Allegato C

Sistemi informativi e rischio di sicurezza

1. Disposizioni di carattere generale

L'affidabilità dei sistemi informativi rappresenta un pre-requisito essenziale per il buon funzionamento dell'istituto e consente agli organi aziendali di assumere decisioni consapevoli e coerenti con gli obiettivi aziendali.

I sistemi informativo-contabili sono adeguati al contesto operativo e ai rischi ai quali l'istituto è esposto.

Essi hanno un elevato grado di attendibilità, registrano correttamente e con la massima tempestività i fatti di gestione, consentono di ricostruire l'attività dell'istituto a qualsiasi data, partitamente per ciascuno dei servizi di pagamento prestati e, per gli istituti di moneta elettronica, anche in relazione all'attività di emissione moneta elettronica.

La circostanza che l'istituto utilizzi diverse procedure settoriali (contabilità, segnalazioni, antiriciclaggio, ecc.) non inficia la qualità e l'integrità dei dati né comporta la creazione di archivi non coerenti.

I sistemi informativi garantiscono elevati livelli di sicurezza. A tal fine, gli istituti individuano, documentano e mantengono aggiornati adeguati presidi volti a garantire: la sicurezza fisica e logica dell'*hardware* e del *software*, comprendenti procedure di *back-up* dei dati e di *disaster recovery;* l'individuazione e il controllo dei soggetti autorizzati ad accedere ai sistemi e le relative abilitazioni (ad es. mediante l'istituzione e tenuta di un registro degli accessi ai sistemi ICT); la possibilità di risalire agli autori degli inserimenti o delle modifiche dei dati e di ricostruire la serie storica dei dati modificati ([1]).

Con riferimento alla prestazione dei servizi di pagamento tramite internet, gli istituti applicano gli "Orientamenti finali in materia di sicurezza dei pagamenti via internet" emanati dall'EBA secondo quanto previsto nel Capitolo XIII.

In linea con l'impostazione generale della disciplina in materia di controlli interni e gestione dei rischi e fermi restando i casi in cui gli Orientamenti prescrivono obblighi specifici (come nel caso dell'utilizzo dell'"autenticazione forte"), gli istituti applicano le disposizioni contenute negli Orientamenti secondo il principio di proporzionalità, cioè tenuto conto della dimensione e complessità operative, della natura dell'attività svolta, della tipologia dei servizi prestati.

Inoltre, su un piano più generale, è necessario che la disponibilità di risorse informatiche e umane sia adeguata all'operatività aziendale.

([1]) Le misure di sicurezza prevedono, di norma, controlli su più livelli a presidio dello stesso rischio (cd. approccio di "difesa in profondità").

2. Il sistema di gestione della sicurezza ([1])

Il sistema di gestione del rischio di sicurezza è idoneo a identificare, misurare e mitigare i rischi cui l'istituto è esposto. Questo sistema è pienamente integrato nel complessivo sistema di governo e gestione dei rischi aziendali.

L'articolazione dei compiti e delle responsabilità è chiaramente definita. Il sistema di gestione è rivisto con cadenza almeno annuale per assicurarne l'efficacia nel tempo([2]).

In particolare gli istituti:

i) classificano le funzioni aziendali e le risorse informatiche in termini di esposizione al rischio di sicurezza attuale e potenziale, ai fini dell'identificazione del loro grado di criticità ([3]);

ii) predispongono adeguate misure per prevenire e mitigare i rischi di sicurezza;

iii) nel trattamento dei dati sensibili relativi ai pagamenti, definiscono e formalizzano i processi di raccolta, instradamento, trattamento, memorizzazione e/o archiviazione nonché di accesso degli stessi, al fine di garantirne l'integrità e la riservatezza. In tale ambito gli istituti istituiscono e aggiornano un registro dei soggetti che hanno accesso ai dati sensibili relativi ai pagamenti;

iv) monitorano nel continuo i rischi e le vulnerabilità che possono avere impatti sulle proprie funzioni aziendali, funzioni critiche e risorse informatiche;

v) adottano misure per prevenire e gestire gli incidenti operativi o relativi alla sicurezza e individuano i soggetti responsabili dell'assistenza ai clienti in relazione ai reclami concernenti la sicurezza dei servizi di pagamento prestati. I gravi incidenti operativi o relativi alla sicurezza che interessano direttamente o indirettamente gli istituti sono comunicati senza indugio alla Banca d'Italia con le modalità e nei termini da essa stabiliti, anche tenuto conto degli "Orientamenti finali in materia di segnalazione dei gravi incidenti ai sensi della direttiva 2015/2366/UE (PSD2)" emanati dall'EBA. Gli istituti utilizzano il modulo disponibile sul sito *internet* dell'Istituto. Se l'incidente incide o potrebbe incidere sugli interessi finanziari dei propri utenti di servizi di pagamento, gli istituti informano altresì quest'ultimi senza indugio dell'incidente e di tutte le misure a disposizione che possono adottare per attenuarne gli effetti negativi ([4]);

([1]) Cfr., inoltre, "Orientamenti finali sulle misure di sicurezza per i rischi operativi e di sicurezza dei servizi di pagamento ai sensi della direttiva 2015/2366/UE (PSD2)".

([2]) La revisione è effettuata, in ogni caso, prima di modifiche sostanziali dell'infrastruttura ICT o a seguito del verificarsi di gravi incidenti di sicurezza.

([3]) Ai fini di questa classificazione, essi valutano l'impatto di eventuali violazioni dei livelli di sicurezza, integrità e disponibilità e alla probabilità del verificarsi di minacce che potrebbero causare tali violazioni.

([4]) *Cfr*., Articolo 96, paragrafo 1, comma 2, della PSD2.

vi) valutano, con cadenza almeno annuale, l'adeguatezza del sistema di mitigazione e controllo adottato per identificare e misurare il rischio di sicurezza e, sulla base delle valutazioni effettuate, predispongono e attuano misure correttive ([1]). I documenti recanti queste valutazioni devono essere tenuti a disposizione per eventuali richieste della Banca d'Italia;

vii) assicurano che i propri dipendenti siano adeguatamente formati in tema di rischio di sicurezza (ad es. mediante corsi di formazione mirati in tema di sicurezza informatica, ecc.).

Nel rispetto del principio di proporzionalità, ai fini della definizione, attuazione e monitoraggio delle misure da adottare a fronte dei rischi operativi e di sicurezza nella prestazione dei servizi di pagamento e di emissione di moneta elettronica, gli istituti applicano gli "Orientamenti finali sulle misure di sicurezza per i rischi operativi e di sicurezza dei servizi di pagamento ai sensi della direttiva 2015/2366/UE (PSD2)".

3. Piano di emergenza e continuità operativa

Gli istituti definiscono un piano di emergenza e continuità operativa che formalizza i principi, fissa gli obiettivi, descrive le procedure e individua le risorse per la gestione di situazioni di crisi e per limitare le perdite in caso di gravi interruzioni dell'operatività conseguenti a incidenti di portata settoriale, aziendale ovvero a catastrofi estese che colpiscono l'istituto o le sue controparti rilevanti.

In coerenza con la politica di governo e gestione dei rischi, il piano di emergenza e continuità operativa:

- definisce le possibili misure di risposta e ripristino a fronte di diversi scenari di crisi ai quali gli istituti potrebbero essere esposti, ivi compresi quelli estremi purché plausibili, e degli impatti potenziali;

- individua canali di comunicazione capaci di garantire, in caso di crisi, un'informativa tempestiva e appropriata a tutte le parti interessate rilevanti sia interne sia esterne (ad es. i fornitori di servizi esterni).

Gli istituti definiscono le misure da adottare in caso di cessazione dei propri servizi di pagamento e/o dei contratti vigenti, per evitare effetti negativi sui sistemi di pagamento e sugli utenti e per garantire l'esecuzione delle operazioni di pagamento in corso. Queste misure sono descritte in un'apposita sezione del piano di emergenza e di continuità operativa.

([1]) Questa valutazione è necessaria in caso di previste modiche nelle infrastrutture processi e procedure che possono riguardare la sicurezza dell'istituto.

4. Esenzione dall'obbligo di predisporre il meccanismo di emergenza di cui all'articolo 33(4) del Regolamento delegato (UE) 2018/389 della Commissione

Nel rispetto di quanto previsto dal Regolamento delegato (UE) 2018/389 della Commissione, gli istituti che prestano servizi di pagamento di radicamento di conti di pagamento che intendono richiedere l'esenzione dalla predisposizione del meccanismo di emergenza ("interfaccia di *fall-back*") previsto dall'art. 33, par.4 del Regolamento si attengono a quanto previsto dagli Orientamenti dell'ABE sulle condizioni per beneficiare dell'esenzione dal meccanismo di emergenza a norma dell'articolo 33, paragrafo 6, del regolamento (UE) 2018/389 (EBA/GL/2018/07) del 4 dicembre 2018.