I

(Atti legislativi)

DIRETTIVE

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

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 ([1]),

deliberando secondo la procedura legislativa ordinaria ([2]),

considerando quanto segue:

(1) Le reti e i sistemi e servizi informativi svolgono un ruolo vitale nella società. È essenziale che essi siano affidabili e sicuri per le attività economiche e sociali e in particolare ai fini del funzionamento del mercato interno.

(2) La portata, la frequenza e l'impatto degli incidenti a carico della sicurezza stanno aumentando e rappresentano una grave minaccia per il funzionamento delle reti e dei sistemi informativi. Tali sistemi possono inoltre diventare un bersaglio per azioni intenzionalmente tese a danneggiare o interrompere il funzionamento dei sistemi. Tali incidenti possono impedire l'esercizio delle attività economiche, provocare notevoli perdite finanziarie, minare la fiducia degli utenti e causare gravi danni all'economia dell'Unione.

(3) Le reti e i sistemi informativi, e in prima linea internet, svolgono un ruolo essenziale nell'agevolare i movimenti transfrontalieri di beni, servizi e persone. Tenendo conto di questa dimensione transnazionale, gravi perturbazioni di tali sistemi, intenzionali o meno e indipendentemente dal luogo in cui si verificano, possono ripercuotersi su singoli Stati membri e avere conseguenze in tutta l'Unione. La sicurezza delle reti e dei sistemi informativi è quindi essenziale per l'armonioso funzionamento del mercato interno.

(4) Basandosi sui notevoli progressi compiuti nell'ambito del Forum europeo degli Stati membri nel promuovere le discussioni e gli scambi di buone pratiche, come l'elaborazione dei principi della collaborazione europea in caso di crisi cibernetica, è opportuno istituire un gruppo di cooperazione composto da rappresentanti degli Stati membri, dalla Commissione e dall'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA) al fine di sostenere e agevolare la cooperazione strategica fra gli Stati membri in relazione alla sicurezza

([1]) GU C 271 del 19.9.2013, pag. 133.
([2]) Posizione del Parlamento europeo del 13 marzo 2014 (non ancora pubblicata nella Gazzetta ufficiale) e posizione del Consiglio in prima lettura del 17 maggio 2016 (non ancora pubblicata nella Gazzetta ufficiale). Posizione del Parlamento europeo del 6 luglio 2016 (non ancora pubblicata nella Gazzetta ufficiale).

delle reti e dei sistemi informativi. Perché tale gruppo sia efficace e inclusivo è essenziale che tutti gli Stati membri dispongano di un livello minimo di capacità e si dotino di una strategia per garantire un livello elevato di sicurezza delle reti e dei sistemi informativi sul loro territorio. È inoltre opportuno che agli operatori di servizi essenziali e ai fornitori di servizi digitali si applichino obblighi in materia di sicurezza e notifica per promuovere una cultura della gestione dei rischi e garantire la segnalazione degli incidenti più gravi.

(5) Le capacità esistenti non bastano a garantire un livello elevato di sicurezza delle reti e dei sistemi informativi nell'Unione. I livelli di preparazione negli Stati membri sono molto diversi tra loro il che ha comportato una frammentazione degli approcci nell'Unione. Ne deriva un livello disomogeneo di protezione dei consumatori e delle imprese che compromette il livello globale di sicurezza delle reti e dei sistemi informativi nell'Unione. La mancanza di obblighi comuni imposti agli operatori di servizi essenziali e ai fornitori di servizi digitali rende inoltre impossibile la creazione di un meccanismo globale ed efficace di cooperazione a livello dell'Unione. Le università e i centri di ricerca svolgono un ruolo determinante nell'incentivare la ricerca, lo sviluppo e l'innovazione in tali settori.

(6) Per una risposta efficace alle sfide in materia di sicurezza delle reti e dei sistemi informativi è pertanto necessario un approccio globale a livello di Unione, che contempli la creazione di una capacità minima comune e disposizioni minime in materia di pianificazione, scambio di informazioni, cooperazione e obblighi comuni di sicurezza per gli operatori di servizi essenziali e i fornitori di servizi digitali. Nulla osta tuttavia a che gli operatori di servizi essenziali e i fornitori di servizi digitali applichino misure di sicurezza che siano più rigorose di quelle previste ai sensi della presente direttiva.

(7) È opportuno che la presente direttiva si applichi sia agli operatori di servizi essenziali che ai fornitori di servizi digitali in modo da coprire tutti i relativi rischi e incidenti. È opportuno tuttavia che gli obblighi imposti agli operatori di servizi essenziali e ai fornitori di servizi digitali non si applichino alle imprese che forniscono reti pubbliche di comunicazioni o servizi di comunicazione elettronica accessibili al pubblico, ai sensi della direttiva 2002/21/CE del Parlamento europeo e del Consiglio ([1]), perché tali imprese sono soggette a specifici obblighi di sicurezza e integrità previsti da detta direttiva; i suddetti obblighi non dovrebbero inoltre applicarsi ai prestatori di servizi fiduciari ai sensi del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio ([2]), che sono soggetti agli obblighi di sicurezza previsti in tale regolamento.

(8) La presente direttiva dovrebbe lasciare impregiudicata la possibilità, per ciascuno Stato membro, di adottare le misure necessarie per assicurare la tutela degli interessi essenziali della sua sicurezza, salvaguardare l'ordine pubblico e la pubblica sicurezza e consentire la ricerca, l'individuazione e il perseguimento dei reati. Conformemente all'articolo 346 del trattato sul funzionamento dell'Unione europea (TFUE), nessuno Stato membro è tenuto a fornire informazioni la cui divulgazione sia dallo stesso considerata contraria agli interessi essenziali della propria sicurezza. In tale contesto sono pertinenti la decisione 2013/488/UE del Consiglio ([3]) e gli accordi di non divulgazione o gli accordi di non divulgazione informali, quale il protocollo del semaforo (*Traffic Light Protocol*).

(9) Determinati settori dell'economia sono già regolamentati, o potrebbero esserlo in futuro, da atti giuridici settoriali dell'Unione comprendenti norme in materia di sicurezza delle reti e dei sistemi informativi. Ogniqualvolta tali atti giuridici dell'Unione contengono disposizioni che impongono obblighi in materia di sicurezza delle reti e dei sistemi informativi o di notifica di incidenti, si dovrebbero applicare tali disposizioni se gli obblighi ivi contenuti hanno effetti almeno equivalenti a quelli previsti dalla presente direttiva. Gli Stati membri dovrebbero allora applicare le disposizioni dell'atto giuridico settoriale dell'Unione, comprese quelle in materia di giurisdizione, e non compiere il processo di identificazione per gli operatori di servizi essenziali di cui alla presente direttiva. In tale contesto gli Stati membri dovrebbero fornire alla Commissione informazioni in merito all'applicazione di tali disposizioni sulla *lex specialis*. Nel determinare se gli obblighi in materia di sicurezza delle reti e dei sistemi informativi e di notifica di incidenti contenuti negli atti giuridici settoriali dell'Unione siano equivalenti a quelli di cui alla presente direttiva, si dovrebbero tenere in considerazione esclusivamente le disposizioni degli atti giuridici dell'Unione pertinenti e la loro applicazione negli Stati membri.

(10) Nel settore del trasporto per via d'acqua, gli obblighi di sicurezza per le compagnie, le navi, gli impianti portuali, i porti e i servizi di gestione del traffico navale, ai sensi degli atti giuridici dell'Unione, riguardano tutte le operazioni, compresi i sistemi di radio e telecomunicazione, i sistemi informatici e le reti. Una parte delle procedure obbligatorie da seguire prevede la segnalazione di tutti gli incidenti e dovrebbe pertanto essere considerata come *lex specialis*, nella misura in cui detti obblighi siano almeno equivalenti alle corrispondenti disposizioni della presente direttiva.

([1]) Direttiva 2002/21/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002, che istituisce un quadro normativo comune per le reti ed i servizi di comunicazione elettronica (direttiva quadro) (GU L 108 del 24.4.2002, pag. 33).

([2]) 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).

([3]) Decisione 2013/488/UE del Consiglio, del 23 settembre 2013, sulle norme di sicurezza per le informazioni classificate UE (GU L 274 del 15.10.2013, pag. 1).

(11) Nell'identificare gli operatori nel settore del trasporto per via d'acqua, gli Stati membri dovrebbero tener conto dei codici internazionali e delle linee guida attuali e futuri sviluppati in particolare dall' Organizzazione marittima internazionale, al fine di fornire ai singoli operatori marittimi un approccio coerente.

(12) La regolamentazione e la vigilanza nel settore bancario e in quello delle infrastrutture dei mercati finanziari sono altamente armonizzate a livello dell'Unione, mediante l'applicazione del diritto primario e secondario dell'Unione e delle norme sviluppate con le autorità europee di vigilanza. All'interno dell'unione bancaria, l'applicazione e la vigilanza con riguardo a tali obblighi sono assicurate dal meccanismo di vigilanza unico. Per gli Stati membri che non fanno parte dell'Unione bancaria esse sono assicurate dalle pertinenti autorità nazionali di regolamentazione del settore bancario. In altri ambiti della regolamentazione del settore finanziario, il Sistema europeo di vigilanza finanziaria assicura anch'esso un elevato grado di analogia e convergenza nelle pratiche di vigilanza. Anche l'Autorità europea degli strumenti finanziari e dei mercati svolge un ruolo di vigilanza diretto per taluni soggetti (vale a dire agenzie di rating del credito e repertori di dati sulle negoziazioni).

(13) Il rischio operativo rappresenta un elemento cruciale della regolamentazione e vigilanza prudenziali nel settore bancario e in quello delle infrastrutture dei mercati finanziari. Copre tutte le operazioni comprese la sicurezza, l'integrità e la resilienza delle reti e dei sistemi informativi. Gli obblighi riguardo a tali sistemi, che spesso vanno al di là di quelli previsti nell'ambito della presente direttiva, sono stabiliti in vari atti giuridici dell'Unione, comprendenti le norme sull'accesso all'attività degli enti creditizi e sulla vigilanza prudenziale degli enti creditizi e delle imprese di investimento e le norme sui requisiti prudenziali per gli enti creditizi e le imprese di investimento, comprendenti obblighi in materia di rischio operativo, nonché le norme sui mercati degli strumenti finanziari, comprendenti obblighi sulla valutazione del rischio per le imprese di investimento e per i mercati regolamentati, le norme sugli strumenti derivati OTC, le controparti centrali e i repertori di dati sulle negoziazioni, comprendenti obblighi in materia di rischio operativo per le controparti centrali e i repertori di dati sulle negoziazioni, e le norme sul miglioramento del regolamento titoli nell'Unione e sui depositari centrali di titoli, comprendenti obblighi in materia di rischio operativo. Inoltre, gli obblighi in materia di notifica di incidenti rientrano nella normale prassi di vigilanza nel settore finanziario e sono spesso inclusi nei manuali di vigilanza. Gli Stati membri dovrebbero prendere in considerazione dette norme e obblighi nell'applicazione della *lex specialis*.

(14) Come rilevato dalla Banca centrale europea nel suo parere del 25 luglio 2014 ([1]), la presente direttiva non incide sul regime previsto dal diritto dell'Unione per la sorveglianza dell'Eurosistema sui sistemi di pagamento e di regolamento. Sarebbe opportuno che le autorità responsabili di tale sorveglianza scambino esperienze sugli aspetti riguardanti la sicurezza delle reti e dei sistemi informativi con le autorità competenti ai sensi della presente direttiva. Lo stesso vale per i membri del Sistema europeo di banche centrali non appartenenti alla zona Euro che esercitano tale sorveglianza sui sistemi di pagamento e di regolamento sulla base di leggi e regolamenti nazionali.

(15) Un mercato online consente ai consumatori e ai professionisti di concludere contratti di vendita o di servizi online con i professionisti, e costituisce la destinazione finale per la conclusione di tali contratti. Non dovrebbe contemplare servizi online che fungono solo da intermediari per servizi di un terzo con cui, in ultima istanza, possono essere conclusi i contratti. Non dovrebbe pertanto contemplare i servizi online che raffrontano i prezzi di particolari prodotti o servizi forniti da diversi professionisti e rimandano quindi l'utente al professionista prescelto per l'acquisto del prodotto. I servizi informatici forniti dal mercato online possono comprendere trattamento di operazioni, aggregazioni di dati o profilazione degli utenti. I negozi di applicazioni, che operano come negozi online e consentono la distribuzione digitale di applicazioni o programmi software, è devono essere considerati un tipo di mercato online.

(16) In linea di principio, un motore di ricerca online consente all'utente di effettuare ricerche in tutti i siti web sulla base di un'interrogazione su qualsiasi tema. In alternativa, può concentrarsi sui siti web in una lingua particolare. La definizione di motore di ricerca online fornita nella presente direttiva non dovrebbe contemplare funzioni di ricerca limitate al contenuto di un sito web specifico, indipendentemente dal fatto che la funzione di ricerca sia messa a disposizione da un motore di ricerca esterno. Non dovrebbe contemplare neppure i servizi online che raffrontano i prezzi di particolari prodotti o servizi forniti da diversi professionisti e rimandano quindi l'utente al professionista prescelto per l'acquisto del prodotto.

(17) I servizi nella nuvola (*cloud computing*) coprono un'ampia gamma di attività che possono essere fornite sulla base di modelli diversi. Ai fini della presente direttiva, l'espressione «servizi nella nuvola» comprende i servizi che consentono l'accesso a un insieme scalabile ed elastico di risorse informatiche condivisibili. Dette risorse informatiche comprendono risorse quali reti, server o altre infrastrutture, archiviazione, applicazioni e servizi. Il termine «scalabile» si riferisce alle risorse informatiche che sono assegnate in modo flessibile dal fornitore di servizi nella nuvola, indipendentemente dall'ubicazione geografica delle risorse, per gestire le fluttuazioni della domanda. L'espressione «insieme elastico» è usata per descrivere quelle risorse informatiche che sono fornite e

([1]) GU C 352 del 7.10.2014, pag. 4.

diffuse in base alla richiesta, al fine di aumentare e ridurre rapidamente le risorse disponibili in base al carico di lavoro. Il termine «condivisibile» è usato per descrivere le risorse informatiche che sono fornite a una molteplicità di utenti che condividono un accesso comune al servizio, mentre il trattamento è effettuato separatamente per ogni utente anche se il servizio è fornito a partire dalla stessa apparecchiatura elettronica.

(18) La funzione di un punto di interscambio internet (IXP) è interconnettere le reti. Un IXP non fornisce accesso alla rete, né funziona da fornitore o carrier di transito. Non fornisce nepure altri servizi non correlati all'interconnessione, per quanto ciò non impedisca a un operatore IXP di fornire servizi non correlati. Lo scopo di un IXP è connettere reti tecnicamente e organizzativamente separate. Per descrivere una rete tecnicamente indipendente si usa l'espressione sistema autonomo.

(19) Gli Stati membri dovrebbero essere competenti per determinare quali soggetti soddisfino i criteri stabiliti nella definizione di operatore di servizi essenziali. Al fine di garantire un approccio uniforme, è opportuno che la definizione di operatore di servizi essenziali sia applicata in modo coerente da tutti gli Stati membri. A tal fine la presente direttiva prevede la valutazione dei soggetti attivi in specifici settori e sottosettori, la definizione di un elenco di servizi essenziali, l'esame di un elenco comune di fattori intersettoriali per stabilire se un potenziale incidente avrebbe effetti negativi rilevanti, un processo di consultazione che coinvolga gli Stati membri interessati nel caso di soggetti che forniscono servizi in più Stati membri, e il sostegno del gruppo di cooperazione nel processo di identificazione. Al fine di garantire che eventuali evoluzioni del mercato siano tenute accuratamente in considerazione, l'elenco di operatori identificati dovrebbe essere rivisto periodicamente dagli Stati membri e aggiornato ove necessario. Infine, gli Stati membri dovrebbero trasmettere alla Commissione le informazioni necessarie per valutare in che misure tale metodologia comune consenta un'applicazione coerente della definizione da parte degli Stati membri.

(20) Nel processo di identificazione degli operatori di servizi essenziali, gli Stati membri dovrebbero valutare, almeno per ciascun sottosettore di cui alla presente direttiva, quali servizi debbano essere considerati essenziali per il mantenimento di attività sociali ed economiche fondamentali e se i soggetti elencati nei settori e sottosettori di cui alla presente direttiva, che forniscono tali servizi, rispettino i criteri per l'identificazione degli operatori. Nel valutare se un soggetto fornisce un servizio essenziale per il mantenimento di attività sociali ed economiche fondamentali, è sufficiente esaminare se tale soggetto fornisce un servizio incluso nell'elenco di servizi esenziali. Si dovrebbe inoltre dimostrare che la fornitura del servizio essenziale dipende dalle reti e dai sistemi informativi. Infine, nel valutare se un incidente avrebbe un effetto negativo significativo sulla fornitura del servizio, gli Stati membri dovrebbero tenere conto di una serie di fattori intersettoriali, nonché, ove opportuno, di fattori settoriali.

(21) Ai fini dell'identificazione di operatori di servizi essenziali, lo stabilimento in uno Stato membro implica l'effettivo e reale svolgimento di 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.

(22) È possibile che soggetti che operano nei settori e sottosettori di cui alla presente direttiva forniscano sia servizi essenziali che non essenziali. Nel settore del trasporto aereo, ad esempio, gli aeroporti forniscono servizi che potrebbero essere considerati essenziali da uno Stato membro, come la gestione delle piste, ma anche una serie di servizi che potrebbero essere considerati non essenziali, come l'allestimento di aree commerciali. Gli operatori di servizi essenziali dovrebbero essere soggetti a specifici obblighi di sicurezza solo in relazione ai servizi considerati essenziali. Ai fini dell'identificazione degli operatori, gli Stati membri dovrebbero pertanto definire un elenco di servizi considerati essenziali.

(23) L'elenco di servizi dovrebbe contenere tutti i servizi forniti nel territorio di un determinato Stato membro che soddisfano i requisiti di cui alla presente direttiva. Gli Stati membri dovrebbero poter integrare l'elenco esistente includendovi nuovi servizi. L'elenco di servizi dovrebbe servire agli Stati membri come riferimento per l'identificazione degli operatori di servizi essenziali. Ha lo scopo di identificare i tipi di servizi essenziali in ciascuno dei settori di cui alla presente direttiva, distinguendoli così dalle attività non essenziali di cui potrebbe essere responsabile un soggetto attivo in un determinato settore. L'elenco di servizi stilato da ciascuno Stato membro costituirebbe un ulteriore contributo nella valutazione della pratica regolamentare di ciascuno Stato membro al fine di assicurare il livello globale di coerenza del processo di identificazione fra gli Stati membri.

(24) Ai fini del processo di identificazione è opportuno che, nel caso in cui un soggetto fornisca un servizio essenziale in due o più Stati membri, tali Stati membri intraprendano discussioni bilaterali o multilaterali tra di loro. Questo processo di consultazione è inteso ad aiutarli a valutare la natura critica dell'operatore in termini di impatto transfrontaliero, consentendo in tal modo a ciascuno degli Stati membri interessati di presentare la propria posizione in merito ai rischi connessi ai servizi forniti. Gli Stati membri interessati dovrebbero tener conto delle rispettive posizioni in tale processo dovrebbero poter chiedere l'assistenza del gruppo di cooperazione al riguardo.

(25) In seguito al processo di identificazione, gli Stati membri dovrebbero adottare misure nazionali dirette a determinare i soggetti cui si applicano gli obblighi in materia di sicurezza delle reti e dei sistemi informativi. Tale risultato potrebbe essere raggiunto adottando un elenco di tutti gli operatori di servizi essenziali oppure adottando misure nazionali comprendenti criteri oggettivi quantificabili, quali la produzione dell'operatore o il numero di utenti, che rendano possibile determinare a quali soggetti si applichino i predetti obblighi in materia di sicurezza delle reti e dei sistemi informativi. Le misure nazionali, siano esse già esistenti o adottate nel contesto della presente direttiva, dovrebbero includere tutte le misure giuridiche, le misure amministrative e le prassi che rendano possibile l'identificazione degli operatori di servizi essenziali ai sensi della presente direttiva.

(26) Per fornire un'indicazione dell'importanza in relazione al settore interessato degli operatori identificati di servizi essenziali, gli Stati membri dovrebbero tener conto del numero e delle dimensioni di tali operatori identificati, ad esempio in termini di quota di mercato o di quantitativo prodotto o trasportato, senza essere obbligati a divulgare informazioni che rivelerebbero gli operatori identificati.

(27) Al fine di stabilire se un incidente avrebbe effetti negativi rilevanti sulla fornitura di un servizio, gli Stati membri dovrebbero tener conto di svariati fattori, quali il numero di utenti collegati a tale servizio per scopi privati o professionali. L'uso di detto servizio può essere diretto, indiretto o intermediato. Nel valutare l'impatto che un incidente potrebbe avere, in termini di entità e di durata, sulle attività economiche e sociali o sulla pubblica sicurezza, gli Stati membri dovrebbero altresì valutare il tempo che presumibilmente trascorrerebbe prima che la discontinuità inizi a produrre un impatto negativo.

(28) In aggiunta ai fattori intersettoriali si dovrebbe tener conto anche di fattori settoriali al fine di stabilire se un incidente avrebbe effetti negativi rilevanti sulla fornitura di un servizio essenziale. Tali fattori potrebbero comprendere: per i fornitori di energia, il volume o la quota di energia nazionale prodotta; per i fornitori di petrolio, il volume su base giornaliera; per il trasporto aereo, inclusi aeroporti e vettori aerei, il trasporto ferroviario e i porti marittimi, la quota di volume di traffico nazionale e il numero di passeggeri o di operazioni di trasporto merci su base annua; per il settore bancario o le infrastrutture dei mercati finanziari, la loro importanza sistemica in base alle attività totali o al rapporto tra tali attività totali e il PIL; per il settore sanitario, il numero di pazienti assistiti dal fornitore su base annua; per la produzione, il trattamento e la fornitura di acqua, il volume e il numero e i tipi di utenti riforniti, inclusi, ad esempio, ospedali, servizi pubblici, organizzazioni o persone fisiche, nonché l'esistenza di fonti idriche alternative per servire la stessa area geografica.

(29) Per conseguire e mantenere un livello elevato di sicurezza della rete e dei sistemi informativi è opportuno che ogni Stato membro disponga di una strategia nazionale in materia di sicurezza della rete e dei sistemi informativi che definisca gli obiettivi strategici e gli interventi strategici concreti da attuare.

(30) 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 ed evitare duplicazioni, è opportuno che gli Stati membri abbiano la facoltà di designare più di un'autorità nazionale competente responsabile di soddisfare i compiti connessi alla sicurezza delle reti e dei sistemi informativi degli operatori di servizi essenziali e dei fornitori di servizi digitali di cui alla presente direttiva.

(31) Onde agevolare la cooperazione e la comunicazione transfrontaliere e permettere che la presente direttiva sia attuata efficacemente, è necessario che ogni Stato membro, fatti salvi gli accordi settoriali in materia di regolamentazione, designi un punto di contatto nazionale unico incaricato di coordinare le questioni relative alla sicurezza delle reti e dei sistemi informativi e la cooperazione transfrontaliera a livello di Unione. Le autorità competenti e i punti di contatto unici dovrebbero essere dotate di risorse adeguate sul piano tecnico, finanziario e umano per garantire loro di eseguire in modo efficiente ed efficace i compiti loro assegnati e conseguire in questo modo gli obiettivi della presente direttiva. Poiché la presente direttiva è intesa a migliorare il funzionamento del mercato interno creando un clima di fiducia e sicurezza, gli organi degli Stati membri devono poter cooperare in modo efficace con gli attori economici ed essere strutturati di conseguenza.

(32) Le autorità competenti o i gruppi di intervento per la sicurezza informatica in caso di incidente («CSIRT») dovrebbero ricevere le notifiche di incidenti. I punti di contatto unici non dovrebbero ricevere direttamente le notifiche di incidenti, a meno che non fungano anche da autorità competente o da un CSIRT. Un'autorità competente o un CSIRT dovrebbe tuttavia poter incaricare il punto di contatto unico di trasmettere notifiche di incidenti ai punti di contatto unici degli altri Stati membri interessati.

(33) Per garantire l'effettiva fornitura di informazioni agli Stati membri e alla Commissione, una relazione sintetica dovrebbe essere presentata dal punto di contatto unico al gruppo di cooperazione e dovrebbe essere resa anonima per tutelare la riservatezza delle notifiche e dell'identità degli operatori di servizi essenziali e dei fornitori di servizi digitali, dal momento che non occorrono informazioni sull'identità dei soggetti notificanti per lo scambio di migliori prassi nel gruppo di cooperazione. La relazione sintetica dovrebbe includere informazioni sul numero di notifiche ricevute nonché un'indicazione della natura degli incidenti notificati, come i tipi di violazioni della sicurezza, la loro gravità o la loro durata.

(34) È opportuno che gli Stati membri siano dotati delle capacità tecniche e organizzative necessarie a prevenire, individuare, rispondere e attenuare i rischi e gli incidenti a carico delle reti e dei sistemi informativi. 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, in modo da garantire l'esistenza di capacità effettive e compatibili per far fronte ai rischi e agli incidenti e garantire un'efficiente collaborazione a livello di Unione. Per consentire a tutti i tipi di operatori di servizi essenziali e fornitori di servizi digitali di beneficiare di tali capacità e cooperazione, gli Stati membri dovrebbero assicurare che tutti i tipi siano contemplati da un CSIRT designato. 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.

(35) Poiché la maggioranza delle reti e dei sistemi informativi è gestita da privati, la collaborazione tra il settore pubblico e il settore privato è essenziale. Gli operatori di servizi essenziali e i fornitori di servizi digitali dovrebbero essere incoraggiati a portare avanti propri meccanismi informali di collaborazione per garantire la sicurezza delle reti e dei sistemi informativi. Il gruppo di cooperazione dovrebbe avere la possibilità, se del caso, di invitare le parti interessate a partecipare alle discussioni. Per incoraggiare efficacemente la condivisione di informazioni e migliori pratiche, è essenziale garantire che gli operatori di servizi essenziali e i fornitori di servizi digitali che partecipano a tali scambi non siano svantaggiati in conseguenza della loro cooperazione.

(36) L'ENISA dovrebbe assistere gli Stati membri e la Commissione mettendo loro a disposizione le proprie competenze e consulenze e agevolando lo scambio di migliori prassi. In particolare, nell'applicazione della presente direttiva la Commissione dovrebbe consultare l'ENISA e gli Stati membri ne dovrebbero avere la facoltà. Per creare capacità e conoscenze tra gli Stati membri, il gruppo di cooperazione dovrebbe anche servire da strumento per scambiare migliori prassi, discutere delle capacità e della preparazione degli Stati membri e, su base volontaria, assistere i propri membri nella valutazione delle strategie nazionali in materia di sicurezza della rete e dei sistemi informativi, nella creazione di capacità e valutare le esercitazioni in materia di sicurezza della rete e dei sistemi informativi.

(37) Laddove opportuno, gli Stati membri dovrebbero poter utilizzare o adattare le strutture organizzative o le strategie esistenti al momento di applicare la presente direttiva.

(38) I rispettivi compiti del gruppo di cooperazione e dell'ENISA sono interdipendenti e complementari. In linea generale, l'ENISA dovrebbe assistere il gruppo di cooperazione nell'esecuzione dei suoi compiti, in linea con l'obiettivo dell'ENISA nel regolamento (UE) n. 526/2013 del Parlamento europeo e del Consiglio [1], vale a dire di assistere le istituzioni, gli organi e gli organismi dell'Unione e gli Stati membri nell'attuazione delle politiche necessarie a soddisfare le prescrizioni legali e regolamentari in materia di sicurezza della rete e dei sistemi informativi previste dagli atti giuridici vigenti e futuri dell'Unione. In particolare, l'ENISA dovrebbe fornire assistenza nei settori corrispondenti ai propri compiti di cui al regolamento (UE) n. 526/2013, vale a dire analizzare strategie in materia di sicurezza della rete e dei sistemi informativi, sostenere l'organizzazione e lo svolgimento di esercitazioni a livello dell'Unione in materia di sicurezza della rete e dei sistemi informativi e scambiare informazioni e migliori prassi in materia di sensibilizzazione e formazione. L'ENISA dovrebbe anche partecipare all'elaborazione di linee guida per i criteri settoriali per determinare la rilevanza dell'impatto di un incidente.

[1] Regolamento (UE) n. 526/2013 del Parlamento europeo e del Consiglio, del 21 maggio 2013, relativo all'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA) e che abroga il regolamento (CE) n. 460/2004 (GU L 165 del 18.6.2013, pag. 41).

(39) Al fine di promuovere un livello avanzato di sicurezza delle reti e dei sistemi informativi, il gruppo di cooperazione dovrebbe, se del caso, collaborare con le istituzioni, gli organi e gli organismi competenti dell'Unione per scambiare conoscenze e migliori prassi e fornire consulenze sugli aspetti in materia sicurezza delle reti e dei sistemi informativi che potrebbero avere un impatto sulle loro attività, nel rispetto dei meccanismi esistenti per lo scambio di informazioni riservate. Nella collaborazione con le autorità incaricate dell'applicazione delle norme su aspetti relativi alla sicurezza della rete e dei sistemi informativi che possono avere un impatto sull'attività di questi ultimi, il gruppo di cooperazione dovrebbe avvalersi dei canali di informazione e delle reti esistenti.

(40) Le informazioni sugli incidenti sono sempre più preziose per il pubblico in generale e per le imprese, in particolare le piccole e medie imprese. In alcuni casi, tali informazioni sono già fornite attraverso siti web a livello nazionale, nella lingua di un determinato paese e ponendo l'accento principalmente su incidenti ed avvenimenti con una dimensione nazionale. Poiché sempre più spesso le imprese operano a livello transfrontaliero e i cittadini utilizzano servizi online, le informazioni sugli incidenti dovrebbero essere fornite in forma aggregata a livello dell'Unione. Il segretariato della rete di CSIRT è incoraggiato a gestire un sito web o a ospitare una pagina dedicata su un sito web esistente in cui si mettano a disposizione del pubblico informazioni generali sui principali incidenti verificatisi in tutta l'Unione, con particolare attenzione agli interessi e alle esigenze delle imprese. I CSIRT partecipanti alla rete di CSIRT sono incoraggiati a fornire, su base volontaria, le informazioni da pubblicare su tale sito web senza comprendere informazioni riservate o sensibili.

(41) Qualora le informazioni siano considerate riservate in virtù di norme dell'Unione e nazionali sulla riservatezza degli affari, è opportuno che tale riservatezza sia garantita nello svolgimento delle attività e nella realizzazione degli obiettivi stabiliti dalla presente direttiva.

(42) Esercitazioni che simulino scenari di incidenti in tempo reale sono essenziali per verificare la preparazione e la cooperazione degli Stati membri in materia di sicurezza delle reti e dei sistemi informativi. Il ciclo di esercitazioni CyberEurope coordinato dall'ENISA con la partecipazione degli Stati membri è uno strumento utile per verificare ed elaborare raccomandazioni su come migliorare nel tempo il trattamento in caso di incidenti a livello dell'Unione. Dato che attualmente gli Stati membri non hanno l'obbligo di pianificare esercitazioni né di parteciparvi, la creazione della rete di CSIRT ai sensi della presente direttiva dovrebbe consentire agli Stati membri di partecipare ad esercitazioni sulla base di accurate scelte strategiche e di pianificazione. Il gruppo di cooperazione istituito ai sensi della presente direttiva dovrebbe discutere le decisioni strategiche relative alle esercitazioni, in particolare, ma non esclusivamente, per quanto riguarda la regolarità delle esercitazioni e la concezione degli scenari. È opportuno che l'ENISA, conformemente al suo mandato, sostenga l'organizzazione e lo svolgimento di esercitazioni a livello dell'Unione mettendo le proprie competenze e consulenze a disposizione del gruppo di cooperazione e della rete di CSIRT.

(43) Data la natura planetaria dei problemi relativi alla sicurezza delle reti e dei sistemi informativi, è necessaria una cooperazione internazionale più stretta per migliorare le norme di sicurezza e gli scambi di informazioni e promuovere un approccio globale comune agli aspetti della sicurezza.

(44) La responsabilità di garantire la sicurezza delle reti e dei sistemi informativi incombe in larga misura agli operatori di servizi essenziali e ai fornitori di servizi digitali. È opportuno promuovere e sviluppare attraverso adeguati obblighi regolamentari e pratiche industriali volontarie una cultura della gestione del rischio, che comprende la valutazione del rischio e l'attuazione di misure di sicurezza commisurate al rischio corso. È altresì fondamentale creare affidabili condizioni di parità per l'efficace funzionamento del gruppo di cooperazione e della rete di CSIRT in modo da garantire la collaborazione effettiva di tutti gli Stati membri.

(45) La presente direttiva si applica soltanto a quelle amministrazioni pubbliche che sono identificate come operatori di servizi essenziali. Spetta pertanto agli Stati membri garantire la sicurezza delle reti e dei sistemi informativi delle pubbliche amministrazioni che non rientrano nel campo di applicazione della presente direttiva.

(46) Le misure di gestione del rischio comprendono misure per individuare eventuali rischi di incidenti, per prevenire, rilevare e affrontare incidenti nonché per attenuarne l'impatto. La sicurezza delle reti e dei sistemi informativi comprende la sicurezza di dati conservati, trasmessi e trattati.

(47) Le autorità competenti dovrebbero mantenere la possibilità di adottare linee guida nazionali riguardanti le circostanze in cui gli operatori di servizi essenziali sono tenuti a notificare gli incidenti.

(48) Molte imprese nell'Unione si affidano a fornitori di servizi digitali per la fornitura dei loro servizi. Poiché alcuni servizi digitali potrebbero rappresentare una risorsa importante per i loro utenti, compresi gli operatori di servizi essenziali, e poiché tali utenti potrebbero non sempre disporre di alternative, la presente direttiva dovrebbe applicarsi anche ai fornitori di detti servizi. La sicurezza, la continuità e l'affidabilità del tipo di servizi digitali di cui alla presente direttiva sono essenziali per il buon funzionamento di molte imprese. La perturbazione di detto servizio digitale potrebbe impedire la fornitura di altri servizi che si basano su di esso e potrebbe dunque avere un impatto su attività economiche e sociali fondamentali nell'Unione. Tali servizi digitali potrebbero pertanto rivestire un'importanza fondamentale per il buon funzionamento delle imprese che dipendono da essi nonché per la partecipazione di tali imprese al mercato interno e agli scambi commerciali transfrontalieri nell'Unione. Tali fornitori di servizi digitali che sono soggetti alla presente direttiva sono quelli che si ritiene offrano servizi digitali su cui fanno sempre più affidamento molte imprese dell'Unione.

(49) I fornitori di servizi digitali dovrebbero garantire un livello di sicurezza commisurato al grado di rischio per la sicurezza dei servizi digitali da essi forniti, data l'importanza dei loro servizi per le operazioni di altre imprese all'interno dell'Unione. In pratica, per gli operatori di servizi essenziali che spesso sono essenziali per il mantenimento delle attività sociali ed economiche critiche, il grado di rischio è più elevato che per i fornitori di servizi digitali. Pertanto, gli obblighi di sicurezza per i fornitori di servizi digitali dovrebbero essere meno rigidi. I fornitori di servizi digitali dovrebbero rimanere liberi di adottare le misure che ritengono adeguate alla gestione dei rischi che corre la sicurezza delle loro reti e dei loro sistemi informativi. Per via della loro natura transfrontaliera, i fornitori di servizi digitali dovrebbero essere oggetto di un approccio più armonizzato a livello di Unione. È opportuno agevolare la specificazione e l'attuazione di tali misure attraverso atti di esecuzione.

(50) Anche se i produttori di hardware e gli sviluppatori di software non sono operatori di servizi essenziali, né sono fornitori di servizi digitali, i loro prodotti rafforzano la sicurezza delle reti e dei sistemi informativi. Essi svolgono pertanto un ruolo importante nel permettere agli operatori di servizi essenziali e ai fornitori di servizi digitali di mettere in sicurezza le loro reti e i loro sistemi informativi. Tali prodotti hardware e software sono già soggetti alle norme esistenti sulla garanzia dei prodotti.

(51) Le misure tecniche e organizzative imposte agli operatori di servizi essenziali e ai fornitori di servizi digitali non dovrebbero richiedere che una particolare informazione commerciale o un particolare prodotto della tecnologia delle comunicazioni sia concepito, sviluppato e fabbricato in una maniera particolare.

(52) È opportuno che gli operatori di servizi essenziali e i fornitori di servizi digitali garantiscano la sicurezza delle reti e dei sistemi informativi di cui fanno uso. Si tratta in particolare di rete e sistemi informativi privati gestiti dal loro personale IT interno oppure la cui sicurezza sia stata esternalizzata. Gli obblighi di sicurezza e di notifica dovrebbero applicarsi agli operatori di servizi essenziali e ai fornitori di servizi digitali indipendentemente dal fatto che la manutenzione delle loro reti e dei loro sistemi informativi sia eseguita al loro interno o sia esternalizzata.

(53) Per evitare di imporre un onere finanziario e amministrativo sproporzionato agli operatori di servizi essenziali e ai fornitori di servizi digitali, è opportuno che gli obblighi siano proporzionati al rischio corso dalla rete e dal sistema informativo di cui si tratta, tenendo conto dello stato dell'arte di tali misure. Nel caso di fornitori di servizi digitali, questi obblighi non dovrebbero applicarsi alle microimprese e alle piccole imprese.

(54) Qualora facciano uso di servizi offerti da fornitori di servizi digitali, in particolare di servizi nella nuvola (cloud computing), le pubbliche amministrazioni degli Stati membri potrebbero voler imporre ai fornitori di tali servizi misure di sicurezza supplementari che vadano al di là di quanto i fornitori di servizi digitali offrirebbero normalmente in base ai requisiti della presente direttiva. Dovrebbero poter procedere in tal senso mediante obblighi contrattuali.

(55) Le definizioni di mercato online, motore di ricerca online e servizio nella nuvola (*cloud computing*) di cui alla presente direttiva sono formulate ai fini specifici di quest'ultima e fatti salvi altri strumenti.

(56) La presente direttiva non dovrebbe impedire agli Stati membri di adottare misure nazionali che obblighino gli organismi del settore pubblico a garantire specifici requisiti di sicurezza nell'ambito degli appalti di servizi nella nuvola. Tali misure nazionali dovrebbero applicarsi all'organismo del settore pubblico di cui si tratta e non al fornitore di servizi nella nuvola.

(57) Stanti le differenze fondamentali tra gli operatori di servizi essenziali, in particolare per il loro collegamento diretto con le infrastrutture fisiche, e i fornitori di servizi digitali, in particolare per la loro natura transnazionale, la presente direttiva dovrebbe adottare un approccio differenziato al livello di armonizzazione relativo ai due gruppi di soggetti. Per gli operatori di servizi essenziali, gli Stati membri dovrebbero poter identificare gli operatori pertinenti ed imporre requisiti più rigorosi di quelli previsti dalla presente direttiva. Gli Stati membri non dovrebbero identificare i fornitori di servizi digitali, in quanto la presente direttiva dovrebbe applicarsi a tutti i fornitori di servizi digitali rientranti nel suo campo di applicazione. Inoltre, la presente direttiva e i relativi atti di esecuzione dovrebbero assicurare un elevato livello di armonizzazione per i fornitori di servizi digitali con riguardo agli obblighi di notifica e di sicurezza. Ciò dovrebbe consentire che i fornitori di servizi digitali siano trattati in modo uniforme in tutta l' Unione, in modo proporzionato alla loro natura e al grado di rischio cui potrebbero essere esposti.

(58) La presente direttiva non dovrebbe precludere agli Stati membri di imporre obblighi di sicurezza e di notifica a soggetti che non sono fornitori di servizi digitali rientranti nell'ambito di applicazione della presente direttiva, fatti salvi gli obblighi imposti agli Stati membri dal diritto dell'Unione.

(59) È opportuno che le autorità competenti provvedano in particolare alla salvaguardia dell'esistenza di canali informali e affidabili di scambio di informazioni. La pubblicità degli incidenti segnalati alle autorità competenti dovrebbe contemperare l'opportunità che il pubblico sia informato delle minacce esistenti nei confronti di possibili danni di immagine e commerciali per gli operatori di servizi essenziali e i fornitori di servizi digitali che segnalano gli incidenti. Nell'attuare gli obblighi di notifica è opportuno che le autorità competenti e i CSIRT tengano adeguatamente conto della necessità di mantenere strettamente riservate le informazioni sulle vulnerabilità del prodotto prima di diffondere i rimedi di sicurezza appropriati.

(60) I prestatori di servizi digitali dovrebbero essere soggetti ad attività di vigilanza *ex post* semplificate e reattive, giustificate dalla natura dei loro servizi e delle loro operazioni. L'autorità competente interessata dovrebbe pertanto adottare misure solo quando ottiene la prova, ad esempio dallo stesso fornitore di servizi digitali, da un'altra autorità competente, compresa un'autorità competente di un altro Stato membro, o da un utente del servizio, che un fornitore di servizi digitali non rispetta gli obblighi della presente direttiva, in particolare in seguito al verificarsi di un incidente. Pertanto, l'autorità competente non dovrebbe avere un obbligo generale di vigilanza sui fornitori di servizi digitali.

(61) È opportuno che le autorità competenti possiedano i mezzi necessari all'assolvimento dei loro compiti, come la facoltà di ottenere informazioni sufficienti per valutare il livello di sicurezza delle reti e dei sistemi informativi.

(62) Gli incidenti possono essere causati da attività criminali e i relativi interventi di prevenzione, indagine e perseguimento sono supportati dal coordinamento e dalla cooperazione tra operatori di servizi essenziali, fornitori di servizi digitali, autorità competenti e autorità di contrasto. Se si sospetta che un incidente sia connesso ad attività criminali gravi ai sensi del diritto dell'Unione o nazionale, gli Stati membri dovrebbero incoraggiare gli operatori di servizi essenziali e i fornitori di servizi digitali a segnalare alle autorità di contrasto competenti gli incidenti di cui si sospetta la natura criminale grave. Se del caso, è auspicabile che il coordinamento tra le autorità competenti e le autorità di contrasto dei diversi Stati membri sia facilitato dal Centro europeo per la lotta alla criminalità informatica (EC3) e dall'ENISA.

(63) In molti casi gli incidenti compromettono dati personali. Al riguardo è opportuno che le autorità competenti e le autorità responsabili della protezione dei dati collaborino e si scambino informazioni su tutti gli aspetti pertinenti per affrontare le violazioni ai dati personali determinate dagli incidenti.

(64) La competenza giurisdizionale rispetto ai fornitori di servizi digitali dovrebbe spettare allo Stato membro, in cui il fornitore di servizi digitali di cui si tratta ha lo stabilimento principale nell'Unione, che in principio corrisponde al luogo in cui il fornitore ha la sua sede sociale nell'Unione. Lo stabilimento implica l'effettivo e reale svolgimento di 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. Questo criterio non

dovrebbe dipendere dal fatto che le reti e i sistemi informativi 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 per la sua determinazione.

(65) Qualora un fornitore di servizi digitali non stabilito nell'Unione offra servizi nell'Unione, questi dovrebbe designare un rappresentante. Per determinare se tale fornitore di servizi digitali stia offrendo servizi nell'Unione, è opportuno verificare se risulta che il fornitore di servizi digitali stia progettando di fornire servizi a persone in uno o più Stati membri. La semplice accessibilità nell'Unione del sito internet del fornitore di servizi digitali 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 fornitore di servizi digitali è stabilito, è 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 fornitore di servizi digitali stia progettando di offrire servizi all'interno dell'Unione. Il rappresentante dovrebbe agire a nome del fornitore di servizi digitali e dovrebbe essere possibile per le autorità competente o i CSIRT contattare il rappresentante. Quest'ultimo dovrebbe essere esplicitamente designato mediante mandato scritto del fornitore di servizi digitali affinché agisca a suo nome con riguardo agli obblighi che a quest'ultimo derivano dalla presente direttiva, compresa la segnalazione di incidenti.

(66) La standardizzazione degli obblighi di sicurezza è un'esigenza che nasce dal mercato. Per garantire un'applicazione convergente delle norme di sicurezza è opportuno che gli Stati membri incoraggino il rispetto o la conformità a norme specifiche volte a garantire un livello elevato di sicurezza delle reti e dei sistemi informativi in tutta l'Unione. L'ENISA dovrebbe assistere gli Stati membri mediante consulenza e linee guida. A tal fine, potrebbe essere utile elaborare norme armonizzate a norma del regolamento (UE) n. 1025/2012 del Parlamento europeo e del Consiglio ([1]).

(67) Soggetti non rientranti nell'ambito di applicazione della presente direttiva potrebbero subire incidenti aventi un impatto rilevante sui servizi forniti. Qualora tali soggetti ritengano che sia nell'interesse pubblico notificare il verificarsi di tali incidenti, dovrebbero poterlo fare su base volontaria. Tali notifiche dovrebbero essere trattate dalle autorità competenti o dai CSIRT, purché il loro trattamento non rappresenti un onere sproporzionato o eccessivo per gli Stati membri interessati.

(68) Al fine di garantire condizioni uniformi di esecuzione della presente direttiva, dovrebbero essere attribuite alla Commissione competenze di esecuzione per prevedere le modalità procedurali necessarie per il funzionamento del gruppo di cooperazione e gli obblighi di sicurezza e di notifica applicabili ai fornitori di servizi digitali. Tali competenze di esecuzione dovrebbero essere esercitate conformemente al regolamento (UE) n. 182/2011 del Parlamento europeo e del Consiglio ([2]). Nell'adottare atti di esecuzione relativi alle modalità procedurali necessarie per il funzionamento del gruppo di cooperazione, la Commissione dovrebbe tenere nella massima considerazione il parere dell'ENISA.

(69) Nell'adottare atti di esecuzione sugli obblighi di sicurezza per i fornitori di servizi digitali, la Commissione dovrebbe tenere nella massima considerazione il parere dell'ENISA e dovrebbe consultare le parti interessate. Inoltre, la Commissione è incoraggiata a tener conto degli esempi seguenti: relativamente alla sicurezza dei sistemi e degli impianti: sicurezza fisica e dell'ambiente, sicurezza delle forniture, controllo dell'accesso alla rete ed ai sistemi informativi e integrità della rete e dei sistemi informativi; relativamente alla gestione degli incidenti: procedure per la gestione degli incidenti, capacità di rilevazione degli incidenti, comunicazione e segnalazione degli incidenti; relativamente alla gestione della continuità operativa: strategia per la continuità del servizio e piani di emergenza, capacità di ripristino in caso di disastro; e relativamente a monitoraggio, audit e test: prassi in materia di monitoraggio e registrazione, esercitazioni dei piani di emergenza, test delle reti e dei sistemi informativi, valutazioni della sicurezza e controllo di conformità.

(70) Nell'attuazione della presente direttiva la Commissione dovrebbe coordinarsi adeguatamente con i comitati settoriali competenti e gli organi costituiti a livello dell'Unione nei settori disciplinati dalla presente direttiva.

([1]) 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).

([2]) 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).

(71) È opportuno che la Commissione riesamini la presente direttiva a scadenze regolari, in consultazione con le parti interessate, in particolare per valutare la necessità di modificarle in funzione delle evoluzioni della società, della politica, delle tecnologie o delle condizioni del mercato.

(72) Lo scambio di informazioni sui rischi e sugli incidenti all'interno del gruppo di cooperazione e della rete di CSIRT e il rispetto degli obblighi di notifica degli incidenti alle autorità nazionali competenti o ai CSIRT potrebbero richiedere il trattamento di dati personali. Tale trattamento dovrebbe essere conforme alla direttiva 95/46/CE del Parlamento europeo e del Consiglio ([1]) e al regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio ([2]). Nell'applicazione della presente direttiva si applica, per quanto di ragione, il regolamento (CE) n. 1049/2001 del Parlamento europeo e del Consiglio ([3]).

(73) Il Garante europeo della protezione dei dati è stato consultato conformemente all'articolo 28, paragrafo 2, del regolamento (CE) n. 45/2001 e ha espresso un parere il 14 giugno 2013 ([4]).

(74) Poiché l'obiettivo della presente direttiva, vale a dire conseguire un elevato livello comune di sicurezza delle reti e dei sistemi informativi nell'Unione, non può essere conseguito in misura sufficiente dagli Stati membri ma, a motivo della portata e degli effetti dell'azione, può essere conseguito meglio a livello di Unione, quest'ultima può intervenire in base 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.

(75) 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 applicata nel rispetto di tali diritti e principi,

HANNO ADOTTATO LA PRESENTE DIRETTIVA:

CAPO I

DISPOSIZIONI GENERALI

Articolo 1

Oggetto e ambito di applicazione

1. La presente direttiva stabilisce misure volte a conseguire un livello comune elevato di sicurezza della rete e dei sistemi informativi nell'Unione così da migliorare il funzionamento del mercato interno.

2. A tal fine la presente direttiva:

a) fa obbligo a tutti gli Stati membri di adottare una strategia nazionale in materia di sicurezza della rete e dei sistemi informativi;

b) 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 tra di essi;

c) crea una rete di gruppi di intervento per la sicurezza informatica in caso di incidente («rete CSIRT») per contribuire allo sviluppo della fiducia tra Stati membri e promuovere una cooperazione operativa rapida ed efficace;

([1]) Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (GU L 281 del 23.11.1995, pag. 31).

([2]) Regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio, del 18 dicembre 2000, concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati (GU L 8 del 12.1.2001, pag. 1).

([3]) Regolamento (CE) n. 1049/2001 del Parlamento europeo e del Consiglio, del 30 maggio 2001, relativo all'accesso del pubblico ai documenti del Parlamento europeo, del Consiglio e della Commissione (GU L 145 del 31.5.2001, pag. 43).

([4]) GU C 32 del 4.2.2014, pag. 19.

d) stabilisce obblighi di sicurezza e di notifica per gli operatori di servizi essenziali e per i fornitori di servizi digitali;

e) fa obbligo agli Stati membri di designare autorità nazionali competenti, punti di contatto unici e CSIRT con compiti connessi alla sicurezza della rete e dei sistemi informativi.

3. Gli obblighi di sicurezza e di notifica di cui alla presente direttiva non si applicano alle imprese che sono soggette agli obblighi di cui agli articoli 13 *bis* e 13 *ter* della direttiva 2002/21/CE, né ai prestatori di servizi fiduciari che sono soggetti agli obblighi di cui all'articolo 19 del regolamento (UE) n. 910/2014.

4. La presente direttiva si applica fatte salve la direttiva 2008/114/CE del Consiglio ([1]) e le direttive 2011/93/UE ([2]) e 2013/40/UE ([3]) 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 degli affari, 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 allo scopo. Tale scambio di informazioni tutela la riservatezza di dette informazioni e protegge la sicurezza e gli interessi commerciali degli operatori di servizi essenziali e dei fornitori di servizi digitali.

6. La presente direttiva lascia impregiudicate le misure adottate dagli Stati membri per salvaguardare le funzioni essenziali dello Stato, in particolare di tutela della sicurezza nazionale, comprese le misure volte a tutelare le informazioni, la cui divulgazione sia dagli Stati membri considerata contraria agli interessi essenziali della loro sicurezza, e di mantenimento dell'ordine pubblico, in particolare a fini di indagine, accertamento e perseguimento di reati.

7. Qualora un atto giuridico settoriale dell'Unione faccia obbligo agli operatori di servizi essenziali o ai fornitori di servizi digitali di assicurare la sicurezza delle loro reti e dei loro sistemi informativi o di notificare gli incidenti, nella misura in cui gli effetti di tali obblighi siano almeno equivalenti a quelli degli obblighi di cui alla presente direttiva, si applicano le disposizioni di detto atto giuridico settoriale dell'Unione.

Articolo 2

Trattamento di dati personali

1. Il trattamento di dati personali ai sensi della presente direttiva è effettuato ai sensi della direttiva 95/46/CE.

2. Il trattamento di dati personali da parte di istituzioni e organismi dell'Unione ai sensi della presente direttiva è effettuato a norma del regolamento (CE) n. 45/2001.

Articolo 3

Armonizzazione minima

Fatto salvo l'articolo 16, paragrafo 10, e gli obblighi loro imposti dal diritto dell'Unione, gli Stati membri possono adottare o mantenere in vigore disposizioni atte a conseguire un livello di sicurezza più elevato della rete e dei sistemi informativi.

([1]) 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).

([2]) 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).

([3]) 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).

Articolo 4

Definizioni

Ai fini della presente direttiva si intende per:

1) «rete e sistema informativo»:

   a) una rete di comunicazione elettronica ai sensi dell'articolo 2, lettera a), della direttiva 2002/21/CE;

   b) qualsiasi dispositivo o gruppo di dispositivi interconnessi o collegati, uno o più dei quali eseguono, in base ad un programma, un trattamento automatico di dati digitali; o

   c) i dati digitali conservati, trattati, estratti o trasmessi per mezzo di reti o dispositivi di cui alle lettere a) e b), per il loro funzionamento, uso, protezione e manutenzione;

2) «sicurezza della rete e dei sistemi informativi», la capacità di una rete e dei sistemi informativi di resistere, a un determinato livello di riservatezza, a ogni azione che comprometta la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati conservati o trasmessi o trattati e dei relativi servizi offerti o accessibili tramite tale rete o sistemi informativi;

3) «strategia nazionale per la sicurezza della rete e dei sistemi informativi», un quadro che prevede obiettivi e priorità strategici in materia di sicurezza della rete e dei sistemi informativi a livello nazionale;

4) «operatore di servizi essenziali», soggetto pubblico o privato, di un tipo di cui all'allegato II, che soddisfa i criteri di cui all'articolo 5, paragrafo 2;

5) «servizio digitale», un servizio ai sensi dell'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio ([1]) di un tipo elencato nell'allegato III;

6) «fornitore di servizio digitale», qualsiasi persona giuridica che fornisce un servizio digitale;

7) «incidente», ogni evento con un reale effetto pregiudizievole per la sicurezza della rete e dei sistemi informativi;

8) «trattamento dell'incidente», tutte le procedure necessarie per l'identificazione, l'analisi e il contenimento di un incidente e l'intervento in caso di incidente;

9) «rischio», ogni circostanza o evento ragionevolmente individuabile con potenziali effetti pregiudizievoli per la sicurezza della rete e dei sistemi informativi;

10) «rappresentante», la persona fisica o giuridica stabilita nell'Unione espressamente designata ad agire per conto di un fornitore di servizi che non è stabilito nell'Unione, a cui l'autorità nazionale competente o un CSIRT può rivolgersi in luogo del fornitore di servizi digitali, per quanto riguarda gli obblighi di quest'ultimo ai sensi della presente direttiva;

11) «norma», una norma ai sensi dell'articolo 2, punto 1, del regolamento (UE) n. 1025/2012;

12) «specifica», una specifica tecnica ai sensi dell'articolo 2, punto 4, del regolamento (UE) n. 1025/2012;

13) «punto di interscambio internet (IXP)», una infrastruttura di rete che consente l'interconnessione di più di due sistemi autonomi indipendenti, 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;

14) «Sistema dei nomi di dominio» (DNS), è un sistema distribuito e gerarchico di naming in una rete che inoltra le richieste dei nomi di dominio;

([1]) 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).

15) «fornitore di servizi DNS», un soggetto che fornisce servizi DNS sul internet;

16) «registro dei nomi di dominio di primo livello», un soggetto che amministra e opera la registrazione di nomi di dominio internet nell'ambito di uno specifico dominio di primo livello (TLD);

17) «mercato online», un servizio digitale che consente ai consumatori e/o ai professionisti, come definiti rispettivamente all'articolo 4, paragrafo 1, lettera a) e all'articolo 4, paragrafo 1, lettera b), della direttiva 2013/11/UE del Parlamento europeo e del Consiglio ([1]), di concludere contratti di vendita o di servizi online con i professionisti sia sul sito web del mercato online sia sul sito web di un professionista che utilizza i servizi informatici forniti dal mercato online;

18) «motore di ricerca online», un servizio digitale che consente all'utente di effettuare ricerche, in linea di principio, su tutti i siti web o su siti web in una lingua particolare sulla base di un'interrogazione su qualsiasi tema sotto forma di parola chiave, frase o di altra immissione, e fornisce i link in cui possono essere trovate le informazioni relative al contenuto richiesto;

19) «servizio nella nuvola (*cloud computing*)», un servizio digitale che consente l'accesso a un insieme scalabile e elastico di risorse informatiche condivisibili;

Articolo 5

Identificazione degli operatori di servizi essenziali

1. Entro il 9 novembre 2018, gli Stati membri identificano, per ciascun settore e sottosettore di cui all'allegato II, gli operatori di servizi essenziali con una sede nel loro territorio.

2. I criteri per l'identificazione degli operatori di servizi essenziali di cui all'articolo 4, punto 4, sono i seguenti:

a) un soggetto fornisce un servizio che è essenziale per il mantenimento di attività sociali e/o economiche fondamentali;

b) la fornitura di tale servizio dipende dalla rete e dai sistemi informativi; e

c) un incidente avrebbe effetti negativi rilevanti sulla fornitura di tale servizio.

3. Ai fini del paragrafo 1, ciascuno Stato membro istituisce un elenco dei servizi di cui al paragrafo 2, lettera a).

4. Ai fini del paragrafo 1, qualora un soggetto fornisca un servizio di cui al paragrafo 2, lettera a), in due o più Stati membri, questi ultimi avviano consultazioni reciproche. Tale consultazione si svolge prima che sia presa una decisione sull'identificazione.

5. Gli Stati membri riesaminano e, se del caso, aggiornano su base regolare, ed almeno ogni due anni dopo il 9 maggio 2018, l'elenco di operatori di servizi essenziali identificati.

6. In conformità ai compiti di cui all'articolo 11, il gruppo di cooperazione ha il ruolo di favorire un approccio coerente degli Stati membri nel processo di identificazione degli operatori di servizi essenziali.

7. Ai fini del riesame di cui all'articolo 23 ed entro il 9 novembre 2018, e in seguito ogni due anni, gli Stati membri trasmettono alla Commissione le informazioni che le sono necessarie per consentirle di valutare l'attuazione della presente direttiva, in particolare la coerenza degli approcci degli Stati membri in merito all'identificazione degli operatori di servizi essenziali. Tali informazioni comprendono come minimo:

a) le misure nazionali che consentono l'identificazione degli operatori di servizi essenziali;

([1]) Direttiva 2013/11/UE del Parlamento europeo e del Consiglio, del 21 maggio 2013, sulla risoluzione alternativa delle controversie dei consumatori, che modifica il regolamento (CE) n. 2006/2004 e la direttiva 2009/22/CE (Direttiva sull'ADR per i consumatori) (GU L 165 del 18.6.2013, pag. 63).

b) l'elenco dei servizi di cui al paragrafo 3;

c) il numero degli operatori di servizi essenziali identificati per ciascun settore di cui all'allegato II ed un'indicazione della loro importanza in relazione a tale settore;

d) le soglie, ove esistono, per determinare il pertinente livello di fornitura con riferimento al numero di utenti che dipendono da tale servizio di cui all'articolo 6, paragrafo 1, lettera a), o all'importanza di tale particolare operatore di servizi essenziali di cui all'articolo 6, paragrafo 1, lettera f).

Al fine di contribuire alla comunicazione di informazioni comparabili, la Commissione, tenendo nella massima considerazione il parere dell'ENISA, può adottare opportuni orientamenti tecnici sui parametri relativi alle informazioni di cui al presente paragrafo.

Articolo 6

Effetti negativi rilevanti

1. Nella determinazione della rilevanza degli effetti negativi di cui all'articolo 5, paragrafo 2, lettera c), gli Stati membri tengono conto almeno dei seguenti fattori intersettoriali:

a) il numero di utenti che dipendono dal servizio fornito dal soggetto interessato;

b) la dipendenza di altri settori di cui all'allegato II dal servizio fornito da tale soggetto;

c) l'impatto che gli incidenti potrebbero avere, in termini di entità e di durata, sulle attività economiche e sociali o sulla pubblica sicurezza;

d) la quota di mercato di detto soggetto;

e) la diffusione geografica relativamente all'area che potrebbe essere interessata da un incidente;

f) l'importanza del soggetto per il mantenimento di un livello sufficiente del servizio, tenendo conto della disponibilità di strumenti alternativi per la fornitura di tale servizio.

2. Al fine di determinare se un incidente avrebbe effetti negativi rilevanti, gli Stati membri tengono altresì conto, ove opportuno, di fattori settoriali.

CAPO II

QUADRI NAZIONALI PER LA SICUREZZA DELLA RETE E DEI SISTEMI INFORMATIVI

Articolo 7

Strategia nazionale in materia di sicurezza della rete e dei sistemi informativi

1. Ogni Stato membro adotta una strategia nazionale in materia di sicurezza della rete e dei sistemi informativi che definisce gli obiettivi strategici e le opportune misure strategiche e regolamentari al fine di conseguire e mantenere un livello elevato di sicurezza delle reti e dei sistemi informativi e contempla almeno i settori di cui all'allegato II e i servizi di cui all'allegato III. La strategia nazionale in materia di sicurezza delle reti e dei sistemi informativi affronta in particolare i seguenti aspetti:

a) gli obiettivi e le priorità della strategia nazionale in materia di sicurezza delle reti e dei sistemi informativi;

b) un quadro di *governance* per conseguire gli obiettivi e le priorità della strategia nazionale in materia di sicurezza delle reti e dei sistemi informativi, inclusi i ruoli e le responsabilità degli organismi pubblici e degli altri attori pertinenti;

c) l'individuazione delle misure di preparazione, risposta e recupero, inclusa la collaborazione tra settore pubblico e settore privato;

d) un'indicazione di programmi di formazione, sensibilizzazione e istruzione relativi alla strategia in materia di sicurezza delle reti e dei sistemi informativi;

e) un'indicazione di piani di ricerca e sviluppo relativi alla strategia in materia di sicurezza delle reti e dei sistemi informativi;

f) un piano di valutazione dei rischi per individuare i rischi;

g) un elenco dei vari attori coinvolti nell'attuazione della strategia nazionale in materia di sicurezza delle reti e dei sistemi informativi.

2. Gli Stati membri possono chiedere l'assistenza dell'ENISA nello sviluppo delle strategie nazionali in materia di sicurezza delle reti e dei sistemi informativi.

3. Gli Stati membri comunicano le loro strategie nazionali in materia di sicurezza della rete e dei sistemi informativi alla Commissione entro tre mesi dalla loro adozione. A tal fine gli Stati membri possono escludere elementi della strategia riguardanti la sicurezza nazionale.

Articolo 8

Autorità nazionali competenti e punto di contatto unico

1. Ogni Stato membro designa una o più autorità nazionali competenti in materia di sicurezza delle reti e dei sistemi informativi («autorità competente»), che si occupino almeno dei settori di cui all'allegato II e i servizi di cui all'allegato III. Gli Stati membri possono affidare questo ruolo a una o più autorità esistenti.

2. Le autorità competenti controllano l'applicazione della presente direttiva a livello nazionale.

3. Ogni Stato membro designa un punto di contatto unico nazionale in materia di sicurezza delle reti e dei sistemi informativi («punto di contatto unico»). Gli Stati membri possono affidare questo ruolo a un'autorità esistente. Se uno Stato membro designa soltanto un'autorità competente, quest'ultima è anche il punto di contatto unico.

4. Il punto di contatto unico svolge una funzione di collegamento per garantire la cooperazione transfrontaliera delle autorità degli Stati membri con le autorità competenti negli altri Stati membri e con il gruppo di cooperazione di cui all'articolo 11 e la rete di CSIRT di cui all'articolo 12.

5. Gli Stati membri garantiscono che le autorità competenti e i punti di contatto unici siano dotati di risorse adeguate per svolgere in modo efficiente ed efficace i compiti loro assegnati 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.

6. Ove opportuno e conformemente al diritto nazionale, le autorità competenti e il punto di contatto unico consultano le autorità di contrasto e le autorità per la protezione dei dati nazionali competenti e collaborano con esse.

7. Ogni Stato membro comunica senza indugio alla Commissione la designazione dell'autorità competente e del punto di contatto unico, i loro compiti e qualsiasi ulteriore modifica dei medesimi. Ogni Stato membro rende pubblica la designazione dell'autorità competente e del punto di contatto unico. La Commissione pubblica l'elenco dei punti di contatto unici designati.

Articolo 9

Gruppi di intervento per la sicurezza informatica in caso di incidente (CSIRT)

1. Ogni Stato membro designa uno o più CSIRT che sia conforme ai requisiti di cui all'allegato I, punto 1, che si occupi almeno dei settori di cui all'allegato II e dei servizi di cui all'allegato III e abbia il compito di trattare gli incidenti e i rischi secondo una procedura ben definita. È possibile creare un CSIRT all'interno dell'autorità competente.

2. Gli Stati membri provvedono a che i CSIRT siano dotati di risorse adeguate per svolgere in modo efficace i loro compiti, precisati nell'allegato I, punto 2.

Gli Stati membri garantiscono la collaborazione effettiva, efficiente e sicura dei loro CSIRT nella rete di CSIRT di cui all'articolo 12.

3. Gli Stati membri garantiscono che i suoi CSIRT abbiano accesso a un'infrastruttura di informazione e comunicazione appropriata, sicura e resiliente a livello nazionale.

4. Gli Stati membri comunicano alla Commissione il mandato dei loro CSIRT e gli elementi principali della procedura di trattamento degli incidenti loro affidata.

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

Articolo 10

Cooperazione a livello nazionale

1. Se sono separati, l'autorità competente, 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 garantiscono che le autorità competenti o i CSIRT ricevano le notifiche di incidenti trasmesse ai sensi della presente direttiva. Ove uno Stato membro decida che i CSIRT non ricevano le notifiche, questi ultimi hanno accesso, nella misura necessaria per l'esecuzione dei loro compiti, ai dati sugli incidenti notificati dagli operatori di servizi essenziali ai sensi dell'articolo 14, paragrafi 3 e 5, o dai fornitori di servizi digitali ai sensi dell'articolo 16, paragrafi 3 e 6.

3. Gli Stati membri garantiscono che le autorità competenti o i CSIRT informano i punti di contatti unici in merito alle notifiche di incidenti trasmesse ai sensi della presente direttiva.

Entro il 9 agosto 2018 e in seguito ogni anno, una volta all'anno il punto di contatto unico trasmette una relazione sintetica al gruppo di cooperazione in merito alle notifiche ricevute, compresi il numero di notifiche e la natura degli incidenti notificati, e alle azioni intraprese a norma dell'articolo 14, paragrafi 3 e 5, e dell'articolo 16, paragrafi 3 e 6.

CAPO III

COOPERAZIONE

Articolo 11

Gruppo di cooperazione

1. Al fine di sostenere e agevolare la cooperazione strategica e lo scambio di informazioni fra Stati membri, di sviluppare la fiducia e nell'ottica di conseguire un livello comune elevato di sicurezza delle reti e dei servizi informativi nell'Unione, è istituito un gruppo di cooperazione.

Il gruppo di cooperazione svolge i suoi compiti sulla base di programmi di lavoro biennali, come indicato al paragrafo 3, secondo comma.

2. Il gruppo di cooperazione è composto da rappresentanti degli Stati membri, della Commissione e dell'ENISA.

Ove opportuno, il gruppo di cooperazione può invitare a partecipare ai suoi lavori i rappresentanti delle parti interessate.

La Commissione ne assicura il segretariato.

3. Il gruppo di cooperazione ha i seguenti compiti:

a) fornire orientamento strategico per le attività della rete di CSIRT istituita ai sensi dell'articolo 12;

b) scambiare buone pratiche sullo scambio di informazioni relative alla notifica di incidenti di cui all'articolo 14, paragrafi 3 e 5, e all'articolo 16, paragrafi 3 e 6;

c) scambiare migliori pratiche fra gli Stati membri e, in collaborazione con l'ENISA, fornire loro assistenza per la creazione di capacità in materia di sicurezza delle reti e dei sistemi informativi;

d) discutere le capacità e lo stato di preparazione degli Stati membri e valutare, su base volontaria, le strategie nazionali in materia di sicurezza delle reti e dei sistemi informativi e l'efficacia dei CSIRT e individuare le migliori pratiche;

e) scambiare informazioni e migliori pratiche in materia di sensibilizzazione e formazione;

f) scambiare informazioni e migliori pratiche in materia di ricerca e sviluppo riguardo alla sicurezza delle reti e dei sistemi informativi;

g) ove opportuno, scambiare esperienze in materia di sicurezza delle reti e dei sistemi informativi con le istituzioni, gli organi e gli organismi pertinenti dell'Unione;

h) discutere le norme e le specifiche di cui all'articolo 19 con i rappresentanti delle pertinenti organizzazioni di normalizzazione europee;

i) raccogliere informazioni sulle migliori pratiche in relazione ai rischi e agli incidenti;

j) esaminare, su base annuale, le relazioni sintetiche di cui all'articolo 10, paragrafo 3, secondo comma;

k) discutere il lavoro svolto riguardo a esercitazioni in materia di sicurezza delle reti e dei sistemi informativi, programmi di istruzione e formazione, comprese le attività svolte dall'ENISA;

l) con l'assistenza dell'ENISA, scambiare migliori pratiche connesse all'identificazione degli operatori di servizi essenziali da parte degli Stati membri, anche in relazione alle dipendenze transfrontaliere riguardo a rischi e incidenti;

m) discutere modalità per la comunicazione di notifiche di incidenti di cui agli articoli 14 e 16.

Entro il 9 febbraio 2018 e in seguito ogni due anni, il gruppo di cooperazione stabilisce un programma di lavoro, coerente con gli obiettivi della presente direttiva, sulle azioni da intraprendere per attuarne gli obiettivi e i compiti.

4. Ai fini del riesame di cui all'articolo 23 ed entro il 9 agosto 2018 e, successivamente, ogni 18 mesi, il gruppo di cooperazione elabora una relazione in cui valuta l'esperienza acquisita riguardo alla cooperazione strategica realizzata ai sensi del presente articolo.

5. La Commissione adotta atti di esecuzione che prevedono le modalità procedurali necessarie per il funzionamento del gruppo di cooperazione. Tali atti di esecuzione sono adottati secondo la procedura di esame di cui all'articolo 22, paragrafo 2.

Ai fini del primo comma, la Commissione trasmette il primo progetto di atto di esecuzione al comitato di cui all'articolo 22, paragrafo 1, entro il 9 febbraio 2017.

Articolo 12

Rete di CSIRT

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

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

3. La rete di CSIRT ha i seguenti compiti:

a) scambiare informazioni sui servizi, sulle operazioni e sulle capacità di cooperazione dei CSIRT;

b) su richiesta del rappresentante di un CSIRT di uno Stato membro potenzialmente interessato da un incidente, scambiare e discutere informazioni non sensibili sul piano commerciale connesse a tale incidente e i rischi associati; tuttavia, qualsiasi CSIRT di uno Stato membro può rifiutare di contribuire a tale discussione se ciò rischia di compromettere l'indagine sull'incidente;

c) scambiare e mettere a disposizione su base volontaria informazioni non riservate su singoli incidenti;

d) su richiesta di un rappresentante di un CSIRT di uno Stato membro, discutere e, ove possibile, individuare un intervento coordinato per un incidente rilevato nella giurisdizione di quello stesso Stato membro;

e) fornire sostegno agli Stati membri nel far fronte a incidenti transfrontalieri sulla base dell'assistenza reciproca volontaria;

f) discutere, esaminare e individuare ulteriori forme di cooperazione operativa, anche in relazione a:

   i) categorie di rischi e di incidenti;

   ii) preallarmi;

   iii) assistenza reciproca;

   iv) principi e modalità di coordinamento, quando gli Stati membri intervengono a proposito di rischi e incidenti transfrontalieri;

g) informare il gruppo di cooperazione in merito alle proprie attività e a ulteriori forme di cooperazione operativa discusse sulla scorta della lettera f) e chiedere orientamenti in merito;

h) discutere gli insegnamenti appresi dalle esercitazioni in materia di sicurezza delle reti e dei sistemi informativi, comprese quelle organizzate dall'ENISA;

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

j) formulare 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 23 ed entro il 9 agosto 2018 e, successivamente, ogni 18 mesi, la rete di CSIRT elabora una relazione in cui valuta l'esperienza acquisita riguardo alla cooperazione operativa, comprese conclusioni e raccomandazioni, realizzata ai sensi del presente articolo. Tale relazione è trasmessa anche al gruppo di cooperazione.

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

Articolo 13

Cooperazione internazionale

L'Unione può concludere accordi internazionali ai sensi dell'articolo 218 TFUE con paesi terzi o organizzazioni internazionali che consentono e organizzano la loro partecipazione a talune delle attività del gruppo di cooperazione. Tali accordi tengono conto della necessità di garantire la protezione adeguata dei dati.

CAPO IV

SICUREZZA DELLA RETE E DEI SISTEMI INFORMATIVI DEGLI OPERATORI DI SERVIZI ESSENZIALI

Articolo 14

Obblighi in materia di sicurezza e notifica degli incidenti

1. Gli Stati membri provvedono affinché gli operatori di servizi essenziali adottino misure tecniche e organizzative adeguate e proporzionate alla gestione dei rischi posti alla sicurezza delle reti e dei sistemi informativi che usano nelle loro operazioni. Tenuto conto delle conoscenze più aggiornate in materia, dette misure assicurano un livello di sicurezza della rete e dei sistemi informativi adeguato al rischio esistente.

2. Gli Stati membri provvedono affinché gli operatori di servizi essenziali adottino misure adeguate per prevenire e minimizzare l'impatto di incidenti a carico della sicurezza della rete e dei sistemi informativi utilizzati per la fornitura di tali servizi essenziali, al fine di assicurare la continuità di tali servizi.

3. Gli Stati membri provvedono affinché gli operatori di servizi essenziali notifichino senza indebito ritardo all'autorità competente o al CSIRT gli incidenti aventi un impatto rilevante sulla continuità dei servizi essenziali prestati. Le notifiche includono le informazioni che consentono all'autorità competente o al CSIRT di determinare qualsiasi impatto transfrontaliero dell'incidente. La notifica non espone la parte che la effettua a una maggiore responsabilità.

4. Per determinare la rilevanza dell'impatto di un incidente si tiene conto in particolare dei seguenti parametri:

a) il numero di utenti interessati dalla perturbazione del servizio essenziale;

b) la durata dell'incidente;

c) la diffusione geografica relativamente all'area interessata dall'incidente.

5. Sulla base delle informazioni fornite nella notifica da parte dell'operatore di servizi essenziali, l'autorità competente o il CSIRT informa l'altro o gli altri Stati membri interessati se l'incidente ha un impatto rilevante sulla continuità dei servizi essenziali in quello Stato membro. A tal fine l'autorità competente o il CSIRT preserva, conformemente al diritto dell'Unione o alla legislazione nazionale conforme al diritto dell'Unione, la sicurezza e gli interessi commerciali dell'operatore di servizi essenziali, nonché la riservatezza delle informazioni fornite nella sua notifica.

Ove le circostanze lo consentano, l'autorità competente o il CSIRT fornisce all'operatore di servizi essenziali che effettua la notifica di incidente le pertinenti informazioni relative al seguito della notifica stessa, come le informazioni che possano facilitare un trattamento efficace dell'incidente.

Su richiesta dell'autorità competente o del CSIRT, il punto di contatto unico trasmette le notifiche di cui al primo comma ai punti di contatto unici degli altri Stati membri interessati.

6. Dopo aver consultato l'operatore notificante dei servizi essenziali, l'autorità competente o il CSIRT può informare il pubblico in merito ai singoli incidenti, qualora sia necessaria la sensibilizzazione del pubblico per evitare un incidente o gestire un incidente in corso.

7. Le autorità competenti, agendo unitamente nell'ambito del gruppo di cooperazione, possono elaborare e adottare orientamenti sulle circostanze in cui gli operatori di servizi essenziali sono tenuti a notificare gli incidenti, compresi i parametri per determinare la rilevanza dell'impatto di un incidente di cui al paragrafo 4.

Articolo 15

Attuazione e controllo

1. Gli Stati membri provvedono affinché le autorità competenti siano dotate dei poteri e dei mezzi necessari per valutare la conformità degli operatori di servizi essenziali agli obblighi loro imposti dall'articolo 14 e i relativi effetti sulla sicurezza della rete e dei sistemi informativi.

2. Gli Stati membri provvedono affinché le autorità competenti siano dotate dei poteri e dei mezzi per richiedere agli operatori di servizi essenziali di fornire:

a) le informazioni necessarie per valutare la sicurezza della loro rete e dei loro sistemi informativi, compresi i documenti relativi alle politiche di sicurezza;

b) la prova dell'effettiva attuazione delle politiche di sicurezza, come i risultati di un audit sulla sicurezza svolto dall'autorità competente o da un revisore abilitato e, in quest'ultimo caso, metterne a disposizione dell'autorità competente i risultati, inclusi gli elementi di prova.

Quando richiede tali informazioni o prove, l'autorità competente indica lo scopo della stessa specificando il tipo di informazioni da fornire.

3. A seguito della valutazione delle informazioni o dei risultati degli audit sulla sicurezza di cui al paragrafo 2, l'autorità competente può emanare istruzioni vincolanti per gli operatori di servizi essenziali al fine di porre rimedio alle carenze individuate.

4. L'autorità competente opera in stretta cooperazione con le autorità responsabili della protezione dei dati nei casi di incidenti che comportano violazioni di dati personali.

CAPO V

SICUREZZA DELLA RETE E DEI SISTEMI INFORMATIVI DEI FORNITORI DI SERVIZI DIGITALI

Articolo 16

Obblighi in materia di sicurezza e notifica degli incidenti

1. Gli Stati membri provvedono affinché i fornitori di servizi digitali identifichino e adottino misure tecniche e organizzative adeguate e proporzionate alla gestione dei rischi posti alla sicurezza della rete e dei sistemi informativi che utilizzano nel contesto dell'offerta di servizi di cui all'allegato III all'interno dell'Unione. Tenuto conto delle conoscenze più aggiornate in materia, tali misure assicurano un livello di sicurezza della rete e dei sistemi informativi adeguato al rischio esistente e tengono conto dei seguenti elementi:

a) la sicurezza dei sistemi e degli impianti;

b) trattamento degli incidenti;

c) gestione della continuità operativa;

d) monitoraggio, audit e test;

e) conformità con le norme internazionali.

2. Gli Stati membri provvedono affinché i fornitori di servizi digitali adottino misure per prevenire e minimizzare l'impatto di incidenti a carico della sicurezza della rete e dei sistemi informativi del fornitore di servizi digitali sui servizi di cui all'allegato III offerti all'interno dell'Unione, al fine di assicurare la continuità di tali servizi.

3. Gli Stati membri provvedono affinché i fornitori di servizi digitali notifichino senza indebito ritardo all'autorità competente o al CSIRT qualsiasi incidente avente un impatto rilevante sulla fornitura di un servizio di cui all'allegato III che essi offrono all'interno dell'Unione. Le notifiche includono le informazioni che consentono all'autorità competente o al CSIRT di determinare la rilevanza di qualsiasi impatto transfrontaliero. La notifica non espone la parte che la effettua a una maggiore responsabilità.

4. Al fine di determinare se l'impatto di un incidente sia sostanziale, sono tenuti in considerazione, in particolare, i seguenti parametri:

a) il numero di utenti interessati dall'incidente, in particolare gli utenti che dipendono dal servizio per la fornitura dei propri servizi;

b) la durata dell'incidente;

c) la diffusione geografica relativamente all'area interessata dall'incidente;

d) la portata della perturbazione del funzionamento del servizio;

e) la portata dell'impatto sulle attività economiche e sociali.

L'obbligo di notificare un incidente si applica soltanto qualora il fornitore di servizi digitali abbia accesso alle informazioni necessarie per valutare l'impatto di un incidente nei confronti dei parametri di cui al primo comma.

5. Qualora un operatore di servizi essenziali dipenda da una terza parte fornitrice di servizi digitali per la fornitura di un servizio che è indispensabile per il mantenimento di attività economiche e sociali fondamentali, l'operatore stesso notifica qualsiasi impatto rilevante per la continuità di servizi essenziali dovuto ad un incidente a carico di tale operatore.

6. Se del caso, e in particolare se l'incidente di cui al paragrafo 3 riguarda due o più Stati membri, l'autorità competente o il CSIRT informa gli altri Stati membri coinvolti. A tal fine le autorità competenti, i CSIRT e i punti di contatto unici tutelano, nel rispetto del diritto dell'Unione o della legislazione nazionale conforme al diritto dell'Unione, la sicurezza e gli interessi commerciali del fornitore del servizio digitale nonché la riservatezza delle informazioni fornite.

7. Dopo aver consultato il fornitore di servizi digitali interessato, l'autorità competente o il CSIRT e, se del caso, le autorità o i CSIRT degli altri Stati membri interessati, possono informare il pubblico riguardo ai singoli incidenti o chiedere al fornitore di servizi digitali di provvedervi, qualora sia necessaria la sensibilizzazione del pubblico per evitare un incidente o gestirne uno in corso, o qualora la divulgazione dell'incidente sia altrimenti nell'interesse pubblico.

8. La Commissione adotta atti di esecuzione che specifichino ulteriormente gli elementi di cui al paragrafo 1 e i parametri elencati nel paragrafo 4 del presente articolo. Tali atti di esecuzione sono adottati secondo la procedura di esame di cui all'articolo 22, paragrafo 2, entro il 9 agosto 2017.

9. La Commissione può adottare atti di esecuzione che stabiliscono i formati e le procedure applicabili agli obblighi di notifica. Tali atti di esecuzione sono adottati secondo la procedura di esame di cui all'articolo 22, paragrafo 2.

10. Fatto salvo l'articolo 1, paragrafo 6, gli Stati membri non impongono ulteriori obblighi in materia di sicurezza o di notifica ai fornitori di servizi digitali.

11. Il capo V non si applica alle microimprese e alle piccole imprese quali definite nella raccomandazione 2003/361/CE della Commissione ([1]).

([1]) 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).

Articolo 17

Attuazione e controllo

1. Gli Stati membri provvedono affinché le autorità competenti adottino provvedimenti, se necessario, mediante misure di vigilanza *ex post*, quando ottengono la prova che un fornitore di servizi digitali non rispetta gli obblighi di cui all'articolo 16. Tale prova può essere presentata dall'autorità competente di un altro Stato membro in cui è fornito il servizio.

2. Ai fini del paragrafo 1, le autorità competenti sono dotate dei poteri e dei mezzi necessari per imporre ai prestatori di servizi digitali di:

a) fornire le informazioni necessarie per valutare la sicurezza della loro rete e dei loro sistemi informativi, compresi i documenti relativi alle politiche di sicurezza;

b) rimediare a qualsiasi mancato adempimento degli obblighi di cui all'articolo 16.

3. Se un fornitore di servizi digitali ha lo stabilimento principale o un rappresentante in uno Stato membro, ma la sua rete o i suoi sistemi informativi sono ubicati in uno o più altri Stati membri, l'autorità competente dello Stato membro dello stabilimento principale o del rappresentante e le autorità competenti dei suddetti altri Stati membri cooperano e si assistono reciprocamente in funzione delle necessità. Tale assistenza e cooperazione può comprendere scambi di informazioni tra le autorità competenti interessate e richieste di adottare le misure di vigilanza di cui al paragrafo 2.

Articolo 18

Giurisdizione e territorialità

1. Ai fini della presente direttiva, un fornitore di servizi digitali è considerato soggetto alla giurisdizione dello Stato membro in cui ha lo stabilimento principale. Un fornitore di servizi digitali è considerato avere il suo stabilimento principale in uno Stato membro quando ha la sua sede sociale in tale Stato membro.

2. Un fornitore di servizi digitali che non è stabilito nell'Unione, ma offre servizi di cui all'allegato III all'interno dell'Unione, designa un rappresentate nell'Unione. Il rappresentante è stabilito in uno di quegli Stati membri in cui sono offerti i servizi. Il fornitore di servizi digitali è considerato soggetto alla giurisdizione dello Stato membro in cui è stabilito il suo rappresentante.

3. La designazione di un rappresentante da parte di un fornitore di servizi digitali fa salve le azioni legali che potrebbero essere avviate nei confronti del fornitore stesso di servizi digitali.

CAPO VI

NORMAZIONE E NOTIFICA VOLONTARIA

Articolo 19

Normazione

1. Per promuovere l'attuazione convergente dell'articolo 14, paragrafi 1 e 2, e dell'articolo 16, paragrafi 1 e 2, gli Stati membri, senza fare 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 della rete e dei sistemi informativi.

2. L'ENISA, in collaborazione con gli Stati membri, redige pareri e linee guida 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 20

Notifica volontaria

1. Fatto salvo l'articolo 3, i soggetti che non sono stati identificati come operatori di servizi essenziali e non sono fornitori di servizi digitali possono notificare, su base volontaria, gli incidenti aventi un impatto rilevante sulla continuità dei servizi da loro prestati.

2. Nel trattamento delle notifiche, gli Stati membri agiscono secondo la procedura di cui all'articolo 14. Gli Stati membri possono trattare le notifiche obbligatorie prioritariamente rispetto alle notifiche volontarie. Le notifiche volontarie sono trattate soltanto qualora tale trattamento non costituisca un onere sproporzionato o eccessivo per gli Stati membri interessati.

La notifica volontaria non può avere l'effetto di imporre al soggetto notificante alcun obbligo a cui non sarebbe stato sottoposto se non avesse effettuato tale notifica.

CAPO VII

DISPOSIZIONI FINALI

Articolo 21

Sanzioni

Gli Stati membri stabiliscono le norme relative alle sanzioni da irrogare in caso di violazione delle disposizioni nazionali di attuazione della presente direttiva e adottano tutti i provvedimenti necessari per la loro applicazione. Le sanzioni previste sono effettive, proporzionate e dissuasive. Gli Stati membri notificano tali norme e provvedimenti alla Commissione entro il 9 maggio 2018 e provvedono a darle immediata notifica di ogni successiva modifica.

Articolo 22

Procedura di comitato

1. La Commissione è assistita dal comitato per la sicurezza delle reti e dei sistemi informativi. Tale comitato 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.

Articolo 23

Riesame

1. Entro il 9 maggio 2019, la Commissione presenta al Parlamento europeo e al Consiglio una relazione di valutazione della coerenza dell'approccio adottato dagli Stati membri nell'identificazione degli operatori di servizi essenziali.

2. La Commissione riesamina periodicamente il funzionamento della presente direttiva e presenta una relazione in proposito al Parlamento europeo e al Consiglio. 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 dei CSIRT sull'esperienza acquisita a livello strategico e operativo. Nell'ambito del riesame, la Commissione valuta anche l'elenco di cui agli allegati II e III e la coerenza nell'identificazione degli operatori di servizi essenziali e dei servizi nei settori di cui all'allegato II. La prima relazione è presentata entro il 9 maggio 2021.

Articolo 24

Misure transitorie

1. Fatto salvo l'articolo 25 e al fine di fornire agli Stati membri ulteriori possibilità di un'adeguata cooperazione durante il periodo di recepimento, il gruppo di cooperazione e la rete di CSIRT iniziano a svolgere i compiti di cui all'articolo 11, paragrafo 3, e all'articolo 12, paragrafo 3, rispettivamente entro il 9 febbraio 2017.

2. Per il periodo compreso dal 9 febbraio 2017 al 9 novembre 2018 e al fine di sostenere gli Stati membri nell'adottare un approccio coerente nel processo di identificazione degli operatori di servizi essenziali, il gruppo di cooperazione esamina la procedura, la sostanza e il tipo delle misure nazionali che consentono l'identificazione degli operatori di servizi essenziali in un settore specifico conformemente ai criteri di cui agli articoli 5 e 6. Il gruppo di cooperazione esamina altresì, su richiesta di uno Stato membro, specifici progetti di misure nazionali di tale Stato membro volte a consentire l'identificazione degli operatori di servizi essenziali in un settore specifico conformemente ai criteri di cui agli articoli 5 e 6.

3. Entro il 9 febbraio 2017 e ai fini del presente articolo, gli Stati membri assicurano un'adeguata rappresentanza in seno al gruppo di cooperazione e alla rete di CSIRT.

Articolo 25

Recepimento

1. Gli Stati membri adottano e pubblicano, entro il 9 maggio 2018, 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 10 maggio 2018.

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.

2. Gli Stati membri comunicano alla Commissione il testo delle disposizioni fondamentali di diritto interno che adottano nel settore disciplinato dalla presente direttiva.

Articolo 26

Entrata in vigore

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

Articolo 27

Destinatari

Gli Stati membri sono destinatari della presente direttiva.

Fatto a Strasburgo, il 6 luglio 2016

Per il Parlamento europeo	*Per il Consiglio*
Il presidente	*Il presidente*
M. SCHULZ	I. KORČOK

ALLEGATO I

REQUISITI E COMPITI DI GRUPPI DI INTERVENTO PER LA SICUREZZA INFORMATICA IN CASO DI INCIDENTE (CSIRT)

I requisiti e i compiti dei CSIRT sono adeguatamente e chiaramente definiti nel quadro di una strategia e/o di una regolamentazione nazionale. Essi includono quanto segue:

1) Requisiti per i CSIRT

   a) I CSIRT garantiscono un alto livello di disponibilità dei propri servizi di comunicazione, evitando singoli punti di guasto, e dispongono di vari mezzi che permettono loro di essere contattati e di contattare altri in qualsiasi momento. Inoltre, i canali di comunicazione sono chiaramente specificati e ben noti alla loro base di utenti e ai partner con cui collaborano.

   b) I locali dei CSIRT e i sistemi informativi di supporto sono ubicati in siti sicuri.

   c) Continuità operativa:

      i) i CSIRT sono dotati di un sistema adeguato di gestione e inoltro delle richieste in modo da facilitare i passaggi;

      ii) i CSIRT dispongono di personale sufficiente per garantirne l'operatività 24 ore su 24;

      iii) i CSIRT operano in base a un'infrastruttura di cui è garantita la continuità. A tal fine è necessario che siano disponibili sistemi ridondanti e spazi di lavoro di backup.

   d) I CSIRT hanno la possibilità, se lo desiderano, di partecipare a reti di cooperazione internazionale.

2) Compiti dei CSIRT

   a) I compiti dei CSIRT comprendono almeno:

      i) monitoraggio degli incidenti a livello nazionale;

      ii) emissione di preallarmi, allerte, annunci e divulgazione di informazioni alle parti interessate in merito a rischi e incidenti;

      iii) intervento in caso di incidente;

      iv) analisi dinamica dei rischi e degli incidenti, nonché sensibilizzazione situazionale;

      v) partecipazione alla rete dei CSIRT;

   b) i CSIRT stabiliscono relazioni di cooperazione con il settore privato;

   c) per facilitare la cooperazione, i CSIRT promuovono l'adozione e l'uso di prassi comuni o standardizzate nei seguenti settori:

      i) procedure di trattamento degli incidenti e dei rischi;

      ii) sistemi di classificazione degli incidenti, dei rischi e delle informazioni.

ALLEGATO II

TIPI DI SOGGETTI AI FINI DELL'ARTICOLO 4, PUNTO 4

Settore	Sottosettore	Tipo di soggetto
1. Energia	a) Energia elettrica	— Impresa elettrica quale definita all'articolo 2, punto 35, della direttiva 2009/72/CE del Parlamento europeo e del Consiglio ([1]) che esercita attività di «fornitura» quale definita all'articolo 2, punto 19, di tale direttiva
		— Gestori del sistema di distribuzione quali definiti all'articolo 2, punto 6, della direttiva 2009/72/CE
		— Gestori del sistema di trasmissione quali definiti all'articolo 2, punto 4, della direttiva 2009/72/CE
	b) Petrolio	— Gestori di oleodotti
		— Gestori di impianti di produzione, raffinazione, trattamento, deposito e trasporto di petrolio
	c) Gas	— Imprese fornitrici quali definite all'articolo 2, punto 8, della direttiva 2009/73/CE del Parlamento europeo e del Consiglio ([2])
		— Gestori del sistema di distribuzione quali definiti all'articolo 2, punto 6, della direttiva 2009/73/CE
		— Gestori del sistema di trasmissione quali definiti all'articolo 2, punto 4, della direttiva 2009/73/CE
		— Gestori dell'impianto di stoccaggio quali definiti all'articolo 2, punto 10, della direttiva 2009/73/CE
		— Gestori del sistema GNL quale definiti all'articolo 2, punto 12, della direttiva 2009/73/CE
		— Imprese di gas naturale quale definite all'articolo 2, punto 1, della direttiva 2009/73/CE
		— Gestori di impianti di raffinazione e trattamento di gas naturale
2. Trasporti	a) Trasporto aereo	— Vettori aerei quali definiti all'articolo 3, punto 4, del regolamento (CE) n. 300/2008 del Parlamento europeo e del Consiglio ([3])
		— Gestori aeroportuali quali definiti all'articolo 2, punto 2, della direttiva 2009/12/CE del Parlamento europeo e del Consiglio ([4]), aeroporti quali definiti all'articolo 2, punto 1, di tale direttiva, compresi gli aeroporti centrali di cui all'allegato II, sezione 2, del regolamento (UE) n. 1315/2013 del Parlamento europeo e del Consiglio ([5]), e soggetti che gestiscono impianti annessi situati in aeroporti

Settore	Sottosettore	Tipo di soggetto
		— Operatori attivi nel controllo della gestione del traffico che forniscono servizi di controllo del traffico aereo quale definito all'articolo 2, punto 1, del regolamento (CE) n. 549/2004 del Parlamento europeo e del Consiglio ([6])
	b) Trasporto ferroviario	— Gestori dell'infrastruttura quali definiti all'articolo 3, punto 2, della direttiva 2012/34/UE del Parlamento europeo e del Consiglio ([7])
		— Imprese ferroviarie quali definite all'articolo 3, punto 1, della direttiva 2012/34/UE, compresi gli operatori degli impianti di servizio quali definiti all'articolo 3, punto 12, della direttiva 2012/34/UE
	c) Trasporto per vie d'acqua	— compagnie di navigazione per il trasporto per vie d'acqua interne, marittimo e costiero di passeggeri e merci quali definite nell'allegato I del regolamento (CE) n. 725/2004 del Parlamento europeo e del Consiglio ([8]), escluse le singole navi gestite da tale compagnia
		— organi di gestione dei porti quali definiti all'articolo 3, punto 1, della direttiva 2005/65/CE del Parlamento europeo e del Consiglio ([9]), compresi i relativi impianti portuali quali definiti all'articolo 2, punto 11, del regolamento (CE) n. 725/2004, e soggetti che gestiscono opere e attrezzature all'interno di porti
		— Gestori di servizi di assistenza al traffico marittimo quali definiti all'articolo 3, lettera o), della direttiva 2002/59/CE del Parlamento europeo e del Consiglio ([10])
	d) Trasporto su strada	— Autorità stradali quali definite all'articolo 2, punto 12, del regolamento delegato (UE) 2015/962 della Commissione ([11]) responsabili del controllo della gestione del traffico
		— Gestori di sistemi di trasporto intelligenti quali definiti all'articolo 4, punto 1, della direttiva 2010/40/UE del Parlamento europeo e del Consiglio ([12]);
3. Settore bancario		Enti creditizi quali definiti all'articolo 4, punto 1, del regolamento (UE) n. 575/2013 del Parlamento europeo e del Consiglio ([13])
4. Infrastrutture dei mercati finanziari		— Gestori delle sedi di negoziazione quali definite all'articolo 4, punto 24, della direttiva 2014/65/UE del Parlamento europeo e del Consiglio ([14])
		— Controparte centrale quale definita all'articolo 2, punto 1, del regolamento (UE) n. 648/2012 del Parlamento europeo e del Consiglio ([15])
5. Settore sanitario	Istituti sanitari (compresi ospedali e cliniche private)	Prestatori di assistenza sanitaria quali definiti all'articolo 3, lettera g), della direttiva 2011/24/UE del Parlamento europeo e del Consiglio ([16])

Settore	Sottosettore	Tipo di soggetto
6. Fornitura e distribuzione di acqua potabile		Fornitori e distributori di acque destinate al consumo umano, quali definite all'articolo 2, punto 1, lettera a), della direttiva 98/83/CE del Consiglio ([17]), ma esclusi i distributori per i quali la distribuzione di acque destinate al consumo umano è solo una parte della loro attività generale di distribuzione di altri prodotti e beni che non sono considerati servizi essenziali
7. Infrastrutture digitali		— IXP
		— DNS
		— TLD

([1]) Direttiva 2009/72/CE del Parlamento europeo e del Consiglio, del 13 luglio 2009, relativa a norme comuni per il mercato interno dell'energia elettrica e che abroga la direttiva 2003/54/CE (GU L 211 del 14.8.2009, pag. 55).
([2]) Direttiva 2009/73/CE del Parlamento europeo e del Consiglio, del 13 luglio 2009, relativa a norme comuni per il mercato interno del gas naturale e che abroga la direttiva 2003/55/CE (GU L 211 del 14.8.2009, pag. 94).
([3]) Regolamento (CE) n. 300/2008 del Parlamento europeo e del Consiglio, dell'11 marzo 2008, che istituisce norme comuni per la sicurezza dell'aviazione civile e che abroga il regolamento (CE) n. 2320/2002 (GU L 97 del 9.4.2008, pag. 72).
([4]) Direttiva 2009/12/CE del Parlamento europeo e del Consiglio, dell'11 marzo 2009, concernente i diritti aeroportuali (GU L 70 del 14.3.2009, pag. 11).
([5]) Regolamento (UE) n. 1315/2013 del Parlamento europeo e del Consiglio, dell'11 dicembre 2013, sugli orientamenti dell'Unione per lo sviluppo della rete transeuropea dei trasporti e che abroga la decisione n. 661/2010/UE (GU L 348 del 20.12.2013, pag. 1).
([6]) Regolamento (CE) n. 549/2004 del Parlamento europeo e del Consiglio, del 10 marzo 2004, che stabilisce i principi generali per l'istituzione del cielo unico europeo («regolamento quadro») (GU L 96 del 31.3.2004, pag. 1).
([7]) Direttiva 2012/34/UE del Parlamento europeo e del Consiglio, del 21 novembre 2012, che istituisce uno spazio ferroviario europeo unico (GU L 343 del 14.12.2012, pag. 32).
([8]) Regolamento (CE) n. 725/2004 del Parlamento europeo e del Consiglio, del 31 marzo 2004, relativo al miglioramento della sicurezza delle navi e degli impianti portuali (GU L 129 del 29.4.2004, pag. 6).
([9]) Direttiva 2005/65/CE del Parlamento europeo e del Consiglio, del 26 ottobre 2005, relativa al miglioramento della sicurezza dei porti (GU L 310 del 25.11.2005, pag. 28).
([10]) Direttiva 2002/59/CE del Parlamento europeo e del Consiglio, del 27 giugno 2002, relativa all'istituzione di un sistema comunitario di monitoraggio del traffico navale e d'informazione e che abroga la direttiva 93/75/CEE del Consiglio (GU L 208 del 5.8.2002, pag. 10).
([11]) Regolamento delegato (UE) 2015/962 della Commissione, del 18 dicembre 2014, che integra la direttiva 2010/40/UE del Parlamento europeo e del Consiglio relativamente alla predisposizione in tutto il territorio dell'Unione europea di servizi di informazione sul traffico in tempo reale (GU L 157 del 23.6.2015, pag. 21).
([12]) Direttiva 2010/40/UE del Parlamento europeo e del Consiglio, del 7 luglio 2010, sul quadro generale per la diffusione dei sistemi di trasporto intelligenti nel settore del trasporto stradale e nelle interfacce con altri modi di trasporto (GU L 207 del 6.8.2010, pag. 1).
([13]) Regolamento (UE) n. 575/2013 del Parlamento europeo e del Consiglio, del 26 giugno 2013, relativo ai requisiti prudenziali per gli enti creditizi e le imprese di investimento e che modifica il regolamento (UE) n. 648/2012 (GU L 176 del 27.6.2013, pag. 1).
([14]) Direttiva 2014/65/UE del Parlamento europeo e del Consiglio, del 15 maggio 2014, relativa ai mercati degli strumenti finanziari e che modifica la direttiva 2002/92/CE e la direttiva 2011/61/UE (GU L 173 del 12.6.2014, pag. 349).
([15]) Regolamento (UE) n. 648/2012 del Parlamento europeo e del Consiglio, del 4 luglio 2012, sugli strumenti derivati OTC, le controparti centrali e i repertori di dati sulle negoziazioni (GU L 201 del 27.7.2012, pag. 1).
([16]) Direttiva 2011/24/UE del Parlamento europeo e del Consiglio, del 9 marzo 2011, concernente l'applicazione dei diritti dei pazienti relativi all'assistenza sanitaria transfrontaliera (GU L 88 del 4.4.2011, pag. 45).
([17]) Direttiva 98/83/CE del Consiglio, del 3 novembre 1998, concernente la qualità delle acque destinate al consumo umano (GU L 330 del 5.12.1998, pag. 32).

ALLEGATO III

TIPI DI SERVIZI DIGITALI AI FINI DELL'ARTICOLO 4, PUNTO 5

1. Mercato online
2. Motore di ricerca online
3. Servizi nella nuvola (cloud computing)