurezza a livello dell'Unione di cui all'articolo 19, paragrafo 5. I controlli minimi e avanzati di cibersicurezza modificati elaborati a norma del paragrafo 2 si basano sulla relazione di valutazione del rischio per la cibersicurezza a livello regionale di cui all'articolo 21, paragrafo 2.

5. I controlli minimi di cibersicurezza comprendono controlli per proteggere le informazioni scambiate a norma dell'articolo 46.

6. Entro 12 mesi dall'approvazione dei controlli minimi e avanzati di cibersicurezza a norma dell'articolo 8, paragrafo 5, o dopo ciascun aggiornamento a norma dell'articolo 8, paragrafo 10, i soggetti elencati all'articolo 2, paragrafo 1, e identificati come soggetti a impatto critico e ad alto impatto a norma dell'articolo 24, durante la definizione del piano di attenuazione dei rischi a livello di soggetto a norma dell'articolo 26, paragrafo 5, applicano i controlli minimi di cibersicurezza all'interno del perimetro di alto impatto e i controlli avanzati di cibersicurezza all'interno del perimetro di impatto critico.

Articolo 30

Deroghe ai controlli minimi e avanzati di cibersicurezza

1. I soggetti elencati all'articolo 2, paragrafo 1, possono chiedere alla rispettiva autorità competente una deroga all'obbligo di applicare i controlli minimi e avanzati di cibersicurezza di cui all'articolo 29, paragrafo 6. L'autorità competente può concedere la deroga per uno dei motivi seguenti:

   (a) in circostanze eccezionali, se il soggetto può dimostrare che i costi di attuazione dei controlli di cibersicurezza superano significativamente i benefici. L'ACER e l'ENTSO per l'energia elettrica, in cooperazione con l'EU

DSO, possono elaborare congiuntamente orientamenti per stimare i costi dei controlli di cibersicurezza, ad uso dei soggetti;

(b) se il soggetto fornisce un piano di trattamento del rischio a livello di soggetto che attenua i rischi per la cibersicurezza utilizzando controlli alternativi a un livello accettabile conformemente ai criteri di accettazione del rischio di cui all'articolo 26, paragrafo 3, lettera b).

2. Entro tre mesi dal ricevimento della richiesta di cui al paragrafo 1, l'autorità competente interessata decide se concedere una deroga ai controlli minimi e avanzati di cibersicurezza. Le deroghe ai controlli minimi o avanzati di cibersicurezza sono concesse per un massimo di tre anni, con possibilità di rinnovo.

3. Le informazioni aggregate e anonimizzate per le deroghe concesse sono incluse in allegato alla relazione globale di valutazione transfrontaliera del rischio per la cibersicurezza dell'energia elettrica di cui all'articolo 23. Se necessario, l'ENTSO per l'energia elettrica e l'EU DSO aggiornano congiuntamente l'elenco.

Articolo 31

Verifica del quadro comune per la cibersicurezza dell'energia elettrica

1. Entro 24 mesi dall'adozione dei controlli di cui all'articolo 28, paragrafo 1, lettere a), b) e c), e dall'istituzione del sistema di gestione della cibersicurezza di cui alla lettera d) del medesimo articolo, il soggetto a impatto critico individuato a norma dell'articolo 24, paragrafo 1, è in grado di dimostrare la propria conformità al sistema di gestione della cibersicurezza e ai controlli minimi o avanzati di cibersicurezza, su richiesta dell'autorità competente.

2. Il soggetto a impatto critico adempie all'obbligo di cui al paragrafo 1 sottoponendosi a audit di sicurezza condotti da terzi indipendenti, conformemente ai requisiti di cui all'articolo 25, paragrafo 2, oppure partecipando a un sistema nazionale di verifica a norma dell'articolo 25, paragrafo 1.

3. La verifica della conformità del soggetto a impatto critico al sistema di gestione della cibersicurezza e ai controlli minimi o avanzati di cibersicurezza interessa tutti gli asset all'interno del perimetro di impatto critico del soggetto a impatto critico.

4. La verifica della conformità del soggetto a impatto critico al sistema di gestione della cibersicurezza e ai controlli minimi o avanzati di cibersicurezza si esegue nuovamente non più di 36 mesi dopo la fine della prima verifica e successivamente ogni tre anni.

5. Il soggetto a impatto critico definito conformemente all'articolo 24 dimostra la propria conformità ai controlli di cui all'articolo 28, paragrafo 1, lettere a), b) e c), e l'istituzione del sistema di gestione della cibersicurezza di cui alla lettera d) del medesimo articolo riferendo all'autorità competente in merito all'esito della verifica di conformità.

Articolo 32

Sistema di gestione della cibersicurezza

1. Entro 24 mesi dal ricevimento della notifica dell'autorità competente che lo individua come soggetto ad alto impatto o a impatto critico a norma dell'articolo 24, paragrafo 6, il soggetto ad alto impatto e a impatto critico istituisce un sistema di gestione della cibersicurezza, che successivamente riesamina ogni tre anni, al fine di:

   (a) determinare l'ambito di applicazione del sistema di gestione della cibersicurezza tenendo conto delle interfacce e delle dipendenze con altri soggetti;

   (b) garantire che l'integralità della sua alta dirigenza sia portata a conoscenza dei pertinenti obblighi giuridici e contribuisca attivamente all'attuazione del sistema di gestione della cibersicurezza con decisioni tempestive e reazioni rapide;

   (c) garantire la disponibilità delle risorse necessarie per il sistema di gestione della cibersicurezza;

   (d) istituire una politica in materia di cibersicurezza che è documentata e comunicata internamente in seno al soggetto e alle parti interessate dai rischi per la sicurezza;

   (e) attribuire e comunicare le responsabilità per i ruoli attinenti alla cibersicurezza;

   (f) gestire i rischi per la cibersicurezza a livello di soggetto come definito all'articolo 26;

   (g) determinare e fornire le risorse necessarie per l'attuazione, il mantenimento e il miglioramento continuo del sistema di gestione della cibersicurezza, tenendo conto delle necessarie competenze e della conoscenza delle risorse per la cibersicurezza;

   (h) determinare la comunicazione interna ed esterna pertinente alla cibersicurezza;

   (i) creare, aggiornare e controllare le informazioni documentate relative al sistema di gestione della cibersicurezza;

   (j) valutare le prestazioni e l'efficacia del sistema di gestione della cibersicurezza;

   (k) effettuare audit interni a intervalli pianificati per garantire che il sistema di gestione della cibersicurezza sia attuato e mantenuto in modo efficace;

   (l) riesaminare l'attuazione del sistema di gestione della cibersicurezza a intervalli pianificati; controllare e correggere la non conformità delle risorse e delle attività alle politiche, alle procedure e agli orientamenti del sistema di gestione della cibersicurezza.

2. L'ambito di applicazione del sistema di gestione della cibersicurezza comprende tutti gli asset all'interno del perimetro ad alto impatto e a impatto critico del soggetto ad alto impatto e a impatto critico.

3. Le autorità competenti, evitando di imporre o discriminare l'uso di un particolare tipo di tecnologia, incoraggiano l'uso di norme e specifiche europee o internazionali relative ai sistemi di gestione e pertinenti alla sicurezza dei sistemi informatici e di rete.

Articolo 33

Controlli minimi e avanzati di cibersicurezza nella catena di approvvigionamento

1. Entro 7 mesi dalla presentazione del primo progetto di relazione di valutazione del rischio per la cibersicurezza a livello dell'Unione a norma dell'articolo 19, paragrafo 4, i TSO, con l'assistenza dell'ENTSO per l'energia elettrica e in cooperazione con l'EU DSO, elaborano una proposta di controlli minimi e avanzati di cibersicurezza nella catena di approvvigionamento volti ad attenuare i rischi che vi sono stati individuati dalle valutazioni del rischio per la cibersicurezza a livello dell'Unione, integrando i controlli minimi e avanzati di cibersicurezza elaborati a norma dell'articolo 29. I controlli minimi e avanzati di cibersicurezza nella catena di approvvigionamento sono elaborati insieme ai controlli minimi e avanzati di cibersicurezza a norma dell'articolo 29. I controlli minimi e avanzati di cibersicurezza nella catena di approvvigionamento coprono l'intero ciclo di vita di tutti i prodotti TIC, servizi TIC e processi TIC all'interno dei perimetri ad alto impatto o a impatto critico del soggetto ad alto impatto o a impatto critico. Il gruppo di cooperazione NIS è consultato in sede di elaborazione della proposta di controlli minimi e avanzati di cibersicurezza nella catena di approvvigionamento.

2. I controlli minimi di cibersicurezza nella catena di approvvigionamento consistono in controlli, per i soggetti ad alto impatto e a impatto critico, che:

   (a) comprendono raccomandazioni per gli appalti di prodotti TIC, servizi TIC e processi TIC con riferimento alle specifiche di cibersicurezza, riguardanti almeno:

      i) i controlli dei precedenti personali del personale del fornitore partecipante alla catena di approvvigionamento che tratta informazioni sensibili o ha accesso agli asset ad alto impatto o a impatto critico del soggetto. Il controllo dei precedenti personali può comprendere una verifica dell'identità e dei precedenti del personale o dei contraenti di un soggetto conformemente al diritto e alle procedure nazionali e al diritto dell'Unione pertinente e applicabile, compresi il regolamento (UE) 2016/679 e la direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio[24]. I controlli dei precedenti personali sono proporzionati e strettamente limitati a quanto necessario. Sono effettuati al solo scopo di valutare un potenziale rischio per la sicurezza del soggetto. Devono essere proporzionali ai requisiti commerciali, alla classificazione delle informazioni a cui gli interessati hanno accesso e ai rischi percepiti, e possono essere effettuati dal soggetto stesso, da una società esterna che effettua uno screening o da un organismo pubblico;

      ii) i processi di progettazione, sviluppo e produzione sicuri e controllati di prodotti TIC, servizi TIC e processi TIC, che promuovono la progettazione e lo sviluppo di prodotti TIC, servizi TIC e processi TIC, comprendenti misure tecniche adeguate per garantire la cibersicurezza;

[24] Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio (GU L 119 del 4.5.2016, pag. 89).

iii) la progettazione di sistemi informatici e di rete in cui operano dispositivi non ritenuti affidabili, anche quando situati all'interno di un perimetro sicuro, che richiedono la verifica di tutte le richieste ricevute e l'applicazione del principio del privilegio minimo;

iv) l'accesso del fornitore agli asset del soggetto;

v) gli obblighi contrattuali del fornitore di proteggere e limitare l'accesso alle informazioni sensibili del soggetto;

vi) il capitolato di appalto per la cibersicurezza imposto ai subcontraenti del fornitore;

vii) la tracciabilità dell'applicazione delle specifiche di cibersicurezza dallo sviluppo alla produzione fino alla fornitura dei prodotti TIC, servizi TIC o processi TIC;

viii) il sostegno agli aggiornamenti di sicurezza durante l'intero ciclo di vita dei prodotti TIC, servizi TIC o processi TIC;

ix) il diritto di sottoporre ad audit la cibersicurezza nei processi di progettazione, sviluppo e produzione del fornitore; e

x) la valutazione del profilo di rischio del fornitore;

(b) impongono a tali soggetti di tenere conto delle raccomandazioni per gli appalti di cui alla lettera a) al momento di concludere contratti con fornitori, collaboratori e altri partecipanti alla catena di approvvigionamento, riguardanti le consegne ordinarie di prodotti TIC, servizi TIC e processi TIC, nonché eventi e circostanze non previsti quali la risoluzione e la riassegnazione di contratti in caso di negligenza della parte contrattuale;

(c) impongono a tali soggetti di tenere conto dei risultati delle pertinenti valutazioni coordinate del rischio per la sicurezza delle catene di approvvigionamento critiche effettuate a norma dell'articolo 22, paragrafo 1, della direttiva (UE) 2022/2555;

(d) includono criteri per selezionare e appaltare fornitori in grado di soddisfare le specifiche di cibersicurezza di cui alla lettera a) e che possiedono un livello di cibersicurezza adeguato ai rischi per la cibersicurezza del prodotto TIC, del servizio TIC o dei processi TIC forniti;

(e) includono criteri per diversificare le fonti di approvvigionamento per i prodotti TIC, i servizi TIC e i processi TIC e ridurre il rischio di dipendenza da un fornitore;

(f) includono criteri per monitorare, rivedere o verificare periodicamente le specifiche di cibersicurezza per i processi operativi interni del fornitore durante l'intero ciclo di vita di ciascun prodotto TIC, servizio TIC e processo TIC.

3. Per le specifiche di cibersicurezza interessate dalla raccomandazione per gli appalti riguardo alla cibersicurezza di cui al paragrafo 2, lettera a), i soggetti ad alto impatto o a impatto critico utilizzano i principi relativi agli appalti a norma della direttiva 2014/24/CE, conformemente all'articolo 35, paragrafo 4, del presente regolamento, o definiscono le proprie specifiche sulla base dei risultati della valutazione del rischio per la cibersicurezza a livello di soggetto.

4. I controlli avanzati di cibersicurezza nella catena di approvvigionamento comprendono controlli per i soggetti a impatto critico destinati a verificare, durante la procedura di appalto, che i prodotti TIC, i servizi TIC e i processi TIC che saranno utilizzati come asset a impatto critico soddisfino le specifiche di cibersicurezza. Il prodotto TIC, il servizio TIC o il processo TIC è verificato mediante un sistema europeo di certificazione della cibersicurezza di cui all'articolo 31 o mediante attività di verifica selezionate e organizzate dal soggetto. Il dettaglio e l'ampiezza delle attività di verifica sono sufficienti a garantire che il prodotto TIC, il servizio TIC o il processo TIC possa essere utilizzato per attenuare i rischi individuati nella valutazione del rischio a livello di soggetto. Il soggetto a impatto critico documenta le misure adottate per ridurre i rischi individuati.

5. I controlli minimi e avanzati di cibersicurezza nella catena di approvvigionamento si applicano agli appalti di prodotti TIC, di servizi TIC e di processi TIC. I controlli minimi e avanzati di cibersicurezza della catena di approvvigionamento si applicheranno alle procedure di appalto nei soggetti individuati come ad alto impatto e a impatto critico a norma dell'articolo 24 avviate sei mesi dopo l'adozione o l'aggiornamento dei controlli minimi e avanzati di cibersicurezza di cui all'articolo 29.

6. Entro 6 mesi dalla stesura della relazione di valutazione del rischio per la cibersicurezza a livello regionale a norma dell'articolo 21, paragrafo 2, i TSO, con l'assistenza dell'ENTSO per l'energia elettrica e in cooperazione con l'EU DSO, propongono all'autorità competente una modifica dei controlli minimi e avanzati di cibersicurezza nella catena di approvvigionamento. La proposta sarà conforme all'articolo 8, paragrafo 10, e terrà conto dei rischi individuati nella valutazione del rischio a livello regionale.

Articolo 34

Matrice di mappatura dei controlli di cibersicurezza dell'energia elettrica in riferimento alle norme

1. Entro 7 mesi dalla presentazione del primo progetto di relazione di valutazione del rischio per la cibersicurezza a livello dell'Unione a norma dell'articolo 19, paragrafo 4, i TSO, con l'assistenza dell'ENTSO per l'energia elettrica, in cooperazione con l'EU DSO e in consultazione con l'ENISA, elaborano una proposta di matrice per la mappatura dei controlli di cui all'articolo 28, paragrafo 1, lettere a) e b), in riferimento a determinate norme europee e internazionali nonché alle pertinenti specifiche tecniche ("matrice di mappatura"). L'ENTSO per l'energia elettrica e l'EU DSO documentano l'equivalenza fra i diversi controlli e i controlli di cui all'articolo 28, paragrafo 1, lettere a) e b).

2. Le autorità competenti possono fornire all'ENTSO per l'energia elettrica e all'EU DSO una mappatura dei controlli di cui all'articolo 28, paragrafo 1, lettere a) e b), con un riferimento ai relativi quadri legislativi o regolamentari nazionali, comprese le pertinenti norme nazionali degli Stati membri a norma dell'articolo 25 della direttiva (UE) 2022/2555. Se l'autorità competente dello Stato membro fornisce una mappatura nazionale di questo tipo, l'ENTSO per l'energia elettrica e l'EU DSO la integrano nella matrice di mappatura.

3. Entro 6 mesi dalla stesura della relazione di valutazione del rischio per la cibersicurezza a livello regionale a norma dell'articolo 21, paragrafo 2, i TSO, con l'assistenza dell'ENTSO per l'energia elettrica, in cooperazione con l'EU DSO e in

consultazione con l'ENISA, propongono all'autorità competente una modifica della matrice di mappatura. La proposta sarà conforme all'articolo 8, paragrafo 10, e terrà conto dei rischi individuati nella valutazione del rischio a livello regionale.

CAPO IV

RACCOMANDAZIONI PER GLI APPALTI RIGUARDO ALLA CIBERSICUREZZA

Articolo 35

Raccomandazioni per gli appalti riguardo alla cibersicurezza

1. I TSO, con l'assistenza dell'ENTSO per l'energia elettrica e in cooperazione con l'EU DSO, elaborano, in un programma di lavoro da stabilire e aggiornare ogni volta che viene adottata una relazione regionale di valutazione del rischio per la cibersicurezza, serie di raccomandazioni non vincolanti per gli appalti riguardo alla cibersicurezza che i soggetti ad alto impatto e a impatto critico possono utilizzare come base per gli appalti di prodotti TIC, servizi TIC e processi TIC nei perimetri ad alto impatto e a impatto critico. Il programma di lavoro contiene:

   (a) una descrizione e una classificazione dei tipi di prodotti TIC, servizi TIC e processi TIC utilizzati dai soggetti ad alto impatto e a impatto critico nel perimetro ad alto impatto e a impatto critico;

   (b) un elenco dei tipi di prodotti TIC, servizi TIC e processi TIC per i quali è elaborata una serie di raccomandazioni non vincolanti riguardo alla cibersicurezza sulla base delle pertinenti relazioni di valutazione del rischio per la cibersicurezza a livello regionale e delle priorità dei soggetti ad alto impatto e a impatto critico.

2. Entro 6 mesi dall'adozione o dall'aggiornamento della relazione di valutazione del rischio per la cibersicurezza a livello regionale, l'ENTSO per l'energia elettrica, in cooperazione con l'EU DSO, trasmette all'ACER una sintesi del programma di lavoro.

3. I TSO, con l'assistenza dell'ENTSO per l'energia elettrica e in cooperazione con l'EU DSO, si adoperano per garantire che le raccomandazioni non vincolanti per gli appalti riguardo alla cibersicurezza elaborate sulla base della pertinente valutazione del rischio per la cibersicurezza a livello regionale siano simili o comparabili tra le diverse regioni di gestione del sistema. Le serie di raccomandazioni per gli appalti riguardo alla cibersicurezza coprono almeno le specifiche di cui all'articolo 33, paragrafo 2, lettera a). Ove possibile, le specifiche sono selezionate tra le norme europee e internazionali.

4. I TSO, con l'assistenza dell'ENTSO per l'energia elettrica e in collaborazione con l'EU DSO, garantiscono che le serie di raccomandazioni per gli appalti riguardo alla cibersicurezza:

   (a) rispettino i principi di aggiudicazione degli appalti a norma della direttiva 2014/24/CE; e

   (b) siano compatibili con i più recenti sistemi europei di certificazione della cibersicurezza disponibili per il prodotto TIC, il servizio TIC o il processo TIC e ne tengano conto.

Articolo 36

Orientamenti sull'uso dei sistemi europei di certificazione della cibersicurezza per gli appalti di prodotti TIC, servizi TIC e processi TIC

1. Le raccomandazioni non vincolanti per gli appalti riguardo alla cibersicurezza elaborate a norma dell'articolo 35 possono includere orientamenti settoriali sull'uso dei sistemi europei di certificazione della cibersicurezza, ogniqualvolta sia disponibile un sistema adeguato per un tipo di prodotto TIC, servizio TIC o processo TIC utilizzato dai soggetti a impatto critico, fatto salvo il quadro per l'istituzione di sistemi europei di certificazione della cibersicurezza a norma dell'articolo 46 del regolamento (UE) 2019/881.

2. I TSO, con l'assistenza dell'ENTSO per l'energia elettrica e in cooperazione con l'EU DSO, cooperano strettamente con l'ENISA nel fornire gli orientamenti settoriali specifici inclusi nelle raccomandazioni non vincolanti per gli appalti riguardo alla cibersicurezza a norma del paragrafo 1.

CAPO V

FLUSSI DI INFORMAZIONI, ATTACCHI INFORMATICI E GESTIONE DELLE CRISI

Articolo 37

Disposizioni sulla condivisione delle informazioni

1. L'autorità competente che riceve informazioni relative a un attacco informatico da segnalare:

   (a) valuta il livello di riservatezza di tali informazioni e informa il soggetto in merito all'esito della sua valutazione senza indebito ritardo e comunque entro 24 ore dal ricevimento delle informazioni;

   (b) si adopera per reperire eventuali altri attacchi informatici analoghi nell'Unione segnalati ad altre autorità competenti, al fine di correlare le informazioni ricevute nel contesto dell'attacco informatico da segnalare con quelle fornite nel contesto di altri attacchi informatici e di arricchire le informazioni esistenti, rafforzando e coordinando le risposte alle minacce alla cibersicurezza;

   (c) è responsabile della rimozione dei segreti commerciali e dell'anonimizzazione delle informazioni conformemente alle pertinenti disposizioni nazionali e dell'Unione;

   (d) condivide le informazioni con i punti di contatto unici nazionali, i CSIRT e tutte le autorità competenti designate a norma dell'articolo 4 in altri Stati membri, senza indebito ritardo ed entro 24 ore dalla presa di conoscenza di un attacco informatico da segnalare, e trasmette periodicamente informazioni aggiornate a dette autorità o organismi;

   (e) diffonde le informazioni relative all'attacco informatico, previa anonimizzazione e rimozione dei segreti commerciali a norma della lettera c) ai soggetti a impatto critico e ad alto impatto nel proprio Stato membro, senza indebito ritardo ed entro 24 ore dal ricevimento delle informazioni di cui alla

lettera a) e trasmette periodicamente informazioni aggiornate che consentano ai soggetti di organizzare efficacemente la propria difesa;

(f) possono chiedere al soggetto ad alto impatto o a impatto critico che ha riferito l'informazione su un attacco informatico da segnalare di diffonderla in modo sicuro ad altri soggetti che potrebbero esserne interessati, al fine di generare una consapevolezza situazionale nel settore dell'energia elettrica e prevenire il concretizzarsi di un rischio che potrebbe aggravarsi e diventare un incidente di cibersicurezza transfrontaliero;

(g) condivide con l'ENISA una relazione di sintesi, previa anonimizzazione e rimozione dei segreti commerciali, con le informazioni relative all'attacco informatico.

2. Il CSIRT che viene a conoscenza di una vulnerabilità sfruttata attivamente non risolta:

(a) la condivide senza indugio con l'ENISA attraverso un adeguato canale sicuro per lo scambio di informazioni, salvo se diversamente specificato in altre normative dell'Unione;

(b) presta assistenza al soggetto interessato per ottenere dal fabbricante o dal prestatore una gestione efficace, coordinata e rapida della vulnerabilità sfruttata attivamente non risolta o misure di attenuazione efficaci ed efficienti;

(c) condivide le informazioni disponibili con il fornitore e chiede al fabbricante o al prestatore, ove possibile, di individuare un elenco di CSIRT negli Stati membri interessati dalla vulnerabilità sfruttata attivamente non risolta cui trasmettere le medesime informazioni;

(d) condivide le informazioni disponibili con i CSIRT individuati al punto precedente, sulla base del principio della necessità di conoscere;

(e) condivide, ove esistano, strategie e misure di attenuazione della vulnerabilità sfruttata attivamente non risolta oggetto della segnalazione.

3. L'autorità competente che viene a conoscenza di una vulnerabilità sfruttata attivamente non risolta:

(a) condivide, ove esistano, strategie e misure di attenuazione della vulnerabilità sfruttata attivamente non risolta oggetto della segnalazione, in coordinazione con i CSIRT del proprio Stato membro;

(b) condivide le informazioni con un CSIRT dello Stato membro in cui è stata segnalata la vulnerabilità sfruttata attivamente non risolta.

4. L'autorità competente che viene a conoscenza di una vulnerabilità non risolta di cui non ha motivo di ritenere che sia già stata sfruttata attivamente si coordina senza indebito ritardo con il CSIRT ai fini della divulgazione coordinata della vulnerabilità come stabilito all'articolo 12, paragrafo 1, della direttiva (UE) 2022/2555.

5. Il CSIRT che riceve informazioni relative a minacce informatiche da uno o più soggetti ad alto impatto o a impatto critico a norma dell'articolo 38, paragrafo 6, diffonde tali informazioni e ogni altra informazione rilevante ai fini della prevenzione, dell'individuazione, della risposta o dell'attenuazione del relativo rischio per i soggetti a impatto critico e ad alto impatto nel suo Stato membro e, se del caso, a tutti i CSIRT interessati e al suo punto di contatto unico nazionale, senza indebito ritardo ed entro quattro ore dal ricevimento delle informazioni.

6. L'autorità competente che viene a conoscenza di informazioni relative a minacce informatiche provenienti da uno o più soggetti ad alto impatto o a impatto critico le trasmette al CSIRT ai fini del paragrafo 5.

7. Le autorità competenti possono delegare, in tutto o in parte, le responsabilità di cui ai paragrafi 3 e 4 per quanto riguarda uno o più soggetti ad alto impatto o a impatto critico che operano in più di uno Stato membro a un'altra autorità competente in uno di tali Stati membri, previo accordo tra le autorità competenti interessate.

8. I TSO, con l'assistenza dell'ENTSO per l'energia elettrica e in cooperazione con l'EU DSO, elaborano una metodologia della scala di classificazione degli attacchi informatici entro il [*OP: inserire la data corrispondente a 12 mesi dall'entrata in vigore del presente regolamento*]. I TSO, con l'assistenza dell'ENTSO per l'energia elettrica e dell'EU DSO, possono chiedere alle autorità competenti di consultare l'ENISA e le loro autorità competenti per la cibersicurezza per ricevere assistenza nell'elaborazione di tale scala di classificazione. La metodologia consente di classificare la gravità di un attacco informatico con una scala a cinque livelli, di cui i due più elevati sono "alta" e "critica". La classificazione si basa sulla valutazione dei parametri seguenti:

   (a) l'impatto potenziale, considerando gli asset e i perimetri esposti, determinato conformemente all'articolo 26, paragrafo 4, lettera c); e

   (b) la gravità dell'attacco informatico.

9. Entro il [*OP: inserire la data corrispondente a due anni dall'entrata in vigore del presente regolamento*], l'ENTSO per l'energia elettrica, in collaborazione con l'EU DSO, effettua uno studio di fattibilità per valutare se è possibile sviluppare, e a quali costi finanziari, uno strumento comune che consenta a tutti i soggetti di condividere le informazioni con le autorità nazionali competenti.

10. Lo studio di fattibilità esamina la possibilità che tale strumento comune:

   (a) sostenga i soggetti ad alto impatto e a impatto critico con informazioni attinenti alla sicurezza delle operazioni di flussi transfrontalieri di energia elettrica, quali la segnalazione quasi in tempo reale di attacchi informatici, allarmi precoci connessi alla cibersicurezza e vulnerabilità non divulgate di apparecchiature in uso nel sistema elettrico;

   (b) sia mantenuto in un ambiente adeguato e altamente affidabile;

   (c) consenta la raccolta di dati dai soggetti a impatto critico e ad alto impatto e faciliti la rimozione delle informazioni riservate e l'anonimizzazione dei dati e la loro rapida diffusione a soggetti a impatto critico e ad alto impatto.

11. L'ENTSO per l'energia elettrica, in cooperazione con l'EU DSO:

   (a) nel valutare la fattibilità consulta l'ENISA e il gruppo di cooperazione NIS, i punti di contatto unici nazionali e i rappresentanti dei principali portatori di interessi;

   (b) presenta i risultati dello studio di fattibilità all'ACER e al gruppo di cooperazione NIS.

12. L'ENTSO per l'energia elettrica, in cooperazione con l'EU DSO, può analizzare e agevolare le iniziative proposte da soggetti a impatto critico e ad alto impatto per valutare e sperimentare tali strumenti di condivisione di informazioni.

Articolo 38

Ruolo dei soggetti ad alto impatto e a impatto critico nella condivisione delle informazioni

1. Il soggetto ad alto impatto e a impatto critico:

   (a) stabilisce, per tutti gli asset all'interno del proprio perimetro di cibersicurezza determinato a norma dell'articolo 26, paragrafo 4, lettera c), almeno le capacità del centro operativo per la cibersicurezza di:

      i) garantire che i sistemi informatici e di rete e le applicazioni forniscano registri della sicurezza per il monitoraggio della sicurezza finalizzato a consentire l'individuazione di anomalie e raccogliere informazioni sugli attacchi informatici;

      ii) monitorare la sicurezza, ivi compreso individuare le intrusioni e valutare le vulnerabilità dei sistemi informatici e di rete;

      iii) effettuare analisi e, se necessario, adottare tutte le misure necessarie sotto la propria responsabilità e secondo le proprie capacità per proteggere il soggetto;

      iv) partecipare alla raccolta e alla condivisione delle informazioni di cui al presente articolo.

   (b) ha il diritto di acquisire, in tutto o in parte, le capacità di cui alla lettera a) tramite MSSP. I soggetti a impatto critico e ad alto impatto rispondono dell'operato degli MSSP e ne supervisionano l'attività;

   (c) designa un punto di contatto unico a livello di soggetto ai fini della condivisione delle informazioni.

2. L'ENISA può emanare orientamenti non vincolanti sull'acquisizione di tali capacità o sul subappalto del servizio agli MSSP, nell'ambito del compito definito all'articolo 6, paragrafo 2, del regolamento (UE) 2019/881.

3. Il soggetto a impatto critico e ad alto impatto condivide le informazioni rilevanti relative a un attacco informatico da segnalare con i propri CSIRT e con la propria autorità competente, senza indebito ritardo ed entro quattro ore dal momento in cui viene a conoscenza del fatto che l'incidente è da segnalare.

4. Le informazioni relative a un attacco informatico sono considerate da segnalare quando la valutazione dell'attacco informatico eseguita dal soggetto interessato stima una criticità da "alta" a "critica", secondo la metodologia della scala di classificazione degli attacchi informatici a norma dell'articolo 37, paragrafo 8. Il punto di contatto unico a livello di soggetto designato a norma del paragrafo 1, lettera c), comunica la classificazione dell'incidente.

5. Qualora i soggetti a impatto critico e ad alto impatto notifichino informazioni rilevanti relative a vulnerabilità sfruttate attivamente non risolte a un CSIRT, quest'ultimo può trasmetterle alla propria autorità competente. Alla luce del livello di sensibilità delle informazioni notificate, il CSIRT può trattenere le informazioni o ritardarne la trasmissione sulla base di giustificati motivi connessi alla cibersicurezza.

6. Il soggetto a impatto critico e ad alto impatto trasmette senza indebito ritardo ai propri CSIRT tutte le informazioni relative a una minaccia informatica da segnalare che possa avere un effetto transfrontaliero. Le informazioni relative a una minaccia

informatica sono considerate da segnalare quando è soddisfatta almeno una delle seguenti condizioni:

(a) le informazioni hanno rilevanza per altri soggetti a impatto critico e ad alto impatto a fini di prevenzione, individuazione, risposta o attenuazione dell'impatto del rischio;

(b) le tecniche, tattiche e procedure individuate utilizzate nel contesto di un attacco conseguono informazioni quali indirizzi URL o IP compromessi, hash o qualsiasi altro attributo utile per contestualizzare e correlare l'attacco;

(c) una minaccia informatica può essere ulteriormente valutata e contestualizzata con informazioni aggiuntive fornite da prestatori di servizi o da terzi non soggetti al presente regolamento.

7. All'atto della condivisione delle informazioni a norma del presente articolo, il soggetto a impatto critico e ad alto impatto specifica quanto segue:

(a) che le informazioni sono trasmesse a norma del presente regolamento;

(b) se le informazioni riguardano:

i) un attacco informatico da segnalare di cui al paragrafo 3;

ii) vulnerabilità sfruttate attivamente non risolte che non sono di dominio pubblico, di cui al paragrafo 4;

iii) una minaccia informatica da segnalare di cui al paragrafo 5;

(c) nel caso di un attacco informatico da segnalare, il livello dell'attacco informatico secondo la metodologia della scala di classificazione degli attacchi informatici di cui all'articolo 37, paragrafo 8, e le informazioni che determinano tale classificazione, compresa almeno la criticità dell'attacco informatico.

8. Quando il soggetto critico o ad alto impatto notifica un incidente significativo a norma dell'articolo 23 della direttiva (UE) 2022/2555 e la segnalazione dell'incidente a norma di tale articolo contiene le informazioni pertinenti di cui al paragrafo 3 del presente articolo, la segnalazione del soggetto a norma dell'articolo 23, paragrafo 1, di detta direttiva costituisce una segnalazione di informazioni ai sensi del paragrafo 3 del presente articolo.

9. Il soggetto a impatto critico e ad alto impatto riferisce alla propria autorità competente o al proprio CSIRT indicando chiaramente le informazioni specifiche che devono essere condivise esclusivamente con l'autorità competente o il CSIRT nei casi in cui la condivisione delle informazioni potrebbe essere fonte di un attacco informatico. Il soggetto a impatto critico e ad alto impatto ha il diritto di fornire una versione non riservata delle informazioni al CSIRT competente.

Articolo 39

Individuazione degli attacchi informatici e trattamento delle relative informazioni

1. I soggetti a impatto critico e ad alto impatto acquisiscono le capacità necessarie per gestire gli attacchi informatici individuati con il necessario sostegno della pertinente autorità competente, dell'ENTSO per l'energia elettrica e dell'EU DSO. I soggetti a impatto critico e ad alto impatto possono essere sostenuti dal CSIRT designato nei

loro rispettivi Stati membri nell'ambito del compito assegnato ai CSIRT dall'articolo 11, paragrafo 5, lettera a), della direttiva (UE) 2022/2555. I soggetti ad impatto critico e ad alto impatto attuano processi efficaci per individuare, classificare e dare risposta agli attacchi informatici che incideranno o potrebbero incidere sui flussi transfrontalieri di energia elettrica, al fine di ridurne al minimo l'impatto.

2. Se un attacco informatico ha un effetto sui flussi transfrontalieri di energia elettrica, i punti di contatto unici a livello dei soggetti a impatto critico e ad alto impatto interessati cooperano per condividere informazioni tra loro, coordinati dall'autorità competente dello Stato membro in cui l'attacco informatico è stato segnalato per la prima volta.

3. I soggetti a impatto critico e ad alto impatto:

   (a) garantiscono che il loro punto di contatto unico a livello di soggetto abbia accesso, in base alla necessità di conoscere, alle informazioni ricevute dal punto di contatto unico nazionale tramite la rispettiva autorità competente;

   (b) salvo se si sia già provveduto in tal senso a norma dell'articolo 3, paragrafo 4, della direttiva (UE) 2022/2555, notificano all'autorità competente dello Stato membro in cui sono stabiliti e al punto di contatto unico nazionale un elenco dei loro punti di contatto unici per la cibersicurezza a livello di soggetto:

      i) da cui l'autorità competente e il punto di contatto unico nazionale possono aspettarsi di ricevere informazioni sugli attacchi informatici da segnalare;

      ii) a cui le autorità competenti e i punti di contatto unici nazionali possono dover trasmettere informazioni;

   (c) stabiliscono procedure di gestione degli attacchi informatici, compresi i ruoli e le responsabilità, i compiti e le reazioni sulla base dell'evoluzione osservabile dell'attacco informatico all'interno dei perimetri a impatto critico e ad alto impatto;

   (d) sottopongono a prova le procedure generali di gestione degli attacchi informatici almeno ogni anno sperimentando almeno uno scenario che incide direttamente o indirettamente sui flussi transfrontalieri di energia elettrica. Tale prova annuale può essere condotta da soggetti a impatto critico e ad alto impatto durante le esercitazioni periodiche di cui all'articolo 43. Qualsiasi attività di risposta in tempo reale agli attacchi informatici di gravità almeno al livello 2 della scala, secondo la metodologia di classificazione degli attacchi informatici di cui all'articolo 37, paragrafo 8, e derivanti da problemi di cibersicurezza, può fungere da prova annuale del piano di risposta agli attacchi informatici.

4. I compiti di cui al paragrafo 1 possono essere delegati dagli Stati membri anche ai centri di coordinamento regionali conformemente all'articolo 37, paragrafo 2, del regolamento (UE) 2019/943.

Articolo 40

Gestione delle crisi

1. Quando l'autorità competente determina che una crisi dell'energia elettrica è connessa a un attacco informatico che ha un impatto su più di uno Stato membro, le autorità

competenti degli Stati membri interessati, le autorità competenti per la cibersicurezza, le autorità competenti per la preparazione ai rischi e le autorità di gestione delle crisi informatiche nei sistemi informatici e di rete degli Stati membri colpiti istituiscono congiuntamente un gruppo ad hoc di coordinamento transfrontaliero di crisi.

2. Il gruppo ad hoc di coordinamento transfrontaliero di crisi:

   (a) coordina il recupero efficiente e l'ulteriore diffusione di tutte le informazioni pertinenti sulla cibersicurezza ai soggetti partecipanti al processo di gestione della crisi;

   (b) organizza la comunicazione tra tutti i soggetti interessati dalla crisi e le autorità competenti, al fine di ridurre le sovrapposizioni e aumentare l'efficienza delle analisi e delle risposte tecniche per porre rimedio alle crisi simultanee dell'energia elettrica derivanti da problemi di cibersicurezza;

   (c) mette a disposizione dei soggetti colpiti dall'incidente, in cooperazione con i CSIRT competenti, le competenze necessarie, compresa la consulenza operativa sull'attuazione di eventuali misure di attenuazione;

   (d) notifica e fornisce aggiornamenti periodici sullo stato dell'incidente alla Commissione e al gruppo di coordinamento per l'energia elettrica, secondo i principi di protezione di cui all'articolo 46;

   (e) chiede consulenza alle autorità, alle agenzie o ai soggetti che possono offrire assistenza per attenuare la crisi dell'energia elettrica.

3. Se l'attacco informatico rientra – o si prevede che possa rientrare – nella classificazione di incidente di cibersicurezza su vasta scala, il gruppo ad hoc di coordinamento transfrontaliero di crisi informa immediatamente le autorità nazionali di gestione delle crisi informatiche negli Stati membri interessati dall'incidente, a norma dell'articolo 9, paragrafo 1, della direttiva (UE) 2022/2555, nonché la Commissione e EU CyCLONe. In tale situazione, il gruppo ad hoc di coordinamento transfrontaliero di crisi sostiene EU CyCLONe riguardo alle specificità settoriali.

4. I soggetti a impatto critico e ad alto impatto elaborano e detengono capacità, orientamenti interni e piani di preparazione e tengono a disposizione membri del personale per partecipare all'individuazione e all'attenuazione delle crisi transfrontaliere. Il soggetto a impatto critico o ad alto impatto colpito da una crisi simultanea dell'energia elettrica indaga sulle cause alla radice di tale crisi in cooperazione con la sua autorità competente, per determinare in che misura la crisi sia connessa a un attacco informatico.

5. I compiti di cui al paragrafo 4 possono essere delegati dagli Stati membri anche ai centri di coordinamento regionali conformemente all'articolo 37, paragrafo 2, del regolamento (UE) 2019/943.

Articolo 41

Gestione delle crisi di cibersicurezza e piani di risposta

1. Entro 24 mesi dalla notifica all'ACER della relazione di valutazione del rischio a livello dell'Unione, l'ACER, in stretta cooperazione con l'ENISA, l'ENTSO per l'energia elettrica, l'EU DSO, le autorità competenti, le autorità competenti per la cibersicurezza, le autorità competenti per la preparazione ai rischi, le autorità

nazionali di regolazione e le autorità nazionali di gestione delle crisi informatiche nei sistemi informatici e di rete, elabora un piano di gestione delle crisi di cibersicurezza e di risposta a livello dell'Unione per il settore dell'energia elettrica.

2. Entro 12 mesi dall'elaborazione, da parte dell'ACER, del piano di gestione delle crisi di cibersicurezza e di risposta a livello dell'Unione per il settore dell'energia elettrica a norma del paragrafo 1, l'autorità competente elabora un piano nazionale di gestione delle crisi di cibersicurezza e di risposta per i flussi transfrontalieri di energia elettrica che tenga conto del piano di gestione delle crisi di cibersicurezza a livello dell'Unione e del piano nazionale di preparazione ai rischi istituito a norma dell'articolo 10 del regolamento (UE) 2019/941. Tale piano è coerente con il piano di risposta agli incidenti e alle crisi di cibersicurezza su vasta scala a norma dell'articolo 9, paragrafo 4, della direttiva (UE) 2022/2555. L'autorità competente si coordina con i soggetti a impatto critico e ad alto impatto e con l'autorità competente per la preparazione ai rischi nel proprio Stato membro.

3. Il piano nazionale di risposta agli incidenti e alle crisi di cibersicurezza su vasta scala a norma dell'articolo 9, paragrafo 4, della direttiva (UE) 2022/2555 è considerato un piano nazionale di gestione delle crisi di cibersicurezza a norma del presente articolo se include disposizioni in materia di gestione delle crisi e risposta alle crisi per i flussi transfrontalieri di energia elettrica.

4. I compiti elencati ai paragrafi 1 e 2 possono essere delegati dagli Stati membri anche ai centri di coordinamento regionali conformemente all'articolo 37, paragrafo 2, del regolamento (UE) 2019/943.

5. I soggetti a impatto critico e ad alto impatto garantiscono che i loro processi di gestione delle crisi connesse alla cibersicurezza:

   (a) dispongano di procedure compatibili di gestione degli incidenti di cibersicurezza a livello transfrontaliero, di cui all'articolo 6, punto 8), della direttiva (UE) 2022/2555, formalmente integrate nei loro piani di gestione delle crisi;

   (b) facciano parte delle attività generali di gestione delle crisi.

6. Entro 12 mesi dalla notifica dei soggetti ad alto impatto e a impatto critico a norma dell'articolo 24, paragrafo 6, e successivamente ogni tre anni, i soggetti a impatto critico e ad alto impatto elaborano un piano di gestione delle crisi a livello di soggetto per una crisi connessa alla cibersicurezza, che inseriscono nei loro piani generali di gestione delle crisi. Tale piano include almeno:

   (a) disposizioni per la dichiarazione dello stato di crisi di cui all'articolo 14, paragrafi 2 e 3, del regolamento (UE) 2019/941;

   (b) ruoli e responsabilità chiari per la gestione delle crisi, compreso il ruolo di altri soggetti pertinenti a impatto critico e ad alto impatto;

   (c) informazioni di contatto aggiornate e disposizioni per la comunicazione e la condivisione delle informazioni durante una situazione di crisi, compreso il collegamento con i CSIRT.

7. Le misure per la gestione delle crisi di cui all'articolo 21, paragrafo 2, lettera c), della direttiva (UE) 2022/2555 sono considerate un piano di gestione delle crisi a livello di soggetto per il settore dell'energia elettrica ai sensi del presente articolo se includono tutti gli elementi elencati al paragrafo 6.

8. I piani di gestione delle crisi sono sperimentati durante le esercitazioni di cibersicurezza di cui agli articoli 43, 44 e 45.

9. I soggetti a impatto critico e ad alto impatto includono i loro piani di gestione delle crisi a livello di soggetto nei loro piani di continuità operativa per i processi a impatto critico e ad alto impatto. I piani di gestione delle crisi a livello di soggetto comprendono:

   (a) processi che dipendono dalla disponibilità, dall'integrità e dall'affidabilità dei servizi informatici;

   (b) tutti i siti di continuità operativa, compresi quelli per hardware e software;

   (c) tutti i ruoli e responsabilità interni connessi ai processi di continuità operativa.

10. I soggetti a impatto critico e ad alto impatto aggiornano i loro piani di gestione delle crisi a livello di soggetto almeno ogni tre anni e ogniqualvolta necessario.

11. L'ACER aggiorna il piano di gestione delle crisi di cibersicurezza e di risposta a livello dell'Unione per il settore dell'energia elettrica elaborato a norma del paragrafo 1 almeno ogni tre anni e ogniqualvolta necessario.

12. L'autorità competente aggiorna il piano nazionale di gestione delle crisi di cibersicurezza e di risposta per i flussi transfrontalieri di energia elettrica elaborato a norma del paragrafo 2 almeno ogni tre anni e ogniqualvolta necessario.

13. I soggetti a impatto critico e ad alto impatto sperimentano i loro piani di continuità operativa almeno una volta ogni tre anni o in seguito a modifiche di rilievo apportate a un processo a impatto critico. L'esito della prova del piano di continuità operativa è documentato. I soggetti a impatto critico e ad alto impatto possono includere la prova del loro piano di continuità operativa nelle esercitazioni di cibersicurezza.

14. I soggetti a impatto critico e ad alto impatto aggiornano il loro piano di continuità operativa ogniqualvolta necessario e almeno una volta ogni tre anni, tenendo conto dell'esito della prova.

15. Se una prova individua carenze nel piano di continuità operativa, il soggetto a impatto critico e ad alto impatto le corregge entro 180 giorni di calendario dalla verifica ed effettua una nuova prova per dimostrare l'efficacia delle misure correttive.

16. Il soggetto a impatto critico o ad alto impatto che non è in grado di correggere le carenze entro 180 giorni di calendario include i motivi nella relazione da trasmettere alla propria autorità competente a norma dell'articolo 27.

Articolo 42

Capacità di preallarme di cibersicurezza per il settore dell'energia elettrica

1. Le autorità competenti cooperano con l'ENISA per acquisire capacità di preallarme di cibersicurezza per l'energia elettrica nell'ambito dell'assistenza agli Stati membri a norma dell'articolo 6, paragrafo 2, e dell'articolo 7 del regolamento (UE) 2019/881.

2. Le capacità di preallarme di cibersicurezza per l'energia elettrica consentono all'ENISA, nello svolgimento dei compiti di cui all'articolo 7, paragrafo 7, del regolamento (UE) 2019/881, di:

   (a) raccogliere informazioni condivise su base volontaria da:

i) CSIRT e autorità competenti;

ii) i soggetti di cui all'articolo 2 del presente regolamento;

iii) ogni altro soggetto che intenda condividere informazioni pertinenti su base volontaria;

(b) valutare e classificare le informazioni raccolte;

(c) valutare le informazioni cui l'ENISA ha accesso per individuare le condizioni di rischio informatico e gli indicatori pertinenti per aspetti dei flussi transfrontalieri di energia elettrica;

(d) individuare le condizioni e gli indicatori spesso correlati agli attacchi informatici nel settore dell'energia elettrica;

(e) stabilire, attraverso la valutazione e l'individuazione dei fattori di rischio, se debbano essere effettuate ulteriori analisi e azioni preventive;

(f) informare le autorità competenti in merito ai rischi individuati e alle azioni preventive raccomandate specificamente per i soggetti interessati;

(g) informare tutti i soggetti elencati all'articolo 2 in merito ai risultati della valutazione delle informazioni conformemente alle lettere b), c) e d);

(h) includere periodicamente le informazioni pertinenti nella relazione sulla situazione tecnica della cibersicurezza pubblicata a norma dell'articolo 7, paragrafo 6, del regolamento (UE) 2019/881;

(i) ricavare dalle informazioni raccolte, ove possibile, dati indicanti una potenziale violazione della sicurezza o un attacco informatico ("indicatori di compromissione").

3. I CSIRT diffondono senza indugio le informazioni ricevute dall'ENISA ai soggetti interessati, nell'ambito dei loro compiti definiti all'articolo 11, paragrafo 3, lettera b), della direttiva (UE) 2022/2555.

4. L'ACER controlla l'efficacia delle capacità di preallarme di cibersicurezza per l'energia elettrica. L'ENISA assiste l'ACER fornendo tutte le informazioni necessarie a norma dell'articolo 6, paragrafo 2, e dell'articolo 7, paragrafo 1, del regolamento (UE) 2019/881. L'analisi di tale attività di controllo rientra nel controllo di cui all'articolo 12 del presente regolamento.

CAPO VI

QUADRO DELL'ESERCITAZIONE DI CIBERSICUREZZA PER L'ENERGIA ELETTRICA

Articolo 43

Esercitazioni di cibersicurezza a livello di soggetto e di Stato membro

1. Entro il 31 dicembre dell'anno successivo alla notifica dei soggetti ad impatto critico, e successivamente ogni tre anni, il soggetto ad impatto critico effettua un'esercitazione di cibersicurezza comprendente uno o più scenari con attacchi informatici che incidono direttamente o indirettamente sui flussi transfrontalieri di energia elettrica e relativi ai rischi individuati durante le valutazioni del rischio per la

cibersicurezza a livello di Stato membro e di soggetto conformemente all'articolo 20 e all'articolo 27.

2. In deroga al paragrafo 1, le autorità competenti per la preparazione ai rischi, previa consultazione dell'autorità competente e della pertinente autorità di gestione delle crisi di cibersicurezza designata o istituita a norma dell'articolo 9 della direttiva (UE) 2022/2555, possono decidere di organizzare un'esercitazione di cibersicurezza a livello di Stato membro, come descritto al paragrafo 1, anziché a livello di soggetto. A tale riguardo, l'autorità competente informa:

   (a) tutti i soggetti a impatto critico del proprio Stato membro, l'autorità nazionale di regolazione, i CSIRT e le autorità competenti per la cibersicurezza al più tardi entro il 30 giugno dell'anno precedente l'esercitazione di cibersicurezza a livello di soggetto;

   (b) ciascun soggetto che partecipa all'esercitazione di cibersicurezza a livello di Stato membro al più tardi 6 mesi prima dello svolgimento dell'esercitazione.

3. L'autorità competente per la preparazione ai rischi, con il sostegno tecnico dei suoi CSIRT, organizza l'esercitazione di cibersicurezza di cui al paragrafo 2 a livello di Stato membro in modo indipendente o nel contesto di una diversa esercitazione di cibersicurezza nel medesimo Stato membro. Al fine di poter raggruppare tali esercitazioni, l'autorità competente per la preparazione ai rischi può rinviare di un anno l'esercitazione di cibersicurezza a livello di Stato membro di cui al paragrafo 1.

4. Le esercitazioni di cibersicurezza a livello di soggetto e di Stato membro sono coerenti con i quadri nazionali di gestione delle crisi informatiche conformemente all'articolo 9, paragrafo 4, lettera d), della direttiva (UE) 2022/2555.

5. Entro il [*OP: inserire la data corrispondente al 31 dicembre del secondo anno successivo all'entrata in vigore del presente regolamento*], e successivamente ogni tre anni, l'ENTSO per l'energia elettrica, in cooperazione con l'EU DSO, mette a disposizione un modello di scenario di esercitazione per effettuare le esercitazioni di cibersicurezza a livello di soggetto e di Stato membro di cui al paragrafo 1. Il modello tiene conto dei risultati della più recente valutazione del rischio per la cibersicurezza a livello di soggetto e di Stato membro e include i principali criteri di riuscita. L'ENTSO per l'energia elettrica e l'EU DSO coinvolgono l'ACER e l'ENISA nell'elaborazione del modello.

Articolo 44

Esercitazioni di cibersicurezza regionali o transregionali

1. Entro il [*OP: inserire la data corrispondente al 31 dicembre del quinto anno successivo all'entrata in vigore del presente regolamento*], e successivamente ogni tre anni, in ciascuna regione di gestione di sistema l'ENTSO per l'energia elettrica organizza, in cooperazione con l'EU DSO, un'esercitazione di cibersicurezza regionale. Partecipano all'esercitazione di cibersicurezza regionale i soggetti a impatto critico della regione di gestione di sistema. L'ENTSO per l'energia elettrica, in cooperazione con l'EU DSO, può organizzare, in luogo di un esercizio regionale di cibersicurezza, un'esercitazione di cibersicurezza transregionale in più di una regione di gestione di sistema nello stesso arco di tempo. L'esercitazione dovrebbe tenere conto di altri scenari e valutazioni del rischio per la cibersicurezza esistenti elaborati a livello dell'Unione.

2. L'ENISA sostiene l'ENTSO per l'energia elettrica e l'EU DSO nella preparazione e nell'organizzazione dell'esercitazione di cibersicurezza a livello regionale o transregionale.

3. L'ENTSO per l'energia elettrica, in coordinamento con l'EU DSO, informa i soggetti a impatto critico che partecipano all'esercitazione di cibersicurezza regionale o transregionale sei mesi prima dello svolgimento dell'esercitazione.

4. L'organizzatore di un'esercitazione di cibersicurezza periodica a livello dell'Unione a norma dell'articolo 7, paragrafo 5, del regolamento (UE) 2019/881, o di qualsiasi esercitazione obbligatoria di cibersicurezza relativa al settore dell'energia elettrica all'interno dello stesso perimetro geografico, può invitare l'ENTSO per l'energia elettrica e l'EU DSO a partecipare. In tali casi, l'obbligo di cui al paragrafo 1 non si applica, a condizione che tutti i soggetti a impatto critico della regione di gestione del sistema partecipino alla stessa esercitazione.

5. Se partecipano a un'esercitazione di cibersicurezza di cui al paragrafo 4, l'ENTSO per l'energia elettrica e l'EU DSO possono rinviare di un anno l'esercitazione di cibersicurezza regionale o interregionale di cui al paragrafo 1.

6. Entro il [*OP: inserire la data corrispondente al 31 dicembre del terzo anno successivo all'entrata in vigore del presente regolamento*], e successivamente ogni tre anni, l'ENTSO per l'energia elettrica, in coordinamento con l'EU DSO, mette a disposizione un modello di esercitazione per effettuare le esercitazioni di cibersicurezza regionali e transregionali. Il modello tiene conto dei risultati della più recente valutazione del rischio per la cibersicurezza a livello regionale e include i principali criteri di riuscita. L'ENTSO per l'energia elettrica consulta la Commissione e può chiedere il parere dell'ACER, dell'ENISA e del Centro comune di ricerca sull'organizzazione e sull'esecuzione delle esercitazioni di cibersicurezza regionali e transregionali.

Articolo 45

Esito delle esercitazioni di cibersicurezza a livello di soggetto, di Stato membro, regionale o transregionale

1. Su richiesta del soggetto a impatto critico, i prestatori di servizi critici partecipano alle esercitazioni di cibersicurezza di cui all'articolo 43, paragrafi 1 e 2, e all'articolo 44, paragrafo 1, quando prestano servizi per il soggetto a impatto critico nell'area corrispondente all'ambito dell'esercitazione di cibersicurezza.

2. Gli organizzatori delle esercitazioni di cibersicurezza di cui all'articolo 43, paragrafi 1 e 2, e all'articolo 44, paragrafo 1, con il parere dell'ENISA se essi lo richiedono e a norma dell'articolo 7, paragrafo 5, del regolamento (UE) 2019/881, analizzano e completano l'esercitazione di cibersicurezza con una relazione di sintesi degli insegnamenti tratti, indirizzata a tutti i partecipanti. La relazione comprende:

   (a) gli scenari di esercitazione, i resoconti delle riunioni, le principali posizioni, i successi e gli insegnamenti tratti a qualsiasi livello della catena del valore dell'energia elettrica;

   (b) se sono stati soddisfatti i principali criteri di riuscita;

   (c) un elenco di raccomandazioni per i soggetti che partecipano all'esercitazione di cibersicurezza al fine di correggere, adattare o modificare processi di crisi,

procedure, modelli di governance associati ed eventuali impegni contrattuali esistenti con prestatori di servizi critici.

3. Se richiesto dalla rete di CSIRT, dal gruppo di cooperazione NIS o da EU CyCLONe, gli organizzatori delle esercitazioni di cibersicurezza di cui all'articolo 43, paragrafi 1 e 2, e all'articolo 44, paragrafo 1, ne condividono i risultati. Gli organizzatori condividono con ciascun soggetto partecipante alle esercitazioni le informazioni di cui al paragrafo 2, lettere a) e b). Gli organizzatori condividono l'elenco delle raccomandazioni di cui al paragrafo 2, lettera c), esclusivamente con i soggetti cui sono destinate le raccomandazioni.

4. Gli organizzatori delle esercitazioni di cibersicurezza di cui all'articolo 43, paragrafi 1 e 2, e all'articolo 44, paragrafo 1, verificano periodicamente con i soggetti partecipanti alle esercitazioni l'attuazione delle raccomandazioni a norma del paragrafo 2, lettera c), del presente articolo.

CAPO VII

PROTEZIONE DELLE INFORMAZIONI

Articolo 46

Principi per la protezione delle informazioni scambiate

1. I soggetti elencati all'articolo 2, paragrafo 1, garantiscono che le informazioni fornite, ricevute, scambiate o trasmesse a norma del presente regolamento sono accessibili solo in base al principio della necessità di conoscere e conformemente alle pertinenti disposizioni nazionali e dell'Unione in materia di sicurezza delle informazioni.

2. I soggetti elencati all'articolo 2, paragrafo 1, garantiscono che le informazioni fornite, ricevute, scambiate o trasmesse a norma del presente regolamento sono trattate e tracciate durante il loro intero ciclo di vita e possano essere divulgate alla fine del loro ciclo di vita solo dopo essere state anonimizzate.

3. I soggetti elencati all'articolo 2, paragrafo 1, provvedono affinché siano predisposte tutte le necessarie misure di protezione di natura organizzativa e tecnica per salvaguardare e tutelare la riservatezza, l'integrità, la disponibilità e la non disconoscibilità delle informazioni fornite, ricevute, scambiate o trasmesse a norma del presente regolamento, indipendentemente dai mezzi utilizzati. Le misure di protezione:

   (a) sono proporzionate;

   (b) tengono conto dei rischi per la cibersicurezza connessi a minacce note passate ed emergenti alle quali le informazioni possono essere soggette nel contesto del presente regolamento;

   (c) si basano, per quanto possibile, su norme e migliori pratiche nazionali, europee o internazionali;

   (d) sono documentate.

4. I soggetti elencati all'articolo 2, paragrafo 1, garantiscono che chiunque abbia avuto accesso alle informazioni fornite, ricevute, scambiate o trasmesse a norma del presente regolamento sia portato a conoscenza delle disposizioni di sicurezza applicabili a livello di soggetto e sulle misure e procedure pertinenti per la protezione

delle informazioni. I medesimi soggetti provvedono affinché la persona interessata riconosca la responsabilità di proteggere le informazioni secondo le istruzioni impartite.

5. I soggetti elencati all'articolo 2, paragrafo 1, garantiscono che l'accesso alle informazioni fornite, ricevute, scambiate o trasmesse a norma del presente regolamento sia limitato alle persone fisiche:

   (a) autorizzate ad accedere alle informazioni sulla base delle loro funzioni e limitatamente all'esecuzione dei compiti loro assegnati;

   (b) per le quali il soggetto sia stato in grado di valutare i principi etici e di integrità e non vi siano prove di esito negativo di una verifica dei precedenti personali volto a valutare l'affidabilità della persona conformemente alle migliori pratiche e ai requisiti di sicurezza standard del soggetto e, se necessario, alle disposizioni legislative e regolamentari nazionali.

6. I soggetti elencati all'articolo 2, paragrafo 1, ottengono il consenso scritto della persona fisica o giuridica che ha originariamente creato o fornito le informazioni prima di inviarle a terzi che non rientrano nell'ambito di applicazione del presente regolamento.

7. Il soggetto elencato all'articolo 2, paragrafo 1, può ritenere di condividere le informazioni in deroga ai paragrafi 1 e 4 del presente articolo al fine di prevenire una crisi simultanea dell'energia elettrica derivante da problemi di cibersicurezza o qualsiasi crisi transfrontaliera nell'Unione in un altro settore. In tal caso, il soggetto:

   (a) consulta l'autorità competente ed è autorizzato da quest'ultima a condividere le informazioni;

   (b) anonimizza le informazioni senza privarle degli elementi necessari per informare il pubblico di un rischio imminente e grave per i flussi transfrontalieri di energia elettrica e delle possibili misure di attenuazione;

   (c) salvaguarda l'identità dell'originatore e dei soggetti che hanno trattato le informazioni a norma del presente regolamento.

8. In deroga al paragrafo 6, le autorità competenti possono fornire le informazioni fornite, ricevute, scambiate o trasmesse a norma del presente regolamento a terzi non elencati all'articolo 2, paragrafo 1, senza il previo consenso scritto dell'originatore delle informazioni ma informandolo il prima possibile. Prima di divulgare le informazioni fornite, ricevute, scambiate o trasmesse a norma del presente regolamento a terzi non elencati all'articolo 2, paragrafo 1, l'autorità competente prende ragionevoli provvedimenti per garantire che il terzo interessato sia a conoscenza delle disposizioni di sicurezza in vigore e riceve ragionevoli garanzie della capacità di quest'ultimo di proteggere le informazioni ricevute in conformità dei paragrafi da 1 a 5. L'autorità competente anonimizza le informazioni senza privarle degli elementi necessari per informare il pubblico di un rischio imminente e grave per i flussi transfrontalieri di energia elettrica e di possibili misure di attenuazione e salvaguarda l'identità dell'originatore delle informazioni. In tal caso, il terzo non elencato all'articolo 2, paragrafo 1, protegge le informazioni ricevute conformemente alle disposizioni già in vigore a livello di soggetto o, qualora ciò non sia possibile, alle disposizioni e alle istruzioni fornite dall'autorità competente.

9. Il presente articolo non si applica ai soggetti non elencati all'articolo 2, paragrafo 1, ai quali sono trasmesse informazioni a norma del paragrafo 6 del presente articolo. In

tal caso si applica il paragrafo 7 del presente articolo o l'autorità competente può fornire al soggetto disposizioni scritte da applicare nei casi in cui siano ricevute informazioni a norma del presente regolamento.

Articolo 47

Riservatezza delle informazioni

1. Le informazioni fornite, ricevute, scambiate o trasmesse a norma del presente regolamento sono soggette alle condizioni in materia di segreto professionale di cui ai paragrafi da 2 a 5 del presente articolo e alle prescrizioni di cui all'articolo 65 del regolamento (UE) 2019/943. Le informazioni fornite, ricevute, scambiate o trasmesse tra i soggetti elencati all'articolo 2 del presente regolamento sono protette, ai fini dell'attuazione del presente regolamento, tenendo conto del livello di riservatezza delle informazioni applicato dall'originatore.
2. Ai soggetti elencati all'articolo 2 si applica l'obbligo del segreto professionale.
3. Le autorità competenti per la cibersicurezza, le autorità nazionali di regolazione, le autorità competenti per la preparazione ai rischi e i CSIRT si scambiano tutte le informazioni necessarie per svolgere i loro compiti.
4. Ai fini dell'attuazione dell'articolo 23, le informazioni ricevute, scambiate o trasmesse tra i soggetti elencati all'articolo 2, paragrafo 1, sono anonimizzate e aggregate.
5. Le informazioni ricevute dal soggetto o dall'autorità cui si applica il presente regolamento nell'espletamento delle loro mansioni non possono essere divulgate ad altri soggetti o autorità, fatti salvi i casi disciplinati dalla normativa nazionale, dalle altre disposizioni del presente regolamento o da altre norme pertinenti dell'Unione.
6. Fatta salva la legislazione nazionale o dell'Unione, l'autorità, il soggetto o la persona fisica che riceve informazioni a norma del presente regolamento non può utilizzarle per scopi diversi dallo svolgimento delle funzioni attribuitele o attribuitegli a norma del presente regolamento.
7. Entro il [*OP: inserire la data corrispondente a 12 mesi dall'entrata in vigore del presente regolamento*] l'ACER, previa consultazione dell'ENISA, di tutte le autorità competenti, dell'ENTSO per l'energia elettrica e l'EU DSO, emana orientamenti sui meccanismi che consentono a tutti i soggetti elencati all'articolo 2, paragrafo 1, di scambiare informazioni, in particolare i flussi di comunicazione previsti, e sui metodi per anonimizzare e aggregare le informazioni ai fini dell'attuazione del presente articolo.
8. Le informazioni che sono riservate in forza di disposizioni nazionali e dell'Unione sono scambiate con la Commissione e le altre autorità del caso soltanto se necessario ai fini dell'applicazione del presente regolamento. Le informazioni scambiate sono limitate alle informazioni necessarie e commisurate a tale scopo. Lo scambio di informazioni tutela la riservatezza di dette informazioni e protegge la sicurezza e gli interessi commerciali dei soggetti a impatto critico o ad alto impatto.

CAPO VIII

DISPOSIZIONI FINALI

Articolo 48

Disposizioni transitorie

1. Fino all'approvazione dei termini e delle condizioni o delle metodologie di cui all'articolo 6, paragrafo 2, o dei piani di cui all'articolo 6, paragrafo 3, l'ENTSO per l'energia elettrica, in cooperazione con l'EU DSO, elabora orientamenti non vincolanti sulle questioni seguenti:

   (a) un indice provvisorio di impatto sulla cibersicurezza dell'energia elettrica (ECII) a norma del paragrafo 2;

   (b) un elenco provvisorio dei processi ad alto impatto e a impatto critico a livello dell'Unione a norma del paragrafo 4; e

   (c) un elenco provvisorio delle norme e dei controlli europei e internazionali disposti dalla legislazione nazionale che hanno rilevanza per gli aspetti di cibersicurezza dei flussi transfrontalieri di energia elettrica a norma del paragrafo 6.

2. Entro il [*OP: inserire la data corrispondente a quattro mesi dall'entrata in vigore del presente regolamento*], l'ENTSO per l'energia elettrica, in cooperazione con l'EU DSO, elabora una raccomandazione di ECII provvisorio. L'ENTSO per l'energia elettrica, in cooperazione con l'EU DSO, notifica la raccomandazione di ECII provvisorio alle autorità competenti.

3. Quattro mesi dopo il ricevimento della raccomandazione di ECII provvisorio, o al più tardi entro il [*OP: inserire la data corrispondente a otto mesi dopo l'entrata in vigore*], le autorità competenti individuano i candidati a soggetti ad alto impatto e a impatto critico nel loro Stato membro sulla base dell'ECII provvisorio e redigono un elenco provvisorio di soggetti ad alto impatto e a impatto critico. I soggetti ad alto impatto e a impatto critico individuati nell'elenco provvisorio possono adempiere volontariamente ai loro obblighi di cui al presente regolamento sulla base di un principio di precauzione. Entro il [*OP: inserire la data corrispondente a nove mesi dopo l'entrata in vigore del presente regolamento*], le autorità competenti notificano ai soggetti individuati nell'elenco provvisorio che sono stati identificati come soggetti ad alto impatto o a impatto critico.

4. Entro il [*OP: inserire la data corrispondente a sei mesi dall'entrata in vigore del presente regolamento*], l'ENTSO per l'energia elettrica, in cooperazione con l'EU DSO, elabora un elenco provvisorio di processi ad alto impatto e a impatto critico a livello dell'Unione. I soggetti notificati a norma del paragrafo 3 che decidono di adempiere volontariamente agli obblighi di cui al presente regolamento sulla base di un principio di precauzione utilizzano l'elenco provvisorio dei processi ad alto impatto e a impatto critico per determinare i perimetri provvisori ad alto impatto e a impatto critico e per determinare quali attività devono essere incluse nella prima valutazione del rischio per la cibersicurezza a livello di soggetto.

5. Entro il [*OP: inserire la data corrispondente a tre mesi dall'entrata in vigore*], l'autorità competente a norma dell'articolo 4, paragrafo 1, trasmette all'ENTSO per

l'energia elettrica e all'EU DSO un elenco dei propri atti legislativi nazionali che hanno rilevanza per gli aspetti di cibersicurezza dei flussi transfrontalieri di energia elettrica.

6. Entro il [*OP: inserire la data corrispondente a 12 mesi dall'entrata in vigore del presente regolamento*], l'ENTSO per l'energia elettrica, in cooperazione con l'EU DSO, elabora un elenco provvisorio delle norme e dei controlli europei e internazionali disposti dalla legislazione nazionale che hanno rilevanza per gli aspetti di cibersicurezza dei flussi transfrontalieri di energia elettrica, tenendo conto delle informazioni fornite dalle autorità competenti.

7. L'elenco provvisorio delle norme e dei controlli europei e internazionali comprende:

   (a) le norme europee e internazionali e gli atti legislativi nazionali contenenti orientamenti sulle metodologie per la gestione dei rischi per la cibersicurezza a livello di soggetto; e

   (b) i controlli di cibersicurezza equivalenti ai controlli che presumibilmente faranno parte dei controlli minimi e avanzati di cibersicurezza.

8. In sede di ultimazione dell'elenco provvisorio di norme, l'ENTSO per l'energia elettrica e l'EU DSO tengono conto dei pareri espressi dall'ENISA e dall'ACER. L'ENTSO per l'energia elettrica e l'EU DSO pubblicano sui loro siti web l'elenco provvisorio delle norme e dei controlli europei e internazionali.

9. L'ENTSO per l'energia elettrica e l'EU DSO consultano l'ENISA e l'ACER in merito alle proposte di orientamenti non vincolanti elaborate a norma del paragrafo 1.

10. In attesa dell'elaborazione dei controlli minimi e avanzati di cibersicurezza a norma dell'articolo 29 e della loro adozione a norma dell'articolo 8, tutti i soggetti elencati all'articolo 2, paragrafo 1, si adoperano per applicare progressivamente gli orientamenti non vincolanti elaborati a norma del paragrafo 1.

Articolo 49

Entrata in vigore

Il presente regolamento entra in vigore il ventesimo giorno successivo alla pubblicazione nella *Gazzetta ufficiale dell'Unione europea*.

Il presente regolamento è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri.

Fatto a Bruxelles, il 11.3.2024

Per la Commissione
La presidente
Ursula VON DER LEYEN