2024/1774

25.6.2024

REGOLAMENTO DELEGATO (UE) 2024/1774 DELLA COMMISSIONE

del 13 marzo 2024

che integra il regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione che specificano gli strumenti, i metodi, i processi e le politiche per la gestione dei rischi informatici e il quadro semplificato per la gestione dei rischi informatici

(Testo rilevante ai fini del SEE)

LA COMMISSIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea,

visto il regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n. 909/2014 e (UE) 2016/1011 ([1]), in particolare l'articolo 15, quarto comma, e l'articolo 16, paragrafo 3, quarto comma,

considerando quanto segue:

(1) Il regolamento (UE) 2022/2554 si applica a un'ampia varietà di entità finanziarie che differiscono per dimensioni, struttura, organizzazione interna, natura e complessità delle loro attività e che quindi presentano maggiori o minori elementi di complessità o di rischio. Per garantire che tale varietà sia tenuta in debita considerazione, qualsiasi prescrizione relativa a politiche, procedure, protocolli e strumenti per la sicurezza delle TIC e a un quadro semplificato per la gestione dei rischi informatici dovrebbe essere proporzionata alle dimensioni, alla struttura, all'organizzazione interna, alla natura e alla complessità di tali entità finanziarie e ai rischi corrispondenti.

(2) Per lo stesso motivo, le entità finanziarie soggette al regolamento (UE) 2022/2554 dovrebbero avere una certa flessibilità nel modo in cui si conformano agli obblighi relativi alle politiche, alle procedure, ai protocolli e agli strumenti per la sicurezza delle TIC e a un eventuale quadro semplificato per la gestione dei rischi informatici. Per questo motivo, le entità finanziarie dovrebbero essere autorizzate a utilizzare la documentazione già in loro possesso per ottemperare agli obblighi di documentazione che ne derivano. Ne consegue che l'elaborazione, la documentazione e l'attuazione di specifiche politiche per la sicurezza delle TIC dovrebbero essere richieste solo per alcuni elementi essenziali, tenendo conto, tra l'altro, delle pratiche e delle norme del settore più avanzate. Inoltre, per tenere conto degli aspetti specifici dell'attuazione tecnica, è necessario elaborare, documentare e attuare procedure per la sicurezza delle TIC che coprano gli aspetti specifici dell'attuazione tecnica, tra cui la gestione della capacità e delle prestazioni, la gestione delle vulnerabilità e delle patch, la sicurezza dei dati e dei sistemi e il logging.

(3) Per garantire la corretta attuazione nel tempo delle politiche, delle procedure, dei protocolli e degli strumenti per la sicurezza delle TIC di cui al titolo II, capo I, del presente regolamento, è importante che le entità finanziarie assegnino e mantengano correttamente tutti i ruoli e le responsabilità relativi alla sicurezza delle TIC e che stabiliscano le conseguenze della mancata osservanza delle politiche o delle procedure per la sicurezza delle TIC.

(4) Per limitare il rischio di conflitti di interessi, le entità finanziarie dovrebbero garantire la separazione dei compiti nell'assegnazione dei ruoli e delle responsabilità in materia di TIC.

(5) Per garantire la flessibilità e semplificare il quadro di controllo delle entità finanziarie, queste ultime non dovrebbero essere tenute a elaborare disposizioni specifiche sulle conseguenze della mancata osservanza delle politiche, delle procedure e dei protocolli per la sicurezza delle TIC di cui al titolo II, capo I, del presente regolamento, qualora tali disposizioni siano già contenute in un'altra politica o procedura.

([1]) GU L 333 del 27.12.2022, pag. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj.

(6) In un ambiente dinamico in cui i rischi informatici evolvono costantemente, è importante che le entità finanziarie elaborino le loro politiche di sicurezza delle TIC sulla base delle pratiche più avanzate e, se del caso, delle norme definite all'articolo 2, punto 1), del regolamento (UE) n. 1025/2012 del Parlamento europeo e del Consiglio ([2]). Ciò dovrebbe consentire alle entità finanziarie di cui al titolo II del presente regolamento di rimanere informate e preparate in un panorama in continua evoluzione.

(7) Per garantire la propria resilienza operativa digitale, le entità finanziarie di cui al titolo II del presente regolamento dovrebbero, nell'ambito delle politiche, delle procedure, dei protocolli e degli strumenti per la sicurezza delle TIC, elaborare e attuare una politica di gestione delle risorse TIC, procedure di gestione della capacità e delle prestazioni e politiche e procedure per le operazioni riguardanti le TIC. Tali politiche e procedure sono necessarie per garantire il monitoraggio dello stato delle risorse TIC durante il loro ciclo di vita, in modo da utilizzarle e mantenerle in modo efficace (gestione delle risorse TIC). Tali politiche e procedure dovrebbero inoltre garantire l'ottimizzazione del funzionamento dei sistemi di TIC e che le prestazioni dei sistemi e della capacità di TIC soddisfino gli obiettivi aziendali e di sicurezza delle informazioni stabiliti (gestione della capacità e delle prestazioni). Infine, tali politiche e procedure dovrebbero garantire una gestione e un funzionamento quotidiani efficaci e regolari dei sistemi di TIC (operazioni riguardanti le TIC), riducendo al minimo il rischio di perdita di riservatezza, integrità e disponibilità dei dati. Tali politiche e procedure sono quindi necessarie per garantire la sicurezza delle reti, per fornire adeguate salvaguardie contro le intrusioni e l'uso improprio dei dati e per preservare la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati.

(8) Al fine di garantire una corretta gestione del rischio dei sistemi legacy, le entità finanziarie dovrebbero registrare e monitorare le date di fine dei servizi di assistenza informatica forniti da terzi. A causa dell'impatto potenziale che può avere una perdita di riservatezza, integrità e disponibilità dei dati, nel registrare e monitorare tali date di fine le entità finanziarie dovrebbero concentrarsi sulle risorse o sui sistemi di TIC che sono essenziali per le operazioni aziendali.

(9) I controlli crittografici possono garantire la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati. Le entità finanziarie di cui al titolo II del presente regolamento dovrebbero quindi individuare e attuare tali controlli sulla base di un approccio basato sul rischio. A tal fine, le entità finanziarie dovrebbero cifrare i dati in questione a riposo, in transito o, se necessario, in uso, sulla base dei risultati di un duplice processo, ossia la classificazione dei dati e una valutazione completa dei rischi informatici. Data la complessità del processo di cifratura dei dati in uso, le entità finanziarie di cui al titolo II del presente regolamento dovrebbero cifrare i dati in uso solo se ciò è appropriato alla luce dei risultati della valutazione dei rischi informatici. Le entità finanziarie di cui al titolo II del presente regolamento dovrebbero tuttavia essere in grado, qualora la cifratura dei dati in uso non sia fattibile o sia troppo complessa, di proteggere la riservatezza, l'integrità e la disponibilità dei dati in questione attraverso altre misure di sicurezza delle TIC. Dati i rapidi sviluppi tecnologici nel campo delle tecniche crittografiche, le entità finanziarie di cui al titolo II del presente regolamento dovrebbero tenersi aggiornate sugli sviluppi della crittoanalisi che le riguardano e tenere conto delle pratiche e delle norme più avanzate. Le entità finanziarie di cui al titolo II del presente regolamento dovrebbero quindi seguire un approccio flessibile, basato sull'attenuazione e sul monitoraggio dei rischi, per affrontare il panorama dinamico delle minacce crittografiche, comprese quelle derivanti dai progressi in ambito quantistico.

(10) La sicurezza delle operazioni riguardanti le TIC e le politiche, le procedure, i protocolli e gli strumenti operativi sono essenziali per garantire la riservatezza, l'integrità e la disponibilità dei dati. Un aspetto fondamentale è la rigorosa separazione degli ambienti di produzione delle TIC dagli ambienti in cui i sistemi di TIC sono sviluppati e testati o da altri ambienti non di produzione. Tale separazione dovrebbe servire come importante misura di sicurezza delle TIC contro l'accesso non intenzionale e non autorizzato, le modifiche e le cancellazioni dei dati nell'ambiente di produzione, che potrebbero causare gravi perturbazioni delle operazioni commerciali delle entità finanziarie di cui al titolo II del presente regolamento. Tuttavia, considerando le attuali pratiche di sviluppo dei sistemi di TIC, in circostanze eccezionali le entità finanziarie dovrebbero essere autorizzate a effettuare test in ambienti di produzione, a condizione di giustificare tali test e di ottenere l'approvazione richiesta.

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

(11) Data la rapida evoluzione del panorama delle TIC, delle vulnerabilità delle TIC e delle minacce informatiche, è necessario un approccio proattivo e completo per identificare, valutare e affrontare le vulnerabilità delle TIC. Senza questo approccio, le entità finanziarie, i loro clienti, utenti o controparti potrebbero essere gravemente esposti a rischi che ne metterebbero a repentaglio la resilienza operativa digitale, la sicurezza delle reti e la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati che le politiche e le procedure per la sicurezza delle TIC dovrebbero proteggere. Le entità finanziarie di cui al titolo II del presente regolamento dovrebbero quindi identificare e correggere le vulnerabilità del loro ambiente TIC e sia le entità finanziarie che i loro fornitori terzi di servizi TIC dovrebbero aderire a un quadro di gestione delle vulnerabilità coerente, trasparente e responsabile. Per lo stesso motivo, le entità finanziarie dovrebbero monitorare le vulnerabilità delle TIC utilizzando risorse affidabili e strumenti automatizzati, verificando che i fornitori terzi di servizi TIC assicurino un'azione tempestiva sulle vulnerabilità dei servizi TIC prestati.

(12) La gestione delle patch dovrebbe costituire una parte fondamentale delle politiche e delle procedure per la sicurezza delle TIC che, attraverso i test e l'implementazione in un ambiente controllato, mirano a risolvere le vulnerabilità identificate e a prevenire le perturbazioni dovute all'installazione delle patch.

(13) Per garantire una comunicazione tempestiva e trasparente delle potenziali minacce alla sicurezza che potrebbero avere un impatto sull'entità finanziaria e sui suoi portatori di interessi, le entità finanziarie dovrebbero definire procedure per una comunicazione responsabile delle vulnerabilità delle TIC ai clienti, alle controparti e al pubblico. Nel definire tali procedure, le entità finanziarie dovrebbero considerare alcuni fattori, tra cui la gravità della vulnerabilità, l'impatto potenziale di tale vulnerabilità sui portatori di interessi e la disponibilità di una correzione o di misure di attenuazione.

(14) Per consentire l'assegnazione dei diritti di accesso utente, le entità finanziarie di cui al titolo II del presente regolamento dovrebbero adottare misure rigorose per accertare l'identificazione univoca delle persone e dei sistemi che accederanno alle informazioni dell'entità finanziaria. In caso contrario, le entità finanziarie sarebbero esposte a potenziali accessi non autorizzati, violazioni dei dati e attività fraudolente, compromettendo così la riservatezza, l'integrità e la disponibilità dei dati finanziari sensibili. Sebbene l'uso di account generici o condivisi dovrebbe essere eccezionalmente consentito in circostanze specificate dalle entità finanziarie, queste ultime dovrebbero garantire il mantenimento della responsabilità per le azioni intraprese attraverso tali account. In assenza di tale salvaguardia, i potenziali utenti malintenzionati potrebbero ostacolare le misure investigative e correttive, esponendo le entità finanziarie ad attività malevole non individuate o a sanzioni per mancata conformità.

(15) Per gestire il rapido progresso degli ambienti TIC, le entità finanziarie di cui al titolo II del presente regolamento dovrebbero attuare solide politiche e procedure di gestione dei progetti relativi alle TIC al fine di mantenere la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati. Tali politiche e procedure di gestione dei progetti relativi alle TIC dovrebbero identificare gli elementi necessari per gestire efficacemente tali progetti, comprese le modifiche, le acquisizioni, la manutenzione e gli sviluppi dei sistemi di TIC dell'entità finanziaria, indipendentemente dalla metodologia di gestione dei progetti relativi alle TIC scelta dall'entità finanziaria. Nel contesto di tali politiche e procedure, le entità finanziarie dovrebbero adottare pratiche e metodi di test adatti alle loro esigenze, attenendosi a un approccio basato sul rischio e garantendo il mantenimento di un ambiente TIC sicuro, affidabile e resiliente. Per garantire l'attuazione sicura di un progetto relativo alle TIC, le entità finanziarie dovrebbero assicurarsi che il personale di specifici settori aziendali o ruoli influenzati o interessati dal progetto relativo alle TIC possa fornire le informazioni e le competenze necessarie. Per garantire una sorveglianza efficace, dovrebbero essere presentate all'organo di gestione relazioni sui progetti relativi alle TIC, in particolare sui progetti che riguardano funzioni essenziali o importanti e sui rischi associati. Le entità finanziarie dovrebbero adattare la frequenza e i dettagli delle relazioni e dei riesami sistematici e continui all'importanza e alle dimensioni dei progetti relativi alle TIC interessati.

(16) È necessario garantire che i pacchetti software che le entità finanziarie di cui al titolo II del presente regolamento acquisiscono e sviluppano siano integrati in modo efficace e sicuro nell'ambiente TIC esistente, conformemente agli obiettivi aziendali e di sicurezza delle informazioni stabiliti. È quindi opportuno che le entità finanziarie valutino attentamente tali pacchetti software. A tal fine, e per identificare le vulnerabilità e le potenziali lacune nella sicurezza tanto dei pacchetti software quanto dei sistemi di TIC in generale, le entità finanziarie dovrebbero effettuare test di sicurezza delle TIC. Per valutare l'integrità dei software e garantire che l'uso di tali software non comporti rischi per la sicurezza delle TIC, le entità finanziarie dovrebbero anche esaminare i codici sorgente dei software acquisiti, compresi, ove possibile, i software proprietari forniti da fornitori terzi di servizi TIC, utilizzando metodi di test sia statici che dinamici.

(17) Le modifiche, a prescindere dalla loro portata, comportano rischi intrinseci e potrebbero comportare rischi significativi in termini di perdita di riservatezza, integrità e disponibilità dei dati, con conseguenti gravi perturbazioni dell'attività. Per salvaguardare le entità finanziarie da potenziali vulnerabilità e debolezze delle TIC che potrebbero esporle a rischi significativi, è necessario un rigoroso processo di verifica per confermare che tutte le modifiche soddisfino i necessari requisiti di sicurezza delle TIC. Le entità finanziarie di cui al titolo II del presente regolamento dovrebbero quindi, come elemento essenziale delle loro politiche e procedure per la sicurezza delle TIC, disporre di solide politiche e procedure di gestione delle modifiche delle TIC. Per sostenere l'obiettività e l'efficacia del processo di gestione delle modifiche delle TIC, prevenire i conflitti di interessi e garantire che le modifiche delle TIC siano valutate in modo obiettivo, è necessario separare le funzioni responsabili dell'approvazione delle modifiche dalle funzioni che le richiedono e le attuano. Per ottenere transizioni efficaci, un'attuazione controllata delle modifiche delle TIC e perturbazioni minime del funzionamento dei sistemi di TIC, è opportuno che le entità finanziarie assegnino ruoli e responsabilità chiari che garantiscano che le modifiche delle TIC siano pianificate, adeguatamente testate e che sia assicurata la qualità. Per garantire che i sistemi di TIC continuino a funzionare efficacemente e per fornire una rete di sicurezza alle entità finanziarie, queste ultime dovrebbero elaborare e attuare anche procedure di fall-back. Le entità finanziarie dovrebbero identificare chiaramente le procedure di fall-back e assegnare le responsabilità per garantire una risposta rapida ed efficace in caso di modifiche delle TIC non andate a buon fine.

(18) Al fine di individuare, gestire e segnalare gli incidenti connessi alle TIC, le entità finanziarie di cui al titolo II del presente regolamento dovrebbero definire una politica relativa agli incidenti connessi alle TIC che comprenda le componenti di un processo di gestione degli incidenti connessi alle TIC. A tal fine, è opportuno che le entità finanziarie identifichino tutti i contatti pertinenti all'interno e all'esterno dell'organizzazione che possano facilitare il corretto coordinamento e l'attuazione delle diverse fasi del processo. Per ottimizzare l'individuazione degli incidenti connessi alle TIC e la risposta agli stessi e per identificare le tendenze di tali incidenti, che rappresentano una preziosa fonte di informazioni grazie alle quali le entità finanziarie possono identificare e affrontare le cause e i problemi di fondo in modo efficace, le entità finanziarie dovrebbero in particolare analizzare in dettaglio gli incidenti connessi alle TIC che ritengono più significativi, anche in ragione del loro regolare ripetersi.

(19) Al fine di garantire l'individuazione tempestiva ed efficace delle attività anomale, le entità finanziarie di cui al titolo II del presente regolamento dovrebbero raccogliere, monitorare e analizzare le diverse fonti di informazione e dovrebbero assegnare i relativi ruoli e responsabilità. Per quanto riguarda le fonti interne di informazioni, i log sono una fonte estremamente rilevante, ma è opportuno che le entità finanziarie non facciano affidamento solo su di essi. Le entità finanziarie dovrebbero invece considerare informazioni più ampie che includano quanto riportato da altre funzioni interne, in quanto tali funzioni sono spesso una fonte preziosa di informazioni pertinenti. Per lo stesso motivo, è opportuno che le entità finanziarie analizzino e monitorino le informazioni raccolte da fonti esterne, comprese le informazioni provenienti da fornitori terzi di TIC sugli incidenti che interessano i loro sistemi e le loro reti, e altre fonti di informazione che le entità finanziarie ritengono pertinenti. Nella misura in cui tali informazioni costituiscono dati personali, si applica il diritto dell'Unione in materia di protezione dei dati. È opportuno che i dati personali siano limitati a quanto necessario per l'individuazione dell'incidente.

(20) Per facilitare l'individuazione degli incidenti connessi alle TIC, le entità finanziarie dovrebbero conservare le prove di tali incidenti. Per garantire, da un lato, che tali prove siano conservate per un periodo sufficientemente lungo e per evitare, dall'altro, un onere normativo eccessivo, è opportuno che le entità finanziarie determinino il periodo di conservazione tenendo conto, tra l'altro, della criticità dei dati e degli obblighi di conservazione derivanti dal diritto dell'Unione.

(21) Per garantire che gli incidenti connessi alle TIC siano individuati in tempo, le entità finanziarie di cui al titolo II del presente regolamento dovrebbero considerare non esaustivi i criteri identificati per attivare l'individuazione degli incidenti connessi alle TIC e le risposte ad essi. Inoltre, sebbene sia opportuno che le entità finanziarie prendano in considerazione ciascuno di tali criteri, non dovrebbe essere necessario che le circostanze descritte nei criteri si verifichino simultaneamente e si dovrebbe considerare in modo appropriato l'importanza dei servizi TIC interessati per l'avvio dei processi di individuazione degli incidenti connessi alle TIC e di risposta agli stessi.

(22) Nell'elaborare una politica di continuità operativa delle TIC, le entità finanziarie di cui al titolo II del presente regolamento dovrebbero tenere conto delle componenti essenziali della gestione dei rischi informatici comprese le strategie di gestione e comunicazione degli incidenti connessi alle TIC, il processo di gestione delle modifiche delle TIC e i rischi associati ai fornitori terzi di servizi TIC.

(23) È necessario definire la serie di scenari che le entità finanziarie di cui al titolo II del presente regolamento dovrebbero prendere in considerazione sia per l'attuazione dei piani di risposta e ripristino relativi alle TIC sia per i test dei piani di continuità operativa delle TIC. Tali scenari dovrebbero servire alle entità finanziarie come punto di partenza per analizzare sia la rilevanza e la plausibilità di ogni scenario sia la necessità di elaborare scenari alternativi. Le entità finanziarie dovrebbero concentrarsi sugli scenari in cui gli investimenti in misure di resilienza potrebbero essere più efficienti ed efficaci. Testando il passaggio tra l'infrastruttura TIC primaria e la capacità ridondante, i backup e le attrezzature ridondanti, gli enti finanziari dovrebbero valutare se la capacità, il backup e le attrezzature funzionano efficacemente per un periodo di tempo sufficiente e garantire il ripristino del normale funzionamento dell'infrastruttura delle TIC primarie conformemente agli obiettivi di ripristino.

(24) È necessario stabilire prescrizioni per il rischio operativo e, in particolare, per la gestione dei progetti e delle modifiche relativi alle TIC e per la gestione della continuità operativa delle TIC, sulla base di quelle già previste per le controparti centrali, i depositari centrali di titoli e le sedi di negoziazione ai sensi, rispettivamente, dei regolamenti (UE) n. 648/2012 ([3]), (UE) n. 600/2014 ([4]) e (UE) n. 909/2014 ([5]) del Parlamento europeo e del Consiglio.

(25) L'articolo 6, paragrafo 5, del regolamento (UE) 2022/2554 impone alle entità finanziarie di riesaminare il proprio quadro per la gestione dei rischi informatici e di presentare all'autorità competente una relazione in merito a tale riesame. Per consentire alle autorità competenti un'agevole elaborazione delle informazioni contenute in tali relazioni e per garantire un'adeguata trasmissione di tali informazioni, è opportuno che le entità finanziarie presentino tali relazioni in un formato elettronico che permetta la ricerca al suo interno.

(26) È opportuno che le prescrizioni per le entità finanziarie soggette al quadro semplificato per la gestione dei rischi informatici di cui all'articolo 16 del regolamento (UE) 2022/2554 si concentrino sulle aree e sugli elementi essenziali che, alla luce della portata, del rischio, delle dimensioni e della complessità di tali entità finanziarie, sono come minimo necessari per garantire la riservatezza, l'integrità, la disponibilità e l'autenticità dei dati e dei servizi di tali entità finanziarie. In tale contesto, le suddette entità finanziarie dovrebbero disporre di un quadro di gestione e di controllo interno con responsabilità chiare per consentire un quadro per la gestione dei rischi efficace e solido. Inoltre, al fine di ridurre l'onere amministrativo e operativo, tali entità finanziarie dovrebbero elaborare e documentare una sola politica, ossia una politica di sicurezza dell'informazione che specifichi le norme e i principi di alto livello necessari per tutelare la riservatezza, l'integrità, la disponibilità e l'autenticità dei dati e dei servizi di tali entità finanziarie.

(27) Le disposizioni del presente regolamento si riferiscono all'ambito del quadro per la gestione dei rischi informatici, indicando gli elementi specifici applicabili alle entità finanziarie conformemente all'articolo 15 del regolamento (UE) 2022/2554 e definendo il quadro semplificato per la gestione dei rischi informatici per le entità finanziarie di cui all'articolo 16, paragrafo 1, di tale regolamento. Per garantire la coerenza tra il quadro per la gestione dei rischi informatici ordinario e quello semplificato, e considerando che tali disposizioni dovrebbero entrare in applicazione contemporaneamente, è opportuno includere tali disposizioni in un unico atto legislativo.

(28) Il presente regolamento si basa sul progetto di norme tecniche di regolamentazione presentato alla Commissione dall'Autorità bancaria europea, dall'Autorità europea delle assicurazioni e delle pensioni aziendali e professionali e dall'Autorità europea degli strumenti finanziari e dei mercati (autorità europee di vigilanza), in consultazione con l'Agenzia dell'Unione europea per la cibersicurezza (ENISA).

([3]) Regolamento (UE) n. 648/2012 del Parlamento europeo e del Consiglio, del 4 luglio 2012, sugli strumenti derivati OTC, le controparti centrali e i repertori di dati sulle negoziazioni (GU L 201 del 27.7.2012, pag. 1, ELI: http://data.europa.eu/eli/reg/2012/648/oj).

([4]) Regolamento (UE) n. 600/2014 del Parlamento europeo e del Consiglio, del 15 maggio 2014, sui mercati degli strumenti finanziari e che modifica il regolamento (UE) n. 648/2012 (GU L 173 del 12.6.2014, pag. 84, ELI: http://data.europa.eu/eli/reg/2014/600/oj).

([5]) Regolamento (UE) n. 909/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, relativo al miglioramento del regolamento titoli nell'Unione europea e ai depositari centrali di titoli e recante modifica delle direttive 98/26/CE e 2014/65/UE e del regolamento (UE) n. 236/2012 (GU L 257 del 28.8.2014, pag. 1, ELI: http://data.europa.eu/eli/reg/2014/909/oj).

(29) Il comitato congiunto delle autorità europee di vigilanza di cui all'articolo 54 del regolamento (UE) n. 1093/2010 del Parlamento europeo e del Consiglio ([6]), all'articolo 54 del regolamento (UE) n. 1094/2010 del Parlamento europeo e del Consiglio ([7]) e all'articolo 54 del regolamento (UE) n. 1095/2010 del Parlamento europeo e del Consiglio ([8]) ha condotto consultazioni pubbliche sul progetto di norme tecniche di regolamentazione su cui si basa il presente regolamento, ha analizzato i potenziali costi e benefici delle norme proposte e ha chiesto il parere del gruppo delle parti interessate nel settore bancario, istituito ai sensi dell'articolo 37 del regolamento (UE) n. 1093/2010, dei gruppi delle parti interessate nel settore dell'assicurazione e della riassicurazione e nel settore dei fondi pensionistici aziendali e professionali, istituiti ai sensi dell'articolo 37 del regolamento (UE) n. 1094/2010, e del gruppo delle parti interessate nel settore degli strumenti finanziari e dei mercati, istituito ai sensi dell'articolo 37 del regolamento (UE) n. 1095/2010.

(30) Nella misura in cui il trattamento dei dati personali è necessario per adempiere agli obblighi di cui al presente atto, dovrebbero trovare piena applicazione i regolamenti (UE) 2016/679 ([9]) e (UE) 2018/1725 ([10]) del Parlamento europeo e del Consiglio. Ad esempio, si dovrebbe rispettare il principio della minimizzazione dei dati quando si raccolgono dati personali per garantire un'adeguata individuazione degli incidenti. Anche il Garante europeo della protezione dei dati è stato consultato in merito al progetto del presente atto,

HA ADOTTATO IL PRESENTE REGOLAMENTO:

TITOLO I

PRINCIPIO GENERALE

Articolo 1

Profilo di rischio complessivo e complessità

Nell'elaborare e attuare le politiche, le procedure, i protocolli e gli strumenti di sicurezza delle TIC di cui al titolo II e il quadro semplificato per la gestione dei rischi informatici di cui al titolo III, si tiene conto delle dimensioni e del profilo di rischio complessivo dell'entità finanziaria, nonché della natura, della portata e degli elementi di maggiore o minore complessità dei suoi servizi, attività e operazioni, compresi gli elementi relativi a:

a) cifratura e crittografia;

b) sicurezza delle operazioni riguardanti le TIC;

c) sicurezza della rete;

([6]) Regolamento (UE) n. 1093/2010 del Parlamento europeo e del Consiglio, del 24 novembre 2010, che istituisce l'Autorità europea di vigilanza (Autorità bancaria europea), modifica la decisione n. 716/2009/CE e abroga la decisione 2009/78/CE della Commissione (GU L 331 del 15.12.2010, pag. 12, ELI: http://data.europa.eu/eli/reg/2010/1093/oj).

([7]) Regolamento (UE) n. 1094/2010 del Parlamento europeo e del Consiglio, del 24 novembre 2010, che istituisce l'Autorità europea di vigilanza (Autorità europea delle assicurazioni e delle pensioni aziendali e professionali), modifica la decisione n. 716/2009/CE e abroga la decisione 2009/79/CE della Commissione (GU L 331 del 15.12.2010, pag. 48, ELI: http://data.europa.eu/eli/reg/2010/1094/oj).

([8]) Regolamento (UE) n. 1095/2010 del Parlamento europeo e del Consiglio, del 24 novembre 2010, che istituisce l'Autorità europea di vigilanza (Autorità europea degli strumenti finanziari e dei mercati), modifica la decisione n. 716/2009/CE e abroga la decisione 2009/77/CE della Commissione (GU L 331 del 15.12.2010, pag. 84, ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

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

([10]) 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).

d) gestione dei progetti e delle modifiche relativi alle TIC;

e) il potenziale impatto dei rischi informatici sulla riservatezza, l'integrità e la disponibilità dei dati, e quello delle perturbazioni sulla continuità e la disponibilità delle attività dell'entità finanziaria.

TITOLO II

ULTERIORE ARMONIZZAZIONE DI STRUMENTI, METODI, PROCESSI E POLITICHE DI GESTIONE DEL RISCHIO INFORMATICO AI SENSI DELL'ARTICOLO 15 DEL REGOLAMENTO (UE) 2022/2554

CAPO I

Politiche, procedure, protocolli e strumenti per la sicurezza delle TIC

Sezione 1

Articolo 2

Elementi generali delle politiche, delle procedure, dei protocolli e degli strumenti per la sicurezza delle TIC

1. Le entità finanziarie assicurano che le loro politiche per la sicurezza delle TIC, la sicurezza delle informazioni nonché le procedure, i protocolli e gli strumenti correlati di cui all'articolo 9, paragrafo 2, del regolamento (UE) 2022/2554 siano integrati nel loro quadro per la gestione dei rischi informatici. Le entità finanziarie definiscono politiche, procedure, protocolli e strumenti per la sicurezza delle TIC di cui al presente capo che:

a) garantiscono la sicurezza delle reti;

b) contengono adeguate salvaguardie contro le intrusioni e l'uso illecito dei dati;

c) preservano la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati, anche con tecniche crittografiche;

d) garantiscono un'accurata e pronta trasmissione dei dati senza gravi perturbazioni né indebiti ritardi.

2. Le entità finanziarie provvedono affinché le politiche per la sicurezza delle TIC di cui al paragrafo 1:

a) siano allineate agli obiettivi in materia di sicurezza delle informazioni dell'entità finanziaria inclusi nella strategia di resilienza operativa digitale di cui all'articolo 6, paragrafo 8, del regolamento (UE) 2022/2554;

b) indichino la data di approvazione formale delle politiche per la sicurezza delle TIC da parte dell'organo di gestione;

c) contengano indicatori e misure per:

   i) monitorare l'attuazione delle politiche, delle procedure, dei protocolli e degli strumenti per la sicurezza delle TIC;

   ii) registrare le eccezioni a tale attuazione;

   iii) garantire la resilienza operativa digitale dell'entità finanziaria nel caso delle eccezioni di cui al punto ii);

d) specifichino le responsabilità del personale a tutti i livelli per garantire la sicurezza delle TIC dell'entità finanziaria;

e) specifichino le conseguenze dell'inosservanza delle politiche per la sicurezza delle TIC da parte del personale dell'entità finanziaria, laddove non siano previste disposizioni in tal senso in altre politiche dell'entità finanziaria;

f) elenchino la documentazione da conservare;

g) specifichino le modalità di separazione dei compiti nel contesto del modello delle tre linee di difesa o di un altro modello interno di gestione e controllo del rischio, a seconda dei casi, per evitare conflitti di interessi;

h) tengano conto delle pratiche più avanzate e, se del caso, delle norme definite all'articolo 2, punto 1), del regolamento (UE) n. 1025/2012;

i) identifichino i ruoli e le responsabilità per l'elaborazione, l'attuazione e la manutenzione delle politiche, delle procedure, dei protocolli e degli strumenti per la sicurezza delle TIC;

j) siano sottoposte a riesame in conformità dell'articolo 6, paragrafo 5, del regolamento (UE) 2022/2554;

k) tengano conto di modifiche sostanziali riguardanti l'entità finanziaria, comprese modifiche sostanziali nelle attività o nei processi dell'entità finanziaria, nel panorama delle minacce informatiche o negli obblighi giuridici applicabili.

Sezione 2

Articolo 3

Gestione dei rischi informatici

Le entità finanziarie elaborano, documentano e attuano politiche e procedure per la gestione dei rischi informatici contenenti tutti gli elementi seguenti:

a) l'indicazione dell'approvazione del livello di tolleranza per i rischi informatici stabilito in conformità dell'articolo 6, paragrafo 8, lettera b), del regolamento (UE) 2022/2554;

b) una procedura e una metodologia per condurre la valutazione dei rischi informatici, che identifichino:

   i) le vulnerabilità e le minacce che interessano o potrebbero interessare le funzioni commerciali supportate, i sistemi di TIC e le risorse TIC che supportano tali funzioni;

   ii) gli indicatori quantitativi o qualitativi per misurare l'impatto e la probabilità delle vulnerabilità e delle minacce di cui al punto i);

c) la procedura per identificare, attuare e documentare le misure di trattamento dei rischi informatici per i rischi identificati e valutati, compresa la determinazione delle misure di trattamento dei rischi informatici necessarie per far rientrare il rischio informatico nel livello di tolleranza per i rischi di cui alla lettera a);

d) per i rischi informatici residui ancora presenti dopo l'attuazione delle misure di trattamento dei rischi informatici di cui alla lettera c):

   i) disposizioni relative all'identificazione di tali rischi informatici residui;

   ii) l'assegnazione di ruoli e responsabilità per quanto riguarda:

      (1) l'accettazione dei rischi informatici residui che superano il livello di tolleranza per i rischi dell'entità finanziaria di cui alla lettera a);

      (2) il processo di riesame di cui al punto iv) della presente lettera d);

   iii) l'elaborazione di un inventario dei rischi informatici residui accettati, compresa la motivazione della loro accettazione;

   iv) disposizioni relative al riesame, almeno una volta all'anno, dei rischi informatici residui accettati, che comprendano:

      1) l'identificazione di eventuali cambiamenti nei rischi informatici residui;

      2) la valutazione delle misure di attenuazione disponibili;

      3) la valutazione della validità e dell'applicabilità, alla data del riesame, delle motivazioni che giustificano l'accettazione dei rischi informatici residui;

e) disposizioni sul monitoraggio:

   i) di qualsiasi cambiamento nel panorama dei rischi informatici e delle minacce informatiche;

   ii) di vulnerabilità e minacce interne ed esterne;

   iii) del rischio informatico dell'entità finanziaria, che consentano di individuare tempestivamente i cambiamenti che potrebbero influire sul suo profilo di rischio informatico;

f) disposizioni relative a un processo per garantire che si tenga conto di eventuali modifiche alla strategia aziendale e alla strategia di resilienza operativa digitale dell'entità finanziaria.

Ai fini del primo comma, lettera c), la procedura di cui a tale lettera garantisce:

a) il monitoraggio dell'efficacia delle misure di trattamento dei rischi informatici attuate;

b) la valutazione del raggiungimento dei livelli di tolleranza per i rischi fissati dall'entità finanziaria;

c) la valutazione del fatto che l'entità finanziaria abbia intrapreso azioni per correggere o migliorare tali misure, ove necessario.

Sezione 3

Gestione delle risorse TIC

Articolo 4

Politica di gestione delle risorse TIC

1. Nell'ambito delle politiche, delle procedure, dei protocolli e degli strumenti per la sicurezza delle TIC di cui all'articolo 9, paragrafo 2, del regolamento (UE) 2022/2554, le entità finanziarie elaborano, documentano e attuano una politica in materia di gestione delle risorse TIC.

2. La politica in materia di gestione delle risorse TIC di cui al paragrafo 1:

a) prescrive il monitoraggio e la gestione del ciclo di vita delle risorse TIC identificate e classificate in conformità dell'articolo 8, paragrafo 1, del regolamento (UE) 2022/2554;

b) prescrive che l'entità finanziaria tenga registrazioni di tutti gli elementi seguenti:

   i) l'identificativo univoco di ciascuna risorsa TIC;

   ii) informazioni sull'ubicazione, fisica o logica, di tutte le risorse TIC;

   iii) la classificazione di tutte le risorse TIC di cui all'articolo 8, paragrafo 1, del regolamento (UE) 2022/2254;

   iv) l'identità dei proprietari delle risorse TIC;

   v) le funzioni o i servizi commerciali supportati dalla risorsa TIC;

   vi) i requisiti di continuità operativa delle TIC, compresi gli obiettivi di tempo di ripristino e punto di ripristino;

   vii) se la risorsa TIC può essere o è esposta a reti esterne, compreso Internet;

   viii) i collegamenti e le interdipendenze tra le risorse TIC e le funzioni commerciali che utilizzano ciascuna risorsa TIC;

   ix) se applicabile, per tutte le risorse TIC, le date di fine dei servizi di assistenza regolare, estesa e personalizzata del fornitore terzo di servizi TIC, dopo le quali tali risorse TIC non sono più supportate dal loro fornitore o da un fornitore terzo di servizi TIC;

c) per le entità finanziarie diverse dalle microimprese, prescrive che tali entità finanziarie conservino i registri delle informazioni necessarie per effettuare una valutazione specifica dei rischi informatici su tutti i sistemi di TIC legacy di cui all'articolo 8, paragrafo 7, del regolamento (UE) 2022/2554.

Articolo 5

Procedura di gestione delle risorse TIC

1. Le entità finanziarie elaborano, documentano e attuano una procedura per la gestione delle risorse TIC.

2. La procedura per la gestione delle risorse TIC di cui al paragrafo 1 specifica i criteri per effettuare la valutazione della criticità dei patrimoni informativi e delle risorse TIC a supporto delle funzioni commerciali. La valutazione tiene conto:

a) del rischio informatico relativo a tali funzioni commerciali e alle loro dipendenze dal patrimonio informativo o dalle risorse TIC;

b) di come la perdita di riservatezza, integrità e disponibilità di tali patrimoni informativi e risorse TIC avrebbe un impatto sulle attività e sui processi commerciali delle entità finanziarie.

Sezione 4

Cifratura e crittografia

Articolo 6

Cifratura e controlli crittografici

1. Nell'ambito delle politiche, delle procedure, dei protocolli e degli strumenti per la sicurezza delle TIC di cui all'articolo 9, paragrafo 2, del regolamento (UE) 2022/2554, le entità finanziarie elaborano, documentano e attuano una politica in materia di cifratura e controlli crittografici.

2. Le entità finanziarie elaborano la politica in materia di cifratura e controlli crittografici di cui al paragrafo 1 sulla base dei risultati di una classificazione dei dati approvata e di una valutazione dei rischi informatici. La politica contiene norme relative a tutti gli aspetti seguenti:

a) la cifratura dei dati a riposo e in transito;

b) la cifratura dei dati in uso, ove necessario;

c) la cifratura delle connessioni di rete interne e del traffico con l'esterno;

d) la gestione delle chiavi crittografiche di cui all'articolo 7, che stabilisce le norme sul corretto uso, la protezione e il ciclo di vita delle chiavi crittografiche.

Ai fini della lettera b), qualora non sia possibile la cifratura dei dati in uso, le entità finanziarie trattano i dati in uso in un ambiente separato e protetto o adottano misure equivalenti per garantire la riservatezza, l'integrità, l'autenticità e la disponibilità dei dati.

3. Le entità finanziarie includono nella politica in materia di cifratura e controlli crittografici di cui al paragrafo 1 i criteri per la selezione delle tecniche crittografiche e delle pratiche d'uso, tenendo conto delle pratiche più avanzate e delle norme definite all'articolo 2, punto 1), del regolamento (UE) n. 1025/2012, e la classificazione delle pertinenti risorse TIC stabilita conformemente all'articolo 8, paragrafo 1, del regolamento (UE) 2022/2554. Le entità finanziarie che non sono in grado di attenersi alle pratiche o alle norme più avanzate o di utilizzare le tecniche più affidabili adottano misure di attenuazione e di monitoraggio che garantiscano la resilienza alle minacce informatiche.

4. Le entità finanziarie includono nella politica in materia di cifratura e controlli crittografici di cui al paragrafo 1 disposizioni per aggiornare o modificare, se necessario, la tecnologia crittografica sulla base degli sviluppi della crittoanalisi. Tali aggiornamenti o modifiche garantiscono la resilienza della tecnologia crittografica alle minacce informatiche, come stabilito dall'articolo 10, paragrafo 2, lettera a). Le entità finanziarie che non sono in grado di aggiornare o modificare la tecnologia crittografica adottano misure di attenuazione e di monitoraggio che garantiscano la resilienza alle minacce informatiche.

5. Le entità finanziarie includono nella politica in materia di cifratura e controlli crittografici di cui al paragrafo 1 l'obbligo di registrare l'adozione delle misure di attenuazione e di monitoraggio adottate in conformità dei paragrafi 3 e 4 e di fornire una spiegazione motivata di tale scelta.

Articolo 7

Gestione delle chiavi crittografiche

1. Le entità finanziarie includono nella politica di gestione delle chiavi crittografiche di cui all'articolo 6, paragrafo 2, lettera d), prescrizioni per la gestione delle chiavi crittografiche durante il loro intero ciclo di vita, compresi la generazione, il rinnovo, la conservazione, il backup, l'archiviazione, il recupero, la trasmissione, il ritiro, la revoca e la distruzione di tali chiavi crittografiche.

2. Le entità finanziarie identificano e attuano controlli per proteggere le chiavi crittografiche durante il loro intero ciclo di vita per evitarne la perdita, l'accesso non autorizzato, la divulgazione e la modifica. Le entità finanziarie concepiscono tali controlli sulla base dei risultati della classificazione dei dati approvata e della valutazione dei rischi informatici.

3. Le entità finanziarie elaborano e attuano metodi per sostituire le chiavi crittografiche in caso di perdita, compromissione o danneggiamento delle stesse.

4. Le entità finanziarie creano e mantengono un registro per tutti i certificati e i dispositivi di archiviazione dei certificati almeno per le risorse TIC che supportano funzioni essenziali o importanti. Le entità finanziarie mantengono tale registro aggiornato.

5. Le entità finanziarie garantiscono il tempestivo rinnovo dei certificati prima della loro scadenza.

Sezione 5

Sicurezza delle operazioni riguardanti le TIC

Articolo 8

Politiche e procedure per le operazioni riguardanti le TIC

1. Nell'ambito delle politiche, delle procedure, dei protocolli e degli strumenti per la sicurezza delle TIC di cui all'articolo 9, paragrafo 2, del regolamento (UE) 2022/2554, le entità finanziarie elaborano, documentano e attuano politiche e procedure per gestire le operazioni riguardanti le TIC. Tali politiche e procedure specificano in che modo le entità finanziarie gestiscono, monitorano, controllano e ripristinano le proprie risorse TIC, compresa la documentazione delle operazioni riguardanti le TIC.

2. Le politiche e le procedure per le operazioni riguardanti le TIC di cui al paragrafo 1 contengono tutti gli elementi seguenti:

a) una descrizione delle risorse TIC che includa tutti gli elementi seguenti:

   i) requisiti relativi alla sicurezza dell'installazione, della manutenzione, della configurazione e della disinstallazione di un sistema di TIC;

   ii) requisiti relativi alla gestione del patrimonio informativo utilizzato dalle risorse TIC, inclusi il trattamento e l'elaborazione, sia automatizzati che manuali;

   iii) requisiti relativi all'identificazione e al controllo dei sistemi di TIC legacy;

b) i controlli e il monitoraggio dei sistemi di TIC, comprendenti tutti gli elementi seguenti:

   i) requisiti di backup e ripristino dei sistemi di TIC;

   ii) requisiti di scheduling, tenendo conto delle interdipendenze tra i sistemi di TIC;

   iii) protocolli per le informazioni di audit trail e log di sistema;

   iv) requisiti per garantire che l'esecuzione dell'audit interno e di altri test riduca al minimo le perturbazioni delle operazioni commerciali;

   v) requisiti sulla separazione degli ambienti di produzione delle TIC dagli ambienti di sviluppo, test e da altri ambienti non di produzione;

   vi) requisiti per condurre lo sviluppo e i test in ambienti separati dall'ambiente di produzione;

   vii) requisiti per condurre lo sviluppo e i test in ambienti di produzione;

c) gestione degli errori relativi ai sistemi di TIC, che comprenda tutti gli elementi seguenti:

i) procedure e protocolli per la gestione degli errori;

ii) contatti dell'assistenza e dei livelli successivi di intervento, compresi i contatti dell'assistenza esterna in caso di problemi operativi o tecnici imprevisti;

iii) procedure di riavvio, riesecuzione e ripristino dei sistemi di TIC da utilizzare in caso di perturbazione dei sistemi di TIC.

Ai fini della lettera b), punto v), la separazione considera tutte le componenti dell'ambiente, compresi gli account, i dati o le connessioni, come previsto dall'articolo 13, primo comma, lettera a).

Ai fini della lettera b), punto vii), le politiche e le procedure di cui al paragrafo 1 prevedono che i casi in cui i test sono eseguiti in un ambiente di produzione siano chiaramente identificati, motivati, abbiano una durata limitata e siano approvati dalla funzione competente conformemente all'articolo 16, paragrafo 6. Le entità finanziarie garantiscono la disponibilità, la riservatezza, l'integrità e l'autenticità dei sistemi di TIC e dei dati di produzione durante le attività di sviluppo e di test nell'ambiente di produzione.

Articolo 9

Gestione della capacità e delle prestazioni

1. Nell'ambito delle politiche, delle procedure, dei protocolli e degli strumenti per la sicurezza delle TIC di cui all'articolo 9, paragrafo 2, del regolamento (UE) 2022/2554, le entità finanziarie elaborano, documentano e attuano procedure di gestione della capacità e delle prestazioni per:

a) l'identificazione dei requisiti di capacità dei loro sistemi di TIC;

b) l'applicazione dell'ottimizzazione delle risorse;

c) le procedure di monitoraggio per mantenere e migliorare:

i) la disponibilità dei dati e dei sistemi di TIC;

ii) l'efficienza dei sistemi di TIC;

iii) la prevenzione della carenza di capacità TIC.

2. Le procedure di gestione della capacità e delle prestazioni di cui al paragrafo 1 garantiscono che le entità finanziarie adottino misure adeguate per tener conto delle specificità dei sistemi di TIC con processi di appalto o di approvazione lunghi o complessi o dei sistemi di TIC ad alta intensità di risorse.

Articolo 10

Gestione delle vulnerabilità e delle patch

1. Nell'ambito delle politiche, delle procedure, dei protocolli e degli strumenti per la sicurezza delle TIC di cui all'articolo 9, paragrafo 2, del regolamento (UE) 2022/2554, le entità finanziarie elaborano, documentano e attuano procedure per la gestione delle vulnerabilità.

2. Le procedure per la gestione delle vulnerabilità di cui al paragrafo 1:

a) identificano e aggiornano risorse informative pertinenti e attendibili per creare e mantenere la consapevolezza rispetto alle vulnerabilità;

b) garantiscono l'esecuzione di scansioni e valutazioni automatizzate delle vulnerabilità delle risorse TIC, la cui frequenza e portata sono commisurate alla classificazione effettuata conformemente all'articolo 8, paragrafo 1, del regolamento (UE) 2022/2554 e al profilo di rischio complessivo della risorsa TIC;

c) verificano se:

i) i fornitori terzi di servizi TIC gestiscono le vulnerabilità relative ai servizi TIC forniti all'entità finanziaria;

ii) tali fornitori di servizi segnalano all'entità finanziaria almeno le vulnerabilità critiche nonché le statistiche e le tendenze in modo tempestivo;

d) tengono traccia dell'utilizzo di:

i) librerie di terze parti, comprese quelle open-source, utilizzate dai servizi TIC a supporto di funzioni essenziali o importanti;

ii) servizi TIC sviluppati dall'entità finanziaria stessa o specificamente personalizzati o sviluppati per l'entità finanziaria da un fornitore terzo di servizi TIC;

e) definiscono procedure per la comunicazione responsabile delle vulnerabilità ai clienti, alle controparti e al pubblico;

f) danno priorità all'applicazione di patch e ad altre misure di attenuazione per risolvere le vulnerabilità identificate;

g) monitorano e verificano la correzione delle vulnerabilità;

h) prevedono la registrazione di tutte le vulnerabilità individuate che riguardano i sistemi di TIC e il monitoraggio della loro risoluzione.

Ai fini della lettera b), le entità finanziarie eseguono la scansione e la valutazione automatizzate delle vulnerabilità delle risorse TIC per le risorse TIC che supportano funzioni essenziali o importanti con cadenza almeno settimanale.

Ai fini della lettera c), le entità finanziarie richiedono ai fornitori terzi di servizi TIC di indagare sulle pertinenti vulnerabilità, di determinare le cause di fondo e di attuare le opportune azioni di attenuazione.

Ai fini della lettera d), le entità finanziarie monitorano, se del caso in collaborazione con il fornitore terzo di servizi TIC, la versione e gli eventuali aggiornamenti delle librerie di terze parti. Nel caso di risorse TIC o di componenti di risorse TIC pronti all'uso (disponibili in commercio) acquisiti e utilizzati nell'ambito di servizi TIC che non supportano funzioni essenziali o importanti, le entità finanziarie tracciano l'utilizzo, per quanto possibile, di librerie di terze parti, comprese le librerie open-source.

Ai fini della lettera f), le entità finanziarie considerano la criticità della vulnerabilità, la classificazione effettuata conformemente all'articolo 8, paragrafo 1, del regolamento (UE) 2022/2554 e il profilo di rischio delle risorse TIC interessate dalle vulnerabilità identificate.

3. Nell'ambito delle politiche, delle procedure, dei protocolli e degli strumenti per la sicurezza delle TIC di cui all'articolo 9, paragrafo 2, del regolamento (UE) 2022/2554, le entità finanziarie elaborano, documentano e attuano procedure per la gestione delle patch.

4. Le procedure per la gestione delle patch di cui al paragrafo 3:

a) per quanto possibile, identificano e valutano le patch e gli aggiornamenti di software e hardware disponibili utilizzando strumenti automatizzati;

b) identificano le procedure di emergenza per la correzione mediante patch e l'aggiornamento delle risorse TIC;

c) testano e applicano le patch di software e hardware e gli aggiornamenti di cui all'articolo 8, paragrafo 2, lettera b), punti v), vi) e vii);

d) stabiliscono scadenze per l'installazione di patch e aggiornamenti software e hardware e procedure di attivazione dei livelli successivi di intervento nel caso in cui tali scadenze non possano essere rispettate.

Articolo 11

Sicurezza dei dati e dei sistemi

1. Nell'ambito delle politiche, delle procedure, dei protocolli e degli strumenti per la sicurezza delle TIC di cui all'articolo 9, paragrafo 2, del regolamento (UE) 2022/2554, le entità finanziarie elaborano, documentano e attuano una procedura per la sicurezza dei dati e dei sistemi.

2. La procedura per la sicurezza dei dati e dei sistemi di cui al paragrafo 1 contiene tutti gli elementi seguenti relativi alla sicurezza dei dati e dei sistemi di TIC, secondo la classificazione effettuata in conformità dell'articolo 8, paragrafo 1, del regolamento (UE) 2022/2554:

a) le restrizioni di accesso di cui all'articolo 21 del presente regolamento, a supporto dei requisiti di protezione per ciascun livello di classificazione;

b) l'identificazione di una configurazione di base sicura per le risorse TIC che riduca al minimo l'esposizione di tali risorse alle minacce informatiche e misure per verificare regolarmente che tali configurazioni di base siano effettivamente applicate;

c) l'identificazione di misure di sicurezza per garantire che nei sistemi di TIC e nei dispositivi endpoint siano installati solo software autorizzati;

d) l'identificazione di misure di sicurezza contro i codici malevoli;

e) l'identificazione di misure di sicurezza per garantire che solo i supporti di memorizzazione dei dati, i sistemi e i dispositivi endpoint autorizzati siano utilizzati per trasferire e memorizzare i dati dell'entità finanziaria;

f) gli obblighi seguenti per proteggere l'uso dei dispositivi endpoint portatili e dei dispositivi endpoint privati non portatili:

   i) l'obbligo di utilizzare una soluzione di gestione per gestire da remoto i dispositivi endpoint e cancellare da remoto i dati dell'entità finanziaria;

   ii) l'obbligo di utilizzare meccanismi di sicurezza che non possono essere modificati, rimossi o aggirati da membri del personale o da fornitori terzi di servizi TIC senza autorizzazione;

   iii) l'obbligo di utilizzare dispositivi di archiviazione dati rimovibili solo quando il rischio informatico residuo rimane entro il livello di tolleranza per i rischi dell'entità finanziaria di cui all'articolo 3, primo comma, lettera a);

g) il processo per cancellare in modo sicuro i dati, presenti nei locali dell'entità finanziaria o conservati all'esterno, che l'entità finanziaria non ha più bisogno di raccogliere o conservare;

h) il processo per smaltire o dismettere in modo sicuro i dispositivi di archiviazione dati presenti nei locali dell'entità finanziaria o conservati all'esterno contenenti informazioni riservate;

i) l'identificazione e l'attuazione di misure di sicurezza per prevenire la perdita e la fuga di dati per i sistemi e per i dispositivi endpoint;

j) l'attuazione di misure di sicurezza per garantire che il telelavoro e l'uso di dispositivi endpoint privati non abbiano un impatto negativo sulla sicurezza delle TIC dell'entità finanziaria;

k) per le risorse o i servizi TIC gestiti da un fornitore terzo di servizi TIC, l'identificazione e l'attuazione di obblighi volti a mantenere la resilienza operativa digitale, conformemente ai risultati della classificazione dei dati e della valutazione dei rischi informatici.

Ai fini della lettera b), la configurazione di base sicura di cui alla stessa lettera tiene conto delle pratiche più avanzate e delle tecniche appropriate stabilite nelle norme definite all'articolo 2, punto 1), del regolamento (UE) n. 1025/2012.

Ai fini della lettera k), le entità finanziarie considerano quanto segue:

a) l'applicazione delle impostazioni raccomandate dal fornitore sugli elementi gestiti dall'entità finanziaria;

b) una chiara ripartizione dei ruoli e delle responsabilità in materia di sicurezza delle informazioni tra l'entità finanziaria e il fornitore terzo di servizi TIC, conformemente al principio della piena responsabilità dell'entità finanziaria nei confronti del suo fornitore terzo di servizi TIC di cui all'articolo 28, paragrafo 1, lettera a), del regolamento (UE) 2022/2554 e, per le entità finanziarie di cui all'articolo 28, paragrafo 2, del medesimo regolamento, conformemente alla politica dell'entità finanziaria per l'utilizzo dei servizi TIC a supporto di funzioni essenziali o importanti;

c) la necessità di garantire e mantenere adeguate competenze all'interno dell'entità finanziaria nella gestione e nella sicurezza del servizio utilizzato;

d) misure tecniche e organizzative per ridurre al minimo i rischi legati all'infrastruttura utilizzata dal fornitore terzo di servizi TIC per i suoi servizi TIC, tenendo conto delle pratiche più avanzate e delle norme definite all'articolo 2, punto 1), del regolamento (UE) n. 1025/2012.

Articolo 12

Logging

1. Nell'ambito delle salvaguardie contro le intrusioni e l'uso improprio dei dati, le entità finanziarie elaborano, documentano e attuano procedure, protocolli e strumenti di logging.

2. Le procedure, i protocolli e gli strumenti di logging di cui al paragrafo 1 contengono tutti gli elementi seguenti:

a) l'identificazione degli eventi da registrare nei log, il periodo di conservazione dei log e le misure per proteggere e gestire i dati di log, tenendo conto dello scopo per cui i log sono creati;

b) l'allineamento del livello di dettaglio dei log con il loro scopo e utilizzo per consentire l'efficace individuazione di attività anomale di cui all'articolo 24;

c) l'obbligo di registrare nei log gli eventi relativi a tutti gli aspetti seguenti:

   i) controllo degli accessi logici e fisici di cui all'articolo 21 e gestione delle identità;

   ii) gestione della capacità;

   iii) gestione delle modifiche;

   iv) operazioni riguardanti le TIC, comprese le attività dei sistemi di TIC;

   v) attività di traffico di rete, comprese le prestazioni della rete delle TIC;

d) misure per proteggere i sistemi di logging e le informazioni di log a riposo, in transito e, se del caso, in uso da manomissioni, cancellazioni e accessi non autorizzati;

e) misure per individuare eventuali guasti ai sistemi di logging;

f) fatti salvi i requisiti normativi applicabili ai sensi del diritto dell'Unione o nazionale, la sincronizzazione degli orologi di ciascuno dei sistemi di TIC dell'entità finanziaria su una fonte temporale di riferimento documentata e affidabile.

Ai fini della lettera a), le entità finanziarie stabiliscono il periodo di conservazione, tenendo conto degli obiettivi aziendali e di sicurezza delle informazioni, del motivo della registrazione dell'evento nei log e dei risultati della valutazione dei rischi informatici.

Sezione 6

Sicurezza della rete

Articolo 13

Gestione della sicurezza della rete

Le entità finanziarie, nell'ambito delle salvaguardie che garantiscono la sicurezza delle reti contro le intrusioni e l'uso improprio dei dati, elaborano, documentano e attuano politiche, procedure, protocolli e strumenti per la gestione della sicurezza della rete che comprendano tutti gli aspetti seguenti:

a) la separazione e la segmentazione delle reti e dei sistemi di TIC tenendo in considerazione:

   i) la criticità o l'importanza della funzione che le reti e i sistemi di TIC supportano;

   ii) la classificazione effettuata conformemente all'articolo 8, paragrafo 1, del regolamento (UE) 2022/2554;

   iii) il profilo di rischio complessivo delle risorse TIC che utilizzano tali reti e sistemi di TIC;

b) la documentazione di tutte le connessioni di rete e dei flussi di dati dell'entità finanziaria;

c) l'uso di una rete separata e dedicata per l'amministrazione delle risorse TIC;

d) l'identificazione e l'attuazione di controlli di accesso alla rete per prevenire e individuare le connessioni alla rete dell'entità finanziaria da parte di dispositivi o sistemi non autorizzati o di endpoint non conformi ai requisiti di sicurezza dell'entità finanziaria;

e) la cifratura delle connessioni di rete che passano su reti aziendali, reti pubbliche, reti domestiche, reti di terzi e reti wireless, per i protocolli di comunicazione utilizzati, tenendo conto dei risultati della classificazione dei dati approvata, dei risultati della valutazione dei rischi informatici e della cifratura delle connessioni di rete di cui all'articolo 6, paragrafo 2;

f) la configurazione delle reti in linea con i requisiti di sicurezza delle TIC stabiliti dall'entità finanziaria, tenendo conto delle pratiche più avanzate per garantire la riservatezza, l'integrità e la disponibilità della rete;

g) la protezione del traffico di rete tra le reti interne e Internet e altre connessioni esterne;

h) l'identificazione dei ruoli e delle responsabilità e delle fasi per la specifica, l'implementazione, l'approvazione, la modifica e il riesame delle regole del firewall e dei filtri di connessione;

i) l'esecuzione di riesami dell'architettura di rete e della configurazione della sicurezza di rete una volta all'anno, e periodicamente per le microimprese, al fine di identificare potenziali vulnerabilità;

j) le misure per isolare temporaneamente, ove necessario, sottoreti e componenti e dispositivi di rete;

k) l'implementazione di una configurazione di base sicura di tutti i componenti della rete e l'hardening della rete e dei dispositivi di rete in linea con le istruzioni del fornitore, le pratiche più avanzate e, se del caso, con le norme definite all'articolo 2, punto 1), del regolamento (UE) n. 1025/2012;

l) le procedure per limitare, bloccare e terminare le sessioni di sistema e remote dopo un determinato periodo di inattività;

m) per gli accordi sui servizi di rete:

   i) l'identificazione e la specifica delle misure di sicurezza delle TIC e delle informazioni, dei livelli di servizio e dei requisiti di gestione di tutti i servizi di rete;

   ii) se tali servizi sono forniti da un fornitore infragruppo di servizi TIC o da fornitori terzi di servizi TIC.

Ai fini della lettera h), le entità finanziarie effettuano periodicamente il riesame delle regole del firewall e dei filtri di connessione in base alla classificazione effettuata conformemente all'articolo 8, paragrafo 1, del regolamento (UE) 2022/2554 e al profilo di rischio complessivo dei sistemi di TIC coinvolti. Per i sistemi TIC che supportano funzioni essenziali o importanti, le entità finanziarie verificano l'adeguatezza delle regole del firewall e dei filtri di connessione esistenti almeno ogni sei mesi.

Articolo 14

Protezione delle informazioni in transito

1. Nell'ambito delle salvaguardie volte a preservare la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati, le entità finanziarie elaborano, documentano e attuano politiche, procedure, protocolli e strumenti per proteggere le informazioni in transito. In particolare, le entità finanziarie garantiscono tutti gli aspetti seguenti:

a) la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati durante la trasmissione di rete e la definizione di procedure per valutare la conformità a tali requisiti;

b) la prevenzione e l'individuazione di fughe di dati e il trasferimento sicuro delle informazioni tra l'entità finanziaria e le parti esterne;

c) che gli obblighi in materia di riservatezza o gli accordi di non divulgazione che riflettono le esigenze dell'entità finanziaria in materia di protezione delle informazioni sia per il personale dell'entità finanziaria che per i terzi siano attuati, documentati e regolarmente riesaminati.

2. Le entità finanziarie elaborano le politiche, le procedure, i protocolli e gli strumenti per proteggere le informazioni in transito di cui al paragrafo 1 sulla base dei risultati della classificazione dei dati approvata e della valutazione dei rischi informatici.

Sezione 7

Gestione delle modifiche e dei progetti relativi alle TIC

Articolo 15

Gestione dei progetti relativi alle TIC

1. Nell'ambito delle salvaguardie volte a preservare la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati, le entità finanziarie elaborano, documentano e attuano una politica di gestione dei progetti relativi alle TIC.

2. La politica di gestione dei progetti relativi alle TIC di cui al paragrafo 1 specifica gli elementi che garantiscono una gestione efficace dei progetti relativi alle TIC per l'acquisizione, la manutenzione e, se del caso, lo sviluppo dei sistemi di TIC dell'entità finanziaria.

3. La politica di gestione dei progetti relativi alle TIC di cui al paragrafo 1 contiene tutti gli elementi seguenti:

a) gli obiettivi dei progetti relativi alle TIC;

b) la gestione dei progetti relativi alle TIC, compresi ruoli e responsabilità;

c) la pianificazione, la tempistica e le fasi dei progetti relativi alle TIC;

d) la valutazione dei rischi dei progetti relativi alle TIC;

e) i pertinenti punti di controllo;

f) i requisiti per la gestione delle modifiche;

g) la verifica di tutti i requisiti, compresi quelli di sicurezza, e il relativo processo di approvazione al momento dell'installazione di un sistema di TIC nell'ambiente di produzione.

4. La politica di gestione dei progetti relativi alle TIC di cui al paragrafo 1 garantisce un'attuazione sicura del progetto relativo alle TIC attraverso la fornitura delle informazioni e delle competenze necessarie da parte dell'area aziendale o delle funzioni aziendali interessate da tale progetto.

5. Conformemente alla valutazione dei rischi dei progetti relativi alle TIC di cui al paragrafo 3, lettera d), la politica di gestione dei progetti relativi alle TIC di cui al paragrafo 1 prevede che la realizzazione e l'avanzamento dei progetti relativi alle TIC che hanno un impatto sulle funzioni essenziali o importanti dell'entità finanziaria e i rischi ad essi associati siano comunicati all'organo di gestione come segue:

a) singolarmente o in forma aggregata, a seconda dell'importanza e delle dimensioni dei progetti relativi alle TIC;

b) periodicamente e, se necessario, in base agli eventi.

Articolo 16

Acquisizione, sviluppo e manutenzione dei sistemi di TIC

1. Nell'ambito delle salvaguardie volte a preservare la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati, le entità finanziarie elaborano, documentano e attuano una politica che disciplina l'acquisizione, lo sviluppo e la manutenzione dei sistemi di TIC. Tale politica:

a) identifica le pratiche in materia di sicurezza e le metodologie relative all'acquisizione, allo sviluppo e alla manutenzione dei sistemi di TIC;

b) prevede l'identificazione di:

   i) specifiche tecniche e specifiche tecniche delle TIC, come definite all'articolo 2, punti 4) e 5), del regolamento (UE) n. 1025/2012;

   ii) requisiti relativi all'acquisizione, allo sviluppo e alla manutenzione dei sistemi di TIC, con particolare attenzione ai requisiti di sicurezza delle TIC e alla loro approvazione da parte della funzione commerciale pertinente e del proprietario della risorsa TIC, conformemente ai meccanismi di governance interna dell'entità finanziaria;

c) specifica le misure di attenuazione del rischio di alterazione non intenzionale o di manipolazione intenzionale dei sistemi di TIC durante lo sviluppo, la manutenzione e l'installazione di tali sistemi nell'ambiente di produzione.

2. Le entità finanziarie elaborano, documentano e attuano una procedura di acquisizione, sviluppo e manutenzione dei sistemi di TIC per il test e l'approvazione di tutti i sistemi di TIC prima del loro utilizzo e dopo la manutenzione, conformemente all'articolo 8, paragrafo 2, lettera b), punti v), vi) e vii). Il livello dei test deve essere commisurato alla criticità delle procedure aziendali e delle risorse TIC interessate. I test sono concepiti per verificare che i nuovi sistemi di TIC siano adeguati alle prestazioni previste, anche per quanto riguarda la qualità dei software sviluppati internamente.

Le controparti centrali, oltre ai requisiti di cui al primo comma, coinvolgono, se opportuno, nella progettazione e nella conduzione dei test di cui al primo comma:

a) i partecipanti diretti e i clienti;

b) le controparti centrali interoperabili;

c) altre parti interessate.

I depositari centrali di titoli, oltre ai requisiti di cui al primo comma, coinvolgono, se opportuno, nella progettazione e nella conduzione dei test di cui al primo comma:

a) gli utenti;

b) i fornitori di utenze critiche e di servizi critici;

c) altri depositari centrali di titoli;

d) altre infrastrutture di mercato;

e) qualsiasi altro ente con cui i depositari centrali di titoli abbiano identificato interdipendenze nella loro politica di continuità operativa.

3. La procedura di cui al paragrafo 2 prevede l'esecuzione di esami del codice sorgente che coprono sia i test statici che quelli dinamici. Tali test comprendono test di sicurezza per i sistemi e le applicazioni esposti a Internet conformemente all'articolo 8, paragrafo 2, lettera b), punti v), vi) e vii). Le entità finanziarie:

a) identificano e analizzano le vulnerabilità e le anomalie del codice sorgente;

b) adottano un piano d'azione per affrontare tali vulnerabilità e anomalie;

c) monitorano l'attuazione del piano d'azione.

4. La procedura di cui al paragrafo 2 prevede test di sicurezza dei pacchetti software da effettuare al più tardi nella fase di integrazione, conformemente all'articolo 8, paragrafo 2, lettera b), punti v), vi) e vii).

5. La procedura di cui al paragrafo 2 prevede che:

a) negli ambienti non di produzione siano memorizzati solo dati di produzione anonimizzati, pseudonimizzati o randomizzati;

b) le entità finanziarie tutelino l'integrità e la riservatezza dei dati negli ambienti non di produzione.

6. In deroga al paragrafo 5, la procedura di cui al paragrafo 2 può prevedere che i dati di produzione siano memorizzati solo per specifiche occasioni di test, per periodi di tempo limitati e previa approvazione della funzione competente e segnalazione di tali occasioni alla funzione di gestione dei rischi informatici.

7. La procedura di cui al paragrafo 2 prevede l'attuazione di controlli per proteggere l'integrità del codice sorgente dei sistemi di TIC sviluppati internamente o da un fornitore terzo di servizi TIC e forniti all'entità finanziaria da un fornitore terzo di servizi TIC.

8. La procedura di cui al paragrafo 2 prevede che il software proprietario e, ove possibile, il codice sorgente fornito da fornitori terzi di servizi TIC o proveniente da progetti open-source, siano analizzati e testati conformemente al paragrafo 3 prima di essere installati nell'ambiente di produzione.

9. I paragrafi da 1 a 8 del presente articolo si applicano anche ai sistemi di TIC sviluppati o gestiti da utenti esterni alla funzione TIC, utilizzando un approccio basato sul rischio.

Articolo 17

Gestione delle modifiche delle TIC

1. Nell'ambito delle salvaguardie volte a preservare la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati, le entità finanziarie includono nelle procedure per la gestione delle modifiche delle TIC di cui all'articolo 9, paragrafo 4, lettera e), del regolamento (UE) 2022/2554, per tutte le modifiche a software, hardware, componenti firmware, sistemi o parametri di sicurezza, tutti gli elementi seguenti:

a) una verifica del rispetto dei requisiti di sicurezza delle TIC;

b) i meccanismi per garantire l'indipendenza delle funzioni che approvano le modifiche e delle funzioni responsabili della richiesta e dell'attuazione di tali modifiche;

c) una chiara descrizione dei ruoli e delle responsabilità per garantire che:

   i) le modifiche siano specificate e pianificate;

   ii) sia prevista una transizione adeguata;

   iii) le modifiche siano testate e finalizzate in modo controllato;

   iv) vi sia un'efficace garanzia della qualità;

d) la documentazione e la comunicazione dei dettagli della modifica, tra cui:

   i) lo scopo e la portata della modifica;

   ii) la tempistica per l'implementazione della modifica;

   iii) i risultati attesi;

e) l'identificazione delle responsabilità e delle procedure di fall-back, comprese le responsabilità e le procedure per l'interruzione delle modifiche o per il ripristino in caso di modifiche non implementate correttamente;

f) procedure, protocolli e strumenti per la gestione delle modifiche di emergenza che forniscano adeguate salvaguardie;

g) procedure per documentare, rivalutare, valutare e approvare le modifiche di emergenza dopo la loro implementazione, comprese soluzioni workaround e patch;

h) l'identificazione dell'impatto potenziale di una modifica sulle misure di sicurezza delle TIC esistenti e la valutazione dell'eventualità che tale modifica richieda l'adozione di ulteriori misure di sicurezza delle TIC.

2. Dopo aver apportato modifiche significative ai loro sistemi di TIC, le controparti centrali e i depositari centrali di titoli sottopongono i loro sistemi di TIC a test rigorosi simulando condizioni di stress.

Se del caso, le controparti centrali coinvolgono nella progettazione e nella conduzione dei test di cui al primo comma:

a) i partecipanti diretti e i clienti;

b) le controparti centrali interoperabili;

c) altre parti interessate.

Se del caso, i depositari centrali di titoli coinvolgono nella progettazione e nella conduzione dei test di cui al primo comma:

a) gli utenti;

b) i fornitori di utenze critiche e di servizi critici;

c) altri depositari centrali di titoli;

d) altre infrastrutture di mercato;

e) qualsiasi altro ente con cui i depositari centrali di titoli abbiano identificato interdipendenze nella loro politica di continuità operativa delle TIC.

Sezione 8

Articolo 18

Sicurezza fisica e ambientale

1. Nell'ambito delle salvaguardie volte a preservare la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati, le entità finanziarie specificano, documentano e attuano una politica in materia di sicurezza fisica e ambientale. Le entità finanziarie elaborano tale politica alla luce del panorama delle minacce informatiche, conformemente alla classificazione effettuata ai sensi dell'articolo 8, paragrafo 1, del regolamento (UE) 2022/2554, e alla luce del profilo di rischio complessivo delle risorse TIC e dei patrimoni informativi accessibili.

2. La politica in materia di sicurezza fisica e ambientale di cui al paragrafo 1 contiene tutti gli elementi seguenti:

a) un riferimento alla sezione della politica sul controllo dei diritti di gestione degli accessi di cui all'articolo 21, primo comma, lettera g);

b) le misure per proteggere da attacchi, incidenti e minacce e pericoli ambientali i locali, i centri di elaborazione dati dell'entità finanziaria e le aree designate come sensibili dall'entità finanziaria, dove risiedono le risorse TIC e i patrimoni informativi;

c) le misure volte a garantire la sicurezza delle risorse TIC, sia all'interno che all'esterno dei locali dell'entità finanziaria, tenendo conto dei risultati della valutazione dei rischi informatici relativi alle risorse TIC pertinenti;

d) le misure volte a garantire la disponibilità, l'autenticità, l'integrità e la riservatezza delle risorse TIC, dei patrimoni informativi e dei dispositivi di controllo degli accessi fisici dell'entità finanziaria attraverso un'adeguata manutenzione;

e) le misure per preservare la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati, tra cui:

   i) una politica «*clear desk*» per i documenti cartacei;

   ii) una politica «*clear screen*» per le strutture di elaborazione delle informazioni.

Ai fini della lettera b), le misure di protezione dalle minacce e dai pericoli ambientali sono commisurate all'importanza dei locali, dei centri di elaborazione dati, delle aree designate come sensibili e alla criticità delle operazioni o dei sistemi di TIC ivi ubicati.

Ai fini della lettera c), la politica in materia di sicurezza fisica e ambientale di cui al paragrafo 1 contiene misure per fornire una protezione adeguata alle risorse TIC non presidiate.

CAPO II

Politica delle risorse umane e controllo degli accessi

Articolo 19

Politica delle risorse umane

Le entità finanziarie includono nella loro politica delle risorse umane o in altre politiche pertinenti tutti gli elementi seguenti relativi alla sicurezza delle TIC:

a) l'identificazione e l'assegnazione di eventuali responsabilità specifiche in materia di sicurezza delle TIC;

b) l'obbligo, per il personale dell'entità finanziaria e dei fornitori terzi di servizi TIC che utilizzano o accedono alle risorse TIC dell'entità finanziaria, di:

i) essere informati e rispettare le politiche, le procedure e i protocolli di sicurezza delle TIC dell'entità finanziaria;

ii) essere a conoscenza dei canali di segnalazione predisposti dall'entità finanziaria per l'individuazione di comportamenti anomali, compresi, se del caso, i canali di segnalazione stabiliti in linea con la direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio ([11]);

iii) per il personale, restituire all'entità finanziaria, alla cessazione del rapporto di lavoro, tutte le risorse TIC e i patrimoni informativi materiali in loro possesso che appartengono all'entità finanziaria.

Articolo 20

Gestione delle identità

1. Nell'ambito del controllo dei diritti di gestione degli accessi, le entità finanziarie elaborano, documentano e attuano politiche e procedure di gestione delle identità che garantiscano l'identificazione e l'autenticazione univoca delle persone fisiche e dei sistemi che accedono alle informazioni delle entità finanziarie per consentire l'assegnazione dei diritti di accesso utente in conformità dell'articolo 21.

2. Le politiche e le procedure di gestione delle identità di cui al paragrafo 1 contengono tutti gli elementi seguenti:

a) fatto salvo l'articolo 21, primo comma, lettera c), a ciascun membro del personale dell'entità finanziaria o del personale dei fornitori terzi di servizi TIC che accede ai patrimoni informativi e alle risorse TIC dell'entità finanziaria è assegnata un'identità univoca corrispondente a un account utente univoco;

b) un processo di gestione del ciclo di vita delle identità e degli account che gestisce la creazione, la modifica, il riesame e l'aggiornamento, la disattivazione temporanea e la cessazione di tutti gli account.

Ai fini della lettera a), le entità finanziarie conservano i registri di tutte le assegnazioni di identità. Tali registri sono conservati in seguito a una riorganizzazione dell'entità finanziaria o dopo la fine del rapporto contrattuale, fatti salvi gli obblighi di conservazione previsti dal diritto dell'Unione e nazionale applicabile.

Ai fini della lettera b), le entità finanziarie adottano, ove possibile e opportuno, soluzioni automatizzate per il processo di gestione del ciclo di vita delle identità.

Articolo 21

Controllo degli accessi

Nell'ambito del controllo dei diritti di gestione degli accessi, le entità finanziarie elaborano, documentano e attuano una politica che contiene tutti gli elementi seguenti:

a) l'assegnazione dei diritti di accesso alle risorse TIC in base ai principi della necessità di sapere, della necessità di usare e del privilegio minimo, anche per l'accesso remoto e di emergenza;

b) una separazione dei compiti, concepita per impedire l'accesso ingiustificato ai dati critici o per impedire l'assegnazione di combinazioni di diritti di accesso che potrebbero essere utilizzati per eludere i controlli;

c) una disposizione sulla responsabilità degli utenti, limitando per quanto possibile l'uso di account utente generici e condivisi e garantendo che gli utenti siano in ogni momento identificabili per le azioni eseguite nei sistemi di TIC;

([11]) Direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione (GU L 305 del 26.11.2019, pag. 17, ELI: http://data.europa.eu/eli/dir/2019/1937/oj).

d) una disposizione sulle restrizioni di accesso alle risorse TIC, che definisca i controlli e gli strumenti per prevenire l'accesso non autorizzato;

e) procedure di gestione degli account per concedere, modificare o revocare i diritti di accesso per gli account utente e generici, compresi gli account amministratore generici, che comprendano disposizioni relative a tutti gli aspetti seguenti:

   i) l'assegnazione di ruoli e responsabilità per la concessione, il riesame e la revoca dei diritti di accesso;

   ii) l'assegnazione di accessi privilegiati, di emergenza e di amministratore in base alla necessità di utilizzo o ad hoc per tutti i sistemi di TIC;

   iii) la revoca dei diritti di accesso senza indebito ritardo al termine del rapporto di lavoro o quando l'accesso non è più necessario;

   iv) l'aggiornamento dei diritti di accesso quando sono necessarie modifiche e almeno una volta all'anno per tutti i sistemi di TIC diversi da quelli che supportano funzioni essenziali o importanti e almeno ogni sei mesi per i sistemi di TIC che supportano funzioni essenziali o importanti;

f) i metodi di autenticazione, che comprendano tutti gli aspetti seguenti:

   i) l'uso di metodi di autenticazione commisurati alla classificazione effettuata in conformità dell'articolo 8, paragrafo 1, del regolamento (UE) 2022/2554 e al profilo di rischio complessivo delle risorse TIC, tenendo conto delle pratiche più avanzate;

   ii) l'uso di metodi di autentificazione robusti, conformemente alle pratiche e alle tecniche più avanzate, per l'accesso remoto alla rete dell'entità finanziaria, per l'accesso privilegiato, per l'accesso alle risorse TIC che supportano funzioni essenziali o importanti o per le risorse TIC accessibili al pubblico;

g) le misure di controllo degli accessi fisici, tra cui:

   i) l'identificazione e il logging delle persone fisiche autorizzate ad accedere ai locali, ai centri di elaborazione dati, alle aree designate come sensibili dall'entità finanziaria in cui risiedono le risorse TIC e i patrimoni informativi;

   ii) la concessione dei diritti di accesso fisico alle risorse TIC critiche solo alle persone autorizzate, secondo i principi della necessità di sapere e del privilegio minimo, e su base ad hoc;

   iii) il monitoraggio dell'accesso fisico ai locali, ai centri di elaborazione dati e alle aree designate come sensibili dall'entità finanziaria in cui risiedono le risorse TIC, i patrimoni informativi o entrambi;

   iv) il riesame dei diritti di accesso fisico per garantire la revoca tempestiva dei diritti di accesso non necessari.

Ai fini della lettera e), punto i), le entità finanziarie stabiliscono il periodo di conservazione, tenendo conto degli obiettivi aziendali e di sicurezza delle informazioni, dei motivi della registrazione dell'evento nei log e dei risultati della valutazione dei rischi informatici.

Ai fini della lettera e), punto ii), le entità finanziarie utilizzano, ove possibile, account dedicati per lo svolgimento di compiti amministrativi sui sistemi di TIC. Ove possibile e opportuno, le entità finanziarie adottano soluzioni automatizzate per la gestione degli accessi privilegiati.

Ai fini della lettera g), punto i), l'identificazione e il logging sono commisurati all'importanza dei locali, dei centri di elaborazione dati, delle aree designate come sensibili e alla criticità delle operazioni o dei sistemi di TIC ivi ubicati.

Ai fini della lettera g), punto iii), il monitoraggio è commisurato alla classificazione effettuata conformemente all'articolo 8, paragrafo 1, del regolamento (UE) 2022/2554 e alla criticità dell'area cui si accede.

CAPO III

Individuazione degli incidenti connessi alle TIC e risposta agli stessi

Articolo 22

Politica di gestione degli incidenti connessi alle TIC

Nell'ambito dei meccanismi per individuare le attività anomale, compresi i problemi di prestazione della rete delle TIC e gli incidenti connessi alle TIC, le entità finanziarie elaborano, documentano e attuano una politica relativa agli incidenti connessi alle TIC attraverso la quale:

a) documentano il processo di gestione degli incidenti connessi alle TIC di cui all'articolo 17 del regolamento (UE) 2022/2554;

b) stilano un elenco dei pertinenti contatti con le funzioni interne e i portatori di interessi esterni che sono direttamente coinvolti nella sicurezza delle operazioni riguardanti le TIC, anche per quanto riguarda:

   i) l'individuazione e il monitoraggio delle minacce informatiche;

   ii) l'individuazione di attività anomale;

   iii) la gestione delle vulnerabilità;

c) definiscono, attuano e gestiscono meccanismi tecnici, organizzativi e operativi per supportare il processo di gestione degli incidenti connessi alle TIC, compresi i meccanismi per consentire una tempestiva individuazione di attività e comportamenti anomali conformemente all'articolo 23 del presente regolamento;

d) conservano tutte le prove relative agli incidenti connessi alle TIC per un periodo non superiore a quello necessario per le finalità per cui i dati sono raccolti, commisurato alla criticità delle funzioni commerciali interessate, dei processi di supporto e dei patrimoni informativi e delle risorse TIC, conformemente all'articolo 15 del regolamento delegato (UE) 2024/1772 della Commissione ([12]) e a qualsiasi obbligo di conservazione applicabile ai sensi del diritto dell'Unione;

e) definiscono e attuano meccanismi di analisi degli incidenti significativi o ricorrenti connessi alle TIC e degli schemi relativi al numero e al verificarsi di incidenti connessi alle TIC.

Ai fini della lettera d), le entità finanziarie conservano le prove di cui alla stessa lettera in modo sicuro.

Articolo 23

Individuazione di attività anomale e criteri per l'individuazione degli incidenti connessi alle TIC e la risposta agli stessi

1. Le entità finanziarie stabiliscono ruoli e responsabilità chiari per individuare e rispondere efficacemente agli incidenti connessi alle TIC e alle attività anomale.

2. Il meccanismo per individuare tempestivamente le attività anomale, compresi i problemi di prestazione della rete TIC e gli incidenti connessi alle TIC, di cui all'articolo 10, paragrafo 1, del regolamento (UE) 2022/2554, consente alle entità finanziarie di:

a) raccogliere, monitorare e analizzare tutti gli elementi seguenti:

   i) i fattori interni ed esterni, compresi almeno i log acquisiti ai sensi dell'articolo 12 del presente regolamento, le informazioni provenienti dalle funzioni commerciali e TIC e qualsiasi problema segnalato dagli utenti dell'entità finanziaria;

   ii) le potenziali minacce informatiche interne ed esterne, considerando gli scenari comunemente utilizzati dagli attori delle minacce e quelli basati sulle attività di analisi delle minacce;

([12]) Regolamento delegato (UE) 2024/1772 della Commissione, del 13 marzo 2024, che integra il regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione che specificano i criteri per la classificazione degli incidenti connessi alle TIC e delle minacce informatiche, stabiliscono le soglie di rilevanza e specificano i dettagli delle segnalazioni di gravi incidenti (GU L, 2024/1772, 25.6.2024, ELI: http://data.europa.eu/eli/reg_del/2024/1772/oj).

iii) la notifica, da parte di un fornitore terzo di servizi TIC dell'entità finanziaria, di incidenti connessi alle TIC individuati nei sistemi e nelle reti TIC del fornitore terzo di servizi TIC e che possono avere un impatto sull'entità finanziaria;

b) identificare attività e comportamenti anomali e applicare strumenti che generino allarmi per attività e comportamenti anomali, almeno per le risorse TIC e i patrimoni informativi a supporto di funzioni essenziali o importanti;

c) dare priorità agli allarmi di cui alla lettera b) per consentire la gestione degli incidenti connessi alle TIC individuati entro i tempi di risoluzione previsti, come specificato dalle entità finanziarie, sia durante che al di fuori dell'orario di lavoro;

d) registrare, analizzare e valutare qualsiasi informazione pertinente su tutte le attività e i comportamenti anomali in modo automatico o manuale.

Ai fini della lettera b), gli strumenti di cui alla stessa lettera contengono gli strumenti che forniscono allarmi automatici basati su regole predefinite per identificare le anomalie che incidono sulla completezza e sull'integrità delle fonti di dati o dell'acquisizione dei log.

3. Le entità finanziarie proteggono qualsiasi registrazione delle attività anomale da manomissioni e accessi non autorizzati a riposo, in transito e, se del caso, in uso.

4. Le entità finanziarie registrano nei log tutte le informazioni pertinenti per ciascuna attività anomala individuata in modo da consentire:

a) l'identificazione della data e dell'ora in cui si è verificata l'attività anomala;

b) l'identificazione della data e dell'ora di individuazione dell'attività anomala;

c) l'identificazione del tipo di attività anomala.

5. Per l'avvio dei processi di individuazione degli incidenti connessi alle TIC e di risposta agli stessi di cui all'articolo 10, paragrafo 2, del regolamento (UE) 2022/2554, le entità finanziarie considerano tutti i criteri seguenti:

a) indicazioni del fatto che in un sistema o in una rete TIC possa essere stata condotta un'attività malevola o che tale sistema o rete TIC possa essere stato compromesso;

b) perdite di dati individuate in relazione alla disponibilità, all'autenticità, all'integrità e alla riservatezza dei dati;

c) impatto negativo individuato sulle operazioni e sulle transazioni dell'entità finanziaria;

d) indisponibilità dei sistemi e della rete TIC;

6. Ai fini del paragrafo 5, le entità finanziarie considerano anche la criticità dei servizi interessati.

CAPO IV

Gestione della continuità operativa delle TIC

Articolo 24

Componenti della politica di continuità operativa delle TIC

1. Le entità finanziarie includono nella loro politica di continuità operativa delle TIC di cui all'articolo 11, paragrafo 1, del regolamento (UE) 2022/2554 tutti gli elementi seguenti:

a) una descrizione:

i) degli obiettivi della politica di continuità operativa delle TIC, compresa l'interrelazione tra le TIC e la continuità operativa complessiva, e tenendo conto dei risultati dell'analisi dell'impatto sulle attività aziendali (*Business Impact Analysis*, BIA) di cui all'articolo 11, paragrafo 5, del regolamento (UE) 2022/2554;

ii) dell'ambito di applicazione degli accordi, dei piani, delle procedure e dei meccanismi di continuità operativa delle TIC, comprese le limitazioni e le esclusioni;

iii) dell'arco di tempo che deve essere coperto dagli accordi, dai piani, dalle procedure e dai meccanismi di continuità operativa delle TIC;

iv) dei criteri di attivazione e disattivazione dei piani di continuità operativa delle TIC, dei piani di risposta e ripristino relativi alle TIC e dei piani di comunicazione delle crisi;

b) disposizioni in materia di:

i) governance e organizzazione per l'attuazione della politica di continuità operativa delle TIC, compresi ruoli, responsabilità e procedure di attivazione dei livelli successivi di intervento, garantendo la disponibilità di risorse sufficienti;

ii) allineamento tra i piani di continuità operativa delle TIC e i piani generali di continuità operativa, per quanto riguarda almeno tutti gli aspetti seguenti:

1) i potenziali scenari di disfunzione, compresi gli scenari di cui all'articolo 26, paragrafo 2, del presente regolamento;

2) gli obiettivi di ripristino, specificando che l'entità finanziaria è in grado di ripristinare l'operatività delle proprie funzioni essenziali o importanti dopo le perturbazioni rispettando un obiettivo in materia di tempi di ripristino e un obiettivo in materia di punti di ripristino;

iii) l'elaborazione di piani di continuità operativa TIC per gravi perturbazioni dell'attività all'interno di tali piani, e la definizione delle priorità delle azioni di continuità operativa delle TIC utilizzando un approccio basato sul rischio;

iv) l'elaborazione, il test e il riesame dei piani di risposta e ripristino relativi alle TIC, conformemente agli articoli 25 e 26 del presente regolamento;

v) il riesame dell'efficacia degli accordi, dei piani, delle procedure e dei meccanismi di continuità operativa delle TIC attuati, conformemente all'articolo 26 del presente regolamento;

vi) l'allineamento della politica di continuità operativa delle TIC rispetto a:

1) la politica di comunicazione di cui all'articolo 14, paragrafo 2, del regolamento (UE) 2022/2554;

2) le azioni di comunicazione e gestione delle crisi di cui all'articolo 11, paragrafo 2, lettera e), del regolamento (UE) 2022/2554.

2. Oltre ai requisiti di cui al paragrafo 1, le controparti centrali provvedono affinché la loro politica di continuità operativa delle TIC:

a) preveda un tempo massimo di ripristino delle funzioni essenziali non superiore a due ore;

b) tenga conto dei collegamenti esterni e delle interdipendenze all'interno delle infrastrutture finanziarie, comprese le sedi di negoziazione compensate dalla controparte centrale, i sistemi di pagamento e di regolamento titoli e gli enti creditizi utilizzati dalla controparte centrale o da una controparte centrale collegata;

c) preveda la predisposizione di dispositivi per:

i) garantire la continuità delle funzioni essenziali o importanti della controparte centrale sulla base di scenari catastrofici;

ii) mantenere un sito secondario per il trattamento dati in grado di garantire la continuità delle funzioni essenziali o importanti della controparte centrale, identico al sito primario;

iii) mantenere o avere accesso immediato a un sito operativo secondario, per consentire al personale di garantire la continuità del servizio in caso di indisponibilità del sito primario;

iv) considerare la necessità di altri siti per il trattamento dati, in particolare se la diversità dei profili di rischio dei siti primari e secondari non garantisce sufficientemente che gli obiettivi di continuità operativa della controparte centrale saranno raggiunti in tutti gli scenari.

Ai fini della lettera a), le controparti centrali completano le procedure e i pagamenti di fine giornata all'ora e nel giorno richiesti in tutte le circostanze.

Ai fini della lettera c), punto i), i dispositivi di cui a tale punto riguardano la disponibilità di risorse umane adeguate, il periodo massimo di inutilizzabilità delle funzioni essenziali e il passaggio e ripristino in un sito secondario.

Ai fini della lettera c), punto ii), il sito secondario per il trattamento dati di cui alla suddetta lettera ha un profilo di rischio geografico distinto da quello del sito primario.

3. Oltre ai requisiti di cui al paragrafo 1, i depositari centrali di titoli provvedono affinché la loro politica di continuità operativa delle TIC:

a) tenga conto di tutti i collegamenti e le interdipendenze con gli utenti, i fornitori di utenze critiche e di servizi critici, gli altri depositari centrali di titoli e altre infrastrutture di mercato;

b) preveda che gli accordi in materia di continuità operativa delle TIC garantiscano che l'obiettivo di tempo di ripristino per le funzioni essenziali o importanti non sia superiore a due ore.

4. Oltre ai requisiti di cui al paragrafo 1, le sedi di negoziazione provvedono affinché la loro politica di continuità operativa delle TIC garantisca che:

a) la negoziazione possa riprendere entro approssimativamente due ore dall'evento perturbatore;

b) la quantità massima di dati che potrebbe essere persa dai servizi informatici della sede di negoziazione dopo un evento perturbatore sia prossima allo zero.

Articolo 25

Test dei piani di continuità operativa delle TIC

1. Nel testare i piani di continuità operativa delle TIC ai sensi dell'articolo 11, paragrafo 6, del regolamento (UE) 2022/2554, le entità finanziarie tengono conto dell'analisi dell'impatto sulle attività aziendali (BIA) dell'entità finanziaria e della valutazione dei rischi informatici di cui all'articolo 3, paragrafo 1, lettera b), del presente regolamento.

2. Le entità finanziarie valutano, nel testare i loro piani di continuità operativa delle TIC di cui al paragrafo 1, se sono in grado di garantire la continuità delle funzioni essenziali o importanti dell'entità finanziaria. I test:

a) sono effettuati sulla base di scenari di test che simulano potenziali perturbazioni, compresa un'adeguata serie di scenari gravi ma plausibili;

b) comprendono il test dei servizi TIC forniti da fornitori terzi di servizi TIC, ove applicabile;

c) per le entità finanziarie diverse dalle microimprese di cui all'articolo 11, paragrafo 6, secondo comma, del regolamento (UE) 2022/2554, contengono scenari di passaggio dall'infrastruttura TIC primaria alla capacità ridondante, ai backup e alle attrezzature ridondanti;

d) sono concepiti per mettere in discussione i presupposti su cui si basano i piani di continuità operativa, compresi i meccanismi di governance e i piani di comunicazione delle crisi;

e) contengono procedure per verificare la capacità del personale delle entità finanziarie, dei fornitori terzi di servizi TIC, dei sistemi di TIC e dei servizi TIC di rispondere adeguatamente agli scenari debitamente presi in considerazione conformemente all'articolo 26, paragrafo 2.

Ai fini della lettera a), le entità finanziarie includono sempre nei test gli scenari considerati per l'elaborazione dei piani di continuità operativa.

Ai fini della lettera b), le entità finanziarie prendono in debita considerazione gli scenari legati all'insolvenza o a disfunzioni dei fornitori terzi di servizi TIC o ai rischi politici nelle giurisdizioni dei fornitori terzi di servizi TIC, se del caso.

Ai fini della lettera c), il test verifica se almeno le funzioni essenziali o importanti possono essere eseguite in modo appropriato per un periodo di tempo sufficiente e se è possibile ripristinare il normale funzionamento.

3. Oltre ai requisiti di cui al paragrafo 2, le controparti centrali coinvolgono nei test dei loro piani di continuità operativa delle TIC, di cui al paragrafo 1:

a) i partecipanti diretti;

b) i fornitori esterni;

c) i pertinenti enti dell'infrastruttura finanziaria con cui le controparti centrali hanno identificato interdipendenze nelle loro politiche di continuità operativa.

4. Oltre ai requisiti di cui al paragrafo 2, i depositari centrali di titoli coinvolgono nei test dei loro piani di continuità operativa delle TIC, di cui al paragrafo 1, a seconda dei casi:

a) gli utenti dei depositari centrali di titoli;

b) i fornitori di utenze critiche e di servizi critici;

c) altri depositari centrali di titoli;

d) altre infrastrutture di mercato;

e) qualsiasi altro ente con cui i depositari centrali di titoli abbiano identificato interdipendenze nella loro politica di continuità operativa.

5. Le entità finanziarie documentano i risultati dei test di cui al paragrafo 1. Tutte le carenze individuate in seguito a tali test sono analizzate, affrontate e comunicate all'organo di gestione.

Articolo 26

Piani di risposta e ripristino relativi alle TIC

1. Nell'elaborare i piani di risposta e ripristino relativi alle TIC di cui all'articolo 11, paragrafo 3, del regolamento (UE) 2022/2554, le entità finanziarie tengono conto dei risultati dell'analisi dell'impatto sulle attività aziendali (BIA) dell'entità finanziaria. Il piano di risposta e ripristino relativo alle TIC:

a) specifica le condizioni che ne determinano l'attivazione o la disattivazione e le eventuali eccezioni per tale attivazione o disattivazione;

b) descrive le azioni da intraprendere per garantire la disponibilità, l'integrità, la continuità e il ripristino almeno dei sistemi e dei servizi TIC a supporto di funzioni essenziali o importanti dell'entità finanziaria;

c) è concepito per soddisfare gli obiettivi di ripristino delle operazioni delle entità finanziarie;

d) è documentato e reso disponibile al personale coinvolto nell'esecuzione dei piani di risposta e ripristino relativi alle TIC ed è facilmente accessibile in caso di emergenza;

e) prevede opzioni di ripristino sia a breve che a lungo termine, compreso il ripristino parziale dei sistemi;

f) stabilisce gli obiettivi dei piani di risposta e ripristino relativi alle TIC e le condizioni per dichiarare la proficua esecuzione di tali piani.

Ai fini della lettera d), le entità finanziarie specificano chiaramente ruoli e responsabilità.

2. I piani di risposta e ripristino relativi alle TIC di cui al paragrafo 1 identificano gli scenari pertinenti, compresi quelli di gravi perturbazioni delle attività e di accresciuta probabilità del verificarsi di una perturbazione. Tali piani sviluppano scenari basati sulle informazioni correnti relative alle minacce e sugli insegnamenti tratti da precedenti eventi di perturbazioni delle attività. Le entità finanziarie tengono debitamente conto di tutti gli scenari seguenti:

a) attacchi informatici e passaggio tra l'infrastruttura TIC primaria e la capacità ridondante, i backup e le attrezzature ridondanti;

b) scenari in cui la qualità dell'esercizio di una funzione essenziale o importante si deteriora a un livello inaccettabile o viene meno, e considerano adeguatamente il potenziale impatto dell'insolvenza o di altre disfunzioni di pertinenti fornitori terzi di servizi TIC;

c) disfunzione parziale o totale dei locali, compresi gli uffici e le sedi aziendali, e dei centri di elaborazione dati;

d) disfunzione sostanziale delle risorse TIC o dell'infrastruttura di comunicazione;

e) non disponibilità di un numero critico di personale o di membri del personale incaricati di garantire la continuità delle operazioni;

f) impatto dei cambiamenti climatici e degli eventi legati al degrado ambientale, delle catastrofi naturali, delle pandemie e degli attacchi fisici, comprese le intrusioni e gli attacchi terroristici;

g) attacchi interni;

h) instabilità politica e sociale anche, se del caso, nella giurisdizione del fornitore terzo di servizi TIC e nel luogo in cui i dati sono memorizzati ed elaborati;

i) interruzioni di corrente generalizzate.

3. Qualora non sia possibile attuare le misure primarie di ripristino a breve termine a causa di costi, rischi, logistica o circostanze impreviste, i piani di risposta e ripristino relativi alle TIC di cui al paragrafo 1 prendono in considerazione opzioni alternative.

4. Nell'ambito dei piani di risposta e ripristino relativi alle TIC di cui al paragrafo 1, le entità finanziarie considerano e attuano misure di continuità per attenuare le disfunzioni dei fornitori terzi di servizi TIC a supporto di funzioni essenziali o importanti dell'entità finanziaria.

CAPO V

Relazione sul riesame del quadro per la gestione dei rischi informatici

Articolo 27

Formato e contenuto della relazione sul riesame del quadro per la gestione dei rischi informatici

1. Le entità finanziarie presentano la relazione sul riesame del quadro per la gestione dei rischi informatici di cui all'articolo 6, paragrafo 5, del regolamento (UE) 2022/2554 in un formato elettronico che permetta la ricerca al suo interno.

2. Le entità finanziarie includono nella relazione di cui al paragrafo 1 tutte le informazioni seguenti:

a) una sezione introduttiva che:

   i) identifica chiaramente l'entità finanziaria oggetto della relazione e descrive la sua struttura di gruppo, se pertinente;

   ii) descrive il contesto della relazione in termini di natura, portata e complessità dei servizi, delle attività e delle operazioni dell'entità finanziaria, della sua organizzazione, delle funzioni essenziali identificate, della strategia, dei principali progetti o attività in corso, dei rapporti e della sua dipendenza da servizi e sistemi di TIC interni e appaltati o delle implicazioni che una perdita totale o un grave degrado di tali sistemi avrebbe in termini di funzioni essenziali o importanti e di efficienza del mercato;

   iii) riassume le modifiche di rilievo apportate al quadro per la gestione dei rischi informatici rispetto alla precedente relazione presentata;

   iv) fornisce una sintesi di livello esecutivo del profilo di rischio informatico corrente e a breve termine, del panorama delle minacce, della valutazione dell'efficacia dei controlli e della posizione in materia di sicurezza dell'entità finanziaria;

b) la data di approvazione della relazione da parte dell'organo di gestione dell'entità finanziaria;

c) una descrizione del motivo del riesame del quadro per la gestione dei rischi informatici conformemente all'articolo 6, paragrafo 5, del regolamento (UE) 2022/2554;

d) le date di inizio e fine del periodo del riesame;

e) l'indicazione della funzione responsabile del riesame;

f) una descrizione delle modifiche e dei miglioramenti di rilievo apportati al quadro per la gestione dei rischi informatici rispetto al riesame precedente;

g) una sintesi delle risultanze del riesame e un'analisi e una valutazione dettagliate della gravità delle debolezze, delle carenze e delle lacune del quadro per la gestione dei rischi informatici durante il periodo del riesame;

h) una descrizione delle misure volte ad affrontare le debolezze, le carenze e le lacune identificate, che comprenda tutti gli elementi seguenti:

   i) una sintesi delle misure adottate per porre rimedio alle debolezze, alle carenze e alle lacune identificate;

   ii) una data prevista per l'attuazione delle misure e le date relative al controllo interno dell'attuazione, comprese le informazioni sullo stato di avanzamento dell'attuazione di tali misure alla data di redazione della relazione, spiegando, se del caso, se esiste il rischio di non rispettare le scadenze;

   iii) gli strumenti da utilizzare e l'identificazione della funzione responsabile dell'esecuzione delle misure, specificando se gli strumenti e le funzioni sono interni o esterni;

   iv) una descrizione dell'impatto delle modifiche previste dalle misure sulle risorse di bilancio, umane e materiali dell'entità finanziaria, comprese le risorse dedicate all'attuazione di eventuali misure correttive;

   v) le informazioni sul processo di informazione dell'autorità competente, se del caso;

   vi) nel caso in cui le debolezze, le carenze o le lacune identificate non siano oggetto di misure correttive, una spiegazione dettagliata dei criteri utilizzati per analizzare l'impatto di tali debolezze, carenze o lacune, per valutare il relativo rischio informatico residuo e dei criteri utilizzati per accettare il relativo rischio residuo;

i) informazioni sugli ulteriori sviluppi previsti del quadro per la gestione dei rischi informatici;

j) le conclusioni derivanti dal riesame del quadro per la gestione dei rischi informatici;

k) informazioni relative ai riesami precedenti, tra cui:

   i) un elenco dei riesami precedenti effettuati fino a quel momento;

   ii) se del caso, lo stato di attuazione delle misure correttive identificate nell'ultima relazione;

   iii) nel caso in cui le misure correttive proposte in occasione di riesami precedenti si siano rivelate inefficaci o abbiano creato problemi imprevisti, una descrizione di come tali misure correttive potrebbero essere migliorate o di tali problemi imprevisti;

l) le fonti di informazione utilizzate per la preparazione della relazione, compresi tutti gli elementi seguenti:

   i) per le entità finanziarie diverse dalle microimprese di cui all'articolo 6, paragrafo 6, del regolamento (UE) 2022/2554, i risultati degli audit interni;

   ii) i risultati delle valutazioni della conformità;

   iii) i risultati dei test di resilienza operativa digitale e, se del caso, i risultati di test avanzati, basati su test di penetrazione guidati dalla minaccia (*threat-led penetration testing* — TLPT), di strumenti, sistemi e processi TIC;

   iv) fonti esterne.

Ai fini della lettera c), se il riesame è stato avviato a seguito di istruzioni delle autorità di vigilanza o di conclusioni scaturite da pertinenti test di resilienza operativa digitale o da processi di audit, la relazione contiene riferimenti espliciti a tali istruzioni o conclusioni, in modo da consentire l'identificazione del motivo per cui è stato avviato il riesame. Se il riesame è stato avviato a seguito di incidenti connessi alle TIC, la relazione contiene l'elenco di tutti gli incidenti connessi alle TIC con l'analisi delle cause di fondo.

Ai fini della lettera f), la descrizione contiene un'analisi dell'impatto delle modifiche sulla strategia di resilienza operativa digitale, sul quadro di controllo interno delle TIC e sul quadro per la gestione dei rischi informatici dell'entità finanziaria.

TITOLO III

QUADRO SEMPLIFICATO PER LA GESTIONE DEI RISCHI INFORMATICI PER LE ENTITÀ FINANZIARIE DI CUI ALL'ARTICOLO 16, PARAGRAFO 1, DEL REGOLAMENTO (UE) 2022/2554

CAPO I

Quadro semplificato per la gestione dei rischi informatici

Articolo 28

Governance e organizzazione

1. Le entità finanziarie di cui all'articolo 16, paragrafo 1, del regolamento (UE) 2022/2554 predispongono un quadro di gestione e di controllo interno che garantisce una gestione efficace e prudente dei rischi informatici al fine di acquisire un elevato livello di resilienza operativa digitale.

2. Le entità finanziarie di cui al paragrafo 1, nell'ambito del quadro semplificato per la gestione dei rischi informatici, provvedono affinché il loro organo di gestione:

a) abbia la responsabilità generale di assicurare che il quadro semplificato per la gestione dei rischi informatici consenta di realizzare la strategia aziendale dell'entità finanziaria conformemente alla sua propensione al rischio e garantisca che il rischio informatico sia considerato in tale contesto;

b) definisca chiaramente ruoli e responsabilità per tutti i compiti connessi alle TIC;

c) definisca gli obiettivi di sicurezza delle informazioni e i requisiti in materia di TIC;

d) approvi, supervisioni e riesamini periodicamente:

   i) la classificazione dei patrimoni informativi dell'entità finanziaria di cui all'articolo 30, paragrafo 1, del presente regolamento, l'elenco dei principali rischi identificati, l'analisi dell'impatto sull'attività e le relative politiche;

   ii) i piani di continuità operativa dell'entità finanziaria e le misure di risposta e recupero di cui all'articolo 16, paragrafo 1, lettera f), del regolamento (UE) 2022/2554;

e) assegni e riesamini almeno una volta all'anno le risorse finanziarie necessarie per soddisfare le esigenze di resilienza operativa digitale dell'entità finanziaria rispetto a tutti i tipi di risorse, compresi i pertinenti programmi di sensibilizzazione sulla sicurezza delle TIC e le attività di formazione sulla resilienza operativa digitale nonché le competenze in materia di TIC per tutto il personale;

f) specifichi e attui le politiche e le misure di cui ai capi I, II e III del presente titolo per identificare, valutare e gestire i rischi informatici a cui l'entità finanziaria è esposta;

g) identifichi e attui le procedure, i protocolli TIC e gli strumenti necessari per proteggere tutti i patrimoni informativi e le risorse TIC;

h) garantisca che il personale dell'entità finanziaria sia tenuto aggiornato con conoscenze e competenze adeguate per comprendere e valutare i rischi informatici e il loro impatto sulle operazioni dell'entità finanziaria, in funzione del rischio informatico gestito;

i) stabilisca le modalità di comunicazione, tra cui la frequenza, la forma e il contenuto delle relazioni all'organo di gestione sulla sicurezza delle informazioni e sulla resilienza operativa digitale.

3. Le entità finanziarie di cui al paragrafo 1 possono, conformemente alla normativa settoriale dell'Unione e nazionale, esternalizzare a fornitori infragruppo di servizi TIC o a fornitori terzi di servizi TIC i compiti di verifica della conformità ai requisiti in materia di gestione dei rischi informatici. In caso di esternalizzazione, le entità finanziarie rimangono pienamente responsabili di verificare la conformità ai requisiti in materia di gestione dei rischi informatici.

4. Le entità finanziarie di cui al paragrafo 1 garantiscono un'opportuna separazione e indipendenza tra funzioni di controllo e funzioni di audit interno.

5. Le entità finanziarie di cui al paragrafo 1 provvedono affinché il loro quadro semplificato per la gestione dei rischi informatici sia sottoposto a verifiche di audit interne effettuate da addetti all'audit in linea con i piani di audit delle entità finanziarie. Tali addetti all'audit possiedono conoscenze, competenze ed esperienze adeguate in materia di rischi informatici e sono indipendenti. La frequenza e l'oggetto delle verifiche di audit in materia di TIC sono commisurati ai rischi connessi alle TIC cui è esposta l'entità finanziaria.

6. Sulla base delle risultanze della verifica di audit di cui al paragrafo 5, le entità finanziarie di cui al paragrafo 1 provvedono a verificare e correggere tempestivamente le criticità emerse da tale verifica.

Articolo 29

Politica e misure di sicurezza delle informazioni

1. Le entità finanziarie di cui all'articolo 16, paragrafo 1, del regolamento (UE) 2022/2554 elaborano, documentano e attuano una politica di sicurezza delle informazioni nel contesto del quadro semplificato per la gestione dei rischi informatici. La politica di sicurezza delle informazioni specifica le norme e i principi di alto livello per tutelare la riservatezza, l'integrità, la disponibilità e l'autenticità dei dati e dei servizi che le entità finanziarie forniscono.

2. Sulla base della politica di sicurezza delle informazioni di cui al paragrafo 1, le entità finanziarie di cui al paragrafo 1 stabiliscono e attuano misure di sicurezza delle TIC per attenuare la loro esposizione al rischio informatico, comprese le misure di attenuazione messe in atto dai fornitori terzi di servizi TIC.

Le misure di sicurezza delle TIC includono tutte le misure di cui agli articoli da 30 a 38.

Articolo 30

Classificazione dei patrimoni informativi e delle risorse TIC

1. Nell'ambito del quadro semplificato per la gestione dei rischi informatici di cui all'articolo 16, paragrafo 1, lettera a), del regolamento (UE) 2022/2554, le entità finanziarie di cui al paragrafo 1 di tale articolo identificano, classificano e documentano tutte le funzioni essenziali o importanti, i patrimoni informativi e le risorse TIC che le supportano e le loro interdipendenze. Le entità finanziarie riesaminano tale identificazione e classificazione in base alle necessità.

2. Le entità finanziarie di cui al paragrafo 1 identificano tutte le funzioni essenziali o importanti supportate da fornitori terzi di servizi TIC.

Articolo 31

Gestione dei rischi informatici

1. Le entità finanziarie di cui all'articolo 16, paragrafo 1, del regolamento (UE) 2022/2554 includono nel loro quadro semplificato per la gestione dei rischi informatici tutti gli elementi seguenti:

a) la determinazione dei livelli di tolleranza per i rischi informatici, conformemente alla propensione al rischio dell'entità finanziaria;

b) l'identificazione e la valutazione dei rischi informatici a cui l'entità finanziaria è esposta;

c) la specifica delle strategie di attenuazione almeno per i rischi informatici che non rientrano nei livelli di tolleranza per i rischi dell'entità finanziaria;

d) il monitoraggio dell'efficacia delle strategie di attenuazione di cui alla lettera c);

e) l'identificazione e la valutazione dei rischi informatici e di sicurezza delle informazioni derivanti da qualsiasi modifica di rilievo del sistema di TIC o dei servizi TIC, dei processi o delle procedure e dai risultati dei test di sicurezza delle TIC e dopo qualsiasi incidente grave connesso alle TIC.

2. Le entità finanziarie di cui al paragrafo 1 effettuano e documentano periodicamente la valutazione dei rischi informatici in funzione del profilo di rischio informatico delle entità finanziarie.

3. Le entità finanziarie di cui al paragrafo 1 monitorano costantemente le minacce e le vulnerabilità rilevanti per le loro funzioni essenziali o importanti, nonché per i patrimoni informativi e le risorse TIC, e riesaminano regolarmente gli scenari di rischio che hanno un impatto su tali funzioni essenziali o importanti.

4. Le entità finanziarie di cui al paragrafo 1 stabiliscono soglie di allarme e criteri per l'attivazione e l'avvio dei processi di risposta agli incidenti connessi alle TIC.

Articolo 32

Sicurezza fisica e ambientale

1. Le entità finanziarie di cui all'articolo 16, paragrafo 1, del regolamento (UE) 2022/2554 identificano e attuano misure di sicurezza fisica elaborate sulla base del panorama delle minacce e conformemente alla classificazione di cui all'articolo 30, paragrafo 1, del presente regolamento, del profilo di rischio complessivo delle risorse TIC e dei patrimoni informativi accessibili.

2. Le misure di cui al paragrafo 1 proteggono i locali delle entità finanziarie e, se del caso, i centri di elaborazione dati delle entità finanziarie in cui risiedono le risorse TIC e i patrimoni informativi da accessi non autorizzati, attacchi e incidenti, nonché da minacce e pericoli ambientali.

3. La protezione dalle minacce e dai pericoli ambientali è commisurata all'importanza dei locali interessati e, se del caso, dei centri di elaborazione dati e alla criticità delle operazioni o dei sistemi di TIC ivi ubicati.

CAPO II

Ulteriori elementi di sistemi, protocolli e strumenti per ridurre al minimo l'impatto dei rischi informatici

Articolo 33

Controllo degli accessi

Le entità finanziarie di cui all'articolo 16, paragrafo 1, del regolamento (UE) 2022/2554 elaborano, documentano e attuano procedure per il controllo degli accessi logici e fisici e applicano, monitorano e riesaminano periodicamente tali procedure. Le suddette procedure contengono gli elementi di controllo degli accessi logici e fisici seguenti:

a) i diritti di accesso ai patrimoni informativi, alle risorse TIC e alle loro funzioni supportate, nonché alle sedi operative critiche dell'entità finanziaria sono gestiti in base ai principi della necessità di sapere, della necessità di usare e del privilegio minimo, anche per gli accessi remoti e di emergenza;

b) la responsabilità degli utenti, che garantisce che gli utenti possano essere identificati per le azioni eseguite nei sistemi di TIC;

c) le procedure di gestione degli account per concedere, modificare o revocare i diritti di accesso per gli account utente e generici, compresi gli account amministratore generici;

d) i metodi di autenticazione, commisurati alla classificazione di cui all'articolo 30, paragrafo 1, e al profilo di rischio complessivo delle risorse TIC e basati sulle pratiche più avanzate;

e) i diritti di accesso sono riesaminati periodicamente e revocati quando non sono più necessari.

Ai fini della lettera c), l'entità finanziaria assegna l'accesso privilegiato, di emergenza e di amministratore in base alla necessità di uso o ad hoc per tutti i sistemi di TIC, e lo registra nei log conformemente all'articolo 34, primo comma, lettera f).

Ai fini della lettera d), le entità finanziarie utilizzano metodi di autentificazione robusti basati sulle pratiche più avanzate per l'accesso remoto alla rete dell'entità finanziaria, per l'accesso privilegiato e per l'accesso alle risorse TIC a supporto di funzioni essenziali o importanti che sono disponibili al pubblico.

Articolo 34

Sicurezza delle operazioni riguardanti le TIC

Le entità finanziarie di cui all'articolo 16, paragrafo 1, del regolamento (UE) 2022/2554, nell'ambito dei loro sistemi, protocolli e strumenti e per tutte le risorse TIC:

a) monitorano e gestiscono il ciclo di vita di tutte le risorse TIC;

b) monitorano se le risorse TIC sono supportate da fornitori terzi di servizi TIC delle entità finanziarie, ove applicabile;

c) identificano i requisiti di capacità delle proprie risorse TIC e le misure per mantenere e migliorare la disponibilità e l'efficienza dei sistemi di TIC e prevenire le carenze di capacità TIC prima che si concretizzino;

d) eseguono scansioni e valutazioni automatizzate delle vulnerabilità delle risorse TIC commisurate alla loro classificazione di cui all'articolo 30, paragrafo 1, e al profilo di rischio complessivo della risorsa TIC, e applicano patch per risolvere le vulnerabilità identificate;

e) gestiscono i rischi relativi a risorse TIC obsolete, non supportate o legacy;

f) registrano nei log gli eventi relativi al controllo degli accessi logici e fisici, alle operazioni riguardanti le TIC, comprese le attività di sistema e di traffico di rete, e alla gestione delle modifiche delle TIC;

g) identificano e attuano misure per monitorare e analizzare le informazioni su attività e comportamenti anomali per le operazioni essenziali o importanti riguardanti le TIC;

h) attuano misure per monitorare le informazioni pertinenti e aggiornate sulle minacce informatiche;

i) attuano misure per identificare possibili fughe di informazioni, codici malevoli e altre minacce alla sicurezza, nonché vulnerabilità pubblicamente note in software e hardware e verificano la disponibilità di nuovi aggiornamenti di sicurezza corrispondenti.

Ai fini della lettera f), le entità finanziarie allineano il livello di dettaglio dei log allo scopo e all'utilizzo della risorsa TIC che li produce.

Articolo 35

Sicurezza dei dati, dei sistemi e delle reti

Le entità finanziarie di cui all'articolo 16, paragrafo 1, del regolamento (UE) 2022/2554, nell'ambito dei loro sistemi, protocolli e strumenti, elaborano e attuano salvaguardie che garantiscono la sicurezza delle reti contro le intrusioni e l'uso improprio dei dati e che preservano la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati. In particolare, le entità finanziarie, tenendo conto della classificazione di cui all'articolo 30, paragrafo 1, del presente regolamento, stabiliscono tutti gli elementi seguenti:

a) l'identificazione e l'attuazione di misure di protezione dei dati in uso, in transito e a riposo;

b) l'identificazione e l'attuazione di misure di sicurezza relative all'uso di software, supporti di memorizzazione dei dati, sistemi e dispositivi endpoint utilizzati per trasferire e memorizzare dati dell'entità finanziaria;

c) l'identificazione e l'attuazione di misure per prevenire e individuare connessioni non autorizzate alla rete dell'entità finanziaria e per proteggere il traffico di rete tra le reti interne dell'entità finanziaria e Internet e altre connessioni esterne;

d) l'identificazione e l'attuazione di misure che garantiscano la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati durante le trasmissioni di rete;

e) un processo per cancellare in modo sicuro i dati nei locali o memorizzati esternamente che l'entità finanziaria non ha più bisogno di raccogliere o conservare;

f) un processo per smaltire o dismettere in modo sicuro i dispositivi di archiviazione dati presenti nei locali o quelli conservati all'esterno contenenti informazioni riservate;

g) l'identificazione e l'attuazione di misure per garantire che il telelavoro e l'uso di dispositivi endpoint privati non abbiano un impatto negativo sulla capacità dell'entità finanziaria di svolgere le proprie attività critiche in modo adeguato, tempestivo e sicuro.

Articolo 36

Test di sicurezza delle TIC

1. Le entità finanziarie di cui all'articolo 16, paragrafo 1, del regolamento (UE) 2022/2554 stabiliscono e attuano un piano relativo ai test di sicurezza delle TIC per convalidare l'efficacia delle loro misure di sicurezza delle TIC elaborate conformemente agli articoli 33, 34 e 35 e agli articoli 37 e 38 del presente regolamento. Le entità finanziarie provvedono affinché tale piano tenga conto delle minacce e delle vulnerabilità identificate nell'ambito del quadro semplificato per la gestione dei rischi informatici di cui all'articolo 31 del presente regolamento.

2. Le entità finanziarie di cui al paragrafo 1 riesaminano, valutano e testano le misure di sicurezza delle TIC, tenendo conto del profilo di rischio complessivo delle risorse TIC dell'entità finanziaria.

3. Le entità finanziarie di cui al paragrafo 1 monitorano e valutano i risultati dei test di sicurezza e aggiornano di conseguenza le loro misure di sicurezza senza ritardi ingiustificati nel caso di sistemi di TIC a supporto di funzioni essenziali o importanti.

Articolo 37

Acquisizione, sviluppo e manutenzione dei sistemi di TIC

Le entità finanziarie di cui all'articolo 16, paragrafo 1, del regolamento (UE) 2022/2554 progettano e attuano, se del caso, una procedura che disciplina l'acquisizione, lo sviluppo e la manutenzione dei sistemi di TIC secondo un approccio basato sul rischio. Tale procedura:

a) garantisce che, prima di qualsiasi acquisizione o sviluppo di sistemi di TIC, siano chiaramente specificati e approvati dalla funzione aziendale interessata i requisiti funzionali e non funzionali, compresi quelli relativi alla sicurezza delle informazioni;

b) garantisce che i sistemi di TIC siano testati e approvati prima del loro primo utilizzo e prima di introdurre modifiche nell'ambiente di produzione;

c) identifica le misure di attenuazione del rischio di alterazione non intenzionale o di manipolazione intenzionale dei sistemi di TIC durante lo sviluppo e l'implementazione nell'ambiente di produzione.

Articolo 38

Gestione delle modifiche e dei progetti relativi alle TIC

1. Le entità finanziarie di cui all'articolo 16, paragrafo 1, del regolamento (UE) 2022/2554 elaborano, documentano e attuano una procedura di gestione dei progetti relativi alle TIC e specificano i ruoli e le responsabilità per la sua attuazione. Tale procedura copre tutte le fasi dei progetti relativi alle TIC, dal loro avvio alla loro chiusura.

2. Le entità finanziarie di cui al paragrafo 1 elaborano, documentano e attuano una procedura per la gestione delle modifiche delle TIC per garantire che tutte le modifiche ai sistemi di TIC siano registrate, testate, valutate, approvate, attuate e verificate in modo controllato e con le opportune salvaguardie per preservare la resilienza operativa digitale dell'entità finanziaria.

CAPO III

Gestione della continuità operativa delle TIC

Articolo 39

Componenti del piano di continuità operativa delle TIC

1. Le entità finanziarie di cui all'articolo 16, paragrafo 1, del regolamento (UE) 2022/2554 elaborano i loro piani di continuità operativa delle TIC tenendo conto dei risultati dell'analisi della loro esposizione a gravi perturbazioni dell'attività e del loro potenziale impatto, nonché degli scenari a cui potrebbero essere esposte le loro risorse TIC a supporto di funzioni essenziali o importanti, compreso uno scenario di attacco informatico.

2. I piani di continuità operativa delle TIC di cui al paragrafo 1:

a) sono approvati dall'organo di gestione dell'entità finanziaria;

b) sono documentati e facilmente accessibili in caso di emergenza o crisi;

c) assegnano risorse sufficienti per la loro esecuzione;

d) stabiliscono livelli e tempi di ripristino pianificati per il ripristino e la ripresa delle funzioni e delle principali dipendenze interne ed esterne, anche per quanto riguarda i fornitori terzi di servizi TIC;

e) identificano le condizioni che potrebbero richiedere l'attivazione dei piani di continuità operativa delle TIC e le azioni da intraprendere per garantire la disponibilità, la continuità e il ripristino delle risorse TIC delle entità finanziarie a supporto di funzioni essenziali o importanti;

f) identificano le misure di ripristino e recupero per le funzioni commerciali essenziali o importanti, i processi di supporto, i patrimoni informativi e le loro interdipendenze per evitare effetti negativi sul funzionamento delle entità finanziarie;

g) identificano le misure e le procedure di backup che precisano il perimetro dei dati soggetti a backup e la frequenza minima del backup, in base alla criticità della funzione che utilizza tali dati;

h) considerano opzioni alternative laddove il ripristino non sia fattibile a breve termine a causa di costi, rischi, logistica o circostanze impreviste;

i) specificano le modalità di comunicazione interna ed esterna, compresi i piani di attivazione dei livelli successivi di intervento;

j) sono aggiornati in base agli insegnamenti tratti da incidenti, test, nuovi rischi e minacce identificati, a obiettivi di ripristino modificati, a modifiche di rilievo dell'organizzazione dell'entità finanziaria e delle risorse TIC che supportano funzioni commerciali o essenziali.

Ai fini della lettera f), le misure di cui alla stessa lettera prevedono l'attenuazione delle disfunzioni dei fornitori terzi critici.

Articolo 40

Test dei piani di continuità operativa

1. Le entità finanziarie di cui all'articolo 16, paragrafo 1, del regolamento (UE) 2022/2554 testano i loro piani di continuità operativa di cui all'articolo 39 del presente regolamento, compresi gli scenari di cui a tale articolo, almeno una volta all'anno per le procedure di back-up e ripristino, o in occasione di ogni modifica di rilievo del piano di continuità operativa.

2. I test dei piani di continuità operativa di cui al paragrafo 1 dimostrano che le entità finanziarie di cui allo stesso paragrafo sono in grado di garantire la continuità delle loro attività fino al ripristino delle operazioni essenziali e identificano eventuali carenze in tali piani.

3. Le entità finanziarie di cui al paragrafo 1 documentano i risultati dei test dei piani di continuità operativa e le eventuali carenze identificate risultanti da tali test sono analizzate, affrontate e segnalate all'organo di gestione.

CAPO IV

Relazione sul riesame del quadro semplificato per la gestione dei rischi informatici

Articolo 41

Formato e contenuto della relazione sul riesame del quadro semplificato per la gestione dei rischi informatici

1. Le entità finanziarie di cui all'articolo 16, paragrafo 1, del regolamento (UE) 2022/2554 presentano la relazione sul riesame del quadro per la gestione dei rischi informatici di cui al paragrafo 2 di tale articolo in un formato elettronico che permetta la ricerca al suo interno.

2. La relazione di cui al paragrafo 1 contiene tutte le informazioni seguenti:

a) una sezione introduttiva che fornisce:

   i) una descrizione del contesto della relazione in termini di natura, portata e complessità dei servizi, delle attività e delle operazioni dell'entità finanziaria, della sua organizzazione, delle funzioni essenziali identificate, della strategia, dei principali progetti o attività in corso, dei rapporti e della dipendenza dell'entità finanziaria da servizi e sistemi di TIC interni e appaltati o delle implicazioni che una perdita totale o un grave degrado di tali sistemi avrebbe sulle funzioni essenziali o importanti e sull'efficienza del mercato;

   ii) una sintesi di livello esecutivo dei rischi informatici corrente e a breve termine, del panorama delle minacce, della valutazione dell'efficacia dei controlli e della posizione in materia di sicurezza dell'entità finanziaria;

   iii) informazioni sull'area oggetto della relazione;

   iv) una sintesi delle modifiche di rilievo apportate al quadro per la gestione dei rischi informatici rispetto alla precedente relazione;

   v) una sintesi e una descrizione dell'impatto delle modifiche e dei miglioramenti di rilievo apportati al quadro semplificato per la gestione dei rischi informatici rispetto alla relazione precedente;

b) se del caso, la data di approvazione della relazione da parte dell'organo di gestione dell'entità finanziaria;

c) una descrizione delle ragioni del riesame, comprensiva di:

   i) nel caso in cui il riesame sia stato avviato a seguito di istruzioni delle autorità di vigilanza, la prova di tali istruzioni;

   ii) nel caso in cui il riesame sia stato avviato a seguito del verificarsi di incidenti connessi alle TIC, l'elenco di tutti gli incidenti connessi alle TIC con la relativa analisi delle cause di fondo;

d) la data di inizio e di fine del periodo del riesame;

e) la persona responsabile del riesame;

f) una sintesi delle risultanze e un'autovalutazione della gravità delle debolezze, delle carenze e delle lacune identificate nel quadro per la gestione dei rischi informatici per il periodo del riesame, compresa un'analisi dettagliata delle stesse;

g) misure di riparazione individuate per affrontare le debolezze, le carenze e le lacune del quadro semplificato per la gestione dei rischi informatici e la data prevista per l'attuazione di tali misure, compreso il seguito dato alle debolezze, alle carenze e alle lacune identificate nelle relazioni precedenti, qualora tali debolezze, carenze e lacune non siano ancora state risolte;

h) conclusioni generali sul riesame del quadro semplificato per la gestione dei rischi informatici, compresi eventuali ulteriori sviluppi previsti.

TITOLO IV

DISPOSIZIONI FINALI

Articolo 42

Entrata in vigore

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

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

Fatto a Bruxelles, il 13 marzo 2024

Per la Commissione
La presidente
Ursula VON DER LEYEN