Politica per la Continuità Operativa ICT

Poste Italiane

Redazione	Vanes Montanari	TA
Verifica	Giuseppe Lasco	DG
Approvazione	Consiglio d'Amministrazione	-

N. Versione	Data di Approvazione	Paragrafi modificati	Motivazioni dell'aggiornamento
1.0	12/12/2024	-	Prima versione

Sommario

Introduzione

Il presente documento integra la Politica di Gestione delle Crisi e della Continuità Operativa di Gruppo.

Data la crescente digitalizzazione e interconnessione di ogni settore e la conseguente proliferazione di servizi e prodotti digitali a carattere finanziario e assicurativo, nonché l'evoluzione normativa in materia, si rende necessario integrare la suddetta politica con un focus sulla resilienza operativa, ovvero: la capacità dell'entità finanziaria/assicurativa di creare, assicurare e riesaminare la propria integrità operativa da un punto di vista tecnologico, garantendo, direttamente o indirettamente, tramite il ricorso ai servizi offerti da fornitori terzi, l'intera gamma delle soluzioni ICT necessarie per garantire la sicurezza delle reti e dei sistemi informativi impiegati, su cui si fondano la costante offerta dei servizi e la loro qualità.

1 Obiettivi, ambito di applicazione e modalità di recepimento

L'obiettivo è quello di garantire la continuità delle funzioni essenziali o importanti dell'entità finanziarie e assicurative, fornire una risposta rapida, appropriata ed efficace per tutti gli incidenti ICT, attivare senza ritardo le procedure di risposta e ripristino ed effettuare le corrette azioni di comunicazione e di gestione delle crisi.

Il presente documento entra in vigore dalla data di approvazione; l'implementazione deve avvenire conseguentemente, tenendo conto degli adempimenti societari, degli specifici requisiti organizzativi e tecnologici, nonché economici dell'Organizzazione.

Il Documento si applica a Poste Italiane S.p.A., compreso il Patrimonio Bancoposta, e, previo processo di recepimento, alle Società del Gruppo appartenenti all'ambito finanziario e assicurativo. Le SdG ricevono il presente documento e lo recepiscono tempestivamente.

2 Definizioni, abbreviazioni e acronimi

Acronimi

Acronimo/abbreviazione	Descrizione
BCM	Business Continuity Management
BIA	Business Impact Analysis
CCNL	Contratto Collettivo Nazionale del Lavoro
C.d.A.	Consiglio d'Amministrazione
CERT	Computer Emergency Response Team
DG	Direttore Generale
DORA	Digital Operational Resilience Act
GDPR	General Data Protection Regulation
ICT	Information and Communication Technologies
IT	Information Technology
ISO	International Organization for Standardization
RPO	Recovery Point Objectives
RTO	Recovery Time Objectives
SCIGR	Sistema di Controllo Interno e Gestione Rischi
S.d.G.	Società del Gruppo
SI	Sicurezza Informatica
S.p.A.	Società per Azioni
TA	Tutela Aziendale
UGI	Unità Gestione Incidenti

Definizioni

Termine	Definizione
Azione correttiva	Azione per eliminare la causa di una non conformità e per prevenirne il ripetersi.
Business Continuity Management / Gestione Continuità Operativa	Processo di gestione che identifica l'impatto che un evento emergenziale può causare sull'erogazione dei servizi critici/sistemici e fornisce un quadro per costruire delle soluzioni atte a garantire la continuità del servizio che salvaguarda gli interessi delle principali terze parti, la reputazione, il brand e l'attività di creazione del valore.

Termine	Definizione
	Per BancoPosta la normativa di riferimento è la circolare 285 del 17.12.2013 di Banca d'Italia.
Business Impact Analysis	Processo di analisi delle attività e dell'effetto che un'interruzione dell'attività può avere su di esse.
Comitato di Continuità Operativa	Organo aziendale che attua le azioni necessarie alla gestione della continuità operativa, sia in condizioni ordinarie che in condizioni di incidente interruttivo.
Crisi	Situazione anomale ed instabile che minaccia la strategia dell'Organizzazione, gli obiettivi, la reputazione e/o la redditività.
Data Center	Sala macchine (anche sala Ced – Centro elaborazione dati) che ospita server, storage, gruppi di continuità e tutte le apparecchiature che consentono di governare i processi, le comunicazioni così come i servizi che supportano qualsiasi attività aziendale.
Disaster Recovery	Strategia definita in previsione di un qualsiasi evento tecnico o di altra natura in grado di mettere in crisi un sistema informatico compromettendone il corretto funzionamento e che ha come obiettivo il più rapido e completo possibile ripristino delle funzioni e dei dati presenti nel sistema stesso. È una delle soluzioni previste per lo scenario di indisponibilità dei sistemi informativi.
Escalation	Conduzione della gestione di un incidente caratterizzata da un aumento progressivo dei livelli aziendali coinvolti, fino a giungere, ove necessario, all'Amministratore Delegato.
Impatto	Conseguenza negativa per l'azienda causata dal verificarsi di un evento avverso.
Incidente	Situazione che può, o potrebbe portare ad un'interruzione, una perdita, un'emergenza o una crisi.
Miglioramento continuo	Attività ricorrente volto al migliorare la performance.
Non conformità	Mancato soddisfacimento di un requisito.
Piano di Continuità Operativa di Gruppo	Documento strategico che indica il perimetro di Gruppo, le fasi di gestione della continuità operativa, gli scenari gestiti e le soluzioni individuate.
Piano di Disaster Recovery e Continuità Operativa ICT	Documento che stabilisce le misure tecniche e organizzative per fronteggiare eventi che provochino l'indisponibilità dei centri di elaborazione dati. Il piano di disaster recovery, finalizzato a consentire il funzionamento delle procedure informatiche rilevanti in siti alternativi a quelli di produzione, costituisce parte integrante del piano di continuità operativa.

Termine	Definizione
Piano Settoriale	Documento di dettaglio, predisposto con riferimento a una specifica area di business, che guida l'organizzazione a rispondere, recuperare, riprendere e ripristinare i propri servizi/processi ad un livello di operatività predefinito a seguito di un'interruzione.
Presidi di Sicurezza	Funzioni deputate al presidio di specifici ambiti di sicurezza ed in particolare al monitoraggio, alla classificazione, al trattamento, all'escalation, alla notifica ed alla divulgazione degli incidenti rientranti nel perimetro di competenza.
Rischio	Effetto di incertezza sugli obiettivi, espresso dal prodotto tra la probabilità di accadimento di un evento e l'impatto che questo evento potrebbe causare.
Scenario	Scenario d'indisponibilità, previsto o imprevisto che si delinea quando occorre un incidente tale da causare l'impossibilità di erogare il servizio. Lo scenario può riguardare l'indisponibilità del sito operativo, delle risorse, dei sistemi informativi oppure di un fornitore.
Test	Verifica oggettiva e riproducibile che consente di valutare il raggiungimento di un obiettivo, comprensiva anche di esercitazioni che coinvolgono più perimetri di competenza.
UGI	Organo aziendale che garantisce le azioni necessarie alla gestione ed al coordinamento degli incidenti segnalati dai Presidi di Sicurezza.

3 Principi di riferimento

Le attività disciplinate dal presente documento devono essere svolte nel rispetto delle vigenti disposizioni di legge nonché dei principi e delle regole di comportamento contenuti nel Codice Etico e Politica Integrata del Gruppo Poste Italiane e negli altri strumenti normativi aziendali.

Il presente documento si ispira ai principi generali riportati nella Linea Guida '*Sistema di Controllo Interno e Gestione Rischi (SCIGR)'*, cui si rimanda per il relativo dettaglio.

4 Governance e Responsabilità

Di seguito una breve descrizione dei principali ruoli e delle entità deputate alla gestione delle crisi, della continuità operativa e degli incidenti di Gruppo; per maggiori dettagli si rimanda alla Linea Guida Crisi e Continuità Operativa di Gruppo.

- ✓ **Consiglio di Amministrazione**
  Il Consiglio di Amministrazione di Poste Italiane S.p.A., rappresenta il ruolo di indirizzo e controllo a livello strategico nella gestione delle crisi e della continuità operativa di Gruppo, dispone le nomine e le deleghe verso il Responsabile Gestione Crisi di Gruppo e il Responsabile Gestione Continuità Operativa ed Emergenze di Gruppo.

- ✓ **Consiglio di Amministrazione del Soggetto Obbligato**
  Il Consiglio di Amministrazione del Soggetto Obbligato, stabilisce i principi e gli obiettivi del sistema di gestione della crisi e della continuità operativa, esaminando e recependo i relativi documenti di Gruppo e approvando il “Piano di Continuità Operativa di Gruppo” per il perimetro di propria pertinenza.

- ✓ **Amministratore Delegato**
  L’Amministratore Delegato di Poste Italiane S.p.A., è informato tempestivamente all’apertura della crisi, tiene aggiornato il C.d.A. sugli sviluppi e le decisioni prese per il ritorno alla normalità. Promuove, inoltre, le azioni di miglioramento continuo dei Sistemi di Gestione della Crisi e della Continuità Operativa in condizioni di normale operatività.

- ✓ **Amministratore Delegato Soggetto Obbligato/Responsabile Soggetto Obbligato**
  L’Amministratore Delegato Soggetto Obbligato/Responsabile Soggetto Obbligato esamina i documenti del sistema di gestione della crisi e della continuità operativa di Gruppo per il perimetro di propria pertinenza. In caso di discontinuità operativa e/o crisi è coinvolto dai Responsabili preposti al fine di valutare e notificare la dichiarazione di crisi all’Autorità di Vigilanza di riferimento.

- ✓ **Responsabile Gestione Crisi di Gruppo**
  Opera ed agisce con piena delega del Consiglio di Amministrazione e dell'Amministratore Delegato, ai quali risponde in ordine alle scelte e alle decisioni prese dalla dichiarazione della crisi fino al ritorno alla normalità.
  Presiede l’Unità di Crisi.

- ✓ **Responsabile Gestione Continuità Operativa ed Emergenze di Gruppo**
  Indirizza e supervisiona le attività relative al Sistema di Gestione della Continuità Operativa di Gruppo e al Sistema di Gestione degli Incidenti di Gruppo.
  Presiede il Comitato di Continuità Operativa.

- ✓ **Responsabile Gestione Incidenti di Gruppo**
  Gestisce gli incidenti e rappresenta l’interfaccia verso il Responsabile Gestione Continuità Operativa ed Emergenze di Gruppo.
  Presiede l’Unità Gestione Incidenti.

- ✓ **Risk Manager di Gruppo**
  È responsabile di definire e aggiornare il framework metodologico di gestione del Rischio e gli strumenti finalizzati all'individuazione, valutazione/misurazione e monitoraggio dei rischi del Gruppo, supporta l’azione di gestione delle crisi e della continuità operativa del Gruppo stimando e definendo i livelli di propensione al rischio da sottoporre al Consiglio di Amministrazione, coerentemente con le linee guida di riferimento.

- ✓ **Responsabile Funzione di Controllo**
  Vigila sulla completezza, adeguatezza, funzionalità e affidabilità in termini di efficacia del sistema dei controlli interni, documentando l’attività di verifica svolta e le evidenze emerse, individuando eventuali violazioni delle procedure e delle norme applicabili al Gruppo.

- ✓ **Unità di Crisi**
  Entità costituita dai rappresentanti delle Funzioni/Società del Gruppo coinvolte per garantire le migliori azioni da intraprendere per rispondere alla crisi.

- ✓ **Comitato di Continuità Operativa**
  Entità costituita dai rappresentanti delle Funzioni/Società del Gruppo coinvolte per garantire le azioni necessarie alla gestione della continuità operativa, sia in condizioni ordinarie che in condizioni di incidente interruttivo. Il Comitato si avvale del supporto delle funzioni aziendali competenti per lo svolgimento delle attività.

- ✓ **Unità Gestione Incidenti**
  Entità costituita per garantire le azioni necessarie alla gestione e al coordinamento degli incidenti segnalati dai Presidi di Sicurezza.

- ✓ **Referente Piano di Comunicazione**
  È responsabile di definire il Piano di comunicazione interno ed esterno che serve a garantire un flusso di informazioni tempestivo e accurato durante l'incidente grave, la discontinuità operativa o la crisi. Il Piano include informazioni di contatto per le parti chiave interessate, modelli di comunicazione pre-approvati e protocolli per i media e le relazioni pubbliche

4.1 Business Continuity

Il Piano di Continuità Operativa di Gruppo, i Piani Settoriali di Continuità Operativa e il Piano Disaster Recovery e Continuità Operativa ICT, devono includere l'identificazione dei processi critici, definendo chiaramente le funzioni e i servizi essenziali per il mantenimento dell'operatività e devono esplicitare le dipendenze interne ed esterne, comprese le risorse umane chiave, i sistemi IT, i fornitori e le altre risorse fondamentali.

La BIA deve essere condotta annualmente per identificare processi/prodotti critici, valutare l'impatto delle interruzioni e definire l'ordine di priorità per le attività di recupero mediante una valutazione dell'impatto potenziale di gravi perturbazioni delle attività mediante criteri quantitativi e qualitativi, utilizzando se del caso dati interni ed esterni e analisi di scenario. La BIA identifica i processi critici, i sistemi, le dipendenze da terzi nonché le loro interdipendenze e le risorse necessarie per il recupero, stabilendo i Recovery Time Objectives (RTO) e i Recovery Point Objectives (RPO) per le attività essenziali. Nel determinare gli obiettivi in materia di punti di ripristino e tempi di ripristino di ciascuna funzione, le entità finanziarie tengono conto del fatto che si tratti di una funzione essenziale o importante e del potenziale impatto complessivo sull'efficienza del mercato. Questi obiettivi in materia di tempi garantiscono che i livelli di servizi concordati siano rispettati anche in scenari estremi. La BIA deve essere rivista e aggiornata regolarmente per riflettere i cambiamenti organizzativi, tecnologici e/o normativi.

I servizi ICT e l'infrastruttura ICT sono progettati ed utilizzati in piena conformità con la BIA effettuata, in particolare garantendo adeguatamente la ridondanza di tutte le componenti essenziali. In particolare, i sistemi informativi a supporto delle attività finanziarie mantengono almeno un sito secondario di trattamento dati dotato di risorse, capacità, funzioni e personale.
L'attivazione dei sistemi di Disaster Recovery e di backup non mette a repentaglio la sicurezza dei sistemi informatici e di rete né, la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati.

I Piani devono essere testati almeno una volta all'anno con diversi scenari per valutare l'efficacia delle strategie di risposta e recupero. I risultati dei test devono essere documentati, rivisti e utilizzati per migliorare la documentazione e i processi di gestione della continuità operative e/o delle crisi.

Devono essere stabilite procedure di risposta alle emergenze, con azioni immediate per affrontare scenari come incidenti informatici, disastri naturali e pandemie. Inoltre, è necessario dettagliare i piani di recupero, specificando le fasi di ripristino delle operazioni interrotte nel rispetto degli obiettivi di Recovery Time Objective (RTO) e Recovery Point Objective (RPO) definiti.

È necessario prevedere una valutazione completa dei rischi effettuata per identificare potenziali minacce alla Continuità Operativa, incluse le minacce gestite nell'ambito della valutazione del rischio informatico, disastri naturali, guasti ai sistemi e interruzioni della catena di fornitura. Devono essere implementate strategie di mitigazione per ridurre la

probabilità e l'impatto delle interruzioni. Tra le strategie di gestione del rischio, devono essere inclusi ridondanze dei sistemi, backup dei dati, misure di cybersicurezza e gestione della catena di fornitura.

Devono essere stabilite strategie di risposta e recupero per ripristinare le funzioni critiche entro i valori di RTO e RPO definiti. Queste strategie devono includere il Disaster Recovery, che deve comprendere procedure di backup e ripristino per dati e applicazioni, incluse soluzioni basate sul cloud. Devono essere previste disposizioni per Alternative Work Arrangements, che contemplino la possibilità di lavoro da remoto, sedi alternative e relativi piani di comunicazione. Inoltre, si deve prevede la Supply Chain Continuity, che implica la collaborazione con fornitori e partner di terze parti per garantire la Continuità Operativa.

4.2 Test ed Esercitazioni

Per garantire l'efficacia dei Piani di Continuità Operativa è necessario condurre test ed esercitazioni, che possono essere di vario tipo ed essere focalizzati sugli aspetti organizzativi, procedurali e tecnologici. Per i dettagli si rimanda al Piano di Continuità Operativa di Gruppo, al Piano Disaster Recovery e Continuità Operativa ICT e alla Procedura dei Test di Resilienza Operativa e relativa documentazione.

Di seguito una descrizione delle tipologie di test ed esercitazioni:

- ✓ i Table-Top Exercise consistono in simulazioni teoriche con il personale chiave per esaminare le risposte a scenari specifici, con particolare attenzione alla presa di decisioni e al coordinamento;
- ✓ esercitazioni che simulano scenari realistici, come attacchi informatici o violazioni di dati. Includono l'attivazione completa del Piano di Continuità Operativa, il test delle capacità di recupero IT, del lavoro alternativo e della resilienza della catena di fornitura;
- ✓ esercitazioni in tempo reale per testare l'attuazione delle procedure di recupero e dei sistemi di backup;
- ✓ IT System Failover Test sono test trimestrali del failure e recupero dei sistemi IT critici e comprendono backup e verifiche sull'integrità dei dati;
- ✓ Test Continuità Terze Parti che prevedono la verifica che i loro Piani di Continuità Operativa siano allineati ai requisiti di Poste Italiane;
- ✓ Advanced Penetration Test per valutare la capacità di difesa di una organizzazione attraverso la conduzione di attacchi informatici simulati, utilizzando tecniche avanzate di test di penetrazione per replicare scenari di minaccia informatica reali;
- ✓ Threat-Led Penetration Testing Exercise per valutare la capacità dell'organizzazione di rilevare, rispondere e recuperare da attacchi e incidenti informatici sofisticati;
- ✓ simulazione di incidente Multi-Dipartimentale per valutare la capacità dell'organizzazione di valutare la prontezza di più Funzioni/Società del Gruppo a collaborare efficacemente durante un incidente. La simulazione è realizzata su larga scala e coinvolge tutti o gran parte delle principali Funzioni/Società del Gruppo;
- ✓ test Attacco Cyber ha come obiettivo quello di testare la preparazione e le capacità di risposta dell'organizzazione in caso di un incidente di cybersecurity che colpisca sistemi informativi a supporto dei processi aziendali, una funzione critica con un basso obiettivo di tempo di recupero (RTO) e di punto di recupero (RPO);
- ✓ test Fallimento Data Center è progettato per verificare la capacità dell'organizzazione di rispondere e riprendersi da un'interruzione completa del data center, che impatta le funzioni aziendali critiche;
- ✓ Il test Fallimento Parziale dei Data Center ha come obiettivo quello di verificare la capacità dell'organizzazione di rispondere e riprendersi da un'interruzione parziale del data center, che impatta sulle funzioni aziendali critiche ospitate nel data center primario, effettuando un ripristino dei dati dal backup e recuperando quelli mancanti;
- ✓ Il test di Sabotaggio o Minaccia Interna ha come obiettivo quello di valutare la risposta dell'organizzazione a una potenziale minaccia interna o a un'azione interna dannosa con impatto sui processi critici, ivi inclusi eventuali ripristino e recupero dei dati di backup disponibili;
- ✓ Il test Pandemia ha come obiettivo quello di valutare la capacità dell'organizzazione di mantenere le operazioni durante un periodo prolungato in cui una parte significativa della forza lavoro non è disponibile o lavora a distanza a causa di una crisi sanitaria;
- ✓ test di non Conformità alla normativa per valutare la capacità dell'organizzazione di rispondere a uno scenario in cui viene identificata una violazione normativa;

Al fine di garantire una completa verifica dei processi e sistemi dell'organizzazione e necessario prevedere test con le terze parti che partecipano all'erogazione dei servizi.

Tali test devono essere di due tipologie:

- ✓ Il test Continuità Terze Parti ha come obiettivo quello di garantire che i fornitori e/o i fornitori di servizi terzi critici dispongano di piani e capacità di continuità operativa solidi e di valutare la capacità dei fornitori di continuare l'erogazione del servizio e di mantenere la riservatezza, l'integrità e la disponibilità dei dati in caso di instabilità politica e sociale nelle giurisdizioni dei fornitori di servizi ICT. Per raggiungere questo scopo, si richiedono test regolari di continuità e prove delle misure di resilienza da parte dei fornitori chiave, inclusi esercizi da tavolo.
- ✓ Il test "Incidente Terze parti" ha come obiettivo quello di verificare la capacità di rispondere ad un guasto o a un'interruzione di un fornitore di terze parti critico che fornisce servizi essenziali, come ad esempio cloud hosting o gateway di pagamento. Il metodo prevede la simulazione dell'indisponibilità del fornitore, con la successiva revisione ed attivazione dell'accordo con il fornitore alternativo o del piano di emergenza per garantire la continuazione dei servizi essenziali.

I test devono essere documentati e devono evidenziare eventuali vulnerabilità e aree di miglioramento. I risultati dei test devono essere analizzati e permettere la predisposizione di un piano di rientro che indichi le azioni correttive individuate al fine di mitigare i rischi e migliorare l'efficienza dell'Organizzazione.

La frequenza dei test deve avere cadenza triennale, biennale, annuale o più volte l'anno laddove si evidenzino specifiche necessità.

4.3 Gestione Incidenti

La gestione degli incidenti di Gruppo deve prevedere l'insieme di risorse, procedure e strumenti necessari per una efficace applicazione del processo, che include le fasi di preparazione, rilevazione e segnalazione, analisi e valutazione, risposta e miglioramento continuo.
Per i dettagli si rimanda alla *Linea Guida Gestione Eventi e Incidenti di Gruppo.*

4.4 Piano di Comunicazione

Il Piano di comunicazione interno ed esterno deve garantire un flusso di informazioni tempestivo e accurato durante l'incidente grave, la discontinuità operativa o la crisi. Esso include informazioni di contatto per le parti chiave interessate, modelli di comunicazione pre-approvati e protocolli per i media e le relazioni pubbliche.
Per i dettagli si rimanda al *Piano di Comunicazione per la Gestione delle Crisi* e al *Piano di Comunicazione della Continuità Operativa.*

4.5 Formazione e sensibilizzazione

Devono essere condotti regolarmente programmi di formazione e sensibilizzazione per garantire che tutti i dipendenti comprendano i loro ruoli e le loro responsabilità in caso di incidente, discontinuità operativa e crisi. La formazione deve includere esercizi annuali sulla Continuità Operativa, programmi di sensibilizzazione sulla sicurezza informatica e formazione specifica per le risorse deputate alla gestione della continuità operativa.

4.6 Conformità e Audit

Le Funzioni aziendali preposte devono garantire la conformità agli indirizzi della presente Politica attraverso controlli di linea, una gestione dei rischi e della compliance e controlli di internal auditing.

4.7 Miglioramento Continuo

Il miglioramento continuo deve basarsi sul monitoraggio proattivo dei cambiamenti normativi, delle best practice di settore e delle minacce emergenti, integrando sistematicamente i feedback derivanti dai test ed esercitazioni, dall'analisi degli incidenti e dagli esiti degli audit, al fine di rafforzare la resilienza, ottimizzare i processi e garantire la costante efficacia della Gestione delle Crisi, Continuità Operativa e incidenti di Gruppo.

5 Responsabilità di aggiornamento

Il *Responsabile Gestione Continuità Operativa ed Emergenze di Gruppo* cura l'aggiornamento del presente documento ogni qual volta subentri una variazione del modello organizzativo e di governance e del contesto normativo, operativo o del mercato di riferimento che modifichi in maniera significativa il profilo di rischio ovvero i processi ivi disciplinati.

Le Funzioni coinvolte nelle attività disciplinate dal presente documento sono responsabili della rilevazione e della segnalazione al *Responsabile Gestione Continuità Operativa ed Emergenze di Gruppo* degli accadimenti aziendali di carattere operativo che possono comportare la necessità di aggiornamento.

A fronte di modifiche di carattere non sostanziale, quali ad esempio la variazione di denominazione delle funzioni aziendali, aggiornamenti normativi, che non hanno impatti sulle soluzioni definite, o degli strumenti informatici senza impatti rilevanti sui processi disciplinati, il responsabile della funzione owner del documento aggiorna il documento, non attivando il processo di verifica e approvazione, ma garantendo l'informativa ai destinatari del documento stesso.

6 Riferimenti

Il presente documento è definito in coerenza con gli strumenti normativi interni e i riferimenti normativi esterni vigenti applicabili al Gruppo Poste Italiane. In particolare:

Esterni

- CCNL per i Dirigenti di Aziende produttrici di Beni e Servizi

Normativi e legali:

- **Regolamento UE 2016/679 "GDPR"** - "Regolamento del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE": regolamento generale sulla protezione dei dati personali, direttamente applicabile dal 25 maggio 2018 in tutti gli Stati membri dell'Unione Europea.
- **Regolamento (UE) 2022/2554** - Digital Operational Resilience Act (DORA), è una normativa dell'Unione Europea che stabilisce un quadro di requisiti per migliorare la resilienza operativa digitale delle entità finanziarie. Pubblicato il 27 dicembre 2022, DORA fa parte di un pacchetto legislativo dell'UE volto a rafforzare la capacità del settore finanziario di prevenire, rispondere e riprendersi da incidenti informatici e altre interruzioni operative.
- **Circolare 285 del 2013 della Banca d'Italia** - Disposizioni di Vigilanza per le Banche, è un documento chiave che stabilisce le norme e le regolamentazioni per il settore bancario italiano. Il Titolo IV della Circolare è dedicato ai "*Controlli interni, sistema informativo e continuità operativa*."
- **D.Lgs. 8 giugno 2001, n. 231** "Disciplina della responsabilità amministrativa delle persone giuridiche, delle Società e delle associazioni anche prive di personalità giuridica, a norma dell'art. 11 della legge 29 settembre 2000, n. 300".
- **Regolamento IVASS n. 38 del 3 luglio 2018** – Disposizioni in materia di sistema di governo societario.

Standard:

- **ISO/IEC 27001:2022** "Information security, cybersecurity and privacy protection – Information security management systems – Requirements".
- **ISO 22301:2019** - Security and resilience - Business continuity management systems – Requirements.

Interni

- Politica Integrata del Gruppo Poste Italiane
- Politica per la Gestione delle Crisi e della Continuità Operativa di Gruppo
- Linea Guida '*Gestione Crisi e Continuità Operativa di Gruppo'*
- Linea Guida '*Gestione Eventi e Incidenti di Gruppo'*
- Linea Guida '*Sistema di Controllo Interno e Gestione Rischi (SCIGR)*'
- Linea Guida '*Sistema di segnalazione delle violazioni (*whistleblowing)'
- Linea Guida '*Sistema Normativo Aziendale*'
- Piano di Continuità Operativa di Gruppo
- Piano Disaster Recovery e Continuità Operativa ICT
- Procedura Gestione Documenti
- Codice Etico del Gruppo Poste Italiane

- Compendio dei poteri di Poste Italiane
- CCNL per il personale non dirigente di Poste Italiane
- Modello di Organizzazione, Gestione e Controllo di Poste Italiane S.p.A. ai sensi del Decreto Legislativo n. 231/2001 - “Responsabilità Amministrativa della Società”
- Linea Guida "Flussi informativi 231 all'Organismo di Vigilanza di Poste Italiane"

7 Sistemi di gestione e/o modelli organizzativi/normative di riferimento

Modello ai sensi del Decreto Legislativo n. 231/2001	☐
Modello 262	☐
Modello Privacy	☐
Sistema di Gestione per la Qualità (SGQ)	☐
Sistema di Gestione per la sicurezza delle informazioni (SGSI)	☒
Sistema di Gestione Ambientale (EMS)	☐
Sistema di Gestione per la sicurezza e la tutela della salute sui luoghi di lavoro (SGSL)	☐
Sistema di Gestione Anticorruzione (SGA)	☐
Sistema di Gestione dell'energia consumata per usi propri (EnMS)	☐
Gestione dei Servizi Informatici (ITSM)	☒
Sistema di Gestione della Compliance (CMS)	☐
Normativa di Settore/Disposizioni da Organi di Vigilanza (es: normative bancarie, finanziarie, assicurative, postale…)	☒
Patrimonio BancoPosta	☒

8 Destinatari

- Le Funzioni di Poste Italiane interessate dal processo, incluso BancoPosta Patrimonio separato;
- PostePay;
- Gruppo PosteVita;
- BancoPosta Fondi SGR.

I destinatari del documento devono assicurare la diffusione della documentazione all'interno della propria Funzione, in coerenza con gli ambiti operativi ed applicativi di riferimento.

**** QUESTA È L'ULTIMA PAGINA DEL DOCUMENTO ****