Orientamenti

EBA/GL/2019/04

28 novembre 2019

Orientamenti dell'ABE sulla gestione dei rischi relativi alle tecnologie dell'informazione e della comunicazione (Information and Communication Technology - ICT) e di sicurezza

Conformità e obblighi di comunicazione

Status giuridico dei presenti orientamenti

1. Il presente documento contiene gli orientamenti emanati ai sensi dell'articolo 16 del regolamento (UE) n. 1093/2010[1]. Conformemente all'articolo 16, paragrafo 3, del regolamento (UE) n. 1093/2010, le autorità competenti e gli enti finanziari sono tenuti a compiere ogni sforzo per conformarsi agli orientamenti.

2. Gli orientamenti presentano il parere dell'ABE in merito alle prassi di vigilanza adeguate all'interno del Sistema europeo di vigilanza finanziaria o alle modalità di applicazione del diritto dell'Unione europea in una particolare area. Le autorità competenti di cui all'articolo 4, paragrafo 2, del regolamento (UE) n. 1093/2010 sono tenute a conformarsi a detti orientamenti integrandoli opportunamente nelle rispettive prassi di vigilanza (ad esempio modificando il proprio quadro giuridico o le proprie procedure di vigilanza), anche quando gli orientamenti sono diretti principalmente agli enti.

Obblighi di notifica

3. Ai sensi dell'articolo 16, paragrafo 3, del regolamento (UE) n. 1093/2010, le autorità competenti devono notificare all'ABE entro il ([gg.mm.aaaa]) se sono conformi o se intendono conformarsi agli orientamenti in questione; in alternativa sono tenute a indicare le ragioni della mancata conformità. Qualora entro il termine indicato non sia pervenuta alcuna notifica da parte delle autorità competenti, queste sono ritenute dall'ABE non conformi. Le notifiche dovrebbero essere inviate trasmettendo il modulo disponibile sul sito web dell'ABE all'indirizzo compliance@eba.europa.eu con il riferimento «EBA/GL/2019/04» da persone debitamente autorizzate a segnalare la conformità per conto delle rispettive autorità competenti. Ogni eventuale variazione dello status di conformità deve essere altresì comunicata all'ABE.

4. Le notifiche sono pubblicate sul sito web dell'ABE ai sensi dell'articolo 16, paragrafo 3.

[1] 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).

Oggetto, ambito di applicazione e definizioni

Oggetto

5. I presenti orientamenti si basano sulle disposizioni dell'articolo 74 della direttiva 2013/36/UE (CRD) relativo alla governance interna e derivano dal mandato di emanare orientamenti previsto dall'articolo 95, paragrafo 3, della direttiva 2015/2366 (PSD2).

6. Gli orientamenti specificano le misure di gestione dei rischi che gli istituti finanziari (quali definiti di seguito al paragrafo 9) devono adottare ai sensi dell'articolo 74 della CRD per gestire i rischi relativi all'uso delle tecnologie dell'informazione e della comunicazione (Information and Communication Technlogy - ICT) e alla sicurezza per tutte le attività e che i prestatori di servizi di pagamento (quali definiti di seguito al paragrafo 9) devono adottare ai sensi dell'articolo 95, paragrafo 1, della PSD2, per gestire i rischi operativi e di sicurezza (intesi come «rischi ICT e di sicurezza») relativi ai servizi di pagamento che forniscono. Gli orientamenti comprendono requisiti relativi alla sicurezza dell'informazione, inclusa la sicurezza informatica, nella misura in cui le informazioni sono detenute su sistemi ICT.

Ambito di applicazione

7. I presenti orientamenti si applicano alla gestione dei rischi ICT e di sicurezza all'interno degli istituti finanziari (quali definiti al paragrafo 9). Ai fini dei presenti orientamenti, il termine «rischi ICT e di sicurezza» si riferisce ai rischi operativi e di sicurezza di cui all'articolo 95 della PSD2 per la prestazione di servizi di pagamento.

8. Per i prestatori di servizi di pagamento (quali definiti al paragrafo 9) i presenti orientamenti si applicano alla prestazione di servizi di pagamento, in linea con l'ambito di applicazione e il mandato di cui all'articolo 95 della PSD2. Per gli enti (quali definiti al paragrafo 9) i presenti orientamenti si applicano a tutte le attività da essi svolte.

Destinatari

9. I presenti orientamenti sono rivolti agli istituti finanziari, che ai fini degli orientamenti comprendono 1) i prestatori di servizi di pagamento, quali definiti all'articolo 4, paragrafo 11, della PSD2, e 2) gli enti, vale a dire gli enti creditizi e le imprese di investimento secondo la definizione di cui all'articolo 4, paragrafo 1, punto 3), del regolamento (UE) n. 575/2013. I presenti orientamenti si applicano inoltre alle autorità competenti quali definite all'articolo 4, paragrafo 1, punto 40), del regolamento (UE) n. 575/2013, compresa la Banca centrale europea relativamente ai compiti ad essa attribuiti dal regolamento (UE) n. 1024/2013, e alle autorità competenti ai sensi della PSD2, come indicato all'articolo 4, paragrafo 2, lettera i), del regolamento (UE) n. 1093/2010.

Definizioni

10. Se non altrimenti specificato, i termini utilizzati e definiti nella direttiva 2013/36/UE (CRD), nel regolamento (UE) n. 575/2013 (CRR) e nella direttiva (UE) 2015/2366 (PSD2) hanno lo stesso significato negli orientamenti. Ai fini dei presenti orientamenti, si applicano inoltre le definizioni riportate di seguito:

Rischio ICT e di sicurezza	Il rischio di perdita dovuta alla violazione della riservatezza, la carente integrità dei sistemi e dei dati, l'inadeguatezza o l'indisponibilità dei sistemi e dei dati o l'incapacità di sostituire la tecnologia dell'informazione (IT) entro ragionevoli limiti di tempo e costi nel caso di modifica dei requisiti del contesto esterno o dell'attività (ossia l'agilità)[2]. Questo comprende i rischi di sicurezza derivanti da processi interni inadeguati o errati o da eventi esterni, compresi gli attacchi informatici o una sicurezza fisica inadeguata.
Organo di gestione	(a) Per gli enti creditizi e le imprese di investimento questo termine ha il medesimo significato di cui alla definizione dell'articolo 3, paragrafo 1, punto 7), della direttiva 2013/36/UE. (b) Per gli istituti di pagamento o istituti di moneta elettronica, questo termine indica i direttori o le persone responsabili della gestione dell'istituto di pagamento e dell'istituto di moneta elettronica e, se rilevanti, le persone responsabili della gestione delle attività connesse ai servizi di pagamento degli istituti di pagamento e degli istituti di moneta elettronica. (c) Per i prestatori di servizi di pagamento di cui all'articolo 1, paragrafo 1, lettere c), e) ed f), della direttiva (UE) 2015/2366, questo termine ha il significato che gli viene attribuito dalla normativa nazionale o dell'UE applicabile.
Incidente operativo o di sicurezza	Singolo evento o serie di eventi collegati, non pianificati dall'istituto finanziario, che ha, o probabilmente avrà, un impatto negativo sull'integrità, la disponibilità, la riservatezza, e/o l'autenticità dei servizi.
Alta dirigenza	(a) Per gli enti creditizi e le imprese di investimento questo termine ha il medesimo significato di cui alla definizione dell'articolo 3, paragrafo 1, punto 9), della direttiva 2013/36/UE. (b) Per gli istituti di pagamento e gli istituti di moneta elettronica, questo termine indica le persone fisiche che esercitano funzioni esecutive in un istituto, sono responsabili della

[2] Definizione tratta dagli orientamenti dell'ABE sulle procedure e sulle metodologie comuni per il processo di revisione e valutazione prudenziale (SREP) del 19 dicembre 2014 (ABE/GL/2014/13), modificati da ABE/GL/2018/03.

	gestione quotidiana dell'istituto e ne devono rispondere all'organo di gestione. (c) Per i prestatori di servizi di pagamento di cui all'articolo 1, paragrafo 1, lettere c), e) ed f), della direttiva (UE) 2015/2366, questo termine ha il significato che gli viene attribuito dalla normativa nazionale o dell'UE applicabile.
Propensione al rischio	Il livello complessivo e i tipi di rischio che i prestatori di servizi di pagamento e gli enti sono disposti ad assumere per conseguire gli obiettivi strategici che si sono prefissati, in funzione della loro capacità di tollerare il rischio, in linea con il loro modello di business.
Funzione di audit	(a) Per gli enti creditizi e le imprese di investimento, la funzione di audit è quella indicata nella sezione 22 degli orientamenti dell'ABE sulla governance interna (EBA/GL/2017/11). (b) Per i prestatori di servizi di pagamento diversi dagli enti creditizi, la funzione di audit deve essere indipendente nell'ambito o nei confronti del prestatore di servizi di pagamento e può essere una funzione di audit interno e/o esterno.
Progetti ICT	Qualsiasi progetto, o parte di esso, in cui i sistemi e i servizi ICT sono modificati, sostituiti, dismessi o implementati. I progetti ICT possono far parte di più ampi programmi ICT o di trasformazione aziendale.
Soggetto terzo	Un'organizzazione che abbia stretto rapporti commerciali o stipulato contratti con un'entità per la fornitura di un prodotto o un servizio[3].
Risorsa informativa	Una raccolta di informazioni, tangibile o intangibile, che merita protezione.
Risorsa ICT	Qualunque software o hardware presenti nel contesto aziendale.
Sistemi ICT[4]	ICT adottato come parte di un meccanismo o di una rete di interconnessione a supporto delle operazioni di un istituto finanziario.
Servizi ICT[5]	I servizi forniti dai sistemi ICT a uno o più utenti interni o esterni. Tali servizi comprendono ad esempio: servizi di inserimento, archiviazione, elaborazione e comunicazione di dati, ma anche servizi di monitoraggio, di supporto alle attività e alle decisioni aziendali.

[3] Definizione tratta dagli elementi fondamentali del G7 per la gestione dei rischi digitali legati a soggetti terzi nel settore finanziario.
[4] Definizione tratta dagli orientamenti sulla valutazione dei rischi ICT a norma del processo di revisione e valutazione prudenziale (SREP) (EBA/GL/2017/05).
[5] Ibidem.

Attuazione

Data di applicazione

11. I presenti orientamenti si applicano a decorrere dal 30 giugno 2020.

Abrogazione

12. Gli orientamenti sulle misure di sicurezza per i rischi operativi e di sicurezza (EBA/GL/2017/17) pubblicati nel 2017 saranno abrogati dai presenti orientamenti alla data di applicazione di questi ultimi.

Orientamenti sulla gestione dei rischi ICT e di sicurezza

1.1. Proporzionalità

1. Tutti gli istituti finanziari dovrebbero essere conformi a tutte le disposizioni contenute nei presenti orientamenti in modo proporzionato e tenendo in conto della dimensione degli istituti finanziari, della loro organizzazione interna e della natura, portata, complessità e rischiosità dei prodotti e dei servizi che gli istituti finanziari forniscono o intendono fornire.

1.2. Governance e strategia

1.2.1. Governance

2. L'organo di gestione dovrebbe garantire che l'istituto finanziario disponga di un quadro di riferimento per la governance e i controlli interni adeguato ai propri rischi ICT e di sicurezza. L'organo di gestione dovrebbe stabilire chiaramente ruoli e responsabilità per le funzioni ICT, per la gestione dei rischi relativi alla sicurezza dell'informazione e per la continuità operativa, compresi quelli dell'organo di gestione e dei suoi comitati.

3. L'organo di gestione dovrebbe garantire che la quantità e le abilità del personale dell'istituto finanziario siano adeguate a supportare le esigenze operative dell'ICT e dei processi di gestione dei rischi ICT e di sicurezza dell'istituto su base continuativa, oltre ad assicurare l'attuazione della propria strategia ICT. L'organo di gestione dovrebbe garantire che il bilancio stanziato sia adeguato a soddisfare i requisiti di cui sopra. Inoltre, gli istituti finanziari dovrebbero garantire che tutto il personale, compreso quello che riveste ruoli chiave, riceva una formazione adeguata sui rischi ICT e di sicurezza, compresa la sicurezza dell'informazione, con cadenza annuale o con maggiore frequenza se necessario (cfr. anche la sezione 1.4.7).

4. L'organo di gestione ha la responsabilità generale di definire, approvare e supervisionare l'attuazione della strategia ICT dell'istituto finanziario nell'ambito della sua strategia aziendale, nonché di istituire un quadro di riferimento efficace per la gestione dei rischi ICT e di sicurezza.

1.2.2. Strategia

5. La strategia ICT dovrebbe essere allineata alla strategia aziendale generale degli istituti finanziari e dovrebbe definire:

    a) il modo in cui l'ICT degli istituti finanziari dovrebbe evolvere per supportare e partecipare efficacemente alla loro strategia aziendale, specificando in particolare l'evoluzione della struttura organizzativa, le modifiche dei sistemi ICT e le dipendenze chiave da soggetti terzi;
    b) la strategia e l'evoluzione pianificata dell'architettura ICT, comprese le dipendenze da soggetti terzi;
    c) obiettivi chiari in materia di sicurezza dell'informazione, con particolare attenzione ai sistemi e ai servizi ICT, al personale e ai processi.

6. Gli istituti finanziari dovrebbero stabilire una serie di piani d'azione contenenti le misure da adottare per conseguire l'obiettivo indicato dalla strategia ICT. Tali piani dovrebbero essere comunicati a tutto il personale interessato (compresi contraenti e fornitori terzi, ove applicabile e pertinente). I piani d'azione dovrebbero essere riesaminati periodicamente per garantirne la pertinenza e l'adeguatezza. Gli istituti finanziari dovrebbero inoltre stabilire processi per monitorare e misurare l'efficacia dell'attuazione della propria strategia ICT.

1.2.3. Ricorso a fornitori terzi

7. Fatti salvi gli orientamenti dell'ABE in materia di esternalizzazione (ABE/GL/2019/02) e l'articolo 19 della PSD2, quando le funzioni operative dei servizi di pagamento e/o i servizi e i sistemi ICT utilizzati da qualsiasi attività sono esternalizzati, anche a entità del gruppo, o quando si fa ricorso a fornitori terzi, gli istituti finanziari dovrebbero garantire l'efficacia delle misure di attenuazione dei rischi definite dal proprio quadro di gestione dei rischi, comprese le misure descritte nei presenti orientamenti.

8. Per garantire la continuità dei servizi e dei sistemi ICT, gli istituti finanziari dovrebbero adoperarsi affinché i contratti e gli accordi sul livello dei servizi (sia in circostanze normali che in caso di interruzione del servizio; cfr. anche la sezione 1.7.2) conclusi con i fornitori (fornitori esterni, entità del gruppo o fornitori terzi) comprendano quanto segue:

    a) misure e obiettivi adeguati e proporzionati in materia di sicurezza dell'informazione, compresi i requisiti minimi di sicurezza informatica, specifiche relative al ciclo di vita dei dati dell'istituto finanziario ed eventuali requisiti relativi alla cifratura dei dati, alla sicurezza di rete e ai processi di monitoraggio della sicurezza, e l'ubicazione dei centri dati;
    b) procedure di gestione degli incidenti operativi e di sicurezza, tra cui notifica e attivazione dei livelli successivi di intervento.

9. Gli istituti finanziari dovrebbero monitorare e ottenere garanzie per quanto riguarda il livello di conformità dei suddetti fornitori agli obiettivi di sicurezza, alle misure e alle prestazioni previste dell'istituto finanziario.

1.3. Quadro di riferimento per la gestione dei rischi ICT e di sicurezza

1.3.1. Organizzazione e obiettivi

10. Gli istituti finanziari dovrebbero individuare e gestire i propri rischi ICT e di sicurezza. La funzione (o le funzioni) ICT responsabili dei sistemi ICT, dei processi e delle operazioni di sicurezza dovrebbero disporre di processi e controlli adeguati a garantire che tutti i rischi siano individuati, analizzati, misurati, monitorati, gestiti, segnalati e mantenuti entro i limiti della propensione al rischio dell'istituto finanziario, oltre a garantire che i progetti e i sistemi realizzati e le attività svolte siano conformi ai requisiti esterni e interni.

11. Gli istituti finanziari dovrebbero assegnare la responsabilità della gestione e della supervisione dei rischi ICT e di sicurezza a una funzione di controllo, conformemente ai requisiti della sezione 19 degli orientamenti dell'ABE sulla governance interna (EBA/GL/2017/11). Gli istituti finanziari dovrebbero garantire l'indipendenza e l'obiettività di tale funzione di controllo, separandola adeguatamente dai processi operativi dell'ICT. Questa funzione di controllo dovrebbe rispondere direttamente all'organo di gestione ed essere responsabile del monitoraggio e del controllo dell'adesione al quadro di riferimento per la gestione dei rischi ICT e di sicurezza. Nello specifico, la funzione di controllo dovrebbe garantire che i rischi ICT e di sicurezza siano individuati, misurati, valutati, gestiti, monitorati e segnalati. Gli istituti finanziari dovrebbero garantire che tale funzione di controllo non sia responsabile di alcun audit interno.

    Secondo un approccio basato sul rischio, la funzione di audit interno dovrebbe avere la capacità di riesaminare tutte le attività e le unità organizzative di un istituto finanziario relative a ICT e sicurezza in modo indipendente e offrendo una oggettiva garanzia di conformità alle policy e procedure dell'istituto medesimo e ai requisiti esterni, aderendo ai requisiti della sezione 22 degli orientamenti dell'ABE sulla governance interna (EBA/GL/2017/11).

12. Gli istituti finanziari dovrebbero definire e assegnare i ruoli e le responsabilità chiave, stabilendo i relativi rapporti gerarchici, al fine di garantire l'efficacia del quadro di riferimento per la gestione dei rischi ICT e di sicurezza. Tale quadro dovrebbe essere pienamente integrato e allineato con i processi di gestione dei rischi degli istituti finanziari.

13. Il quadro di riferimento per la gestione dei rischi ICT e di sicurezza dovrebbe comprendere l'attuazione di processi finalizzati a:

    a) determinare la propensione al rischio per quanto riguarda i rischi ICT e di sicurezza, in accordo con la propensione al rischio dell'istituto finanziario;
    b) individuare e valutare i rischi ICT e di sicurezza ai quali un istituto finanziario è esposto;
    c) definire le misure, tra cui i controlli, per l'attenuazione dei rischi ICT e di sicurezza;

d) monitorare l'efficacia di tali misure e il numero di incidenti segnalati, compresi, per i prestatori di servizi di pagamento, gli incidenti notificati ai sensi dell'articolo 96 della PSD2 che riguardano le attività relative alla ICT, e intervenire per correggere tali misure se necessario;
e) riferire all'organo di gestione in merito ai rischi ICT e di sicurezza e ai relativi controlli;
f) individuare e valutare se vi siano rischi ICT e di sicurezza derivanti da importanti modifiche dei sistemi o dei servizi ICT, di processi o procedure e/o a seguito di incidenti operativi o di sicurezza significativi.

14. Gli istituti finanziari dovrebbero garantire che il quadro di riferimento per la gestione dei rischi ICT e di sicurezza sia documentato e continuamente migliorato, sulla base di quanto appreso durante la sua attuazione e il suo monitoraggio. Il quadro di riferimento per la gestione dei rischi ICT e di sicurezza dovrebbe essere approvato e rivisto almeno una volta all'anno dall'organo di gestione.

1.3.2. Individuazione delle funzioni, dei processi e delle risorse

15. Gli istituti finanziari dovrebbero individuare, stabilire e mantenere aggiornato l'inventario delle proprie funzioni aziendali, dei ruoli e dei processi di supporto per determinare l'importanza e le interdipendenze di ciascuno di essi in relazione ai rischi ICT e di sicurezza.

16. Inoltre, gli istituti finanziari dovrebbero individuare, stabilire e mantenere aggiornato l'inventario delle risorse informatiche che supportano le funzioni aziendali e i processi di supporto, quali i sistemi ICT, il personale, i contraenti, i soggetti terzi e le dipendenze da altri sistemi e processi interni ed esterni, per essere in grado quanto meno di gestire le risorse informatiche che supportano le funzioni e i processi aziendali critici.

1.3.3. Classificazione e valutazione dei rischi

17. Gli istituti finanziari dovrebbero classificare sotto il profilo della criticità le funzioni aziendali, i processi che le supportano e le risorse informatiche di cui ai paragrafi 15 e 16.

18. Per definire la criticità delle funzioni aziendali, dei processi di supporto e delle risorse informatiche individuate, gli istituti finanziari dovrebbero considerare come minimo i requisiti di riservatezza, integrità e disponibilità. Dovrebbero essere assegnate responsabilità chiare per le risorse informatiche.

19. Nell'effettuare la valutazione dei rischi, gli istituti finanziari dovrebbero riesaminare l'adeguatezza della classificazione delle risorse informatiche e della relativa documentazione.

20. Gli istituti finanziari dovrebbero individuare i rischi ICT e di sicurezza che incidono sulle funzioni aziendali, sui processi di supporto e sulle risorse informatiche identificate e classificate, in funzione della loro criticità. Questa valutazione dei rischi dovrebbe essere svolta e documentata con cadenza annuale o, se necessario, a intervalli più brevi. Tali valutazioni dei rischi dovrebbero essere effettuate anche a seguito di importanti modifiche dell'infrastruttura, dei processi o delle procedure che incidono sulle funzioni aziendali, sui processi di supporto o

sulle risorse informatiche, e la valutazione dei rischi dell'istituto finanziario dovrebbe essere aggiornata di conseguenza.

21. Gli istituti finanziari dovrebbero garantire il monitoraggio continuo delle minacce e delle vulnerabilità, nonché rivedere periodicamente gli scenari di rischio che hanno impatti sui processi aziendali, sulle funzioni di supporto e sulle risorse informatiche.

1.3.4. Attenuazione dei rischi

22. Sulla base delle valutazioni dei rischi, gli istituti finanziari dovrebbero determinare quali sono le misure essenziali per ridurre a livelli accettabili i rischi ICT e di sicurezza individuati, valutando inoltre se è necessario apportare modifiche ai processi aziendali, alle misure di controllo, ai sistemi e servizi ICT esistenti. Gli istituti finanziari dovrebbero considerare il tempo necessario per attuare tali modifiche e per adottare misure provvisorie di attenuazione adeguate per ridurre al minimo i rischi ICT e di sicurezza, affinché rimangano nei limiti della propensione al rischio dell'istituto finanziario per i rischi ICT e di sicurezza.

23. Gli istituti finanziari dovrebbero definire e attuare misure per attenuare i rischi ICT e di sicurezza individuati e per proteggere le risorse informatiche conformemente alla loro classificazione.

1.3.5. Segnalazione

24. Gli istituti finanziari dovrebbero segnalare i risultati della valutazione dei rischi all'organo di gestione in maniera chiara e tempestiva. Tale segnalazione non pregiudica l'obbligo dei prestatori di servizi di pagamento di fornire alle autorità competenti una valutazione aggiornata e approfondita dei rischi, come stabilito dall'articolo 95, paragrafo 2, della direttiva (UE) 2015/2366.

1.3.6. Audit

25. La governance, i sistemi e i processi di un istituto finanziario per quanto riguarda i rischi ICT e di sicurezza dovrebbero essere sottoposti a audit periodico da auditor in possesso di sufficienti conoscenze, abilità e competenze in materia di rischi ICT e di sicurezza e in materia di pagamenti (per i prestatori di servizi di pagamento), allo scopo di fornire all'organo di gestione una assicurazione indipendente sulla loro efficacia. Gli auditor dovrebbero essere indipendenti nell'ambito o nei confronti dell'istituto finanziario. La frequenza e l'obiettivo di tali audit dovrebbero essere commisurati ai relativi rischi ICT e di sicurezza .

26. L'organo di gestione di un istituto finanziario dovrebbe approvare il piano di audit, compresi eventuali audit riferiti all'ICT, e ogni sua modifica significativa. Il piano di audit e la sua esecuzione, compresa la frequenza degli audit, dovrebbero riflettere ed essere proporzionati ai rischi dell'istituto finanziario, compresi quelli riferiti all'ICT e alla sicurezza, ed essere aggiornati regolarmente.

27. Un processo formale di follow-up che includa disposizioni per la verifica e la correzione tempestive dei risultati critici dell'audit sull'ICT dovrebbe essere istituito.

1.4. Sicurezza dell'informazione

1.4.1. Policy di sicurezza dell'informazione

28. Gli istituti finanziari dovrebbero formulare e documentare una policy di sicurezza dell'informazione, che dovrebbe definire i principi e le regole di alto livello finalizzati a proteggere la riservatezza, l'integrità e la disponibilità dei dati e delle informazioni degli istituti finanziari e dei loro clienti. Per i prestatori di servizi di pagamento, questa policy è individuata nel documento relativo alla policy di sicurezza da adottarsi in conformità all'articolo 5, paragrafo 1, lettera j), della direttiva (UE) 2015/2366. La policy di sicurezza dell'informazione dovrebbe essere in linea con gli obiettivi di sicurezza dell'informazione dell'istituto finanziario ed essere basata sugli specifici risultati del processo di valutazione dei rischi. La policy dovrebbe essere approvata dall'organo di gestione.

29. La policy dovrebbe comprendere una descrizione dei ruoli e delle responsabilità principali nella gestione della sicurezza dell'informazione e dovrebbe stabilire i requisiti per il personale e i contraenti, i processi e la tecnologia in relazione alla sicurezza dell'informazione, riconoscendo che il personale e i contraenti a tutti i livelli hanno responsabilità nel garantire la sicurezza dell'informazione degli istituti finanziari. La policy dovrebbe garantire la riservatezza, l'integrità e la disponibilità delle risorse logiche e fisiche critiche di un istituto finanziario, di altre risorse e dei dati sensibili, siano essi inutilizzati, in transito o in uso. La policy di sicurezza dell'informazione dovrebbe essere comunicata a tutto il personale e ai contraenti dell'istituto finanziario.

30. Sulla base della policy di sicurezza dell'informazione, gli istituti finanziari dovrebbero stabilire e attuare misure di sicurezza per attenuare i rischi ICT e di sicurezza ai quali sono esposti. Tali misure dovrebbero comprendere:

    a) organizzazione e governance, conformemente ai paragrafi 10 e 11;
    b) sicurezza logica (sezione 1.4.2);
    c) sicurezza fisica (sezione 1.4.3);
    d) sicurezza delle operazioni ICT (sezione 1.4.4);
    e) monitoraggio della sicurezza (sezione 1.4.5);
    f) analisi, valutazione e verifica della sicurezza dell'informazione (sezione 1.4.6);
    g) formazione e sensibilizzazione sulla sicurezza dell'informazione (sezione 1.4.7).

1.4.2. Sicurezza logica

31. Gli istituti finanziari dovrebbero definire, documentare e attuare procedure per il controllo logico degli accessi (gestione dell'identità e degli accessi). Queste procedure dovrebbero essere attuate, applicate, monitorate e periodicamente riesaminate. Le procedure dovrebbero inoltre prevedere controlli per il monitoraggio delle anomalie. Tali procedure dovrebbero, come minimo, attuare i seguenti elementi, dove il termine «utente» comprende anche gli utenti tecnici:

(a) **«Need-to-know», minimo privilegio e separazione dei compiti:** gli istituti finanziari dovrebbero gestire i diritti di accesso alle risorse informatiche e ai loro sistemi di supporto sulla base di quanto è necessario sapere (principio del «need-to-know»), anche per quanto concerne l'accesso remoto. Agli utenti dovrebbero essere concessi i diritti di accesso minimi strettamente necessari per l'esecuzione dei loro compiti (principio del «minimo privilegio»), in modo da impedire l'accesso ingiustificato a un'ampia serie di dati o l'assegnazione di combinazioni di diritti di accesso che possono essere utilizzati per aggirare i controlli (principio della «separazione dei compiti»).

(b) **Responsabilità degli utenti:** gli istituti finanziari dovrebbero limitare, per quanto possibile, l'uso di account utente generici e condivisi e garantire che gli utenti possano essere identificati per le azioni svolte nei sistemi ICT.

(c) **Diritti di accesso privilegiato:** gli istituti finanziari dovrebbero controllare rigidamente l'accesso privilegiato al sistema limitando strettamente e sorvegliando attentamente gli account in possesso di ampie autorizzazioni di accesso (ad esempio, gli account degli amministratori). Al fine di garantire la sicurezza delle comunicazioni e ridurre il rischio, l'accesso amministrativo da remoto a sistemi ICT critici dovrebbe essere concesso esclusivamente sulla base delle esigenze conoscitive contingenti e qualora siano applicate soluzioni di autenticazione forte.

(d) **Registrazione delle attività degli utenti:** quanto meno, tutte le attività degli utenti privilegiati dovrebbero essere registrate e monitorate. I registri degli accessi dovrebbero essere protetti per impedire modifiche o cancellazioni non autorizzate e conservati per un periodo commisurato alla criticità delle funzioni aziendali, dei processi di supporto e delle risorse informatiche individuate, conformemente alla sezione 1.3.3, fatti salvi gli obblighi di conservazione previsti dalla normativa nazionale e dell'UE. Gli istituti finanziari dovrebbero utilizzare questi registri per facilitare l'individuazione di attività anomale nella prestazione dei servizi, nonché le relative indagini.

(e) **Gestione degli accessi:** i diritti di accesso dovrebbero essere concessi, revocati o modificati tempestivamente, secondo procedure di approvazione predefinite che coinvolgano il proprietario delle informazioni a cui si accede (proprietario delle risorse informatiche). In caso di cessazione del rapporto di lavoro, i diritti di accesso dovrebbero essere revocati tempestivamente.

(f) **Ri-certificazione degli accessi:** i diritti di accesso dovrebbero essere riesaminati periodicamente per garantire che gli utenti non godano di privilegi eccessivi e che i diritti di accesso siano revocati quando non sono più necessari.

(g) **Metodi di autenticazione:** gli istituti finanziari dovrebbero applicare metodi di autenticazione che siano sufficientemente solidi da garantire in modo adeguato ed efficace il rispetto delle policy e delle procedure di controllo degli accessi. I metodi di autenticazione dovrebbero essere commisurati alla criticità dei sistemi ICT, delle informazioni o del processo a cui si accede. Ciò dovrebbe comprendere, quanto meno, password complesse o metodi di autenticazione più forti (come l'autenticazione a due fattori), in funzione del rischio pertinente.

32. L'accesso ai dati e ai sistemi ICT per mezzo di applicazioni informatiche dovrebbe essere limitato a quanto strettamente necessario per la prestazione del servizio in questione.

1.4.3. Sicurezza fisica

33. Gli istituti finanziari dovrebbero definire, documentare e attuare misure di sicurezza fisica per proteggere dall'accesso non autorizzato e da rischi ambientali i propri locali, data center e aree sensibili.

34. L'accesso fisico ai sistemi ICT dovrebbe essere permesso soltanto a persone autorizzate. L'autorizzazione dovrebbe essere rilasciata in base ai compiti e alle responsabilità individuali e limitandosi alle persone formate e monitorate in modo adeguato. L'accesso fisico dovrebbe essere riesaminato regolarmente per garantire che i diritti di accesso non più necessari siano revocati tempestivamente quando non richiesti.

35. Misure adeguate di protezione dai rischi ambientali dovrebbero essere commisurate all'importanza degli edifici e alla criticità delle operazioni o dei sistemi ICT situati al loro interno.

1.4.4. Sicurezza delle operazioni ICT

36. Gli istituti finanziari dovrebbero attuare procedure per prevenire il verificarsi di problemi di sicurezza nei sistemi e servizi ICT e dovrebbero ridurre al minimo il loro impatto sull'erogazione dei servizi ICT. Tali procedure dovrebbero comprendere le misure seguenti:

    a) l'individuazione delle potenziali vulnerabilità, che dovrebbero essere valutate e corrette garantendo che il software e il firmware siano aggiornati, compreso il software fornito dagli istituti finanziari ai loro utenti interni ed esterni, mediante la distribuzione di patch di sicurezza critiche o la realizzazione di controlli compensativi;
    b) la realizzazione di configurazione di sicurezza di base per tutti i componenti di rete;
    c) la realizzazione di una rete segmentata, di sistemi per la prevenzione della perdita di dati e per la cifratura del traffico di rete (in base alla classificazione dei dati);
    d) la protezione degli endpoint, compresi server, stazioni di lavoro e dispositivi mobili; gli istituti finanziari dovrebbero valutare se gli endpoint soddisfano gli standard di sicurezza da essi definiti prima che questi ottengano l'accesso alla rete aziendale;
    e) la messa in atto di meccanismi per verificare l'integrità del software, del firmware e dei dati;
    f) la cifratura dei dati memorizzati e in transito (in base alla classificazione dei dati).

37. Inoltre, gli istituti finanziari dovrebbero stabilire, su base continuativa, se le modifiche al contesto operativo esistente influenzino le misure di sicurezza adottate o se si renda necessaria l'adozione di ulteriori misure per mitigare adeguatamente i relativi rischi. Tali modifiche dovrebbero essere formalmente parte del processo di gestione del cambiamento adottato dagli istituti finanziari, il quale dovrebbe garantire che le modifiche siano adeguatamente pianificate, verificate, documentate, autorizzate e attuate.

1.4.5. Monitoraggio della sicurezza

38. Gli istituti finanziari dovrebbero stabilire e attuare policy e procedure per rilevare attività anomale che potrebbero incidere sulla sicurezza dell'informazione degli istituti finanziari e per rispondere adeguatamente a tali eventi. Nell'ambito di questo monitoraggio continuo, gli

istituti finanziari dovrebbero attuare capacità adeguate ed efficaci per rilevare intrusioni fisiche o logiche e violazioni della riservatezza, dell'integrità e della disponibilità delle risorse informatiche. I processi di rilevazione e monitoraggio continuo dovrebbero riguardare:

a) i fattori interni ed esterni pertinenti, comprese le funzioni di gestione del business e dell'ICT
b) le transazioni, al fine di individuare abusi negli accessi da parte di terzi o di altri, ovvero eventuali abusi interni;
c) potenziali minacce interne ed esterne.

39. Gli istituti finanziari dovrebbero definire e attuare processi e strutture organizzative per la rilevazione ed il monitoraggio continuo delle minacce alla sicurezza che potrebbero pregiudicare in modo sostanziale la loro capacità di prestare servizi. Gli istituti finanziari dovrebbero monitorare attivamente gli sviluppi tecnologici per garantire di essere aggiornati sui rischi per la sicurezza. Gli istituti finanziari dovrebbero attuare misure per rilevare, ad esempio, possibili perdite di dati, codici malevoli (malware) e altre minacce per la sicurezza, nonché le vulnerabilità note del software e dell'hardware e dovrebbero controllare i corrispondenti aggiornamenti di sicurezza.

40. Il processo di monitoraggio della sicurezza dovrebbe inoltre aiutare un istituto finanziario a comprendere la natura degli incidenti operativi o di sicurezza, a individuare le tendenze e favorire le indagini dell'organizzazione.

1.4.6. Analisi, valutazione e verifica della sicurezza dell'informazione

41. Gli istituti finanziari dovrebbero eseguire una vasta gamma di analisi, valutazioni e verifiche della sicurezza dell'informazione per garantire l'effettiva individuazione delle vulnerabilità nei loro sistemi e servizi ICT. Ad esempio, gli istituti finanziari possono effettuare un'analisi delle lacune («gap analysis») rispetto agli standard di sicurezza dell'informazione, alle analisi di conformità, agli audit interni ed esterni dei sistemi informatici o alle analisi della sicurezza fisica. Inoltre, gli istituti finanziari dovrebbero adottare buone prassi quali revisioni del codice sorgente, analisi della vulnerabilità, penetration test e pratiche di Red Team.

42. Gli istituti finanziari dovrebbero istituire e attuare un quadro di riferimento per la verifica della sicurezza dell'informazione che convalidi la robustezza e l'efficacia delle loro misure di sicurezza dell'informazione, nonché garantire che tale quadro di riferimento consideri le minacce e le vulnerabilità individuate grazie al monitoraggio delle minacce e al processo di valutazione dei rischi ICT e di sicurezza.

43. Il quadro di riferimento per la verifica della sicurezza dell'informazione dovrebbe garantire che le verifiche:

a) siano eseguite da revisori indipendenti, in possesso di sufficienti conoscenze, abilità e competenze in materia di verifica delle misure di sicurezza dell'informazione e non coinvolti nello sviluppo di tali misure;

b) comprendano vulnerability scan e penetration test (compresi quelli basati sulle minacce, ove necessario e appropriato) adeguate al livello di rischio individuato nei sistemi e nei processi aziendali.

44. Gli istituti finanziari dovrebbero eseguire verifiche continuative e ripetute delle misure di sicurezza. Per tutti i sistemi ICT critici (paragrafo 17), tali verifiche dovrebbero essere eseguite almeno annualmente e, per i prestatori di servizi di pagamento, esse fanno parte della valutazione generale dei rischi operativi e di sicurezza relativi ai servizi di pagamento prestati, conformemente all'articolo 95, paragrafo 2, della PSD2. Per i sistemi non critici le verifiche dovrebbero essere periodiche, secondo un approccio basato sul rischio, e comunque eseguite almeno ogni tre anni.

45. Gli istituti finanziari dovrebbero garantire che siano effettuate verifiche delle misure di sicurezza in caso di modifiche dell'infrastruttura, dei processi o delle procedure e se sono apportate modifiche a causa di gravi incidenti operativi o di sicurezza, o a causa del rilascio di applicazioni critiche connesse ad internet, nuove o significativamente modificate.

46. Gli istituti finanziari dovrebbero monitorare e valutare i risultati ottenuti dalle verifiche della sicurezza e di conseguenza aggiornare senza indebiti ritardi le misure di sicurezza nel caso dei sistemi ICT critici.

47. Per i prestatori di servizi di pagamento, il quadro di riferimento per la verifica della sicurezza dovrebbe comprendere anche le misure rilevanti per 1) i terminali e i dispositivi utilizzati per la prestazione dei servizi di pagamento, 2) i terminali e i dispositivi utilizzati per l'autenticazione degli utenti dei servizi di pagamento e 3) i dispositivi e il software forniti dai prestatori di servizi di pagamento agli utenti per generare/ricevere un codice di autenticazione.

48. In base alle minacce di sicurezza osservate e alle modifiche realizzate, si dovrebbero condurre verifiche per considerare scenari di potenziali attacchi rilevanti e noti.

1.4.7. Formazione e sensibilizzazione sulla sicurezza dell'informazione

49. Gli istituti finanziari dovrebbero definire un piano di formazione, comprensivo di programmi periodici di sensibilizzazione sulla sicurezza, destinato a tutti i propri dipendenti e fornitori per garantire che essi siano preparati ad adempiere i compiti e le responsabilità loro assegnati conformemente alle specifiche policy e procedure di sicurezza, per ridurre errori umani, furti, frodi, uso improprio o perdita e su come affrontare i rischi relativi alla sicurezza dell'informazione. Gli istituti finanziari dovrebbero garantire che il piano di formazione offra a tutti i loro dipendenti e fornitori occasioni formative almeno a cadenza annuale.

1.5. Gestione delle operazioni ICT

50. Gli istituti finanziari dovrebbero gestire le operazioni ICT sulla base di procedure e processi documentati e realizzati (che, per i prestatori di servizi di pagamento, includono la policy di sicurezza di cui all'articolo 5, paragrafo 1, lettera j), della PSD2) e approvati dall'organo di gestione. Questa serie di documenti dovrebbe definire le modalità di funzionamento, monitoraggio e controllo dei sistemi e servizi ICT degli istituti finanziari, compresa la

documentazione delle operazioni ICT critiche, e dovrebbe consentire agli istituti finanziari di mantenere aggiornato l'inventario delle risorse ICT.

51. Gli istituti finanziari dovrebbero assicurare che le prestazioni operative dell'ICT siano in linea con i propri requisiti aziendali. Gli istituti finanziari dovrebbero mantenere e migliorare, ove possibile, l'efficienza delle attività operative dell'ICT compresa, ma non limitandosi a, l'esigenza di considerare come ridurre al minimo i potenziali errori derivanti dall'esecuzione di attività manuali.

52. Gli istituti finanziari dovrebbero attuare procedure di registrazione e monitoraggio delle attività operative dell'ICT critiche al fine di consentire la rilevazione, l'analisi e la correzione degli errori.

53. Gli istituti finanziari dovrebbero tenere un inventario aggiornato delle loro risorse ICT (compresi i sistemi ICT, i dispositivi di rete, le banche dati, ecc.). Tale inventario dovrebbe contenere la configurazione delle risorse ICT, i collegamenti e le interdipendenze tra di esse, per consentire una corretta configurazione e un adeguato processo di gestione dei cambiamenti.

54. L'inventario delle risorse ICT dovrebbe essere sufficientemente dettagliato da consentire la rapida individuazione di una risorsa ICT, della sua ubicazione, della sua classificazione di sicurezza e della relativa titolarità. Le interdipendenze tra le risorse dovrebbero essere documentate in modo che siano d'aiuto nella risposta agli incidenti operativi e di sicurezza, compresi gli attacchi cyber.

55. Gli istituti finanziari dovrebbero monitorare e gestire il ciclo di vita delle risorse ICT, per garantire che continuino a soddisfare e a sostenere i requisiti aziendali e di gestione dei rischi. Gli istituti finanziari dovrebbero controllare se le risorse ICT sono supportate dai loro fornitori e sviluppatori esterni o interni e se tutte le patch e gli aggiornamenti pertinenti sono applicati in base a processi documentati. I rischi derivanti da risorse ICT non aggiornate o non più supportate dovrebbero essere valutati e attenuati.

56. Gli istituti finanziari dovrebbero attuare processi di pianificazione e monitoraggio delle prestazioni e della capacità per prevenire, individuare e rispondere in modo tempestivo a importanti problemi di prestazioni dei sistemi ICT e di riduzione delle loro capacità.

57. Gli istituti finanziari dovrebbero definire e attuare procedure di backup e ripristino dei dati e dei sistemi ICT per garantire il loro recupero quando necessario. L'ambito e la frequenza dei backup dovrebbero essere definiti in linea con le esigenze di ripristino dell'operatività e la criticità dei dati e dei sistemi ICT , oltre ad essere valutati in base alla analisi dei rischi effettuata. Le procedure di backup e di ripristino dovrebbero essere sottoposte a verifiche periodiche.

58. Gli istituti finanziari dovrebbero garantire che i backup dei dati e dei sistemi ICT siano conservati in modo sicuro e in luoghi sufficientemente distanti dal sito primario, in modo da non essere esposti agli stessi rischi.

3.5.1 Gestione di incidenti e problemi ICT

59. Gli istituti finanziari dovrebbero istituire e attuare un processo di gestione degli incidenti e dei problemi per monitorare e registrare gli incidenti operativi e di sicurezza in ambito ICT e per consentire agli istituti finanziari di continuare o di riprendere, in modo tempestivo, le funzioni

e i processi aziendali critici qualora si verifichino interruzioni del servizio . Gli istituti dovrebbero definire criteri e soglie appropriati per la classificazione di eventi quali gli incidenti operativi o di sicurezza, in base a quanto previsto nella sezione «Definizioni» dei presenti orientamenti, nonché definire indicatori di preallerta che consentano l'individuazione rapida di incidenti operativi o di sicurezza. Tali criteri e soglie, per i prestatori di servizi di pagamento, non pregiudicano la classificazione dei gravi incidenti ai sensi dell'articolo 96 della PSD2 e degli orientamenti in materia di segnalazione dei gravi incidenti ai sensi della PSD2 (EBA/GL/2017/10).

60. Per ridurre al minimo l'impatto degli eventi negativi e consentire un ripristino tempestivo, gli istituti finanziari dovrebbero istituire processi e strutture organizzative adeguate a garantire, in modo coerente ed integrato, un monitoraggio, una gestione e un follow-up degli incidenti operativi e di sicurezza e per assicurare che le cause di fondo siano individuate e rimosse al fine di evitare il verificarsi di incidenti ripetuti. Il processo di gestione di incidenti e problemi dovrebbe stabilire:

    a) le procedure per individuare, tracciare, registrare, categorizzare e classificare gli incidenti secondo una priorità, in base alla criticità aziendale;
    b) i ruoli e le responsabilità per i diversi scenari di incidente (ad esempio errori, malfunzionamenti, attacchi informatici);
    c) le procedure di gestione dei problemi per individuare, analizzare e risolvere le cause di fondo di uno o più incidenti: un istituto finanziario dovrebbe analizzare gli incidenti operativi o di sicurezza che potrebbero riguardarlo e che sono stati individuati o si sono verificati all'interno e/o all'esterno dell'organizzazione, e dovrebbe considerare gli insegnamenti fondamentali appresi da queste analisi e aggiornare di conseguenza le proprie misure di sicurezza;
    d) piani di comunicazione interna efficaci, comprese le procedure di segnalazione degli incidenti e di escalation, applicabili anche ai reclami dei clienti in materia di sicurezza, per garantire che:
        i) gli incidenti con un impatto negativo potenzialmente elevato sui sistemi e servizi ICT critici siano segnalati all'alta dirigenza competente e ai responsabili dell'ICT;
        ii) l'organo di gestione sia informato con una comunicazione ad-hoc nel caso di incidenti significativi e, quanto meno, tenuto al corrente dell'impatto, della risposta e dei controlli supplementari da definire a seguito degli incidenti.
    e) procedure di risposta agli incidenti per attenuare gli impatti conseguenti e garantire che il servizio diventi operativo e sicuro in modo tempestivo;
    f) piani di comunicazione esterna specifici per le funzioni e i processi aziendali critici, al fine di:
        i) collaborare con i soggetti interessati per garantire una risposta efficace e un pronto recupero dall'incidente;

ii) fornire informazioni tempestive ai soggetti esterni (ad esempio clienti, altri partecipanti al mercato, autorità di vigilanza), se del caso e in linea con la normativa applicabile.

1.6. Gestione dei progetti e dei cambiamenti ICT

1.6.1. Gestione dei progetti ICT

61. Gli istituti finanziari dovrebbero mettere in atto un piano e/o un processo per il governo dei progetti che definisca i ruoli, il coinvolgimento e le responsabilità per supportare efficacemente l'attuazione della strategia ICT.

62. Gli istituti finanziari dovrebbero monitorare e attenuare adeguatamente i rischi derivanti dal proprio portafoglio di progetti ICT (gestione del piano), tenendo conto anche dei rischi che potrebbero scaturire dalle interdipendenze tra progetti diversi e dalle dipendenze di più progetti dalle stesse risorse e/o competenze.

63. Gli istituti finanziari dovrebbero definire e attuare una policy di gestione dei progetti ICT che comprenda come minimo:

    a) gli obiettivi del progetto;
    b) i ruoli e le responsabilità;
    c) una valutazione dei rischi del progetto;
    d) il piano, i tempi e le fasi del progetto;
    e) le tappe fondamentali;
    f) i requisiti di gestione dei cambiamenti.

64. La policy di gestione dei progetti ICT dovrebbe garantire che i requisiti di sicurezza dell'informazione siano analizzati e approvati da una funzione indipendente rispetto a quella di sviluppo.

65. Gli istituti finanziari dovrebbero garantire che tutte le aree interessate da un progetto ICT siano rappresentate nel team di progetto e che quest'ultimo abbia le conoscenze necessarie per garantire un'attuazione sicura e di successo del progetto.

66. L'avvio e l'avanzamento dei progetti ICT e i rischi ad essi associati dovrebbero essere comunicati all'organo di gestione, individualmente o in forma aggregata, in funzione dell'importanza e delle dimensioni dei progetti ICT, su base regolare o puntuale, a seconda dei casi. Gli istituti finanziari dovrebbero includere il rischio dei progetti nel loro quadro di riferimento per la gestione dei rischi.

1.6.2. Acquisizione e sviluppo di sistemi ICT

67. Gli istituti finanziari dovrebbero sviluppare e attuare un processo che disciplini l'acquisizione, lo sviluppo e la manutenzione dei sistemi ICT. Tale processo dovrebbe essere progettato utilizzando un approccio basato sul rischio.

68. Gli istituti finanziari dovrebbero garantire, prima di qualsiasi acquisizione o sviluppo di sistemi ICT, che i requisiti funzionali e non funzionali (compresi i requisiti di sicurezza dell' informazione) siano chiaramente definiti e approvati dalla dirigenza aziendale competente.

69. Gli istituti finanziari dovrebbero garantire l'adozione di misure volte ad attenuare il rischio di alterazioni non intenzionali o manipolazioni intenzionali dei sistemi ICT durante lo sviluppo e nell'implementazione in ambiente di produzione.

70. Gli istituti finanziari dovrebbero disporre di una metodologia per verificare e approvare i sistemi ICT prima del loro primo utilizzo. Tale metodologia dovrebbe prendere in considerazione la criticità dei processi e delle risorse aziendali. I test dovrebbero garantire che i nuovi sistemi ICT funzionino come previsto. Gli istituti dovrebbero inoltre utilizzare ambienti di test che riflettano adeguatamente l'ambiente di produzione.

71. Gli istituti finanziari dovrebbero testare i sistemi ICT, i servizi ICT e le misure di sicurezza dell'informazione per individuare potenziali debolezze, violazioni e incidenti di sicurezza.

72. Gli istituti finanziari dovrebbero realizzare ambienti ICT separati per garantire un'adeguata segregazione delle attività e per mitigare l'impatto di modifiche non verificate dei sistemi di produzione. Nello specifico, gli istituti finanziari dovrebbero garantire la segregazione degli ambienti di produzione da quelli di sviluppo e di test e da altri ambienti non produttivi. Gli istituti finanziari dovrebbero garantire l'integrità e la riservatezza dei dati di produzione in ambienti non produttivi. L'accesso ai dati di produzione è riservato ai soli utenti autorizzati.

73. Gli istituti finanziari dovrebbero attuare misure per proteggere l'integrità dei codici sorgente dei sistemi ICT sviluppati internamente. Dovrebbero inoltre documentare in modo esaustivo lo sviluppo, l'implementazione, il funzionamento e/o la configurazione dei sistemi ICT per ridurre completamente qualsiasi dipendenza non necessaria da esperti in materia. La documentazione dei sistemi ICT dovrebbe contenere, quando possibile, quanto meno la documentazione per l'utente, la documentazione tecnica del sistema e le procedure operative.

74. I processi di acquisizione e sviluppo di sistemi ICT di un istituto finanziario dovrebbero applicarsi anche ai sistemi ICT sviluppati o gestiti direttamente dagli utenti delle funzioni aziendali esterne all'organizzazione dell'ICT (ad esempio, applicazioni informatiche dell'utente finale) utilizzando un approccio basato sul rischio. L'istituto finanziario dovrebbe tenere un registro di queste applicazioni che supportano funzioni o processi aziendali critici.

1.6.3. Gestione dei cambiamenti ICT

75. Gli istituti finanziari dovrebbero istituire e attuare un processo di gestione dei cambiamenti ICT per garantire che tutte le modifiche dei sistemi ICT siano registrate, testate, valutate, approvate, implementate e verificate in modo controllato. Gli istituti finanziari dovrebbero gestire i cambiamenti durante le emergenze (vale a dire le modifiche che devono essere introdotti il più presto possibile) seguendo procedure che forniscano garanzie adeguate.

76. Gli istituti finanziari dovrebbero stabilire se modifiche del contesto operativo esistente influenzino le misure di sicurezza adottate o comportino l'adozione di ulteriori misure per mitigare i relativi rischi. Tali modifiche dovrebbero essere coerenti con il processo di gestione del cambiamento formalizzato dagli istituti finanziari.

1.7. Gestione della continuità operativa

77. Gli istituti finanziari dovrebbero istituire un solido processo di gestione della continuità operativa per massimizzare le loro capacità di prestare servizi su base continuativa e per limitare le perdite in caso di gravi interruzioni dell'operatività, conformemente all'articolo 85, paragrafo 2, della direttiva 2013/36/UE e al titolo VI degli orientamenti dell'ABE sulla governance interna (EBA/GL/2017/11).

1.7.1. Analisi di impatto sull'operatività

78. Nell'ambito di una solida gestione della continuità operativa, gli istituti finanziari dovrebbero condurre un'analisi di impatto aziendale (Business Impact Analysis-BIA) esaminando la propria esposizione a diverse interruzioni dell'operatività e valutando i loro potenziali impatti (anche in termini di riservatezza, integrità e disponibilità), con un approccio sia quantitativo che qualitativo, utilizzando dati interni e/o esterni (ad esempio, dati di fornitori terzi rilevanti per un processo aziendale o dati di pubblico dominio che possono essere utili per l'analisi di impatto sull'operatività), e condurre inoltre un'analisi di scenario. L'analisi di impatto sull'operatività dovrebbe considerare la criticità delle funzioni aziendali, dei processi di supporto, dei soggetti terzi e delle risorse informatiche individuate e classificate, nonché le loro interdipendenze, conformemente alla sezione 1.3.3.

79. Gli istituti finanziari dovrebbero garantire che i loro sistemi ICT e servizi ICT siano progettati e allineati con la BIA, ad esempio prevedendo la ridondanza di alcune componenti critiche per evitare che interruzioni si ripercuotano su tali componenti.

1.7.2. Pianificazione della continuità operativa

80. Sulla base delle analisi di impatto sull'operatività, gli istituti finanziari dovrebbero elaborare piani di continuità operativa, che dovrebbero essere documentati e approvati dai rispettivi organi di gestione. Tali piani dovrebbero considerare specificamente i rischi che potrebbero incidere negativamente sui sistemi ICT e sui servizi ICT. I piani dovrebbero supportare gli obiettivi di proteggere e, se necessario, ripristinare la riservatezza, l'integrità e la disponibilità delle funzioni aziendali, dei processi di supporto e delle risorse informatiche degli istituti finanziari. Durante l'elaborazione di tali piani gli istituti finanziari dovrebbero coordinarsi con i soggetti interessati interni ed esterni rilevanti, se del caso.

81. Gli istituti finanziari dovrebbero adottare piani di continuità operativa per garantire di poter reagire adeguatamente a potenziali scenari di guasto e di riuscire a ripristinare le operazioni delle funzioni aziendali critiche a seguito di interruzioni entro un determinato tempo massimo di ripristino («recovery time objective», RTO: il tempo massimo entro il quale un sistema o un processo deve essere ripristinato dopo un incidente) e un determinato punto di ripristino

prefissato («recovery point objective», RPO: il periodo massimo durante il quale è accettabile che i dati vadano persi in caso di incidente). Nei casi di gravi interruzioni dell'operatività che attivano specifici piani di continuità operativa, gli istituti finanziari dovrebbero stabilire la priorità delle azioni di continuità operativa usando un approccio basato sul rischio, che può essere a sua volta basato sulle valutazioni dei rischi effettuate ai sensi della sezione 1.3.3. Per i prestatori di servizi di pagamento ciò può comprendere, ad esempio, facilitare il successivo trattamento delle transazioni critiche mentre proseguono le azioni correttive.

82. Gli istituti finanziari nel proprio piano di continuità operativa dovrebbero prendere in considerazione una serie di diversi scenari ai quali potrebbero essere esposti, , compresi quelli estremi purché plausibili, tra cui uno scenario di attacco informatico, e valutarne gli impatti potenziali. Sulla base di questi scenari, gli istituti finanziari dovrebbero descrivere come viene garantita la continuità dei sistemi ICT e dei servizi ICT, nonché la sicurezza dell'informazione dell'istituto finanziario.

1.7.3. Piani di risposta e di ripristino

83. Sulla base delle analisi di impatto aziendale (paragrafo 78) e degli scenari plausibili (paragrafo 82), gli istituti finanziari dovrebbero elaborare piani di risposta e di ripristino. Tali piani dovrebbero specificare le condizioni che potrebbero provocare l'attivazione dei piani stessi e le azioni da intraprendere per garantire la disponibilità, la continuità e il ripristino quanto meno dei sistemi e servizi ICT critici degli istituti finanziari. I piani di risposta e di ripristino dovrebbero mirare a conseguire gli obiettivi di ripristino dell'operatività degli istituti finanziari.

84. I piani di risposta e di ripristino dovrebbero considerare le opzioni di ripristino sia a breve che a lungo termine. I piani dovrebbero:

    a) essere focalizzati sul ripristino dell'operatività delle funzioni aziendali critiche, dei processi di supporto, delle risorse informatiche e delle loro interdipendenze per evitare effetti negativi sul funzionamento degli istituti finanziari e sul sistema finanziario, compresi i sistemi di pagamento e gli utenti dei servizi di pagamento, oltre a garantire l'esecuzione delle transazioni di pagamento pendenti;
    b) essere documentati e messi a disposizione reparti aziendali e di supporto, nonché prontamente accessibili in caso di emergenza;
    c) essere aggiornati sulla base di quanto appreso dagli incidenti, dalle verifiche, dall'individuazione di nuovi rischi e minacce, nonché dai cambiamenti degli obiettivi e dalle priorità di ripristino.

85. I piani dovrebbero anche considerare opzioni alternative nel caso in cui il ripristino non fosse fattibile nel breve periodo a causa di costi, rischi, fattori logistici o circostanze impreviste.

86. Inoltre, nell'ambito dei piani di risposta e di ripristino, gli istituti finanziari dovrebbero considerare e attuare misure di continuità per mitigare gli effetti delle inadempienze dei fornitori terzi, che sono di fondamentale importanza per la continuità dei servizi ICT di un istituto finanziario (in linea con le disposizioni degli orientamenti dell'ABE in materia di esternalizzazione (EBA/GL/2019/02) relative ai piani di continuità operativa).

1.7.4. Verifica dei piani

87. Gli istituti finanziari dovrebbero verificare periodicamente i propri piani di continuità operativa. In particolare, dovrebbero garantire che i piani di continuità operativa delle funzioni aziendali critiche, dei processi di supporto, delle risorse informatiche e delle loro interdipendenze (compresi quelli forniti da soggetti terzi, se del caso) siano verificati almeno con cadenza annuale, conformemente al paragrafo 89.

88. I piani di continuità operativa dovrebbero essere aggiornati almeno annualmente, sulla base dei risultati delle verifiche, delle informazioni sulle minacce esistenti e di quanto appreso dagli eventi precedenti. Tutte le modifiche degli obiettivi di ripristino (tra cui RTO e RPO) e/o delle funzioni aziendali, dei processi di supporto e delle risorse informatiche dovrebbero inoltre essere prese in considerazione, se del caso, quale base per l'aggiornamento dei piani di continuità operativa.

89. Le verifiche dei piani di continuità operativa degli istituti finanziari dovrebbero dimostrare che gli istituti sono in grado di sostenere la redditività delle loro attività fino a quando le operazioni critiche non vengono ristabilite. In particolare, esse dovrebbero:

    a) prevedere la verifica di una serie adeguata di scenari gravi ma plausibili, inclusi quelli presi in considerazione per l'elaborazione dei piani di continuità operativa (nonché la verifica dei servizi forniti da soggetti terzi, se possibile); ciò dovrebbe includere il trasferimento delle funzioni aziendali critiche, dei processi di supporto e delle risorse informatiche all'ambiente di «disaster recovery» e la dimostrazione che possono così essere gestiti per un periodo di tempo sufficientemente rappresentativo e che il normale funzionamento può essere successivamente ripristinato;
    b) essere progettate in modo tale da mettere alla prova le ipotesi su cui i piani di continuità operativa si fondano, inclusi le disposizioni organizzative e i piani di comunicazione in caso di crisi;
    c) includere procedure per verificare la capacità del personale e dei fornitori, nonché dei sistemi e servizi ICT degli istituti finanziari di rispondere adeguatamente agli scenari di cui al paragrafo 89, lettera a).

90. I risultati delle verifiche dovrebbero essere documentati ed eventuali carenze individuate a seguito delle verifiche dovrebbero essere analizzate, affrontate e segnalate all'organo di gestione.

1.7.5. Comunicazione in caso di crisi

91. In caso di interruzione dell'operatività o emergenza aziendale e durante l'attuazione dei piani di continuità operativa, gli istituti finanziari dovrebbero garantire di avere delle efficaci misure per la comunicazione in caso di crisi, tali da comunicare in modo tempestivo e appropriato a tutti i soggetti interessati rilevanti, interni ed esterni, comprese le autorità nazionali ove richiesto dalla normativa nazionale, e ai fornitori di servizi pertinenti (fornitori esterni, entità del gruppo o fornitori terzi).

1.8. Gestione del rapporto con gli utenti dei servizi di pagamento

92. I prestatori di servizi di pagamento dovrebbero definire e attuare processi per accrescere le conoscenze degli utenti dei servizi di pagamento sui rischi per la sicurezza connessi ai servizi stessi, fornendo agli utenti assistenza e orientamento.

93. L'assistenza e l'orientamento forniti agli utenti dei servizi di pagamento dovrebbero essere aggiornati in base alle nuove minacce e vulnerabilità; gli aggiornamenti dovrebbero essere comunicati agli utenti.

94. Laddove permesso dalle modalità di funzionamento del servizio, i prestatori di servizi di pagamento dovrebbero consentire agli utenti di disattivare specifiche funzionalità di pagamento connesse ai servizi di pagamento offerti.

95. Qualora, ai sensi dell'articolo 68, paragrafo 1, della direttiva (UE) 2015/2366, un prestatore di servizi di pagamento abbia concordato con il pagatore limiti di spesa per le operazioni di pagamento eseguite mediante specifici strumenti di pagamento, il prestatore dovrebbe concedere al pagatore la possibilità di modificare tali limiti elevandoli al limite massimo concordato.

96. I prestatori di servizi di pagamento dovrebbero offrire agli utenti la possibilità di ricevere avvisi in caso di tentativi, iniziati e/o falliti, di effettuare operazioni di pagamento, consentendo così agli utenti di rilevare un uso fraudolento o dannoso del proprio account.

97. I prestatori di servizi di pagamento dovrebbero tenere gli utenti al corrente degli aggiornamenti delle procedure di sicurezza che li riguardano per la prestazione dei servizi di pagamento.

98. I prestatori di servizi di pagamento dovrebbero fornire agli utenti assistenza su tutte le domande, le richieste di aiuto e le notifiche di anomalie o le questioni riguardanti la sicurezza dei servizi di pagamento. Gli utenti dei servizi di pagamento dovrebbero essere adeguatamente informati su come ottenere tale assistenza.