2024/2690

18.10.2024

REGOLAMENTO DI ESECUZIONE (UE) 2024/2690 DELLA COMMISSIONE

del 17 ottobre 2024

recante modalità di applicazione della direttiva (UE) 2022/2555 per quanto riguarda i requisiti tecnici e metodologici delle misure di gestione dei rischi di cibersicurezza e l'ulteriore specificazione dei casi in cui un incidente è considerato significativo per quanto riguarda i fornitori di servizi DNS, i registri dei nomi di dominio di primo livello, i fornitori di servizi di cloud computing, i fornitori di servizi di data center, i fornitori di reti di distribuzione dei contenuti, i fornitori di servizi gestiti, i fornitori di servizi di sicurezza gestiti, i fornitori di mercati online, di motori di ricerca online e di piattaforme di servizi di social network e i prestatori di servizi fiduciari

(Testo rilevante ai fini del SEE)

LA COMMISSIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea,

vista la direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2) ([1]), in particolare l'articolo 21, paragrafo 5, primo comma, e l'articolo 23, paragrafo 11, secondo comma,

considerando quanto segue:

(1) Per quanto riguarda i fornitori di servizi DNS, i registri dei nomi di dominio di primo livello, i fornitori di servizi di cloud computing, i fornitori di servizi di data center, i fornitori di reti di distribuzione dei contenuti, i fornitori di servizi gestiti, i fornitori di servizi di sicurezza gestiti, i fornitori di mercati online, di motori di ricerca online e di piattaforme di servizi di social network e i prestatori di servizi fiduciari di cui all'articolo 3 della direttiva (UE) 2022/2555 (i soggetti pertinenti), il presente regolamento mira a stabilire i requisiti tecnici e metodologici delle misure di cui all'articolo 21, paragrafo 2, della suddetta direttiva e a specificare ulteriormente i casi in cui un incidente dovrebbe essere considerato significativo a norma dell'articolo 23, paragrafo 3, della medesima.

(2) Tenendo conto della natura transfrontaliera delle loro attività e al fine di assicurare un quadro coerente per i prestatori di servizi fiduciari, per tali prestatori il presente regolamento dovrebbe specificare ulteriormente i casi in cui un incidente deve essere considerato significativo, oltre a stabilire i requisiti tecnici e metodologici delle misure di gestione dei rischi di cibersicurezza.

(3) A norma dell'articolo 21, paragrafo 5, terzo comma, della direttiva (UE) 2022/2555, i requisiti tecnici e metodologici delle misure di gestione dei rischi di cibersicurezza di cui all'allegato del presente regolamento si basano su norme europee e internazionali, quali ISO/IEC 27001, ISO/IEC 27002 ed ETSI EN 319401, e su specifiche tecniche, quali CEN/TS 18026:2024, pertinenti per la sicurezza dei sistemi informativi e di rete.

(4) Per quanto concerne l'attuazione e l'applicazione dei requisiti tecnici e metodologici delle misure di gestione dei rischi di cibersicurezza di cui all'allegato del presente regolamento, in linea con il principio di proporzionalità, nel conformarsi a tali requisiti tecnici e metodologici è opportuno tenere debitamente conto dell'esposizione al rischio divergente dei soggetti pertinenti, quali la criticità del soggetto pertinente, i rischi cui è esposto, le dimensioni e la struttura del soggetto pertinente, nonché la probabilità che si verifichino incidenti e la loro gravità, compreso il loro impatto sociale ed economico.

([1]) GU L 333 del 27.12.2022, pag. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj.

(5) In linea con il principio di proporzionalità, qualora non possano attuare alcuni dei requisiti tecnici e metodologici delle misure di gestione dei rischi di cibersicurezza in ragione delle loro dimensioni, i soggetti pertinenti dovrebbero poter adottare altre misure compensative idonee a conseguire la finalità di tali requisiti. Ad esempio, nel definire i ruoli, le responsabilità e le autorità per la sicurezza delle reti e dei sistemi informativi all'interno del soggetto pertinente, i microsoggetti potrebbero avere difficoltà a separare funzioni e settori di responsabilità contrastanti. Tali soggetti dovrebbero poter prendere in considerazione misure compensative quali una sorveglianza mirata da parte della dirigenza del soggetto in questione o un aumento delle attività di monitoraggio e registrazione.

(6) Alcuni requisiti tecnici e metodologici stabiliti nell'allegato del presente regolamento dovrebbero essere applicati ai soggetti pertinenti se opportuno, se applicabile o nella misura del possibile. Qualora ritenga che l'applicazione di determinati requisiti tecnici e metodologici di cui all'allegato del presente regolamento non sia opportuna, applicabile o possibile, un soggetto pertinente dovrebbe documentare in modo comprensibile le ragioni di tale decisione. Nell'esercizio delle funzioni di vigilanza le autorità nazionali competenti possono tenere conto del tempo necessario affinché i soggetti pertinenti attuino i requisiti tecnici e metodologici delle misure di gestione dei rischi di cibersicurezza.

(7) L'Agenzia dell'Unione europea per la cibersicurezza (ENISA) o le autorità nazionali competenti a norma della direttiva (UE) 2022/2555 possono fornire orientamenti al fine di sostenere i soggetti pertinenti nell'individuazione, nell'analisi e nella valutazione dei rischi ai fini dell'attuazione dei requisiti tecnici e metodologici relativi all'istituzione e al mantenimento di un quadro adeguato per la gestione dei rischi. Tra tali orientamenti possono figurare, in particolare, valutazioni dei rischi nazionali e settoriali, nonché valutazioni dei rischi specifiche per un determinato tipo di soggetto. Tali orientamenti possono comprendere altresì strumenti o modelli per lo sviluppo di un quadro per la gestione dei rischi a livello dei soggetti pertinenti. Anche i quadri, gli orientamenti o altri meccanismi previsti dal diritto nazionale degli Stati membri, nonché le pertinenti norme europee e internazionali, possono aiutare i soggetti pertinenti a dimostrare la propria conformità al presente regolamento. L'ENISA o le autorità nazionali competenti a norma della direttiva (UE) 2022/2555 possono inoltre sostenere i soggetti pertinenti nell'individuazione e nell'attuazione di soluzioni adeguate per trattare i rischi individuati nel contesto di tali valutazioni dei rischi. Tali orientamenti dovrebbero lasciare impregiudicati gli obblighi per i soggetti pertinenti di individuare e documentare i rischi posti alla sicurezza dei sistemi informativi e di rete e di attuare i requisiti tecnici e metodologici delle misure di gestione dei rischi di cibersicurezza di cui all'allegato del presente regolamento in funzione delle loro esigenze e risorse.

(8) Le misure di sicurezza delle reti in relazione i) alla transizione verso protocolli di comunicazione a livello di rete di ultima generazione, ii) all'introduzione di norme moderne di comunicazione via posta elettronica concordate a livello internazionale e interoperabili e iii) all'applicazione delle migliori pratiche per la sicurezza del DNS e per la sicurezza dell'instradamento in Internet, come pure per l'igiene dell'instradamento, comportano sfide specifiche per quanto concerne l'individuazione delle migliori norme e delle migliori tecniche di diffusione disponibili. Al fine di conseguire quanto prima un livello comune elevato di cibersicurezza tra le reti, la Commissione, con l'assistenza dell'ENISA e in collaborazione con le autorità competenti, l'industria (compresa l'industria delle telecomunicazioni) e altri portatori di interessi, dovrebbe sostenere lo sviluppo di un forum multipartecipativo incaricato di individuare tali migliori norme e tecniche di diffusione disponibili. Gli orientamenti multipartecipativi in questione non dovrebbero pregiudicare l'obbligo per i soggetti pertinenti di attuare i requisiti tecnici e metodologici delle misure di gestione dei rischi di cibersicurezza di cui all'allegato del presente regolamento.

(9) A norma dell'articolo 21, paragrafo 2, lettera a), della direttiva (UE) 2022/2555, oltre alle politiche di analisi dei rischi, i soggetti essenziali e importanti dovrebbero disporre di politiche di sicurezza dei sistemi informativi. A tal fine, i soggetti pertinenti dovrebbero stabilire una politica di sicurezza dei sistemi informativi e di rete nonché politiche specifiche per tematica, quali le politiche sul controllo dell'accesso, che dovrebbero essere coerenti con la politica di sicurezza dei sistemi informativi e di rete. Quest'ultima politica dovrebbe essere il documento di livello più elevato che definisce l'approccio generale dei soggetti pertinenti alla sicurezza dei sistemi informativi e di rete e dovrebbe essere approvata dagli organi di gestione dei soggetti pertinenti. Le politiche specifiche per tematica dovrebbero essere approvate da un livello di dirigenza adeguato. Tale politica dovrebbe inoltre stabilire indicatori e misure volti a monitorare la sua attuazione nonché lo stato corrente del livello di maturità della sicurezza delle reti e dei sistemi informativi dei soggetti pertinenti, in particolare al fine di agevolare la sorveglianza dell'attuazione delle misure di gestione dei rischi di cibersicurezza attraverso gli organi di gestione.

(10) Ai fini dei requisiti tecnici e metodologici di cui all'allegato del presente regolamento, il termine «utente» dovrebbe comprendere tutte le persone fisiche e giuridiche che hanno accesso ai sistemi informativi e di rete del soggetto in questione.

(11) Per individuare e affrontare i rischi per la sicurezza dei sistemi informativi e di rete, i soggetti pertinenti dovrebbero istituire e mantenere un quadro adeguato per la gestione dei rischi. Nell'ambito del quadro per la gestione dei rischi, i soggetti pertinenti dovrebbero stabilire, attuare e monitorare un piano di trattamento dei rischi. I soggetti pertinenti possono utilizzare tale piano per individuare le misure e le opzioni di trattamento dei rischi e definirne l'ordine di priorità. Tra le opzioni di trattamento dei rischi figurano, in particolare, la prevenzione, la riduzione o, in casi eccezionali, l'accettazione del rischio. La scelta delle opzioni di trattamento dei rischi dovrebbe tenere conto dei risultati della valutazione dei rischi effettuata dal soggetto pertinente ed essere conforme alla sua politica di sicurezza dei sistemi informativi e di rete. Per applicare le opzioni di trattamento dei rischi prescelte, i soggetti pertinenti dovrebbero adottare le misure di trattamento dei rischi adeguate.

(12) Per individuare eventi, quasi incidenti e incidenti, i soggetti pertinenti dovrebbero monitorare i propri sistemi informativi e di rete e dovrebbero adottare misure volte a valutare eventi, quasi incidenti e incidenti. Tali misure dovrebbero essere in grado di consentire il rilevamento tempestivo di attacchi fondati sulle reti basati su modelli anomali di traffico in ingresso o in uscita e di attacchi di negazione del servizio.

(13) Quando conducono un'analisi dell'impatto sulle attività aziendali (*business impact analysis*), i soggetti pertinenti sono incoraggiati a effettuare un'analisi completa che stabilisca, a seconda dei casi, i tempi di inattività massimi tollerabili e gli obiettivi in termini di tempi di ripristino, punto di ripristino e fornitura di servizi.

(14) Al fine di attenuare i rischi derivanti dalla loro catena di approvvigionamento e dalle relazioni con i loro fornitori, i soggetti pertinenti dovrebbero stabilire una politica di sicurezza della catena di approvvigionamento che disciplini le loro relazioni con i loro diretti fornitori e fornitori di servizi. Tali soggetti dovrebbero specificare nei contratti con i loro diretti fornitori o fornitori di servizi clausole di sicurezza adeguate che impongano ad esempio l'adozione, se opportuno, di misure di gestione dei rischi di cibersicurezza conformemente all'articolo 21, paragrafo 2, della direttiva (UE) 2022/2555 o ad altri requisiti giuridici analoghi.

(15) I soggetti pertinenti dovrebbero effettuare periodicamente test di sicurezza sulla base di una politica e di procedure apposite al fine di verificare se le misure di gestione dei rischi di cibersicurezza siano attuate e funzionino correttamente. I test di sicurezza possono essere svolti su sistemi informativi e di rete specifici oppure sul soggetto pertinente nel suo complesso e possono contemplare test automatizzati o manuali, test di penetrazione, scansioni delle vulnerabilità, test statici e dinamici di sicurezza delle applicazioni, test di configurazione o audit della sicurezza. I soggetti pertinenti possono effettuare test di sicurezza sui loro sistemi informativi e di rete al momento della loro creazione, in seguito ad ammodernamenti o modifiche delle infrastrutture o delle applicazioni che ritengono essere significativi/e oppure in seguito a interventi di manutenzione. I risultati dei test di sicurezza dovrebbero orientare le politiche e le procedure dei soggetti pertinenti al fine di valutare l'efficacia delle misure di gestione dei rischi di cibersicurezza, nonché riesami indipendenti delle loro politiche in materia di sicurezza delle reti e dei sistemi informativi.

(16) Al fine di evitare perturbazioni e danni significativi causati dallo sfruttamento delle vulnerabilità non corrette tramite patch nei sistemi informativi e di rete, i soggetti pertinenti dovrebbero stabilire e applicare adeguate procedure di gestione delle patch di sicurezza che siano in linea con le loro procedure di gestione delle modifiche, di gestione delle vulnerabilità e di gestione dei rischi, nonché con altre procedure pertinenti. I soggetti pertinenti dovrebbero adottare misure proporzionate alle loro risorse per garantire che le patch di sicurezza non introducano ulteriori vulnerabilità o instabilità. In caso di prevista inaccessibilità del servizio causata dall'applicazione di patch di sicurezza, i soggetti pertinenti sono incoraggiati a informare debitamente i clienti in anticipo.

(17) I soggetti pertinenti dovrebbero gestire i rischi derivanti dall'acquisizione di prodotti delle tecnologie dell'informazione e della comunicazione (TIC) o servizi TIC da fornitori o fornitori di servizi e dovrebbero ottenere la garanzia che i prodotti TIC o i servizi TIC che acquisiranno conseguano determinati livelli di protezione della cibersicurezza, ad esempio mediante certificati europei di cibersicurezza e dichiarazioni di conformità dell'UE per i prodotti TIC o i servizi TIC rilasciati nell'ambito di un sistema europeo di certificazione della cibersicurezza adottato a norma dell'articolo 49 del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio ([2]). Qualora stabiliscano requisiti di sicurezza da applicare ai prodotti TIC da acquisire, i soggetti pertinenti dovrebbero tenere conto dei requisiti essenziali di cibersicurezza stabiliti nel regolamento del Parlamento europeo e del Consiglio relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali.

(18) Al fine di fornire protezione contro minacce informatiche e sostenere la prevenzione e il contenimento delle violazioni dei dati, i soggetti pertinenti dovrebbero attuare soluzioni per la sicurezza delle reti. Tra le soluzioni tipiche per la sicurezza delle reti figurano l'uso di firewall per proteggere le reti interne dei soggetti pertinenti, la limitazione delle connessioni e dell'accesso ai servizi qualora tali connessioni e accesso siano assolutamente necessari e l'uso di reti private virtuali per l'accesso remoto, nonché la possibilità di consentire le connessioni dei fornitori di servizi soltanto previa richiesta di autorizzazione e per un periodo di tempo determinato, quale la durata di un'operazione di manutenzione.

(19) Per proteggere le proprie reti e i propri sistemi informativi da software malevoli e non autorizzati, i soggetti pertinenti dovrebbero attuare controlli volti a impedire o rilevare l'uso di software non autorizzati e, se opportuno, dovrebbero utilizzare software di rilevamento e risposta. I soggetti pertinenti dovrebbero inoltre prendere in considerazione l'attuazione di misure volte a ridurre al minimo la superficie di attacco, ridurre le vulnerabilità che possono essere sfruttate dagli autori degli attacchi, controllare l'esecuzione delle applicazioni negli endpoint e utilizzare filtri delle applicazioni per la posta elettronica e il web al fine di ridurre l'esposizione a contenuti malevoli.

(20) A norma dell'articolo 21, paragrafo 2, lettera g), della direttiva (UE) 2022/2555, gli Stati membri devono provvedere affinché i soggetti essenziali e importanti applichino pratiche di igiene informatica di base e forniscano formazione in materia di cibersicurezza. Tra le pratiche di igiene informatica di base possono figurare principi zero trust, aggiornamenti del software, configurazione dei dispositivi, segmentazione della rete, gestione delle identità e degli accessi o sensibilizzazione degli utenti, organizzazione di attività di formazione per il personale e sensibilizzazione in merito alle minacce informatiche, al phishing o alle tecniche di ingegneria sociale. Le pratiche di igiene informatica costituiscono parte di diversi requisiti tecnici e metodologici delle misure di gestione dei rischi di cibersicurezza di cui all'allegato del presente regolamento. Per quanto riguarda le pratiche di igiene informatica di base per gli utenti, i soggetti pertinenti dovrebbero prendere in considerazione pratiche quali una politica «clear desk» (scrivania pulita) e «clear screen» (schermo pulito), l'uso di mezzi di autenticazione a più fattori e di altro tipo, pratiche sicure per l'uso della posta elettronica e della navigazione sul web, la protezione dal phishing e dall'ingegneria sociale e pratiche sicure di lavoro a distanza.

(21) Al fine di impedire l'accesso non autorizzato alle loro risorse, i soggetti pertinenti dovrebbero stabilire e attuare una politica specifica per tematica sull'accesso da parte delle persone fisiche e dei sistemi informativi e di rete, quali le applicazioni.

(22) Per evitare che i dipendenti possano ad esempio usare in modo improprio i diritti di accesso all'interno di un soggetto pertinente per nuocere e causare danni, i soggetti pertinenti dovrebbero prendere in considerazione adeguate misure di gestione della sicurezza del personale e sensibilizzare l'organico in merito a tali rischi. I soggetti pertinenti dovrebbero istituire, comunicare e mantenere un processo disciplinare per la gestione delle violazioni delle loro politiche di sicurezza dei sistemi informativi e di rete, che può essere integrato in altri processi disciplinari da essi istituiti. La verifica dei precedenti personali dei dipendenti e, se applicabile, dei diretti fornitori e fornitori di servizi dei soggetti pertinenti dovrebbe contribuire all'obiettivo della sicurezza delle risorse umane dei soggetti pertinenti, e può includere misure quali controlli dei precedenti penali o delle passate funzioni professionali, a seconda delle funzioni che il dipendente esercita in seno al soggetto pertinente e in linea con la politica di sicurezza dei sistemi informativi e di rete di tale soggetto.

([2]) Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cibersicurezza») (GU L 151 del 7.6.2019, pag. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

(23) L'autenticazione a più fattori può migliorare la cibersicurezza dei soggetti, che dovrebbero prenderla in considerazione in particolare quando gli utenti accedono ai sistemi informativi e di rete da ubicazioni remote o quando accedono a informazioni sensibili o ad account privilegiati e ad account di amministrazione dei sistemi. L'autenticazione a più fattori può essere combinata con altre tecniche volte a richiedere fattori aggiuntivi in circostanze specifiche, sulla base di norme e modelli predefiniti, quali l'accesso da un'ubicazione, da un dispositivo o in un orario insoliti.

(24) I soggetti pertinenti dovrebbero gestire e proteggere le risorse di valore attraverso una sana gestione, che dovrebbe fungere anche da base per l'analisi dei rischi e la gestione della continuità operativa. I soggetti pertinenti dovrebbero gestire tanto le risorse materiali quanto quelle immateriali e creare un inventario delle risorse, associarle a un livello di classificazione definito, gestirle e monitorarle e adottare misure volte a proteggerle durante tutto il loro ciclo di vita.

(25) La gestione delle risorse dovrebbe contemplarne la classificazione in base al tipo, alla sensibilità, al livello di rischio e ai requisiti di sicurezza, nonché comportare l'applicazione di misure e controlli adeguati per garantirne la disponibilità, l'integrità, la riservatezza e l'autenticità. Classificando le risorse in base al livello di rischio, i soggetti pertinenti dovrebbero poter applicare misure e controlli di sicurezza adeguati volti a proteggere le risorse quali la crittografia, il controllo dell'accesso, compreso il controllo dell'accesso perimetrale, fisico e logico, i backup, la registrazione e il monitoraggio, la conservazione e lo smaltimento. Nell'effettuare un'analisi dell'impatto sulle attività aziendali, i soggetti pertinenti possono stabilire il livello di classificazione sulla base delle conseguenze che subirebbero nel caso di una perturbazione delle risorse. Tutti i dipendenti dei soggetti che gestiscono le risorse dovrebbero avere familiarità con le politiche e le istruzioni in materia di gestione delle risorse.

(26) La granularità dell'inventario delle risorse dovrebbe essere adeguata alle esigenze dei soggetti pertinenti. Un inventario completo delle risorse potrebbe comprendere, per ciascuna risorsa, quanto meno un identificativo unico, il proprietario, una descrizione, l'ubicazione, il tipo, il tipo e la classificazione delle informazioni trattate nella risorsa, la data dell'ultimo aggiornamento o dell'ultima patch, la classificazione nel contesto della valutazione dei rischi e la fine del ciclo di vita. Nell'individuare il proprietario di una risorsa, i soggetti pertinenti dovrebbero altresì individuare la persona competente per la protezione della risorsa.

(27) L'assegnazione e l'organizzazione dei ruoli, delle responsabilità e delle autorità in materia di cibersicurezza dovrebbero costituire una struttura coerente per la governance e l'attuazione della cibersicurezza in seno ai soggetti pertinenti e dovrebbero garantire una comunicazione efficace in caso di incidenti. Nel definire le responsabilità e nell'assegnarle a determinati ruoli, i soggetti pertinenti dovrebbero prendere in considerazione ruoli quali il responsabile capo della sicurezza delle informazioni, il responsabile della sicurezza delle informazioni, il responsabile della gestione degli incidenti, l'auditor o altre figure equivalenti comparabili. I soggetti pertinenti possono assegnare ruoli e responsabilità a parti esterne, quali i fornitori terzi di servizi TIC.

(28) Conformemente all'articolo 21, paragrafo 2, della direttiva (UE) 2022/2555, le misure di gestione dei rischi di cibersicurezza devono essere basate su un approccio multirischio mirante a proteggere i sistemi informativi e di rete e il loro ambiente fisico da eventi quali furti, incendi, inondazioni, problemi di telecomunicazione o interruzioni di corrente, o da qualsiasi accesso fisico non autorizzato nonché dai danni alle informazioni detenute dai soggetti essenziali o importanti e agli impianti di trattamento delle informazioni di questi ultimi e dalle interferenze con tali informazioni o impianti che possano compromettere la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati conservati, trasmessi o elaborati o dei servizi offerti da tali sistemi informativi e di rete o accessibili attraverso di essi. I requisiti tecnici e metodologici delle misure di gestione dei rischi di cibersicurezza dovrebbero pertanto riguardare anche la sicurezza fisica e ambientale dei sistemi informativi e di rete, includendo misure volte a proteggere tali sistemi da guasti del sistema, errori umani, azioni malevole o fenomeni naturali. Tra gli ulteriori esempi di minacce fisiche e ambientali figurano i terremoti, le esplosioni, il sabotaggio, le minacce interne, i disordini civili, i rifiuti tossici e le emissioni ambientali. La prevenzione di perdite, danni o compromissioni a carico dei sistemi informativi e di rete o dell'interruzione delle loro attività a causa di guasti e perturbazioni dei servizi pubblici di sostegno dovrebbero contribuire all'obiettivo della continuità operativa in seno ai soggetti pertinenti. Inoltre la protezione dalle minacce fisiche e ambientali dovrebbe contribuire alla sicurezza della manutenzione dei sistemi informativi e di rete in seno ai soggetti pertinenti.

(29) I soggetti pertinenti dovrebbero progettare e attuare misure di protezione dalle minacce fisiche e ambientali e stabilire soglie di controllo minime e massime per tali minacce, nonché monitorare i parametri ambientali. Essi dovrebbero ad esempio prendere in considerazione l'installazione di sistemi per il rilevamento precoce di allagamenti nelle zone in cui sono situati i sistemi informativi e di rete. Per quanto riguarda il pericolo di incendio, i soggetti pertinenti dovrebbero prendere in considerazione la creazione di un compartimento antincendio separato per il data center, l'uso di materiali resistenti al fuoco e sensori per il monitoraggio della temperatura e dell'umidità, il collegamento dell'edificio a un sistema di allarme antincendio che preveda una notifica automatica al servizio antincendio locale e sistemi di rilevamento ed estinzione precoci degli incendi. I soggetti pertinenti dovrebbero inoltre effettuare periodicamente esercitazioni antincendio e ispezioni antincendio. Al fine di assicurare la disponibilità di alimentazione elettrica, i soggetti pertinenti dovrebbero inoltre prendere in considerazione la protezione contro la sovratensione e l'alimentazione di emergenza corrispondente, conformemente alle norme pertinenti. Inoltre, dato che il surriscaldamento rappresenta un rischio per la disponibilità dei sistemi informativi e di rete, i soggetti pertinenti, in particolare i fornitori di servizi di data center, potrebbero prendere in considerazione sistemi adeguati, continui e ridondanti di condizionamento dell'aria.

(30) Il presente regolamento deve specificare ulteriormente i casi in cui un incidente dovrebbe essere considerato significativo ai fini dell'articolo 23, paragrafo 3, della direttiva (UE) 2022/2555. I criteri dovrebbero essere tali da consentire ai soggetti pertinenti di valutare se un incidente è significativo, al fine di notificarlo conformemente alla suddetta direttiva. I criteri fissati nel presente regolamento dovrebbero inoltre essere considerati esaustivi, fatto salvo l'articolo 5 della direttiva (UE) 2022/2555. Il presente regolamento specifica i casi in cui un incidente dovrebbe essere considerato significativo stabilendo casi orizzontali e specifici per tipo di soggetto.

(31) A norma dell'articolo 23, paragrafo 4, della direttiva (UE) 2022/2555, i soggetti pertinenti dovrebbero essere tenuti a notificare gli incidenti significativi entro i termini stabiliti da tale disposizione. I termini per la notifica decorrono dal momento in cui il soggetto viene a conoscenza di tali incidenti significativi. Il soggetto pertinente è quindi tenuto a segnalare gli incidenti che, sulla base della sua valutazione iniziale, potrebbero causare una grave perturbazione operativa dei servizi o perdite finanziarie per il soggetto in questione, o ripercuotersi su altre persone fisiche o giuridiche causando perdite materiali o immateriali considerevoli. Qualora abbia rilevato un evento sospetto, o dopo che un possibile incidente è stato sottoposto alla sua attenzione da un terzo, come una persona fisica, un cliente, un soggetto, un'autorità, un'organizzazione mediatica o un'altra fonte, il soggetto pertinente dovrebbe pertanto valutare tempestivamente l'evento sospetto per determinare se costituisce un incidente e, in caso affermativo, determinarne la natura e la gravità. Il soggetto pertinente è quindi da ritenersi «a conoscenza» dell'incidente significativo se, dopo tale valutazione iniziale, è ragionevolmente certo che si sia verificato un incidente significativo.

(32) Al fine di stabilire se un incidente è significativo, se del caso, i soggetti pertinenti dovrebbero conteggiare il numero di utenti interessati dall'incidente, tenendo conto dei clienti commerciali e finali con i quali i soggetti pertinenti hanno un rapporto contrattuale, nonché delle persone fisiche e giuridiche associate ai clienti commerciali. Qualora un soggetto pertinente non sia in grado di calcolare il numero di utenti interessati, ai fini del calcolo del numero totale di utenti interessati dall'incidente dovrebbe essere presa in considerazione la stima del possibile numero massimo di utenti interessati. La significatività di un incidente che riguarda un servizio fiduciario dovrebbe essere determinata non soltanto tramite il numero di utenti, ma anche tramite il numero di parti facenti affidamento sulla certificazione, in quanto esse possono essere parimenti interessate da un incidente significativo che riguarda un servizio fiduciario in relazione alle perturbazioni operative e alle perdite materiali o immateriali. Di conseguenza, se applicabile, i prestatori di servizi fiduciari dovrebbero tenere conto altresì del numero di parti facenti affidamento sulla certificazione ai fini della determinazione della significatività di un incidente. A tal fine, per parti facenti affidamento sulla certificazione si dovrebbero intendere le persone fisiche o giuridiche che fanno affidamento su un servizio fiduciario.

(33) Le operazioni di manutenzione che comportano una disponibilità limitata o un'indisponibilità dei servizi non dovrebbero essere considerate incidenti significativi se tale disponibilità limitata o indisponibilità del servizio è dovuta a un'operazione di manutenzione programmata. Inoltre, qualora un servizio non sia disponibile in ragione di interruzioni programmate, quali interruzioni o indisponibilità sulla base di un accordo contrattuale prestabilito, tali eventi non dovrebbero essere considerati un incidente significativo.

(34) La durata di un incidente che incide sulla disponibilità di un servizio dovrebbe essere misurata a partire dalla perturbazione della corretta fornitura del servizio fino al momento del ripristino. Qualora un soggetto pertinente non sia in grado di determinare il momento in cui ha avuto inizio la perturbazione, la durata dell'incidente dovrebbe essere misurata a partire dal momento in cui l'incidente è stato rilevato o dal momento in cui l'incidente è stato registrato nei registri di rete o di sistema o in altre fonti di dati, a seconda dell'evento che si verifica per primo.

(35) L'indisponibilità totale di un servizio dovrebbe essere misurata dal momento in cui il servizio è completamente indisponibile per gli utenti fino al momento in cui le attività o le operazioni regolari sono state ripristinate al livello del servizio fornito prima dell'incidente. Se un soggetto pertinente non è in grado di stabilire quando è iniziata la completa indisponibilità di un servizio, l'indisponibilità dovrebbe essere misurata dal momento in cui è stata rilevata da tale soggetto.

(36) Ai fini della determinazione delle perdite finanziarie dirette derivanti da un incidente, i soggetti pertinenti dovrebbero tenere conto di tutte le perdite finanziarie da essi subite a seguito dell'incidente, quali i costi per la sostituzione o il trasferimento di software, hardware o infrastrutture, i costi del personale, compresi i costi associati alla sostituzione o al trasferimento del personale, all'assunzione di personale supplementare, alla remunerazione di straordinari e al recupero di competenze perdute o compromesse, le spese dovute all'inosservanza degli obblighi contrattuali, i costi per risarcimenti e indennizzi ai clienti, le perdite dovute a mancate entrate, i costi associati alla comunicazione interna ed esterna, i costi di consulenza, compresi quelli relativi alla consulenza legale, ai servizi forensi e ai servizi per rimediare all'incidente, nonché altri costi associati all'incidente. Tuttavia le sanzioni amministrative e i costi necessari per il funzionamento quotidiano dell'impresa non dovrebbero essere considerati perdite finanziarie derivanti da un incidente, compresi i costi per la manutenzione generale di infrastrutture, attrezzature, hardware e software, per l'aggiornamento delle competenze del personale, i costi interni o esterni per il miglioramento dell'impresa in seguito all'incidente, compresi gli ammodernamenti, i miglioramenti e le iniziative di valutazione dei rischi e i premi assicurativi. I soggetti pertinenti dovrebbero calcolare gli importi delle perdite finanziarie sulla base dei dati disponibili e, se non fosse possibile determinare gli importi effettivi delle perdite finanziarie, dovrebbero stimarli.

(37) Inoltre i soggetti pertinenti dovrebbero essere tenuti a segnalare gli incidenti che hanno causato o che sono in grado di causare il decesso di persone fisiche o danni considerevoli alla salute di persone fisiche, in quanto tali incidenti sono casi particolarmente gravi che causano perdite materiali o immateriali considerevoli. Ad esempio un incidente che interessa un soggetto pertinente potrebbe causare l'indisponibilità di servizi sanitari o di emergenza, o la perdita della riservatezza o dell'integrità dei dati con effetti sulla salute delle persone fisiche. Al fine di stabilire se un incidente abbia causato o sia in grado di causare danni considerevoli alla salute di una persona fisica, i soggetti pertinenti dovrebbero valutare se l'incidente abbia causato o sia in grado di causare lesioni gravi e un cattivo stato di salute. A tal fine i soggetti pertinenti non dovrebbero essere tenuti a raccogliere ulteriori informazioni a cui non hanno accesso.

(38) Si dovrebbe ritenere che la disponibilità limitata si verifichi in particolare quando un servizio fornito da un soggetto pertinente è notevolmente più lento rispetto al tempo di risposta medio o quando non sono disponibili tutte le funzionalità di un servizio. Ove possibile, per valutare i ritardi nei tempi di risposta dovrebbero essere utilizzati criteri oggettivi basati sui tempi di risposta medi dei servizi forniti dai soggetti pertinenti. Una funzionalità di un servizio potrebbe essere, ad esempio, una funzionalità di chat o di ricerca di immagini.

(39) Un accesso non autorizzato e che si sospetta essere malevolo ai sistemi informativi e di rete di un soggetto pertinente dovrebbe essere considerato un incidente significativo se è in grado di causare gravi perturbazioni operative. Ad esempio, se un autore di una minaccia informatica si posiziona nei sistemi informativi e di rete di un soggetto pertinente al fine di causare perturbazioni dei servizi in futuro, tale incidente dovrebbe essere considerato significativo.

(40) Gli incidenti ricorrenti che sono collegati tra loro dalla stessa causa di fondo apparente e che singolarmente non soddisfano i criteri per essere definiti un incidente significativo dovrebbero essere considerati collettivamente come un incidente significativo, a condizione che soddisfino collettivamente il criterio della perdita finanziaria e che si siano verificati almeno due volte negli ultimi sei mesi. Tali incidenti ricorrenti possono essere un'indicazione di carenze e debolezze significative nelle procedure di gestione dei rischi di cibersicurezza del soggetto pertinente e nel suo livello di maturità in materia di cibersicurezza. Possono inoltre causare perdite finanziarie significative al soggetto pertinente.

(41) La Commissione ha scambiato pareri e cooperato con il gruppo di cooperazione e l'ENISA in merito al progetto di atto di esecuzione, conformemente all'articolo 21, paragrafo 5, e all'articolo 23, paragrafo 11, della direttiva (UE) 2022/2555.

(42) Conformemente all'articolo 42, paragrafo 1, del regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio ([3]), il Garante europeo della protezione dei dati è stato consultato e ha formulato il suo parere il 1º settembre 2024.

(43) Le misure di cui al presente regolamento sono conformi al parere del comitato istituito in conformità all'articolo 39 della direttiva (UE) 2022/2555,

HA ADOTTATO IL PRESENTE REGOLAMENTO:

Articolo 1

Oggetto

Il presente regolamento stabilisce i requisiti tecnici e metodologici delle misure di cui all'articolo 21, paragrafo 2, della direttiva (UE) 2022/2555 e specifica ulteriormente i casi in cui un incidente è considerato significativo ai sensi dell'articolo 23, paragrafo 3, della medesima direttiva per quanto riguarda i fornitori di servizi DNS, i registri dei nomi di dominio di primo livello, i fornitori di servizi di cloud computing, i fornitori di servizi di data center, i fornitori di reti di distribuzione dei contenuti, i fornitori di servizi gestiti, i fornitori di servizi di sicurezza gestiti, i fornitori di mercati online, di motori di ricerca online e di piattaforme di servizi di social network, nonché i prestatori di servizi fiduciari (i soggetti pertinenti).

Articolo 2

Requisiti tecnici e metodologici

1. Per i soggetti pertinenti i requisiti tecnici e metodologici delle misure di gestione dei rischi di cibersicurezza di cui all'articolo 21, paragrafo 2, lettere da a) a j), della direttiva (UE) 2022/2555 sono stabiliti nell'allegato del presente regolamento.

2. Nell'attuare e nell'applicare i requisiti tecnici e metodologici delle misure di gestione dei rischi di cibersicurezza di cui all'allegato del presente regolamento, i soggetti pertinenti garantiscono un livello di sicurezza dei sistemi informativi e di rete adeguato ai rischi esistenti. A tal fine, nel conformarsi ai requisiti tecnici e metodologici delle misure di gestione dei rischi di cibersicurezza di cui all'allegato del presente regolamento, tali soggetti tengono debitamente conto del grado di esposizione ai rischi, delle proprie dimensioni, della probabilità che si verifichino incidenti e della relativa gravità, compreso l'impatto sociale ed economico.

([3]) Regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE (GU L 295 del 21.11.2018, pag. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

Qualora l'allegato del presente regolamento preveda l'applicazione di un requisito tecnico o metodologico di una misura di gestione dei rischi di cibersicurezza «se opportuno», «se applicabile» o «nella misura del possibile», e qualora un soggetto pertinente ritenga che l'applicazione di determinati requisiti tecnici e metodologici non sia opportuna, applicabile o possibile, il soggetto pertinente documenta in modo comprensibile le ragioni di tale decisione.

Articolo 3

Incidenti significativi

1. Un incidente è considerato significativo ai fini dell'articolo 23, paragrafo 3, della direttiva (UE) 2022/2555 per quanto riguarda i soggetti pertinenti se sono soddisfatti uno o più dei criteri seguenti:

a) l'incidente ha causato o è in grado di causare al soggetto pertinente una perdita finanziaria diretta superiore a 500 000 EUR o, se tale importo è inferiore, al 5 % del suo fatturato totale annuo dell'esercizio precedente;

b) l'incidente ha causato o è in grado di causare l'esfiltrazione di segreti commerciali, quali definiti all'articolo 2, punto 1), della direttiva (UE) 2016/943, del soggetto pertinente;

c) l'incidente ha causato o è in grado di causare il decesso di una persona fisica;

d) l'incidente ha causato o è in grado di causare danni considerevoli alla salute di una persona fisica;

e) si è verificato un accesso non autorizzato ai sistemi informativi e di rete, che si sospetta essere malevolo ed è in grado di causare gravi perturbazioni operative;

f) l'incidente soddisfa i criteri di cui all'articolo 4;

g) l'incidente soddisfa uno o più criteri di cui agli articoli da 5 a 14.

2. Le interruzioni programmate del servizio e le conseguenze previste delle operazioni di manutenzione programmata effettuate dai soggetti pertinenti o per loro conto non sono considerate incidenti significativi.

3. Nel calcolare il numero di utenti interessati da un incidente ai fini degli articoli 7 e da 9 a 14, i soggetti pertinenti tengono conto di tutti gli elementi seguenti:

a) il numero di clienti che hanno un contratto con il soggetto pertinente che concede loro l'accesso ai sistemi informativi e di rete del soggetto pertinente o ai servizi offerti da tali sistemi o accessibili tramite tali sistemi;

b) il numero di persone fisiche e giuridiche associate a clienti commerciali che utilizzano i sistemi informativi e di rete del soggetto o i servizi offerti da tali sistemi o accessibili tramite tali sistemi.

Articolo 4

Incidenti ricorrenti

Gli incidenti che singolarmente non sono considerati un incidente significativo ai sensi dell'articolo 3 sono considerati collettivamente come un unico incidente significativo se soddisfano tutti i criteri seguenti:

a) si sono verificati almeno due volte nell'arco di sei mesi;

b) presentano la stessa causa di fondo apparente;

c) soddisfano collettivamente il criterio di cui all'articolo 3, paragrafo 1, lettera a).

Articolo 5

Incidenti significativi riguardanti i fornitori di servizi DNS

Per quanto riguarda i fornitori di servizi DNS, un incidente è considerato significativo a norma dell'articolo 3, paragrafo 1, lettera g), se soddisfa uno o più dei criteri seguenti:

a) un servizio di risoluzione dei nomi di dominio ricorsivo o autorevole è completamente indisponibile per più di 30 minuti;

b) per un periodo superiore a un'ora, il tempo di risposta medio di un servizio di risoluzione dei nomi di dominio ricorsivo o autorevole alle richieste di DNS è superiore a 10 secondi;

c) l'integrità, la riservatezza o l'autenticità dei dati conservati, trasmessi o elaborati relativi alla fornitura del servizio di risoluzione dei nomi di dominio autorevole è compromessa, tranne nei casi in cui i dati relativi a meno di 1 000 nomi di dominio gestiti dal fornitore di servizi DNS, pari a non più dell'1 % dei nomi di dominio gestiti da detto fornitore, non siano corretti a causa di una configurazione errata.

Articolo 6

Incidenti significativi riguardanti i registri dei nomi di dominio di primo livello

Per quanto riguarda i registri dei nomi di dominio di primo livello, un incidente è considerato significativo a norma dell'articolo 3, paragrafo 1, lettera g), se soddisfa uno o più dei criteri seguenti:

a) un servizio di risoluzione dei nomi di dominio autorevole è completamente indisponibile;

b) per un periodo superiore a un'ora, il tempo di risposta medio di un servizio di risoluzione dei nomi di dominio autorevole alle richieste di DNS è superiore a 10 secondi;

c) l'integrità, la riservatezza o l'autenticità dei dati conservati, trasmessi o elaborati relativi al funzionamento tecnico del dominio di primo livello è compromessa.

Articolo 7

Incidenti significativi riguardanti i fornitori di servizi di cloud computing

Per quanto riguarda i fornitori di servizi di cloud computing, un incidente è considerato significativo a norma dell'articolo 3, paragrafo 1, lettera g), se soddisfa uno o più dei criteri seguenti:

a) un servizio di cloud computing fornito è completamente indisponibile per più di 30 minuti;

b) la disponibilità di un servizio di cloud computing di un fornitore è limitata per oltre il 5 % degli utenti di tale servizio nell'Unione o per oltre 1 milione di tali utenti nell'Unione, a seconda di quale valore sia inferiore, per un periodo di tempo superiore a un'ora;

c) l'integrità, la riservatezza o l'autenticità dei dati conservati, trasmessi o elaborati relativi alla fornitura di un servizio di cloud computing è compromessa in ragione di un'azione che si sospetta essere malevola;

d) l'integrità, la riservatezza o l'autenticità dei dati conservati, trasmessi o elaborati relativi alla fornitura di un servizio di cloud computing è compromessa con un impatto su oltre il 5 % degli utenti di tale servizio nell'Unione o su oltre 1 milione di tali utenti nell'Unione, a seconda di quale valore sia inferiore.

Articolo 8

Incidenti significativi riguardanti i fornitori di servizi di data center

Per quanto riguarda i fornitori di servizi di data center, un incidente è considerato significativo a norma dell'articolo 3, paragrafo 1, lettera g), se soddisfa uno o più dei criteri seguenti:

a) un servizio di data center di un data center gestito dal fornitore è completamente indisponibile;

b) la disponibilità di un servizio di data center di un data center gestito dal fornitore è limitata per un periodo di tempo superiore a un'ora;

c) l'integrità, la riservatezza o l'autenticità dei dati conservati, trasmessi o elaborati relativi alla fornitura di un servizio di data center è compromessa in ragione di un'azione che si sospetta essere malevola;

d) l'accesso fisico a un data center gestito dal fornitore è compromesso.

Articolo 9

Incidenti significativi riguardanti i fornitori di reti di distribuzione dei contenuti

Per quanto riguarda i fornitori di reti di distribuzione dei contenuti, un incidente è considerato significativo a norma dell'articolo 3, paragrafo 1, lettera g), se soddisfa uno o più dei criteri seguenti:

a) una rete di distribuzione dei contenuti è completamente indisponibile per più di 30 minuti;

b) la disponibilità di una rete di distribuzione dei contenuti è limitata per oltre il 5 % degli utenti di tale rete nell'Unione o per oltre 1 milione di tali utenti nell'Unione, a seconda di quale valore sia inferiore, per un periodo di tempo superiore a un'ora;

c) l'integrità, la riservatezza o l'autenticità dei dati conservati, trasmessi o elaborati relativi alla fornitura di una rete di distribuzione dei contenuti è compromessa in ragione di un'azione che si sospetta essere malevola;

d) l'integrità, la riservatezza o l'autenticità dei dati conservati, trasmessi o elaborati relativi alla fornitura di una rete di distribuzione dei contenuti è compromessa con un impatto su oltre il 5 % degli utenti di tale rete nell'Unione o su oltre 1 milione di tali utenti nell'Unione, a seconda di quale valore sia inferiore.

Articolo 10

Incidenti significativi riguardanti i fornitori di servizi gestiti e i fornitori di servizi di sicurezza gestiti

Per quanto riguarda i fornitori di servizi gestiti e i fornitori di servizi di sicurezza gestiti, un incidente è considerato significativo a norma dell'articolo 3, paragrafo 1, lettera g), se soddisfa uno o più dei criteri seguenti:

a) un servizio gestito o un servizio di sicurezza gestito è completamente indisponibile per più di 30 minuti;

b) la disponibilità di un servizio gestito o di un servizio di sicurezza gestito è limitata per oltre il 5 % degli utenti di tale servizio nell'Unione o per oltre 1 milione di tali utenti nell'Unione, a seconda di quale valore sia inferiore, per un periodo di tempo superiore a un'ora;

c) l'integrità, la riservatezza o l'autenticità dei dati conservati, trasmessi o elaborati relativi alla fornitura di un servizio gestito o di un servizio di sicurezza gestito è compromessa in ragione di un'azione che si sospetta essere malevola;

d) l'integrità, la riservatezza o l'autenticità dei dati conservati, trasmessi o elaborati relativi alla fornitura di un servizio gestito o di un servizio di sicurezza gestito è compromessa con un impatto su oltre il 5 % degli utenti del servizio gestito o del servizio di sicurezza gestito nell'Unione o su oltre 1 milione di tali utenti nell'Unione, a seconda di quale valore sia inferiore.

Articolo 11

Incidenti significativi riguardanti i fornitori di mercati online

Per quanto riguarda i fornitori di mercati online, un incidente è considerato significativo a norma dell'articolo 3, paragrafo 1, lettera g), se soddisfa uno o più dei criteri seguenti:

a) un mercato online è completamente indisponibile per oltre il 5 % degli utenti di tale mercato nell'Unione o per oltre 1 milione di tali utenti nell'Unione, a seconda di quale valore sia inferiore;

b) oltre il 5 % degli utenti di un mercato online nell'Unione o oltre 1 milione di tali utenti nell'Unione, a seconda di quale valore sia inferiore, risente della disponibilità limitata del mercato online;

c) l'integrità, la riservatezza o l'autenticità dei dati conservati, trasmessi o elaborati relativi alla fornitura di un mercato online è compromessa in ragione di un'azione che si sospetta essere malevola;

d) l'integrità, la riservatezza o l'autenticità dei dati conservati, trasmessi o elaborati relativi alla fornitura di un mercato online è compromessa con un impatto su oltre il 5 % degli utenti di tale mercato nell'Unione o su oltre 1 milione di tali utenti nell'Unione, a seconda di quale valore sia inferiore.

Articolo 12

Incidenti significativi riguardanti i fornitori di motori di ricerca online

Per quanto riguarda i fornitori di motori di ricerca online, un incidente è considerato significativo a norma dell'articolo 3, paragrafo 1, lettera g), se soddisfa uno o più dei criteri seguenti:

a) un motore di ricerca online è completamente indisponibile per oltre il 5 % degli utenti di tale motore di ricerca nell'Unione o per oltre 1 milione di tali utenti nell'Unione, a seconda di quale valore sia inferiore;

b) oltre il 5 % degli utenti di un motore di ricerca online nell'Unione o oltre 1 milione di tali utenti nell'Unione, a seconda di quale valore sia inferiore, risente della disponibilità limitata del motore di ricerca online;

c) l'integrità, la riservatezza o l'autenticità dei dati conservati, trasmessi o elaborati relativi alla fornitura di un motore di ricerca online è compromessa in ragione di un'azione che si sospetta essere malevola;

d) l'integrità, la riservatezza o l'autenticità dei dati conservati, trasmessi o elaborati relativi alla fornitura di un motore di ricerca online è compromessa con un impatto su oltre il 5 % degli utenti di tale motore di ricerca nell'Unione o su oltre 1 milione di tali utenti nell'Unione, a seconda di quale valore sia inferiore.

Articolo 13

Incidenti significativi riguardanti i fornitori di piattaforme di servizi di social network

Per quanto riguarda i fornitori di piattaforme di servizi di social network, un incidente è considerato significativo a norma dell'articolo 3, paragrafo 1, lettera g), se soddisfa uno o più dei criteri seguenti:

a) la piattaforma di servizi di social network è completamente indisponibile per oltre il 5 % degli utenti di tale piattaforma nell'Unione o per oltre 1 milione di tali utenti nell'Unione, a seconda di quale valore sia inferiore;

b) oltre il 5 % degli utenti di una piattaforma di servizi di social network nell'Unione o oltre 1 milione di tali utenti nell'Unione, a seconda di quale valore sia inferiore, risente della disponibilità limitata della piattaforma di servizi di social network;

c) l'integrità, la riservatezza o l'autenticità dei dati conservati, trasmessi o elaborati relativi alla fornitura di una piattaforma di servizi di social network è compromessa in ragione di un'azione che si sospetta essere malevola;

d) l'integrità, la riservatezza o l'autenticità dei dati conservati, trasmessi o elaborati relativi alla fornitura di una piattaforma di servizi di social network è compromessa con un impatto su oltre il 5 % degli utenti di tale piattaforma nell'Unione o su oltre 1 milione di tali utenti nell'Unione, a seconda di quale valore sia inferiore.

Articolo 14

Incidenti significativi riguardanti i prestatori di servizi fiduciari

Per quanto riguarda i prestatori di servizi fiduciari, un incidente è considerato significativo a norma dell'articolo 3, paragrafo 1, lettera g), se soddisfa uno o più dei criteri seguenti:

a) un servizio fiduciario è completamente indisponibile per più di 20 minuti;

b) un servizio fiduciario non è disponibile per gli utenti o per le parti facenti affidamento sulla certificazione per più di un'ora calcolata sulla base di una settimana di calendario;

c) oltre l'1 % degli utenti o delle parti facenti affidamento sulla certificazione nell'Unione o oltre 200 000 utenti o parti facenti affidamento sulla certificazione nell'Unione, a seconda di quale valore sia inferiore, risentono della disponibilità limitata di un servizio fiduciario;

d) l'accesso fisico a un'area in cui sono ubicati i sistemi informativi e di rete e il cui accesso è limitato al personale di fiducia del prestatore di servizi fiduciari o la protezione di tale accesso fisico sono compromessi;

e) l'integrità, la riservatezza o l'autenticità dei dati conservati, trasmessi o elaborati relativi alla fornitura di un servizio fiduciario è compromessa con un impatto su oltre lo 0,1 % degli utenti o delle parti facenti affidamento sulla certificazione o su oltre 100 utenti o parti facenti affidamento sulla certificazione del servizio fiduciario nell'Unione, a seconda di quale valore sia inferiore.

Articolo 15

Abrogazione

Il regolamento di esecuzione (UE) 2018/151 della Commissione ([4]) è abrogato.

Articolo 16

Entrata in vigore e applicazione

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

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

Fatto a Bruxelles, il 17 ottobre 2024

Per la Commissione
La presidente
Ursula VON DER LEYEN

([4]) Regolamento di esecuzione (UE) 2018/151 della Commissione, del 30 gennaio 2018, recante modalità di applicazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio per quanto riguarda l'ulteriore specificazione degli elementi che i fornitori di servizi digitali devono prendere in considerazione ai fini della gestione dei rischi posti alla sicurezza delle reti e dei sistemi informativi e dei parametri per determinare l'eventuale impatto rilevante di un incidente (GU L 26 del 31.1.2018, pag. 48, ELI: http://data.europa.eu/eli/reg_impl/2018/151/oj).

ALLEGATO

Requisiti tecnici e metodologici di cui all'articolo 2 del presente regolamento

1. **Politica di sicurezza dei sistemi informativi e di rete [articolo 21, paragrafo 2, lettera a), della direttiva (UE) 2022/2555]**

1.1. *Politica di sicurezza dei sistemi informativi e di rete*

1.1.1. Ai fini dell'articolo 21, paragrafo 2, lettera a), della direttiva (UE) 2022/2555, la politica di sicurezza dei sistemi informativi e di rete deve:

a) definire l'approccio dei soggetti pertinenti alla gestione della sicurezza dei loro sistemi informativi e di rete;

b) essere adeguata alla strategia e agli obiettivi aziendali dei soggetti pertinenti e complementare a tale strategia e tali obiettivi;

c) stabilire obiettivi di sicurezza dei sistemi informativi e di rete;

d) includere un impegno al miglioramento continuo della sicurezza dei sistemi informativi e di rete;

e) includere un impegno a fornire le risorse adeguate necessarie per la sua attuazione, compresi il personale, le risorse finanziarie, i processi, gli strumenti e le tecnologie necessari;

f) essere comunicata ai dipendenti e alle parti esterne interessate pertinenti ed essere da essi riconosciuta;

g) definire i ruoli e le responsabilità a norma del punto 1.2;

h) elencare la documentazione da conservare e la durata della sua conservazione;

i) elencare le politiche specifiche per tematica;

j) stabilire indicatori e misure volti a monitorare la sua attuazione e lo stato corrente del livello di maturità della sicurezza dei sistemi informativi e di rete dei soggetti pertinenti;

k) indicare la data dell'approvazione formale da parte degli organi di gestione dei soggetti pertinenti («organi di gestione»).

1.1.2. La politica di sicurezza dei sistemi informativi e di rete deve essere riesaminata e, se opportuno, aggiornata dagli organi di gestione almeno annualmente e qualora si verifichino incidenti significativi o cambiamenti significativi delle operazioni o dei rischi. Il risultato dei riesami deve essere documentato.

1.2. *Ruoli, responsabilità e autorità*

1.2.1. Nel contesto della loro politica di sicurezza dei sistemi informativi e di rete di cui al punto 1.1, i soggetti pertinenti devono stabilire le responsabilità e le autorità in materia di sicurezza dei sistemi informativi e di rete e assegnarle a ruoli, attribuendole in base alle esigenze dei soggetti pertinenti e comunicandole agli organi di gestione.

1.2.2. I soggetti pertinenti devono imporre a tutto il personale e ai terzi di applicare la sicurezza dei sistemi informativi e di rete conformemente alla relativa politica, alle politiche specifiche per tematica e alle procedure dei soggetti pertinenti.

1.2.3. Almeno una persona deve riferire direttamente agli organi di gestione in merito a questioni relative alla sicurezza dei sistemi informativi e di rete.

1.2.4. A seconda delle dimensioni dei soggetti pertinenti, la sicurezza dei sistemi informativi e di rete deve essere trattata da ruoli o compiti specifici svolti in aggiunta ai ruoli esistenti.

1.2.5. Le funzioni e i settori di responsabilità contrastanti devono essere separati, se applicabile.

1.2.6. I ruoli, le responsabilità e le autorità devono essere riesaminati e, se opportuno, aggiornati dagli organi di gestione a intervalli pianificati e qualora si verifichino incidenti significativi o cambiamenti significativi delle operazioni o dei rischi.

2. **Politica di gestione dei rischi [articolo 21, paragrafo 2, lettera a), della direttiva (UE) 2022/2555]**

2.1. *Quadro di gestione dei rischi*

2.1.1. Ai fini dell'articolo 21, paragrafo 2, lettera a), della direttiva (UE) 2022/2555, i soggetti pertinenti devono istituire e mantenere un quadro di gestione dei rischi adeguato al fine di individuare e affrontare i rischi per la sicurezza dei sistemi informativi e di rete. I soggetti pertinenti devono eseguire e documentare valutazioni dei rischi e, sulla base dei risultati, stabilire, attuare e monitorare un piano di trattamento dei rischi. I risultati della valutazione dei rischi e i rischi residui devono essere accettati dagli organi di gestione o, se applicabile, da persone che sono responsabili e dispongono dell'autorità per gestire i rischi, a condizione che i soggetti pertinenti garantiscano una segnalazione adeguata agli organi di gestione.

2.1.2. Ai fini del punto 2.1.1, i soggetti pertinenti devono stabilire procedure per l'individuazione, l'analisi, la valutazione e il trattamento dei rischi («processo di gestione dei rischi di cibersicurezza»). Il processo di gestione dei rischi di cibersicurezza deve essere parte integrante del processo generale di gestione dei rischi dei soggetti pertinenti, se applicabile. Nell'ambito del processo di gestione dei rischi di cibersicurezza, i soggetti pertinenti devono:

a) seguire una metodologia di gestione dei rischi;

b) stabilire il livello di tolleranza per i rischi conformemente alla propensione al rischio dei soggetti pertinenti;

c) stabilire e mantenere criteri di rischio pertinenti;

d) in linea con un approccio multirischio, individuare e documentare i rischi per la sicurezza dei sistemi informativi e di rete, in particolare in relazione a terzi, come pure i rischi che potrebbero causare perturbazioni in termini di disponibilità, integrità, autenticità e riservatezza dei sistemi informativi e di rete, compresa l'individuazione dei singoli punti di vulnerabilità (*single points of failure*);

e) analizzare i rischi per la sicurezza dei sistemi informativi e di rete, compresi la minaccia, la probabilità, l'impatto e il livello di rischio, tenendo conto delle informazioni di intelligence relative alle minacce informatiche e delle vulnerabilità;

f) valutare i rischi individuati sulla base dei criteri di rischio;

g) individuare le opzioni e le misure adeguate per il trattamento dei rischi e attribuirvi la priorità;

h) monitorare costantemente l'attuazione delle misure di trattamento dei rischi;

i) individuare i soggetti competenti per l'attuazione delle misure di trattamento dei rischi e la tempistica per tale attuazione;

j) documentare in un piano di trattamento dei rischi, in modo comprensibile, le misure di trattamento dei rischi scelte e le ragioni che giustificano l'accettazione di rischi residui.

2.1.3. Nell'individuare le opzioni e le misure adeguate di trattamento dei rischi e nel definirne un ordine di priorità, i soggetti pertinenti devono tenere conto dei risultati della valutazione dei rischi, dei risultati della procedura volta a valutare l'efficacia delle misure di gestione dei rischi di cibersicurezza, dei costi di attuazione in relazione ai benefici attesi, della classificazione delle risorse di cui al punto 12.1 e dell'analisi dell'impatto sulle attività aziendali (*business impact analysis*) di cui al punto 4.1.3.

2.1.4. I soggetti pertinenti devono riesaminare e, se opportuno, aggiornare i risultati della valutazione dei rischi e il piano di trattamento dei rischi a intervalli pianificati e almeno con cadenza annuale, nonché qualora si verifichino incidenti significativi o cambiamenti significativi delle operazioni o dei rischi.

2.2. *Monitoraggio della conformità*

2.2.1. I soggetti pertinenti devono riesaminare periodicamente il rispetto delle loro politiche di sicurezza dei sistemi informativi e di rete nonché delle loro politiche specifiche per tematica, regole e norme. Gli organi di gestione devono essere informati in merito allo stato della sicurezza dei sistemi informativi e di rete sulla base dei riesami di conformità mediante relazioni periodiche.

2.2.2. I soggetti pertinenti devono mettere in atto un sistema efficace di comunicazione della conformità che sia adeguato alle loro strutture, ai loro ambienti operativi e al loro panorama delle minacce. Tale sistema di comunicazione della conformità deve essere in grado di fornire agli organi di gestione una visione informata dello stato corrente della gestione dei rischi da parte dei soggetti pertinenti.

2.2.3. I soggetti pertinenti devono effettuare il monitoraggio della conformità a intervalli pianificati e qualora si verifichino incidenti significativi o cambiamenti significativi delle operazioni o dei rischi.

2.3. *Riesame indipendente della sicurezza dei sistemi informativi e di rete*

2.3.1. I soggetti pertinenti devono riesaminare in modo indipendente il loro approccio alla gestione della sicurezza dei sistemi informativi e di rete e alla sua attuazione, considerando anche le persone, i processi e le tecnologie.

2.3.2. I soggetti pertinenti devono sviluppare e mantenere processi volti a effettuare riesami indipendenti che devono essere svolti da persone che dispongono di competenze adeguate in materia di audit. Se il riesame indipendente è effettuato da membri del personale del soggetto pertinente, le persone che effettuano i riesami non devono appartenere alla linea gerarchica del personale del settore oggetto del riesame. Se le loro dimensioni non consentono tale separazione nella linea gerarchica, i soggetti pertinenti devono mettere in atto misure alternative per garantire l'imparzialità dei riesami.

2.3.3. I risultati dei riesami indipendenti, compresi i risultati del monitoraggio della conformità di cui al punto 2.2 e del monitoraggio e della misurazione di cui al punto 7, devono essere comunicati agli organi di gestione. Si devono adottare azioni correttive oppure si deve accettare il rischio residuo secondo i criteri di accettazione dei rischi dei soggetti pertinenti.

2.3.4. I riesami indipendenti devono essere svolti a intervalli pianificati e qualora si verifichino incidenti significativi o cambiamenti significativi delle operazioni o dei rischi.

3. **Gestione degli incidenti [articolo 21, paragrafo 2, lettera b), della direttiva (UE) 2022/2555]**

3.1. *Politica di gestione degli incidenti*

3.1.1. Ai fini dell'articolo 21, paragrafo 2, lettera b), della direttiva (UE) 2022/2555, i soggetti pertinenti devono stabilire e attuare una politica di gestione degli incidenti che stabilisca i ruoli, le responsabilità e le procedure per rilevare, analizzare e contenere gli incidenti o rispondere agli stessi, nonché per il recupero dagli incidenti, e per documentare e segnalare gli incidenti in maniera tempestiva.

3.1.2. La politica di cui al punto 3.1.1 deve essere coerente con il piano di continuità operativa e di ripristino in caso di disastro di cui al punto 4.1. Tale politica deve comprendere:

a) un sistema di categorizzazione degli incidenti coerente con la valutazione e la classificazione degli eventi effettuate a norma del punto 3.4.1;

b) piani di comunicazione efficaci, anche per quanto concerne il coinvolgimento della gerarchia e la segnalazione;

c) l'assegnazione di ruoli relativi al rilevamento degli incidenti e alla risposta adeguata agli stessi a dipendenti competenti;

d) documenti da utilizzare nel corso del rilevamento degli incidenti e della risposta agli stessi, quali manuali di risposta agli incidenti, diagrammi per il coinvolgimento della gerarchia, elenchi di contatti e modelli.

3.1.3. I ruoli, le responsabilità e le procedure stabiliti nella politica devono essere sottoposti a test e riesaminati e, se opportuno, aggiornati a intervalli pianificati e in seguito a incidenti significativi o cambiamenti significativi delle operazioni o dei rischi.

3.2. *Monitoraggio e registrazione*

3.2.1. I soggetti pertinenti devono stabilire procedure e utilizzare strumenti per monitorare e registrare le attività sui loro sistemi informativi e di rete al fine di individuare eventi che potrebbero essere considerati incidenti e rispondervi di conseguenza per attenuarne l'impatto.

3.2.2. Nella misura del possibile, tale monitoraggio deve essere automatizzato ed effettuato in modo continuo o periodico, in funzione delle capacità operative. I soggetti pertinenti devono attuare le loro attività di monitoraggio in modo da ridurre al minimo i falsi positivi e i falsi negativi.

3.2.3. Sulla base delle procedure di cui al punto 3.2.1, i soggetti pertinenti devono gestire, documentare e riesaminare i registri. I soggetti pertinenti devono redigere un elenco delle risorse da sottoporre a registrazione sulla base dei risultati della valutazione dei rischi effettuata a norma del punto 2.1. Se opportuno, i registri devono comprendere:

a) il pertinente traffico di rete in uscita e in entrata;

b) la creazione, la modifica o la cancellazione degli utenti dei sistemi informativi e di rete dei soggetti pertinenti e l'estensione delle autorizzazioni;

c) l'accesso a sistemi e applicazioni;

d) gli eventi relativi all'autenticazione;

e) tutti gli accessi privilegiati ai sistemi e alle applicazioni nonché tutte le attività svolte dagli account amministrativi;

f) l'accesso o le modifiche ai file critici di configurazione e di backup;

g) i registri di eventi e i registri provenienti da strumenti di sicurezza, quali antivirus, sistemi di rilevamento di intrusioni o firewall;

h) l'uso delle risorse del sistema e relative prestazioni;

i) l'accesso fisico agli impianti;

j) l'accesso alle apparecchiature e ai dispositivi di rete e il relativo utilizzo;

k) l'attivazione, l'arresto e la messa in pausa dei vari registri;

l) gli eventi ambientali.

3.2.4. I registri devono essere riesaminati periodicamente al fine di individuare eventuali tendenze insolite o indesiderate. Se opportuno, i soggetti pertinenti devono stabilire valori adeguati per le soglie di allarme. Se i valori stabiliti per la soglia di allarme vengono superati, l'allarme deve attivarsi, se opportuno, automaticamente. I soggetti pertinenti devono assicurare che, in caso di allarme, sia avviata tempestivamente una risposta qualificata e adeguata.

3.2.5. I soggetti pertinenti devono gestire ed effettuare copie di backup dei registri per un periodo di tempo predefinito e proteggerli da accessi o modifiche non autorizzati.

3.2.6. Nella misura del possibile i soggetti pertinenti devono garantire che tutti i sistemi dispongano di origini dell'ora sincronizzate in modo da poter correlare i registri tra i sistemi per la valutazione degli eventi. I soggetti pertinenti devono redigere e tenere un elenco di tutte le risorse oggetto di registrazione e garantire che i sistemi di monitoraggio e registrazione siano ridondanti. La disponibilità dei sistemi di monitoraggio e registrazione deve essere monitorata indipendentemente dai sistemi che stanno monitorando.

3.2.7. Le procedure e l'elenco delle risorse oggetto di registrazione devono essere riesaminati e, se opportuno, aggiornati a intervalli regolari e in seguito a incidenti significativi.

3.3. *Segnalazione di eventi*

3.3.1. I soggetti pertinenti devono mettere in atto un meccanismo semplice che consenta ai loro dipendenti, fornitori e clienti di segnalare eventi sospetti.

3.3.2. I soggetti pertinenti devono, se opportuno, comunicare il meccanismo di segnalazione degli eventi ai loro fornitori e clienti e impartire ai propri dipendenti formazioni periodiche sulle modalità di utilizzo del meccanismo.

3.4. *Valutazione e classificazione degli eventi*

3.4.1. I soggetti pertinenti devono valutare gli eventi sospetti al fine di stabilire se costituiscono incidenti e, in caso affermativo, ne devono determinare la natura e la gravità.

3.4.2. Ai fini del punto 3.4.1, i soggetti pertinenti devono agire come segue:

a) effettuare la valutazione sulla base di criteri predefiniti stabiliti in anticipo e di un triage al fine di stabilire l'ordine di priorità del contenimento e dell'eradicazione degli incidenti;

b) valutare trimestralmente l'esistenza di incidenti ricorrenti di cui all'articolo 4 del presente regolamento;

c) riesaminare i registri adeguati ai fini della valutazione e della classificazione degli eventi;

d) mettere in atto un processo per la correlazione e l'analisi dei registri; e

e) rivalutare e riclassificare gli eventi nel caso in cui diventino disponibili nuove informazioni o in seguito all'analisi di informazioni precedentemente disponibili.

3.5. *Risposta agli incidenti*

3.5.1. I soggetti pertinenti devono rispondere agli incidenti conformemente a procedure documentate e in modo tempestivo.

3.5.2. Le procedure di risposta agli incidenti devono comprendere le fasi seguenti:

a) contenimento degli incidenti al fine di prevenire la diffusione delle conseguenze dell'incidente;

b) eradicazione al fine di evitare il protrarsi o la ricomparsa dell'incidente;

c) recupero dall'incidente, se necessario.

3.5.3. I soggetti pertinenti devono stabilire piani e procedure di comunicazione:

a) con i team di risposta agli incidenti di sicurezza informatica (*Computer Security Incident Response Teams*, CSIRT) o, se applicabile, con le autorità competenti, in relazione alla notifica di incidenti;

b) per la comunicazione tra i membri del proprio personale e con i pertinenti portatori di interessi esterni ai soggetti pertinenti.

3.5.4. I soggetti pertinenti devono registrare le attività di risposta agli incidenti conformemente alle procedure di cui al punto 3.2.1 e le prove corrispondenti.

3.5.5. A intervalli pianificati i soggetti pertinenti devono sottoporre a test le loro procedure di risposta agli incidenti.

3.6. *Riesami successivi agli incidenti*

3.6.1. Se opportuno, i soggetti pertinenti devono effettuare riesami successivi agli incidenti dopo il recupero dagli incidenti stessi. Tali riesami successivi agli incidenti devono individuare, ove possibile, la causa di fondo dell'incidente e dare luogo a insegnamenti tratti documentati al fine di ridurre il verificarsi e le conseguenze di incidenti futuri.

3.6.2. I soggetti pertinenti devono provvedere affinché i riesami successivi agli incidenti contribuiscano a migliorare il loro approccio alla sicurezza dei sistemi informativi e di rete, le loro misure di trattamento dei rischi e le loro procedure di gestione e rilevamento degli incidenti e di risposta agli stessi.

3.6.3. I soggetti pertinenti devono riesaminare a intervalli pianificati se gli incidenti abbiano dato luogo a riesami successivi agli incidenti.

4. **Continuità operativa e gestione delle crisi [articolo 21, paragrafo 2, lettera c), della direttiva (UE) 2022/2555]**

4.1. *Piano di continuità operativa e di ripristino in caso di disastro*

4.1.1. Ai fini dell'articolo 21, paragrafo 2, lettera c), della direttiva (UE) 2022/2555, i soggetti pertinenti devono stabilire e mantenere un piano di continuità operativa e di ripristino in caso di disastro da applicare in caso di incidenti.

4.1.2. Le operazioni dei soggetti pertinenti devono essere ripristinate conformemente a tale piano di continuità operativa e di ripristino in caso di disastro. Detto piano deve essere basato sui risultati della valutazione dei rischi effettuata a norma del punto 2.1 e deve comprendere, se opportuno, gli elementi seguenti:

a) finalità, ambito di applicazione e pubblico;

b) ruoli e responsabilità;

c) contatti principali e canali di comunicazione (interni ed esterni);

d) condizioni per l'attivazione e la disattivazione del piano;

e) ordine di ripristino delle operazioni;

f) piani di ripristino per operazioni specifiche, compresi gli obiettivi di ripristino;

g) risorse necessarie, compresi i backup e le ridondanze;

h) ripristino e ripresa delle attività a partire dalle misure temporanee.

4.1.3. I soggetti pertinenti devono effettuare un'analisi dell'impatto sulle attività aziendali al fine di valutare il potenziale impatto di perturbazioni gravi delle loro operazioni aziendali e, sulla base dei risultati di tale analisi, devono stabilire i requisiti di continuità per i sistemi informativi e di rete.

4.1.4. Il piano di continuità operativa e di ripristino in caso di disastro deve essere sottoposto a test, riesaminato e, se opportuno, aggiornato a intervalli pianificati e in seguito a incidenti significativi o cambiamenti significativi delle operazioni o dei rischi. I soggetti pertinenti devono provvedere affinché tali piani integrino gli insegnamenti tratti da detti test.

4.2. *Gestione di backup e ridondanza*

4.2.1. I soggetti pertinenti devono conservare copie di backup dei dati e fornire risorse disponibili sufficienti, tra cui impianti, sistemi informativi e di rete e personale, per garantire un livello adeguato di ridondanza.

4.2.2. Sulla base dei risultati della valutazione dei rischi effettuata a norma del punto 2.1 e del piano di continuità operativa, i soggetti pertinenti devono stabilire piani di backup comprendenti gli elementi seguenti:

a) tempi di ripristino;

b) assicurazione della completezza e correttezza delle copie di backup, compresi i dati di configurazione e i dati conservati nell'ambiente di servizi di cloud computing;

c) conservazione di copie di backup (online o offline) in uno o più luoghi sicuri, che non si trovino nella medesima rete del sistema e che si trovino a una distanza sufficiente da sfuggire a qualsiasi danno causato da un disastro presso il sito principale;

d) controlli adeguati degli accessi fisici e logici alle copie di backup, conformemente al livello di classificazione delle risorse;

e) ripristino dei dati da copie di backup;

f) periodi di conservazione basati su obblighi commerciali e normativi.

4.2.3. I soggetti pertinenti devono effettuare controlli periodici dell'integrità delle copie di backup.

4.2.4. Sulla base dei risultati della valutazione dei rischi effettuata a norma del punto 2.1 e del piano di continuità operativa, i soggetti pertinenti devono assicurare la disponibilità di risorse sufficienti mediante una ridondanza quanto meno parziale degli elementi seguenti:

a) sistemi informativi e di rete;

b) risorse, compresi impianti, attrezzature e forniture;

c) personale avente le responsabilità, l'autorità e le competenze necessarie;

d) canali di comunicazione adeguati.

4.2.5. Se opportuno, i soggetti pertinenti devono provvedere affinché il monitoraggio e l'adeguamento delle risorse, compresi gli impianti, i sistemi e il personale, si basino debitamente sui requisiti in materia di backup e ridondanza.

4.2.6. I soggetti pertinenti devono sottoporre periodicamente a test il ripristino di copie di backup e le ridondanze al fine di garantire che, in condizioni di ripristino, tali copie e ridondanze possano essere affidabili e comprendano le copie, i processi e le conoscenze necessari per effettuare un ripristino efficace. I soggetti pertinenti devono documentare i risultati dei test e, se necessario, adottare misure correttive.

4.3. *Gestione delle crisi*

4.3.1. I soggetti pertinenti devono mettere in atto un processo per la gestione delle crisi.

4.3.2. I soggetti pertinenti devono provvedere affinché il processo di gestione delle crisi comprenda quanto meno gli elementi seguenti:

a) ruoli e responsabilità del personale e, se opportuno, dei fornitori e dei fornitori di servizi, specificando l'assegnazione dei ruoli in situazioni di crisi, comprese le misure specifiche da seguire;

b) mezzi di comunicazione adeguati tra i soggetti pertinenti e le autorità competenti pertinenti;

c) applicazione di misure adeguate per garantire il mantenimento della sicurezza dei sistemi informativi e di rete in situazioni di crisi.

Ai fini della lettera b), il flusso di informazioni tra i soggetti pertinenti e le autorità competenti pertinenti deve comprendere tanto le comunicazioni obbligatorie, quali le segnalazioni di incidenti e le tempistiche corrispondenti, quanto le comunicazioni non obbligatorie.

4.3.3. I soggetti pertinenti devono attuare un processo per gestire e utilizzare le informazioni ricevute dai CSIRT o, se applicabile, dalle autorità competenti in merito a incidenti, vulnerabilità, minacce o possibili misure di mitigazione.

4.3.4. I soggetti pertinenti devono sottoporre a test, riesaminare e, se opportuno, aggiornare il piano di gestione delle crisi periodicamente o a seguito di incidenti significativi o di cambiamenti significativi delle operazioni o dei rischi.

5. **Sicurezza della catena di approvvigionamento [articolo 21, paragrafo 2, lettera d), della direttiva (UE) 2022/2555]**

5.1. *Politica di sicurezza della catena di approvvigionamento*

5.1.1. Ai fini dell'articolo 21, paragrafo 2, lettera d), della direttiva (UE) 2022/2555, i soggetti pertinenti devono stabilire, attuare e applicare una politica di sicurezza della catena di approvvigionamento che disciplini le relazioni con i loro diretti fornitori e fornitori di servizi al fine di attenuare i rischi individuati per la sicurezza dei sistemi informativi e di rete. Nel contesto della politica di sicurezza della catena di approvvigionamento, i soggetti pertinenti devono individuare il loro ruolo in tale catena e comunicarlo ai loro diretti fornitori e fornitori di servizi.

5.1.2. Nell'ambito della politica di sicurezza della catena di approvvigionamento di cui al punto 5.1.1, i soggetti pertinenti devono stabilire i criteri per selezionare e concedere appalti a fornitori e fornitori di servizi. Tali criteri devono includere quanto segue:

a) le pratiche in materia di cibersicurezza dei fornitori e dei fornitori di servizi, comprese le loro procedure di sviluppo sicuro;

b) la capacità dei fornitori e dei fornitori di servizi di soddisfare le specifiche di cibersicurezza stabilite dai soggetti pertinenti;

c) la qualità e la resilienza complessive dei prodotti delle tecnologie dell'informazione e della comunicazione (TIC) e dei servizi TIC e le misure di gestione dei rischi di cibersicurezza in essi incorporate, compresi i rischi e il livello di classificazione dei prodotti TIC e dei servizi TIC;

d) la capacità dei soggetti pertinenti di diversificare le fonti di approvvigionamento e di limitare la dipendenza da un unico fornitore, se applicabile.

5.1.3. Nel definire la loro politica di sicurezza della catena di approvvigionamento, i soggetti pertinenti devono tenere conto dei risultati delle valutazioni coordinate dei rischi per la sicurezza delle catene di approvvigionamento critiche effettuate conformemente all'articolo 22, paragrafo 1, della direttiva (UE) 2022/2555, se applicabile.

5.1.4. Sulla base della politica di sicurezza della catena di approvvigionamento e tenendo conto dei risultati della valutazione dei rischi effettuata conformemente al punto 2.1 del presente allegato, i soggetti pertinenti devono provvedere affinché i loro contratti con i fornitori e i fornitori di servizi specifichino, se opportuno mediante accordi sul livello dei servizi, gli elementi seguenti, se opportuno:

a) i requisiti di cibersicurezza per i fornitori o i fornitori di servizi, compresi i requisiti relativi alla sicurezza nell'acquisizione di servizi TIC o prodotti TIC di cui al punto 6.1;

b) i requisiti in materia di sensibilizzazione, competenze e formazione e, se opportuno, certificazioni adeguate, imposti ai dipendenti dei fornitori o dei fornitori di servizi;

c) i requisiti relativi alla verifica dei precedenti personali dei dipendenti dei fornitori e dei fornitori di servizi;

d) l'obbligo per i fornitori e i fornitori di servizi di notificare senza indebito ritardo ai soggetti pertinenti gli incidenti che presentano un rischio per la sicurezza dei sistemi informativi e di rete di tali soggetti;

e) il diritto a effettuare audit o il diritto a ricevere relazioni di audit;

f) l'obbligo per i fornitori e i fornitori di servizi di gestire le vulnerabilità che presentano un rischio per la sicurezza dei sistemi informativi e di rete dei soggetti pertinenti;

g) i requisiti in materia di subappalto e, se i soggetti pertinenti consentono il subappalto, i requisiti di cibersicurezza per i subappaltatori conformemente ai requisiti di cibersicurezza di cui alla lettera a);

h) gli obblighi per i fornitori e i fornitori di servizi al momento della risoluzione del contratto, quali il recupero e lo smaltimento delle informazioni ottenute dai fornitori e dai fornitori di servizi nell'esercizio dei loro compiti.

5.1.5. I soggetti pertinenti devono tenere conto degli elementi di cui ai punti 5.1.2 e 5.1.3 nel contesto del processo di selezione dei nuovi fornitori e dei fornitori di servizi, nonché della procedura di appalto di cui al punto 6.1.

5.1.6. I soggetti pertinenti devono riesaminare la politica di sicurezza della catena di approvvigionamento nonché monitorare e valutare le modifiche delle pratiche di cibersicurezza dei fornitori e dei fornitori di servizi, intervenendo se necessario, a intervalli pianificati e quando si verificano cambiamenti significativi delle operazioni o dei rischi oppure incidenti significativi connessi alla fornitura di servizi TIC o che incidono sulla sicurezza dei prodotti TIC forniti dai fornitori e dai fornitori di servizi.

5.1.7. Ai fini del punto 5.1.6 i soggetti pertinenti devono:

a) monitorare periodicamente le relazioni sull'attuazione degli accordi sul livello dei servizi, se applicabile;

b) esaminare gli incidenti relativi ai prodotti TIC e ai servizi TIC di fornitori e fornitori di servizi;

c) valutare la necessità di riesami non programmati e documentare i risultati in modo comprensibile;

d) analizzare i rischi presentati dalle modifiche relative ai prodotti TIC e ai servizi TIC dei fornitori e dei fornitori di servizi e, se opportuno, adottare tempestivamente misure di attenuazione.

5.2. *Elenco dei fornitori e dei fornitori di servizi*

I soggetti pertinenti devono tenere e mantenere aggiornato un registro dei loro diretti fornitori e fornitori di servizi, comprendente:

a) punti di contatto per ciascun diretto fornitore e fornitore di servizi;

b) un elenco di prodotti TIC, servizi TIC e processi TIC forniti ai soggetti pertinenti dal diretto fornitore o fornitore di servizi in questione.

6. **Sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informativi e di rete [articolo 21, paragrafo 2, lettera e), della direttiva (UE) 2022/2555]**

6.1. *Sicurezza dell'acquisizione di servizi TIC o prodotti TIC*

6.1.1. Ai fini dell'articolo 21, paragrafo 2, lettera e), della direttiva (UE) 2022/2555, i soggetti pertinenti, sulla base della valutazione dei rischi effettuata a norma del punto 2.1, devono stabilire e attuare processi per gestire i rischi derivanti dall'acquisizione, dai fornitori o dai fornitori di servizi, di servizi TIC o prodotti TIC per componenti critici per la sicurezza dei loro sistemi informativi e di rete durante tutto il loro ciclo di vita.

6.1.2. Ai fini del punto 6.1.1, i processi di cui a tale punto devono comprendere:

a) requisiti di sicurezza da applicare ai servizi TIC o ai prodotti TIC da acquisire;

b) requisiti relativi agli aggiornamenti di sicurezza durante l'intero ciclo di vita dei servizi TIC o dei prodotti TIC oppure relativi alla sostituzione dopo la fine del periodo di supporto;

c) informazioni che descrivono i componenti hardware e software utilizzati nei servizi TIC o nei prodotti TIC;

d) informazioni che descrivono le funzioni di cibersicurezza implementate nei servizi TIC o nei prodotti TIC e la configurazione necessaria per il loro funzionamento sicuro;

e) la garanzia della conformità dei servizi TIC o dei prodotti TIC ai requisiti di sicurezza di cui alla lettera a);

f) metodi per convalidare la conformità dei servizi TIC o dei prodotti TIC forniti ai requisiti di sicurezza dichiarati, nonché la documentazione dei risultati della convalida.

6.1.3. I soggetti pertinenti devono riesaminare e, se opportuno, aggiornare i processi a intervalli pianificati e qualora si verifichino incidenti significativi.

6.2. *Ciclo di vita dello sviluppo sicuro*

6.2.1. Prima di sviluppare un sistema informativo e di rete, compreso il software, i soggetti pertinenti devono stabilire norme per lo sviluppo sicuro di sistemi informativi e di rete e applicarle quando sviluppano tali sistemi internamente o quando esternalizzano lo sviluppo di tali sistemi. Dette norme devono riguardare tutte le fasi di sviluppo, comprese le specifiche, la progettazione, lo sviluppo, l'implementazione e i test.

6.2.2. Ai fini del punto 6.2.1, i soggetti pertinenti devono:

a) effettuare un'analisi dei requisiti di sicurezza nelle fasi delle specifiche e della progettazione di qualsiasi progetto di sviluppo o acquisizione intrapreso dai soggetti pertinenti o per conto di questi ultimi;

b) applicare principi per la creazione di sistemi sicuri e principi di programmazione sicura a tutte le attività di sviluppo dei sistemi informativi, quali la promozione della cibersicurezza fin dalla progettazione e delle architetture zero trust;

c) stabilire i requisiti di sicurezza relativi agli ambienti di sviluppo;

d) stabilire e implementare processi di test della sicurezza nel ciclo di vita dello sviluppo;

e) selezionare, proteggere e gestire adeguatamente i dati relativi ai test di sicurezza;

f) sanificare e anonimizzare i dati dei test in base alla valutazione dei rischi effettuata a norma del punto 2.1.

6.2.3. In caso di sviluppo esternalizzato di sistemi informativi e di rete, i soggetti pertinenti devono anche applicare le politiche e le procedure di cui ai punti 5 e 6.1.

6.2.4. A intervalli pianificati, i soggetti pertinenti devono riesaminare e, se necessario, aggiornare le loro norme in materia di sviluppo sicuro.

6.3. *Gestione della configurazione*

6.3.1. I soggetti pertinenti devono adottare misure adeguate per istituire, documentare, implementare e monitorare configurazioni, comprese le configurazioni di sicurezza di hardware, software, servizi e reti.

6.3.2. Ai fini del punto 6.3.1, i soggetti pertinenti devono:

a) definire e garantire la sicurezza nelle configurazioni per i loro hardware, software e servizi e le loro reti;

b) definire e attuare processi e strumenti volti a fare rispettare le configurazioni sicure definite per l'hardware, il software, i servizi e le reti, per i sistemi di nuova installazione e per i sistemi in funzione durante il loro ciclo di vita.

6.3.3. I soggetti pertinenti devono riesaminare e, se opportuno, aggiornare le configurazioni a intervalli pianificati o qualora si verifichino incidenti significativi o cambiamenti significativi delle operazioni o dei rischi.

6.4. *Gestione delle modifiche, riparazioni e manutenzione*

6.4.1. I soggetti pertinenti devono applicare procedure di gestione delle modifiche per controllare le modifiche di sistemi informativi e di rete. Se applicabile, tali procedure devono essere coerenti con le politiche generali di gestione delle modifiche dei soggetti pertinenti.

6.4.2. Le procedure di cui al punto 6.4.1 devono essere applicate alle versioni (*release*), ai cambiamenti e alle modifiche di emergenza di qualsiasi software e hardware in funzionamento nonché alle modifiche della configurazione. Le procedure devono garantire che tali modifiche siano documentate e, sulla base della valutazione dei rischi effettuata a norma del punto 2.1, siano sottoposte a test e valutate in considerazione del potenziale impatto prima di essere attuate.

6.4.3. Nel caso in cui non sia stato possibile seguire le normali procedure di gestione delle modifiche a causa di un'emergenza, i soggetti pertinenti devono documentare il risultato della modifica apportata e la spiegazione del motivo per cui non è stato possibile seguire le procedure.

6.4.4. I soggetti pertinenti devono riesaminare e, se opportuno, aggiornare le procedure a intervalli pianificati e qualora si verifichino incidenti significativi o cambiamenti significativi delle operazioni o dei rischi.

6.5. *Test di sicurezza*

6.5.1. I soggetti pertinenti devono stabilire, attuare e applicare una politica e procedure per i test di sicurezza.

6.5.2. I soggetti pertinenti devono:

a) stabilire, sulla base della valutazione dei rischi effettuata a norma del punto 2.1, la necessità, la portata, la frequenza e il tipo dei test di sicurezza;

b) effettuare test di sicurezza secondo una metodologia di test documentata, che contempli i componenti che in base a un'analisi dei rischi sono stati ritenuti rilevanti per il funzionamento sicuro;

c) documentare il tipo, la portata, il tempo e i risultati dei test, compresa la valutazione della criticità e delle azioni di mitigazione per ciascuna risultanza;

d) applicare azioni di mitigazione in caso di risultanze critiche.

6.5.3. I soggetti pertinenti devono riesaminare e, se opportuno, aggiornare le loro politiche in materia di test di sicurezza a intervalli pianificati.

6.6. *Gestione delle patch di sicurezza*

6.6.1. I soggetti pertinenti devono specificare e applicare procedure, coerenti con le procedure di gestione delle modifiche di cui al punto 6.4.1, nonché con le procedure di gestione delle vulnerabilità e di gestione dei rischi e con le altre pertinenti procedure di gestione, al fine di garantire che:

a) le patch di sicurezza siano applicate entro un termine ragionevole dal momento in cui diventano disponibili;

b) le patch di sicurezza siano sottoposte a test prima di essere applicate nei sistemi di produzione;

c) le patch di sicurezza provengano da fonti affidabili e siano controllate per verificarne l'integrità;

d) siano attuate misure supplementari e siano accettati rischi residui nei casi in cui non sia disponibile o non sia applicata una patch conformemente al punto 6.6.2.

6.6.2. In deroga al punto 6.6.1, lettera a), i soggetti pertinenti possono scegliere di non applicare patch di sicurezza quando gli svantaggi derivanti dalla loro applicazione superano i benefici in termini di cibersicurezza. I soggetti pertinenti devono documentare e motivare debitamente le ragioni di tale decisione.

6.7. *Sicurezza delle reti*

6.7.1. I soggetti pertinenti devono adottare misure adeguate per proteggere i sistemi informativi e di rete dalle minacce informatiche.

6.7.2. Ai fini del punto 6.7.1, i soggetti pertinenti devono:

a) documentare l'architettura della rete in modo comprensibile e aggiornato;

b) determinare e applicare controlli per proteggere i domini di rete interni dei soggetti pertinenti da accessi non autorizzati;

c) configurare i controlli per prevenire gli accessi e le comunicazioni di rete non necessari per il funzionamento dei soggetti pertinenti;

d) stabilire e applicare controlli per l'accesso remoto ai sistemi informativi e di rete, compreso l'accesso da parte dei fornitori di servizi;

e) non utilizzare sistemi impiegati per l'amministrazione dell'attuazione della politica di sicurezza per altre finalità;

f) vietare esplicitamente o disattivare le connessioni e i servizi non necessari;

g) se opportuno, consentire l'accesso ai propri sistemi informativi e di rete esclusivamente mediante dispositivi autorizzati;

h) consentire connessioni dei fornitori di servizi soltanto previa richiesta di autorizzazione e per un periodo di tempo determinato, quale la durata di un'operazione di manutenzione;

i) stabilire una comunicazione tra sistemi distinti soltanto attraverso canali affidabili che sono isolati da altri canali di comunicazione attraverso la separazione logica, crittografica o fisica e garantire l'identificazione dei loro punti finali e la protezione dei dati dei canali dalla modifica o dalla divulgazione;

j) adottare un piano di attuazione per effettuare la transizione completa verso protocolli di comunicazione a livello di rete di ultima generazione in modo sicuro, adeguato e graduale, e stabilire misure volte ad accelerare tale transizione;

k) adottare un piano di attuazione per l'adozione di norme moderne di comunicazione via posta elettronica concordate a livello internazionale e interoperabili al fine di rendere sicure le comunicazioni via posta elettronica in modo da mitigare le vulnerabilità legate alle minacce connesse alla posta elettronica e stabilire misure volte ad accelerare tale adozione;

l) applicare le migliori pratiche per la sicurezza del DNS e per la sicurezza e l'igiene dell'instradamento in internet del traffico proveniente dalla rete e ad essa destinato.

6.7.3. I soggetti pertinenti devono riesaminare e, se opportuno, aggiornare tali misure a intervalli pianificati e qualora si verifichino incidenti significativi o cambiamenti significativi delle operazioni o dei rischi.

6.8. *Segmentazione della rete*

6.8.1. I soggetti pertinenti devono segmentare i sistemi in reti o zone conformemente ai risultati della valutazione dei rischi di cui al punto 2.1. Tali soggetti devono segmentare i loro sistemi e le loro reti dai sistemi e dalle reti di terzi.

6.8.2. A tal fine, i soggetti pertinenti devono:

a) considerare il rapporto funzionale, logico e fisico, compresa l'ubicazione, tra sistemi e servizi affidabili;

b) concedere l'accesso a una rete o a una zona sulla base di una valutazione dei suoi requisiti di sicurezza;

c) conservare in zone sicure i sistemi critici per il funzionamento dei soggetti pertinenti o per la sicurezza;

d) realizzare una zona smilitarizzata all'interno delle loro reti di comunicazione atta a garantire la sicurezza delle comunicazioni provenienti dalle loro reti o a esse destinate;

e) limitare l'accesso e le comunicazioni tra le zone e al loro interno a quanto necessario per il funzionamento dei soggetti pertinenti o per la sicurezza;

f) separare la rete dedicata all'amministrazione dei sistemi informativi e di rete dalla rete operativa dei soggetti pertinenti;

g) separare i canali di amministrazione della rete dal restante traffico di rete;

h) separare i sistemi di produzione per i servizi dei soggetti pertinenti dai sistemi utilizzati per lo sviluppo e i test, compresi i backup.

6.8.3. I soggetti pertinenti devono riesaminare e, se opportuno, aggiornare la segmentazione della rete a intervalli pianificati e qualora si verifichino incidenti significativi o cambiamenti significativi delle operazioni o dei rischi.

6.9. *Protezione da software malevoli e non autorizzati*

6.9.1. I soggetti pertinenti devono proteggere le loro reti e i loro sistemi informativi dai software malevoli e non autorizzati.

6.9.2. A tal fine devono attuare in particolare misure volte a rilevare o prevenire l'utilizzo di software malevoli o non autorizzati. I soggetti pertinenti devono provvedere, se opportuno, affinché i loro sistemi informativi e di rete siano dotati di un software di rilevamento e risposta, aggiornato periodicamente conformemente alla valutazione dei rischi effettuata a norma del punto 2.1 e agli accordi contrattuali con i fornitori.

6.10. *Gestione e divulgazione delle vulnerabilità*

6.10.1. I soggetti pertinenti devono ottenere informazioni sulle vulnerabilità tecniche nei loro sistemi informativi e di rete, valutare la loro esposizione a tali vulnerabilità e adottare misure adeguate per gestirle.

6.10.2. Ai fini del punto 6.10.1, i soggetti pertinenti devono:

a) monitorare le informazioni sulle vulnerabilità attraverso canali adeguati, quali i bollettini dei CSIRT, le autorità competenti o le informazioni messe a disposizione da fornitori o fornitori di servizi;

b) effettuare, se opportuno, scansioni delle vulnerabilità e registrare le prove dei risultati di tali scansioni, a intervalli pianificati;

c) affrontare, senza indebito ritardo, le vulnerabilità identificate come critiche per le loro operazioni;

d) garantire che la gestione delle vulnerabilità sia compatibile con le proprie procedure di gestione delle modifiche, di gestione delle patch di sicurezza, di gestione dei rischi e di gestione degli incidenti;

e) stabilire una procedura per la divulgazione delle vulnerabilità conformemente alla politica nazionale di divulgazione coordinata delle vulnerabilità applicabile.

6.10.3. Laddove giustificato dall'impatto potenziale della vulnerabilità, i soggetti pertinenti devono creare e attuare un piano per mitigarla. In altri casi i soggetti pertinenti devono documentare e motivare la ragione per cui la vulnerabilità non richiede alcun rimedio.

6.10.4. I soggetti pertinenti devono riesaminare e, se opportuno, aggiornare a intervalli pianificati i canali che utilizzano per monitorare le informazioni sulle vulnerabilità.

7. **Strategie e procedure per valutare l'efficacia delle misure di gestione dei rischi di cibersicurezza [articolo 21, paragrafo 2, lettera f), della direttiva (UE) 2022/2555]**

7.1. Ai fini dell'articolo 21, paragrafo 2, lettera f), della direttiva (UE) 2022/2555, i soggetti pertinenti devono stabilire, attuare e applicare una strategia e procedure per valutare se le misure di gestione dei rischi di cibersicurezza da essi adottate siano attuate e mantenute efficacemente.

7.2. La strategia e le procedure di cui al punto 7.1 devono tenere conto dei risultati della valutazione dei rischi di cui al punto 2.1 e di incidenti significativi passati. I soggetti pertinenti devono stabilire:

a) quali misure di gestione dei rischi di cibersicurezza devono essere monitorate e misurate, compresi i processi e i controlli;

b) i metodi di monitoraggio, misurazione, analisi e valutazione, a seconda dei casi, per garantire risultati validi;

c) quando devono essere effettuate le attività di monitoraggio e misurazione;

d) il soggetto competente per il monitoraggio e la misurazione dell'efficacia delle misure di gestione dei rischi di cibersicurezza;

e) quando i risultati del monitoraggio e della misurazione devono essere analizzati e valutati.

f) il soggetto che deve analizzare e valutare tali risultati.

7.3. I soggetti pertinenti devono riesaminare e, se opportuno, aggiornare le strategie e le procedure a intervalli pianificati e qualora si verifichino incidenti significativi o cambiamenti significativi delle operazioni o dei rischi.

8. **Pratiche di igiene informatica di base e formazione in materia di sicurezza [articolo 21, paragrafo 2, lettera g), della direttiva (UE) 2022/2555]**

8.1. *Sensibilizzazione e pratiche di igiene informatica di base*

8.1.1. Ai fini dell'articolo 21, paragrafo 2, lettera g), della direttiva (UE) 2022/2555, i soggetti pertinenti devono provvedere affinché i loro dipendenti, compresi i membri degli organi di gestione, nonché i diretti fornitori e fornitori di servizi, siano consapevoli dei rischi, siano informati in merito all'importanza della cibersicurezza e applichino pratiche di igiene informatica.

8.1.2. Ai fini del punto 8.1.1, i soggetti pertinenti devono offrire ai loro dipendenti, compresi i membri degli organi di gestione, nonché, se opportuno, i diretti fornitori e fornitori di servizi conformemente al punto 5.1.4, un programma di sensibilizzazione che deve:

a) essere programmato nel corso del tempo, in modo tale che le attività siano ripetute e coinvolgano i nuovi dipendenti;

b) essere istituito in linea con la politica di sicurezza dei sistemi informativi e di rete, le politiche specifiche per tematica e le procedure pertinenti in materia di sicurezza dei sistemi informativi e di rete;

c) trattare le minacce informatiche pertinenti, le misure di gestione dei rischi di cibersicurezza in vigore, i punti di contatto e le risorse per informazioni supplementari e consulenze su questioni relative alla cibersicurezza, nonché le pratiche di igiene informatica per gli utenti.

8.1.3. Se opportuno, il programma di sensibilizzazione deve essere sottoposto a test per valutarne l'efficacia. Il programma di sensibilizzazione deve essere aggiornato e offerto a intervalli pianificati, tenendo conto dei cambiamenti nelle pratiche di igiene informatica e del panorama corrente delle minacce, nonché dei rischi per i soggetti pertinenti.

8.2. *Formazione in materia di sicurezza*

8.2.1. I soggetti pertinenti devono individuare i dipendenti i cui ruoli richiedono una serie di capacità e competenze rilevanti per la sicurezza e provvedere affinché ricevano una formazione periodica in materia di sicurezza dei sistemi informativi e di rete.

8.2.2. I soggetti pertinenti devono stabilire, attuare e applicare un programma di formazione in linea con la politica di sicurezza dei sistemi informativi e di rete, le politiche specifiche per tematica e altre procedure pertinenti in materia di sicurezza dei sistemi informativi e di rete, che stabilisca le esigenze di formazione per ruoli e posizioni specifici sulla base di criteri.

8.2.3. La formazione di cui al punto 8.2.1 deve essere pertinente alla funzione professionale del dipendente e deve esserne valutata l'efficacia. La formazione deve tenere conto delle misure di sicurezza in vigore e comprendere gli elementi seguenti:

a) istruzioni relative alla configurazione e al funzionamento sicuri dei sistemi informativi e di rete, compresi i dispositivi mobili;

b) informazioni sulle minacce informatiche note;

c) formazione sul comportamento da tenere in caso di eventi rilevanti per la sicurezza.

8.2.4. I soggetti pertinenti devono erogare formazione ai membri del personale che assumono posizioni o ruoli nuovi che richiedono una serie di capacità e competenze rilevanti per la sicurezza.

8.2.5. Il programma deve essere aggiornato e attuato periodicamente tenendo conto delle politiche e delle norme applicabili, dei ruoli assegnati e delle responsabilità, nonché delle minacce informatiche note e degli sviluppi tecnologici.

9. **Crittografia [articolo 21, paragrafo 2, lettera h), della direttiva (UE) 2022/2555]**

9.1. Ai fini dell'articolo 21, paragrafo 2, lettera h), della direttiva (UE) 2022/2555, i soggetti pertinenti devono stabilire, attuare e applicare una politica e procedure relative alla crittografia, al fine di garantire un uso adeguato ed efficace della crittografia stessa per proteggere la riservatezza, l'autenticità e l'integrità dei dati in linea con la classificazione delle risorse dei soggetti pertinenti e con i risultati della valutazione dei rischi effettuata a norma del punto 2.1.

9.2. La politica e le procedure di cui al punto 9.1 devono stabilire:

a) conformemente alla classificazione delle risorse dei soggetti pertinenti, il tipo, la robustezza e la qualità delle misure crittografiche necessarie per proteggere le risorse dei soggetti pertinenti, compresi i dati a riposo e i dati in transito;

b) sulla base della lettera a), i protocolli o le famiglie di protocolli da adottare, nonché gli algoritmi crittografici, la robustezza dell'algoritmo di crittografia, le soluzioni crittografiche e le pratiche d'uso da approvare e il cui uso deve essere richiesto in seno ai soggetti pertinenti, seguendo, se opportuno, un approccio di agilità crittografica;

c) l'approccio dei soggetti pertinenti alla gestione delle chiavi, compresi, se opportuno, i metodi relativi agli aspetti seguenti:

i) generazione di chiavi diverse per sistemi e applicazioni crittografici;

ii) rilascio e ottenimento di certificati a chiave pubblica;

iii) distribuzione di chiavi ai soggetti previsti, comprese le modalità di attivazione delle chiavi al loro ricevimento;

iv) conservazione delle chiavi, compresa la modalità con cui gli utenti autorizzati ottengono accesso alle chiavi stesse;

v) modifica o aggiornamento delle chiavi, comprese le norme relative alle tempistiche e alle modalità di modifica delle chiavi;

vi) gestione di chiavi compromesse;

vii) revoca di chiavi, comprese le modalità per ritirare o disattivare le chiavi;

viii) recupero di chiavi perse o corrotte;

ix) attività di backup o archiviazione di chiavi;

x) distruzione di chiavi;

xi) registrazione e audit delle attività connesse alla gestione delle chiavi;

xii) definizione delle date di attivazione e disattivazione delle chiavi al fine di garantire che possano essere utilizzate soltanto per il periodo di tempo specificato conformemente alle norme dell'organizzazione in materia di gestione delle chiavi.

9.3. I soggetti pertinenti devono riesaminare e, se opportuno, aggiornare le loro politiche e procedure a intervalli pianificati, tenendo conto dello stato dell'arte in materia di crittografia.

10. **Sicurezza delle risorse umane [articolo 21, paragrafo 2, lettera i), della direttiva (UE) 2022/2555]**

10.1. *Sicurezza delle risorse umane*

10.1.1. Ai fini dell'articolo 21, paragrafo 2, lettera i), della direttiva (UE) 2022/2555, i soggetti pertinenti devono provvedere affinché i loro dipendenti e i loro diretti fornitori e fornitori di servizi, ove applicabile, comprendano e si impegnino a rispettare le loro responsabilità in materia di sicurezza, in funzione dei servizi offerti e del posto di lavoro assegnato nonché in linea con la politica di sicurezza dei sistemi informativi e di rete dei soggetti pertinenti.

10.1.2. Il requisito di cui al punto 10.1.1 deve comprendere gli aspetti seguenti:

a) meccanismi volti a garantire che tutti i dipendenti, i diretti fornitori e fornitori di servizi, ove applicabile, comprendano e rispettino le pratiche standard di igiene informatica applicate dai soggetti pertinenti a norma del punto 8.1;

b) meccanismi volti a garantire che tutti gli utenti con accesso amministrativo o privilegiato siano consapevoli dei loro ruoli, delle loro responsabilità e delle loro autorità e agiscano in maniera corrispondente;

c) meccanismi volti a garantire che i membri degli organi di gestione comprendano il loro ruolo, le loro responsabilità e le loro autorità in materia di sicurezza dei sistemi informativi e di rete e agiscano in maniera corrispondente;

d) meccanismi per l'assunzione di personale qualificato per i rispettivi ruoli, quali verifiche delle referenze, procedure di controllo, convalida di certificazioni o prove scritte.

10.1.3. I soggetti pertinenti devono riesaminare l'assegnazione del personale ai ruoli specifici conformemente al punto 1.2, nonché il loro impegno in termini di risorse umane a tale riguardo, a intervalli pianificati e quanto meno una volta l'anno. Se necessario tali soggetti devono aggiornare l'incarico.

10.2. *Verifica dei precedenti personali*

10.2.1. I soggetti pertinenti devono provvedere nei limiti del possibile affinché sia effettuata una verifica dei precedenti personali dei loro dipendenti e, se applicabile, dei diretti fornitori e fornitori di servizi conformemente al punto 5.1.4, se necessario per il loro ruolo, le loro responsabilità e le loro autorizzazioni.

10.2.2. Ai fini del punto 10.2.1, i soggetti pertinenti devono:

a) mettere in atto criteri che definiscano i ruoli, le responsabilità e le autorità che devono essere esercitati soltanto da persone i cui precedenti personali sono stati verificati;

b) garantire che la verifica di cui al punto 10.2.1 sia effettuata prima che le persone inizino a esercitare tali ruoli, responsabilità e autorità, tenendo conto delle leggi, delle normative e dei codici etici applicabili in relazione ai requisiti operativi, alla classificazione delle risorse di cui al punto 12.1 e ai sistemi informativi e di rete a cui sarà concesso l'accesso, nonché ai rischi percepiti.

10.2.3. I soggetti pertinenti devono riesaminare e, se opportuno, aggiornare la politica a intervalli pianificati e aggiornarla ove necessario.

10.3. *Procedure in caso di cessazione o modifica del rapporto di lavoro*

10.3.1. I soggetti pertinenti devono provvedere affinché le responsabilità e le funzioni in materia di sicurezza dei sistemi informativi e di rete che rimangono valide dopo la cessazione o la modifica del rapporto di lavoro dei loro dipendenti siano definite a livello contrattuale e applicate.

10.3.2. Ai fini del punto 10.3.1, i soggetti pertinenti devono includere nei termini e nelle condizioni di lavoro, nel contratto o nell'accordo della persona in questione le responsabilità e le funzioni che continuano a essere valide in seguito alla cessazione del rapporto di lavoro o alla risoluzione del contratto, ad esempio le clausole in materia di riservatezza.

10.4. *Processo disciplinare*

10.4.1. I soggetti pertinenti devono istituire, comunicare e mantenere un processo disciplinare per la gestione delle violazioni delle politiche di sicurezza delle reti e dei sistemi informativi. Tale processo deve tenere conto dei pertinenti requisiti giuridici, statutari, contrattuali e operativi.

10.4.2. I soggetti pertinenti devono riesaminare e, se opportuno, aggiornare il processo disciplinare a intervalli pianificati e qualora necessario in ragione di cambiamenti giuridici o cambiamenti significativi delle operazioni o dei rischi.

11. **Controllo dell'accesso [articolo 21, paragrafo 2, lettere i) e j), della direttiva (UE) 2022/2555]**

11.1. *Strategia di controllo dell'accesso*

11.1.1. Ai fini dell'articolo 21, paragrafo 2, lettera i), della direttiva (UE) 2022/2555, i soggetti pertinenti devono stabilire, documentare e attuare strategie di controllo dell'accesso logico e fisico per l'accesso ai loro sistemi informativi e di rete, sulla base dei requisiti operativi e dei requisiti di sicurezza dei sistemi informativi e di rete.

11.1.2. Le strategie di cui al punto 11.1.1 devono:

a) comprendere l'accesso da parte di persone, compresi il personale, i visitatori e i soggetti esterni quali i fornitori e i fornitori di servizi;

b) comprendere l'accesso da parte di sistemi informativi e di rete;

c) garantire che l'accesso sia consentito esclusivamente agli utenti adeguatamente autenticati.

11.1.3. I soggetti pertinenti devono riesaminare e, se opportuno, aggiornare tali strategie a intervalli pianificati e qualora si verifichino incidenti significativi o cambiamenti significativi delle operazioni o dei rischi.

11.2. *Gestione dei diritti di accesso*

11.2.1. I soggetti pertinenti devono fornire, modificare, rimuovere e documentare i diritti di accesso ai sistemi informativi e di rete conformemente alla strategia di controllo dell'accesso di cui al punto 11.1.

11.2.2. I soggetti pertinenti devono:

a) assegnare e revocare i diritti di accesso sulla base dei principi della necessità di sapere, del privilegio minimo e della separazione delle funzioni;

b) garantire che i diritti di accesso siano modificati di conseguenza in caso di cessazione o cambiamento del rapporto di lavoro;

c) garantire che l'accesso ai sistemi informativi e di rete sia autorizzato dalle persone pertinenti;

d) garantire che i diritti di accesso comprendano in maniera adeguata l'accesso da parte di terzi, quali visitatori, fornitori e fornitori di servizi, in particolare limitando i diritti di accesso in termini di portata e durata;

e) tenere un registro dei diritti di accesso concessi;

f) applicare la registrazione alla gestione dei diritti di accesso.

11.2.3. I soggetti pertinenti devono riesaminare i diritti di accesso a intervalli pianificati e devono modificarli sulla base di cambiamenti organizzativi. I soggetti pertinenti devono documentare i risultati di tale riesame, comprese le necessarie modifiche dei diritti di accesso.

11.3. *Account privilegiati e account di amministrazione dei sistemi*

11.3.1. I soggetti pertinenti devono mantenere politiche di gestione di account privilegiati e account di amministrazione dei sistemi nell'ambito della strategia di controllo dell'accesso di cui al punto 11.1.

11.3.2. Le politiche di cui al punto 11.3.1 devono:

a) stabilire procedure rigorose di identificazione, di autenticazione, quali l'autenticazione a più fattori, e di autorizzazione per gli account privilegiati e gli account di amministrazione dei sistemi;

b) creare account specifici da utilizzare esclusivamente per le operazioni di amministrazione dei sistemi, quali attività di installazione, configurazione, gestione o manutenzione;

c) individualizzare e limitare il più possibile i privilegi di amministrazione dei sistemi;

d) prevedere che gli account di amministrazione dei sistemi siano utilizzati esclusivamente per connettersi ai sistemi di amministrazione del sistema.

11.3.3. I soggetti pertinenti devono riesaminare i diritti di accesso degli account privilegiati e degli account di amministrazione dei sistemi a intervalli pianificati, devono modificarli sulla base di cambiamenti organizzativi e devono documentare i risultati del riesame, comprese le modifiche necessarie dei diritti di accesso.

11.4. *Sistemi di amministrazione*

11.4.1. I soggetti pertinenti devono limitare e controllare l'uso dei sistemi di amministrazione del sistema conformemente alla strategia di controllo dell'accesso di cui al punto 11.1.

11.4.2. A tal fine, i soggetti pertinenti devono:

a) utilizzare i sistemi di amministrazione del sistema esclusivamente per fini di amministrazione del sistema e non per altre operazioni;

b) separare logicamente tali sistemi dai software applicativi non utilizzati per fini di amministrazione del sistema;

c) proteggere l'accesso ai sistemi di amministrazione del sistema attraverso l'autenticazione e la crittografia.

11.5. *Identificazione*

11.5.1. I soggetti pertinenti devono gestire l'intero ciclo di vita delle identità dei sistemi informativi e di rete e dei loro utenti.

11.5.2. A tal fine, i soggetti pertinenti devono:

a) creare identità uniche per i sistemi informativi e di rete e i loro utenti;

b) collegare l'identità degli utenti a una singola persona;

c) garantire la sorveglianza delle identità dei sistemi informativi e di rete;

d) applicare la registrazione alla gestione delle identità.

11.5.3. I soggetti pertinenti devono consentire l'esistenza di identità assegnate a più persone, quali le identità condivise, soltanto laddove ciò sia necessario per motivi aziendali od operativi e sia soggetto a un processo di approvazione esplicita e a documentazione. I soggetti pertinenti devono tenere conto delle identità assegnate a più persone nel quadro di gestione dei rischi di cibersicurezza di cui al punto 2.1.

11.5.4. I soggetti pertinenti devono riesaminare periodicamente le identità dei sistemi informativi e di rete e dei loro utenti e, se non sono più necessarie, le devono disattivare senza indugio.

11.6. *Autenticazione*

11.6.1. I soggetti pertinenti devono implementare procedure e tecnologie di autenticazione sicura basate su restrizioni dell'accesso e sulla strategia di controllo dell'accesso.

11.6.2. A tal fine, i soggetti pertinenti devono:

a) garantire che la forza dell'autenticazione sia adeguata alla classificazione della risorsa a cui si accede;

b) controllare l'assegnazione agli utenti e la gestione delle informazioni segrete di autenticazione mediante un processo che garantisca la riservatezza delle informazioni, compresa la consulenza al personale in merito alla gestione adeguata delle informazioni di autenticazione;

c) richiedere la modifica delle credenziali di autenticazione all'inizio, a intervalli predefiniti e qualora si sospetti che le credenziali siano state compromesse;

d) imporre una reimpostazione delle credenziali di autenticazione e il blocco degli utenti dopo un numero predefinito di tentativi di accesso non riusciti;

e) terminare le sessioni inattive dopo un periodo predefinito di inattività; e

f) richiedere credenziali separate per gli accessi privilegiati o l'accesso ad account di amministrazione.

11.6.3. I soggetti pertinenti devono, nella misura del possibile, utilizzare metodi di autenticazione all'avanguardia, in funzione del rischio associato valutato e della classificazione della risorsa a cui si accede, nonché informazioni di autenticazione uniche.

11.6.4. I soggetti pertinenti devono riesaminare le procedure e le tecnologie di autenticazione a intervalli pianificati.

11.7. *Autenticazione a più fattori*

11.7.1. I soggetti pertinenti devono provvedere affinché gli utenti siano autenticati tramite molteplici fattori di autenticazione o meccanismi di autenticazione continua al fine di accedere ai sistemi informativi e di rete dei soggetti pertinenti, se opportuno, in funzione della classificazione della risorsa oggetto dell'accesso.

11.7.2. I soggetti pertinenti devono garantire che la forza dell'autenticazione sia adeguata alla classificazione della risorsa oggetto dell'accesso.

12. **Gestione delle risorse [articolo 21, paragrafo 2, lettera i), della direttiva (UE) 2022/2555]**

12.1. *Classificazione delle risorse*

12.1.1. Ai fini dell'articolo 21, paragrafo 2, lettera i), della direttiva (UE) 2022/2555, i soggetti pertinenti devono stabilire i livelli di classificazione di tutte le risorse, comprese le informazioni, rientranti nell'ambito dei loro sistemi informativi e di rete per il livello di protezione richiesto.

12.1.2. Ai fini del punto 12.1.1, i soggetti pertinenti devono:

a) stabilire un sistema di livelli di classificazione per le risorse;

b) associare tutte le risorse a un livello di classificazione, in base a requisiti di riservatezza, integrità, autenticità e disponibilità, al fine di indicare la protezione richiesta in base alla sensibilità, alla criticità, al rischio e al valore commerciale di tali risorse;

c) allineare i requisiti di disponibilità delle risorse agli obiettivi di consegna e ripristino stabiliti nei loro piani di continuità operativa e di ripristino in caso di disastro.

12.1.3. I soggetti pertinenti devono effettuare riesami periodici dei livelli di classificazione delle risorse e aggiornarli, se opportuno.

12.2. *Gestione delle risorse*

12.2.1. I soggetti pertinenti devono stabilire, attuare e applicare una politica per la gestione corretta delle risorse, comprese le informazioni, conformemente alla loro politica di sicurezza dei sistemi informativi e di rete e comunicare la politica per la gestione corretta delle risorse a chiunque utilizzi o gestisca risorse.

12.2.2. Tale politica deve:

a) comprendere l'intero ciclo di vita delle risorse, compresi l'acquisizione, l'uso, la conservazione, il trasporto e lo smaltimento;

b) fornire regole in merito all'uso sicuro, alla conservazione sicura, al trasporto sicuro e alla cancellazione e distruzione irreversibili delle risorse;

c) prevedere che il trasferimento abbia luogo in modo sicuro, in funzione del tipo di risorsa che deve essere trasferita.

12.2.3. I soggetti pertinenti devono riesaminare e, se opportuno, aggiornare tale politica a intervalli pianificati e qualora si verifichino incidenti significativi o cambiamenti significativi delle operazioni o dei rischi.

12.3. *Politica in materia di supporti rimovibili*

12.3.1. I soggetti pertinenti devono stabilire, attuare e applicare una politica in materia di gestione dei supporti di memorizzazione rimovibili e la devono comunicare ai propri dipendenti e ai terzi che gestiscono supporti di memorizzazione rimovibili nei locali dei soggetti pertinenti o in altri luoghi in cui tali supporti rimovibili sono collegati ai sistemi informativi e di rete dei soggetti pertinenti.

12.3.2. Tale politica deve:

a) prevedere un divieto tecnico di collegamento di supporti rimovibili a meno che non vi sia un motivo organizzativo per il loro utilizzo;

b) prevedere la disabilitazione dell'autoesecuzione a partire da tali supporti e la loro scansione al fine di rilevare codici malevoli prima che siano utilizzati nei sistemi dei soggetti pertinenti;

c) prevedere misure volte a controllare e proteggere i dispositivi di memorizzazione portatili contenenti dati durante il transito e l'immagazzinaggio;

d) se opportuno, prevedere misure per l'uso di tecniche crittografiche per proteggere i dati presenti su supporti di memorizzazione rimovibili.

12.3.3. I soggetti pertinenti devono riesaminare e, se opportuno, aggiornare tale politica a intervalli pianificati e qualora si verifichino incidenti significativi o cambiamenti significativi delle operazioni o dei rischi.

12.4. *Inventario delle risorse*

12.4.1. I soggetti pertinenti devono realizzare e mantenere un inventario completo, accurato, aggiornato e coerente delle loro risorse. Essi devono registrare le modifiche delle voci dell'inventario in modo tracciabile.

12.4.2. La granularità dell'inventario delle risorse deve essere adeguata alle esigenze dei soggetti pertinenti. L'inventario deve comprendere gli elementi seguenti:

a) l'elenco delle operazioni e dei servizi e la loro descrizione;

b) l'elenco dei sistemi informativi e di rete e delle altre risorse associate a sostegno delle operazioni e dei servizi dei soggetti pertinenti.

12.4.3. I soggetti pertinenti devono riesaminare e aggiornare periodicamente l'inventario e le loro risorse e documentare la cronologia delle modifiche.

12.5. *Deposito, restituzione o cancellazione delle risorse al momento della cessazione del rapporto di lavoro*

I soggetti pertinenti devono stabilire, attuare e applicare procedure atte a garantire che le loro risorse poste sotto custodia del personale siano depositate, restituite o cancellate al momento della cessazione del rapporto di lavoro e devono documentare il deposito, la restituzione e la cancellazione di tali risorse. Qualora il deposito, la restituzione o la cancellazione delle risorse non sia possibile, i soggetti pertinenti devono provvedere affinché le risorse non possano più accedere ai sistemi informativi e di rete dei soggetti pertinenti conformemente al punto 12.2.2.

13. **Sicurezza ambientale e fisica [articolo 21, paragrafo 2, lettere c), e) ed i), della direttiva (UE) 2022/2555]**

13.1. *Servizi pubblici di sostegno*

13.1.1. Ai fini dell'articolo 21, paragrafo 2, lettera c), della direttiva (UE) 2022/2555, i soggetti pertinenti devono prevenire la perdita, il danneggiamento o la compromissione dei sistemi informativi e di rete o l'interruzione delle loro operazioni a causa di guasti e perturbazioni dei servizi pubblici di supporto.

13.1.2. A tal fine, se opportuno, i soggetti pertinenti devono:

a) proteggere gli impianti da interruzioni di corrente e altre perturbazioni causate da guasti di servizi pubblici di sostegno quali la fornitura di energia elettrica, telecomunicazioni, approvvigionamento idrico e gas, il trattamento di acque reflue, la ventilazione e il condizionamento dell'aria;

b) prendere in considerazione il ricorso alla ridondanza per i servizi pubblici;

c) proteggere i servizi pubblici per l'energia elettrica e le telecomunicazioni, che trasportano dati o forniscono sistemi informativi e di rete, da intercettazioni e danni;

d) monitorare i servizi pubblici di cui alla lettera c) e riferire al personale interno o esterno competente eventi che esulano dalle soglie di controllo minime e massime di cui al punto 13.2.2, lettera b), che incidono sui servizi pubblici;

e) concludere contratti per la fornitura di emergenza con i servizi corrispondenti, ad esempio per il combustibile per la fornitura di energia elettrica di emergenza;

f) monitorare, mantenere e sottoporre a test la fornitura dei sistemi informativi e di rete necessari per il funzionamento del servizio offerto, in particolare l'energia elettrica, il controllo della temperatura e dell'umidità, le telecomunicazioni e la connessione a internet, e garantirne l'efficacia continua.

13.1.3. I soggetti pertinenti devono sottoporre a test, riesaminare e, se opportuno, aggiornare le misure di protezione periodicamente o a seguito di incidenti significativi o cambiamenti significativi delle operazioni o dei rischi.

13.2. *Protezione da minacce fisiche e ambientali*

13.2.1. Ai fini dell'articolo 21, paragrafo 2, lettera e), della direttiva (UE) 2022/2555, i soggetti pertinenti devono prevenire o ridurre le conseguenze di eventi derivanti da minacce fisiche e ambientali, quali catastrofi naturali e altre minacce intenzionali o non intenzionali, sulla base dei risultati della valutazione dei rischi effettuata a norma del punto 2.1.

13.2.2. A tal fine, se opportuno, i soggetti pertinenti devono:

a) progettare e attuare misure di protezione da minacce fisiche e ambientali;

b) determinare soglie minime e massime di controllo per le minacce fisiche e ambientali;

c) monitorare i parametri ambientali e riferire al personale interno o esterno competente gli eventi che esulano dalle soglie di controllo minime e massime di cui alla lettera b).

13.2.3. I soggetti pertinenti devono sottoporre a test, riesaminare e, se opportuno, aggiornare le misure di protezione da minacce fisiche e ambientali periodicamente o a seguito di incidenti significativi o cambiamenti significativi delle operazioni o dei rischi.

13.3. *Controllo dell'accesso perimetrale e fisico*

13.3.1. Ai fini dell'articolo 21, paragrafo 2, lettera i), della direttiva (UE) 2022/2555, i soggetti pertinenti devono prevenire e monitorare l'accesso fisico non autorizzato, i danni e le interferenze concernenti i loro sistemi informativi e di rete.

13.3.2. A tal fine, i soggetti pertinenti devono:

a) sulla base della valutazione dei rischi effettuata a norma del punto 2.1, stabilire e utilizzare perimetri di sicurezza per proteggere le zone in cui sono ubicati i sistemi informativi e di rete e le altre risorse associate;

b) proteggere le zone di cui alla lettera a) mediante adeguati controlli all'ingresso e punti di accesso;

c) progettare e implementare la sicurezza fisica degli uffici, delle sale e degli impianti;

d) monitorare costantemente i propri locali al fine rilevare eventuali accessi fisici non autorizzati.

13.3.3. I soggetti pertinenti devono sottoporre a test, riesaminare e, se opportuno, aggiornare le misure di controllo dell'accesso fisico periodicamente o a seguito di incidenti significativi o cambiamenti significativi delle operazioni o dei rischi.