EIOPA-BoS-20/600

Orientamenti sulla sicurezza e sulla governance della tecnologia dell'informazione e comunicazione

EIOPA – Westhafen Tower, Westhafenplatz 1 – 60327 Francoforte – Germania – Tel. + 49 69-951119-20;
Fax + 49 69-951119-19; e-mail: info@eiopa.europa.eu sito: www.eiopa.europa.eu

Indice

Contesto

1. Ai sensi dell'articolo 16 del regolamento (UE) n. 1094/2010, l'Autorità europea delle assicurazioni e delle pensioni aziendali e professionali (EIOPA) può emanare orientamenti e formulare raccomandazioni indirizzati alle autorità e agli istituti finanziari competenti al fine di istituire prassi di vigilanza uniformi, efficienti ed efficaci e assicurare l'applicazione comune, uniforme e coerente del diritto dell'Unione.

2. A norma dell'articolo 16, paragrafo 3, di detto regolamento, le autorità e gli istituti finanziari competenti sono tenuti a compiere ogni sforzo per conformarsi agli orientamenti e alle raccomandazioni.

3. L'EIOPA ha ravvisato la necessità di elaborare orientamenti specifici sulla sicurezza e sulla governance della tecnologia dell'informazione e comunicazione (ICT) in riferimento agli articoli 41 e 44 della direttiva 2009/138/CE nel contesto dell'analisi effettuata in risposta al piano d'azione FinTech della Commissione europea [COM(2018) 109 final], al piano di convergenza in materia di vigilanza 2018-2019 ([1]) dell'EIOPA e alle successive interazioni con diversi altri interlocutori ([2]).

4. Come indicato nel parere congiunto delle autorità europee di vigilanza alla Commissione europea, gli orientamenti dell'EIOPA sul sistema di governance «*non riflettono adeguatamente l'importanza di trattare la gestione del rischio sulla ICT (compresi quelli informatici)*». Non esistono orientamenti per quanto concerne gli elementi fondamentali generalmente riconosciuti come facenti parte di un'adeguata sicurezza e governance della ICT.

5. Secondo il parere congiunto di cui sopra, l'analisi framework (normativo) europeo ha mostrato che la maggioranza degli Stati membri dell'UE ha definito norme nazionali per la sicurezza e la governance della ICT. Sebbene i requisiti siano simili, il quadro normativo appare ancora frammentato. Inoltre, un'indagine sulle attuali prassi di vigilanza ne ha rivelato la disomogeneità: da «nessuna vigilanza specifica» a «forte vigilanza» (comprese «ispezioni off-site» e «ispezioni on site»).

6. In aggiunta, la complessità della ICT è in aumento, così come la frequenza degli incidenti correlati (compresi quelli informatici), oltre all'aumento dell'impatto negativo di tali incidenti sul funzionamento operativo delle imprese. Per tale motivo, la gestione dei rischi ICT e di sicurezza è fondamentale affinché un'impresa consegua i propri obiettivi strategici, aziendali, operativi e reputazionali.

7. Inoltre, in tutto il settore assicurativo, compresi i modelli di business sia tradizionali sia innovativi, vi è una crescente dipendenza dalla ICT nell'erogazione di servizi assicurativi e nel normale funzionamento operativo delle imprese, ad esempio la digitalizzazione del settore assicurativo (InsurTech, IoT, ecc.) e l'interconnessione mediante canali di telecomunicazione (Internet, connessioni mobile e wireless e reti di comunicazione geografica). Ciò rende le operazioni delle imprese vulnerabili agli incidenti di sicurezza, inclusi gli attacchi informatici. È quindi importante garantire che le imprese siano adeguatamente preparate a gestire i propri rischi ICT e di sicurezza.

([1]) https://www.eiopa.europa.eu/supervisory-convergence-plans-and-reports_en

([2]) La relazione pubblicata dall'EIOPA in risposta al piano d'azione per le tecnologie finanziarie della Commissione europea può essere consultata qui.

8. Inoltre, riconoscendo che le imprese debbano essere preparate per il rischio informatico ([3]) e disporre di un solido quadro di cibersicurezza, i presenti orientamenti includono anche aspetti di cibersicurezza nell'ambito delle misure di sicurezza delle informazioni dell'impresa. Sebbene i presenti orientamenti riconoscano che la cibersicurezza vada affrontata nell'ambito della gestione generale dei rischi ICT e di sicurezza di un'impresa, è importante sottolineare che gli attacchi informatici presentano alcune caratteristiche specifiche, che dovrebbero essere prese in considerazione per garantire che le misure di sicurezza delle informazioni mitighino adeguatamente il rischio informatico:

   a) gli attacchi informatici sono spesso più difficili da gestire (ad esempio in termini di individuazione, protezione, rilevamento, contromisura e recupero completo) rispetto alla maggior parte delle altre fonti di rischio ICT e di sicurezza, e anche l'entità del danno non è facile da quantificare;

   b) alcuni attacchi informatici possono rendere inefficaci la gestione ordinaria dei rischi e i dispositivi messi in atto per la continuità operativa, così come le procedure di disaster recovery, poiché potrebbero propagare malware ai sistemi di backup allo scopo di renderli inutilizzabili o corrompere i dati di backup;

   c) i fornitori di servizi, i broker, gli agenti (autorizzati) e altri intermediari possono diventare veicoli di propagazione di attacchi informatici. Le minacce silenziose e contagiose possono avvalersi dell'interconnettività mediante collegamenti di telecomunicazioni di terzi per raggiungere il sistema ICT dell'impresa. Pertanto, un'impresa interconnessa con scarsa rilevanza individuale può diventare vulnerabile e fonte di propagazione del rischio, e potrebbe avere un impatto sistemico. Stando al principio dell'anello più debole, la cibersicurezza non rappresenta un problema solo per i principali operatori di mercato o fornitori di servizi essenziali.

9. I presenti orientamenti si prefiggono l'obiettivo di:

   a) fornire chiarimenti e trasparenza agli operatori di mercato riguardo alle informazioni minime attese e alle capacità di cibersicurezza, ossia alla configurazione di riferimento per la sicurezza;

   b) evitare potenziali arbitraggi normativi;

   c) promuovere la convergenza in materia di vigilanza per quanto riguarda le aspettative e i processi applicabili in relazione alla sicurezza e alla governance delle ICT come chiave per una corretta gestione dei rischi ICT e di sicurezza.

([3]) Per una definizione di rischio informatico, si rimanda al Cyber Lexicon dell'FSB, 12 novembre 2018, https://www.fsb.org/wp-content/uploads/P121118-1.pdf

Orientamenti sulla sicurezza e sulla governance della tecnologia dell'informazione e comunicazione

Introduzione

1. Come previsto dall'articolo 16 del regolamento (UE) n. 1094/2010 ([4]), l'Autorità europea delle assicurazioni e delle pensioni aziendali e professionali (EIOPA) emana i presenti orientamenti rivolti alle autorità di vigilanza per fornire alle imprese di assicurazione e di riassicurazione (indicate collettivamente come «imprese») le indicazioni in materia di governance previste dalla direttiva 2009/138/CE ([5]) («direttiva Solvency II») e dal regolamento delegato (UE) 2015/35 ([6]) della Commissione («regolamento delegato») da applicare nel contesto della sicurezza e della governance delle tecnologie dell'informazione e della comunicazione (ICT). A tal fine, i presenti orientamenti si basano sulle disposizioni in materia di governance previste dagli articoli 41, 44, 46, 47, 132 e 246 della direttiva solvibilità II e dagli articoli da 258 a 260, 266, da 268 a 271 e 274 del regolamento delegato. Inoltre, si basano anche sulle indicazioni fornite dagli orientamenti dell'EIOPA sul sistema di governance (EIOPA-BoS-14/253) ([7]) e dagli orientamenti dell'EIOPA in materia di esternalizzazione a fornitori di servizi cloud (EIOPA-BoS-19/270) ([8]).
2. Gli orientamenti si applicano sia alle singole imprese sia, *mutatis mutandis*, a livello di gruppo ([9]).
3. Nel conformarsi o nel vigilare la conformità ai presenti orientamenti, le autorità competenti tengono conto del principio di proporzionalità ([10]), per garantire che le disposizioni in materia di governance, comprese quelle relative alla sicurezza e alla governance delle ICT, siano proporzionate alla natura, alla portata e alla complessità dei rischi corrispondenti che le imprese si trovano o possono trovarsi ad affrontare.
4. I presenti orientamenti vanno letti in combinato disposto con la direttiva solvibilità II, il regolamento delegato, gli orientamenti dell'EIOPA sul sistema di governance e quelli in materia di esternalizzazione a fornitori di servizi cloud, che rimangono impregiudicati. I presenti orientamenti sono da intendersi come neutrali sotto il profilo tecnologico e metodologico.

Definizioni

5. Se non definiti nei presenti orientamenti, i termini assumono il significato definito nella direttiva solvibilità II.
6. Ai fini dei presenti orientamenti, si applicano le seguenti definizioni:

([4]) 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).

([5]) Direttiva 2009/138/CE del Parlamento europeo e del Consiglio, del 25 novembre 2009, in materia di accesso ed esercizio delle attività di assicurazione e di riassicurazione (solvibilità II) (GU L 335 del 17.12.2009, pag. 1).

([6]) Regolamento delegato 2015/35 della Commissione, del 10 ottobre 2014, che integra la direttiva 2009/138/CE del Parlamento europeo e del Consiglio in materia di accesso ed esercizio delle attività di assicurazione e di riassicurazione (solvibilità II) (GU L 12 del 17.1.2015, pag. 1).

([7]) https://www.eiopa.europa.eu/content/guidelines-system-governance_en?source=search

([8]) https://www.eiopa.europa.eu/content/guidelines-outsourcing-cloud-service-providers

([9]) Articolo 212, paragrafo 1, della direttiva 2009/138/CE.

([10]) Articolo 29, paragrafo 3, della direttiva 2009/138/CE.

Proprietario della risorsa	Persona o entità avente la responsabilità e l'autorità su una risorsa informativa o ICT.
Disponibilità	Proprietà di accessibilità e usabilità su richiesta (tempestività) di un'entità autorizzata.
Riservatezza	Proprietà per cui le informazioni non sono rese disponibili né divulgate a persone, entità, procedure o sistemi non autorizzati.
Attacco informatico	Qualsiasi tipo di pirateria informatica che comporta un tentativo offensivo/doloso volto a distruggere, rivelare, alterare, disattivare, sottrarre o ottenere l'accesso non autorizzato o a fare un uso non autorizzato di una risorsa informativa ai danni dei sistemi ICT.
Cibersicurezza	Mantenimento della riservatezza, dell'integrità e della disponibilità delle informazioni e/o dei sistemi informativi per il tramite del mezzo informatico.
Risorsa ICT	Qualunque software o hardware presenti nel contesto aziendale.
Progetti ICT	Qualsiasi progetto, o parte di esso, in cui i sistemi e i servizi ICT sono modificati, sostituiti, dismessi o implementati.
Rischio ICT e di sicurezza	Inteso come sottocomponente del rischio operativo; il rischio di perdita dovuta alla violazione della riservatezza, la mancata integrità dei sistemi e dei dati, l'inadeguatezza o l'indisponibilità dei sistemi e dei dati o l'incapacità di sostituire le ICT entro ragionevoli limiti di tempo e costi in caso di modifica ai requisiti del contesto esterno o dell'attività (ossia la flessibilità). Questo comprende i rischi informatici nonché i rischi di sicurezza delle informazioni derivanti da processi interni inadeguati o errati o da eventi esterni, compresi gli attacchi informatici o una sicurezza fisica inadeguata.
Sicurezza delle informazioni	Salvaguardia della riservatezza, dell'integrità e della disponibilità delle informazioni e/o dei sistemi informativi. Inoltre, possono subentrare anche altre proprietà, come l'autenticità, la responsabilità, la non disconoscibilità e l'affidabilità.
Servizi ICT	I servizi erogati tramite sistemi ICT e fornitori di servizi a uno o più utenti interni o esterni.

Sistemi ICT	Insieme di applicazioni, servizi, risorse tecnologiche informative, risorse ICT o altri componenti per la gestione delle informazioni, che comprende l'ambiente operativo.
Risorsa informativa	Una raccolta di informazioni, tangibile o intangibile, che merita protezione.
Integrità	Proprietà di esattezza e completezza.
Incidente operativo o di sicurezza	Singolo evento o serie di eventi collegati non pianificati che ha o probabilmente avrà un impatto negativo sull'integrità, sulla disponibilità e sulla riservatezza dei sistemi e servizi ICT.
Fornitore di servizi	Un terzo che svolge in tutto o in parte un processo, un servizio o un'attività nell'ambito di un accordo di esternalizzazione.
Threat Led Penetration Testing	Tentativo controllato di pregiudicare la resilienza informatica di un'entità simulando le tattiche, le tecniche e le procedure di cui si avvalgono gli autori di minacce nella vita reale. Si basa su minacce mirate e si concentra sulle persone, sui processi e sulla tecnologia di un'entità, con conoscenza predittiva e impatto sulle operazioni minimi.
Vulnerabilità	Debolezza, suscettibilità o difetto di una risorsa o di un controllo che può essere sfruttato da una o più minacce.

7. I presenti orientamenti si applicano a partire dal 1º luglio 2021.

Orientamento 1 – Proporzionalità

8. Le imprese applicano i presenti orientamenti proporzionalmente alla natura, alla portata e alla complessità dei rischi inerenti all'attività che esse svolgono.

Orientamento 2 – La ICT all'interno del sistema di governance

9. L'organo amministrativo, direttivo o di vigilanza (OADV) deve garantire che nell'ambito del sistema di governance delle imprese, con particolare riferimento al sistema di gestione dei rischi e di controllo interno, i rischi ICT e di sicurezza delle imprese siano gestiti in maniera adeguata.

10. L'OADV assicura che il numero e le competenze del personale nelle imprese siano adeguati per soddisfare le esigenze operative della ICT e supportare i processi di gestione dei rischi ICT e di sicurezza in maniera continuativa, oltre ad assicurare l'attuazione della loro strategia in materia di ICT. Inoltre, il personale riceve regolarmente una formazione adeguata sui rischi ICT e di sicurezza, compresa quella sulla sicurezza delle informazioni, come stabilito nell'orientamento 13.

11. L'OADV assicura che le risorse allocate siano adeguate per adempiere ai requisiti di cui sopra.

Orientamento 3 – Strategia in materia di ICT

12. Ricade in capo all'OADV la responsabilità generale di impostare e approvare il piano strategico in materia di ICT delle imprese nel quadro e in conformità della loro strategia aziendale generale, nonché di supervisionarne la comunicazione e l'attuazione.

13. La strategia in materia di ICT definisce almeno:

    a) le modalità con cui si evolvono le ICT delle imprese per favorire e attuare efficacemente la loro strategia aziendale, tra cui l'evoluzione della struttura organizzativa, i modelli di business, il sistema ICT e i rapporti con i principali fornitori di servizi;

    b) l'evoluzione dell'architettura ICT, compresi i rapporti con i fornitori di servizi;

    c) obiettivi chiari in materia di sicurezza delle informazioni, con particolare riguardo ai sistemi e ai servizi ICT, al personale e ai processi.

14. Le imprese assicurano che la strategia in materia di ICT sia attuata, adottata e comunicata tempestivamente a tutto il personale e a tutti i fornitori di servizi interessati, ove applicabile e pertinente.

15. Le imprese istituiscono un processo mediante il quale monitorare e misurare il livello di efficacia dell'attuazione di tale strategia. Tale processo è rivisto e aggiornato regolarmente.

Orientamento 4 – Rischi ICT e di sicurezza nell'ambito del sistema di gestione dei rischi

16. All'OADV compete la responsabilità generale di istituire un sistema efficace per la gestione dei rischi ICT e di sicurezza nel quadro del sistema di gestione globale dei rischi dell'impresa. Ciò prevede la determinazione dei limiti di tolleranza a questo tipo di rischi, in conformità della strategia di rischio dell'impresa, e una relazione scritta periodica sull'esito del processo di gestione dei rischi indirizzata all'OADV.

17. Nell'ambito del proprio sistema di gestione globale dei rischi, in relazione ai rischi ICT e di sicurezza (definendo al contempo il requisito di protezione ICT descritto di seguito), le imprese devono almeno:

    a) delineare e aggiornare regolarmente una mappatura dei propri processi e attività di tipo operativo, aree funzionali, ruoli e risorse (per esempio, risorse informative e risorse ICT) al fine di individuarne la rilevanza e le interdipendenze con i rischi ICT e di sicurezza;

    b) individuare e quantificare tutti i rischi ICT e di sicurezza ai quali sono esposte e classificare i processi e le attività di tipo operativo, le aree funzionali, i ruoli e le risorse (per esempio, risorse informative e risorse ICT) così individuati in termini di criticità. Le imprese valutano altresì i requisiti di protezione almeno per quanto riguarda la riservatezza, l'integrità e la disponibilità dei processi e delle attività di tipo operativo, delle aree funzionali, dei ruoli e delle risorse (per esempio, risorse informative e risorse ICT). I proprietari delle risorse, che sono responsabili della classificazione delle risorse stesse, sono adeguatamente identificati;

c) i metodi utilizzati per stabilire la criticità e il livello di protezione richiesto, con particolare riguardo agli obiettivi di protezione in termini di integrità, disponibilità e riservatezza, fanno sì che i requisiti di protezione risultanti siano coerenti ed esaustivi;

d) la quantificazione dei rischi ICT e di sicurezza è svolta sulla base di criteri di rischio ICT e di sicurezza definiti tenendo conto della criticità dei processi e delle attività di tipo operativo, delle aree funzionali, dei ruoli e delle risorse (per esempio, risorse informative e risorse ICT), dell'entità delle vulnerabilità note e degli incidenti precedenti che hanno avuto ricadute sull'impresa;

e) la valutazione dei rischi ICT e di sicurezza viene effettuata e documentata regolarmente, in particolare prima di qualsiasi cambiamento importante previsto nelle infrastrutture, nei processi o nelle procedure che interessano i processi e le attività di tipo operativo, le aree funzionali, i ruoli e le risorse (per esempio, risorse informative e risorse ICT);

f) sulla base della propria valutazione dei rischi, le imprese definiscono e attuano misure per gestire i rischi ICT e di sicurezza individuati e proteggere le risorse informative in base alla loro classificazione. Va prevista la definizione di misure per gestire i rischi residui in essere.

18. L'esito del processo di gestione dei rischi ICT e di sicurezza è approvato dall'OADV e incluso nel processo di gestione dei rischi operativi nel quadro della gestione globale dei rischi delle imprese.

Orientamento 5 – Audit

19. La governance, i sistemi e i processi delle imprese per quanto riguarda i rischi ICT e di sicurezza sono periodicamente sottoposti ad audit, in linea con il piano di audit delle imprese ([11]), da parte di revisori con adeguate conoscenze, competenze e capacità in materia di rischi ICT e di sicurezza, affinché l'OADV abbia una garanzia indipendente della loro efficacia. La frequenza e l'oggetto di tali audit sono commisurati ai rischi ICT e di sicurezza in questione.

Orientamento 6 – Politica e misure riguardanti la sicurezza delle informazioni

20. Le imprese definiscono una politica scritta sulla sicurezza delle informazioni approvata dall'OADV nella quale siano stabiliti i principi e le norme di alto livello volti a tutelare la riservatezza, l'integrità e la disponibilità delle informazioni delle imprese onde sostenere l'attuazione della strategia in materia di ICT.

21. Tale policy include una descrizione dei ruoli e delle responsabilità principali nella gestione della sicurezza delle informazioni e fissare i requisiti per il personale, i processi e la tecnologia in relazione alla sicurezza delle informazioni, riconoscendo che il personale a tutti i livelli ha la responsabilità di garantire la sicurezza delle informazioni delle imprese.

22. Tale policy va comunicata all'interno dell'impresa e applicata a tutto il personale. Ove praticabile e pertinente, la politica riguardante la sicurezza delle informazioni o parti della stessa è altresì comunicata e applicata ai fornitori di servizi.

23. Sulla base di tale politica, le imprese stabiliscono e attuano procedure e misure di sicurezza delle informazioni più specifiche al fine, tra l'altro, di mitigare i rischi ICT

([11]) Articolo 271 del regolamento delegato.

e di sicurezza ai quali sono esposte. Le procedure in questione includono tutti i processi descritti nei presenti orientamenti.

Orientamento 7 – Funzione di sicurezza delle informazioni

24. Le imprese istituiscono, nell'ambito del proprio sistema di governance e nel rispetto del principio di proporzionalità, una funzione dedicata alla sicurezza delle informazioni, le cui responsabilità sono attribuite a una persona designata. Le imprese assicurano l'indipendenza e l'obiettività di tale funzione, separandola opportunamente dai processi operativi e di sviluppo delle ICT. La persona designata per tale funzione riferisce all'OADV.

25. I compiti di tale funzione sono, in genere, i seguenti:

    a) assistere l'OADV nella definizione e nel rispetto della politica riguardante la sicurezza delle informazioni delle imprese e controllarne l'attuazione;

    b) riferire e prestare consulenza all'OADV regolarmente e in relazione a fattispecie concrete sullo stato della sicurezza delle informazioni e sui relativi sviluppi;

    c) monitorare e riesaminare l'attuazione delle misure di sicurezza delle informazioni;

    d) assicurare il rispetto dei requisiti di sicurezza delle informazioni quando ci si avvale di fornitori di servizi;

    e) assicurare che tutti i dipendenti e i fornitori di servizi che hanno accesso alle informazioni e ai sistemi siano adeguatamente informati in merito alla politica sulla sicurezza delle informazioni, ad esempio mediante sessioni formative e informative sulla sicurezza delle informazioni;

    f) coordinare l'analisi degli incidenti operativi o di sicurezza e riferire all'OADV quelli rilevanti.

Orientamento 8 – Sicurezza logica

26. Le imprese definiscono, documentano e attuano procedure di controllo dell'accesso logico o di sicurezza logica (gestione dell'identità e dell'accesso) in linea con i requisiti di protezione, come definito nell'orientamento 4. Le procedure sono attuate, applicate, monitorate e riviste periodicamente e includono anche controlli per il monitoraggio delle anomalie. Tali procedure, come minimo, attuano i seguenti elementi, dove il termine «utente» comprende anche gli utenti tecnici:

    a) necessità di conoscere (*need to know*), il privilegio minimo e la separazione delle funzioni: le imprese gestiscono i diritti di accesso, compreso l'accesso da remoto alle risorse informative e ai loro sistemi di supporto in base al principio della «necessità di conoscere». Agli utenti sono concessi i diritti di accesso minimi strettamente necessari per l'esecuzione delle loro funzioni (principio del «privilegio minimo»), in modo da impedire l'accesso ingiustificato ai dati o che l'attribuzione di combinazioni di diritti di accesso possa essere utilizzata per aggirare i controlli (principio della «separazione delle funzioni»);

    b) responsabilità degli utenti: le imprese limitano, per quanto possibile, l'uso di account utente generici e condivisi e assicurano che in qualsiasi momento gli utenti possano essere identificati e ricondotti a una persona fisica avente la responsabilità o a un'attività autorizzata per le azioni svolte nei sistemi ICT;

c) diritti di accesso privilegiato: le imprese effettuano rigidi controlli sull'accesso privilegiato al sistema limitando strettamente e sorvegliando attentamente gli account in possesso di ampie autorizzazioni di accesso (ad esempio, gli account degli amministratori);

d) accesso da remoto: onde garantire la sicurezza delle comunicazioni e ridurre il rischio, l'accesso con privilegi di amministratore da remoto a sistemi ICT essenziali è concesso esclusivamente sulla base del principio della necessità di conoscere e qualora siano applicate soluzioni di autenticazione forte;

e) registrazione delle attività degli utenti: le attività degli utenti sono registrate e monitorate in modo proporzionato al rischio; ciò comprende, al minimo, le attività degli utenti privilegiati. I registri degli accessi sono protetti per impedire modifiche o cancellazioni non autorizzate e conservati per un periodo commisurato alla criticità delle aree funzionali, dei processi di supporto e delle risorse informative individuati, fatti salvi gli obblighi di conservazione previsti dalla normativa nazionale e dell'UE. Le imprese utilizzano queste informazioni per favorire l'individuazione e l'indagine di attività anomale rilevate nella fornitura di servizi;

f) gestione dell'accesso: i diritti di accesso sono concessi, annullati e modificati in modo tempestivo, in base a procedure predefinite per l'approvazione, qualora sia coinvolto il proprietario della risorsa informativa interessato. Nel caso in cui l'accesso non sia più necessario, i diritti di accesso sono prontamente revocati;

g) valutazione dell'accesso: i diritti di accesso vanno riveduti periodicamente per garantire che gli utenti non godano di privilegi eccessivi e che i diritti di accesso siano decaduti/estinti quando non sono più necessari;

h) la concessione, la modifica, la revoca dei diritti di accesso sono documentate in modo da facilitarne la comprensione e l'analisi;

i) metodi di autenticazione: le imprese applicano metodi di autenticazione che siano sufficientemente solidi per garantire in modo adeguato ed efficace il rispetto delle politiche e delle procedure di controllo degli accessi. I metodi di autenticazione sono commisurati alla criticità dei sistemi ICT, delle informazioni o dei processi ai quali si accede. Ciò comprende, quanto meno, password complesse o metodi di autenticazione più forti (come l'autenticazione a due fattori), in funzione del rischio pertinente.

27. L'accesso elettronico ai dati e ai sistemi ICT per mezzo di applicazioni è limitato a quanto strettamente necessario per l'erogazione del servizio in questione.

Orientamento 9 – Sicurezza fisica

28. Le misure di sicurezza fisica delle imprese (ad esempio, protezione contro interruzioni di corrente, incendi, alluvioni e accesso fisico non autorizzato) vanno definite, documentate e attuate al fine di proteggere i locali, i centri dati e le aree sensibili da accessi non autorizzati e da pericoli ambientali.

29. L'accesso fisico ai sistemi ICT è consentito soltanto a persone autorizzate. L'autorizzazione viene rilasciata in base ai compiti e alle responsabilità individuali e limitandosi alle persone formate e monitorate in modo adeguato. L'accesso fisico va riesaminato regolarmente per garantire che i diritti di accesso non più necessari siano tempestivamente fatti decadere/estinguere.

30. Le misure adeguate di protezione dai rischi ambientali sono commisurate all'importanza degli edifici e alla criticità delle operazioni o dei sistemi ICT al loro interno.

Orientamento 10 – Sicurezza delle operazioni ICT

31. Le imprese attuano procedure per garantire la riservatezza, l'integrità e la disponibilità dei sistemi e dei servizi ICT al fine di ridurre al minimo l'impatto delle problematiche legate alla sicurezza sulla fornitura di servizi ICT. Tali procedure comprendono le misure seguenti:

    a) l'individuazione delle potenziali vulnerabilità, che sono valutate e corrette garantendo che i sistemi ICT siano aggiornati, compreso il software fornito dalle imprese ai rispettivi utenti interni ed esterni, mediante la distribuzione di patch di sicurezza essenziali, compresi aggiornamenti delle impostazioni antivirus, o la realizzazione di controlli compensativi;

    b) la realizzazione di una configurazione di sicurezza di base per tutti i componenti essenziali quali sistemi operativi, banche dati, router o switch;

    c) la realizzazione di una rete segmentata, di sistemi per la prevenzione della fuga di dati e della cifratura del traffico di rete (in base alla classificazione della risorsa informativa);

    d) la protezione degli endpoint, compresi server, stazioni di lavoro e dispositivi mobili. Le imprese valutano se ciascun endpoint soddisfa gli standard di sicurezza definiti dalle stesse prima di concedere l'accesso alla rete aziendale;

    e) garantire che siano posti in essere meccanismi di controllo dell'integrità per verificare l'integrità dei sistemi ICT;

    f) la cifratura dei dati memorizzati e in transito (in base alla classificazione della risorsa informativa).

Orientamento 11 – Monitoraggio della sicurezza

32. Le imprese stabiliscono e attuano procedure e processi per monitorare costantemente le attività aventi un impatto sulla sicurezza delle informazioni delle imprese stesse. Il monitoraggio include almeno:

    a) i fattori interni ed esterni, comprese le funzioni di amministratore informatico in ambito operativo e ICT;

    b) le transazioni dei fornitori di servizi, di altre entità e degli utenti interni;

    c) le potenziali minacce interne ed esterne.

33. Sulla base del monitoraggio le imprese mettono in atto capacità adeguate ed efficaci per individuare, segnalare e fronteggiare attività e minacce anomale, come intrusioni fisiche o logiche, violazioni della riservatezza, dell'integrità e della disponibilità di risorse informative, codici malevoli e vulnerabilità pubblicamente note per software e hardware.

34. Le segnalazioni provenienti dal monitoraggio della sicurezza consentono alle imprese di comprendere la natura degli incidenti sia operativi che di sicurezza, di individuare le tendenze e di sostenere le indagini interne nonché di assumere decisioni appropriate.

Orientamento 12 – Analisi, valutazione e verifica della sicurezza delle informazioni

35. Le imprese eseguono analisi, valutazioni e verifiche riguardanti la sicurezza delle informazioni, in modo da garantire l'efficace individuazione delle vulnerabilità nei propri sistemi e servizi ICT. Ad esempio, le imprese possono effettuare un'analisi delle lacune («gap analysis») a fronte degli standard di sicurezza delle informazioni, delle analisi di conformità, degli audit interni ed esterni dei sistemi informativi o delle analisi della sicurezza fisica.

36. Le imprese definiscono e attuano policies e procedure per la verifica della sicurezza delle informazioni che convalidi la solidità e l'efficacia delle misure di sicurezza, nonché garantire che tale quadro di riferimento prenda in considerazione le minacce e le vulnerabilità individuate grazie al monitoraggio delle minacce e al processo di valutazione dei rischi ICT e di sicurezza.

37. Le verifiche sono effettuate in modo sicuro e da esperti indipendenti con sufficienti conoscenze, capacità e competenze per sottoporre a verifica le misure di sicurezza delle informazioni.

38. Le imprese effettuano le verifiche regolarmente. L'ambito, la frequenza e il metodo delle verifiche (ad esempio, verifiche concernenti i tentativi di violazione, compresi quelli basati sulle minacce) sono commisurati al livello di rischio individuato. Le verifiche dei sistemi ICT essenziali e le scansioni delle vulnerabilità sono effettuate ogni anno.

39. Le imprese assicurano che siano effettuate verifiche delle misure di sicurezza in caso di modifiche dell'infrastruttura, dei processi o delle procedure e si accertano che tali modifiche siano state apportate a seguito di gravi incidenti operativi o di sicurezza o in ragione della disponibilità di applicazioni essenziali nuove o significativamente aggiornate. Le imprese monitorano e valutano i risultati ottenuti dalle verifiche della sicurezza e aggiornano di conseguenza senza indebiti ritardi le misure di sicurezza nel caso dei sistemi ICT essenziali.

Orientamento 13 – Sessioni formative e informative sulla sicurezza delle informazioni

40. Le imprese definiscono programmi di formazione sulla sicurezza delle informazioni per tutto il personale, compreso l'OADV, per garantire che ricevano la formazione necessaria per poter svolgere i loro compiti e assolvere alle loro responsabilità riducendo gli errori umani, i furti, le frodi, gli usi impropri o le perdite. Le imprese assicurano che il programma di formazione preveda sessioni periodiche per tutto il personale.

41. Le imprese definiscono e attuano programmi periodici sulla sicurezza per informare il personale, compreso l'OADV, su come affrontare i rischi legati alla sicurezza delle informazioni.

Orientamento 14 – Gestione delle operazioni ICT

42. Le imprese gestiscono le proprie operazioni ICT sulla base della loro strategia ICT. Va documentato il modo in cui le imprese operano, monitorano e controllano i sistemi e i servizi ICT, garantendo la documentazione dei processi, delle procedure e delle operazioni ICT essenziali.

43. Le imprese pongono in essere procedure di registrazione e monitoraggio per le operazioni ICT essenziali al fine di consentire il rilevamento, l'analisi e le misure correttive degli errori.

44. Le imprese mantengono un inventario aggiornato delle loro risorse ICT, sufficientemente dettagliato da consentire una rapida individuazione di una risorsa ICT, della relativa ubicazione, classificazione di sicurezza e titolarità.

45. Le imprese monitorano e gestiscono il ciclo di vita delle risorse ICT per assicurare il continuo soddisfacimento e supporto in termini di esigenze aziendali e di gestione dei rischi. Le imprese monitorano le risorse ICT affinché siano supportate dai loro fornitori e sviluppatori interni e che tutte le patch e tutti gli aggiornamenti pertinenti siano applicati rispettando un processo documentato. I rischi derivanti da risorse ICT non aggiornate o non più supportate vanno valutati e attenuati. Le risorse ICT dismesse sono trattate e smaltite in modo sicuro.

46. Le imprese mettono in atto processi di pianificazione e monitoraggio delle prestazioni e della capacità onde prevenire, rilevare e fronteggiare in modo tempestivo importanti problemi riguardanti le prestazioni dei sistemi ICT e le lacune nella capacità delle ICT.

47. Le imprese definiscono e attuano procedure di backup e ripristino dei dati e dei sistemi ICT per garantirne il recovery ove necessario. L'ambito e la frequenza dei backup sono definiti in linea con le esigenze di ripristino aziendale e la criticità dei dati e dei sistemi ICT, oltre a essere valutati sulla scorta dell'analisi dei rischi effettuata. Le procedure di backup e di ripristino sono sottoposte a verifiche regolari.

48. Le imprese assicurano che i backup dei dati e dei sistemi ICT siano conservati in uno o più luoghi esterni al sito principale, che siano sicuri e sufficientemente distanti dal sito principale affinché non vengano esposti agli stessi rischi.

Orientamento 15 – Gestione degli incidenti e dei problemi legati alle ICT

49. Le imprese definiscono e attuano un processo di gestione degli incidenti e dei problemi per monitorare e registrare gli incidenti operativi o di sicurezza e poter continuare o riprendere le funzioni e i processi aziendali essenziali qualora si verifichino interruzioni del servizio.

50. Le imprese definiscono criteri e soglie adeguati per la classificazione di un evento come incidente operativo o di sicurezza e indicatori di allerta (early warning) che consentano l'individuazione precoce di tali incidenti.

51. Per ridurre al minimo l'impatto degli eventi negativi e consentire un ripristino tempestivo, le imprese istituiscono processi e strutture organizzative atti a garantire un monitoraggio, una gestione e un follow-up coerenti e integrati degli incidenti operativi e di sicurezza per assicurare che le cause di fondo siano individuate, affrontate e che vengano adottate azioni o misure correttive per evitare il ripetersi dell'incidente. Il processo di gestione di incidenti e problemi delinea, al minimo:

    a) le procedure tese a individuare, tracciare, registrare, categorizzare e classificare gli incidenti secondo una priorità definita dall'impresa e basata sulla criticità operativa e sugli accordi di servizio;

    b) i ruoli e le responsabilità per i diversi scenari di incidente (ad esempio errori, malfunzionamenti, attacchi informatici);

    c) una procedura di gestione dei problemi per individuare, analizzare e risolvere le cause di fondo di uno o più incidenti; le imprese analizzano gli incidenti operativi o di sicurezza che sono stati individuati o si sono verificati all'interno

e/o all'esterno dell'organizzazione, nonché prendono in considerazione gli insegnamenti fondamentali tratti da queste analisi e aggiornano di conseguenza le 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 aventi un impatto negativo potenzialmente elevato sui sistemi e servizi ICT essenziali siano segnalati all'alta direzione;

   ii. l'OADV sia informato regolarmente nel caso di incidenti significativi e quanto meno tenuto al corrente dell'impatto, della reazione e dei controlli supplementari da definire a causa degli incidenti.

e) procedure di risposta agli incidenti per attenuare l'impatto conseguente e garantire che il servizio diventi tempestivamente operativo e sicuro;

f) piani di comunicazione esterna specifici per le funzioni e i processi aziendali essenziali, al fine di:

   i. collaborare con i soggetti interessati per garantire una risposta efficace e un pronto recupero dall'incidente;

   ii. fornire informazioni tempestive, compreso un rapporto sull'incidente, alle parti esterne, ad esempio clienti, altri partecipanti al mercato, autorità (di vigilanza) competenti, a seconda dei casi e in linea con la normativa applicabile.

Orientamento 16 – Gestione dei progetti ICT

52. Le imprese attuano una metodologia per i progetti ICT (incluse le valutazioni indipendenti sui requisiti di sicurezza) con un adeguato processo di governance e una leadership nell'attuazione del progetto volti a favorire efficacemente l'attuazione della strategia ICT mediante progetti dedicati.

53. Le imprese monitorano e mitigano adeguatamente i rischi derivanti dal portafoglio dei progetti ICT, tenendo conto anche dei rischi che potrebbero scaturire dalle interdipendenze tra progetti diversi e dalle dipendenze di più progetti dalle stesse risorse e competenze.

Orientamento 17 – Acquisizione e sviluppo dei sistemi ICT

54. Le imprese approntano e attuano un processo che disciplini l'acquisizione, lo sviluppo e la manutenzione dei sistemi ICT al fine di garantire che la riservatezza, l'integrità e la disponibilità dei dati da trattare siano messe completamente in sicurezza e che i requisiti di protezione definiti siano rispettati. Tale processo è ideato utilizzando un approccio basato sul rischio.

55. Le imprese garantiscono che, prima di effettuare acquisizioni di sistemi o attività di sviluppo, siano chiaramente definiti i requisiti funzionali e non funzionali (compresi i requisiti di sicurezza delle informazioni) e gli obiettivi tecnici.

56. Le imprese assicurano l'adozione di misure volte a prevenire l'alterazione involontaria o la manipolazione intenzionale dei sistemi ICT durante lo sviluppo.

57. Le imprese dispongono di una metodologia per verificare e approvare i sistemi e i servizi ICT, nonché le misure di sicurezza delle informazioni.

58. Le imprese sottopongono a controlli i sistemi e i servizi ICT nonché le misure di sicurezza delle informazioni per individuare potenziali debolezze, violazioni e incidenti di sicurezza.

59. Le imprese assicurano la separazione degli ambienti di produzione da quelli di sviluppo e di verifica e da altri ambienti non produttivi.

60. Le imprese attuano misure dirette a proteggere l'integrità del codice sorgente (se disponibile) dei sistemi ICT. Vanno inoltre documentate in modo esaustivo lo sviluppo, l'attuazione, il funzionamento e la configurazione dei sistemi ICT per ridurre la dipendenza non necessaria da esperti in materia.

61. I processi di acquisizione e sviluppo dei sistemi ICT delle imprese si applicano anche ai sistemi ICT sviluppati o gestiti direttamente dagli utenti finali dell'area funzionale esterna all'organizzazione delle ICT (ad esempio, applicazioni gestite dall'azienda o applicazioni informatiche dell'utente finale) utilizzando un approccio basato sul rischio. Le imprese mantengono un registro di queste applicazioni che supportano aree funzionali o processi essenziali.

Orientamento 18 – Gestione dei cambiamenti riguardanti le ICT

62. Le imprese istituiscono e attuano un processo di gestione dei cambiamenti riguardanti le ICT per assicurare che tutti i cambiamenti apportati ai sistemi ICT siano registrati, valutati, verificati, approvati, autorizzati e attuati in modo controllato. Deve essere possibile risalire ai cambiamenti sopravvenuti delle ICT per cause urgenti o di emergenza e comunicarli a posteriori al proprietario della risorsa in questione per effettuare un'analisi ex post.

63. Le imprese stabiliscono se cambiamenti al contesto operativo esistente abbiano un impatto sulle misure di sicurezza adottate o comportino l'adozione di ulteriori misure per mitigare i relativi rischi. Tali modifiche devono essere coerenti con il processo di gestione del cambiamento formale delle imprese.

Orientamento 19 – Gestione della continuità operativa

64. Nell'ambito della politica generale sulla continuità operativa delle imprese, l'OADV ha la responsabilità di definire e approvare la politica di continuità ICT delle imprese. La politica di continuità ICT è comunicata in modo appropriato all'interno delle imprese e si applica a tutto il personale interessato e, ove pertinente, ai fornitori di servizi.

Orientamento 20 – Analisi dell'impatto sulle attività

65. Nell'ambito di una sana gestione della continuità operativa, le imprese conducono un'analisi di impatto sulle attività per valutare la propria esposizione a gravi interruzioni dell'attività e il loro potenziale impatto, sotto i profili quantitativo e qualitativo, utilizzando dati interni e esterni e analisi di scenario. L'analisi di impatto sulle attività deve anche prendere in considerazione la criticità dei processi e delle attività aziendali individuati e classificati, le aree funzionali, i ruoli e le risorse (per esempio, le risorse informative e le risorse ICT), nonché le loro interdipendenze in conformità con l'orientamento 4.

66. Le imprese garantiscono che i rispettivi sistemi e servizi ICT siano ideati e allineati con l'analisi di impatto sulle attività, ad esempio prevedendo la ridondanza di alcune componenti essenziali per evitare che le interruzioni causate dagli eventi si ripercuotano su tali componenti.

Orientamento 21 – Pianificazione della continuità operativa

67. I piani di continuità operativa (BCPs, Business Continuity Plans) complessivi delle imprese considerano i rischi materiali suscettibili di ripercuotersi negativamente sui sistemi e sui servizi ICT. I piani definiscono gli obiettivi di proteggere e, laddove necessario, prevedono il ripristino della riservatezza, dell'integrità e della disponibilità dei processi e delle attività di tipo operativo, delle aree funzionali, dei ruoli e delle risorse (per esempio, le risorse informative e le risorse ICT) delle imprese. Durante la fase di definizione di tali piani, le imprese si coordinano con i soggetti interessati interni ed esterni, ove opportuno.

68. Le imprese mettono in atto i BCP per accertarsi di poter reagire in modo appropriato a potenziali scenari di guasto all'interno di un obiettivo di tempo di ripristino (il tempo massimo entro il quale un sistema o un processo deve essere ripristinato dopo un incidente) e di un obiettivo di punto di ripristino (il periodo di tempo massimo durante il quale i dati possono andare persi in caso di incidente a un livello di servizio predefinito).

69. Le imprese tengono conto di una serie di scenari diversi nei loro BCP, compresi scenari estremi ma plausibili e scenari di attacco informatico, e valutarne il potenziale impatto. Sulla base di tali scenari, le imprese descrivono in che modo viene garantita la continuità dei sistemi e dei servizi ICT, nonché la sicurezza delle informazioni delle imprese stesse.

Orientamento 22 – Piani di risposta e ripristino

70. Sulla base delle analisi d'impatto aziendale e degli scenari plausibili, le imprese definiscono piani di risposta e di ripristino. Tali piani precisano le condizioni che potrebbero richiedere l'attivazione del piano e le azioni da intraprendere per garantire l'integrità, la disponibilità, la continuità e il ripristino quanto meno dei sistemi ICT, servizi ICT e dati essenziali delle imprese. I piani di risposta e di ripristino mirano a conseguire gli obiettivi di ripristino delle operazioni delle imprese.

71. Tali piani considerano le opzioni di ripristino a breve termine e, ove necessario, quelle a lungo termine. I piani devono almeno:

    a) essere incentrati sul ripristino delle operazioni dei servizi ICT rilevanti, delle aree funzionali, dei processi di supporto, delle risorse informative e delle loro interdipendenze per evitare effetti negativi sul funzionamento dell'impresa;

    b) essere documentati e messi a disposizione delle unità operative e di supporto, prontamente accessibili in caso di emergenza e recare una chiara definizione dei ruoli e delle responsabilità;

    c) essere costantemente aggiornati sulla base di quanto appreso dagli incidenti, dalle verifiche, dai nuovi rischi e minacce individuati, nonché dai cambiamenti degli obiettivi e dalle priorità di ripristino.

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

73. Nell'ambito dei piani di risposta e ripristino, le imprese prendono in considerazione e attuano misure di continuità per mitigare interruzioni di servizi da parte dei fornitori, che sono di fondamentale importanza per la continuità dei servizi ICT delle imprese (in linea con gli orientamenti dell'EIOPA sul sistema di governance e gli orientamenti in materia di esternalizzazione a fornitori di servizi cloud).

Orientamento 23 – Verifica dei piani

74. Le imprese sottopongono a verifica i rispettivi BCP e garantiscono che il funzionamento dei propri processi e attività essenziali di tipo operativo, le aree funzionali, i ruoli e le risorse (per esempio, le risorse informative e le risorse ICT) e le loro interdipendenze (compresi quelli da parte di fornitori di servizi) siano regolarmente soggetti a verifica secondo il profilo di rischio dell'impresa.

75. I BCP sono aggiornati regolarmente, sulla base dei risultati delle verifiche, delle informazioni sulle minacce esistenti e di quanto appreso dagli eventi precedenti. Sono inclusi anche tutti i cambiamenti pertinenti negli obiettivi di ripristino (inclusi l'obiettivo del tempo di ripristino e l'obiettivo del punto di ripristino) e/o i cambiamenti dei processi e delle attività di tipo operativo, delle aree funzionali, dei ruoli e delle risorse (per esempio, le risorse informative e le risorse ICT).

76. Le verifiche dei BCP devono dimostrare che sono in grado di sostenere l'operatività dell'azienda fino a quando le operazioni essenziali non saranno ristabilite a un livello di servizio predefinito o a una tolleranza in termini di impatto.

77. I risultati delle verifiche sono documentati ed eventuali carenze individuate a seguito delle verifiche vanno analizzate, affrontate e segnalate all'OADV.

Orientamento 24 – Comunicazioni in caso di crisi

78. In caso di interruzione o emergenza e durante l'attuazione dei BCP, le imprese assicurano di aver posto in essere efficaci misure di comunicazione in caso di crisi, in modo tale che tutte le parti interessate interne ed esterne, comprese le autorità di vigilanza competenti, se richiesto dal regolamento nazionale, e i fornitori di servizi interessati, siano informati in modo tempestivo e adeguato.

Orientamento 25 – Esternalizzazione di servizi ICT e sistemi ICT

79. Fatti salvi gli orientamenti dell'EIOPA in materia di esternalizzazione a fornitori di servizi cloud, le imprese garantiscono che, in caso di esternalizzazione di servizi e sistemi ICT, siano soddisfatti gli specifici requisiti per il servizio o il sistema ICT in questione.

80. In caso di esternalizzazione di funzioni essenziali e importanti, le imprese garantiscono che gli obblighi contrattuali del fornitore di servizi (ad esempio il contratto, gli accordi sul livello dei servizi, le disposizioni di risoluzione nei relativi contratti) includano almeno quanto segue:

    a) obiettivi e misure adeguati e proporzionati in riferimento alla sicurezza delle informazioni, compresi i requisiti minimi di sicurezza delle informazioni, le specifiche del ciclo di vita dei dati delle imprese, audit e diritti di accesso e qualsiasi requisito riguardante l'ubicazione dei centri dati e i requisiti di cifratura dei dati, la sicurezza della rete e i processi di monitoraggio della sicurezza;

    b) accordi sul livello dei servizi, per garantire la continuità dei servizi e dei sistemi ICT e obiettivi di prestazione in circostanze normali, nonché quelli previsti dai piani di emergenza in caso di interruzione del servizio;

    c) procedure di gestione degli incidenti operativi e di sicurezza, tra cui notifica e attivazione dei livelli successivi di intervento.

81. Le imprese monitorano e ottengono garanzie per quanto riguarda il livello di conformità dei suddetti fornitori di servizi ai propri obiettivi, misure e obiettivi di prestazione in materia di sicurezza.

Norme sulla conformità e sulla segnalazione

82. Il presente documento contiene orientamenti formulati in applicazione dell'articolo 16 del regolamento (UE) n. 1094/2010. A norma dell'articolo 16, paragrafo 3, di detto regolamento, le autorità competenti e le imprese sono tenute a compiere ogni sforzo per conformarsi agli orientamenti e alle raccomandazioni.

83. Le autorità competenti che sono conformi o intendono conformarsi ai presenti orientamenti li integrano opportunamente nel proprio quadro normativo o di vigilanza.

84. Le autorità competenti devono confermare all'EIOPA se sono conformi o intendono conformarsi ai presenti orientamenti, indicando i motivi, laddove non siano conformi, entro due mesi dalla pubblicazione delle versioni tradotte.

85. In assenza di una risposta entro tale termine, le autorità competenti saranno considerate non conformi in materia di segnalazione e verranno segnalate come tali.

Disposizione finale sulle revisioni

86. I presenti orientamenti saranno soggetti a revisione da parte dell'EIOPA.