COMMISSIONE
EUROPEA

Bruxelles, 16.12.2020
COM(2020) 823 final

2020/0359 (COD)

Proposta di

DIRETTIVA DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, che abroga la direttiva (UE) 2016/1148

(Testo rilevante ai fini del SEE)

{SEC(2020) 430 final} - {SWD(2020) 344 final} - {SWD(2020) 345 final}

RELAZIONE

1. CONTESTO DELLA PROPOSTA

• Motivi e obiettivi della proposta

La presente proposta rientra in un pacchetto di misure volte a migliorare ulteriormente le capacità di resilienza e di risposta agli incidenti di soggetti pubblici e privati, delle autorità competenti e dell'Unione nel suo complesso nel campo della cibersicurezza e della protezione delle infrastrutture critiche. Essa è in linea con le priorità della Commissione di preparare l'Europa per l'era digitale e costruire un'economia pronta per le sfide del futuro e al servizio dei cittadini. La cibersicurezza è una priorità nella risposta della Commissione alla crisi COVID-19. Il pacchetto comprende una nuova strategia per la cibersicurezza mirata a rafforzare l'autonomia strategica dell'Unione per migliorarne la resilienza e la risposta collettiva e creare una rete Internet globale e aperta. Il pacchetto contiene infine una proposta di una direttiva sulla resilienza degli operatori critici di servizi essenziali, che mira a ridurre le minacce fisiche nei confronti di tali operatori.

Questa proposta si basa e abroga la direttiva (UE) 2016/1148 sulla sicurezza delle reti e dei sistemi informativi nell'Unione (direttiva NIS), che è il primo strumento legislativo a livello dell'UE sulla cibersicurezza e prevede misure giuridiche volte a incrementare il livello complessivo di cibersicurezza nell'Unione. La direttiva NIS ha 1) contribuito al miglioramento delle capacità di cibersicurezza a livello nazionale chiedendo agli Stati membri di adottare strategie nazionali per la cibersicurezza e nominare autorità competenti in materia; 2) rafforzato la cooperazione tra Stati membri a livello dell'Unione istituendo vari forum che facilitano lo scambio di informazioni strategiche e operative; e 3) migliorato la resilienza informatica (ciberresilienza) di soggetti pubblici e privati in sette settori specifici (energia, trasporti, banche, infrastrutture dei mercati finanziari, sanità, fornitura e distribuzione di acqua potabile e infrastrutture digitali) e in tre servizi digitali (mercati online, motori di ricerca online e servizi di cloud computing) chiedendo agli Stati membri di garantire che gli operatori di servizi essenziali e i fornitori di servizi digitali introducano requisiti di cibersicurezza e segnalino gli incidenti.

La proposta modernizza il quadro giuridico esistente tenendo conto della crescente digitalizzazione del mercato interno avvenuta negli ultimi anni e del panorama in rapida evoluzione delle minacce alla cibersicurezza. Entrambi i fenomeni si sono ulteriormente amplificati dall'inizio della crisi COVID-19. La proposta affronta inoltre alcune carenze che hanno impedito alla direttiva NIS di realizzare appieno il suo potenziale.

Nonostante gli importanti risultati ottenuti, la direttiva NIS, che ha spianato la strada a un significativo cambiamento di mentalità in relazione all'approccio istituzionale e normativo alla cibersicurezza in molti Stati membri, ha mostrato anche i suoi limiti. La trasformazione digitale della società (intensificata dalla crisi COVID-19) ha ampliato il panorama delle minacce e sta lanciando nuove sfide, che richiedono risposte adeguate e innovative. Gli attacchi informatici sono in continuo aumento, molti dei quali, sempre più sofisticati, provengono da un'ampia gamma di fonti interne ed esterne all'UE.

La valutazione del funzionamento della direttiva NIS, condotta ai fini della valutazione d'impatto, ha identificato i seguenti problemi: 1) il basso livello di ciberresilienza delle imprese operanti nell'UE; 2) i diversi livelli di resilienza tra Stati membri e tra settori; e 3) il basso livello di consapevolezza situazionale comune e la mancanza di una risposta comune alle crisi. Ad esempio, alcuni importanti ospedali di uno Stato membro non rientrano nell'ambito di applicazione della direttiva NIS e pertanto non sono tenuti ad attuare le

risultanti misure di sicurezza, mentre in un altro Stato membro quasi tutti gli ospedali sono soggetti ai requisiti di sicurezza della direttiva NIS.

Essendo un'iniziativa del programma di controllo dell'adeguatezza e dell'efficacia della regolamentazione (REFIT), la proposta mira a ridurre l'onere normativo per le autorità competenti e i costi di conformità per i soggetti pubblici e privati. In particolare, tale obiettivo è raggiunto abolendo l'obbligo per le autorità competenti di individuare gli operatori di servizi essenziali e aumentando il livello di armonizzazione dei requisiti di sicurezza e segnalazione allo scopo di facilitare la conformità normativa per i soggetti che offrono servizi transfrontalieri. Al contempo, alle autorità competenti saranno assegnati anche alcuni nuovi compiti, tra cui la vigilanza di soggetti in settori finora non rientranti nell'ambito di applicazione dalla direttiva NIS.

- **Coerenza con le disposizioni vigenti nel settore normativo interessato**

Questa proposta fa parte di un insieme più ampio di strumenti giuridici esistenti e di future iniziative a livello dell'Unione volte ad aumentare la resilienza di soggetti pubblici e privati alle minacce.

Nel settore della cibersicurezza, si tratta in particolare della direttiva (UE) 2018/1972, che istituisce il codice europeo delle comunicazioni elettroniche (le cui disposizioni relative alla cibersicurezza saranno sostituite con le disposizioni della proposta in esame) e la proposta di un regolamento relativo alla resilienza operativa digitale per il settore finanziario (COM(2020) 595 final), che saranno considerati come *lex specialis* rispetto alla proposta in esame non appena entrambi gli atti entreranno in vigore.

Nel settore della sicurezza fisica, la proposta integra la proposta di direttiva sulla resilienza dei soggetti critici, che costituisce una revisione della direttiva 2008/114/CE relativa all'individuazione e alla designazione delle infrastrutture critiche europee e alla valutazione della necessità di migliorarne la protezione (direttiva sulle infrastrutture critiche europee), la quale istituisce un processo dell'Unione per l'identificazione e la designazione delle infrastrutture critiche europee e definisce un approccio volto a migliorarne la protezione. Nel luglio 2020 la Commissione ha adottato la strategia dell'UE per l'Unione della sicurezza[1], che ha confermato l'aumento dell'interconnessione e dell'interdipendenza tra infrastrutture fisiche e digitali. Tale strategia sottolineava la necessità di un approccio più coerente e omogeneo tra la direttiva ECI sulle infrastrutture critiche europee e la direttiva (UE) 2016/1148 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.

La proposta è pertanto strettamente allineata con la proposta di direttiva sulla resilienza dei soggetti critici, che mira ad aumentare la resilienza di tali soggetti alle minacce fisiche in un elevato numero di settori. La proposta punta a garantire che le autorità competenti previste da entrambi gli atti giuridici adottino misure complementari e scambino le informazioni necessarie per quanto riguarda la resilienza informatica e non, e che in particolare gli operatori critici dei settori considerati "essenziali" dalla proposta in oggetto siano anch'essi soggetti a obblighi più generali di aumento della resilienza, con particolare riguardo ai rischi non informatici.

[1] COM(2020) 605 final.

- **Coerenza con le altre normative dell'Unione**

Come si legge nella comunicazione "Plasmare il futuro digitale dell'Europa"[2], è fondamentale che l'Europa colga tutti i vantaggi dell'era digitale e rafforzi la sua capacità industriale e di innovazione entro limiti sicuri ed etici. La strategia europea per i dati stabilisce quattro pilastri, ossia protezione dei dati, diritti fondamentali, sicurezza e cibersicurezza, come prerequisiti essenziali per una società che, grazie all'uso dei dati, disponga di maggiori strumenti.

In una risoluzione del 12 marzo 2019, il Parlamento europeo ha invitato *"[…] la Commissione a valutare la necessità di estendere ulteriormente l'ambito di applicazione della direttiva NIS ad altri settori e servizi critici, che non sono coperti da una legislazione settoriale"*[3]. Nelle sue conclusioni del 9 giugno 2020, il Consiglio ha accolto con favore *"[…] i piani della Commissione tesi a garantire norme coerenti per gli operatori di mercato e ad agevolare una condivisione delle informazioni sicura, solida e adeguata in materia di minacce e incidenti, anche tramite un riesame della direttiva sulla sicurezza delle reti e dei sistemi informativi (direttiva NIS), nonché a esplorare possibilità per migliorare la ciberresilienza e rispondere in modo più efficace agli attacchi informatici, in particolar modo quelli rivolti ad attività economiche e sociali essenziali, nel rispetto delle competenze degli Stati membri, ivi compresa la responsabilità per la loro sicurezza nazionale"*[4]. Inoltre, l'atto giuridico proposto non pregiudica l'applicazione delle norme in materia di concorrenza stabilite nel trattato sul funzionamento dell'Unione europea (TFUE).

Poiché una parte significativa delle minacce alla cibersicurezza ha origine al di fuori dell'UE, è necessario un approccio coerente alla cooperazione internazionale. La presente direttiva costituisce un modello di riferimento da promuovere nel contesto della cooperazione dell'UE con i paesi terzi, in particolare nella fornitura di assistenza tecnica esterna.

2. BASE GIURIDICA, SUSSIDIARIETÀ E PROPORZIONALITÀ

- **Base giuridica**

La base giuridica della direttiva NIS è l'articolo 114 del trattato sul funzionamento dell'Unione europea (TFUE), il cui obiettivo è l'instaurazione e il funzionamento del mercato interno mediante il rafforzamento delle misure relative al ravvicinamento delle normative nazionali. Conformemente alla sentenza della Corte di giustizia dell'UE nella causa C- 58/08, Vodafone Ltd e altri, il ricorso all'articolo 114 TFUE è giustificato in caso di divergenze tra le normative nazionali qualora queste incidano direttamente sul funzionamento del mercato interno. Analogamente, la Corte ha ritenuto che qualora un atto fondato sull'articolo 114 TFUE abbia già eliminato qualsiasi ostacolo agli scambi nel settore da esso armonizzato, il legislatore dell'Unione non può essere privato della possibilità di adeguare tale atto a qualsivoglia modificazione delle circostanze o evoluzione delle conoscenze, in considerazione del compito affidatogli di vigilare alla protezione degli interessi generali riconosciuti dal trattato. Infine, secondo la Corte le misure relative al ravvicinamento previste dall'articolo 114 TFUE intendono consentire, in funzione del contesto generale e delle circostanze specifiche della materia da armonizzare, un margine di discrezionalità in merito alla tecnica di ravvicinamento più appropriata per ottenere il risultato auspicato. L'atto giuridico proposto

[2] COM(2020)67 final.
[3] https://www.europarl.europa.eu/doceo/document/TA-8-2019-0156_IT.html.
[4] https://data.consilium.europa.eu/doc/document/ST-8711-2020-INIT/it/pdf.

favorirebbe e migliorerebbe l'instaurazione e il funzionamento del mercato interno per i soggetti essenziali e importanti nei seguenti modi: stabilendo norme chiare e generalmente applicabili relative all'ambito di applicazione della direttiva NIS e armonizzando le norme applicabili nel settore della gestione del rischio di cibersicurezza e della segnalazione di incidenti. Le attuali disparità in questo settore, sia a livello legislativo che di vigilanza, nonché a livello nazionale e dell'Unione, costituiscono ostacoli per il mercato interno perché i soggetti impegnati in attività transfrontaliere fanno fronte a obblighi normativi diversi, con possibili sovrapposizioni, e/o a una loro diversa applicazione a scapito dell'esercizio della loro libertà di stabilimento e la libera prestazione di servizi. Norme diverse hanno anche un impatto negativo sulle condizioni della concorrenza nel mercato interno quando si tratta di soggetti dello stesso tipo in Stati membri diversi.

- **Sussidiarietà (per la competenza non esclusiva)**

La resilienza in termini di cibersicurezza all'interno dell'Unione non può essere efficace se affrontata in modo diverso nei vari silos nazionali o regionali. La direttiva NIS ha parzialmente ovviato a questa carenza definendo un quadro per la sicurezza delle reti e dei sistemi informativi a livello nazionale e dell'Unione. Tuttavia, il suo recepimento e la sua attuazione hanno portato alla luce carenze e limiti intrinseci di alcune disposizioni o approcci, come la poco chiara delimitazione del suo ambito di applicazione, che ha determinato differenze significative in termini di portata e intensità dell'intervento effettivo dell'UE a livello di Stati membri. Inoltre, con la crisi COVID-19, l'economia europea è diventata dipendente dai sistemi informatici e di rete come mai prima d'ora, mentre settori e servizi sono sempre più interconnessi. L'intervento dell'UE, che va oltre gli attuali provvedimenti della direttiva NIS, è giustificato principalmente dai seguenti fattori: i) la natura sempre più transfrontaliera delle minacce e delle sfide legate alla NIS; ii) le potenzialità degli interventi dell'Unione volti a migliorare e agevolare strategie nazionali efficaci e coordinate; e iii) il contributo degli interventi strategici concertati e collaborativi volti a un'efficace protezione dei dati e della vita privata.

- **Proporzionalità**

Le norme proposte nella presente direttiva non vanno oltre ciò che è necessario per raggiungere in modo soddisfacente gli obiettivi specifici. L'allineamento e la razionalizzazione previsti delle misure di sicurezza e degli obblighi di segnalazione sono relativi alle richieste degli Stati membri e delle imprese di migliorare il quadro attuale.

La proposta tiene conto delle pratiche già esistenti negli Stati membri. Un livello maggiore di protezione conseguito grazie a misure razionalizzate e coordinate, come quelle proposte, è proporzionale ai rischi sempre più elevati affrontati, compresi quelli che presentano un elemento transfrontaliero; esse sono ragionevoli e corrispondono generalmente agli interessi dei soggetti coinvolti nel garantire la continuità e la qualità dei loro servizi. I costi per garantire una cooperazione sistematica tra Stati membri sarebbero minimi rispetto alle perdite e ai danni economici e sociali causati dagli incidenti di cibersicurezza. Inoltre, le consultazioni dei portatori di interessi tenutesi nel contesto del riesame della direttiva NIS, compresi i risultati della consultazione pubblica e le indagini mirate, dimostrano che la revisione della direttiva NIS, secondo le linee summenzionate, è accolta con favore.

- **Scelta dell'atto giuridico**

La proposta razionalizzerà ulteriormente gli obblighi imposti alle imprese e garantirà un livello più alto di armonizzazione degli stessi. Al contempo, la proposta mira a dotare gli Stati

membri della flessibilità necessaria per tenere conto delle specificità nazionali (come la possibilità di individuare ulteriori soggetti essenziali o importanti al di là dello scenario di riferimento previsto dall'atto giuridico). Il futuro strumento giuridico dovrebbe pertanto essere una direttiva, in quanto questo strumento consente una migliore armonizzazione mirata, nonché un certo livello di flessibilità per le autorità competenti.

3. RISULTATI DELLE VALUTAZIONI EX POST, DELLE CONSULTAZIONI DEI PORTATORI DI INTERESSI E DELLE VALUTAZIONI D'IMPATTO

- **Valutazioni ex post / Vaglio di adeguatezza della legislazione vigente**

La Commissione ha eseguito una valutazione del funzionamento della direttiva NIS[5] analizzando la rilevanza, il valore aggiunto dell'UE, la coerenza, l'efficacia e l'efficienza di tale direttiva. Le principali conclusioni di questa analisi sono le seguenti.

- L'ambito di applicazione della direttiva NIS è troppo limitato in termini di settori considerati, principalmente per i motivi seguenti: i) l'aumento della digitalizzazione negli ultimi anni e il livello più elevato di interconnessione, ii) il fatto che l'ambito di applicazione della direttiva NIS non riflette più tutti i settori digitalizzati che forniscono servizi chiave all'economia e alla società nel suo complesso.
- La direttiva NIS non è sufficientemente chiara per quanto riguarda l'ambito di applicazione per gli operatori di servizi essenziali e le sue disposizioni non chiariscono a sufficienza la competenza nazionale sui fornitori di servizi digitali. Questo ha determinato una situazione in cui determinati tipi di soggetti non sono stati individuati in tutti gli Stati membri e non hanno pertanto l'obbligo di mettere in atto misure di sicurezza e segnalare incidenti.
- La direttiva NIS ha concesso agli Stati membri un'ampia discrezionalità nello stabilire i requisiti di sicurezza e di segnalazione di incidenti per gli operatori di servizi essenziali. La valutazione mostra che in alcuni casi gli Stati membri hanno attuato tali requisiti in modi significativamente diversi, creando oneri aggiuntivi per le società operanti in più di uno Stato membro.
- Il regime di vigilanza e esecuzione della direttiva NIS non è efficace. Gli Stati membri hanno ad esempio mostrato molta riluttanza nell'applicazione delle sanzioni ai soggetti che omettevano di adottare requisiti di sicurezza o di segnalare incidenti. Ciò può avere conseguenze negative per la ciberresilienza di singoli soggetti.
- Le risorse finanziarie e umane accantonate dagli Stati membri per l'adempimento dei loro compiti (come l'identificazione o la vigilanza degli operatori di servizi essenziali), e di conseguenza i diversi livelli di maturità nell'affrontare i rischi di cibersicurezza, variano considerevolmente. Ciò ha ulteriormente accentuato le differenze in termini di ciberresilienza tra gli Stati membri.
- Gli Stati membri non condividono sistematicamente le informazioni tra loro, con conseguenze negative in particolare sull'efficacia delle misure di cibersicurezza e sul livello di consapevolezza situazionale comune a livello dell'UE. Questo vale anche per la condivisione di informazioni tra soggetti privati e per il coinvolgimento tra soggetti privati e strutture di cooperazione a livello dell'UE.

[5] [Allegato 5 della valutazione d'impatto].

- **Consultazioni dei portatori di interessi**

La Commissione ha consultato una vasta gamma di portatori di interessi. Gli Stati membri e i portatori di interessi sono stati invitati a partecipare alla consultazione pubblica e alle indagini e ai seminari organizzati da Wavestone, CEPS e ICF, incaricati dalla Commissione di condurre uno studio a sostegno del riesame della direttiva NIS. Tra i portatori di interessi consultati figurano autorità competenti, organismi dell'Unione preposti alla cibersicurezza, operatori di servizi essenziali, fornitori di servizi digitali, soggetti che forniscono servizi che esulano dall'ambito di applicazione dell'attuale direttiva NIS, associazioni di categoria e organizzazioni di consumatori e cittadini.

La Commissione è inoltre rimasta costantemente in contatto con le autorità competenti incaricate dell'attuazione della direttiva NIS. Il gruppo di cooperazione ha trattato in modo approfondito vari aspetti trasversali e settoriali dell'attuazione. Infine, durante le sue visite nei paesi in relazione alla NIS nel 2019 e nel 2020, la Commissione ha intervistato 154 soggetti pubblici e privati, nonché 117 autorità competenti.

- **Assunzione e uso di perizie**

Un consorzio formato da Wavestone, CEPS e ICF è stato incaricato dalla Commissione al fine di assisterla nel riesame della direttiva NIS[6]. Il consorzio non solo si è messo in contatto, mediante indagini e seminari mirati, con i portatori di interessi direttamente interessati dalla direttiva NIS, ma ha anche consultato diversi esperti nel campo della cibersicurezza, come ricercatori e professionisti del settore.

- **Valutazione d'impatto**

Questa proposta è accompagnata da una valutazione d'impatto[7] che è stata presentata il 23 ottobre 2020 al comitato per il controllo normativo, il quale il 20 novembre 2020 ha espresso un parere positivo con osservazioni. Il comitato per il controllo normativo ha raccomandato miglioramenti in alcuni ambiti allo scopo di: 1) riflettere meglio il ruolo degli effetti di ricaduta transfrontaliera nell'analisi del problema; 2) fornire una più ampia spiegazione di come si realizzerebbe il successo dell'iniziativa; 3) fornire ulteriori giustificazioni all'elenco delle opzioni strategiche; 4) sviluppare ulteriormente il tema dei costi delle misure proposte. La valutazione d'impatto è stata adeguata per affrontare sia questi punti sia le osservazioni più dettagliate del comitato per il controllo normativo. La valutazione ora comprende spiegazioni più dettagliate circa il ruolo degli effetti di ricaduta transfrontaliera nel campo della cibersicurezza, una panoramica più chiara di come può essere misurato il successo dell'iniziativa, una spiegazione più particolareggiata della concezione e della logica alla base delle diverse opzioni strategiche e delle azioni previste nell'ambito di tali opzioni, una spiegazione più dettagliata degli aspetti analizzati in relazione all'ambito di applicazione settoriale della direttiva NIS e maggiori chiarimenti in relazione ai costi.

La Commissione ha preso in esame alcune opzioni strategiche per migliorare il quadro giuridico nel settore della ciberresilienza e della riposta agli incidenti:

---

6 Studio a supporto sostegno del riesame della direttiva (UE) 2016/1148 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (direttiva NIS) – n. 2020-665. Wavestone, CEPS e ICF.

7 **[Link al documento finale e alla scheda riepilogativa da aggiungere.]**

- nessun provvedimento: la direttiva NIS resterebbe invariata e non sarebbe adottata alcun'altra misura di natura non legislativa per affrontare i problemi individuati dalla valutazione della direttiva NIS;
- opzione 1: non vi sarebbe alcun cambiamento a livello legislativo. La Commissione formulerebbe invece raccomandazioni e orientamenti (ad esempio sull'individuazione di operatori di servizi essenziali, sui requisiti di sicurezza, sulle procedure di notifica di incidenti e sulla vigilanza) previa consultazione del gruppo di cooperazione, dell'Agenzia dell'UE per la cibersicurezza (ENISA) e, a seconda dei casi, della rete di team di risposta agli incidenti di sicurezza informatica (CSIRT);
- opzione 2: questa opzione prevede modifiche mirate della direttiva NIS, tra cui un ampliamento dell'ambito di applicazione e diverse altre modifiche volte a garantire alcune soluzioni immediate ai problemi individuati, fornendo maggiore chiarezza e una migliore armonizzazione (come le disposizioni per armonizzare le soglie di identificazione). La direttiva NIS modificata manterrebbe tuttavia i principali elementi di base, l'approccio e le motivazioni;
- opzione 3: questo scenario comporta modifiche sistemiche e strutturali alla direttiva NIS (attraverso una nuova direttiva) e prevede un cambio di approccio più profondo che interessi un segmento più ampio delle economie dell'Unione, seppure con una vigilanza più mirata nei confronti di operatori chiave e di grandi dimensioni. Semplificherebbe altresì gli obblighi imposti alle imprese e garantirebbe un livello più alto di armonizzazione, creerebbe una definizione più efficace degli aspetti operativi e stabilirebbe una chiara base per una migliore responsabilizzazione (accountability) e condivisione delle responsabilità dei vari portatori di interesse per quanto riguarda le misure di cibersicurezza.

La valutazione d'impatto conclude che l'opzione prescelta è l'opzione 3 (ossia modifiche sistemiche e strutturali del quadro NIS). In termini di efficacia, l'opzione prescelta determinerebbe chiaramente l'ambito di applicazione della direttiva NIS, estendendolo a un insieme più rappresentativo di economie e società dell'UE, e la razionalizzazione dei requisiti, unitamente a un quadro più definito di vigilanza e controllo che dovrebbe mirare ad aumentare il livello di conformità. Tale opzione comporta altresì misure volte a migliorare gli approcci di definizione delle politiche a livello degli Stati membri e a cambiarne il paradigma, promuovendo nuovi quadri per la gestione del rischio relativo alle relazioni con i fornitori e la divulgazione coordinata delle vulnerabilità. Al contempo, l'opzione strategica prescelta crea una chiara base per la responsabilizzazione (accountability) e le responsabilità condivise e prevede meccanismi volti a promuovere una maggiore fiducia tra Stati membri, sia a livello di autorità che di industria, incentivando la condivisione di informazioni e garantendo un approccio maggiormente operativo, come ad esempio meccanismi di assistenza reciproca e di revisione tra pari. Questa opzione prevedrebbe anche un quadro di gestione delle crisi a livello dell'UE, basato sulla rete operativa dell'UE varata di recente, e garantirebbe un maggiore coinvolgimento dell'ENISA, entro i limiti del suo mandato attuale, nel mantenere un'accurata panoramica dello stato di cibersicurezza dell'Unione.

In termini di efficienza, sebbene l'opzione prescelta comporterebbe ulteriori costi di conformità e esecuzione per imprese e Stati membri, essa determinerebbe anche efficienti compromessi e sinergie, con le migliori potenzialità tra tutte le opzioni strategiche analizzate per garantire un livello superiore e coerente di ciberresilienza dei soggetti chiave all'interno dell'Unione, con conseguenti risparmi di costi sia per le imprese che per la società. Questa opzione d'intervento determinerebbe alcuni oneri amministrativi e costi di conformità supplementari per le autorità degli Stati membri. Nel complesso, tuttavia, nel medio e lungo

termine porterebbe anche benefici sostanziali mediante una maggiore cooperazione tra Stati membri, anche a livello operativo, nonché incentivando un aumento complessivo delle capacità di cibersicurezza a livello nazionale e regionale attraverso l'assistenza reciproca, i meccanismi di revisione tra pari e una migliore panoramica delle imprese chiave e dell'interazione con le stesse. L'opzione d'intervento prescelta garantirebbe inoltre in larga misura coerenza con altre normative, iniziative o misure strategiche, compresa la *lex specialis* settoriale.

Affrontando il problema attualmente persistente dell'insufficienza del livello di preparazione in materia di cibersicurezza a livello di Stati membri e di società e altre organizzazioni, si potrebbe ottenere un miglioramento in termini di efficienza e riduzione dei costi supplementari derivanti da incidenti di cibersicurezza.

- Per i soggetti essenziali e importanti, l'aumento del livello di preparazione in materia di cibersicurezza potrebbe attenuare la potenziale perdita di entrate a causa di perturbazioni, dovute anche allo spionaggio industriale, e potrebbe ridurre le ingenti spese destinate alla mitigazione ad hoc delle minacce. Tali vantaggi dovrebbero superare i costi d'investimento necessari. La riduzione della frammentazione del mercato interno migliorerebbe anche la parità di condizioni tra operatori.
- Per gli Stati membri ciò potrebbe ulteriormente ridurre il rischio di un aumento delle spese di bilancio destinate alla mitigazione ad hoc delle minacce e i costi supplementari in caso di emergenze legate a incidenti di cibersicurezza.
- Per i cittadini, affrontare il problema degli incidenti di cibersicurezza si tradurrà prevedibilmente in una riduzione delle perdite di reddito dovute a perturbazioni economiche.

L'aumento dei livelli di cibersicurezza negli Stati membri e la capacità delle società e delle autorità di rispondere rapidamente a un incidente e di mitigarne l'impatto, determineranno con tutta probabilità un aumento della fiducia globale dei cittadini nell'economia digitale, con un possibile impatto positivo sulla crescita e sugli investimenti.

L'aumento del livello generale di cibersicurezza è probabile che porti a una maggiore sicurezza generale e a un funzionamento ininterrotto dei servizi essenziali, i quali sono fondamentali per la società. L'iniziativa può inoltre contribuire ad altri impatti sociali, quali la riduzione dei livelli di criminalità informatica e terrorismo e una maggiore protezione civile. L'aumento del livello di preparazione di imprese e altre organizzazioni contro le minacce informatiche può evitare potenziali perdite finanziarie dovute a attacchi informatici, evitando in tal modo la necessità di licenziare i dipendenti.

L'aumento del livello globale di cibersicurezza potrebbe anche prevenire i rischi/danni ambientali in caso di attacco a un servizio essenziale. Questo potrebbe valere in particolare per i settori dell'energia, della distribuzione e dell'approvvigionamento dell'acqua o dei trasporti. Rafforzando le capacità di cibersicurezza, l'iniziativa potrebbe portare a un maggiore utilizzo delle infrastrutture e dei servizi TIC di ultima generazione, che sono anche più sostenibili dal punto di vista ambientale, e alla sostituzione di infrastrutture preesistenti inefficienti e meno sicure. Ciò contribuirà prevedibilmente anche a ridurre il numero di costosi incidenti informatici, liberando risorse disponibili per investimenti sostenibili.

- **Efficienza normativa e semplificazione**

La proposta prevede un'esclusione generale di micro e piccoli soggetti dal campo di applicazione della direttiva NIS e un regime di vigilanza ex post più leggero applicato a un

gran numero di nuovi soggetti nell'ambito del campo di applicazione rivisto (i cosiddetti soggetti importanti). Tali misure mirano a ridurre al minimo ed equilibrare gli oneri che gravano sulle imprese e sulle pubbliche amministrazioni. La proposta sostituisce inoltre il complesso sistema di identificazione degli operatori di servizi essenziali con un obbligo generalmente applicabile e introduce un livello più elevato di armonizzazione degli obblighi di sicurezza e di segnalazione, che ridurrebbe l'onere della conformità, in particolare per i soggetti che forniscono servizi transfrontalieri.

La proposta riduce al minimo i costi di conformità per le PMI, in quanto i soggetti sono tenuti ad adottare solo le misure necessarie a garantire un livello di sicurezza dei sistemi informatici e di rete adeguato al rischio presentato.

- **Diritti fondamentali**

L'UE si impegna a garantire standard elevati in materia di tutela dei diritti fondamentali. Tutti gli accordi volontari di condivisione delle informazioni tra soggetti promossi dalla presente direttiva sarebbero attuati in ambienti sicuri nel pieno rispetto delle norme dell'Unione in materia di protezione dei dati, in particolare il regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio[8].

4. INCIDENZA SUL BILANCIO

Cfr. scheda finanziaria

5. ALTRI ELEMENTI

- **Piani attuativi e modalità di monitoraggio, valutazione e informazione**

La proposta comprende un piano generale di monitoraggio e valutazione dell'impatto sugli obiettivi specifici, che richiede alla Commissione di effettuare una revisione almeno [54 mesi] dopo la data di entrata in vigore e di riferire al Parlamento europeo e al Consiglio sulle sue principali conclusioni.

Il riesame dovrà essere effettuato in linea con gli orientamenti della Commissione per legiferare meglio.

- **Illustrazione dettagliata delle singole disposizioni della proposta**

La proposta è strutturata attorno a diversi settori d'intervento principali, che sono interconnessi e hanno lo scopo di aumentare il livello di cibersicurezza nell'Unione.

Oggetto e ambito di applicazione (articoli 1 e 2)

La direttiva, in particolare: a) stabilisce obblighi per gli Stati membri di adottare una strategia nazionale per la cibersicurezza, designare autorità nazionali competenti, punti di contatto unici e CSIRT; b) prevede che gli Stati membri stabiliscano obblighi di gestione e segnalazione dei rischi di cibersicurezza per i soggetti indicati come soggetti essenziali nell'allegato I e come soggetti importanti nell'allegato II; c) prevede che gli Stati membri stabiliscano obblighi in materia di condivisione delle informazioni sulla cibersicurezza.

[8] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (GU L 119 del 4.5.2016, pag. 1).

La direttiva si applica a taluni soggetti essenziali pubblici o privati che operano nei settori elencati nell'allegato I (energia; trasporti; settore bancario; infrastrutture dei mercati finanziari; settore sanitario, acqua potabile; acque reflue; infrastrutture digitali; pubblica amministrazione e spazio) e a taluni soggetti importanti che operano nei settori elencati nell'allegato II (servizi postali e di corriere; gestione dei rifiuti; fabbricazione, produzione e distribuzione di prodotti chimici; produzione, trasformazione e distribuzione di alimenti; settore della fabbricazione e fornitori di servizi digitali). Le microimprese e le piccole imprese ai sensi della raccomandazione 2003/361/CE della Commissione, del 6 maggio 2003, sono escluse dall'ambito di applicazione della direttiva, ad eccezione dei fornitori di reti di comunicazione elettronica o di servizi di comunicazione elettronica accessibili al pubblico, dei prestatori di servizi fiduciari, dei registri dei nomi di dominio di primo livello (*top-level domain*, TLD) e della pubblica amministrazione, nonché di alcuni altri soggetti, come l'unico fornitore di un servizio in uno Stato membro.

Quadri nazionali di cibersicurezza (articoli da 5 a 11)

Gli Stati membri sono tenuti ad adottare una strategia nazionale per la cibersicurezza che definisca gli obiettivi strategici e le misure politiche e normative appropriate volte a raggiungere e mantenere un livello elevato di cibersicurezza.

La direttiva stabilisce inoltre un quadro per la divulgazione coordinata delle vulnerabilità e impone agli Stati membri di designare CSIRT che agiscano da intermediari fidati e facilitino l'interazione tra i soggetti segnalanti e i fabbricanti o fornitori di prodotti e servizi TIC. L'ENISA è tenuta a sviluppare e mantenere un registro europeo delle vulnerabilità per le vulnerabilità individuate

Gli Stati membri sono tenuti a mettere in atto quadri nazionali di gestione delle crisi di cibersicurezza, tra l'altro designando le autorità nazionali competenti responsabili della gestione di incidenti e crisi di cibersicurezza su vasta scala.

Gli Stati membri sono inoltre tenuti a designare una o più autorità nazionali competenti in materia di cibersicurezza per i compiti di vigilanza previsti dalla presente direttiva e un punto di contatto unico nazionale in materia di cibersicurezza (SPOC) che eserciti una funzione di collegamento per garantire la cooperazione transfrontaliera delle autorità degli Stati membri. Gli Stati membri sono inoltre tenuti a designare i CSIRT.

Cooperazione (articoli da 12 a 16)

La direttiva istituisce un gruppo di cooperazione al fine di sostenere e agevolare la cooperazione strategica e lo scambio di informazioni tra Stati membri e di sviluppare la fiducia. Istituisce inoltre una rete di CSIRT allo scopo di contribuire allo sviluppo della fiducia fra gli Stati membri e di promuovere una cooperazione operativa rapida ed efficace.

È istituita una rete europea delle organizzazioni di collegamento per le crisi informatiche (EU-CyCLONe) per sostenere la gestione coordinata di incidenti e crisi di cibersicurezza su vasta scala e garantire il regolare scambio di informazioni tra gli Stati membri e le istituzioni dell'UE.

L'ENISA è tenuta a presentare, in collaborazione con la Commissione, una relazione annuale sullo stato della cibersicurezza nell'Unione.

La Commissione è tenuta a istituire un sistema di revisione tra pari che consenta di effettuare revisioni tra pari periodiche dell'efficacia delle politiche di cibersicurezza adottate dagli Stati membri.

Obblighi di gestione e segnalazione dei rischi di cibersicurezza (articoli da 17 a 23)

La direttiva impone agli Stati membri di prevedere che gli organi di gestione di tutti i soggetti che rientrano nell'ambito di applicazione approvino le misure di gestione dei rischi di cibersicurezza adottate dai rispettivi soggetti e seguano una formazione specifica in materia di cibersicurezza.

Gli Stati membri sono tenuti a garantire che i soggetti che rientrano nell'ambito di applicazione adottino misure tecniche e organizzative adeguate e proporzionate per gestire i rischi posti alla sicurezza dei sistemi informatici e di rete. Essi hanno inoltre l'obbligo di garantire che i soggetti notifichino alle autorità nazionali competenti o ai CSIRT qualsiasi incidente di cibersicurezza che abbia un impatto significativo sulla fornitura dei loro servizi.

I registri dei TLD e i soggetti che forniscono servizi di registrazione dei nomi di dominio per i TLD devono raccogliere e mantenere dati di registrazione dei nomi di dominio accurati e completi. Inoltre, tali soggetti sono tenuti a fornire un accesso efficiente ai dati di registrazione del dominio per i legittimi richiedenti l'accesso.

Giurisdizione e registrazione (articoli 24 e 25)

Di norma, i soggetti essenziali e importanti sono sottoposti alla giurisdizione dello Stato membro in cui prestano i propri servizi. Tuttavia alcuni tipi di soggetti (fornitori di servizi DNS, registri dei nomi di dominio di primo livello, fornitori di servizi di cloud computing, fornitori di servizi di data center e fornitori di reti di distribuzione dei contenuti, nonché alcuni fornitori di servizi digitali) sono sottoposti alla giurisdizione dello Stato membro in cui hanno lo stabilimento principale nell'Unione In questo modo si garantisce che tali soggetti non si confrontino con una miriade di prescrizioni giuridiche diverse, nella fornitura di servizi transfrontalieri a un livello particolarmente elevato. L'ENISA è tenuta a creare e mantenere un registro dei soggetti di quest'ultimo tipo.

Condivisione di informazioni (articoli 26 e 27)

Gli Stati membri prevedono norme che consentano ai soggetti di partecipare alla condivisione di informazioni relative alla cibersicurezza nel quadro di specifici accordi di condivisione di informazioni in materia di cibersicurezza, in conformità all'articolo 101 TFUE. Inoltre, gli Stati membri consentono ai soggetti che non rientrano nell'ambito di applicazione della presente direttiva di segnalare, su base volontaria, incidenti significativi, minacce informatiche o "quasi incidenti".

Vigilanza e applicazione (articoli da 28 a 34)

Le autorità competenti sono tenute a esercitare la vigilanza sui soggetti che rientrano nell'ambito di applicazione della direttiva e in particolare a garantirne la conformità ai requisiti di sicurezza e di notifica degli incidenti. La direttiva distingue tra un regime di vigilanza ex ante per i soggetti essenziali e un regime di vigilanza ex post per i soggetti importanti, regime quest'ultimo che impone alle autorità competenti di adottare provvedimenti ricevono elementi di prova o indicazioni che un soggetto importante non soddisfa i requisiti di sicurezza e di segnalazione degli incidenti.

La direttiva obbliga inoltre gli Stati membri a imporre sanzioni amministrative pecuniarie ai soggetti essenziali e importanti e definisce alcune sanzioni massime.

Gli Stati membri sono tenuti a cooperare e ad assistersi reciprocamente in funzione delle necessità quando i soggetti prestano servizi in più di uno Stato membro o quando lo stabilimento principale di un soggetto o il suo rappresentante si trova in un determinato Stato membro, ma i suoi sistemi informatici e di rete sono situati in uno o più altri Stati membri.

2020/0359 (COD)

Proposta di

DIRETTIVA DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, che abroga la direttiva (UE) 2016/1148

(Testo rilevante ai fini del SEE)

IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea, in particolare l'articolo 114,

vista la proposta della Commissione europea,

previa trasmissione del progetto di atto legislativo ai parlamenti nazionali,

visto il parere del Comitato economico e sociale europeo[9],

visto il parere del Comitato delle regioni[10],

deliberando secondo la procedura legislativa ordinaria,

considerando quanto segue:

(1) La direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio[11] mirava a sviluppare le capacità di cibersicurezza in tutta l'Unione, ad attenuare le minacce alle reti e ai sistemi informativi utilizzati per fornire servizi essenziali in settori chiave e a garantire la continuità di tali servizi in caso di incidenti di cibersicurezza, contribuendo in tal modo al funzionamento efficace dell'economia e della società dell'Unione.

(2) Dall'entrata in vigore della direttiva (UE) 2016/1148 sono stati compiuti progressi significativi nell'aumentare il livello di resilienza dell'Unione in materia di cibersicurezza. La revisione di tale direttiva ha mostrato quanto quest'ultima sia servita da catalizzatore per l'approccio istituzionale e normativo alla cibersicurezza nell'Unione, aprendo la strada a un significativo cambiamento della mentalità. Tale direttiva ha garantito il completamento dei quadri nazionali definendo le strategie nazionali per la cibersicurezza, stabilendo capacità nazionali e attuando misure normative riguardanti le infrastrutture e gli attori essenziali individuati da ciascuno Stato membro. Ha inoltre contribuito alla cooperazione a livello dell'Unione mediante l'istituzione del gruppo di cooperazione[12] e di una rete di gruppi nazionali di intervento per la sicurezza informatica in caso di incidente ("rete di CSIRT")[13]. Nonostante tali risultati, la revisione della direttiva (UE) 2016/1148 ha rivelato carenze intrinseche che

9 GU C […] del […], pag. […].

10 GU C […] del […], pag. […].

11 Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (GU L 194 del 19.7.2016, pag. 1).

12 Articolo 11 della direttiva (UE) 2016/1148.

13 Articolo 12 della direttiva (UE) 2016/1148.

le impediscono di affrontare efficacemente le sfide attuali ed emergenti in materia di cibersicurezza.

(3) I sistemi informatici e di rete occupano ormai una posizione centrale nella vita di tutti i giorni, con la rapida trasformazione digitale e l'interconnessione della società, anche negli scambi transfrontalieri. Ciò ha portato a un'espansione del panorama delle minacce alla cibersicurezza, con nuove sfide che richiedono risposte adeguate, coordinate e innovative in tutti gli Stati membri. Il numero, la portata, il livello di sofisticazione, la frequenza e l'impatto degli incidenti di cibersicurezza stanno aumentando e rappresentano una grave minaccia per il funzionamento dei sistemi informatici e di rete. Tali incidenti possono quindi impedire l'esercizio delle attività economiche nel mercato interno, provocare perdite finanziarie, minare la fiducia degli utenti e causare gravi danni all'economia e alla società dell'Unione. Pertanto la preparazione e l'efficacia della cibersicurezza sono oggi più che mai essenziali per il corretto funzionamento del mercato interno.

(4) La base giuridica della direttiva (UE) 2016/1148 era l'articolo 114 del trattato sul funzionamento dell'Unione europea (TFUE), il cui obiettivo è l'instaurazione e il funzionamento del mercato interno mediante il rafforzamento delle misure relative al ravvicinamento delle normative nazionali. Gli obblighi di cibersicurezza imposti ai soggetti che forniscono servizi o attività economicamente rilevanti variano notevolmente da uno Stato membro all'altro in termini di tipo di obbligo, livello di dettaglio e metodo di vigilanza. Tali disparità comportano costi aggiuntivi e creano difficoltà per le imprese che offrono beni o servizi transfrontalieri. Gli obblighi imposti da uno Stato membro che sono diversi o addirittura in conflitto con quelli imposti da un altro Stato membro possono incidere in modo sostanziale su tali attività transfrontaliere. Inoltre è probabile che una progettazione o attuazione non ottimale delle norme in materia di cibersicurezza in uno Stato membro abbia ripercussioni sul livello di cibersicurezza di altri Stati membri, in particolare in considerazione degli intensi scambi transfrontalieri. Il riesame della direttiva (UE) 2016/1148 ha evidenziato notevoli divergenze nella sua attuazione da parte degli Stati membri, anche per quanto riguarda il suo ambito di applicazione, la cui delimitazione è stata lasciata in larga misura alla discrezione degli Stati membri. La direttiva (UE) 2016/1148 ha inoltre conferito agli Stati membri un ampio potere discrezionale per quanto riguarda l'attuazione degli obblighi in materia di sicurezza e segnalazione degli incidenti ivi stabiliti. Tali obblighi sono stati pertanto attuati in modi significativamente diversi a livello nazionale. Analoghe divergenze nell'attuazione si sono verificate in relazione alle disposizioni di tale direttiva in materia di vigilanza e esecuzione.

(5) Tutte queste divergenze comportano una frammentazione del mercato interno e possono avere un effetto pregiudizievole sul suo funzionamento, con ripercussioni in particolare sulla fornitura transfrontaliera di servizi e sul livello di resilienza della cibersicurezza dovute all'applicazione di norme diverse. La presente direttiva mira a eliminare tali ampie divergenze tra gli Stati membri, in particolare stabilendo norme minime riguardanti il funzionamento di un quadro normativo coordinato, istituendo meccanismi per una cooperazione efficace tra le autorità responsabili in ciascuno Stato membro, aggiornando l'elenco dei settori e delle attività soggetti agli obblighi in materia di cibersicurezza e prevedendo mezzi di ricorso e sanzioni effettivi che siano funzionali all'efficace applicazione di tali obblighi. La direttiva (UE) 2016/1148 dovrebbe pertanto essere abrogata e sostituita dalla presente direttiva.

(6) La presente direttiva lascia impregiudicata la possibilità, per gli Stati membri, di adottare le misure necessarie a garantire la tutela degli interessi essenziali della loro sicurezza, a salvaguardare l'ordine pubblico e la pubblica sicurezza e a consentire l'indagine, l'accertamento e il perseguimento dei reati, nel rispetto del diritto dell'Unione. Conformemente all'articolo 346 TFUE, nessuno Stato membro è tenuto a fornire informazioni la cui divulgazione sia contraria agli interessi essenziali della propria pubblica sicurezza. In tale contesto sono pertinenti le norme nazionali e dell'Unione per la protezione delle informazioni classificate, gli accordi di non divulgazione o gli accordi di non divulgazione informali, quale il protocollo TLP[14].

(7) Con l'abrogazione della direttiva (UE) 2016/1148, l'ambito di applicazione per settore dovrebbe essere esteso a una parte più ampia dell'economia alla luce delle considerazioni di cui ai considerando da 4 a 6. I settori contemplati dalla direttiva (UE) 2016/1148 dovrebbero pertanto essere ampliati per fornire una copertura completa dei settori e dei servizi di vitale importanza per le principali attività sociali ed economiche nel mercato interno. Le norme non dovrebbero essere diverse a seconda che i soggetti siano operatori di servizi essenziali o fornitori di servizi digitali. Tale differenziazione si è rivelata obsoleta, in quanto non riflette l'effettiva importanza dei settori o dei servizi per le attività sociali ed economiche nel mercato interno.

(8) Conformemente alla direttiva (UE) 2016/1148, gli Stati membri erano responsabili di determinare quali soggetti soddisfacevano i criteri per essere considerati operatori di servizi essenziali ("processo di identificazione"). Al fine di eliminare le ampie divergenze tra gli Stati membri a tale riguardo e garantire la certezza del diritto per quanto riguarda gli obblighi di gestione e segnalazione dei rischi per tutti i soggetti pertinenti, è opportuno stabilire un criterio uniforme che determini quali soggetti rientrano nell'ambito di applicazione della presente direttiva. Tale criterio dovrebbe consistere nell'applicazione della regola della soglia di dimensione, in base alla quale rientrano nell'ambito di applicazione della direttiva tutte le medie e le grandi imprese, quali definite nella raccomandazione 2003/361/CE della Commissione[15], che operano nei settori o forniscono il tipo di servizi contemplati dalla presente direttiva. Gli Stati membri non dovrebbero essere tenuti a redigere un elenco dei soggetti che soddisfano questo criterio relativo alle dimensioni generalmente applicabile.

(9) La presente direttiva dovrebbe tuttavia applicarsi anche ai piccoli o micro soggetti che soddisfano determinati criteri che indicano un ruolo chiave per le economie o le società degli Stati membri o per particolari settori o tipi di servizi. Gli Stati membri dovrebbero essere responsabili di stabilire un elenco di tali soggetti e presentarlo alla Commissione.

(10) La Commissione, in collaborazione con il gruppo di cooperazione, può emanare orientamenti relativi all'attuazione dei criteri applicabili alle microimprese e alle piccole imprese.

(11) A seconda del settore in cui operano o del tipo di servizio che forniscono, i soggetti che rientrano nell'ambito di applicazione della presente direttiva dovrebbero essere

---

[14] Il protocollo TLP (*Traffic Light Protocol*) è uno strumento che consente a chi condivide informazioni di informare il proprio pubblico in merito a eventuali limitazioni dell'ulteriore diffusione di tali informazioni. È utilizzato in quasi tutte le comunità di CSIRT e in alcuni centri di condivisione e di analisi delle informazioni (ISAC).

[15] Raccomandazione 2003/361/CE della Commissione, del 6 maggio 2003, relativa alla definizione delle microimprese, piccole e medie imprese (GU L 124 del 20.5.2003, pag. 36).

classificati in due categorie: essenziali e importanti. Tale categorizzazione dovrebbe tenere conto del livello di criticità del settore o del tipo di servizio, nonché del livello di dipendenza di altri settori o tipi di servizi. Sia ai soggetti essenziali sia a quelli importanti dovrebbero applicarsi gli stessi obblighi di gestione e segnalazione dei rischi. I regimi sanzionatori e di vigilanza tra queste due categorie di soggetti dovrebbero essere differenziati per garantire un giusto equilibrio tra i requisiti e gli obblighi, da un lato, e gli oneri amministrativi derivanti dalla vigilanza della conformità, dall'altro.

(12) La legislazione e gli strumenti settoriali possono contribuire a garantire livelli elevati di cibersicurezza, tenendo pienamente conto delle specificità e delle complessità di tali settori. Qualora un atto giuridico settoriale dell'Unione imponga ai soggetti essenziali o importanti obblighi relativi all'adozione di misure di gestione dei rischi di cibersicurezza o di notifica di incidenti o minacce informatiche significative di effetto almeno equivalente agli obblighi stabiliti nella presente direttiva, dovrebbero applicarsi tali disposizioni settoriali, anche in materia di vigilanza ed esecuzione. La Commissione può emanare orientamenti in relazione all'attuazione della *lex specialis*. La presente direttiva non preclude l'adozione di ulteriori atti settoriali dell'Unione riguardanti le misure di gestione dei rischi di cibersicurezza e le notifiche degli incidenti. La presente direttiva lascia impregiudicate le competenze di esecuzione esistenti conferite alla Commissione in una serie di settori, tra cui i trasporti e l'energia.

(13) Il regolamento XXXX/XXXX del Parlamento europeo e del Consiglio[16] dovrebbe essere considerato un atto giuridico settoriale dell'Unione in relazione alla presente direttiva per quanto riguarda i soggetti del settore finanziario. Invece delle disposizioni stabilite dalla presente direttiva dovrebbero applicarsi quelle del regolamento XXXX/XXXX relative alle misure di gestione dei rischi relativi alle tecnologie dell'informazione e della comunicazione (TIC), alla gestione degli incidenti connessi alle TIC e, in particolare, alla segnalazione degli incidenti, nonché alle prove di resilienza operativa digitale, agli accordi di condivisione delle informazioni e al rischio di terze parti relativo alle TIC. Gli Stati membri non dovrebbero pertanto applicare le disposizioni della presente direttiva riguardanti gli obblighi di gestione e segnalazione dei rischi di cibersicurezza, la condivisione delle informazioni, la vigilanza e l'esecuzione ai soggetti finanziari contemplati dal regolamento XXXX/XXXX. Al tempo stesso è importante mantenere una solida relazione e lo scambio di informazioni con il settore finanziario a norma della presente direttiva. A tal fine il regolamento XXXX/XXXX consente a tutte le autorità di vigilanza finanziaria, alle autorità europee di vigilanza (AEV) per il settore finanziario e alle autorità nazionali competenti a norma del regolamento XXXX/XXXX di partecipare alle discussioni politiche strategiche e ai lavori tecnici del gruppo di cooperazione, nonché di scambiare informazioni e cooperare con i punti di contatto unici designati a norma della presente direttiva e con i CSIRT nazionali. Le autorità competenti a norma del regolamento XXXX/XXXX dovrebbero trasmettere i dettagli degli incidenti più gravi connessi alle TIC anche ai punti di contatto unici designati a norma della presente direttiva. Gli Stati membri dovrebbero inoltre continuare a includere il settore finanziario nelle loro strategie di cibersicurezza e i CSIRT nazionali possono contemplare il settore finanziario nelle loro attività.

[16] *[inserire il titolo completo e il riferimento della pubblicazione nella GU, non appena noti]*

(14) In considerazione delle interconnessioni tra la cibersicurezza e la sicurezza fisica dei soggetti, dovrebbe essere garantito un approccio coerente tra la direttiva (UE) XXX/XXX del Parlamento europeo e del Consiglio[17] e la presente direttiva. A tal fine, gli Stati membri dovrebbero garantire che i soggetti critici e i soggetti equivalenti a norma della direttiva (UE) XXX/XXX siano considerati soggetti essenziali a norma della presente direttiva. Gli Stati membri dovrebbero inoltre garantire che le loro strategie di cibersicurezza prevedano un quadro strategico per un coordinamento rafforzato tra l'autorità competente a norma della presente direttiva e quella prevista dalla direttiva (UE) XXX/XXX nel contesto della condivisione di informazioni su incidenti e minacce informatiche e dell'esercizio dei compiti di vigilanza. Le autorità a norma di entrambe le direttive dovrebbero cooperare e scambiarsi informazioni, in particolare per quanto riguarda l'individuazione dei soggetti critici, delle minacce informatiche, dei rischi di cibersicurezza, degli incidenti che interessano i soggetti critici, nonché le misure di cibersicurezza adottate dai soggetti critici. Su richiesta delle autorità competenti a norma della direttiva (UE) XXX/XXX, alle autorità competenti a norma della presente direttiva dovrebbe essere consentito di esercitare i propri poteri di vigilanza e di esecuzione nei confronti di un soggetto essenziale individuato come critico. A tal fine entrambe le autorità dovrebbero cooperare e scambiarsi informazioni.

(15) Sostenere e preservare un sistema dei nomi di dominio affidabile, resiliente e sicuro è un fattore chiave per mantenere l'integrità di Internet ed è essenziale per il suo funzionamento costante e stabile, da cui dipendono l'economia e la società digitali. La presente direttiva dovrebbe applicarsi a tutti i fornitori di servizi DNS lungo la catena di risoluzione DNS, compresi gli operatori dei server dei nomi radice (*root name server*), dei server dei nomi di dominio di primo livello (*top level domain*, TLD), dei server autorevoli dei nomi per i nomi di dominio e dei risolutori ricorsivi.

(16) I servizi di cloud computing dovrebbero comprendere i servizi che consentono, su richiesta, un ampio accesso remoto a un *pool* scalabile ed elastico di risorse di calcolo condivisibili e distribuite. Tali risorse di calcolo comprendono risorse quali reti, server o altre infrastrutture, sistemi operativi, software, archiviazione, applicazioni e servizi. I modelli di distribuzione del cloud computing dovrebbero comprendere il cloud privato, di comunità, pubblico e ibrido. I suddetti modelli di servizio e di distribuzione hanno lo stesso significato dei termini di servizio e dei modelli di distribuzione di cui alla norma ISO/IEC 17788:2014. La capacità dell'utente di cloud computing di provvedere unilateralmente all'autofornitura di capacità di calcolo, come il tempo di utilizzo di un server o lo spazio di archiviazione in rete, senza alcuna interazione umana da parte del fornitore di servizi di cloud computing potrebbe essere descritta come "amministrazione su richiesta". L'espressione "ampio accesso remoto" (*broad network access*) è utilizzata per descrivere il fatto che le capacità cloud sono fornite sulla rete e accessibili attraverso meccanismi che promuovono l'uso di piattaforme client eterogenee leggere o pesanti (compresi telefoni cellulari, tablet, computer portatili e workstation). Il termine "scalabile" si riferisce alle risorse di calcolo che sono assegnate in modo flessibile dal fornitore di servizi cloud, indipendentemente dall'ubicazione geografica delle risorse, per gestire le fluttuazioni della domanda. L'espressione "pool elastico" è usata per descrivere quelle risorse di calcolo che sono fornite e rilasciate in base alla domanda, al fine di aumentare e diminuire rapidamente le risorse disponibili in base al carico di lavoro. Il termine "condivisibile" è usato per

[17] *[inserire il titolo completo e gli estremi di pubblicazione della GU, quando noti]*

descrivere le risorse di calcolo che sono fornite a una molteplicità di utenti che condividono un accesso comune al servizio, mentre l'elaborazione è effettuata separatamente per ciascun utente anche se il servizio è fornito a partire dalla stessa apparecchiatura elettronica. Il termine "distribuito" è usato per descrivere quelle risorse di calcolo che si trovano su diversi computer o dispositivi collegati in rete e che comunicano e si coordinano tra di loro mediante il passaggio di messaggi.

(17) Dato l'emergere di tecnologie innovative e di nuovi modelli di business, si prevede che compariranno sul mercato nuovi modelli di servizio e di distribuzione del cloud computing in risposta all'evoluzione delle esigenze dei clienti. In tale contesto, i servizi di cloud computing possono essere forniti in una forma altamente distribuita, anche più vicina al luogo in cui i dati vengono generati o raccolti, passando così dal modello tradizionale a un modello altamente distribuito (edge computing).

(18) È possibile che i servizi offerti dai fornitori di servizi di data center non siano sempre forniti sotto forma di servizi di cloud computing. È pertanto possibile che i data center non facciano sempre parte dell'infrastruttura di cloud computing. Al fine di gestire tutti i rischi posti alla sicurezza dei sistemi informatici e di rete, la presente direttiva dovrebbe applicarsi anche ai fornitori di tali servizi di data center che non sono servizi di cloud computing. Ai fini della presente direttiva, il termine "servizio di data center" dovrebbe applicarsi alla fornitura di un servizio che comprende strutture, o gruppi di strutture, dedicate a ospitare, interconnettere e far funzionare in modo centralizzato apparecchiature informatiche e di rete che forniscono servizi di conservazione, elaborazione e trasporto di dati insieme a tutti gli impianti e le infrastrutture per la distribuzione dell'energia e il controllo ambientale. Il termine "servizio di data center" non si applica ai data center interni e aziendali posseduti e gestiti per fini propri dal soggetto interessato.

(19) I fornitori di servizi postali ai sensi della direttiva 97/67/CE del Parlamento europeo e del Consiglio[18], nonché i fornitori di servizi di corriere e di corriere espresso, dovrebbero essere soggetti alla presente direttiva se provvedono ad almeno una delle fasi della catena di consegna postale, in particolare la raccolta, lo smistamento o la distribuzione, compresi i servizi di ritiro. I servizi di trasporto che non sono forniti nell'ambito di una di tali fasi dovrebbero essere esclusi dall'ambito di applicazione dei servizi postali.

(20) Queste crescenti interdipendenze sono il risultato di una rete di fornitura di servizi sempre più transfrontaliera e interdipendente che utilizza infrastrutture chiave in tutta l'Unione nei settori dell'energia, dei trasporti, delle infrastrutture digitali, delle acque potabili e reflue, della sanità, di determinati aspetti della pubblica amministrazione, nonché dello spazio, per quanto riguarda la fornitura di determinati servizi che dipendono da infrastrutture di terra possedute, gestite e utilizzate dagli Stati membri o da soggetti privati, ad esclusione, pertanto, delle infrastrutture possedute, gestite o utilizzate dall'Unione o per suo conto nell'ambito dei suoi programmi spaziali. Tali interdipendenze implicano che qualsiasi perturbazione, anche se inizialmente limitata a un soggetto o a un settore, possa avere effetti a cascata più ampi, con potenziali ripercussioni negative di ampia portata e di lunga durata sulla fornitura di servizi in

[18] Direttiva 97/67/CE del Parlamento europeo e del Consiglio, del 15 dicembre 1997, concernente regole comuni per lo sviluppo del mercato interno dei servizi postali comunitari e il miglioramento della qualità del servizio (GU L 15 del 21.1.1998, pag. 14).

tutto il mercato interno. La pandemia di COVID-19 ha mostrato la vulnerabilità delle nostre società sempre più interdipendenti di fronte a rischi di bassa probabilità.

(21) In considerazione delle differenze esistenti tra le strutture di governance nazionali e al fine di salvaguardare gli accordi settoriali già esistenti o gli organismi di vigilanza e di regolamentazione dell'Unione, è opportuno che gli Stati membri abbiano la facoltà di designare più di un'autorità nazionale competente responsabile di svolgere i compiti connessi alla sicurezza dei sistemi informatici e di rete dei soggetti essenziali e importanti a norma della presente direttiva. Gli Stati membri dovrebbero avere facoltà di assegnare questo ruolo a un'autorità esistente.

(22) Al fine di agevolare la cooperazione e la comunicazione transfrontaliere tra autorità e permettere che la presente direttiva sia attuata efficacemente, è necessario che ogni Stato membro designi un punto di contatto unico nazionale incaricato di coordinare le questioni relative alla sicurezza dei sistemi informatici e di rete e la cooperazione transfrontaliera a livello dell'Unione.

(23) Le autorità competenti o i CSIRT dovrebbero ricevere le notifiche di incidenti dai soggetti in modo efficace ed efficiente. I punti di contatto unici dovrebbero essere incaricati di trasmettere le notifiche degli incidenti ai punti di contatto unici di altri Stati membri interessati. A livello delle autorità degli Stati membri, per garantire un punto di ingresso unico in ciascuno Stato membro, i punti di contatto unici dovrebbero anche ricevere dalle autorità competenti a norma del regolamento XXXX/XXXX le pertinenti informazioni sugli incidenti riguardanti i soggetti del settore finanziario, che i punti di contatto unici dovrebbero poter trasmettere, a seconda dei casi, alle pertinenti autorità nazionali competenti o ai CSIRT a norma della presente direttiva.

(24) Gli Stati membri dovrebbero essere adeguatamente dotati delle capacità tecniche e organizzative necessarie a prevenire, rilevare e attenuare i rischi e gli incidenti a carico dei sistemi informatici e di rete, nonché a rispondervi. Gli Stati membri dovrebbero pertanto assicurare la disponibilità di CSIRT, anche noti come squadre di pronto intervento informatico ("CERT"), ben funzionanti e rispondenti a determinati requisiti essenziali, al fine di garantire l'esistenza di capacità efficaci e compatibili per far fronte ai rischi e agli incidenti e garantire un'efficiente collaborazione a livello dell'Unione. Al fine di rafforzare il rapporto di fiducia tra i soggetti e i CSIRT, nei casi in cui un CSIRT faccia parte dell'autorità competente, gli Stati membri dovrebbero prendere in considerazione la separazione funzionale tra i compiti operativi svolti dai CSIRT, in particolare per quanto riguarda la condivisione delle informazioni e il sostegno ai soggetti, e le attività di vigilanza delle autorità competenti.

(25) Per quanto riguarda i dati personali, i CSIRT dovrebbero essere in grado di fornire, in conformità al regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio[19] per quanto riguarda i dati personali, per conto e su richiesta di un soggetto a norma della presente direttiva, una scansione proattiva dei sistemi informatici e di rete utilizzati per la fornitura dei suoi servizi. Gli Stati membri dovrebbero mirare a garantire un pari livello di capacità tecniche per tutti i CSIRT settoriali. Gli Stati membri possono chiedere l'assistenza dell'Agenzia dell'Unione europea per la cibersicurezza (ENISA) nello sviluppo di CSIRT nazionali.

[19] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (GU L 119 del 4.5.2016, pag. 1).

(26) Data l'importanza della cooperazione internazionale in materia di cibersicurezza, i CSIRT dovrebbero poter partecipare a reti di cooperazione internazionale, oltre alla rete di CSIRT istituita dalla presente direttiva.

(27) Conformemente all'allegato della raccomandazione (UE) 2017/1584 della Commissione relativa alla risposta coordinata agli incidenti e alle crisi di cibersicurezza su vasta scala ("programma")[20], per incidente su vasta scala si dovrebbe intendere un incidente che ha un impatto significativo su almeno due Stati membri o che causa perturbazioni che superano la capacità di risposta di uno Stato membro. A seconda della loro causa e del loro impatto, gli incidenti su vasta scala possono aggravarsi e trasformarsi in vere e proprie crisi che non consentono il corretto funzionamento del mercato interno. Data l'ampia portata e, nella maggior parte dei casi, la natura transfrontaliera di tali incidenti, gli Stati membri e le istituzioni, gli organismi e le agenzie pertinenti dell'Unione dovrebbero cooperare a livello tecnico, operativo e politico per coordinare adeguatamente la risposta in tutta l'Unione.

(28) Poiché lo sfruttamento delle vulnerabilità nei sistemi informatici e di rete può causare perturbazioni e danni significativi, la rapida individuazione e correzione di tali vulnerabilità è un fattore importante per la riduzione dei rischi di cibersicurezza. I soggetti che sviluppano tali sistemi dovrebbero pertanto stabilire procedure adeguate per gestire le vulnerabilità nel momento in cui vengono scoperte. Poiché le vulnerabilità sono spesso rilevate e segnalate (divulgate) da terzi (soggetti segnalanti), il fabbricante o fornitore di prodotti o servizi TIC dovrebbe anche mettere in atto le procedure necessarie per ricevere informazioni sulla vulnerabilità da terzi. A tale riguardo, le norme internazionali ISO/IEC 30111 e ISO/IEC 29417 forniscono rispettivamente orientamenti sulla gestione delle vulnerabilità e sulla divulgazione delle vulnerabilità. Per quanto riguarda la divulgazione delle vulnerabilità, è particolarmente importante il coordinamento tra i soggetti segnalanti e i fabbricanti o fornitori di prodotti o servizi TIC. La divulgazione coordinata delle vulnerabilità consiste in un processo strutturato attraverso il quale le vulnerabilità sono segnalate alle organizzazioni in modo tale da consentire a queste ultime di diagnosticarle ed eliminarle prima che informazioni dettagliate in merito siano divulgate a terzi o al pubblico. La divulgazione coordinata delle vulnerabilità dovrebbe comprendere anche il coordinamento tra il soggetto segnalante e l'organizzazione per quanto riguarda i tempi per la risoluzione e la pubblicazione delle vulnerabilità.

(29) Gli Stati membri dovrebbero pertanto adottare misure volte a facilitare la divulgazione coordinata delle vulnerabilità stabilendo una politica nazionale pertinente. A tale riguardo, gli Stati membri dovrebbero designare un CSIRT che assuma il ruolo di "coordinatore", fungendo da intermediario tra i soggetti segnalanti e i fabbricanti o fornitori di prodotti o servizi TIC ove necessario. I compiti del CSIRT coordinatore dovrebbero comprendere in particolare l'individuazione e il contatto dei soggetti interessati, il sostegno ai soggetti segnalanti, la negoziazione dei tempi di divulgazione e la gestione delle vulnerabilità che interessano più organizzazioni (divulgazione multilaterale di vulnerabilità). Qualora le vulnerabilità interessino più fabbricanti o fornitori di prodotti o servizi TIC stabiliti in più di uno Stato membro, i CSIRT designati di ciascuno degli Stati membri interessati dovrebbero cooperare nell'ambito della rete di CSIRT.

[20] 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).

(30) L'accesso a informazioni corrette e tempestive sulle vulnerabilità che interessano i prodotti e i servizi TIC contribuisce a una migliore gestione dei rischi di cibersicurezza. A tale riguardo le fonti di informazioni pubblicamente disponibili sulle vulnerabilità sono uno strumento importante per i soggetti e i loro utenti, ma anche per le autorità nazionali competenti e i CSIRT. Per questo motivo l'ENISA dovrebbe istituire un registro delle vulnerabilità in cui i soggetti essenziali e importanti e i loro fornitori, nonché i soggetti che non rientrano nell'ambito di applicazione della presente direttiva, possano, su base volontaria, divulgare le vulnerabilità e fornire informazioni su di esse che consentano agli utenti di adottare adeguate misure di attenuazione.

(31) Sebbene simili registri o banche dati delle vulnerabilità esistano già, questi sono ospitati e mantenuti da soggetti non stabiliti nell'Unione. Un registro europeo delle vulnerabilità mantenuto dall'ENISA garantirebbe una maggiore trasparenza, per quanto riguarda la procedura di pubblicazione prima della divulgazione ufficiale della vulnerabilità, e resilienza in caso di perturbazioni o interruzioni nella fornitura di servizi analoghi. Per evitare la duplicazione degli sforzi e perseguire, nella misura del possibile, la complementarità, l'ENISA dovrebbe valutare la possibilità di concludere accordi di cooperazione strutturata con registri simili nelle giurisdizioni di paesi terzi.

(32) Il gruppo di cooperazione dovrebbe stabilire ogni due anni un programma di lavoro comprendente le azioni che il gruppo deve intraprendere per attuare i suoi obiettivi e compiti. Il calendario del primo programma adottato a norma della presente direttiva dovrebbe essere allineato a quello dell'ultimo programma adottato a norma della direttiva (UE) 2016/1148, al fine di evitare eventuali perturbazioni nel lavoro del gruppo.

(33) Nell'elaborare i documenti di orientamento, il gruppo di cooperazione dovrebbe sistematicamente: mappare le soluzioni e le esperienze nazionali, valutare l'impatto dei risultati del gruppo di cooperazione per quanto riguarda gli approcci nazionali, discutere le sfide in materia di attuazione e formulare raccomandazioni specifiche da realizzare attraverso una migliore attuazione delle norme esistenti.

(34) Il gruppo di cooperazione dovrebbe rimanere un forum flessibile ed essere in grado di reagire alle nuove e mutevoli priorità strategiche e alle sfide, tenendo conto nel contempo della disponibilità di risorse. Esso dovrebbe organizzare riunioni congiunte periodiche con i pertinenti portatori di interessi del settore privato di tutta l'Unione per discutere le attività svolte dal gruppo e raccogliere contributi sulle sfide strategiche emergenti. Al fine di rafforzare la cooperazione a livello dell'Unione, il gruppo dovrebbe prendere in considerazione la possibilità di invitare a partecipare ai suoi lavori organismi e agenzie dell'Unione coinvolti nella politica in materia di cibersicurezza, quali il Centro europeo per la lotta alla criminalità informatica (EC3), l'Agenzia dell'Unione europea per la sicurezza aerea (AESA) e l'Agenzia dell'Unione europea per il programma spaziale (EUSPA).

(35) Le autorità competenti e i CSIRT dovrebbero avere la facoltà di partecipare a programmi di scambio per funzionari di altri Stati membri al fine di migliorare la cooperazione. Le autorità competenti dovrebbero adottare le misure necessarie per consentire a funzionari di altri Stati membri di svolgere un ruolo efficace nelle attività dell'autorità competente ospitante.

(36) Ove opportuno l'Unione dovrebbe concludere accordi internazionali, in conformità all'articolo 218 TFUE, con paesi terzi o organizzazioni internazionali, che consentano e organizzino la loro partecipazione ad alcune delle attività del gruppo di cooperazione

e della rete di CSIRT. Tali accordi dovrebbero garantire un'adeguata protezione dei dati.

(37) Gli Stati membri dovrebbero contribuire all'istituzione del quadro di risposta alle crisi di cibersicurezza dell'UE, di cui alla raccomandazione (UE) 2017/1584, attraverso le reti di cooperazione esistenti, in particolare la rete europea delle organizzazioni di collegamento per le crisi informatiche (EU-CyCLONe), la rete di CSIRT e il gruppo di cooperazione. EU-CyCLONe e la rete di CSIRT dovrebbero cooperare sulla base di disposizioni procedurali che definiscano le modalità di tale cooperazione. Il regolamento interno di EU-CyCLONe dovrebbe specificare ulteriormente le modalità di funzionamento della rete, compresi, ma non solo, i ruoli, le modalità di cooperazione, le interazioni con altri attori pertinenti e i modelli per la condivisione delle informazioni, nonché i mezzi di comunicazione. Per la gestione delle crisi a livello dell'Unione, le parti pertinenti dovrebbero affidarsi alle disposizioni dei dispositivi integrati per la risposta politica alle crisi (IPCR). A tal fine la Commissione dovrebbe far ricorso al processo di coordinamento intersettoriale delle crisi ad alto livello del sistema ARGUS. Se la crisi implica un'importante dimensione esterna o una forte correlazione con la politica di sicurezza e di difesa comune (PSDC) dovrebbe essere attivato il meccanismo di risposta alle crisi del servizio europeo per l'azione esterna (SEAE).

(38) Ai fini della presente direttiva, il termine "rischio" dovrebbe riferirsi alla potenziale perdita o perturbazione causata da un incidente di cibersicurezza e dovrebbe essere espresso come combinazione dell'entità di tale perdita o perturbazione e della probabilità che si verifichi tale incidente.

(39) Ai fini della presente direttiva, l'espressione "quasi incidente" (*near miss*) dovrebbe riferirsi a un evento che avrebbe potenzialmente potuto causare un danno, ma che è stato efficacemente evitato prima che si verificasse.

(40) Le misure di gestione dei rischi dovrebbero comprendere misure per individuare eventuali rischi di incidenti, per prevenire, rilevare e gestire incidenti, nonché per attenuarne l'impatto. La sicurezza dei sistemi informatici e di rete dovrebbe comprendere la sicurezza dei dati conservati, trasmessi e elaborati.

(41) Per evitare di imporre un onere finanziario e amministrativo sproporzionato ai soggetti essenziali e importanti, gli obblighi di gestione dei rischi di cibersicurezza dovrebbero essere proporzionati al rischio corso dal sistema informatico e di rete interessato, tenendo conto dello stato dell'arte di tali misure.

(42) I soggetti essenziali e importanti dovrebbero garantire la sicurezza dei sistemi informatici e di rete che utilizzano nelle loro attività. Si tratta in particolare di sistemi informatici e di rete privati gestiti dal loro personale informatico interno oppure la cui sicurezza sia stata esternalizzata. Gli obblighi di gestione e segnalazione dei rischi di cibersicurezza a norma della presente direttiva dovrebbero applicarsi ai pertinenti soggetti essenziali e importanti indipendentemente dal fatto che questi effettuino internamente la manutenzione dei loro sistemi informatici e di rete o che la esternalizzino.

(43) Affrontare i rischi di cibersicurezza derivanti dalla catena di approvvigionamento di un soggetto e dalla sua relazione con i fornitori è particolarmente importante data la prevalenza di incidenti in cui i soggetti sono rimasti vittime di attacchi informatici e in cui i responsabili di atti malevoli sono stati in grado di compromettere la sicurezza dei sistemi informatici e di rete di un soggetto sfruttando le vulnerabilità che interessano

prodotti e servizi di terzi. I soggetti dovrebbero pertanto valutare e tenere in considerazione la qualità complessiva dei prodotti e delle pratiche di cibersicurezza dei loro fornitori e fornitori di servizi, comprese le loro procedure di sviluppo sicuro.

(44) Tra i fornitori di servizi, i fornitori di servizi di sicurezza gestiti (*managed security services providers*, MSSP) in settori quali la risposta agli incidenti, i test di penetrazione, gli audit di sicurezza e la consulenza svolgono un ruolo particolarmente importante nell'assistere i soggetti nei loro sforzi per il rilevamento degli incidenti e la risposta agli stessi. Tali MSSP sono stati tuttavia essi stessi bersaglio di attacchi informatici e, a causa della loro stretta integrazione nelle attività degli operatori, presentano un particolare rischio di cibersicurezza. I soggetti dovrebbero pertanto esercitare una maggiore diligenza nella selezione di un MSSP.

(45) I soggetti dovrebbero inoltre affrontare i rischi di cibersicurezza derivanti dalle loro interazioni e relazioni con altri portatori di interessi nell'ambito di un ecosistema più ampio. In particolare, i soggetti dovrebbero adottare misure adeguate per garantire che la loro cooperazione con gli istituti accademici e di ricerca avvenga in linea con le loro politiche in materia di cibersicurezza e segua le buone pratiche per quanto riguarda l'accesso sicuro e la diffusione delle informazioni in generale e la tutela della proprietà intellettuale in particolare. Analogamente, data l'importanza e il valore dei dati per le attività dei soggetti, questi ultimi dovrebbero adottare tutte le opportune misure di cibersicurezza quando si affidano ai servizi di trasformazione e analisi dei dati forniti da terzi.

(46) Per affrontare ulteriormente i principali rischi relativi alla catena di approvvigionamento e aiutare i soggetti che operano nei settori disciplinati dalla presente direttiva a gestire adeguatamente i rischi di cibersicurezza connessi alla catena di approvvigionamento e ai fornitori, il gruppo di cooperazione, coinvolgendo le autorità nazionali competenti, in cooperazione con la Commissione e l'ENISA, dovrebbe effettuare valutazioni settoriali e coordinate dei rischi relativi alla catena di approvvigionamento, come già fatto per le reti 5G in seguito alla raccomandazione (UE) 2019/534 sulla cibersicurezza delle reti 5G[21], al fine di individuare, per settore, quali sono i servizi, i sistemi o i prodotti TIC critici e le minacce e le vulnerabilità pertinenti.

(47) Le valutazioni dei rischi relativi alla catena di approvvigionamento, alla luce delle caratteristiche del settore interessato, dovrebbero tenere conto dei fattori tecnici e, se opportuno, non tecnici, compresi quelli definiti nella raccomandazione (UE) 2019/534, nella valutazione dei rischi coordinata a livello dell'UE della sicurezza delle reti 5G e nel pacchetto di strumenti dell'UE sulla cibersicurezza del 5G concordato dal gruppo di cooperazione. Per individuare le catene di approvvigionamento che dovrebbero essere soggette a una valutazione coordinata dei rischi, dovrebbero essere presi in considerazione i seguenti criteri: i) la misura in cui i soggetti essenziali e importanti ricorrono e si affidano a specifici servizi, sistemi o prodotti TIC critici; ii) la pertinenza di specifici servizi, sistemi o prodotti TIC critici per lo svolgimento di funzioni critiche o sensibili, compreso il trattamento dei dati personali; iii) la disponibilità di servizi, sistemi o prodotti TIC alternativi; iv) la resilienza dell'intera catena di approvvigionamento di servizi, sistemi o prodotti TIC contro eventi

[21] Raccomandazione (UE) 2019/534 della Commissione, del 26 marzo 2019, Cibersicurezza delle reti 5G (GU L 88 del 29.3.2019, pag. 42).

perturbatori e v) per i servizi, sistemi o prodotti TIC emergenti, la loro potenziale importanza futura per le attività dei soggetti.

(48) Al fine di semplificare gli obblighi giuridici imposti ai fornitori di reti pubbliche di comunicazione elettronica o di servizi di comunicazione elettronica accessibili al pubblico e ai prestatori di servizi fiduciari relativi alla sicurezza dei loro sistemi informatici e di rete, nonché di consentire a tali soggetti e alle rispettive autorità competenti di beneficiare del quadro giuridico istituito dalla presente direttiva (compresa la designazione del CSIRT responsabile della gestione dei rischi e degli incidenti e la partecipazione delle autorità e degli organismi competenti ai lavori del gruppo di cooperazione e della rete di CSIRT), essi dovrebbero essere inclusi nell'ambito di applicazione della presente direttiva. Le corrispondenti disposizioni stabilite nel regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio[22] e nella direttiva (UE) 2018/1972 del Parlamento europeo e del Consiglio[23] relative all'imposizione di obblighi di sicurezza e notifica a questi tipi di soggetti dovrebbero pertanto essere abrogate. Le norme relative agli obblighi di segnalazione dovrebbero lasciare impregiudicati il regolamento (UE) 2016/679 e la direttiva 2002/58/CE del Parlamento europeo e del Consiglio[24].

(49) Se opportuno e per evitare inutili perturbazioni, gli orientamenti nazionali esistenti e la legislazione nazionale adottata per il recepimento delle norme relative alle misure di sicurezza di cui all'articolo 40, paragrafo 1, della direttiva (UE) 2018/1972, nonché dei requisiti di cui all'articolo 40, paragrafo 2, di tale direttiva per quanto riguarda i parametri relativi alla rilevanza di un incidente, dovrebbero continuare a essere utilizzati dalle autorità competenti incaricate della vigilanza e dell'esecuzione ai fini della presente direttiva.

(50) Vista la crescente importanza dei servizi di comunicazione interpersonale indipendenti dal numero, è necessario assicurare che anche tali servizi siano soggetti ad adeguati requisiti di sicurezza in considerazione della loro specificità e della loro rilevanza economica. I fornitori di tali servizi dovrebbero pertanto garantire un livello di sicurezza dei sistemi informatici e di rete adeguato al rischio esistente. Dato che i fornitori di servizi di comunicazione interpersonale indipendenti dal numero solitamente non esercitano un controllo effettivo sulla trasmissione dei segnali sulle reti, il grado di rischio di tali servizi può essere considerato, per certi aspetti, inferiore a quello dei servizi di comunicazione elettronica tradizionali. Lo stesso vale per i servizi di comunicazione interpersonale che utilizzano numeri e che non esercitano un controllo effettivo sulla trasmissione dei segnali.

(51) Il mercato interno dipende più che mai dal funzionamento di Internet. I servizi di quasi tutti i soggetti essenziali e importanti dipendono dai servizi forniti via Internet. Al fine di garantire l'erogazione senza intoppi dei servizi forniti dai soggetti essenziali e importanti, è fondamentale che le reti pubbliche di comunicazione elettronica, quali ad

---

22 Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE (GU L 257 del 28.8.2014, pag. 73).

23 Direttiva (UE) 2018/1972 del Parlamento europeo e del Consiglio, dell'11 dicembre 2018, che istituisce il codice europeo delle comunicazioni elettroniche (GU L 321 del 17.12.2018, pag. 36).

24 Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche) (GU L 201 del 31.7.2002, pag. 37).

esempio le dorsali Internet o i cavi di comunicazione sottomarini, dispongano di adeguate misure di cibersicurezza e segnalino gli incidenti connessi.

(52) Ove opportuno, i soggetti dovrebbero informare i destinatari dei loro servizi di minacce particolari e significative e delle misure che possono adottare per attenuare i rischi che ne derivano. L'obbligo di informare tali destinatari in merito alle minacce non dovrebbe esonerare i soggetti dall'obbligo di adottare, a proprie spese, provvedimenti adeguati e immediati per prevenire eventuali minacce informatiche o porvi rimedio e ristabilire il normale livello di sicurezza del servizio. La fornitura ai destinatari di tali informazioni riguardanti le minacce alla sicurezza dovrebbe essere gratuita.

(53) In particolare, i fornitori di reti pubbliche di comunicazione elettronica o di servizi di comunicazione elettronica accessibili al pubblico dovrebbero informare i destinatari dei servizi di minacce informatiche particolari e significative e delle misure che questi ultimi possono adottare per proteggere la sicurezza delle loro comunicazioni, ad esempio attraverso l'uso di particolari tipi di programmi o tecnologie di cifratura.

(54) Al fine di salvaguardare la sicurezza delle reti e dei servizi di comunicazione elettronica, l'uso della cifratura, in particolare la cifratura end-to-end, dovrebbe essere promosso e, ove necessario, dovrebbe essere reso obbligatorio per i fornitori di tali servizi e reti conformemente ai principi di sicurezza e tutela della vita privata per impostazione predefinita e fin dalla progettazione ai fini dell'articolo 18. L'uso della cifratura end-to-end dovrebbe essere conciliato con i poteri degli Stati membri di garantire la tutela della sicurezza pubblica e dei loro interessi essenziali in materia di sicurezza, nonché di consentire l'indagine, l'accertamento e il perseguimento di reati nel rispetto del diritto dell'Unione. Le soluzioni per l'accesso legittimo alle informazioni nelle comunicazioni che utilizzano la cifratura end-to-end dovrebbero mantenere l'efficacia della cifratura nella protezione della privacy e della sicurezza delle comunicazioni, fornendo nel contempo una risposta efficace alla criminalità.

(55) La presente direttiva stabilisce un approccio in due fasi alla segnalazione degli incidenti al fine di trovare il giusto equilibrio tra, da un lato, una segnalazione rapida che contribuisca ad attenuare la potenziale diffusione di incidenti e consenta ai soggetti di chiedere sostegno e, dall'altro, una segnalazione approfondita che tragga insegnamenti preziosi dai singoli incidenti e migliori nel tempo la resilienza alle minacce informatiche delle singole imprese e di interi settori. Qualora vengano a conoscenza di un incidente, i soggetti dovrebbero essere tenuti a presentare una notifica iniziale entro 24 ore, seguita da una relazione finale entro un mese. La notifica iniziale dovrebbe contenere solo le informazioni strettamente necessarie per informare le autorità competenti dell'incidente e consentire al soggetto di chiedere assistenza, se necessario. Tale notifica, ove applicabile, dovrebbe indicare se l'incidente sia presumibilmente il risultato di un'azione illegittima o malevola. Gli Stati membri dovrebbero garantire che l'obbligo di presentare tale notifica iniziale non sottragga le risorse del soggetto segnalante alle attività relative alla gestione degli incidenti, che dovrebbero essere considerate prioritarie. Per evitare ulteriormente che gli obblighi di segnalazione degli incidenti sottraggano risorse alla gestione della risposta agli incidenti o possano altrimenti compromettere gli sforzi dei soggetti a tale riguardo, gli Stati membri dovrebbero altresì prevedere che, in casi debitamente giustificati e d'intesa con le autorità competenti o con il CSIRT, il soggetto interessato possa derogare dai termini di 24 ore per la notifica iniziale e di un mese per la relazione finale.

(56) I soggetti essenziali e importanti si trovano spesso in una situazione in cui un particolare incidente, a causa delle sue caratteristiche, deve essere segnalato a varie autorità in conseguenza degli obblighi di notifica previsti da vari strumenti giuridici. Tali casi creano ulteriori oneri e possono anche generare incertezze in merito al formato e alle procedure di tali notifiche. In considerazione di ciò e al fine di semplificare la segnalazione degli incidenti di sicurezza, gli Stati membri dovrebbero istituire *un punto di ingresso unico* per tutte le notifiche richieste a norma della presente direttiva e anche a norma di altri atti dell'Unione quali il regolamento (UE) 2016/679 e la direttiva 2002/58/CE. L'ENISA, in collaborazione con il gruppo di cooperazione, dovrebbe elaborare modelli comuni di notifica mediante orientamenti che semplifichino e razionalizzino le informazioni di segnalazione richieste dal diritto dell'Unione e riducano gli oneri per le imprese.

(57) Se si sospetta che un incidente sia connesso ad attività criminali gravi a norma del diritto dell'Unione o nazionale, gli Stati membri dovrebbero incoraggiare i soggetti essenziali e importanti, in base alle norme applicabili ai procedimenti penali in conformità al diritto dell'Unione, a segnalare alle autorità di contrasto pertinenti gli incidenti di cui si sospetta la natura criminale grave. Ove opportuno, e fatte salve le norme in materia di protezione dei dati personali applicabili a Europol, è auspicabile che l'EC3 e l'ENISA agevolino il coordinamento tra le autorità competenti e le autorità di contrasto dei diversi Stati membri.

(58) In molti casi gli incidenti compromettono i dati personali. In tale contesto, le autorità competenti dovrebbero cooperare e scambiarsi informazioni su tutte le questioni pertinenti con le autorità di protezione dei dati e con le autorità di vigilanza a norma della direttiva 2002/58/CE.

(59) Il mantenimento di banche dati precise e complete dei nomi di dominio e dei dati di registrazione (i cosiddetti "dati WHOIS") e la fornitura di un accesso legittimo a tali dati sono essenziali per garantire la sicurezza, la stabilità e la resilienza del DNS, che a sua volta contribuisce a un elevato livello comune di cibersicurezza all'interno dell'Unione. Se l'elaborazione dei dati comprende il trattamento dei dati personali, quest'ultimo deve essere conforme al diritto dell'Unione in materia di protezione dei dati.

(60) La disponibilità e la tempestiva accessibilità di tali dati per le autorità pubbliche, comprese le autorità competenti a norma del diritto dell'Unione o nazionale in materia di prevenzione, indagine o perseguimento di reati, ai CERT, ai CSIRT e, per quanto riguarda i dati dei loro clienti, ai fornitori di reti e servizi di comunicazione elettronica e ai fornitori di tecnologie e servizi di cibersicurezza che agiscono per conto di tali clienti, sono essenziali per prevenire e combattere l'abuso del sistema dei nomi di dominio, in particolare per la prevenzione e il rilevamento degli incidenti di cibersicurezza e la risposta agli stessi. Tale accesso dovrebbe essere conforme al diritto dell'Unione in materia di protezione dei dati nella misura in cui è relativo ai dati personali.

(61) Al fine di garantire la disponibilità di dati di registrazione dei nomi di dominio accurati e completi, i registri dei TLD e i soggetti che forniscono servizi di registrazione dei nomi di dominio per i TLD (i cosiddetti registrar) dovrebbero raccogliere i dati di registrazione dei nomi di dominio e garantirne l'integrità e la disponibilità. In particolare, i registri dei TLD e i soggetti che forniscono servizi di registrazione dei nomi di dominio per i TLD dovrebbero stabilire politiche e procedure per raccogliere e mantenere i dati di registrazione accurati e completi, nonché per

prevenire e rettificare dati di registrazione inesatti in conformità alle norme dell'Unione in materia di protezione dei dati.

(62) I registri dei TLD e i soggetti che forniscono loro servizi di registrazione dei nomi di dominio dovrebbero rendere pubblicamente disponibili i dati di registrazione dei nomi di dominio che non rientrano nell'ambito di applicazione delle norme dell'Unione in materia di protezione dei dati, come i dati riguardanti le persone giuridiche[25]. I registri dei TLD e i soggetti che forniscono servizi di registrazione dei nomi di dominio per i TLD dovrebbero inoltre consentire l'accesso legittimo a specifici dati di registrazione dei nomi di dominio riguardanti le persone fisiche ai legittimi richiedenti l'accesso, in conformità al diritto dell'Unione in materia di protezione dei dati. Gli Stati membri dovrebbero garantire che i registri dei TLD e i soggetti che forniscono loro servizi di registrazione dei nomi di dominio rispondano senza indebito ritardo alle richieste di divulgazione dei dati di registrazione dei nomi di dominio presentate dai legittimi richiedenti l'accesso. I registri dei TLD e i soggetti che forniscono loro servizi di registrazione dei nomi di dominio dovrebbero stabilire politiche e procedure per la pubblicazione e la divulgazione dei dati di registrazione, compresi gli accordi sul livello dei servizi, ai fini del trattamento delle richieste di accesso dei legittimi richiedenti l'accesso. La procedura di accesso può comprendere anche l'uso di un'interfaccia, di un portale o di un altro strumento tecnico per fornire un sistema efficiente per la richiesta dei dati di registrazione e l'accesso agli stessi. Al fine di promuovere pratiche armonizzate in tutto il mercato interno, la Commissione può adottare orientamenti su tali procedure, fatte salve le competenze del comitato europeo per la protezione dei dati.

(63) Tutti i soggetti essenziali e importanti a norma della presente direttiva dovrebbero rientrare nella giurisdizione dello Stato membro in cui forniscono i loro servizi. Se fornisce servizi in più di uno Stato membro, il soggetto dovrebbe rientrare nella giurisdizione separata e concorrente di ciascuno di tali Stati membri. Le autorità competenti di tali Stati membri dovrebbero cooperare, prestarsi assistenza reciproca e, ove opportuno, condurre azioni comuni di vigilanza.

(64) Per tener conto della natura transfrontaliera dei servizi e delle attività dei fornitori di servizi DNS, dei registri dei nomi di dominio di primo livello, dei fornitori di reti di distribuzione dei contenuti, dei fornitori di servizi di cloud computing, dei fornitori di servizi di data center e dei fornitori di servizi digitali, tali soggetti dovrebbero essere posti sotto la giurisdizione di un solo Stato membro. La giurisdizione dovrebbe essere attribuita allo Stato membro in cui il rispettivo soggetto ha lo stabilimento principale nell'Unione. Il criterio dello stabilimento ai fini della presente direttiva implica l'esercizio effettivo dell'attività nel quadro di un'organizzazione stabile. A tale riguardo non è determinante la forma giuridica assunta, sia essa una succursale o una filiale dotata di personalità giuridica. Il rispetto di tale criterio non dovrebbe dipendere dal fatto che i sistemi informatici e di rete siano situati fisicamente in un determinato luogo; la presenza e l'utilizzo dei sistemi in questione non costituiscono di per sé lo stabilimento principale e non sono pertanto criteri decisivi per la sua determinazione. Lo stabilimento principale dovrebbe essere il luogo in cui sono adottate nell'Unione le decisioni relative alle misure di gestione dei rischi di cibersicurezza. Ciò corrisponderà

[25] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, considerando 14: "Il presente regolamento non disciplina il trattamento dei dati personali relativi a persone giuridiche, in particolare imprese dotate di personalità giuridica, compresi il nome e la forma della persona giuridica e i suoi dati di contatto."

di norma alla sede dell'amministrazione centrale delle società nell'Unione. Se tali decisioni non sono adottate nell'Unione, si dovrebbe considerare che lo stabilimento principale sia nello Stato membro in cui il soggetto ha lo stabilimento con il maggior numero di dipendenti nell'Unione. Qualora i servizi siano forniti da un gruppo di imprese, si dovrebbe considerare lo stabilimento principale dell'impresa controllante come lo stabilimento principale del gruppo di imprese.

(65) Qualora un fornitore di servizi DNS, un registro dei nomi di dominio di primo livello, un fornitore di reti di distribuzione dei contenuti, un fornitore di servizi di cloud computing, un fornitore di servizi di data center e un fornitore di servizi digitali non stabilito nell'Unione offra servizi all'interno dell'Unione, esso dovrebbe designare un rappresentante. Per determinare se tale soggetto stia offrendo servizi nell'Unione, è opportuno verificare se risulta che il soggetto stia progettando di fornire servizi a persone in uno o più Stati membri. La semplice accessibilità nell'Unione del sito web del soggetto o di un intermediario, o di un indirizzo di posta elettronica e di altri dati di contatto, o l'impiego di una lingua abitualmente utilizzata nel paese terzo in cui il soggetto è stabilito, è di per sé insufficiente per accertare tale intenzione. Tuttavia fattori quali l'utilizzo di una lingua o di una moneta abitualmente utilizzata in uno o più Stati membri, con la possibilità di ordinare servizi in tale altra lingua, o la menzione di clienti o utenti che si trovano nell'Unione, possono evidenziare che il soggetto sta progettando di offrire servizi all'interno dell'Unione. Il rappresentante dovrebbe agire a nome del soggetto e le autorità competenti o i CSIRT dovrebbero poterlo contattare. Il rappresentante dovrebbe essere esplicitamente designato mediante mandato scritto del soggetto affinché agisca a suo nome con riguardo agli obblighi che a quest'ultimo derivano dalla presente direttiva, compresa la segnalazione di incidenti.

(66) Qualora informazioni considerate classificate in conformità al diritto nazionale o dell'Unione siano scambiate, comunicate o altrimenti condivise a norma delle disposizioni della presente direttiva, dovrebbero essere applicate le corrispondenti norme specifiche sulla gestione delle informazioni classificate.

(67) Di fronte a minacce informatiche che si fanno sempre più complesse e sofisticate, la validità delle misure di rilevamento e prevenzione dipende in larga misura da una costante condivisione tra i soggetti di informazioni di intelligence relative alle minacce e alle vulnerabilità. La condivisione delle informazioni contribuisce a una maggiore consapevolezza delle minacce informatiche che, a sua volta, accresce la capacità dei soggetti di impedire che le minacce si trasformino in incidenti concreti e consente ai soggetti di arginare in maniera più efficace gli effetti degli incidenti e di riprendersi in modo più efficiente. In assenza di orientamenti a livello dell'Unione, numerosi fattori, tra cui in particolare l'incertezza sulla compatibilità con le norme in materia di concorrenza e responsabilità, sembrano aver ostacolato tale condivisione delle informazioni di intelligence.

(68) È quindi opportuno incoraggiare i soggetti a sfruttare collettivamente, sul piano strategico, tattico e operativo, le conoscenze e le esperienze pratiche che hanno acquisito a livello individuale al fine di accrescere le loro capacità di valutare e monitorare adeguatamente le minacce informatiche, difendersi da esse e rispondervi. È pertanto necessario consentire la creazione a livello dell'Unione di meccanismi per accordi volontari di condivisione delle informazioni. A tal fine gli Stati membri dovrebbero sostenere e incoraggiare attivamente anche i soggetti pertinenti che non rientrano nell'ambito di applicazione della presente direttiva a partecipare a tali meccanismi di condivisione delle informazioni. Tali meccanismi dovrebbero essere

attuati nel pieno rispetto delle norme dell'Unione in materia di concorrenza e di protezione dei dati.

(69) Il trattamento dei dati personali, nella misura strettamente necessaria e proporzionata al fine di garantire la sicurezza dei sistemi informatici e di rete da parte di soggetti, autorità pubbliche, CERT, CSIRT e fornitori di tecnologie e servizi di sicurezza, dovrebbe costituire un interesse legittimo del titolare del trattamento in questione di cui al regolamento (UE) 2016/679. Ciò dovrebbe includere misure relative alla prevenzione, al rilevamento e all'analisi degli incidenti e alla risposta agli stessi, misure di sensibilizzazione in relazione a specifiche minacce informatiche, lo scambio di informazioni nel contesto della risoluzione e della divulgazione coordinata delle vulnerabilità, nonché lo scambio volontario di informazioni su tali incidenti, 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. Tali misure possono richiedere il trattamento dei seguenti tipi di dati personali: indirizzi IP, localizzatori uniformi di risorse (URL), nomi di dominio e indirizzi di posta elettronica.

(70) Al fine di rafforzare i poteri e le azioni di vigilanza che contribuiscono a garantire l'effettiva conformità, la presente direttiva dovrebbe prevedere un elenco minimo di azioni e mezzi di vigilanza attraverso i quali le autorità competenti possono vigilare sui soggetti essenziali e importanti. La presente direttiva dovrebbe inoltre stabilire una differenziazione del regime di vigilanza tra i soggetti essenziali e i soggetti importanti al fine di garantire un giusto equilibrio degli obblighi sia per i soggetti che per le autorità competenti. Pertanto i soggetti essenziali dovrebbero essere sottoposti a un regime di vigilanza completo (ex ante ed ex post), mentre i soggetti importanti dovrebbero essere sottoposti a un regime di vigilanza leggero, solo ex post. In base a quest'ultimo i soggetti importanti non dovrebbero documentare sistematicamente il rispetto degli obblighi di gestione dei rischi di cibersicurezza, mentre le autorità competenti dovrebbero attuare un approccio ex post reattivo alla vigilanza e, di conseguenza, non dovrebbero avere un obbligo generale di vigilanza su tali soggetti.

(71) Al fine di rendere efficace l'esecuzione, è opportuno stabilire un elenco minimo di sanzioni amministrative in caso di violazione degli obblighi di gestione e segnalazione dei rischi di cibersicurezza previsti dalla presente direttiva, istituendo un quadro chiaro e coerente per tali sanzioni in tutta l'Unione. Occorre tenere debitamente conto della natura, della gravità e della durata dell'infrazione, del danno effettivamente causato o delle perdite effettivamente subite o del danno o delle perdite potenziali che si sarebbero potuti verificare, del carattere doloso o colposo della violazione, delle azioni intraprese per prevenire o attenuare il danno effettuato e/o le perdite subite, del grado di responsabilità o di eventuali violazioni precedenti pertinenti, del grado di cooperazione con l'autorità competente e di qualsiasi altro fattore aggravante o attenuante. L'imposizione di sanzioni, comprese sanzioni amministrative pecuniarie, dovrebbe essere soggetta a garanzie procedurali appropriate in conformità ai principi generali del diritto dell'Unione e della Carta dei diritti fondamentali dell'Unione europea, inclusi l'effettiva tutela giurisdizionale e il giusto processo.

(72) Al fine di garantire l'efficace applicazione degli obblighi stabiliti nella presente direttiva, ciascuna autorità competente dovrebbe avere il potere di imporre o chiedere l'imposizione di sanzioni amministrative pecuniarie.

(73) Qualora le sanzioni amministrative pecuniarie siano imposte a imprese, queste ultime dovrebbero essere intese quali imprese conformemente agli articoli 101 e 102 TFUE a

tali fini. Qualora le sanzioni amministrative pecuniarie siano imposte a persone che non sono imprese, l'autorità di vigilanza dovrebbe tenere conto del livello generale di reddito nello Stato membro come pure della situazione economica della persona nel valutare l'importo appropriato della sanzione pecuniaria. Dovrebbe spettare agli Stati membri determinare se e in che misura le autorità pubbliche debbano essere soggette a sanzioni amministrative pecuniarie. L'imposizione di una sanzione amministrativa pecuniaria non pregiudica l'applicazione di altri poteri da parte delle autorità competenti o di altre sanzioni previste dalle norme nazionali di recepimento della presente direttiva.

(74) Gli Stati membri dovrebbero poter stabilire le norme relative alle sanzioni penali in caso di violazione delle norme nazionali di recepimento della presente direttiva. Tuttavia l'imposizione di sanzioni penali per le violazioni di tali norme nazionali e delle relative sanzioni amministrative non dovrebbe essere in contrasto con il principio del *ne bis in idem* quale interpretato dalla Corte di giustizia.

(75) Qualora la presente direttiva non armonizzi le sanzioni amministrative o ove necessario in altri casi, ad esempio in caso di violazioni gravi degli obblighi stabiliti nella presente direttiva, gli Stati membri dovrebbero attuare un sistema che preveda sanzioni effettive, proporzionate e dissuasive. La natura di tali sanzioni, penali o amministrative, dovrebbe essere determinata dal diritto degli Stati membri.

(76) Al fine di rafforzare ulteriormente l'efficacia e il carattere dissuasivo delle sanzioni applicabili alle violazioni degli obblighi stabiliti a norma della presente direttiva, le autorità competenti dovrebbero avere la facoltà di applicare sanzioni consistenti nella sospensione di una certificazione o di un'autorizzazione relativa a una parte o alla totalità dei servizi forniti da un soggetto essenziale e nell'imposizione di un divieto temporaneo all'esercizio di funzioni dirigenziali da parte di una persona fisica. Data la loro gravità e l'impatto sulle attività dei soggetti e, in ultima analisi, sui consumatori, tali sanzioni dovrebbero essere applicate solo in proporzione alla gravità della violazione e tenere conto delle circostanze specifiche di ciascun caso, tra cui il carattere doloso o colposo della violazione e le azioni intraprese per prevenire o attenuare il danno effettuato e/o le perdite subite. Tali sanzioni dovrebbero essere applicate solo come ultima ratio, vale a dire solo una volta esaurite le altre pertinenti misure di esecuzione previste dalla presente direttiva, e solo fino a quando i soggetti ai quali si applicano non adottano le misure necessarie per rimediare alle carenze o per conformarsi alle prescrizioni dell'autorità competente per cui tali sanzioni sono state applicate. L'imposizione di tali sanzioni dovrebbe essere soggetta a garanzie procedurali appropriate in conformità ai principi generali del diritto dell'Unione e della Carta dei diritti fondamentali dell'Unione europea, inclusi l'effettiva tutela giurisdizionale, il giusto processo, la presunzione di innocenza e i diritti della difesa.

(77) La presente direttiva dovrebbe stabilire norme di cooperazione tra le autorità competenti e le autorità di controllo conformemente al regolamento (UE) 2016/679 per far fronte alle violazioni relative ai dati personali.

(78) La presente direttiva dovrebbe mirare a garantire un elevato livello di responsabilità per le misure di gestione dei rischi di cibersicurezza e gli obblighi di segnalazione a livello delle organizzazioni. Pertanto gli organismi di gestione dei soggetti che rientrano nell'ambito di applicazione della presente direttiva dovrebbero approvare le misure relative ai rischi di cibersicurezza e vigilare sulla loro attuazione.

(79) Dovrebbe essere introdotto un meccanismo di revisione tra pari che consenta agli esperti designati dagli Stati membri di valutare l'attuazione delle politiche in materia di

cibersicurezza, compreso il livello delle capacità degli Stati membri e le risorse disponibili.

(80) Al fine di tenere conto delle nuove minacce informatiche, degli sviluppi tecnologici o delle specificità settoriali, conformemente all'articolo 290 TFUE alla Commissione dovrebbe essere delegato il potere di adottare atti per quanto riguarda gli elementi relativi alle misure di gestione dei rischi imposte dalla presente direttiva. Alla Commissione dovrebbe inoltre essere conferito il potere di adottare atti delegati che stabiliscano quali categorie di soggetti essenziali sono tenute a ottenere un certificato e nell'ambito di quali sistemi europei di certificazione della cibersicurezza. È di particolare importanza che durante i lavori preparatori la Commissione svolga adeguate consultazioni, anche a livello di esperti, nel rispetto dei principi stabiliti nell'accordo interistituzionale "Legiferare meglio" del 13 aprile 2016[26]. In particolare, al fine di garantire la parità di partecipazione alla preparazione degli atti delegati, il Parlamento europeo e il Consiglio ricevono tutti i documenti contemporaneamente agli esperti degli Stati membri, e i loro esperti hanno sistematicamente accesso alle riunioni dei gruppi di esperti della Commissione incaricati della preparazione di tali atti delegati.

(81) Al fine di garantire condizioni uniformi di attuazione delle pertinenti disposizioni della presente direttiva riguardanti le modalità procedurali necessarie per il funzionamento del gruppo di cooperazione, gli elementi tecnici relativi alle misure di gestione dei rischi o al tipo di informazioni e il formato e la procedura per le notifiche degli incidenti, dovrebbero essere attribuite alla Commissione competenze di esecuzione. È altresì opportuno che tali competenze siano esercitate conformemente al regolamento (UE) n. 182/2011 del Parlamento europeo e del Consiglio[27].

(82) È opportuno che la Commissione riesamini la presente direttiva a scadenze regolari, in consultazione con le parti interessate, in particolare al fine valutare la necessità di modifiche alla luce dei cambiamenti delle condizioni sociali, politiche, tecnologiche o del mercato.

(83) Poiché l'obiettivo della presente direttiva, vale a dire conseguire un elevato livello comune di cibersicurezza nell'Unione, non può essere conseguito in misura sufficiente dagli Stati membri ma, a motivo degli effetti dell'azione, può essere conseguito meglio a livello dell'Unione, quest'ultima può adottare misure in conformità al principio di sussidiarietà sancito dall'articolo 5 del trattato sull'Unione europea. La presente direttiva si limita a quanto è necessario per conseguire tale obiettivo in ottemperanza al principio di proporzionalità enunciato nello stesso articolo.

(84) La presente direttiva rispetta i diritti fondamentali e osserva i principi riconosciuti dalla Carta dei diritti fondamentali dell'Unione europea, in particolare il diritto al rispetto della vita privata e delle comunicazioni, la protezione dei dati personali, la libertà di impresa, il diritto di proprietà, il diritto a un ricorso effettivo dinanzi a un giudice e il diritto al contraddittorio. La presente direttiva dovrebbe essere attuata in conformità a tali diritti e principi,

---

[26] GU L 123 del 12.5.2016, pag. 1.

[27] Regolamento (UE) n. 182/2011 del Parlamento europeo e del Consiglio, del 16 febbraio 2011, che stabilisce le regole e i principi generali relativi alle modalità di controllo da parte degli Stati membri dell'esercizio delle competenze di esecuzione attribuite alla Commissione (GU L 55 del 28.2.2011, pag. 13).

HANNO ADOTTATO LA PRESENTE DIRETTIVA:

CAPO I

Disposizioni generali

Articolo 1

Oggetto

1. La presente direttiva stabilisce misure volte a garantire un livello comune elevato di cibersicurezza nell'Unione.

2. A tal fine la presente direttiva:

   a) fa obbligo agli Stati membri di adottare strategie nazionali in materia di cibersicurezza e designare autorità nazionali competenti, punti di contatto unici e team di risposta agli incidenti di sicurezza informatica (*computer security incident response team*, CSIRT);

   b) stabilisce obblighi in materia di gestione e segnalazione dei rischi di cibersicurezza per i tipi di soggetti definiti soggetti essenziali di cui all'allegato I e soggetti importanti di cui all'allegato II;

   c) stabilisce obblighi in materia di condivisione delle informazioni sulla cibersicurezza.

Articolo 2

Ambito di applicazione

1. La presente direttiva si applica ai tipi di soggetti pubblici e privati definiti soggetti essenziali di cui all'allegato I e soggetti importanti di cui all'allegato II. La presente direttiva non si applica ai soggetti che si qualificano come microimprese e piccole imprese ai sensi della raccomandazione 2003/361/CE della Commissione[28].

2. La presente direttiva si applica tuttavia anche ai soggetti di cui agli allegati I e II, indipendentemente dalle loro dimensioni, qualora:

   a) i servizi siano forniti da uno dei soggetti seguenti:

      i) reti pubbliche di comunicazione elettronica o servizi di comunicazione elettronica accessibili al pubblico di cui all'allegato I, punto 8;

      ii) prestatori di servizi fiduciari di cui all'allegato I, punto 8;

      iii) registri di nomi di dominio di primo livello e fornitori di servizi DNS (*domain name system*, sistema dei nomi di dominio) di cui all'allegato I, punto 8;

[28] Raccomandazione 2003/361/CE della Commissione, del 6 maggio 2003, relativa alla definizione delle microimprese, piccole e medie imprese (GU L 124 del 20.5.2003, pag. 36).

b) il soggetto sia un ente della pubblica amministrazione quale definito all'articolo 4, punto 23;

c) il soggetto sia l'unico fornitore di un servizio in uno Stato membro;

d) una possibile perturbazione del servizio fornito dal soggetto potrebbe avere un impatto sulla sicurezza pubblica, l'incolumità pubblica o la salute pubblica;

e) una possibile perturbazione del servizio fornito dal soggetto potrebbe comportare rischi sistemici, in particolare per i settori nei quali tale perturbazione potrebbe avere un impatto transfrontaliero;

f) il soggetto sia critico in ragione della sua particolare importanza a livello regionale o nazionale per quel particolare settore o tipo di servizio o per altri settori indipendenti nello Stato membro;

g) il soggetto sia identificato come soggetto critico a norma della direttiva (UE) XXXX/XXXX del Parlamento europeo e del Consiglio[29] [direttiva sulla resilienza dei soggetti critici] o come soggetto equivalente a un soggetto critico a norma dell'articolo 7 di tale direttiva.

Gli Stati membri redigono un elenco di soggetti identificati a norma delle lettere da b) a f) e lo trasmettono alla Commissione entro [6 mesi dopo il termine di recepimento]. Gli Stati membri riesaminano l'elenco periodicamente, almeno ogni due anni e, se opportuno, lo aggiornano.

3. La presente direttiva fa salve le competenze degli Stati membri in materia di mantenimento della sicurezza pubblica, difesa e sicurezza nazionale nel rispetto del diritto dell'Unione.

4. La presente direttiva si applica fatte salve la direttiva 2008/114/CE del Consiglio[30] e le direttive 2011/93/UE[31] e 2013/40/UE[32] del Parlamento europeo e del Consiglio.

5. Fatto salvo l'articolo 346 TFUE, le informazioni riservate ai sensi della normativa dell'Unione e nazionale, quale quella sulla riservatezza commerciale, sono scambiate con la Commissione e con altre autorità competenti solo nella misura in cui tale scambio sia necessario ai fini dell'applicazione della presente direttiva. Le informazioni scambiate sono limitate alle informazioni pertinenti 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 essenziali o importanti.

6. Qualora le disposizioni di atti giuridici settoriali dell'Unione facciano obbligo ai soggetti essenziali o importanti di adottare misure di gestione dei rischi di cibersicurezza o di notificare gli incidenti o le minacce informatiche significative, nella misura in cui gli effetti di tali obblighi siano almeno equivalenti a quelli degli obblighi di cui alla presente direttiva, non si applicano le pertinenti disposizioni della

---

29 *[Inserire il titolo completo e il riferimento della pubblicazione nella GU, non appena noti]*.

30 Direttiva 2008/114/CE del Consiglio, dell'8 dicembre 2008, relativa all'individuazione e alla designazione delle infrastrutture critiche europee e alla valutazione della necessità di migliorarne la protezione (GU L 345 del 23.12.2008, pag. 75).

31 Direttiva 2011/93/UE del Parlamento europeo e del Consiglio, del 13 dicembre 2011, relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile, e che sostituisce la decisione quadro 2004/68/GAI del Consiglio (GU L 335 del 17.12.2011, pag. 1).

32 Direttiva 2013/40/UE del Parlamento europeo e del Consiglio, del 12 agosto 2013, relativa agli attacchi contro i sistemi di informazione e che sostituisce la decisione quadro 2005/222/GAI del Consiglio (GU L 218 del 14.8.2013, pag. 8).

presente direttiva, comprese le disposizioni relative alla vigilanza e all'esecuzione di cui al capo VI.

Articolo 3

Armonizzazione minima

Fatti salvi i loro obblighi derivanti dal diritto dell'Unione, gli Stati membri, conformemente alla presente direttiva, possono adottare o mantenere disposizioni che garantiscono un livello più elevato di cibersicurezza.

Articolo 4

Definizioni

Ai fini della presente direttiva si applicano le definizioni seguenti:

1) "sistema informatico e di rete":

   a) una rete di comunicazione elettronica ai sensi dell'articolo 2, punto 1, della direttiva (UE) 2018/1972;

   b) qualsiasi dispositivo o gruppo di dispositivi interconnessi o collegati, uno o più dei quali eseguono, in base a un programma, un'elaborazione automatica di dati digitali;

   c) i dati digitali conservati, elaborati, estratti o trasmessi per mezzo degli elementi di cui alle lettere a) e b), ai fini del loro funzionamento, del loro uso, della loro protezione e della loro manutenzione;

2) "sicurezza dei sistemi informatici e di rete": la capacità dei sistemi informatici e di rete di resistere, con un determinato livello di confidenza, alle azioni che compromettono la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati conservati, trasmessi o elaborati o dei relativi servizi offerti da tali sistemi informatici e di rete o accessibili attraverso di essi;

3) "cibersicurezza": la cibersicurezza ai sensi dell'articolo 2, punto 1, del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio[33];

4) "strategia nazionale per la cibersicurezza": un quadro coerente di uno Stato membro che prevede priorità e obiettivi strategici in materia di sicurezza dei sistemi informatici e di rete in tale Stato membro;

5) "incidente": un evento che compromette la disponibilità, l'autenticità, l'integrità o la riservatezza di dati conservati, trasmessi o elaborati o dei relativi servizi offerti dai sistemi informatici e di rete o accessibili attraverso di essi;

6) "gestione degli incidenti": tutte le azioni e le procedure volte a rilevare, analizzare e contenere un incidente e a rispondervi;

[33] 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).

7) "minaccia informatica": una minaccia informatica ai sensi dell'articolo 2, punto 8, del regolamento (UE) 2019/881;

8) "vulnerabilità": un punto debole, una suscettibilità o un difetto di una risorsa, di un sistema, di un processo o di un controllo che possono essere sfruttati da una minaccia informatica;

9) "rappresentante": qualsiasi persona fisica o giuridica stabilita nell'Unione espressamente designata ad agire per conto di i) un fornitore di servizi DNS, un registro dei nomi di dominio di primo livello (*top-level domain*, TLD), un fornitore di servizi di cloud computing, un fornitore di servizi di data center o un fornitore di reti di distribuzione dei contenuti (*content delivery network*) di cui all'allegato I, punto 8, o ii) soggetti di cui all'allegato II, punto 6, che non sono stabiliti nell'Unione, a cui l'autorità nazionale competente o un CSIRT può rivolgersi in luogo del soggetto per quanto riguarda gli obblighi di quest'ultimo a norma della presente direttiva;

10) "norma": una norma ai sensi dell'articolo 2, punto 1, del regolamento (UE) n. 1025/2012 del Parlamento europeo e del Consiglio[34];

11) "specifica tecnica": una specifica tecnica ai sensi dell'articolo 2, punto 4, del regolamento (UE) n. 1025/2012;

12) "punto di interscambio Internet (IXP)": un'infrastruttura di rete che consente l'interconnessione di più di due reti indipendenti (sistemi autonomi), principalmente al fine di agevolare lo scambio del traffico Internet; un IXP fornisce interconnessione soltanto ai sistemi autonomi; un IXP non richiede che il traffico Internet che passa tra qualsiasi coppia di sistemi autonomi partecipanti passi attraverso un terzo sistema autonomo, né altera o interferisce altrimenti con tale traffico;

13) "sistema dei nomi di dominio (DNS)": un sistema di nomi gerarchico e distribuito che consente agli utenti finali di accedere a servizi e risorse su Internet;

14) "fornitore di servizi DNS": un soggetto che fornisce un servizio di risoluzione dei nomi di dominio autorevole o ricorsivo agli utenti finali di Internet e ad altri fornitori di servizi DNS;

15) "registro dei nomi di dominio di primo livello": un soggetto cui è stato delegato uno specifico dominio di primo livello (TLD) e che è responsabile dell'amministrazione di tale TLD, compresa la registrazione dei nomi di dominio sotto tale TLD, e del funzionamento tecnico di tale TLD, compreso il funzionamento dei server dei nomi, la manutenzione delle banche dati e la distribuzione dei file di zona TLD tra i server dei nomi;

16) "servizio digitale": un servizio ai sensi dell'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio[35];

---

34 Regolamento (UE) n. 1025/2012 del Parlamento europeo e del Consiglio, del 25 ottobre 2012, sulla normazione europea, che modifica le direttive 89/686/CEE e 93/15/CEE del Consiglio nonché le direttive 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE e 2009/105/CE del Parlamento europeo e del Consiglio e che abroga la decisione 87/95/CEE del Consiglio e la decisione n. 1673/2006/CE del Parlamento europeo e del Consiglio (GU L 316 del 14.11.2012, pag. 12).

35 Direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio, del 9 settembre 2015, che prevede una procedura d'informazione nel settore delle regolamentazioni tecniche e delle regole relative ai servizi della società dell'informazione (GU L 241 del 17.9.2015, pag. 1).

17) "mercato online": un servizio digitale ai sensi dell'articolo 2, lettera n), della direttiva 2005/29/CE del Parlamento europeo e del Consiglio[36];

18) "motore di ricerca online": un servizio digitale ai sensi dell'articolo 2, punto 5, del regolamento (UE) 2019/1150 del Parlamento europeo e del Consiglio[37];

19) "servizio di cloud computing": un servizio digitale che consente l'amministrazione su richiesta di un *pool* scalabile ed elastico di risorse di calcolo condivisibili e distribuite e l'ampio accesso remoto a quest'ultimo;

20) "servizio di data center": un servizio che comprende strutture, o gruppi di strutture, dedicate a ospitare, interconnettere e far funzionare in modo centralizzato apparecchiature informatiche e di rete che forniscono servizi di conservazione, elaborazione e trasporto di dati insieme a tutti gli impianti e le infrastrutture per la distribuzione dell'energia e il controllo ambientale;

21) "rete di distribuzione dei contenuti (*content delivery network*)": una rete di server distribuiti geograficamente allo scopo di garantire l'elevata disponibilità, l'accessibilità o la rapida distribuzione di contenuti e servizi digitali agli utenti di Internet per conto di fornitori di contenuti e servizi;

22) "piattaforma di servizi di social network": una piattaforma che consente agli utenti finali di entrare in contatto, condividere, scoprire e comunicare gli uni con gli altri su molteplici dispositivi e, in particolare, attraverso chat, post, video e raccomandazioni;

23) "ente della pubblica amministrazione": un soggetto di uno Stato membro che soddisfa i criteri seguenti:

   a) è istituito allo scopo di soddisfare esigenze di interesse generale e non ha carattere industriale o commerciale;

   b) è dotato di personalità giuridica;

   c) è finanziato in modo maggioritario dallo Stato, da autorità regionali o da altri organismi di diritto pubblico; oppure la sua gestione è soggetta alla vigilanza di tali autorità o organismi; oppure è dotato di un organo di amministrazione, di direzione o di vigilanza in cui più della metà dei membri è designata dallo Stato, da autorità regionali o da altri organismi di diritto pubblico;

   d) ha il potere di adottare, nei confronti di persone fisiche o giuridiche, decisioni amministrative o normative che incidono sui loro diritti relativi alla circolazione transfrontaliera delle merci, delle persone, dei servizi o dei capitali.

   Sono esclusi gli enti della pubblica amministrazione che operano nei settori della sicurezza pubblica, della difesa o della sicurezza nazionale o svolgono attività di contrasto;

---

36 Direttiva 2005/29/CE del Parlamento europeo e del Consiglio, dell'11 maggio 2005, relativa alle pratiche commerciali sleali delle imprese nei confronti dei consumatori nel mercato interno e che modifica la direttiva 84/450/CEE del Consiglio e le direttive 97/7/CE, 98/27/CE e 2002/65/CE del Parlamento europeo e del Consiglio e il regolamento (CE) n. 2006/2004 del Parlamento europeo e del Consiglio ("direttiva sulle pratiche commerciali sleali") (GU L 149 dell'11.6.2005, pag. 22).

37 Regolamento (UE) 2019/1150 del Parlamento europeo e del Consiglio, del 20 giugno 2019, che promuove equità e trasparenza per gli utenti commerciali dei servizi di intermediazione online (GU L 186 dell'11.7.2019, pag. 57).

24) "soggetto": una persona fisica o giuridica, costituita e riconosciuta come tale conformemente al diritto nazionale applicabile nel suo luogo di stabilimento, che può, agendo in nome proprio, esercitare diritti ed essere soggetta a obblighi;

25) "soggetto essenziale": un tipo di soggetto che figura tra i soggetti essenziali di cui all'allegato I;

26) "soggetto importante": un tipo di soggetto che figura tra i soggetti importanti di cui all'allegato II.

CAPO II

Quadri normativi coordinati in materia di cibersicurezza

Articolo 5
Strategia nazionale per la cibersicurezza

1. Ogni Stato membro adotta una strategia nazionale per la cibersicurezza che definisce obiettivi strategici e adeguate misure strategiche e normative al fine di raggiungere e mantenere un livello elevato di cibersicurezza. La strategia nazionale per la cibersicurezza comprende, in particolare, gli elementi seguenti:

   a) una definizione degli obiettivi e delle priorità della strategia per la cibersicurezza dello Stato membro;

   b) un quadro di governance per la realizzazione di tali obiettivi e priorità, comprendente le misure strategiche di cui al paragrafo 2 e i ruoli e le responsabilità degli enti e degli organismi pubblici, nonché di altri attori pertinenti;

   c) una valutazione volta a individuare le risorse e rischi di cibersicurezza pertinenti nello Stato membro;

   d) l'individuazione delle misure volte a garantire la preparazione e la risposta agli incidenti e il successivo recupero dagli stessi, inclusa la collaborazione tra i settori pubblico e privato;

   e) un elenco delle diverse autorità e dei diversi attori coinvolti nell'attuazione della strategia nazionale per la cibersicurezza;

   f) un quadro strategico per il rafforzamento del coordinamento tra le autorità competenti a norma della presente direttiva e della direttiva (UE) XXXX/XXXX del Parlamento europeo e del Consiglio[38] [direttiva sulla resilienza dei soggetti critici] ai fini della condivisione delle informazioni sugli incidenti e sulle minacce informatiche e dello svolgimento di compiti di vigilanza.

2. Nell'ambito della strategia nazionale per la cibersicurezza, gli Stati membri adottano in particolare le misure strategiche seguenti:

   a) misure relative alla cibersicurezza nella catena di approvvigionamento dei prodotti e dei servizi delle tecnologie dell'informazione e della comunicazione

[38] *[Inserire il titolo completo e il riferimento della pubblicazione nella GU, non appena noti]*.

(TIC) utilizzati da soggetti essenziali e importanti per la fornitura dei loro servizi;

b) orientamenti relativi all'inclusione e alla definizione di requisiti relativi alla cibersicurezza per i prodotti e i servizi TIC negli appalti pubblici;

c) misure volte a promuovere e a facilitare la divulgazione coordinata delle vulnerabilità ai sensi dell'articolo 6;

d) misure relative al sostegno della disponibilità generale e dell'integrità del carattere fondamentale pubblico di una rete Internet aperta;

e) misure volte a promuovere e sviluppare competenze, attività di sensibilizzazione e iniziative di ricerca e sviluppo in materia di cibersicurezza;

f) misure per sostenere gli istituti accademici e di ricerca nello sviluppo di strumenti di cibersicurezza e di infrastrutture di rete sicure;

g) misure, procedure pertinenti e strumenti adeguati di condivisione delle informazioni per sostenere la condivisione volontaria di informazioni sulla cibersicurezza tra imprese, nel rispetto del diritto dell'Unione;

h) misure volte a rispondere alle esigenze specifiche delle PMI, in particolare quelle escluse dall'ambito di applicazione della presente direttiva, relativamente a orientamenti e sostegno per rafforzare la loro resilienza alle minacce alla cibersicurezza.

3. Gli Stati membri notificano le loro strategie nazionali per la cibersicurezza alla Commissione entro tre mesi dall'adozione. Gli Stati membri possono omettere dalla notifica informazioni specifiche se e nella misura in cui ciò sia strettamente necessario per preservare la sicurezza nazionale.

4. Gli Stati membri valutano le proprie strategie nazionali per la cibersicurezza almeno ogni quattro anni sulla base di indicatori chiave di prestazione e, se necessario, le modificano. L'Agenzia dell'Unione europea per la cibersicurezza (ENISA) assiste su richiesta gli Stati membri nell'elaborazione di una strategia nazionale e di indicatori chiave di prestazione per la relativa valutazione.

Articolo 6

Divulgazione coordinata delle vulnerabilità e registro europeo delle vulnerabilità

1. Ogni Stato membro designa uno dei propri CSIRT di cui all'articolo 9 come coordinatore ai fini della divulgazione coordinata delle vulnerabilità. Il CSIRT designato agisce da intermediario di fiducia agevolando, se necessario, l'interazione tra il soggetto che effettua la segnalazione e il fabbricante o fornitore di servizi TIC o prodotti TIC. Se la vulnerabilità segnalata riguarda più fabbricanti o fornitori di servizi TIC o prodotti TIC nell'Unione, il CSIRT designato di ciascuno Stato membro interessato coopera con la rete di CSIRT.

2. L'ENISA elabora e mantiene un registro europeo delle vulnerabilità. A tal fine l'ENISA istituisce e gestisce i sistemi informatici, le misure strategiche e le procedure adeguati, volti in particolare a consentire ai soggetti essenziali e importanti e ai relativi fornitori di sistemi informatici e di rete di divulgare e registrare le vulnerabilità presenti nei prodotti TIC o nei servizi TIC, nonché a fornire a tutte le parti interessate l'accesso alle informazioni sulle vulnerabilità contenute nel registro.

Il registro contiene, in particolare, informazioni che illustrano la vulnerabilità, i prodotti TIC o i servizi TIC interessati e la gravità della vulnerabilità in termini di circostanze nelle quali potrebbe essere sfruttata, la disponibilità di relative patch e, qualora queste non fossero disponibili, orientamenti rivolti agli utenti dei prodotti e dei servizi vulnerabili sulle possibili modalità di attenuazione dei rischi derivanti dalle vulnerabilità divulgate.

Articolo 7

Quadri nazionali di gestione delle crisi di cibersicurezza

1. Ogni Stato membro designa una o più autorità competenti responsabili della gestione delle crisi e degli incidenti su vasta scala. Gli Stati membri provvedono affinché le autorità competenti dispongano di risorse adeguate per svolgere i compiti loro assegnati in modo efficace ed efficiente.

2. Ogni Stato membro individua le capacità, le risorse e le procedure che possono essere impiegate in caso di crisi ai fini della presente direttiva.

3. Ogni Stato membro adotta un piano nazionale di risposta agli incidenti e alle crisi di cibersicurezza in cui sono stabiliti gli obiettivi e le modalità della gestione delle crisi e degli incidenti di cibersicurezza su vasta scala. Nel piano sono definiti, in particolare, i seguenti elementi:

   a) gli obiettivi delle misure e delle attività nazionali di preparazione;

   b) i compiti e le responsabilità delle autorità nazionali competenti;

   c) le procedure di gestione delle crisi e i canali di scambio delle informazioni;

   d) le misure di preparazione, comprese le esercitazioni e le attività di formazione;

   e) le pertinenti parti interessate del settore pubblico e privato e le infrastrutture coinvolte;

   f) le procedure nazionali e gli accordi tra gli organismi e le autorità nazionali pertinenti al fine di garantire il sostegno efficace dello Stato membro alla gestione coordinata delle crisi e degli incidenti di cibersicurezza su vasta scala a livello dell'Unione e la sua effettiva partecipazione a tale gestione.

4. Gli Stati membri comunicano alla Commissione le autorità competenti designate di cui al paragrafo 1 e trasmettono i propri piani nazionali di risposta agli incidenti e alle crisi di cibersicurezza di cui al paragrafo 3 entro tre mesi da tali designazioni e dall'adozione di tali piani. Gli Stati membri possono omettere dal piano informazioni specifiche se e nella misura in cui ciò sia strettamente necessario ai fini della loro sicurezza nazionale.

Articolo 8

Autorità nazionali competenti e punti di contatto unici

1. Ogni Stato membro designa una o più autorità competenti responsabili della cibersicurezza e dei compiti di vigilanza di cui al capo VI della presente direttiva. Gli Stati membri possono designare a questo scopo una o più autorità esistenti.

2. Le autorità competenti di cui al paragrafo 1 controllano l'applicazione della presente direttiva a livello nazionale.

3. Ogni Stato membro designa un punto di contatto unico nazionale in materia di cibersicurezza ("punto di contatto unico"). Se uno Stato membro designa soltanto un'autorità competente, quest'ultima è anche il punto di contatto unico per tale Stato membro.

4. Ogni punto di contatto unico svolge una funzione di collegamento per garantire la cooperazione transfrontaliera delle autorità del relativo Stato membro con le autorità pertinenti degli altri Stati membri, nonché per garantire la cooperazione intersettoriale con altre autorità nazionali competenti dello stesso Stato membro.

5. Gli Stati membri provvedono affinché le autorità competenti di cui al paragrafo 1 e i punti di contatto unici dispongano di risorse adeguate per svolgere i compiti loro assegnati in modo efficace ed efficiente e conseguire in questo modo gli obiettivi della presente direttiva. Gli Stati membri garantiscono la collaborazione effettiva, efficiente e sicura dei rappresentanti designati nel gruppo di cooperazione di cui all'articolo 12.

6. Ogni Stato membro notifica alla Commissione, senza indebiti ritardi, l'autorità competente designata di cui al paragrafo 1 e il punto di contatto unico designato di cui al paragrafo 3, i rispettivi compiti e qualsiasi ulteriore modifica dei medesimi. Ogni Stato membro rende pubbliche le designazioni. La Commissione pubblica l'elenco dei punti di contatto unici designati.

Articolo 9

Team di risposta agli incidenti di sicurezza informatica (CSIRT)

1. Ogni Stato membro designa uno o più CSIRT conformi ai requisiti di cui all'articolo 10, paragrafo 1, che si occupano almeno dei settori, dei sottosettori o dei soggetti di cui agli allegati I e II e sono responsabili della gestione degli incidenti conformemente a una procedura ben definita. È possibile istituire un CSIRT all'interno di un'autorità competente di cui all'articolo 8.

2. Gli Stati membri provvedono affinché ogni CSIRT disponga di risorse adeguate per svolgere efficacemente i suoi compiti di cui all'articolo 10, paragrafo 2.

3. Gli Stati membri provvedono affinché ogni CSIRT disponga di un'infrastruttura di informazione e comunicazione adeguata, sicura e resiliente per scambiare informazioni con i soggetti essenziali e importanti e con le altre parti interessate pertinenti. A tal fine gli Stati membri provvedono affinché i CSIRT contribuiscano allo sviluppo di strumenti sicuri per la condivisione delle informazioni.

4. I CSIRT cooperano e, se opportuno, scambiano informazioni pertinenti conformemente all'articolo 26 con comunità settoriali o intersettoriali fidate di soggetti essenziali e importanti.

5. I CSIRT partecipano alle revisioni tra pari organizzate conformemente all'articolo 16.

6. Gli Stati membri garantiscono la collaborazione effettiva, efficiente e sicura dei loro CSIRT nella rete di CSIRT di cui all'articolo 13.

7. Gli Stati membri comunicano alla Commissione senza indebiti ritardi i CSIRT designati conformemente al paragrafo 1 e il CSIRT coordinatore designato

conformemente all'articolo 6, paragrafo 1, nonché i relativi compiti previsti in relazione ai soggetti di cui agli allegati I e II.

8. Gli Stati membri possono chiedere l'assistenza dell'ENISA nello sviluppo di CSIRT nazionali.

Articolo 10
Requisiti e compiti dei CSIRT

1. I CSIRT soddisfano i seguenti requisiti:

   a) i CSIRT garantiscono un alto livello di disponibilità dei propri servizi di comunicazione evitando singoli punti di vulnerabilità (*single points of failure*) e dispongono di vari mezzi che permettono loro di essere contattati e di contattare altri in qualsiasi momento. I CSIRT indicano chiaramente i canali di comunicazione e li rendono noti alla loro base di utenti e ai partner con cui collaborano;

   b) i locali e i sistemi informatici di supporto dei CSIRT sono ubicati in siti sicuri;

   c) i CSIRT sono dotati di un sistema adeguato di gestione e inoltro delle richieste, in particolare per facilitare i trasferimenti in maniera efficace ed efficiente;

   d) i CSIRT dispongono di personale sufficiente a garantirne l'operatività in qualsiasi momento;

   e) i CSIRT sono dotati di sistemi ridondanti e spazi di lavoro di backup al fine di garantire la continuità dei loro servizi;

   f) i CSIRT hanno la possibilità di partecipare a reti di cooperazione internazionale.

2. I CSIRT svolgono i seguenti compiti:

   a) monitorano le minacce informatiche, le vulnerabilità e gli incidenti a livello nazionale;

   b) emettono preallarmi, allerte e bollettini e divulgano informazioni ai soggetti essenziali e importanti, nonché alle altre pertinenti parti interessate, in merito a minacce informatiche, vulnerabilità e incidenti;

   c) forniscono una risposta agli incidenti;

   d) forniscono un'analisi dinamica dei rischi e degli incidenti, nonché una consapevolezza situazionale riguardo alla cibersicurezza;

   e) effettuano, su richiesta di un soggetto, una scansione proattiva dei sistemi informatici e di rete da esso utilizzati per la fornitura dei suoi servizi;

   f) partecipano alla rete di CSIRT e, su richiesta, forniscono assistenza reciproca agli altri membri della rete.

3. I CSIRT instaurano rapporti di cooperazione con i pertinenti attori del settore privato al fine di perseguire meglio gli obiettivi della presente direttiva.

4. Al fine di agevolare la cooperazione, i CSIRT promuovono l'adozione e l'uso di pratiche, sistemi di classificazione e tassonomie standardizzati o comuni per quanto riguarda:

a) le procedure di gestione degli incidenti;

b) la gestione delle crisi di cibersicurezza;

c) la divulgazione coordinata delle vulnerabilità.

Articolo 11
Cooperazione a livello nazionale

1. Se sono separati, le autorità competenti di cui all'articolo 8, il punto di contatto unico e i CSIRT dello stesso Stato membro collaborano per quanto concerne l'adempimento degli obblighi di cui alla presente direttiva.

2. Gli Stati membri provvedono affinché le loro autorità competenti o i loro CSIRT ricevano le notifiche in merito agli incidenti, alle minacce informatiche significative e ai quasi incidenti (*near miss*) trasmesse a norma della presente direttiva. Qualora uno Stato membro decida che i suoi CSIRT non debbano ricevere tali notifiche, a questi ultimi viene dato accesso, nella misura necessaria per lo svolgimento dei loro compiti, ai dati sugli incidenti notificati dai soggetti essenziali o importanti, a norma dell'articolo 20.

3. Ogni Stato membro provvede affinché le sue autorità competenti o i suoi CSIRT informino il suo punto di contatto unico in merito alle notifiche relative agli incidenti, alle minacce informatiche significative e ai quasi incidenti trasmesse a norma della presente direttiva.

4. Nella misura necessaria per l'efficace adempimento dei compiti e degli obblighi stabiliti nella presente direttiva, gli Stati membri provvedono affinché, all'interno di ciascuno Stato membro, vi sia un'adeguata cooperazione tra le autorità competenti e i punti di contatto unici e le autorità di contrasto, le autorità di protezione dei dati, le autorità responsabili delle infrastrutture critiche a norma della direttiva (UE) XXXX/XXXX [direttiva sulla resilienza dei soggetti critici] e le autorità finanziarie nazionali designate conformemente al regolamento (UE) XXXX/XXXX del Parlamento europeo e del Consiglio[39] [il regolamento DORA].

5. Gli Stati membri provvedono affinché le loro autorità competenti forniscano periodicamente alle autorità competenti designate a norma della direttiva (UE) XXXX/XXXX [direttiva sulla resilienza dei soggetti critici] informazioni sui rischi di cibersicurezza, sulle minacce informatiche e sugli incidenti che interessano i soggetti essenziali identificati come critici, o come soggetti equivalenti ai soggetti critici, a norma della direttiva (UE) XXXX/XXXX [direttiva sulla resilienza dei soggetti critici], nonché sulle misure adottate dalle autorità competenti in risposta a tali rischi e incidenti.

CAPO III

[39] *[Inserire il titolo completo e il riferimento della pubblicazione nella GU, non appena noti]*.

Cooperazione

Articolo 12
Gruppo di cooperazione

1. Al fine di sostenere e agevolare la cooperazione strategica e lo scambio di informazioni tra gli Stati membri nell'ambito di applicazione della direttiva, è istituito un gruppo di cooperazione.

2. Il gruppo di cooperazione svolge i suoi compiti sulla base di programmi di lavoro biennali di cui al paragrafo 6.

3. Il gruppo di cooperazione è composto da rappresentanti degli Stati membri, della Commissione e dell'ENISA. Il servizio europeo per l'azione esterna partecipa alle attività del gruppo di cooperazione in qualità di osservatore. Le autorità europee di vigilanza (AEV) conformemente all'articolo 17, paragrafo 5, lettera c), del regolamento (UE) XXXX/XXXX [il regolamento DORA] possono partecipare alle attività del gruppo di cooperazione.

   Ove opportuno, il gruppo di cooperazione può invitare a partecipare ai suoi lavori i rappresentanti dei pertinenti portatori di interessi.

   La Commissione ne assicura il segretariato.

4. Il gruppo di cooperazione svolge i seguenti compiti:

   a) fornisce orientamenti alle autorità competenti in merito al recepimento e all'attuazione della presente direttiva;

   b) scambia migliori pratiche e informazioni relative all'attuazione della presente direttiva, anche per quanto riguarda minacce informatiche, incidenti, vulnerabilità, quasi incidenti, iniziative di sensibilizzazione, attività di formazione, esercitazioni e competenze, sviluppo di capacità, norme e specifiche tecniche;

   c) effettua scambi di consulenza e coopera con la Commissione per quanto riguarda le nuove iniziative strategiche in materia di cibersicurezza;

   d) effettua scambi di consulenza e coopera con la Commissione per quanto riguarda i progetti di atti di esecuzione o delegati della Commissione adottati a norma della presente direttiva;

   e) scambia migliori pratiche e informazioni con le istituzioni, gli organismi, gli uffici e le agenzie pertinenti dell'Unione;

   f) discute le relazioni sulle revisioni tra pari di cui all'articolo 16, paragrafo 7;

   g) discute i risultati delle attività di vigilanza comuni nei casi transfrontalieri di cui all'articolo 34;

   h) fornisce orientamenti strategici alla rete di CSIRT su specifiche questioni emergenti;

   i) contribuisce alle capacità di cibersicurezza in tutta l'Unione agevolando lo scambio di funzionari nazionali attraverso un programma di sviluppo delle capacità che coinvolge il personale delle autorità competenti o dei CSIRT degli Stati membri;

j) organizza riunioni congiunte periodiche con le pertinenti parti interessate del settore privato di tutta l'Unione per discutere le attività svolte dal gruppo e raccogliere contributi sulle sfide strategiche emergenti;

k) discute le attività intraprese per quanto riguarda le esercitazioni di cibersicurezza, compreso il lavoro svolto dall'ENISA.

5. Il gruppo di cooperazione può richiedere alla rete di CSIRT una relazione tecnica su argomenti selezionati.

6. Entro il … [24 mesi dopo la data di entrata in vigore della presente direttiva] e successivamente ogni due anni, il gruppo di cooperazione stabilisce un programma di lavoro sulle azioni da intraprendere per realizzare i propri obiettivi e compiti. Il calendario del primo programma adottato a norma della presente direttiva è allineato a quello dell'ultimo programma adottato a norma della direttiva (UE) 2016/1148.

7. La Commissione può adottare atti di esecuzione che stabiliscono le modalità procedurali necessarie per il funzionamento del gruppo di cooperazione. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 37, paragrafo 2.

8. Il gruppo di cooperazione si riunisce periodicamente, almeno una volta all'anno, con il gruppo per la resilienza dei soggetti critici istituito a norma della direttiva (UE) XXXX/XXXX [direttiva sulla resilienza dei soggetti critici] al fine di promuovere la cooperazione strategica e lo scambio di informazioni.

Articolo 13
Rete di CSIRT

1. Al fine di contribuire allo sviluppo della fiducia e di promuovere una cooperazione operativa rapida ed efficace fra gli Stati membri, è istituita una rete dei CSIRT nazionali.

2. La rete di CSIRT è composta da rappresentanti dei CSIRT degli Stati membri e del CERT-UE. La Commissione partecipa alla rete di CSIRT in qualità di osservatore. L'ENISA ne assicura il segretariato e sostiene attivamente la cooperazione fra i CSIRT.

3. La rete di CSIRT svolge i seguenti compiti:

a) scambia informazioni sulle capacità dei CSIRT;

b) scambia informazioni pertinenti sugli incidenti, i quasi incidenti, le minacce informatiche, i rischi e le vulnerabilità;

c) su richiesta di un rappresentante della rete di CSIRT potenzialmente interessato da un incidente, scambia e discute informazioni relative a tale incidente e alle minacce informatiche, ai rischi e alle vulnerabilità associati;

d) su richiesta di un rappresentante della rete di CSIRT, discute e, ove possibile, attua una risposta coordinata a un incidente identificato nella giurisdizione di tale Stato membro;

e) fornisce sostegno agli Stati membri nel far fronte a incidenti transfrontalieri a norma della presente direttiva;

f) fornisce assistenza ai CSIRT designati di cui all'articolo 6 e coopera con essi per quanto riguarda la gestione della divulgazione coordinata multilaterale di vulnerabilità che riguardano molteplici fabbricanti o fornitori di prodotti TIC, servizi TIC e processi TIC stabiliti in Stati membri differenti;

g) discute e individua ulteriori forme di cooperazione operativa, anche in relazione a:

i) categorie di minacce informatiche e incidenti;

ii) preallarmi;

iii) assistenza reciproca;

iv) principi e modalità di coordinamento in risposta a rischi e incidenti transfrontalieri;

v) contributi al piano nazionale di risposta agli incidenti e alle crisi di cibersicurezza di cui all'articolo 7, paragrafo 3;

h) informa il gruppo di cooperazione sulle proprie attività e sulle ulteriori forme di cooperazione operativa discusse a norma della lettera g) e, se necessario, chiede orientamenti in merito;

i) fa il punto sui risultati delle esercitazioni di cibersicurezza, comprese quelle organizzate dall'ENISA;

j) su richiesta di un singolo CSIRT, discute le capacità e lo stato di preparazione di tale CSIRT;

k) coopera e scambia informazioni con i centri operativi di sicurezza regionali e a livello dell'UE al fine di migliorare la consapevolezza situazionale comune sugli incidenti e le minacce in tutta l'Unione;

l) discute le relazioni sulle revisioni tra pari di cui all'articolo 16, paragrafo 7;

m) formula orientamenti volti ad agevolare la convergenza delle pratiche operative in relazione all'applicazione delle disposizioni del presente articolo in materia di cooperazione operativa.

4. Ai fini del riesame di cui all'articolo 35 ed entro il [24 mesi dopo la data di entrata in vigore della presente direttiva], e successivamente ogni due anni, la rete di CSIRT valuta i progressi compiuti nella cooperazione operativa ed elabora una relazione. Nella relazione, in particolare, vengono elaborate conclusioni sui risultati delle revisioni tra pari di cui all'articolo 16 effettuate in relazione ai CSIRT nazionali e perseguite nell'ambito di tale articolo, comprese conclusioni e raccomandazioni. Tale relazione è trasmessa anche al gruppo di cooperazione.

5. La rete di CSIRT adotta il proprio regolamento interno.

Articolo 14

Rete europea delle organizzazioni di collegamento per le crisi informatiche (EU-CyCLONe)

1. Al fine di sostenere la gestione coordinata a livello operativo degli incidenti e delle crisi di cibersicurezza su vasta scala e di garantire il regolare scambio di informazioni tra gli Stati membri e le istituzioni, gli organismi e le agenzie dell'UE, è

istituita la rete europea delle organizzazioni di collegamento per le crisi informatiche (EU-CyCLONe).

2. EU-CyCLONe è composta da rappresentanti delle autorità di gestione delle crisi degli Stati membri designate conformemente all'articolo 7, della Commissione e dell'ENISA. L'ENISA assicura il segretariato della rete e sostiene lo scambio sicuro di informazioni.

3. EU-CyCLONe svolge i seguenti compiti:

   a) aumenta il livello di preparazione per la gestione di crisi e incidenti su vasta scala;

   b) sviluppa una consapevolezza situazionale condivisa in merito ai pertinenti eventi di cibersicurezza;

   c) coordina la gestione degli incidenti e delle crisi su vasta scala e sostiene il processo decisionale a livello politico in merito a tali incidenti e crisi;

   d) discute i piani nazionali di risposta agli incidenti di cibersicurezza di cui all'articolo 7, paragrafo 2;

4. EU-CyCLONe adotta il proprio regolamento interno.

5. EU-CyCLONe riferisce periodicamente al gruppo di cooperazione in merito alle minacce informatiche, agli incidenti e alle tendenze, concentrandosi in particolare sul relativo impatto sui soggetti essenziali e importanti.

6. EU-CyCLONe coopera con la rete di CSIRT sulla base di modalità procedurali concordate.

Articolo 15

Relazione sullo stato della cibersicurezza nell'Unione

1. L'ENISA, in collaborazione con la Commissione, pubblica una relazione biennale sullo stato della cibersicurezza nell'Unione. La relazione comprende in particolare una valutazione dei seguenti aspetti:

   a) lo sviluppo delle capacità di cibersicurezza nell'Unione;

   b) le risorse tecniche, finanziarie e umane a disposizione delle autorità competenti e delle politiche di cibersicurezza, nonché l'attuazione delle misure di vigilanza ed esecuzione alla luce dei risultati delle revisioni tra pari di cui all'articolo 16;

   c) un indice della cibersicurezza che fornisce una valutazione aggregata del livello di maturità delle capacità di cibersicurezza.

2. La relazione contiene raccomandazioni strategiche specifiche per aumentare il livello di cibersicurezza nell'Unione e una sintesi delle conclusioni tratte per quel determinato periodo nelle relazioni sulla situazione tecnica della cibersicurezza nell'Unione elaborate dall'ENISA conformemente all'articolo 7, paragrafo 6, del regolamento (UE) 2019/881.

Articolo 16

Revisioni tra pari

1. La Commissione, previa consultazione del gruppo di cooperazione e dell'ENISA ed entro 18 mesi dall'entrata in vigore della presente direttiva, stabilisce la metodologia e i contenuti di un sistema di revisioni tra pari per valutare l'efficacia delle politiche di cibersicurezza degli Stati membri. Le revisioni sono condotte da esperti tecnici di cibersicurezza provenienti da Stati membri diversi da quello oggetto di revisione e riguardano almeno gli aspetti seguenti:

   i) l'efficacia dell'attuazione delle prescrizioni in materia di gestione e segnalazione dei rischi di cibersicurezza di cui agli articoli 18 e 20;

   ii) il livello delle capacità, comprese le risorse finanziarie, tecniche e umane disponibili, e l'efficacia dello svolgimento dei compiti delle autorità nazionali competenti;

   iii) le capacità e l'efficacia operative dei CSIRT;

   iv) l'efficacia dell'assistenza reciproca di cui all'articolo 34;

   v) l'efficacia del quadro di condivisione delle informazioni di cui all'articolo 26 della presente direttiva.

2. La metodologia comprende criteri obiettivi, non discriminatori, equi e trasparenti sulla base dei quali gli Stati membri designano esperti idonei a eseguire le revisioni tra pari. L'ENISA e la Commissione designano esperti che partecipano alle revisioni tra pari in qualità di osservatori. La Commissione, sostenuta dall'ENISA, stabilisce, nell'ambito della metodologia di cui al paragrafo 1, un sistema obiettivo, non discriminatorio, equo e trasparente per la selezione e l'assegnazione casuale degli esperti a ciascuna revisione tra pari.

3. Gli aspetti organizzativi delle revisioni tra pari sono decisi dalla Commissione con il sostegno dell'ENISA e, previa consultazione del gruppo di cooperazione, si basano su criteri definiti nella metodologia di cui al paragrafo 1. Le revisioni tra pari valutano gli aspetti di cui al paragrafo 1 per tutti gli Stati membri e i settori, comprese questioni mirate specifiche per uno o più Stati membri o uno o più settori.

4. Le revisioni tra pari comportano visite in loco reali o virtuali e scambi a distanza. In virtù del principio di buona collaborazione, gli Stati membri sottoposti a valutazione forniscono agli esperti designati le informazioni richieste necessarie per la valutazione degli aspetti esaminati. Le informazioni ottenute mediante il processo di revisione tra pari sono utilizzate unicamente a tal fine. Gli esperti che partecipano alla revisione tra pari non divulgano a terzi le eventuali informazioni sensibili o riservate ottenute nel corso di tale revisione.

5. Una volta che sono stati valutati in uno Stato membro, i medesimi aspetti non sono più soggetti a ulteriori revisioni tra pari in tale Stato membro nei due anni successivi alla conclusione di tale revisione, a meno che la Commissione, previa consultazione dell'ENISA e del gruppo di cooperazione, non decida altrimenti.

6. Gli Stati membri provvedono affinché gli eventuali rischi di conflitto di interessi riguardanti gli esperti designati siano rivelati agli altri Stati membri, alla Commissione e all'ENISA senza indebito ritardo.

7. Gli esperti che partecipano alle revisioni tra pari elaborano relazioni sui risultati e sulle conclusioni delle revisioni. Le relazioni sono trasmesse alla Commissione, al

gruppo di cooperazione, alla rete di CSIRT e all'ENISA. Le relazioni sono discusse in seno al gruppo di cooperazione e alla rete di CSIRT. Le relazioni possono essere pubblicate sul sito web dedicato del gruppo di cooperazione.

CAPO IV

Obblighi di gestione e segnalazione dei rischi di cibersicurezza

SEZIONE I

Gestione e segnalazione dei rischi di cibersicurezza

Articolo 17

Governance

1. Gli Stati membri provvedono affinché gli organi di gestione dei soggetti essenziali e importanti approvino le misure di gestione dei rischi di cibersicurezza adottate da tali soggetti al fine di conformarsi all'articolo 18, ne vigilino l'attuazione e siano ritenuti responsabili in caso di mancato rispetto, da parte dei soggetti, degli obblighi di cui al presente articolo.
2. Gli Stati membri provvedono affinché i membri dell'organo di gestione seguano periodicamente attività di formazione specifiche al fine di acquisire conoscenze e competenze sufficienti per comprendere e valutare i rischi di cibersicurezza e le relative pratiche di gestione e il loro impatto sulle attività del soggetto.

Articolo 18

Misure di gestione dei rischi di cibersicurezza

1. Gli Stati membri provvedono affinché i soggetti essenziali e importanti adottino misure tecniche e organizzative adeguate e proporzionate per gestire i rischi posti alla sicurezza dei sistemi informatici e di rete che tali soggetti utilizzano nella fornitura dei loro servizi. Tenuto conto delle conoscenze più aggiornate in materia, tali misure assicurano un livello di sicurezza dei sistemi informatici e di rete adeguato al rischio esistente.
2. Le misure di cui al paragrafo 1 comprendono almeno i seguenti elementi:
   a) analisi dei rischi e politiche di sicurezza dei sistemi informatici;
   b) gestione degli incidenti (prevenzione e rilevamento degli incidenti e risposta agli stessi);
   c) continuità operativa e gestione delle crisi;
   d) sicurezza della catena di approvvigionamento, compresi aspetti relativi alla sicurezza riguardanti i rapporti tra ciascun soggetto e i suoi fornitori o fornitori

di servizi, quali i fornitori di servizi di conservazione ed elaborazione dei dati o di servizi di sicurezza gestiti;

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

f) strategie e procedure (test e audit) per valutare l'efficacia delle misure di gestione dei rischi di cibersicurezza;

g) uso della crittografia e della cifratura.

3. Gli Stati membri provvedono affinché, nel prendere in considerazione le misure adeguate di cui al paragrafo 2, lettera d), i soggetti tengano conto delle vulnerabilità specifiche per ogni fornitore e fornitore di servizi e della qualità complessiva dei prodotti e delle pratiche di cibersicurezza dei propri fornitori e fornitori di servizi, comprese le loro procedure di sviluppo sicuro.

4. Gli Stati membri provvedono affinché, qualora un soggetto rilevi che i suoi servizi o i suoi compiti non rispettano le prescrizioni di cui al paragrafo 2, tale soggetto adotti, senza indebito ritardo, tutte le misure correttive necessarie a rendere conforme il servizio interessato.

5. La Commissione può adottare atti di esecuzione al fine di stabilire le specifiche tecniche e metodologiche relative agli elementi di cui al paragrafo 2. Nell'elaborare tali atti la Commissione procede conformemente alla procedura d'esame di cui all'articolo 37, paragrafo 2, e segue, nella maggior misura possibile, le norme internazionali ed europee, nonché le pertinenti specifiche tecniche.

6. Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 36 al fine di integrare gli elementi di cui al paragrafo 2 per tenere conto di nuove minacce informatiche, sviluppi tecnologici o specificità settoriali.

Articolo 19

Valutazioni dei rischi coordinate a livello dell'UE delle catene di approvvigionamento critiche

1. Il gruppo di cooperazione, in collaborazione con la Commissione e l'ENISA, può effettuare valutazioni coordinate dei rischi per la sicurezza di specifiche catene di approvvigionamento critiche di servizi, sistemi o prodotti TIC, tenendo conto dei fattori di rischio tecnici e, se opportuno, non tecnici.

2. La Commissione, previa consultazione del gruppo di cooperazione e dell'ENISA, identifica i servizi, i sistemi o i prodotti TIC critici specifici che possono essere oggetto della valutazione coordinata dei rischi di cui al paragrafo 1.

Articolo 20

Obblighi di segnalazione

1. Gli Stati membri provvedono affinché i soggetti essenziali e importanti notifichino senza indebito ritardo alle autorità competenti o al CSIRT, conformemente ai paragrafi 3 e 4, eventuali incidenti che hanno un impatto significativo sulla fornitura

dei loro servizi. Se opportuno, tali soggetti notificano senza indebito ritardo ai destinatari dei loro servizi gli incidenti che possono ripercuotersi negativamente sulla fornitura di tali servizi. Gli Stati membri provvedono affinché tali soggetti comunichino, tra l'altro, qualunque informazione che consenta alle autorità competenti o al CSIRT di determinare l'eventuale impatto transfrontaliero dell'incidente.

2. Gli Stati membri provvedono affinché i soggetti essenziali e importanti notifichino senza indebito ritardo alle autorità competenti o al CSIRT qualunque minaccia informatica significativa che secondo tali soggetti avrebbe potuto causare un incidente significativo.

   Se opportuno, tali soggetti notificano senza indebito ritardo ai destinatari dei loro servizi che sono potenzialmente interessati da una minaccia informatica significativa qualsiasi misura o azione correttiva che tali destinatari possono adottare in risposta a tale minaccia. Se opportuno, i soggetti notificano a tali destinatari anche la minaccia stessa. La notifica non espone il soggetto che la effettua a una maggiore responsabilità.

3. Un incidente è considerato significativo se:

   a) ha causato o può causare una perturbazione operativa o perdite finanziarie sostanziali per il soggetto interessato;

   b) si è ripercosso o può ripercuotersi su altre persone fisiche o giuridiche causando perdite materiali o immateriali considerevoli.

4. Gli Stati membri provvedono affinché, ai fini della notifica a norma del paragrafo 1, i soggetti interessati trasmettano alle autorità competenti o al CSIRT:

   a) senza indebito ritardo, e comunque entro 24 ore da quando sono venuti a conoscenza dell'incidente, una notifica iniziale che, se opportuno, indichi se l'incidente sia presumibilmente il risultato di un'azione illegittima o malevola;

   b) su richiesta di un'autorità competente o di un CSIRT, una relazione intermedia sui pertinenti aggiornamenti della situazione;

   c) una relazione finale entro un mese dalla trasmissione della notifica di cui alla lettera a), che comprenda almeno:

      i) una descrizione dettagliata dell'incidente, della sua gravità e del suo impatto;

      ii) il tipo di minaccia o la causa di fondo che ha probabilmente innescato l'incidente;

      iii) le misure di attenuazione adottate e in corso.

   Gli Stati membri dispongono che, in casi debitamente giustificati e con l'accordo delle autorità competenti o del CSIRT, il soggetto interessato possa derogare alle scadenze di cui alle lettere a) e c).

5. Entro 24 ore dal ricevimento della notifica iniziale di cui al paragrafo 4, lettera a), le autorità nazionali competenti o il CSIRT forniscono una risposta al soggetto notificante, comprendente un riscontro iniziale sull'incidente e, su richiesta del soggetto, orientamenti sull'attuazione di possibili misure di attenuazione. Se il CSIRT non ha ricevuto la notifica di cui al paragrafo 1, gli orientamenti sono forniti

dall'autorità competente in collaborazione con il CSIRT. Su richiesta del soggetto interessato, il CSIRT fornisce ulteriore supporto tecnico. Qualora si sospetti che l'incidente abbia carattere criminale, le autorità nazionali competenti o il CSIRT forniscono anche orientamenti sulla segnalazione dell'incidente alle autorità di contrasto.

6. Se opportuno, e in particolare se l'incidente di cui al paragrafo 1 interessa due o più Stati membri, l'autorità competente o il CSIRT ne informa gli altri Stati membri interessati e l'ENISA. Nel farlo le autorità competenti, i CSIRT e i punti di contatto unici tutelano, in conformità al diritto dell'Unione o alla legislazione nazionale conforme al diritto dell'Unione, la sicurezza e gli interessi commerciali del soggetto nonché la riservatezza delle informazioni fornite.

7. Qualora sia necessario sensibilizzare il pubblico per evitare un incidente o affrontare un incidente in corso, o qualora la divulgazione dell'incidente sia altrimenti nell'interesse pubblico, dopo aver consultato il soggetto interessato l'autorità competente o il CSIRT e, se opportuno, le autorità o i CSIRT degli altri Stati membri interessati, possono informare il pubblico riguardo all'incidente o imporre al soggetto di farlo.

8. Su richiesta dell'autorità competente o del CSIRT, il punto di contatto unico inoltra le notifiche ricevute a norma dei paragrafi 1 e 2 ai punti di contatto unici degli altri Stati membri interessati.

9. Il punto di contatto unico trasmette mensilmente all'ENISA una relazione di sintesi che comprende dati anonimizzati e aggregati sugli incidenti, sulle minacce informatiche significative e sui quasi incidenti notificati conformemente ai paragrafi 1 e 2 e all'articolo 27. Al fine di contribuire alla fornitura di informazioni comparabili, l'ENISA può pubblicare orientamenti tecnici sui parametri delle informazioni incluse nella relazione di sintesi.

10. Le autorità competenti forniscono alle autorità competenti designate a norma della direttiva (UE) XXXX/XXXX [direttiva sulla resilienza dei soggetti critici] le informazioni sugli incidenti e sulle minacce informatiche notificati conformemente ai paragrafi 1 e 2 dai soggetti essenziali identificati come soggetti critici o come soggetti equivalenti ai soggetti critici a norma della direttiva (UE) XXXX/XXXX [direttiva sulla resilienza dei soggetti critici].

11. La Commissione può adottare atti di esecuzione che specifichino ulteriormente il tipo di informazioni, il relativo formato e la procedura di trasmissione di una notifica a norma dei paragrafi 1 e 2. La Commissione può anche adottare atti di esecuzione al fine di specificare ulteriormente i casi in cui un incidente debba essere considerato significativo come indicato al paragrafo 3. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 37, paragrafo 2.

Articolo 21

Uso dei sistemi europei di certificazione della cibersicurezza

1. Al fine di dimostrare il rispetto di determinate prescrizioni di cui all'articolo 18, gli Stati membri possono imporre ai soggetti essenziali e importanti di certificare determinati prodotti TIC, servizi TIC e processi TIC nell'ambito di specifici sistemi europei di certificazione della cibersicurezza adottati a norma dell'articolo 49 del

regolamento (UE) 2019/881. I prodotti, i servizi e i processi soggetti a certificazione possono essere sviluppati da un soggetto essenziale o importante o acquistati da terze parti.

2. Alla Commissione è conferito il potere di adottare atti delegati che specifichino quali categorie di soggetti essenziali sono tenute a ottenere un certificato e nell'ambito di quali sistemi europei di certificazione della cibersicurezza a norma del paragrafo 1. Gli atti delegati sono adottati conformemente all'articolo 36.

3. Qualora non siano disponibili sistemi di europei di certificazione della cibersicurezza adeguati ai fini del paragrafo 2, la Commissione può chiedere all'ENISA di preparare una proposta di sistema a norma dell'articolo 48, paragrafo 2, del regolamento (UE) 2019/881.

Articolo 22
Normazione

1. Per promuovere l'attuazione convergente dell'articolo 18, paragrafi 1 e 2, gli Stati membri, senza imposizioni o discriminazioni a favore dell'uso di un particolare tipo di tecnologia, incoraggiano l'uso di norme e specifiche europee o accettate a livello internazionale relative alla sicurezza dei sistemi informatici e di rete.

2. L'ENISA, in collaborazione con gli Stati membri, elabora documenti di consulenza e orientamento riguardanti tanto i settori tecnici da prendere in considerazione in relazione al paragrafo 1, quanto le norme già esistenti, comprese le norme nazionali degli Stati membri, che potrebbero essere applicate a tali settori.

Articolo 23

Banche dati di nomi di dominio e dati di registrazione

1. Per contribuire alla sicurezza, alla stabilità e alla resilienza del DNS, gli Stati membri provvedono affinché i registri dei TLD e i soggetti che forniscono servizi di registrazione dei nomi di dominio per i TLD raccolgano e mantengano dati di registrazione dei nomi di dominio accurati e completi in un'apposita banca dati debitamente soggetta al diritto dell'Unione in materia di protezione dei dati per quanto riguarda i dati personali.

2. Gli Stati membri provvedono affinché le banche dati dei dati di registrazione dei nomi di dominio di cui al paragrafo 1 contengano le informazioni pertinenti per identificare e contattare i titolari dei nomi di dominio e i punti di contatto che amministrano i nomi di dominio sotto i TLD.

3. Gli Stati membri provvedono affinché i registri dei TLD e i soggetti che forniscono servizi di registrazione dei nomi di dominio per i TLD predispongano politiche e procedure per garantire che le banche dati comprendano informazioni accurate e complete. Gli Stati membri provvedono affinché tali politiche e procedure siano rese pubbliche.

4. Gli Stati membri provvedono affinché i registri dei TLD e i soggetti che forniscono servizi di registrazione dei nomi di dominio per i TLD pubblichino, senza indebito

ritardo dopo la registrazione di un nome di dominio, i dati di registrazione del dominio che non sono dati personali.

5. Gli Stati membri provvedono affinché i registri dei TLD e i soggetti che forniscono servizi di registrazione dei nomi di dominio per i TLD, su richiesta legittima e debitamente giustificata di legittimi richiedenti l'accesso, forniscano l'accesso a specifici dati di registrazione dei nomi di dominio, nel rispetto del diritto dell'Unione in materia di protezione dei dati. Gli Stati membri provvedono affinché i registri dei TLD e i soggetti che forniscono servizi di registrazione dei nomi di dominio per i TLD rispondano senza indebito ritardo a tutte le richieste di accesso. Gli Stati membri provvedono affinché le politiche e le procedure di divulgazione di tali dati siano rese pubbliche.

Sezione II

Giurisdizione e registrazione

Articolo 24

Giurisdizione e territorialità

1. I fornitori di servizi DNS, i registri dei nomi di dominio di primo livello, i fornitori di servizi di cloud computing, i fornitori di servizi di data center e i fornitori di reti di distribuzione dei contenuti di cui all'allegato I, punto 8, nonché i fornitori di servizi digitali di cui all'allegato II, punto 6, sono considerati sotto la giurisdizione dello Stato membro in cui hanno lo stabilimento principale nell'Unione.

2. Ai fini della presente direttiva, i soggetti di cui al paragrafo 1 sono considerati avere il loro stabilimento principale nell'Unione nello Stato membro in cui sono adottate le decisioni relative alle misure di gestione dei rischi di cibersicurezza. Se tali decisioni non sono adottate in alcuno stabilimento nell'Unione, lo stabilimento principale è considerato essere nello Stato membro in cui i soggetti hanno lo stabilimento con il maggior numero di dipendenti nell'Unione.

3. Se un soggetto di cui al paragrafo 1 non è stabilito nell'Unione, ma offre servizi nell'Unione, esso designa un rappresentante nell'Unione. Il rappresentante è stabilito in uno degli Stati membri in cui sono offerti i servizi. Tale soggetto è considerato sotto la giurisdizione dello Stato membro in cui è stabilito il suo rappresentante. Nell'assenza di un rappresentante designato nell'Unione a norma del presente articolo, qualsiasi Stato membro in cui il soggetto fornisce servizi può avviare un'azione legale nei confronti del soggetto per mancato rispetto degli obblighi di cui alla presente direttiva.

4. La designazione di un rappresentante da parte di un soggetto di cui al paragrafo 1 fa salve le azioni legali che potrebbero essere avviate nei confronti del soggetto stesso.

Articolo 25

Registro dei soggetti essenziali e importanti

1. L'ENISA crea e mantiene un registro dei soggetti essenziali e importanti di cui all'articolo 24, paragrafo 1. Entro il [12 mesi dopo l'entrata in vigore della presente direttiva], i soggetti trasmettono all'ENISA le informazioni seguenti:

a) il proprio nome;

b) l'indirizzo del proprio stabilimento principale e degli altri stabilimenti legali nell'Unione o, se non sono stabiliti nell'Unione, del proprio rappresentante a norma dell'articolo 24, paragrafo 3;

c) i propri dati di contatto aggiornati, compresi gli indirizzi e-mail e i numeri di telefono.

2. I soggetti di cui al paragrafo 1 notificano all'ENISA qualsiasi modifica delle informazioni trasmesse a norma del paragrafo 1 tempestivamente, e in ogni caso entro tre mesi dalla data in cui è avvenuta la modifica.

3. Dopo aver ricevuto le informazioni di cui al paragrafo 1, l'ENISA le inoltra ai punti di contatto unici a seconda dell'ubicazione indicata dello stabilimento principale di ciascun soggetto o, qualora il soggetto non sia stabilito nell'Unione, del rappresentante designato. Se, oltre allo stabilimento principale nell'Unione, un soggetto di cui al paragrafo 1 ha anche ulteriori stabilimenti in altri Stati membri, l'ENISA informa anche i punti di contatto unici di tali Stati membri.

4. Qualora un soggetto non registri la sua attività o non fornisca le pertinenti informazioni entro i termini di cui al paragrafo 1, gli Stati membri in cui il soggetto fornisce servizi sono competenti a provvedere affinché tale soggetto rispetti gli obblighi di cui alla presente direttiva.

CAPO V

Condivisione delle informazioni

Articolo 26

Accordi di condivisione delle informazioni sulla cibersicurezza

1. Fatto salvo il regolamento (UE) 2016/679, gli Stati membri provvedono affinché i soggetti essenziali e importanti possano scambiarsi pertinenti informazioni sulla cibersicurezza, comprese informazioni relative a minacce informatiche, vulnerabilità, indicatori di compromissione, tattiche, tecniche e procedure, allarmi di cibersicurezza e strumenti di configurazione, se tale condivisione di informazioni:

a) mira a prevenire, rilevare o attenuare gli incidenti o a rispondervi;

b) aumenta il livello di cibersicurezza, in particolare sensibilizzando in merito alle minacce informatiche, limitando o inibendo la capacità di diffusione di tali minacce e sostenendo una serie di capacità di difesa, la risoluzione e la divulgazione delle vulnerabilità, tecniche di rilevamento delle minacce, strategie di attenuazione o fasi di risposta e recupero.

2. Gli Stati membri provvedono affinché lo scambio di informazioni avvenga nell'ambito di comunità fidate di soggetti essenziali e importanti. Tale scambio è attuato mediante accordi di condivisione delle informazioni che tengono conto della natura potenzialmente sensibile delle informazioni condivise, nel rispetto delle norme del diritto dell'Unione di cui al paragrafo 1.

3. Gli Stati membri stabiliscono norme che specificano la procedura, gli elementi operativi (compreso l'uso di piattaforme TIC dedicate), i contenuti e le condizioni degli accordi di condivisione delle informazioni di cui al paragrafo 2. Tali norme stabiliscono anche i dettagli relativi alla partecipazione delle autorità pubbliche a tali accordi, nonché agli elementi operativi, compreso l'uso di piattaforme informatiche dedicate. Gli Stati membri offrono sostegno all'applicazione di tali accordi conformemente alle loro misure strategiche di cui all'articolo 5, paragrafo 2, lettera g).

4. I soggetti essenziali e importanti notificano alle autorità competenti la loro partecipazione agli accordi di condivisione delle informazioni di cui al paragrafo 2 al momento della conclusione di tali accordi o, se opportuno, del loro ritiro da tali accordi, una volta che questo è divenuto effettivo.

5. Nel rispetto del diritto dell'Unione, l'ENISA sostiene la conclusione di accordi per la condivisione delle informazioni di cibersicurezza di cui al paragrafo 2 fornendo orientamenti e migliori pratiche.

Articolo 27

Notifica volontaria di informazioni pertinenti

Gli Stati membri provvedono affinché, fatto salvo l'articolo 3, i soggetti che non rientrano nell'ambito di applicazione della presente direttiva possano trasmettere, su base volontaria, notifiche di incidenti significativi, minacce informatiche o quasi incidenti. Nel trattamento delle notifiche gli Stati membri agiscono secondo la procedura di cui all'articolo 20. Gli Stati membri possono trattare le notifiche obbligatorie prioritariamente rispetto alle notifiche volontarie. La segnalazione volontaria non ha l'effetto di imporre al soggetto che la effettua alcun obbligo aggiuntivo a cui non sarebbe stato sottoposto se non avesse trasmesso la notifica.

CAPO VI

Vigilanza ed esecuzione

Articolo 28

Aspetti generali relativi alla vigilanza e all'esecuzione

1. Gli Stati membri provvedono affinché le autorità competenti monitorino efficacemente e adottino le misure necessarie a garantire il rispetto della presente direttiva, in particolare degli obblighi di cui agli articoli 18 e 20.

2. Le autorità competenti operano in stretta cooperazione con le autorità di protezione dei dati nei casi di incidenti che comportano violazioni di dati personali.

Articolo 29

Vigilanza ed esecuzione per i soggetti essenziali

1. Gli Stati membri provvedono affinché le misure di vigilanza o di esecuzione imposte ai soggetti essenziali per quanto riguarda gli obblighi di cui alla presente direttiva siano effettive, proporzionate e dissuasive, tenuto conto delle circostanze di ciascun singolo caso.

2. Gli Stati membri provvedono affinché le autorità competenti, nell'esercizio dei rispettivi compiti di vigilanza nei confronti dei soggetti essenziali, abbiano il potere di sottoporre tali soggetti a:

   a) ispezioni in loco e vigilanza a distanza, compresi controlli casuali;

   b) audit periodici;

   c) audit sulla sicurezza mirati, basati su valutazioni dei rischi o sulle informazioni disponibili relative ai rischi;

   d) scansioni di sicurezza basate su criteri di valutazione dei rischi obiettivi, non discriminatori, equi e trasparenti;

   e) richieste di informazioni necessarie a valutare le misure di cibersicurezza adottate dal soggetto, comprese le politiche di cibersicurezza documentate, nonché il rispetto degli obblighi di notifica all'ENISA a norma dell'articolo 25, paragrafi 1 e 2;

   f) richieste di accesso a dati, documenti o altre informazioni necessari allo svolgimento dei compiti di vigilanza;

   g) richieste di dati che dimostrino l'attuazione di politiche di cibersicurezza, quali i risultati di audit sulla sicurezza effettuati da un controllore qualificato e i relativi elementi di prova.

3. Nell'esercizio dei loro poteri di cui al paragrafo 2, lettere da e) a g), le autorità competenti dichiarano la finalità della richiesta e specificano le informazioni richieste.

4. Gli Stati membri provvedono affinché le autorità competenti, nell'esercizio dei rispettivi poteri di esecuzione nei confronti dei soggetti essenziali, abbiano il potere di:

   a) emanare avvertimenti relativi al mancato rispetto, da parte dei soggetti, degli obblighi stabiliti dalla presente direttiva;

   b) emanare istruzioni vincolanti o un'ingiunzione che impongano a tali soggetti di porre rimedio alle carenze individuate o alle violazioni degli obblighi stabiliti dalla presente direttiva;

   c) imporre a tali soggetti di porre termine al comportamento che non è conforme agli obblighi stabiliti dalla presente direttiva e di astenersi dal ripeterlo;

   d) imporre a tali soggetti di rendere le loro misure di gestione dei rischi e/o i loro obblighi di segnalazione conformi alle prescrizioni di cui agli articoli 18 e 20 in una maniera ed entro un termine specificati;

   e) imporre a tali soggetti di informare le persone fisiche o giuridiche cui forniscono servizi o attività potenzialmente interessati da una minaccia informatica significativa in merito alle eventuali misure protettive o correttive che possano essere adottate da tali persone fisiche o giuridiche in risposta a tale minaccia;

f) imporre a tali soggetti di attuare le raccomandazioni fornite in seguito a un audit sulla sicurezza entro un termine ragionevole;

g) designare un funzionario addetto alla sorveglianza con compiti ben definiti nell'arco di un periodo di tempo determinato al fine di vigilare sul rispetto degli obblighi dei soggetti di cui agli articoli 18 e 20;

h) imporre a tali soggetti di rendere pubblici gli aspetti di mancato rispetto degli obblighi stabiliti dalla presente direttiva in una maniera specificata;

i) rendere una dichiarazione pubblica che identifica le persone fisiche e giuridiche responsabili della violazione di un obbligo stabilito dalla presente direttiva e illustra la natura di tale violazione;

j) imporre o chiedere l'imposizione, da parte degli organismi o degli organi giurisdizionali pertinenti secondo le legislazioni nazionali, di una sanzione amministrativa pecuniaria a norma dell'articolo 31, in aggiunta alle misure di cui al presente paragrafo, lettere da a) a i), o in luogo di tali misure, a seconda delle circostanze di ciascun singolo caso.

5. Qualora le misure di esecuzione adottate a norma del paragrafo 4, lettere da a) a d), e lettera f), si rivelino inefficaci, gli Stati membri provvedono affinché le autorità competenti abbiano il potere di fissare un termine entro il quale il soggetto essenziale è tenuto ad adottare le misure necessarie a porre rimedio alle carenze o a conformarsi alle prescrizioni di tali autorità. Se le misure richieste non sono adottate entro il termine stabilito, gli Stati membri provvedono affinché le autorità competenti abbiano il potere di:

a) sospendere o chiedere a un organismo di certificazione o autorizzazione di sospendere un certificato o un'autorizzazione relativi a una parte o alla totalità dei servizi o delle attività forniti da un soggetto essenziale;

b) imporre o chiedere l'imposizione, da parte degli organismi o degli organi giurisdizionali pertinenti secondo le legislazioni nazionali, di un divieto temporaneo nei confronti di qualsiasi persona che svolga funzioni dirigenziali a livello di amministratore delegato o rappresentante legale in tale soggetto essenziale, e di qualsiasi altra persona fisica ritenuta responsabile della violazione, di svolgere funzioni dirigenziali in tale soggetto.

Tali sanzioni sono applicate solo finché il soggetto non adotta le misure necessarie a porre rimedio alle carenze o a conformarsi alle prescrizioni dell'autorità competente per le quali le sanzioni sono state applicate.

6. Gli Stati membri provvedono affinché qualsiasi persona fisica responsabile di un soggetto essenziale o che agisca in qualità di suo rappresentante sulla base del potere di rappresentarlo, dell'autorità di prendere decisioni per suo conto o dell'autorità di esercitare un controllo su di esso abbia i poteri per garantirne il rispetto degli obblighi stabiliti dalla presente direttiva. Gli Stati membri provvedono affinché tali persone fisiche possano essere ritenute responsabili dell'inadempimento dei loro doveri di garantire il rispetto degli obblighi stabiliti dalla presente direttiva.

7. Nell'adottare qualsiasi misura di esecuzione o nell'applicare qualsiasi sanzione a norma dei paragrafi 4 e 5, le autorità competenti rispettano i diritti di difesa e tengono conto delle circostanze di ciascun singolo caso e almeno degli elementi seguenti:

a) la gravità della violazione e l'importanza delle disposizioni non rispettate. Tra le violazioni che dovrebbero essere considerate gravi rientrano: le violazioni ripetute, la mancata notifica di incidenti con un effetto negativo rilevante o il mancato rimedio a tali incidenti, il mancato rimedio alle carenze a seguito di istruzioni vincolanti emesse dalle autorità competenti, l'ostacolo degli audit o delle attività di monitoraggio imposte dall'autorità competente a seguito del rilevamento di una violazione e la fornitura di informazioni false o gravemente inesatte relative agli obblighi di gestione o segnalazione dei rischi di cui agli articoli 18 e 20;

b) la durata della violazione, compreso l'aspetto relativo alla reiterazione delle violazioni;

c) il danno effettivamente causato o le perdite effettivamente subite, oppure il danno o le perdite potenziali che si sarebbero potuti verificare, nella misura in cui possono essere determinati. Nel valutare tale aspetto si tiene conto, tra l'altro, delle perdite finanziarie o economiche effettive o potenziali, degli effetti sugli altri servizi e del numero di utenti interessati o potenzialmente interessati;

d) il carattere doloso o colposo della violazione;

e) le misure adottate dal soggetto per prevenire o attenuare il danno e/o le perdite;

f) il rispetto dei codici di condotta o dei meccanismi di certificazione approvati;

g) il livello di cooperazione delle persone fisiche o giuridiche ritenute responsabili con le autorità competenti.

8. Le autorità competenti espongono nei particolari la motivazione delle loro decisioni di esecuzione. Prima di adottare tali decisioni le autorità competenti notificano ai soggetti interessati le loro conclusioni preliminari e concedono a tali soggetti un tempo ragionevole per presentare osservazioni.

9. Gli Stati membri provvedono affinché le loro autorità competenti informino le autorità competenti pertinenti dello Stato membro interessato designate a norma della direttiva (UE) XXXX/XXXX [direttiva sulla resilienza dei soggetti critici] quando esercitano i propri poteri di vigilanza ed esecuzione finalizzati a garantire il rispetto degli obblighi stabiliti dalla presente direttiva da parte di un soggetto essenziale identificato come critico o come soggetto equivalente a un soggetto critico a norma della direttiva (UE) XXXX/XXXX [direttiva sulla resilienza dei soggetti critici]. Su richiesta delle autorità competenti di cui alla direttiva (UE) XXXX/XXXX [direttiva sulla resilienza dei soggetti critici], le autorità competenti possono esercitare i propri poteri di vigilanza ed esecuzione nei confronti di un soggetto essenziale identificato come critico o equivalente.

Articolo 30

Vigilanza ed esecuzione per i soggetti importanti

1. Se ricevono elementi di prova o indicazioni che un soggetto importante non rispetta gli obblighi stabiliti dalla presente direttiva, in particolare dagli articoli 18 e 20, gli Stati membri provvedono affinché le autorità competenti intervengano, se necessario, mediante misure di vigilanza ex post.

2. Gli Stati membri provvedono affinché le autorità competenti, nell'esercizio dei rispettivi compiti di vigilanza nei confronti dei soggetti importanti, abbiano il potere di sottoporre tali soggetti a:

   a) ispezioni in loco e vigilanza ex post a distanza;

   b) audit sulla sicurezza mirati, basati su valutazioni dei rischi o sulle informazioni disponibili relative ai rischi;

   c) scansioni di sicurezza basate su criteri di valutazione dei rischi obiettivi, equi e trasparenti;

   d) richieste di qualsiasi informazione necessaria a valutare ex post le misure di cibersicurezza, comprese le politiche di cibersicurezza documentate, nonché il rispetto degli obblighi di notifica all'ENISA a norma dell'articolo 25, paragrafi 1 e 2;

   e) richieste di accesso a dati, documenti e/o informazioni necessari allo svolgimento dei compiti di vigilanza;

3. Nell'esercizio dei loro poteri a norma del paragrafo 2, lettere d) o e), le autorità competenti dichiarano la finalità della richiesta e specificano le informazioni richieste.

4. Gli Stati membri provvedono affinché le autorità competenti, nell'esercizio dei rispettivi poteri di esecuzione nei confronti dei soggetti importanti, abbiano il potere di:

   a) emanare avvertimenti relativi al mancato rispetto, da parte dei soggetti, degli obblighi stabiliti dalla presente direttiva;

   b) emanare istruzioni vincolanti o un'ingiunzione che impongano a tali soggetti di porre rimedio alle carenze individuate o alla violazione degli obblighi stabiliti dalla presente direttiva;

   c) imporre a tali soggetti di porre termine al comportamento che non rispetta gli obblighi stabiliti dalla presente direttiva e di astenersi dal ripeterlo;

   d) imporre a tali soggetti di rendere le loro misure di gestione dei rischi o i loro obblighi di segnalazione conformi alle prescrizioni di cui agli articoli 18 e 20 in una maniera ed entro un termine specificati;

   e) imporre a tali soggetti di informare le persone fisiche o giuridiche cui forniscono servizi o attività potenzialmente interessati da una minaccia informatica significativa in merito alle eventuali misure protettive o correttive che possano essere adottate da tali persone fisiche o giuridiche in risposta a tale minaccia;

   f) imporre a tali soggetti di attuare le raccomandazioni fornite in seguito a un audit sulla sicurezza entro un termine ragionevole;

   g) imporre a tali soggetti di rendere pubblici gli aspetti di mancato rispetto dei loro obblighi stabiliti dalla presente direttiva in una maniera specificata;

   h) rendere una dichiarazione pubblica che identifica le persone fisiche e giuridiche responsabili della violazione di un obbligo stabilito dalla presente direttiva e illustra la natura di tale violazione;

i) imporre o chiedere l'imposizione, da parte degli organismi o degli organi giurisdizionali pertinenti secondo le legislazioni nazionali, di una sanzione amministrativa pecuniaria a norma dell'articolo 31, in aggiunta alle misure di cui al presente paragrafo, lettere da a) a h), o in luogo di tali misure, a seconda delle circostanze di ciascun singolo caso.

5. L'articolo 29, paragrafi da 6 a 8, si applica anche alle misure di vigilanza ed esecuzione di cui al presente articolo per i soggetti importanti di cui all'allegato II.

Articolo 31

Condizioni generali per imporre sanzioni amministrative pecuniarie ai soggetti essenziali e importanti

1. Gli Stati membri provvedono affinché le sanzioni amministrative pecuniarie imposte ai soggetti essenziali e importanti a norma del presente articolo in relazione alle violazioni degli obblighi stabiliti dalla presente direttiva siano, in ciascun singolo caso, effettive, proporzionate e dissuasive.

2. Le sanzioni amministrative pecuniarie sono imposte, a seconda delle circostanze di ciascun singolo caso, in aggiunta alle misure di cui all'articolo 29, paragrafo 4, lettere da a) a i), all'articolo 29, paragrafo 5, e all'articolo 30, paragrafo 4, lettere da a) a h), o in luogo di tali misure.

3. Nel decidere se imporre una sanzione amministrativa pecuniaria e il relativo importo in ciascun singolo caso si tiene debitamente conto almeno degli elementi di cui all'articolo 29, paragrafo 7.

4. Gli Stati membri provvedono affinché le violazioni degli obblighi di cui all'articolo 18 o all'articolo 20 siano, conformemente ai paragrafi 2 e 3 del presente articolo, soggette a sanzioni pecuniarie amministrative pari a un massimo di almeno 10 000 000 EUR o fino al 2 % del totale del fatturato mondiale annuo per l'esercizio precedente dell'impresa cui il soggetto essenziale o importante appartiene, se tale importo è superiore.

5. Gli Stati membri possono prevedere la facoltà di infliggere penalità di mora al fine di imporre a un soggetto essenziale o importante di cessare una violazione conformemente a una precedente decisione dell'autorità competente.

6. Fatti salvi i poteri delle autorità competenti a norma degli articoli 29 e 30, ogni Stato membro può prevedere norme che dispongano se e in quale misura possono essere imposte sanzioni amministrative pecuniarie agli enti della pubblica amministrazione di cui all'articolo 4, punto 23, soggetti agli obblighi previsti dalla presente direttiva.

Articolo 32

Violazioni che comportano una violazione dei dati personali

1. Qualora le autorità competenti dispongano di elementi che indicano che la violazione da parte di un soggetto essenziale o importante degli obblighi di cui agli articoli 18 e 20 comporta una violazione dei dati personali, quale definita all'articolo 4, punto 12, del regolamento (UE) 2016/679, che deve essere notificata a norma dell'articolo 33

del medesimo regolamento, ne informano le autorità di controllo competenti a norma degli articoli 55 e 56 di tale regolamento entro un termine ragionevole.

2. Qualora le autorità di controllo competenti conformemente agli articoli 55 e 56 del regolamento (UE) 2016/679 decidano di esercitare i propri poteri a norma dell'articolo 58, paragrafo 2, lettera i), del medesimo regolamento e di imporre una sanzione amministrativa pecuniaria, le autorità competenti non impongono una sanzione amministrativa pecuniaria per la stessa violazione a norma dell'articolo 31 della presente direttiva. Le autorità competenti possono tuttavia applicare le misure di esecuzione o esercitare i poteri sanzionatori di cui all'articolo 29, paragrafo 4, lettere da a) a i), all'articolo 29, paragrafo 5, e all'articolo 30, paragrafo 4, lettere da a) ad h), della presente direttiva.

3. Qualora l'autorità di controllo competente a norma del regolamento (UE) 2016/679 sia stabilita in uno Stato membro diverso rispetto all'autorità competente, l'autorità competente può informare l'autorità di controllo stabilita nello stesso Stato membro.

Articolo 33

Sanzioni

1. Gli Stati membri stabiliscono le norme relative alle sanzioni applicabili in caso di violazione delle disposizioni nazionali adottate a norma della presente direttiva e adottano tutte le misure necessarie per assicurarne l'attuazione. Le sanzioni previste sono effettive, proporzionate e dissuasive.

2. Gli Stati membri notificano tali norme e misure alla Commissione, entro [due] anni dall'entrata in vigore della presente direttiva, e provvedono poi a dare notifica, senza indebito ritardo, delle eventuali modifiche successive.

Articolo 34

Assistenza reciproca

1. Se un soggetto essenziale o importante fornisce servizi in più di uno Stato membro o ha lo stabilimento principale o un rappresentante in uno Stato membro, ma i suoi sistemi informatici e di rete sono ubicati in uno o più altri Stati membri, l'autorità competente dello Stato membro dello stabilimento principale o di un altro stabilimento o del rappresentante e le autorità competenti dei suddetti altri Stati membri cooperano e si assistono reciprocamente in funzione delle necessità. Tale cooperazione comprende, almeno, gli aspetti seguenti:

   a) le autorità competenti che applicano misure di vigilanza o di esecuzione in uno Stato membro informano e consultano, attraverso il punto di contatto unico, le autorità competenti degli altri Stati membri interessati in merito alle misure di vigilanza ed esecuzione adottate e al seguito dato a tali misure, conformemente agli articoli 29 e 30;

   b) un'autorità competente può chiedere a un'altra autorità competente di adottare le misure di vigilanza o esecuzione di cui agli articoli 29 e 30;

   c) un'autorità competente, dopo aver ricevuto una richiesta giustificata da un'altra autorità competente, fornisce a tale altra autorità competente assistenza

affinché le misure di vigilanza o esecuzione di cui agli articoli 29 e 30 possano essere attuate in maniera efficace, efficiente e coerente. Tale assistenza reciproca può riguardare richieste di informazioni e misure di vigilanza, comprese richieste di effettuare ispezioni in loco o vigilanza a distanza o audit sulla sicurezza mirati. Un'autorità competente destinataria di una richiesta di assistenza non può respingerla a meno che, a seguito di uno scambio con le altre autorità interessate, l'ENISA e la Commissione non sia stabilito che l'autorità non è competente per fornire l'assistenza richiesta, o che l'assistenza richiesta non è proporzionata ai compiti di vigilanza svolti dall'autorità competente conformemente agli articoli 29 e 30.

2. Se opportuno e di comune accordo le autorità competenti di diversi Stati membri possono svolgere le attività di vigilanza comuni di cui agli articoli 29 e 30.

CAPO VII

Disposizioni transitorie e finali

Articolo 35

Riesame

La Commissione riesamina periodicamente il funzionamento della presente direttiva e presenta una relazione in proposito al Parlamento europeo e al Consiglio. La relazione valuta in particolare la pertinenza dei settori, dei sottosettori, delle dimensioni e dei tipi di soggetti di cui agli allegati I e II per il funzionamento dell'economia e della società in relazione alla cibersicurezza. A tal fine e allo scopo di intensificare ulteriormente la cooperazione strategica e operativa, la Commissione tiene conto delle relazioni del gruppo di cooperazione e della rete di CSIRT sull'esperienza acquisita a livello strategico e operativo. La prima relazione è presentata entro il … [54 mesi dopo la data di entrata in vigore della presente direttiva].

Articolo 36

Esercizio della delega

1. Il potere di adottare atti delegati è conferito alla Commissione alle condizioni stabilite nel presente articolo.

2. Il potere di adottare atti delegati di cui all'articolo 18, paragrafo 6, e all'articolo 21, paragrafo 2, è conferito alla Commissione per un periodo di cinque anni a decorrere dal [...].

3. La delega di potere di cui all'articolo 18, paragrafo 6, e all'articolo 21, paragrafo 2, può essere revocata in qualsiasi momento dal Parlamento europeo o dal Consiglio. La decisione di revoca pone fine alla delega di potere ivi specificata. Gli effetti della decisione decorrono dal giorno successivo alla pubblicazione della decisione nella *Gazzetta ufficiale dell'Unione europea* o da una data successiva ivi specificata. Essa non pregiudica la validità degli atti delegati già in vigore.

4. Prima dell'adozione di un atto delegato la Commissione consulta gli esperti designati da ciascuno Stato membro nel rispetto dei principi stabiliti nell'accordo interistituzionale "Legiferare meglio" del 13 aprile 2016.

5. Non appena adotta un atto delegato, la Commissione ne dà contestualmente notifica al Parlamento europeo e al Consiglio.

6. L'atto delegato adottato a norma dell'articolo 18, paragrafo 6, e dell'articolo 21, paragrafo 2, entra in vigore solo se né il Parlamento europeo né il Consiglio hanno sollevato obiezioni entro il termine di due mesi dalla data in cui esso è stato loro notificato o se, prima della scadenza di tale termine, sia il Parlamento europeo che il Consiglio hanno informato la Commissione che non intendono sollevare obiezioni. Tale termine è prorogato di due mesi su iniziativa del Parlamento europeo o del Consiglio.

Articolo 37

Procedura di comitato

1. La Commissione è assistita da un comitato. Esso è un comitato ai sensi del regolamento (UE) n. 182/2011.

2. Nei casi in cui è fatto riferimento al presente paragrafo, si applica l'articolo 5 del regolamento (UE) n. 182/2011.

3. Laddove il parere del comitato debba essere ottenuto con procedura scritta, questa si conclude senza esito quando, entro il termine per la formulazione del parere, il presidente del comitato decida in tal senso o un membro del comitato lo richieda.

Articolo 38

Recepimento

1. Gli Stati membri adottano e pubblicano entro … [18 mesi dopo la data di entrata in vigore della presente direttiva] le disposizioni legislative, regolamentari e amministrative necessarie per conformarsi alla presente direttiva. Essi ne informano immediatamente la Commissione. Essi applicano tali disposizioni a decorrere dal … [un giorno dopo la data di cui al primo comma].

2. Le disposizioni adottate dagli Stati membri contengono un riferimento alla presente direttiva o sono corredate di tale riferimento all'atto della pubblicazione ufficiale. Le modalità del riferimento sono stabilite dagli Stati membri.

Articolo 39

Modifica del regolamento (UE) n. 910/2014

L'articolo 19 del regolamento (UE) n. 910/2014 è soppresso.

Articolo 40

Modifica della direttiva (UE) 2018/1972

Gli articoli 40 e 41 della direttiva (UE) 2018/1972 sono soppressi.

Articolo 41

Abrogazione

La direttiva (UE) 2016/1148 è abrogata a decorrere dal ... [termine per il recepimento della presente direttiva].

I riferimenti alla direttiva (UE) 2016/1148 si intendono fatti alla presente direttiva e si leggono secondo la tavola di concordanza di cui all'allegato III.

Articolo 42

Entrata in vigore

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

Articolo 43

Destinatari

Gli Stati membri sono destinatari della presente direttiva.

Fatto a Bruxelles, il

Per il Parlamento europeo	*Per il Consiglio*
Il presidente	*Il presidente*

SCHEDA FINANZIARIA LEGISLATIVA

INDICE

1. CONTESTO DELLA PROPOSTA/INIZIATIVA 2
1.1. Titolo della proposta/iniziativa Titolo della proposta/iniziativa 2
1.2. Settore/settori interessati *(cluster di programmi)* 2
1.3. La proposta/iniziativa riguarda: 2
1.4. Motivazione della proposta/iniziativa 2
1.4.1. Necessità nel breve e lungo termine, compreso un calendario dettagliato per fasi di attuazione dell'iniziativa 2
1.4.2. Valore aggiunto dell'intervento dell'Unione (che può derivare da diversi fattori, ad es. un miglior coordinamento, la certezza del diritto, maggiore efficacia o maggiori complementarità). Ai fini del presente punto, per "valore aggiunto dell'intervento dell'Unione" si intende il valore derivante dall'intervento dell'Unione che va ad aggiungersi al valore che avrebbero altrimenti generato gli Stati membri se avessero agito da soli. 2
1.4.3. Insegnamenti tratti da esperienze analoghe 3
1.4.4. Compatibilità ed eventuale sinergia con altri strumenti pertinenti 3
1.5. Durata e incidenza finanziaria 4
1.6. Modalità di gestione previste 4
2. MISURE DI GESTIONE 6
2.1. Disposizioni in materia di monitoraggio e di relazioni 6
2.2. Sistema di gestione e di controllo 6
2.2.1. Giustificazione della o delle modalità di gestione, del meccanismo o dei meccanismi di attuazione del finanziamento, delle modalità di pagamento e della strategia di controllo proposti 6
2.2.2. Informazioni concernenti i rischi individuati e il sistema o i sistemi di controllo interno per ridurli 6
2.2.3. Stima e giustificazione del rapporto costo/efficacia dei controlli (rapporto "costi del controllo ÷ valore dei fondi gestiti") e valutazione dei livelli di rischio di errore previsti (al pagamento e alla chiusura) 6
2.3. Misure di prevenzione delle frodi e delle irregolarità 6
3. INCIDENZA FINANZIARIA PREVISTA DELLA PROPOSTA/INIZIATIVA 7
3.1. Rubrica del quadro finanziario pluriennale e nuova o nuove linee di bilancio di spesa proposte 7
3.2. Incidenza prevista sulle spese 8
3.2.1. Sintesi dell'incidenza prevista sulle spese 8
3.2.2. Sintesi dell'incidenza prevista sugli stanziamenti amministrativi 11
3.2.3. Partecipazione di terzi al finanziamento 13
3.3. Incidenza prevista sulle entrate 13

1. CONTESTO DELLA PROPOSTA/INIZIATIVA

1.1. Titolo della proposta/iniziativa Titolo della proposta/iniziativa

Proposta di direttiva relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, che abroga la direttiva (UE) 2016/1148

1.2. Settore/settori interessati *(cluster di programmi)*

Reti, contenuti e tecnologie delle comunicazioni

1.3. La proposta/iniziativa riguarda:

☐ **una nuova azione**

☐ **una nuova azione a seguito di un progetto pilota/un'azione preparatoria**[40]

☒ **la proroga di un'azione esistente**

☐ **la fusione o il riorientamento di una o più azioni verso un'altra/una nuova azione**

1.4. Motivazione della proposta/iniziativa

1.4.1. Necessità nel breve e lungo termine, compreso un calendario dettagliato per fasi di attuazione dell'iniziativa

L'obiettivo del riesame è aumentare il livello di ciberresilienza di un vasto gruppo di imprese operanti nell'Unione europea in tutti i settori pertinenti, ridurre le incongruenze in termini di resilienza del mercato interno nei settori già contemplati dalla direttiva e migliorare il livello di consapevolezza situazionale comune e la capacità collettiva di preparazione e risposta.

1.4.2. Valore aggiunto dell'intervento dell'Unione (che può derivare da diversi fattori, ad es. un miglior coordinamento, la certezza del diritto, maggiore efficacia o maggiori complementarità). Ai fini del presente punto, per "valore aggiunto dell'intervento dell'Unione" si intende il valore derivante dall'intervento dell'Unione che va ad aggiungersi al valore che avrebbero altrimenti generato gli Stati membri se avessero agito da soli.

La resilienza in termini di cibersicurezza all'interno dell'Unione non può essere efficace se affrontata in modo diverso nei vari silos nazionali o regionali. La direttiva NIS ha ovviato a questa carenza definendo un quadro per la sicurezza delle reti e dei sistemi informativi a livello nazionale e dell'Unione. Tuttavia, il primo riesame periodico della direttiva NIS ha evidenziato alcuni difetti intrinseci, i quali hanno portato a considerevoli disparità tra gli Stati membri in termini di capacità, pianificazione e livello di protezione, che interessano al contempo la parità di condizioni per imprese analoghe sul mercato interno. L'intervento dell'UE, che va oltre le attuali misure della direttiva NIS, è giustificato principalmente dai seguenti fattori: i) la natura transfrontaliera del problema; ii) le potenzialità degli interventi dell'UE volti a migliorare e agevolare strategie nazionali efficaci; iii) il contributo degli interventi strategici concertati e collaborativi della NIS volti a un'efficace protezione dei dati e della vita privata.

[40] A norma dell'articolo 58, paragrafo 2, lettera a) o b), del regolamento finanziario.

Gli obiettivi enunciati possono quindi essere conseguiti meglio con un'azione a livello dell'UE piuttosto che con l'azione dei singoli Stati membri.

1.4.3. Insegnamenti tratti da esperienze analoghe

La direttiva NIS è il primo strumento orizzontale del mercato interno volto a migliorare la resilienza di reti e sistemi nell'Unione rispetto ai rischi di cibersicurezza. Ha già contribuito notevolmente a innalzare il livello comune di cibersicurezza tra gli Stati membri. Il riesame del funzionamento e dell'attuazione della direttiva ha tuttavia evidenziato alcune carenze che, oltre all'aumento della digitalizzazione e alla necessità di risposte più aggiornate, devono essere affrontate nel quadro di un atto giuridico rivisto.

1.4.4. Compatibilità ed eventuale sinergia con altri strumenti pertinenti

La nuova proposta è pienamente coerente con altre iniziative affini, quali la proposta di regolamento relativo alla resilienza operativa digitale per il settore finanziario e la proposta di direttiva sulla resilienza degli operatori critici di servizi essenziali, nonché con il codice europeo delle comunicazioni elettroniche, il regolamento generale sulla protezione dei dati e il regolamento eIDAS.

La proposta è una parte essenziale della strategia dell'UE per l'Unione della sicurezza.

1.5. Durata e incidenza finanziaria

☐ **durata limitata**

– ☐ in vigore a decorrere dal [GG/MM]AAAA fino al [GG/MM]AAAA;

– ☐ incidenza finanziaria dal AAAA al AAAA per gli stanziamenti di impegno e dal AAAA al AAAA per gli stanziamenti di pagamento.

☒ **durata illimitata**

– attuazione con un periodo di avviamento dal 2022 al 2025;

– successivo funzionamento a pieno ritmo.

1.6. Modalità di gestione previste[41]

Gestione diretta a opera della Commissione

– ☒ a opera dei suoi servizi, compreso il suo personale presso le delegazioni dell'Unione;

– ☐ a opera delle agenzie esecutive;

☐ **Gestione concorrente** con gli Stati membri

☐ **Gestione indiretta** affidando compiti di esecuzione del bilancio:

– ☐ a paesi terzi o organismi da questi designati;

– ☐ a organizzazioni internazionali e loro agenzie (specificare);

– ☐ alla BEI e al Fondo europeo per gli investimenti;

– X☐ agli organismi di cui agli articoli 70 e 71 del regolamento finanziario;

– ☐ a organismi di diritto pubblico;

– ☐ a organismi di diritto privato investiti di attribuzioni di servizio pubblico nella misura in cui sono dotati di sufficienti garanzie finanziarie;

– ☐ a organismi di diritto privato di uno Stato membro preposti all'attuazione di un partenariato pubblico-privato e che sono dotati di sufficienti garanzie finanziarie;

– ☐ alle persone incaricate di attuare azioni specifiche della PESC a norma del titolo V del TUE e indicate nel pertinente atto di base.

– *Se è indicata più di una modalità, fornire ulteriori informazioni alla voce "Osservazioni".*

Osservazioni

L'Agenzia dell'Unione europea per la cibersicurezza, ENISA, alla quale con il regolamento sulla cibersicurezza è stato conferito un nuovo mandato permanente, assisterebbe gli Stati membri e la Commissione nell'attuazione della direttiva NIS rivista.

Per effetto della direttiva NIS rivista, dal 2022/2023 l'ENISA avrà ulteriori settori d'intervento. Sebbene tali settori d'intervento siano compresi nei compiti generali dell'ENISA in base al suo mandato, essi determineranno un carico di lavoro supplementare per l'agenzia. Più precisamente, oltre ai suoi settori d'intervento attuali, in base alla proposta della Commissione relativa alla direttiva NIS rivista, l'ENISA dovrà includere specificamente nel

[41] Le spiegazioni sulle modalità di gestione e i riferimenti al regolamento finanziario sono disponibili sul sito BudgWeb: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx.

suo programma di lavoro tra le altre azioni, le seguenti: i) sviluppare e mantenere un registro europeo delle vulnerabilità (articolo 6, paragrafo 2, della proposta), ii) assicurare il segretariato della rete europea delle organizzazioni di collegamento per le crisi informatiche (CyCLONe) (articolo 14 della proposta) e pubblicare una relazione annuale sullo stato della cibersicurezza nell'UE (articolo 15 della proposta), iii) sostenere l'organizzazione di revisioni tra pari tra Stati membri (articolo 16 della proposta), iv) raccogliere dati aggregati sugli incidenti dagli Stati membri e pubblicare orientamenti tecnici (articolo 20, paragrafo 9, della proposta), v) creare e mantenere un registro per soggetti che prestano servizi transfrontalieri (articolo 25 della proposta).

Pertanto, a partire dal 2022 sarà presentata una richiesta di altri 5 ETP con un bilancio corrispondente di circa 0,61 milioni di EUR l'anno a copertura di tali nuovi posti (cfr. scheda finanziaria separata per le agenzie).

2. MISURE DI GESTIONE

2.1. Disposizioni in materia di monitoraggio e di relazioni

Precisare frequenza e condizioni.

La Commissione riesaminerà periodicamente il funzionamento della direttiva e presenterà una relazione al Parlamento europeo e al Consiglio, la prima volta tre anni dopo l'entrata in vigore.

La Commissione valuterà anche il corretto recepimento della direttiva da parte degli Stati membri.

2.2. Sistema di gestione e di controllo

2.2.1. Giustificazione della o delle modalità di gestione, del meccanismo o dei meccanismi di attuazione del finanziamento, delle modalità di pagamento e della strategia di controllo proposti

L'unità della DG CNECT incaricata del settore gestirà l'attuazione della direttiva.

2.2.2. Informazioni concernenti i rischi individuati e il sistema o i sistemi di controllo interno per ridurli

Rischio molto basso, in quanto l'ecosistema della direttiva NIS è già esistente.

2.2.3. Stima e giustificazione del rapporto costo/efficacia dei controlli (rapporto "costi del controllo ÷ valore dei fondi gestiti") e valutazione dei livelli di rischio di errore previsti (al pagamento e alla chiusura)

Non pertinente. Utilizzo del solo bilancio amministrativo ("dotazione globale").

2.3. Misure di prevenzione delle frodi e delle irregolarità

Precisare le misure di prevenzione e tutela in vigore o previste, ad esempio strategia antifrode.

Non pertinente. Utilizzo del solo bilancio amministrativo ("dotazione globale").

3. INCIDENZA FINANZIARIA PREVISTA DELLA PROPOSTA/INIZIATIVA

3.1. Rubrica del quadro finanziario pluriennale e nuova o nuove linee di bilancio di spesa proposte

Rubrica del quadro finanziario pluriennale	Linea di bilancio	Natura della spesa	Partecipazione			
	Numero [Rubrica…7……...……]	Diss./Non diss.[42]	di paesi EFTA[43]	di paesi candidati[44]	di paesi terzi	ai sensi dell'articolo [21, paragrafo 2, lettera b)], del regolamento finanziario
	20 02 06 spese di gestione 20 02 06	Non diss.	NO	NO	NO	NO

[42] Diss. = stanziamenti dissociati / Non diss. = stanziamenti non dissociati.

[43] EFTA: Associazione europea di libero scambio.

[44] Paesi candidati e, se del caso, potenziali candidati dei Balcani occidentali.

3.2. Incidenza prevista sulle spese

3.2.1. Sintesi dell'incidenza prevista sulle spese

Mio EUR (al terzo decimale)

Rubrica del quadro finanziario pluriennale	**<…>**	[Rubrica……...……]

			2021	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	***Periodo successivo al 2027***	**TOTALE**
Stanziamenti operativi (suddivisi in base alle linee di bilancio di cui al punto 3.1)	Impegni	(1)									
	Pagamenti	(2)									
Stanziamenti amministrativi finanziati dalla dotazione del programma[45]	Impegni = Pagamenti	(3)									
TOTALE degli stanziamenti per la dotazione del programma	Impegni	=1+3									
	Pagamenti	=2+3									

Rubrica del quadro finanziario pluriennale	7	"Spese amministrative" Riunioni: le riunioni plenarie del gruppo di cooperazione NIS si svolgono solitamente quattro volte l'anno. La Commissione copre i costi legati alle spese di ristorazione e viaggio dei rappresentanti dei 27 Stati membri (un rappresentante per Stato membro). I costi di una riunione potrebbero raggiungere i 15 000 EUR. Missioni: Le missioni sono legate al monitoraggio dell'attuazione della direttiva NIS. Esempio: In un anno (maggio 2019 - luglio 2020) avremmo dovuto organizzare le

[45] Assistenza tecnica e/o amministrativa e spese di sostegno all'attuazione di programmi e/o azioni dell'UE (ex linee "BA"), ricerca indiretta, ricerca diretta.

		cosiddette "visite nei paesi in relazione alla NIS" e visitare tutti i 27 Stati membri per discutere dell'attuazione della direttiva NIS in tutta l'UE.

Sezione da compilare utilizzando i "dati di bilancio di natura amministrativa" che saranno introdotti nell'allegato della scheda finanziaria legislativa, caricato su DECIDE a fini di consultazione interservizi.

Mio EUR (al terzo decimale)

		2021	2022	2023	2024	2025	2026	2027	*Periodo successivo al 2027*	TOTALE
Risorse umane		1,14	1,14	1,14	1,14	1,14	1,14	**1,14**		**7,98**
Altre spese amministrative		**0,09**	**0,09**	**0,09**	**0,09**	**0,09**	**0,09**	**0,09**		**0,63**
TOTALE degli stanziamenti per la RUBRICA 7 del quadro finanziario pluriennale	(Totale impegni = Totale pagamenti)	**1,23**	**1,23**	**1,23**	**1,23**	**1,23**	**1,23**	**1,23**		**8,61**

Mio EUR (al terzo decimale)

		2021	2022	2023	2024	2025	2026	2027	*Periodo successivo al 2027*	TOTALE
TOTALE degli stanziamenti per tutte le RUBRICHE del quadro finanziario pluriennale	Impegni									
	Pagamenti									

3.2.2. Sintesi dell'incidenza prevista sugli stanziamenti amministrativi

– ☐ La proposta/iniziativa non comporta l'utilizzo di stanziamenti amministrativi.

– ☐X La proposta/iniziativa comporta l'utilizzo di stanziamenti amministrativi, come spiegato di seguito:

Mio EUR (al terzo decimale)

Anni	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**TOTALE**
RUBRICA 7 del quadro finanziario pluriennale								
Risorse umane	1,14	1,14	1,14	1,14	1,14	1,14	**1,14**	**7,98**
Altre spese amministrative	0,09	0,09	0,09	0,09	0,09	0,09	**0,09**	**0,63**
Totale parziale della RUBRICA 7 del quadro finanziario pluriennale	1,23	1,23	1,23	1,23	1,23	1,23	**1,23**	**8,61**

Esclusa la RUBRICA 7[46] del quadro finanziario pluriennale								
Risorse umane								
Altre spese di natura amministrativa								
Totale parziale esclusa la RUBRICA 7 del quadro finanziario pluriennale								

TOTALE	**1,23**	**1,23**	**1,23**	**1,23**	**1,23**	**1,23**	**1,23**	**8,61**

Il fabbisogno di stanziamenti relativi alle risorse umane e alle altre spese di natura amministrativa è coperto dagli stanziamenti della DG già assegnati alla gestione dell'azione e/o riassegnati all'interno della stessa DG, integrati dall'eventuale dotazione supplementare concessa alla DG responsabile nell'ambito della procedura annuale di assegnazione, tenendo conto dei vincoli di bilancio.

[46] Assistenza tecnica e/o amministrativa e spese di sostegno all'attuazione di programmi e/o azioni dell'UE (ex linee "BA"), ricerca indiretta, ricerca diretta.

3.2.2.1. Fabbisogno previsto di risorse umane

– ☐ La proposta/iniziativa non comporta l'utilizzo di risorse umane.

– X☐ La proposta/iniziativa comporta l'utilizzo di risorse umane, come spiegato di seguito:

Stima da esprimere in equivalenti a tempo pieno

Anni		**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**
•Posti della tabella dell'organico (funzionari e agenti temporanei)								
In sede e negli uffici di rappresentanza della Commissione		6	6	6	6	6	6	6
Delegazioni								
Ricerca								
• Personale esterno (in equivalenti a tempo pieno: ETP) - AC, AL, END, INT e JED [47] Rubrica 7								
Finanziato dalla RUBRICA 7 del quadro finanziario pluriennale	- in sede	3	3	3	3	3	3	3
	- nelle delegazioni							
Finanziato dalla dotazione del programma [48]	- in sede							
	- nelle delegazioni							
Ricerca								
Altro (specificare)								
TOTALE		**9**	**9**	**9**	**9**	**9**	**9**	**9**

Il fabbisogno di risorse umane è coperto dal personale della DG già assegnato alla gestione dell'azione e/o riassegnato all'interno della stessa DG, integrato dall'eventuale dotazione supplementare concessa alla DG responsabile nell'ambito della procedura annuale di assegnazione, tenendo conto dei vincoli di bilancio.

Descrizione dei compiti da svolgere:

Funzionari e agenti temporanei	• preparazione di atti delegati in conformità all'articolo 18, paragrafo 6, all'articolo 21, paragrafo 2 e all'articolo 36; • preparazione di atti di esecuzione in conformità all'articolo 12, paragrafo 8, all'articolo 18, paragrafo 5 e all'articolo 20, paragrafo 11; • assicurare il segretariato per il gruppo di cooperazione NIS; • organizzazione delle riunioni plenarie del gruppo di cooperazione NIS e delle riunioni dedicate ai flussi di lavoro; • coordinazione dei lavori degli Stati membri su vari documenti (orientamenti, pacchetti di strumenti, ecc.); • collegamento con altri servizi della Commissione, con l'ENISA e con le autorità nazionali in vista dell'attuazione della direttiva NIS; • analisi dei metodi nazionali e delle migliori pratiche legati all'attuazione della direttiva NIS.
Personale esterno	Supporto a tutti i compiti sopra illustrati in funzione delle necessità

[47] AC = agente contrattuale; AL = agente locale; END = esperto nazionale distaccato; INT = personale interinale (intérimaire); JPD = giovane professionista in delegazione.

[48] Sottomassimale per il personale esterno previsto dagli stanziamenti operativi (ex linee "BA").

3.2.3. Partecipazione di terzi al finanziamento

La proposta/iniziativa:

– X☐ non prevede cofinanziamenti da terzi

– ☐ prevede il cofinanziamento da terzi indicato di seguito:

Stanziamenti in Mio EUR (al terzo decimale)

Anni	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**TOTALE**
Specificare l'organismo di cofinanziamento								
TOTALE degli stanziamenti cofinanziati								

3.3. Incidenza prevista sulle entrate

– ☐X La proposta/iniziativa non ha incidenza finanziaria sulle entrate.

– ☐ La proposta/iniziativa ha la seguente incidenza finanziaria:

☐ sulle risorse proprie

☐ su altre entrate

indicare se le entrate sono destinate a linee di spesa specifiche ☐

Mio EUR (al terzo decimale)

Linea di bilancio delle entrate:	Incidenza della proposta/iniziativa[49]						
	2021	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**
Articolo …….							

Per quanto riguarda le entrate con destinazione specifica, precisare la o le linee di spesa interessate.

Altre osservazioni (ad es. formula/metodo per calcolare l'incidenza sulle entrate o altre informazioni).

[49] Per le risorse proprie tradizionali (dazi doganali, contributi zucchero), indicare gli importi netti, cioè gli importi lordi al netto del 20 % per spese di riscossione.

ALLEGATO
della SCHEDA FINANZIARIA LEGISLATIVA

Nome della proposta/iniziativa:

Proposta di una direttiva che riesamina la direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione

……
……

1. QUANTITÀ e COSTO delle RISORSE UMANE CONSIDERATE NECESSARIE

2. COSTO delle ALTRE SPESE AMMINISTRATIVE

3. METODI di CALCOLO UTILIZZATI per STIMARE I COSTI

3.1 Risorse umane

3.2 Altre spese amministrative

*Il presente allegato, **da compilarsi a cura di ciascuna DG o ciascun servizio che partecipa alla proposta/iniziativa**, accompagna la scheda finanziaria legislativa nel corso della consultazione interservizi.*

Le tabelle di dati sono utilizzate per compilare le tabelle contenute nella scheda finanziaria legislativa. Esse sono esclusivamente destinate ad uso interno della Commissione.

1. Costo delle risorse umane considerate necessarie

☐ La proposta/iniziativa non comporta l'utilizzo di risorse umane

X☐ La proposta/iniziativa comporta l'utilizzo di risorse umane, come spiegato di seguito:

Mio EUR (al terzo decimale)

RUBRICA 7 del quadro finanziario pluriennale		**2021**		**2022**		**2023**		**2024**		**2025**		**2026**		**2027**		**TOTALE**	
		ETP	Stanziamenti	ETP	Stanziamenti	ETP	Stanziamenti	ETP	Stanziamenti	ETP	Stanziamenti	ETP	Stanziamenti	ETP	Stanziamenti	ETP	Stanziamenti
• Posti della tabella dell'organico (funzionari e agenti temporanei)																	
In sede e negli uffici di rappresentanza della Commissione	AD	6	0,9	6	0,9	6	0,9	6	0,9	6	0,9	6	0,9	6	0,9	42	6,3
	AST																
nelle delegazioni	AD																
	AST																
• Personale esterno [50] 0,24																	
Dotazione globale	AC	3	0,24	3	0,24	3	0,24	3	0,24	3	0,24	3	0,24	3	0,24	21	1,68
	FINE																
	INT																
nelle delegazioni	AC																
	AL																
	FINE																

[50] AC = agente contrattuale; AL = agente locale; END = esperto nazionale distaccato; INT = personale interinale (intérimaire); JPD = giovane professionista in delegazione.

	INT																
	JPD																
Altre linee di bilancio (*specificare*)																	
Totale parziale – RUBRICA 7 del quadro finanziario pluriennale		9	1,14	9	1,14	9	1,14	9	1,14	9	1,14	9	1,14	9	1,14	63	7,98

Il fabbisogno di risorse umane è coperto dal personale della DG già assegnato alla gestione dell'azione e/o riassegnato all'interno della stessa DG, integrato dall'eventuale dotazione supplementare concessa alla DG responsabile nell'ambito della procedura annuale di assegnazione, tenendo conto dei vincoli di bilancio.

Esclusa la RUBRICA 7 del quadro finanziario pluriennale		2021		2022		2023		2024		2025		2025		2025		TOTALE	
		ETP	Stanziamenti	ETP	Stanziamenti	ETP	Stanziamenti	ETP	Stanziamenti	ETP	Stanziamenti	ETP	Stanziamenti	ETP	Stanziamenti	ETP	Stanziamenti
• Posti della tabella dell'organico (funzionari e agenti temporanei)																	
Ricerca	AD																
	AST																
• Personale esterno [51]																	
Personale esterno previsto dagli stanziamenti operativi (ex linee "BA")	- in sede AC																
	- in sede FINE																
	- in sede INT																
	- nelle delegazioni AC																
	- nelle delegazioni AL																
	- nelle delegazioni FINE																
	- nelle delegazioni INT																
	- nelle delegazioni JPD																
Ricerca)	AC																
	FINE																
	INT																
Altre linee di bilancio																	

[51] AC = agente contrattuale; AL = agente locale; END = esperto nazionale distaccato; INT = personale interinale (intérimaire); JPD = giovane professionista in delegazione.

(*specificare*)																		
Totale parziale - Esclusa la RUBRICA 7 del quadro finanziario pluriennale																		

Il fabbisogno di risorse umane è coperto dal personale della DG già assegnato alla gestione dell'azione e/o riassegnato all'interno della stessa DG, integrato dall'eventuale dotazione supplementare concessa alla DG responsabile nell'ambito della procedura annuale di assegnazione, tenendo conto dei vincoli di bilancio.

Incidenza prevista sulle risorse umane dell'ENISA

L'Agenzia dell'Unione europea per la cibersicurezza, ENISA, alla quale con il regolamento sulla cibersicurezza è stato conferito un nuovo mandato permanente, assisterebbe gli Stati membri e la Commissione nell'attuazione della direttiva NIS rivista.

Per effetto della direttiva NIS rivista, dal 2022/2023 l'ENISA avrà ulteriori settori d'intervento. Sebbene tali settori d'intervento siano compresi nei compiti generali dell'ENISA in base al suo mandato, essi determineranno un carico di lavoro supplementare per l'agenzia. Più precisamente, oltre ai suoi settori d'intervento attuali, in base alla proposta della Commissione relativa alla direttiva NIS rivista, l'ENISA dovrà includere specificamente nel suo programma di lavoro tra le altre azioni, le seguenti: i) sviluppare e mantenere un registro europeo delle vulnerabilità (articolo 6, paragrafo 2, della proposta), ii) assicurare il segretariato della rete europea delle organizzazioni di collegamento per le crisi informatiche (CyCLONe) (articolo 14 della proposta) e pubblicare una relazione annuale sullo stato della cibersicurezza nell'UE (articolo 15 della proposta), iii) sostenere l'organizzazione di revisioni tra pari tra Stati membri (articolo 16 della proposta), iv) raccogliere dati aggregati sugli incidenti dagli Stati membri e pubblicare orientamenti tecnici (articolo 20, paragrafo 9, della proposta), v) creare e mantenere un registro per soggetti che prestano servizi transfrontalieri (articolo 25 della proposta).

Pertanto, a partire dal 2022 sarà presentata una richiesta di altri 5 ETP con un bilancio corrispondente di circa 0,61 milioni di EUR l'anno a copertura di tali nuovi posti (cfr. scheda finanziaria separata per le agenzie).

Pertanto, a partire dal 2022 sarà presentata una richiesta di altri 5 ETP con un bilancio corrispondente a copertura di tali nuovi posti.

☐ La proposta/iniziativa non comporta l'utilizzo di stanziamenti amministrativi.

☐X La proposta/iniziativa comporta l'utilizzo di stanziamenti amministrativi, come spiegato di seguito:

Mio EUR (al terzo decimale)

	Anno **N** [52] **2022**	Anno **N+1** **2023**	Anno **N+2** **2024**	Anno **N+3** **2025**	Inserire gli anni necessari per evidenziare la durata dell'incidenza (cfr. punto 1.6)			**TOTALE**
Agenti temporanei (gradi AD)	0,450	0,450	0,450	0,450	0,450	0,450		**2,7**

[52] L'anno N è l'anno in cui inizia a essere attuata la proposta/iniziativa. Sostituire "N" con il primo anno di attuazione previsto (ad es: 2021) e così per gli anni a seguire.

Agenti temporanei (gradi AST)								
Agenti contrattuali	0,160	0,160	0,160	0,160	0,160	0,160		
Esperti nazionali distaccati								**0,96**
TOTALE	**0,61**	**0,61**	**0,61**	**0,61**	**0,61**	**0,61**		**3,66**

Fabbisogno di personale (ETP):

	Anno **N** [53] **2022**	Anno **N+1** **2023**	Anno **N+2** **2024**	Anno **N+3** **2025**	Inserire gli anni necessari per evidenziare la durata dell'incidenza (cfr. punto 1.6)	**TOTALE**
Agenti temporanei (gradi AD)	3	3	3	3	3	3		**18**
Agenti temporanei (gradi AST)								
Agenti contrattuali	2	2	2	2	2	2		**12**
Esperti nazionali distaccati								

[53] L'anno N è l'anno in cui inizia a essere attuata la proposta/iniziativa. Sostituire "N" con il primo anno di attuazione previsto (ad es: 2021) e così per gli anni a seguire.

TOTALE	**5**	**5**	**5**	**5**	**5**	**5**		**30**

2. Costo delle altre spese amministrative

☐ La proposta/iniziativa non comporta l'utilizzazione di stanziamenti amministrativi

X☐ La proposta/iniziativa comporta l'utilizzazione di stanziamenti amministrativi, come spiegato di seguito:

Mio EUR (al terzo decimale)

RUBRICA 7 del quadro finanziario pluriennale	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Totale**
In sede:								
Spese per missioni e di rappresentanza	0,03	0,03	0,03	0,03	0,03	0,03	0,03	**0,21**
Spese per conferenze e riunioni	0,06	0,06	0,06	0,06	0,06	0,06	0,06	**0,42**
Comitati[54]								
Studi e consulenze								
Sistemi d'informazione e di gestione								
Attrezzature e servizi TIC[55]								
Altre linee di bilancio (*specificare se del caso*)								

[54] Precisare il tipo di comitato e il gruppo cui appartiene.

[55] TIC: Tecnologie dell'informazione e della comunicazione: consultare DIGIT.

Nelle delegazioni								
Spese per missioni, conferenze e ricevimenti								
Perfezionamento professionale								
Acquisto, affitto e costi connessi								
Materiale, mobilio, forniture e servizi								
Totale parziale della RUBRICA 7 del quadro finanziario pluriennale	0,09	0,09	0,09	0,09	0,09	0,09	0,09	**0,63**

Mio EUR (al terzo decimale)

Esclusa la RUBRICA 7 del quadro finanziario pluriennale	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Totale**
Spese di assistenza tecnica e amministrativa (escluso il personale esterno) dagli stanziamenti operativi (ex linee "BA")								
- in sede								
- nelle delegazioni								
Altre spese di gestione per la ricerca								
Altre linee di bilancio (*specificare se del caso*)								
Totale parziale – Esclusa la RUBRICA 7 del quadro finanziario pluriennale								

TOTALE RUBRICA 7 ed esclusa la RUBRICA 7 del quadro finanziario pluriennale	1,23	1,23	1,23	1,23	1,23	1,23	1,23	**8,61**

Il fabbisogno di stanziamenti amministrativi è coperto dagli stanziamenti già assegnati alla gestione dell'azione e/o che sono stati riassegnati, integrati dall'eventuale dotazione supplementare concessa alla DG responsabile nell'ambito della procedura annuale di assegnazione, tenendo conto dei vincoli di bilancio esistenti.

3. Metodi di calcolo utilizzati per stimare i costi

3.1 Risorse umane

Questa parte stabilisce il metodo di calcolo utilizzato per stimare il fabbisogno di risorse umane [ipotesi sul carico di lavoro, compresi impieghi specifici (profili professionali Sysper 2), categorie di personale e costi medi corrispondenti]

RUBRICA 7 del quadro finanziario pluriennale
NB: I costi medi per ciascuna categoria di personale in sede sono disponibili sul sito BudgWeb: https://myintracomm.ec.europa.eu/budgweb/EN/pre/legalbasis/Pages/pre-040-020_preparation.aspx
• Funzionari e agenti temporanei 6 funzionari ETP) (costo medio 0,150) = 0,9 l'anno - preparazione di atti delegati in conformità all'articolo 18, paragrafo 6, all'articolo 21, paragrafo 2 e all'articolo 36; - preparazione di atti di esecuzione in conformità all'articolo 12, paragrafo 8, all'articolo 18, paragrafo 5 e all'articolo 20, paragrafo 11; - assicurare il segretariato per il gruppo di cooperazione NIS; - organizzazione delle riunioni plenarie del gruppo di cooperazione NIS e delle riunioni dedicate ai flussi di lavoro; - coordinazione dei lavori degli Stati membri su vari documenti (orientamenti, pacchetti di strumenti, ecc.); - collegamento con altri servizi della Commissione, con l'ENISA e con le autorità nazionali in vista dell'attuazione della direttiva NIS; - analisi dei metodi nazionali e delle migliori pratiche legati all'attuazione della direttiva NIS.
• Personale esterno 3 AC (costo medio 0,08) = 0,24 l'anno - Supporto a tutti i compiti sopra illustrati in funzione delle necessità

Esclusa la RUBRICA 7 del quadro finanziario pluriennale
• Soltanto posti a carico del bilancio della ricerca
• Personale esterno

3.2 Altre spese amministrative

Precisare il metodo di calcolo utilizzato per ciascuna linea di bilancio,

in particolare le ipotesi su cui si basa (ad esempio, il numero di riunioni all'anno, i costi medi ecc.)

RUBRICA 7 del quadro finanziario pluriennale

Riunioni: Le riunioni plenarie del gruppo di cooperazione NIS si svolgono solitamente quattro volte l'anno. La Commissione copre i costi legati alle spese di ristorazione e viaggio dei rappresentanti dei 27 Stati membri (un rappresentante per Stato membro). I costi di una riunione potrebbero raggiungere i 15 000 EUR, per un totale di 60 000 EUR l'anno.

Missioni: Le missioni sono legate al monitoraggio dell'attuazione della direttiva NIS. Esempio: In un anno (maggio 2019 - luglio 2020) avremmo dovuto organizzare le cosiddette "visite nei paesi in relazione alla NIS" e visitare tutti i 27 Stati membri per discutere

dell'attuazione della direttiva NIS in tutta l'UE.

Esclusa la RUBRICA 7 del quadro finanziario pluriennale

ALLEGATO 7

della

DECISIONE DELLA COMMISSIONE

relativa alle norme interne sull'esecuzione del bilancio generale dell'Unione europea (sezione Commissione europea) a uso dei servizi della Commissione

SCHEDA FINANZIARIA LEGISLATIVA "AGENZIE"

Questa scheda finanziaria legislativa riguarda la richiesta di aumento del personale dell'ENISA di 5 ETP a partire dal 2022 allo scopo di svolgere attività supplementari legate all'attuazione della direttiva NIS. Tali attività sono già comprese nel mandato dell'ENISA.

Indice

1. CONTESTO DELLA PROPOSTA/INIZIATIVA 16
1.1. Titolo della proposta/iniziativa 16
1.2. Settore/settori interessati 16
1.3. La proposta riguarda 16
1.4. Obiettivi 16
1.4.1. Obiettivi generali 16
1.4.2. Obiettivi specifici 16
1.4.3. Risultati e incidenza previsti 18
1.4.4. Indicatori di prestazione 19
1.5. Motivazione della proposta/iniziativa 19
1.5.1. Necessità nel breve e lungo termine, compreso un calendario dettagliato per fasi di attuazione dell'iniziativa 19
1.5.2. Valore aggiunto dell'intervento dell'Unione (che può derivare da diversi fattori, ad es. un miglior coordinamento, la certezza del diritto, maggiore efficacia o maggiori complementarità). Ai fini del presente punto, per "valore aggiunto dell'intervento dell'Unione" si intende il valore derivante dall'intervento dell'Unione che va ad aggiungersi al valore che avrebbero altrimenti generato gli Stati membri se avessero agito da soli. 20
1.5.3. Insegnamenti tratti da esperienze analoghe 20
1.5.4. Compatibilità con il quadro finanziario pluriennale ed eventuali sinergie con altri strumenti pertinenti 20
1.5.5. Valutazione delle varie opzioni di finanziamento disponibili, comprese le possibilità di riassegnazione 20
1.6. Durata e incidenza finanziaria della proposta/iniziativa 22
1.7. Modalità di gestione previste 22
2. MISURE DI GESTIONE 24
2.1. Disposizioni in materia di monitoraggi e di relazioni 24
2.2. Sistema di gestione e di controllo 24
2.2.1. Giustificazione della o delle modalità di gestione, del meccanismo o dei meccanismi di attuazione del finanziamento, delle modalità di pagamento e della strategia di controllo proposti 24
2.2.2. Informazioni concernenti i rischi individuati e il sistema o i sistemi di controllo interno per ridurli 24
2.2.3. Stima e giustificazione del rapporto costo/efficacia dei controlli (rapporto "costi del controllo ÷ valore dei fondi gestiti") e valutazione dei livelli di rischio di errore previsti (al pagamento e alla chiusura) 24

2.3. Misure di prevenzione delle frodi e delle irregolarità 26
3. INCIDENZA FINANZIARIA PREVISTA DELLA PROPOSTA/INIZIATIVA 26
3.1. Rubrica/rubriche del quadro finanziario pluriennale e linea/linee di bilancio di spesa interessate 26
3.2. Incidenza prevista sulle spese 28
3.2.1. Sintesi dell'incidenza prevista sulle spese 28
3.2.2. Incidenza prevista sugli stanziamenti [dell'organismo] 30
3.2.3. Incidenza prevista sulle risorse umane dell'ENISA 31
3.2.4. Compatibilità con il quadro finanziario pluriennale attuale 34
3.2.5. Partecipazione di terzi al finanziamento 34
3.3. Incidenza prevista sulle entrate 35

1. CONTESTO DELLA PROPOSTA/INIZIATIVA

1.1. Titolo della proposta/iniziativa

Proposta di direttiva relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, che abroga la direttiva (UE) 2016/1148

1.2. Settore/settori interessati

Reti, contenuti e tecnologie delle comunicazioni

1.3. La proposta riguarda

☐ **una nuova azione**

☐ **una nuova azione a seguito di un progetto pilota/un'azione preparatoria**[56]

☒ **la proroga di un'azione esistente**

☐ **la fusione di una o più azioni verso un'altra/una nuova azione**

1.4. Obiettivi

1.4.1. Obiettivi generali

L'obiettivo del riesame è aumentare il livello di ciberresilienza di un vasto gruppo di imprese operanti nell'Unione europea in tutti i settori pertinenti, ridurre le incongruenze in termini di resilienza del mercato interno nei settori già contemplati dalla direttiva e migliorare il livello di consapevolezza situazionale comune e la capacità collettiva di preparazione e risposta.

1.4.2. Obiettivi specifici

Per affrontare il problema del basso livello di ciberresilienza delle imprese che operano nell'Unione europea, l'obiettivo specifico è quello di garantire che i soggetti in tutti i settori che dipendono dai sistemi informatici e di rete e che forniscono servizi chiave all'economia e alla società nel suo complesso siano tenuti ad adottare misure di cibersicurezza e a segnalare gli incidenti al fine di aumentare il livello globale di ciberresilienza in tutto il mercato interno.

Per affrontare il problema del livello incoerente di resilienza tra Stati membri e tra settori, l'obiettivo specifico è quello di garantire che tutti i soggetti attivi in settori disciplinati dal quadro giuridico della NIS, di dimensioni simili e aventi un ruolo comparabile, siano soggetti allo stesso regime normativo (che rientrino o meno nell'ambito di applicazione), indipendentemente dalla giurisdizione a cui sono sottoposte nell'Unione europea.

Al fine di garantire che tutti i soggetti attivi nei settori disciplinati dal quadro giuridico della NIS siano tenuti a rispettare gli stessi obblighi basati sul concetto di gestione del rischio per quanto riguarda le misure di sicurezza e a segnalare tutti gli incidenti sulla base di un insieme uniforme di criteri, gli obiettivi specifici sono garantire che le autorità competenti applichino in modo più efficace le norme stabilite dallo strumento giuridico attraverso misure allineate di vigilanza e applicazione e garantire un livello comparabile di risorse tra gli Stati membri assegnate alle autorità competenti che consentano loro di svolgere i compiti fondamentali definiti dal quadro della NIS.

[56] A norma dell'articolo 58, paragrafo 2, lettera a) o b), del regolamento finanziario.

Per affrontare il problema della consapevolezza situazionale comune e della mancanza di una risposta comune alle crisi, l'obiettivo specifico è di garantire lo scambio di informazioni essenziali tra gli Stati membri introducendo obblighi di condivisione di informazioni e di cooperazione chiari per le autorità competenti in relazione a minacce e incidenti informatici e sviluppando una capacità operativa comune di risposta dell'Unione alle crisi.

1.4.3. Risultati e incidenza previsti

Precisare gli effetti che la proposta/iniziativa dovrebbe avere sui beneficiari/gruppi interessati.

La proposta dovrebbe apportare vantaggi significativi: le stime indicano che può portare a una riduzione pari a 11,3 miliardi di EUR dei costi degli incidenti di cibersicurezza. L'ambito di applicazione settoriale sarebbe notevolmente ampliato nel quadro della NIS, ma oltre ai vantaggi di cui sopra, l'onere che potrebbe essere creato dai requisiti della NIS, in particolare dal punto di vista della vigilanza, sarebbe anche bilanciato sia per i nuovi soggetti da comprendere nell'ambito di applicazione sia per le autorità competenti. Ciò è dovuto al fatto che il nuovo quadro della NIS definirebbe un approccio a due livelli, incentrato su soggetti chiave e di grandi dimensioni e su una differenziazione del regime di vigilanza che consenta la supervisione solo ex post per un ampio numero di tali soggetti, in particolare quelli considerati "importanti" ma non "essenziali".

Complessivamente, la proposta determinerebbe efficienti compromessi e sinergie, con le migliori potenzialità tra tutte le opzioni strategiche analizzate per garantire un livello di ciberresilienza superiore e coerente dei soggetti chiave all'interno dell'Unione, con conseguenti risparmi di costi sia per le imprese che per la società.

La proposta comporterebbe inoltre alcuni costi di conformità e di esecuzione per le autorità competenti degli Stati membri (è stato stimato un aumento complessivo di risorse di circa il 20-30 %). Il nuovo quadro apporterebbe tuttavia anche vantaggi sostanziali attraverso una migliore panoramica delle imprese chiave e l'interazione con esse, una maggiore cooperazione operativa transfrontaliera e a meccanismi di assistenza reciproca e di revisione tra pari. Ciò comporterebbe un aumento generale delle capacità di cibersicurezza nei vari Stati membri.

Per le imprese che rientrerebbero nell'ambito di applicazione del quadro NIS, si stima che per i primi anni successivi all'introduzione del nuovo quadro NIS sarebbe necessario un aumento massimo del 22 % della spesa corrente per la sicurezza delle TIC (tale aumento sarebbe del 12 % per le imprese già rientranti nell'ambito di applicazione della direttiva NIS vigente). Tuttavia, questo aumento medio della spesa per la sicurezza delle TIC porterebbe ad un vantaggio proporzionale di tali investimenti, dovuto in particolare a una considerevole riduzione dei costi degli incidenti di cibersicurezza (stimata a 118 miliardi di EUR in dieci anni).

Le piccole imprese e le microimprese non rientrerebbero nell'ambito di applicazione del quadro NIS. Per le medie imprese, è possibile prevedere un aumento del livello di spesa per la sicurezza delle TIC nei primi anni successivi all'introduzione del nuovo quadro NIS. Allo stesso tempo, l'aumento del livello dei requisiti di sicurezza per tali soggetti incentiverebbe anche le loro capacità di cibersicurezza e contribuirebbe a migliorare la loro gestione del rischio relativo alle TIC.

Vi sarebbe un impatto sui bilanci e sulle amministrazioni nazionali: si prevede un aumento stimato di circa il 20-30 % delle risorse a breve e medio termine.

Non sono previsti altri impatti negativi significativi. La proposta dovrebbe determinare funzionalità di cibersicurezza più solide e di conseguenza avrebbe un impatto attenuante più sostanziale sul numero e sulla gravità degli incidenti, comprese le violazioni di dati. È inoltre probabile che abbia un impatto positivo nel garantire parità di condizioni tra gli Stati membri di tutti i soggetti rientranti nell'ambito di applicazione della NIS e che riduca le asimmetrie inerenti alle informazioni sulla cibersicurezza.

1.4.4. Indicatori di prestazione

Precisare gli indicatori con cui monitorare progressi e risultati.

La valutazione degli indicatori sarà condotta dalla Commissione, con il sostegno dell'ENISA e del gruppo di cooperazione, a partire da tre anni dopo l'entrata in vigore del nuovo atto giuridico NIS. Di seguito sono riportati alcuni indicatori di monitoraggio sulla base dei quali si valuterebbe l'esito positivo del riesame della NIS:

- migliore gestione degli incidenti: adottando misure di cibersicurezza, le imprese non migliorano soltanto la propria capacità di evitare completamente determinati incidenti, ma anche quella di risposta agli incidenti. Gli esiti positivi sono quindi misurati in base ai fattori seguenti: i) la riduzione del tempo medio necessario per rilevare un incidente, ii) il tempo mediamente necessario alle organizzazioni per riprendersi da un incidente e iii) il costo medio di un danno causato da un incidente;

- maggiore consapevolezza dei rischi di cibersicurezza da parte dell'alta dirigenza delle imprese: obbligando le imprese ad adottare misure, una direttiva NIS rivista contribuirebbe ad aumentare la consapevolezza dei rischi legati alla cibersicurezza a livello di alta dirigenza. Questo aspetto può essere misurato analizzando fino a che punto le imprese rientranti nell'ambito di applicazione della NIS diano priorità alla cibersicurezza nelle politiche e nei processi aziendali interni, come dimostrato dalla documentazione interna, dai programmi di formazione pertinenti e dalle attività di sensibilizzazione per i dipendenti, e agli investimenti in TIC correlati alla sicurezza. I dirigenti di tutti i soggetti essenziali e importanti dovrebbero essere anche a conoscenza delle norme stabilite dalla direttiva NIS;

- livellamento della spesa specifica per settore: la spesa per la sicurezza delle TIC varia notevolmente tra i diversi settori dell'UE. Obbligando le imprese di più settori ad adottare misure, si dovrebbe assistere a una riduzione, tra settori e Stati membri, delle deviazioni dalla spesa media per la sicurezza delle TIC specifica per settore in percentuale della spesa complessiva per le TIC;

- autorità competenti più forti e maggiore cooperazione: una direttiva NIS rivista attribuirebbe potenzialmente compiti supplementari alle autorità competenti. Ciò avrebbe un'incidenza misurabile sulle risorse finanziarie e umane destinate alle agenzie di cibersicurezza a livello nazionale e dovrebbe avere un impatto positivo sulla capacità delle autorità competenti di cooperare in modo proattivo e quindi aumentare il numero di casi in cui le autorità competenti si impegnano reciprocamente allo scopo di gestire gli incidenti transfrontalieri o di svolgere attività di vigilanza congiunte;

- maggiore condivisione delle informazioni: la NIS rivista migliorerebbe anche la condivisione delle informazioni tra imprese e con le autorità competenti. Uno degli obiettivi della revisione potrebbe essere quello di aumentare il numero di soggetti che partecipano alle varie forme di condivisione delle informazioni.

1.5. Motivazione della proposta/iniziativa

1.5.1. Necessità nel breve e lungo termine, compreso un calendario dettagliato per fasi di attuazione dell'iniziativa

La proposta punta ad aumentare il livello di ciberresilienza di un vasto gruppo di imprese operanti nell'Unione europea in tutti i settori pertinenti, ridurre le incongruenze in termini di resilienza del mercato interno nei settori già contemplati dalla direttiva e migliorare il livello di consapevolezza situazionale comune e la capacità collettiva di preparazione e risposta. Essa

si baserà sui risultati raggiunti con l'attuazione della direttiva (UE) 2016/1148 negli ultimi quattro anni.

1.5.2. Valore aggiunto dell'intervento dell'Unione (che può derivare da diversi fattori, ad es. un miglior coordinamento, la certezza del diritto, maggiore efficacia o maggiori complementarità). Ai fini del presente punto, per "valore aggiunto dell'intervento dell'Unione" si intende il valore derivante dall'intervento dell'Unione che va ad aggiungersi al valore che avrebbero altrimenti generato gli Stati membri se avessero agito da soli.

La resilienza in termini di cibersicurezza all'interno dell'Unione non può essere efficace se affrontata in modo diverso nei vari silos nazionali o regionali. La direttiva NIS ha ovviato a questa carenza definendo un quadro per la sicurezza delle reti e dei sistemi informativi a livello nazionale e dell'Unione. Tuttavia, il primo riesame periodico della direttiva NIS ha evidenziato alcuni difetti intrinseci, i quali hanno portato a considerevoli disparità tra gli Stati membri in termini di capacità, pianificazione e livello di protezione, che interessano al contempo la parità di condizioni per imprese analoghe sul mercato interno.

L'intervento dell'UE, che va oltre le attuali misure della direttiva NIS, è giustificato principalmente dai seguenti fattori: i) la natura transfrontaliera del problema; ii) le potenzialità degli interventi dell'UE volti a migliorare e agevolare strategie nazionali efficaci; iii) il contributo degli interventi strategici concertati e collaborativi della NIS volti a un'efficace protezione dei dati e della vita privata.

Gli obiettivi enunciati possono quindi essere conseguiti meglio con un'azione a livello dell'UE piuttosto che con l'azione dei singoli Stati membri.

1.5.3. Insegnamenti tratti da esperienze analoghe

La direttiva NIS è il primo strumento orizzontale del mercato interno volto a migliorare la resilienza di reti e sistemi nell'Unione rispetto ai rischi di cibersicurezza. Dalla sua entrata in vigore nel 2016, ha già contribuito notevolmente a innalzare il livello comune di cibersicurezza tra gli Stati membri. Il riesame del funzionamento e dell'attuazione della direttiva ha tuttavia evidenziato alcune carenze che, oltre all'aumento della digitalizzazione e alla necessità di risposte più aggiornate, devono essere affrontate nel quadro di un atto giuridico rivisto.

1.5.4. Compatibilità con il quadro finanziario pluriennale ed eventuali sinergie con altri strumenti pertinenti

La nuova proposta è pienamente coerente con altre iniziative affini, quali la proposta di regolamento relativo alla resilienza operativa digitale per il settore finanziario e la proposta di direttiva sulla resilienza degli operatori critici di servizi essenziali, nonché con il codice europeo delle comunicazioni elettroniche, il regolamento generale sulla protezione dei dati e il regolamento eIDAS.

La proposta è una parte essenziale della strategia dell'UE per l'Unione della sicurezza.

1.5.5. Valutazione delle varie opzioni di finanziamento disponibili, comprese le possibilità di riassegnazione

La gestione di questi compiti da parte dell'ENISA richiede profili specifici e carichi di lavoro supplementari che non possono essere assorbiti senza un aumento delle risorse umane.

1.6. Durata e incidenza finanziaria della proposta/iniziativa

☐ **durata limitata**

– ☐ Proposta/iniziativa in vigore a decorrere dal [GG/MM]AAAA fino al [GG/MM]AAAA

– ☐ Incidenza finanziaria dal AAAA al AAAA

☒ **durata illimitata**

– Attuazione con un periodo di avviamento dal 2022 al 2025;

– successivo funzionamento a pieno ritmo.

1.7. Modalità di gestione previste[57]

☒ **Gestione diretta** a opera della Commissione

mediante:

– ☐ agenzie esecutive

☐ **Gestione concorrente** con gli Stati membri

☐X **Gestione indiretta** con compiti di esecuzione del bilancio affidati:

☐ a organizzazioni internazionali e loro agenzie (specificare);

☐ alla BEI e al Fondo europeo per gli investimenti;

☒ agli organismi di cui agli articoli 70 e 71;

☐ a organismi di diritto pubblico;

☐ a organismi di diritto privato investiti di attribuzioni di servizio pubblico nella misura in cui sono dotati di sufficienti garanzie finanziarie;

☐ a organismi di diritto privato di uno Stato membro preposti all'attuazione di un partenariato pubblico-privato e che sono dotati di sufficienti garanzie finanziarie;

☐ alle persone incaricate di attuare azioni specifiche della PESC a norma del titolo V del TUE e indicate nel pertinente atto di base.

Osservazioni

L'Agenzia dell'Unione europea per la cibersicurezza, ENISA, alla quale con il regolamento sulla cibersicurezza è stato conferito un nuovo mandato permanente, assisterebbe gli Stati membri e la Commissione nell'attuazione della direttiva NIS rivista.

Per effetto della direttiva NIS rivista, dal 2022/2023 l'ENISA avrà ulteriori settori d'intervento. Sebbene tali settori d'intervento siano compresi nei compiti generali dell'ENISA in base al suo mandato, essi determineranno un carico di lavoro supplementare per l'agenzia. Più precisamente, oltre ai suoi settori d'intervento attuali, in base alla proposta della Commissione relativa alla direttiva NIS rivista, l'ENISA dovrà includere specificamente nel suo programma di lavoro tra le altre azioni, le seguenti: i) sviluppare e mantenere un registro europeo delle vulnerabilità (articolo 6, paragrafo 2, della proposta), ii) assicurare il segretariato della rete europea delle organizzazioni di collegamento per le crisi informatiche (CyCLONe) (articolo 14 della proposta) e pubblicare una relazione annuale sullo stato

[57] Le spiegazioni sulle modalità di gestione e i riferimenti al regolamento finanziario sono disponibili sul sito BudgWeb: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx.

della cibersicurezza nell'UE (articolo 15 della proposta), iii) sostenere l'organizzazione di revisioni tra pari tra Stati membri (articolo 16 della proposta), iv) raccogliere dati aggregati sugli incidenti dagli Stati membri e pubblicare orientamenti tecnici (articolo 20, paragrafo 9, della proposta), v) creare e mantenere un registro per soggetti che prestano servizi transfrontalieri (articolo 25 della proposta).

Pertanto, a partire dal 2022 sarà effettuata una richiesta di 5 ETP supplementari con un bilancio corrispondente di circa 0,61 milioni di EUR l'anno a copertura di questi nuovi posti.

2. MISURE DI GESTIONE

2.1. Disposizioni in materia di monitoraggi e di relazioni

Precisare frequenza e condizioni.

La Commissione riesaminerà periodicamente il funzionamento della direttiva e presenterà una relazione al Parlamento europeo e al Consiglio, la prima volta tre anni dopo l'entrata in vigore.

La Commissione valuterà anche il corretto recepimento della direttiva da parte degli Stati membri.

Il monitoraggio e la comunicazione della proposta seguiranno i principi delineati nel mandato permanente dell'ENISA di cui al regolamento (UE) 2019/881 (regolamento sulla cibersicurezza).

Le fonti di dati utilizzate per il monitoraggio previsto sarebbero principalmente l'ENISA, il gruppo di cooperazione, la rete di CSIRT e le autorità degli Stati membri. Oltre ai dati ricavati dalle relazioni (comprese le relazioni annuali di attività) dell'ENISA, del gruppo di cooperazione e della rete di CSIRT, in caso di necessità saranno utilizzati specifici strumenti di raccolta dati (ad esempio le indagini presso le autorità nazionali, Eurobarometro, le relazioni della campagna mensile per la cibersicurezza e le esercitazioni paneuropee).

2.2. Sistema di gestione e di controllo

2.2.1. Giustificazione della o delle modalità di gestione, del meccanismo o dei meccanismi di attuazione del finanziamento, delle modalità di pagamento e della strategia di controllo proposti

L'unità della DG CNECT incaricata del settore gestirà l'attuazione della direttiva.

Per quanto riguarda la gestione dell'ENISA, l'articolo 15 del regolamento sulla cibersicurezza fornisce un elenco dettagliato delle funzioni di controllo del consiglio di amministrazione dell'ENISA.

A norma dell'articolo 31 del regolamento sulla cibersicurezza, il direttore esecutivo dell'ENISA è responsabile dell'esecuzione del bilancio dell'ENISA e il revisore contabile interno della Commissione esercita nei confronti dell'ENISA le stesse competenze di cui dispone nei confronti dei servizi della Commissione. Il consiglio di amministrazione dell'ENISA formula un parere sui conti definitivi della stessa.

2.2.2. Informazioni concernenti i rischi individuati e il sistema o i sistemi di controllo interno per ridurli

Rischio molto basso, poiché l'ecosistema della direttiva NIS è già esistente e riguarda già l'ENISA, che ha un mandato permanente a seguito dell'entrata in vigore del regolamento sulla cibersicurezza nel 2019.

2.2.3. Stima e giustificazione del rapporto costo/efficacia dei controlli (rapporto "costi del controllo ÷ valore dei fondi gestiti") e valutazione dei livelli di rischio di errore previsti (al pagamento e alla chiusura)

L'aumento di bilancio richiesto si applica al titolo 1 ed è destinato a finanziare gli stipendi. Ciò implica un rischio di errore molto basso a livello di pagamenti.

2.3. Misure di prevenzione delle frodi e delle irregolarità

Precisare le misure di prevenzione e tutela in vigore o previste, ad esempio strategia antifrode.

Si applicherebbero le misure di prevenzione e protezione dell'ENISA, in particolare quanto segue:

- il controllo dei pagamenti per tutti i servizi o gli studi necessari viene effettuato dal personale dell'Agenzia prima del pagamento stesso, tenendo conto degli obblighi contrattuali, dei principi economici e delle prassi finanziarie o di sana gestione. Disposizioni antifrode (sorveglianza, obbligo di presentare relazioni, ecc.) saranno inserite in tutti gli accordi e i contratti stipulati tra l'Agenzia e i beneficiari dei pagamenti;

- nella lotta contro la frode, la corruzione e altre attività illegali si applicano senza limitazioni le disposizioni del regolamento (UE, Euratom) n. 883/2013 del Parlamento europeo e del Consiglio, del 25 maggio 1999, relativo alle indagini svolte dall'Ufficio europeo per la lotta antifrode (OLAF);

- a norma dell'articolo 33 del regolamento sulla cibersicurezza, entro il 28 dicembre 2019 l'ENISA ha aderito all'accordo interistituzionale del 25 maggio 1999 tra il Parlamento europeo, il Consiglio dell'Unione europea e la Commissione delle Comunità europee relativo alle indagini interne svolte dall'Ufficio europeo per la lotta antifrode (OLAF). L'ENISA pubblica senza indugio le disposizioni appropriate applicabili a tutti i dipendenti dell'agenzia.

3. INCIDENZA FINANZIARIA PREVISTA DELLA PROPOSTA/INIZIATIVA

3.1. Rubrica/rubriche del quadro finanziario pluriennale e linea/linee di bilancio di spesa interessate

- Linee di bilancio esistenti

Secondo l'ordine delle rubriche del quadro finanziario pluriennale e delle linee di bilancio.

Rubrica del quadro finanziario pluriennale	Linea di bilancio	Natura della spesa	Partecipazione			
	Numero	Diss./Non diss.[58]	di paesi EFTA[59]	di paesi candidati[60]	di paesi terzi	ai sensi dell'articolo 21, paragrafo 2, lettera b), del regolamento finanziario
2	02 10 04	./Non diss.	SÌ	NO	NO	/NO

- Nuove linee di bilancio di cui è chiesta la creazione

Secondo l'ordine delle rubriche del quadro finanziario pluriennale e delle linee di bilancio.

Rubrica del	Linea di bilancio	Tipo di	Partecipazione

[58] Diss. = stanziamenti dissociati / Non diss. = stanziamenti non dissociati.

[59] EFTA: Associazione europea di libero scambio.

[60] Paesi candidati e, se del caso, potenziali candidati dei Balcani occidentali.

quadro finanziario pluriennale		spesa				
	Numero	Diss./Non diss.	di paesi EFTA	di paesi candidati	di paesi terzi	ai sensi dell'articolo 21, paragrafo 2, lettera b), del regolamento finanziario
	[XX.YY.YY.YY]		SÌ/NO	SÌ/NO	SÌ/NO	SÌ/NO

3.2. Incidenza prevista sulle spese

3.2.1. Sintesi dell'incidenza prevista sulle spese

Mio EUR (al terzo decimale)

Rubrica del quadro finanziario pluriennale	Numero	[Rubrica…2 Mercato unico, innovazione e digitale……..……]

[Organismo]: <…ENISA….>			Anno **N**[61] **2022**	Anno **N+1** **2023**	Anno **N+2** **2024**	Anno **N+3** **2025**	Inserire gli anni necessari per evidenziare la durata dell'incidenza (cfr. punto 1.6) **2026**	**2027**		**TOTALE**
Titolo 1:	Impegni	(1)	0,61	0,61	0,61	0,61	0,61	0,61		**3,66**
	Pagamenti	(2)	0,61	0,61	0,61	0,61	0,61	0,61		**3,66**
Titolo 2:	Impegni	(1a)								
	Pagamenti	(2a)								
Titolo 3:	Impegni	(3a)								
	Pagamenti	(3b)								
TOTALE degli stanziamenti per [organismo] <ENISA…….>	Impegni	=1+1a +3a	0,61	0,61	O.61	0,61	0,61	0,61		**3,66**
	Pagamenti	=2+2a +3b	0,61	0,61	0,61	0,61	0,61	0,61		**3,66**

[61] L'anno N è l'anno in cui inizia a essere attuata la proposta/iniziativa. Sostituire "N" con il primo anno di attuazione previsto (ad es: 2021) e così per gli anni a seguire.

Rubrica del quadro finanziario pluriennale	**5**	"Spese amministrative"

Mio EUR (al terzo decimale)

		Anno **N**	Anno **N+1**	Anno **N+2**	Anno **N+3**	Inserire gli anni necessari per evidenziare la durata dell'incidenza (cfr. punto 1.6)			**TOTALE**
DG: <…….>									
• Risorse umane									
• Altre spese amministrative									
TOTALE DG <…….>	Stanziamenti								

TOTALE degli stanziamenti per la RUBRICA 5 del quadro finanziario pluriennale	(Totale impegni = Totale pagamenti)								

Mio EUR (al terzo decimale)

		Anno **N**[62] **2022**	Anno **N+1** **2023**	Anno **N+2** **2024**	Anno **N+3** **2025**	Inserire gli anni necessari per evidenziare la durata dell'incidenza (cfr. punto 1.6) **2026**	**2027**		**TOTALE**
TOTALE degli stanziamenti per le RUBRICHE da 1 a 5 del quadro finanziario pluriennale	Impegni	0,61	0,61	0,61	0,61	0,61	0,61		**3,66**
	Pagamenti	0,61	0,61	0,61	0,61	0,61	0,61		**3,66**

[62] L'anno N è l'anno in cui inizia a essere attuata la proposta/iniziativa. Sostituire "N" con il primo anno di attuazione previsto (ad es: 2021) e così per gli anni a seguire.

3.2.2. Incidenza prevista sugli stanziamenti [dell'organismo]

– ☐x La proposta/iniziativa non comporta l'utilizzo di stanziamenti operativi

– ☐ La proposta/iniziativa comporta l'utilizzo di stanziamenti operativi, come spiegato di seguito:

Stanziamenti di impegno in Mio EUR (al terzo decimale)

Specificare gli obiettivi e i risultati			Anno **N**		Anno **N+1**		Anno **N+2**		Anno **N+3**		Inserire gli anni necessari per evidenziare la durata dell'incidenza (cfr. punto 1.6)						**TOTALE**	
	RISULTATI																	
⇩	Tipo[63]	Costo medio	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N. totale	Costo totale
OBIETTIVO SPECIFICO 1[64]...																		
- Risultato																		
- Risultato																		
- Risultato																		
Totale parziale dell'obiettivo specifico 1																		
OBIETTIVO SPECIFICO 2 ...																		
- Risultato																		
Totale parziale dell'obiettivo specifico 2																		
COSTO TOTALE																		

63 I risultati sono i prodotti e i servizi da fornire (ad esempio, numero di scambi di studenti finanziati, numero di km di strada costruiti ecc.).

64 Come descritto nella sezione 1.4.2. "Obiettivi specifici..."

3.2.3. Incidenza prevista sulle risorse umane dell'ENISA

3.2.3.1. Sintesi

Per effetto della direttiva NIS rivista, dal 2022/2023 l'ENISA avrà ulteriori compiti. Sebbene tali compiti siano compresi nel mandato dell'ENISA, essi determineranno un carico di lavoro aggiuntivo per l'agenzia. Più precisamente, oltre alle sue aree di intervento attuali, in base alla proposta della Commissione di una direttiva NIS rivista l'ENISA avrà il compito, tra gli altri, di i) sviluppare e mantenere un registro europeo delle vulnerabilità (articolo 6, paragrafo 2), ii) assicurare il segretariato della rete europea delle organizzazioni di collegamento per le crisi informatiche (CyCLONe) (articolo 14) e pubblicare una relazione annuale sullo stato della cibersicurezza nell'UE (articolo 15), iii) sostenere l'organizzazione di revisioni tra pari tra Stati membri (articolo 16), iv) raccogliere dati aggregati sugli incidenti dagli Stati membri e pubblicare orientamenti tecnici (articolo 20, paragrafo 9), v) creare e mantenere un registro per soggetti che prestano servizi transfrontalieri (articolo 25).

Pertanto, a partire dal 2022 sarà presentata una richiesta di altri 5 ETP con un bilancio corrispondente a copertura di tali nuovi posti.

– ☐ La proposta/iniziativa non comporta l'utilizzo di stanziamenti amministrativi.

– ☐X La proposta/iniziativa comporta l'utilizzo di stanziamenti amministrativi, come spiegato di seguito:

Mio EUR (al terzo decimale)

	Anno **N** [65] **2022**	Anno **N+1** **2023**	Anno **N+2** **2024**	Anno **N+3** **2025**	Inserire gli anni necessari per evidenziare la durata dell'incidenza (cfr. punto 1.6) **2026**	**2027**		**TOTALE**
Agenti temporanei (gradi AD)	0,450	0,450	0,450	0,450	0,450	0,450		**2,7**
Agenti temporanei (gradi AST)								
Agenti contrattuali	0,160	0,160	0,160	0,160	0,160	0,160		**0,96**
Esperti nazionali distaccati								
TOTALE	**0,61**	**0,61**	**0,61**	**0,61**	**0,61**	**0,61**		**3,66**

Fabbisogno di personale (ETP):

[65] L'anno N è l'anno in cui inizia a essere attuata la proposta/iniziativa. Sostituire "N" con il primo anno di attuazione previsto (ad es: 2021) e così per gli anni a seguire.

	Anno **N** [66] **2022**	Anno **N+1** **2023**	Anno **N+2** **2024**	Anno **N+3** **2025**	Inserire gli anni necessari per evidenziare la durata dell'incidenza (cfr. punto 1.6) **2026** **2027**			**TOTALE**
Agenti temporanei (gradi AD)	3	3	3	3	3	3		**18**
Agenti temporanei (gradi AST)								
Agenti contrattuali	2	2	2	2	2	2		**12**
Esperti nazionali distaccati								
TOTALE	**5**	**5**	**5**	**5**	**5**	**5**		**30**

3.2.3.2. Fabbisogno previsto di risorse umane per la DG di riferimento

– ☐ La proposta/iniziativa non comporta l'utilizzo di risorse umane.

– ☐ La proposta/iniziativa comporta l'utilizzo di risorse umane, come spiegato di seguito:

Stima da esprimere in numeri interi (o, al massimo, con un decimale)

	Anno **N**	Anno **N+1**	Anno **N+2**	Anno **N+3**	Inserire gli anni necessari per evidenziare la durata dell'incidenza (cfr. punto 1.6)		
• **Posti della tabella dell'organico (funzionari e agenti temporanei)**							
XX 01 01 01 (in sede e negli uffici di rappresentanza della Commissione)							
XX 01 01 02 (nelle delegazioni)							
XX 01 05 01 (ricerca indiretta)							
10 01 05 01 (ricerca diretta)							
• **Personale esterno (in equivalenti a tempo pieno: ETP)**[67]							

66 L'anno N è l'anno in cui inizia a essere attuata la proposta/iniziativa. Sostituire "N" con il primo anno di attuazione previsto (ad es: 2021) e così per gli anni a seguire.

XX 01 02 01 (AC, END e INT della dotazione globale)								
XX 01 02 02 (AC, AL, END, INT e JPD nelle delegazioni)								
XX 01 04 ***aa***[68]	- in sede[69]							
	- nelle delegazioni							
XX 01 05 02 (AC, END, INT – ricerca indiretta)								
10 01 05 02 (AC, END, INT - ricerca diretta)								
Altre linee di bilancio (specificare)								
TOTALE								

XX è il settore o il titolo di bilancio interessato.

Il fabbisogno di risorse umane è coperto dal personale della DG già assegnato alla gestione dell'azione e/o riassegnato all'interno della stessa DG, integrato dall'eventuale dotazione supplementare concessa alla DG responsabile nell'ambito della procedura annuale di assegnazione, tenendo conto dei vincoli di bilancio.

Descrizione dei compiti da svolgere:

Funzionari e agenti temporanei	
Personale esterno	

La descrizione del calcolo dei costi per un ETP dovrebbe essere inclusa nell'allegato V, sezione 3.

67 AC = agente contrattuale; AL = agente locale; END = esperto nazionale distaccato; INT = personale interinale (intérimaire); JPD = giovane professionista in delegazione.

68 Sottomassimale per il personale esterno previsto dagli stanziamenti operativi (ex linee "BA").

69 Principalmente per i fondi strutturali, il Fondo europeo agricolo per lo sviluppo rurale (FEASR) e il Fondo europeo per la pesca (FEP).

3.2.4. Compatibilità con il quadro finanziario pluriennale attuale

– ☐x La proposta/iniziativa è compatibile con il quadro finanziario pluriennale attuale.

– ☐ La proposta/iniziativa richiederà una riprogrammazione della pertinente rubrica del quadro finanziario pluriennale.

Spiegare la riprogrammazione richiesta, precisando le linee di bilancio interessate e gli importi corrispondenti. La proposta è compatibile con il quadro finanziario pluriennale 21/27. La compensazione del bilancio necessaria per coprire l'aumento delle risorse umane nell'ENISA sarà effettuata riducendo dello stesso importo il bilancio del programma Europa digitale (DEP) nella stessa rubrica.

– ☐ La proposta/iniziativa richiede l'applicazione dello strumento di flessibilità o la revisione del quadro finanziario pluriennale[70].

Spiegare la necessità, precisando le rubriche e le linee di bilancio interessate e gli importi corrispondenti.

3.2.5. Partecipazione di terzi al finanziamento

– La proposta/iniziativa non prevede cofinanziamenti da terzi.

– La proposta/iniziativa prevede il cofinanziamento indicato di seguito:

Mio EUR (al terzo decimale)

	Anno **N**	Anno **N+1**	Anno **N+2**	Anno **N+3**	Inserire gli anni necessari per evidenziare la durata dell'incidenza (cfr. punto 1.6)			Totale
Specificare l'organismo di cofinanziamento								
TOTALE degli stanziamenti cofinanziati								

[70] Cfr. gli articoli 11 e 17 del regolamento (UE, Euratom) n. 1311/2013 del Consiglio, che stabilisce il quadro finanziario pluriennale per il periodo 2014-2020.

3.3. Incidenza prevista sulle entrate

– ☐ La proposta/iniziativa non ha incidenza finanziaria sulle entrate.

– ☐ La proposta/iniziativa ha la seguente incidenza finanziaria:

☐ sulle risorse proprie

☐ su altre entrate

☐ indicare se le entrate sono destinate a linee di spesa specifiche

Mio EUR (al terzo decimale)

Linea di bilancio delle entrate:	Stanziamenti disponibili per l'esercizio in corso	Incidenza della proposta/iniziativa[71]						
		Anno **N**	Anno **N+1**	Anno **N+2**	Anno **N+3**	Inserire gli anni necessari per evidenziare la durata dell'incidenza (cfr. punto 1.6)		
Articolo …….								

Per quanto riguarda le entrate varie con destinazione specifica, precisare la o le linee di spesa interessate.

Precisare il metodo di calcolo dell'incidenza sulle entrate.

[71] Per le risorse proprie tradizionali (dazi doganali, contributi zucchero), indicare gli importi netti, cioè gli importi lordi al netto del 20 % per spese di riscossione.