ISTITUTO NAZIONALE DELLA PREVIDENZA SOCIALE

Deliberazione n. 155

OGGETTO: Adozione delle misure per l'adempimento degli obblighi di cui agli articoli 23, 24 e 25 del decreto legislativo 4 settembre 2024, n. 138, "*Recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148*".

IL CONSIGLIO DI AMMINISTRAZIONE

Seduta del 28 ottobre 2026

Visto il D.P.R. 30 aprile 1970, n. 639;

Vista la legge 9 marzo 1989, n. 88;

Visto il decreto legislativo 30 giugno 1994, n. 479;

Visto il D.P.R. 24 settembre 1997, n. 366;

Visto il D.P.R. 9 febbraio 2024 di nomina del Presidente dell'Istituto Nazionale della Previdenza Sociale;

Visto il D.P.C.M. 13 marzo 2024 di nomina del Consiglio di Amministrazione dell'Istituto Nazionale della Previdenza Sociale;

Visto il D.M. 29 aprile 2024 di nomina del Direttore generale dell'Istituto Nazionale della Previdenza Sociale;

Visto il Regolamento di organizzazione dell'Istituto, adottato con deliberazione del Consiglio di Amministrazione n. 4 del 6 maggio 2020, da ultimo modificato con determinazione commissariale n. 49 del 14 settembre 2023;

Visto l'Ordinamento delle funzioni centrali e territoriali dell'INPS, adottato con deliberazione del Consiglio di Amministrazione n. 137 del 7 settembre 2022, da ultimo modificato con deliberazione del Consiglio di Amministrazione n. 182 del 12 novembre 2025;

Il Segretario

Firmato digitalmente da:
Gaetano Corsini
Data:28/10/2026 17:58:22

Il Presidente

Firmato digitalmente da:
Gabriele Fava
Data:28/10/2026 17:53:37

REP. n. 620

Vista la direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148, (direttiva NIS2);

Visto il decreto legislativo 4 settembre 2024, n. 138, "*Recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148*";

Visti, in particolare, gli articoli 23, 24 e 25, del citato decreto legislativo, i quali disciplinano gli obblighi degli organi di amministrazione e direttivi dei soggetti NIS, in materia di misure di gestione dei rischi per la sicurezza informatica e di notifica di incidente;

Vista la legge 28 giugno 2024, n. 90, "*Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici*";

Vista la determinazione dell'Agenzia per la cybersicurezza nazionale n. 37932 del 19 febbraio 2025 con cui l'Istituto Nazionale della Previdenza Sociale è stato individuato quale soggetto essenziale tra le Amministrazioni centrali, regionali, locali e di altro tipo;

Vista, altresì, la determinazione dell'Agenzia per la cybersicurezza nazionale n. 379907 del 19 dicembre 2025, che, in fase di prima applicazione, stabilisce le modalità e le specifiche di base per l'adempimento degli obblighi di cui al decreto legislativo n. 138/2024, riportate, per i soggetti essenziali, nell'Allegato 2;

Preso atto delle "Linee Guida NIS - Specifiche di base" predisposte dall'ACN al fine di illustrare gli adempimenti relativi alle misure di sicurezza di base, di cui agli articoli 23 e 24 del d.lgs. n. 138/2024, e agli incidenti significativi di base, di cui all'articolo 25 del medesimo decreto legislativo;

Tenuto conto che le citate misure prevedono, tra l'altro, l'adozione di un modello di organizzazione per la sicurezza informatica e la definizione dei relativi ruoli e responsabilità, di politiche di sicurezza informatica e di un piano per la gestione degli incidenti di sicurezza informatica;

Preso atto che l'Istituto ha già avviato il percorso di adeguamento alla normativa NIS attraverso la realizzazione di adempimenti e di iniziative che hanno consentito di porre le basi organizzative, informative e formative per la successiva fase di attuazione, e che l'*iter* prosegue con la verifica del livello di implementazione delle misure previste, con l'individuazione degli eventuali scostamenti e con la realizzazione dei necessari interventi organizzativi, procedurali e tecnologici;

Preso atto che, nell'ambito delle evidenze documentali richieste per l'attuazione della disciplina NIS, sono stati predisposti i documenti "*Organizzazione per la sicurezza informatica*", "*Politica di sicurezza informatica*" e"*Piano per la gestione degli incidenti di sicurezza informatica*";

Preso atto che i predetti documenti, pur conservando ciascuno la propria autonomia documentale, costituiscono un insieme coordinato e coerente, idoneo a formalizzare l'assetto di governance della sicurezza informatica, i principi e gli indirizzi generali di protezione e il processo di gestione degli incidenti, assicurando coerenza tra responsabilità, misure e modalità operative e rafforzando il presidio del percorso di adeguamento dell'Istituto alla disciplina NIS2;

Vista la relazione della Direzione generale;

Su proposta del Direttore generale

D E L I B E R A

di adottare i documenti "*Organizzazione per la sicurezza informatica*", "*Politica di sicurezza informatica*"e "*Piano per la gestione degli incidenti di sicurezza informatica*", che, allegati alla presente deliberazione, ne costituiscono parte integrante.

Il Direttore generale porrà in essere gli atti necessari e conseguenti all'attuazione della presente deliberazione.

IL SEGRETARIO — IL PRESIDENTE

Gaetano Corsini — Gabriele Fava

Direzione Centrale Tecnologia, informatica e innovazione

Organizzazione per la Sicurezza Informatica

Versione: 1.0

	Nominativo	Ruolo/Azienda	Data
Approvato da:	Valeria Vittimberga	Direttore Generale	
Verificato da:	Massimiliano D'Angelo	Direttore Centrale Tecnologia, Informatica e Innovazione	12-10-2026
Redatto da:	Area Cybersecurity Area Internal Audit, Risk Management e Compliance IT	DCTII	12-10-2026
Indirizzo di Pubblicazione	Pagina intranet della DCTII		
Stato	approvato		
Classificato	uso interno		

Abstract

Il presente documento descrive il modello organizzativo di riferimento per la sicurezza informatica dell'Istituto, individuando i livelli di responsabilità e le strutture coinvolte.

Storico delle Versioni		
Versione	**Data**	**Informazioni sull'aggiornamento**
V 1.0		Prima emissione del documento

Indice

1 Obiettivo 4
2 Definizioni, Abbreviazioni e Acronimi 5
3 Riferimenti 6
4 Principi generali del modello organizzativo 7
5 Assetto organizzativo per la sicurezza informatica 8
5.1 Organi di amministrazione e direttivi 8
5.2 Punto di contatto NIS 8
5.3 Referente CSIRT 9
5.4 Responsabile per la Transizione al Digitale 9
5.5 Comitato di Crisi 10
5.6 Comitato di Coordinamento 10
5.7 Responsabile della Protezione dei Dati 10
5.8 Direzione Centrale Tecnologia, Informatica e Innovazione 11
5.8.1 Funzioni manageriali coinvolte 12
5.9 Funzioni istituzionali di supporto 13
5.9.1 Direzione Centrale Internal Audit, Risk Management, Compliance e Antifrode 13
5.9.2 Ufficio per le attività del Responsabile della Protezione dei Dati 13
5.9.3 Direzione Centrale Risorse Umane 13
5.9.4 Direzione Centrale Formazione e Accademia INPS 13
5.9.5 Direzione Centrale Risorse Strumentali e Centrale Unica Acquisti 13
5.9.6 Direzione Centrale Comunicazione 14
5.9.7 Coordinamento Generale Tecnico Edilizio 14
5.10 Funzioni di business 14
6 Ruoli e responsabilità 15

1 Obiettivo

Il documento ha la finalità di descrivere il modello organizzativo adottato da INPS per la gestione della sicurezza informatica, individuando i livelli di responsabilità e le strutture coinvolte.

Il modello si applica alle strutture dell'Istituto che, a diverso titolo, partecipano alla definizione, attuazione, gestione, controllo o monitoraggio delle misure organizzative, procedurali e tecniche di sicurezza informatica.

2 Definizioni, Abbreviazioni e Acronimi

Termine/Abbreviazione	Definizione
ACN	Agenzia per la Cybersicurezza Nazionale
CSIRT	Computer Security Incident Response Team
CSIRT Italia	Struttura nazionale istituita presso l'Agenzia per la Cybersicurezza Nazionale, specializzata nella prevenzione, gestione e risposta agli incidenti di sicurezza informatica, nonché nel monitoraggio e nell'analisi di minacce, vulnerabilità e incidenti a livello nazionale.
D.lgs.	Decreto Legislativo
DCTII	Direzione Centrale Tecnologia, Informatica e Innovazione
ICT	Information and Communication Technology

Tabella 1 - Definizioni, Abbreviazioni e Acronimi

3 Riferimenti

Per i riferimenti normativi si rimanda al documento "INPS-SGI-GEN-Requisiti Legali e Regolamentari", redatto e mantenuto dalla Direzione Centrale Tecnologia, Informatica e Innovazione (DCTII) nell'ambito del Sistema di Gestione Integrato certificato ISO.

4 Principi generali del modello organizzativo

Il modello organizzativo per la sicurezza informatica si fonda sui seguenti principi:

- **centralità del governo e della supervisione**: le decisioni rilevanti in materia di sicurezza informatica sono ricondotte ad un sistema di indirizzo, approvazione e monitoraggio coerente con l'assetto dell'Istituto;
- **responsabilità diffuse e coordinate**: la sicurezza informatica non è circoscritta a una singola funzione, ma richiede il contributo coordinato di tutte le strutture;
- **coerenza organizzativa e documentale**: il modello organizzativo per la sicurezza informatica è definito in coerenza con l'assetto organizzativo dell'Istituto, con le competenze attribuite alle strutture coinvolte, con la Politica di sicurezza informatica e con i documenti, le procedure, gli atti organizzativi e le nomine che disciplinano specifici ruoli o responsabilità in materia di sicurezza informatica;
- **adeguatezza delle competenze**: i ruoli rilevanti nell'ambito dell'organizzazione per la sicurezza informatica sono attribuiti tenendo conto delle competenze, delle professionalità e dell'esperienza necessarie all'attribuzione delle relative responsabilità.

Il modello di organizzazione per la sicurezza informatica tiene conto delle misure organizzative e delle pratiche maturate nell'ambito dei Sistemi di Gestione implementati nel perimetro certificato ISO e nell'ambito del Perimetro Nazionale di Sicurezza Cibernetica.

5 Assetto organizzativo per la sicurezza informatica

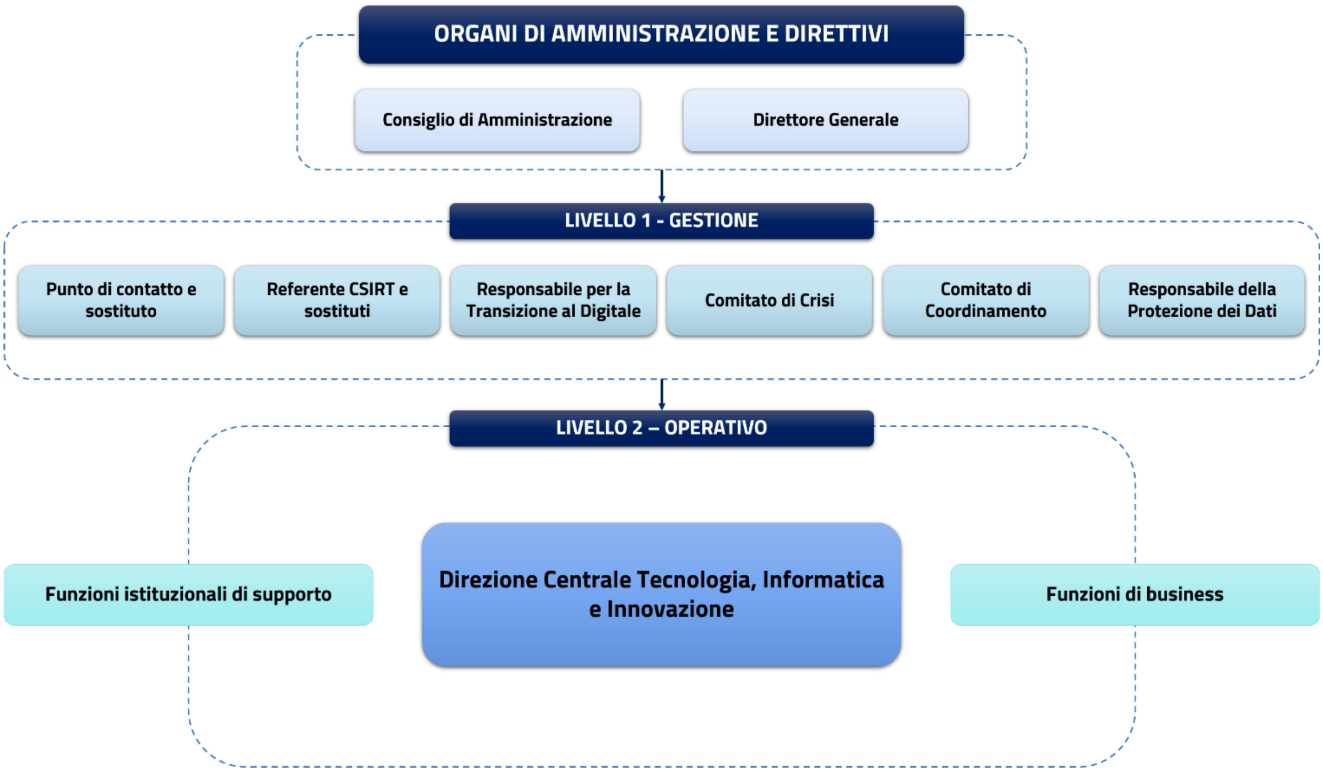


Figura 1 - Schema Logico del modello organizzativo per la Sicurezza Informatica

5.1 Organi di amministrazione e direttivi

Gli organi di amministrazione e direttivi assicurano l'indirizzo, l'adozione e la supervisione complessiva del modello organizzativo per la sicurezza informatica dell'Istituto. In tale ambito, il Consiglio di Amministrazione adotta i documenti previsti dalla normativa applicabile, riceve informative periodiche su rischi, incidenti significativi, stato di attuazione delle misure e iniziative di miglioramento, assume decisioni relative ai rischi residui significativi, alle priorità di trattamento e agli interventi che richiedono indirizzo strategico o allocazione di risorse. Il Direttore Generale presiede al coordinamento delle strutture, sovraintende alla gestione operativa, all'organizzazione e all'attuazione delle misure di sicurezza, presiede il Comitato di Crisi e sottopone al Consiglio di Amministrazione le proposte e le informative di competenza.

5.2 Punto di contatto NIS

Il Punto di contatto NIS è la persona fisica designata ai sensi del D.lgs. 138/2024 (Decreto NIS), incaricata di curare, per conto dell'Istituto, l'attuazione degli adempimenti previsti dalla normativa stessa, nonché l'interlocuzione con l'ACN.

Il Punto di contatto, individuato all'interno dell'Istituto nel Direttore *pro-tempore* della Direzione Centrale Tecnologia, Informatica e Innovazione, riferisce direttamente agli

organi di amministrazione e direttivi, fermo restando che la responsabilità per l'attuazione degli obblighi previsti dalla normativa rimane in capo agli organi di amministrazione e direttivi.

Il Punto di contatto assolve le funzioni di referente per la cybersicurezza ai sensi della legge 90 del 2024.

Il sostituto del Punto di contatto assicura continuità operativa nello svolgimento delle funzioni attribuite, potendo supportare il Punto di contatto e operare, secondo le modalità previste, sulla piattaforma dedicata.

Il Punto di contatto e il suo sostituto sono designati mediante apposito atto di delega del Presidente dell'Istituto.

5.3 Referente CSIRT

Il Referente CSIRT, individuato all'interno dell'Istituto nell'ambito della Direzione centrale Tecnologia, Informatica e Innovazione, Area Cybersecurity, è la persona fisica designata ai sensi del D.lgs. 138/2024, per assicurare l'interlocuzione operativa con il CSIRT Italia e supportare la gestione dei flussi di comunicazione e notifica degli incidenti di sicurezza informatica.

I sostituti del Referente CSIRT assicurano continuità operativa e tempestività nelle comunicazioni con CSIRT Italia, supportando il Referente nello svolgimento delle attività di competenza.

Il Referente CSIRT e i suoi sostituti sono designati dal Punto di contatto mediante apposita registrazione e nomina effettuata sul portale dell'Agenzia per la Cybersicurezza Nazionale (ACN).

5.4 Responsabile per la Transizione al Digitale

Il Responsabile per la Transizione al Digitale, individuato all'interno dell'Istituto nel Direttore *pro-tempore* della Direzione Centrale Tecnologia, Informatica e Innovazione, è la figura prevista dall'art. 17 del Codice dell'Amministrazione Digitale, cui è affidato il coordinamento della trasformazione digitale dell'amministrazione.

Nell'ambito del modello organizzativo per la sicurezza informatica, il Responsabile per la Transizione al Digitale assicura il raccordo tra trasformazione digitale, sviluppo dei servizi pubblici digitali e presidio della sicurezza informatica, contribuendo, per gli ambiti di competenza, all'integrazione dei requisiti di sicurezza nei processi di digitalizzazione, evoluzione tecnologica, interoperabilità e gestione dei sistemi informativi dell'Istituto.

Il Responsabile per la Transizione al Digitale è nominato con deliberazione del Consiglio di Amministrazione.

5.5 Comitato di Crisi

Il Comitato di Crisi, che è stato costituito con determinazione del Direttore Generale n. 181 del 13 luglio 2023, presieduto dal Direttore Generale e composto dai titolari delle Direzioni Centrali di livello dirigenziale generale, dei Coordinamenti Professionali, delle Direzioni Regionali di Puglia e Lazio e della Direzione di Coordinamento Metropolitano di Roma e dal Responsabile della Protezione dei Dati (DPO), rappresenta l'organo di governo e indirizzo della gestione delle situazioni di crisi che possano compromettere la continuità delle attività e dei servizi dell'Istituto.

Il Comitato di Crisi svolge inoltre un ruolo permanente di indirizzo e supervisione del sistema di Continuità Operativa dell'Istituto, promuovendone l'evoluzione, il consolidamento e il miglioramento continuo. In tale ambito contribuisce alla definizione degli indirizzi strategici in materia di Continuità Operativa, favorisce la diffusione della cultura della resilienza organizzativa e supervisiona le iniziative di formazione, test ed esercitazione finalizzate a verificare l'efficacia delle misure adottate.

5.6 Comitato di Coordinamento

Il Comitato di Coordinamento, individuato con determinazione del Direttore Centrale DCTII n. 18 del 24 maggio 2024, presieduto dal Direttore Centrale Tecnologia, Informatica e Innovazione e composto dai titolari delle Aree Manageriali della DCTII, supporta il Comitato di Crisi nella gestione delle situazioni di crisi.

Esso costituisce il presidio di coordinamento operativo del modello di Continuità Operativa dell'Istituto e supporta il processo di gestione degli eventi che possono determinare impatti sulla regolare erogazione dei servizi e sul funzionamento delle strutture organizzative.

5.7 Responsabile della Protezione dei Dati

Il Responsabile della Protezione dei Dati, designato con determinazione presidenziale n. 1 del 2 gennaio 2026, è incaricato di svolgere, in piena autonomia e indipendenza, i seguenti compiti e funzioni:

- informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal Regolamento, nonché da altre disposizioni nazionali o dell'Unione relative alla protezione dei dati;
- sorvegliare l'osservanza del suddetto Regolamento, di altre disposizioni nazionali o dell'Unione relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;

- fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35 del Regolamento;
- cooperare con il Garante per la protezione dei dati personali;
- fungere da punto di contatto con il Garante per la protezione dei dati personali per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36 ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

5.8 Direzione Centrale Tecnologia, Informatica e Innovazione

La Direzione Centrale Tecnologia, Informatica e Innovazione (DCTII) assicura, nell'ambito delle competenze attribuite dall'assetto organizzativo vigente, la gestione, l'evoluzione e il governo del sistema informativo dell'Istituto, garantendo il raccordo tra indirizzi strategici, pianificazione ICT, sviluppo dei servizi digitali, infrastrutture tecnologiche, innovazione, presìdi di cybersicurezza e funzioni di compliance della sicurezza informatica.

Ai fini del modello organizzativo di sicurezza informatica, la Direzione assicura, attraverso le proprie articolazioni organizzative competenti, il presidio delle funzioni di cybersicurezza, gestione del rischio ICT e cyber, compliance della sicurezza informatica, monitoraggio delle azioni di trattamento e attuazione tecnica delle misure di sicurezza, in raccordo con le funzioni competenti in materia di audit, assurance e controlli interni.

In particolare, la Direzione concorre al governo, all'attuazione e al monitoraggio della sicurezza informatica con riferimento a:

- definizione e monitoraggio di standard, requisiti, controlli e misure di sicurezza applicabili a sistemi, infrastrutture, applicazioni, architetture IT, servizi digitali e piattaforme tecnologiche;
- prevenzione, rilevazione e gestione di eventi e incidenti di sicurezza informatica, anche attraverso il coordinamento dei presìdi tecnici dedicati al monitoraggio, all'identificazione delle minacce, alla gestione delle vulnerabilità e al contrasto degli incidenti cyber;
- supporto alla gestione del rischio ICT e cyber e monitoraggio delle relative azioni di trattamento e miglioramento;
- integrazione dei requisiti di sicurezza nei processi ICT, inclusi pianificazione, progettazione, acquisizione, sviluppo, test, esercizio, manutenzione ed evoluzione dei sistemi informativi, delle applicazioni e dei servizi digitali;
- sicurezza delle infrastrutture tecnologiche, delle reti, dei data center, dei sistemi centrali, dei servizi cloud e degli abilitatori tecnologici;
- continuità operativa e disaster recovery dei servizi ICT, al fine di garantire adeguati livelli di disponibilità, ripristino e resilienza dei sistemi e dei servizi informatici;

- gestione delle identità, degli accessi e dei privilegi autorizzativi;
- sicurezza dei dati e del patrimonio informativo, in raccordo con le funzioni competenti in materia di governo dei dati, protezione dei dati personali, classificazione, utilizzo, condivisione, anonimizzazione, mascheramento e pseudonimizzazione;
- sicurezza nei rapporti con fornitori e terze parti ICT, mediante supporto alla Direzione competente per l'integrazione dei requisiti di sicurezza nei processi di acquisizione, nei capitolati, nei contratti, nei livelli di servizio e nei modelli di collaborazione tecnologica;
- predisposizione di informative periodiche per gli Organi di amministrazione e direttivi su rischi, incidenti significativi, stato di attuazione delle misure e iniziative di miglioramento.

Le specifiche attribuzioni delle strutture interne alla Direzione Centrale Tecnologia, Informatica e Innovazione sono disciplinate dagli atti organizzativi.

5.8.1 Funzioni manageriali coinvolte

I ruoli e le responsabilità coinvolti nella conduzione delle attività operative sono specificati nelle procedure e nei disciplinari; in generale, le principali funzioni operative all'interno della Direzione DCTII sono:

- **Cybersecurity**, per la progettazione, realizzazione e gestione delle soluzioni e processi per la sicurezza del patrimonio informativo dell'Istituto, definizione degli standard di sicurezza delle applicazioni, delle architetture, dei sistemi, delle reti e delle postazioni di lavoro. La funzione Cybersecurity coordina inoltre le attività del CERT (Computer Emergency Response/Readiness Team) e del SOC (Security Operation Center) per l'identificazione e gestione delle minacce cyber;
- **Operation, Infrastrutture e Sistemi**, responsabile della gestione dei sistemi, della rete, dell'esercizio delle applicazioni, delle apparecchiature IT e delle postazioni di lavoro dell'Istituto;
- **IT Governance**, per la definizione dei requisiti di sicurezza nelle acquisizioni di prodotti e forniture, la definizione del fabbisogno IT, la raccolta delle specifiche dei Capitolati Tecnici, il provisioning delle forniture IT ed il coordinamento delle attività di esecuzione dei contratti;
- **Internal Audit, Risk Management e Compliance IT**, per supportare l'indirizzo delle attività di progettazione, sviluppo ed esercizio del sistema informativo dell'INPS allo scopo di garantirne l'aderenza ai requisiti di compliance, sicurezza, resilienza e risk management. Verifica la conformità normativa e processuale, coordina audit, certificazioni, piani di trattamento del rischio IT e attività di assurance in coerenza con gli standard dell'Istituto e le buone pratiche di riferimento.

5.9 Funzioni istituzionali di supporto

Ai fini del presente modello, per funzioni istituzionali di supporto si intendono le strutture dell'Istituto che concorrono alla sicurezza informatica attraverso il presidio di ambiti specialistici, organizzativi, procedurali o di controllo non esclusivamente ICT.

Tali funzioni sono incluse nel modello in quanto la sicurezza informatica richiede il raccordo con processi trasversali quali protezione dei dati personali, gestione del personale, formazione, approvvigionamenti, comunicazione istituzionale, sicurezza fisica e ambientale, controlli interni, risk management, audit e compliance.

Le citate funzioni contribuiscono, per gli ambiti di rispettiva competenza, all'attuazione, integrazione e verifica dei presìdi di sicurezza informatica, in raccordo con la DCTII.

5.9.1 Direzione Centrale Internal Audit, Risk Management, Compliance e Antifrode

La Direzione Centrale Internal Audit, Risk Management, Compliance e Antifrode governa i processi di Risk Management, in raccordo con il sistema integrato dei rischi dell'Istituto, ed è responsabile dei controlli interni ed esterni all'Istituto, ivi inclusi i controlli sulle terze parti e sulla catena di fornitura. Inoltre, per gli ambiti di competenza, contribuisce alla coerenza metodologica, al reporting direzionale e alle attività di assurance, audit e follow-up sull'efficacia dei controlli e delle azioni di trattamento.

5.9.2 Ufficio per le attività del Responsabile della Protezione dei Dati

L'Ufficio per le attività del Responsabile della protezione dei dati svolge attività di supporto e collaborazione al Responsabile della Protezione dei Dati nello svolgimento dei suoi compiti istituzionali di informazione, consulenza e sorveglianza previsti dall'art. 39 del Regolamento UE 2016/679.

5.9.3 Direzione Centrale Risorse Umane

La Direzione Centrale Risorse Umane concorre al modello per gli aspetti relativi all'acquisizione, selezione, gestione e valorizzazione delle risorse umane, alla gestione, modifica o cessazione del rapporto di lavoro.

5.9.4 Direzione Centrale Formazione e Accademia INPS

La Direzione Centrale Formazione e Accademia INPS concorre al modello per gli aspetti relativi alla pianificazione, erogazione, monitoraggio e registrazione delle attività formative e di sensibilizzazione in materia di sicurezza informatica, incluse le iniziative rivolte al personale con ruoli specialistici.

5.9.5 Direzione Centrale Risorse Strumentali e Centrale Unica Acquisti

La Direzione Centrale Risorse Strumentali e Centrale Unica Acquisti concorre al modello per gli aspetti relativi agli approvvigionamenti, alle procedure di gara, ai contratti, alle convenzioni, alle clausole di sicurezza e alla gestione delle relazioni con fornitori e terze parti, in raccordo con le aree della DCTII competenti.

5.9.6 Direzione Centrale Comunicazione

La Direzione Centrale Comunicazione concorre al modello per le comunicazioni istituzionali e, ove previsto, per le comunicazioni verso utenti, destinatari dei servizi, stakeholder esterni e pubblico in caso di incidenti, crisi informatiche o eventi che possano incidere sull'erogazione dei servizi.

5.9.7 Coordinamento Generale Tecnico Edilizio

Concorre al modello per gli aspetti di sicurezza fisica e ambientale relativi a immobili, locali tecnici, sale apparati, data center, impianti e continuità fisico-ambientale.

5.10 Funzioni di business

Ai fini del presente modello, per funzioni di business si intendono le strutture dell'Istituto titolari o competenti rispetto all'erogazione dei servizi istituzionali. In tale ambito rientrano, in particolare:

- Direzione Centrale Ammortizzatori Sociali;
- Direzione Centrale Credito Welfare e Strutture Sociali;
- Direzione Centrale Entrate;
- Direzione Centrale Inclusione e Sostegno alla Famiglia e alla Genitorialità;
- Direzione Centrale Pensioni;
- Direzione Centrale Salute e prestazioni di Disabilità;
- Direzione Centrale Servizi al Territorio.

Le funzioni di business sono incluse nel modello organizzativo per la sicurezza informatica in quanto detengono la conoscenza dei servizi erogati, delle informazioni trattate, delle esigenze operative e degli impatti che potrebbero derivare da eventi di indisponibilità, alterazione, perdita o compromissione dei servizi e dei dati.

Tali funzioni concorrono, per i servizi di rispettiva competenza, all'identificazione delle esigenze funzionali, alla classificazione della criticità dei servizi e delle informazioni trattate, alla valutazione degli impatti, nonché alla definizione delle priorità di continuità, ripristino e comunicazione verso utenti e stakeholder.

6 Ruoli e responsabilità

I ruoli e le responsabilità in materia di sicurezza informatica sono definiti in coerenza con l'assetto organizzativo vigente, gli atti di nomina e le disposizioni interne applicabili.

L'elenco degli specifici ruoli e responsabilità in materia di sicurezza informatica, inclusi il Referente per la cybersicurezza, il Punto di contatto NIS, il Referente CSIRT, il Responsabile per la Transizione al Digitale e i sostituti, è riportato nell'Allegato – Ruoli e responsabilità in materia di sicurezza informatica, parte integrante del presente documento.

L'Allegato è aggiornato in caso di variazioni organizzative ed è reso disponibile a tutto l'Istituto secondo le modalità interne previste.

Direzione Centrale Tecnologia, informatica e innovazione

Ruoli e responsabilità in materia di sicurezza informatica

Versione: 1.0

	Nominativo	Ruolo/Azienda	Data
Approvato da:	Valeria Vittimberga	Direttore Generale	
Verificato da:	Massimiliano D'angelo	Direttore Centrale Tecnologia, Informatica e Innovazione	12-10-2026
Redatto da:	Area Cybersecurity Area Internal Audit, Risk Management e Compliance IT	DCTII	12-10-2026
Indirizzo di Pubblicazione	Pagina intranet della DCTII		
Stato	approvato		
Classificato	uso interno		

Storico delle Versioni		
Versione	**Data**	**Informazioni sull'aggiornamento**
V 1.0		Prima emissione del documento

ORGANI DI AMMINISTRAZIONE E DIRETTIVI

Ruolo / Funzione	Responsabilità specifiche	Struttura / Organizzazione	Tipologia
Consiglio di Amministrazione	Adotta i documenti previsti dalla normativa applicabile; riceve informative periodiche su rischi, incidenti significativi, stato di attuazione delle misure e iniziative di miglioramento; assume decisioni relative ai rischi residui significativi, alle priorità di trattamento e agli interventi che richiedono indirizzo strategico o allocazione di risorse	Consiglio di Amministrazione	Interno
Direttore Generale	Presiede al coordinamento delle strutture; sovraintende alla gestione operativa, all'organizzazione e all'attuazione delle misure di sicurezza; presiede il Comitato di crisi; sottopone al Consiglio di Amministrazione le proposte e le informative di competenza	Direttore Generale	Interno

LIVELLO 1 - GESTIONE

Ruolo / Funzione	Responsabilità specifiche	Struttura / Organizzazione	Tipologia
Punto di contatto	Assicura le interlocuzioni previste con l'Autorità nazionale competente NIS e cura il presidio delle comunicazioni connesse al ruolo	Direttore Centrale Tecnologia, Informatica e Innovazione	Interno
Sostituto del punto di contatto	Sostituisce il punto di contatto in caso di assenza o impedimento e ne assicura la continuità operativa	Dirigente Area Cybersecurity	Interno
Referente CSIRT	Assicura l'interlocuzione operativa con il CSIRT Italia e supporta la gestione dei flussi di comunicazione e notifica degli incidenti di sicurezza informatica	Area Cybersecurity	Interno
Sostituto del Referente CSIRT	Sostituisce il Referente CSIRT in caso di assenza o impedimento e ne assicura la continuità operativa	Area Cybersecurity	Interno
Sostituto del Referente CSIRT	Sostituisce il Referente CSIRT in caso di assenza o impedimento e ne assicura la continuità operativa	Fornitore di servizi di cybersecurity	Esterno

Responsabile per la Transizione al Digitale	Assicura il raccordo tra trasformazione digitale, sviluppo dei servizi pubblici digitali e presidio della sicurezza informatica, contribuendo, per gli ambiti di competenza, all'integrazione dei requisiti di sicurezza nei processi di digitalizzazione, evoluzione tecnologica, interoperabilità e gestione dei sistemi informativi dell'Istituto	Direttore Centrale Tecnologia, Informatica e Innovazione	Interno
Comitato di Crisi	Rappresenta l'organo di governo e indirizzo della gestione delle situazioni di crisi che possano compromettere la continuità delle attività e dei servizi dell'Istituto	Direttore Generale; Titolari delle Direzioni Centrali di livello dirigenziale generale, dei Coordinamenti Generali, delle Direzioni Regionali di Puglia e Lazio e della Direzione di Coordinamento Metropolitano di Roma, Responsabile della Protezione dei Dati (DPO)	Interno
Comitato di Coordinamento	Costituisce il presidio di coordinamento operativo del modello di Continuità Operativa dell'Istituto e supporta il processo di gestione degli eventi che possono determinare impatti sulla regolare erogazione dei servizi e sul funzionamento delle strutture organizzative	Direttore Centrale Tecnologia, Informatica e Innovazione; Titolari delle Aree Manageriali DCTII	Interno
Responsabile della Protezione dei Dati (DPO)	Svolge funzioni di consulenza e vigilanza in materia di protezione dei dati personali ai sensi dell'art.39 del GDPR	Responsabile della Protezione dei Dati (DPO)	Interno

LIVELLO 2 - OPERATIVO

Ruolo / Funzione	Responsabilità specifiche	Struttura / Organizzazione	Tipologia
Direzione Centrale Tecnologia, Informatica e Innovazione	Concorre alla gestione, evoluzione e governo del sistema informativo, con specifico presidio delle funzioni di cybersicurezza	Direzione Centrale Tecnologia, Informatica e Innovazione - Area Cybersecurity	Interno
Direzione Centrale Tecnologia, Informatica e Innovazione	Concorre alla gestione, evoluzione e governo del sistema informativo, con specifico presidio delle infrastrutture, dei sistemi e dell'esercizio ICT	Direzione Centrale Tecnologia, Informatica e Innovazione - Area Operation, Infrastrutture e Sistemi	Interno
Direzione Centrale Tecnologia, Informatica e Innovazione	Concorre alla gestione, evoluzione e governo del sistema informativo, assicurando il raccordo con pianificazione ICT, processi di acquisizione e governo delle forniture	Direzione Centrale Tecnologia, Informatica e Innovazione - Area IT Governance	Interno
Direzione Centrale Tecnologia, Informatica e Innovazione	Concorre alla gestione, evoluzione e governo del sistema informativo, assicurando il presidio della compliance, del rischio ICT e cyber, del monitoraggio delle azioni di trattamento e delle attività di assurance	Direzione Centrale Tecnologia, Informatica e Innovazione - Area Internal Audit, Risk Management e Compliance IT	Interno
Funzioni istituzionali di supporto	Contribuiscono, per gli ambiti di rispettiva competenza, all'attuazione, integrazione e verifica dei presidi di sicurezza informatica, in raccordo con la DCTII	Direzione Centrale Internal Audit, Risk Management, Compliance e Antifrode; Direzione Centrale Risorse Umane; Direzione Centrale Formazione e Accademia INPS; Direzione Centrale Risorse Strumentali e Centrale Unica Acquisti; Direzione Centrale Comunicazione; Coordinamento Generale Tecnico Edilizio; Ufficio per le attività del Responsabile della Protezione dei Dati	Interno
Funzioni di business	Concorrono, per i servizi di rispettiva competenza, all'identificazione delle esigenze funzionali, alla classificazione della criticità dei servizi e delle informazioni trattate, alla valutazione degli impatti, nonché alla definizione delle priorità di continuità, ripristino e comunicazione verso utenti e stakeholder	Direzione Centrale Ammortizzatori Sociali; Direzione Centrale Credito Welfare e Strutture Sociali; Direzione Centrale Entrate; Direzione Centrale Inclusione e Sostegno alla Famiglia e alla Genitorialità; Direzione Centrale Pensioni; Direzione Centrale Salute e prestazioni di Disabilità; Direzione Centrale Servizi al Territorio	Interno

Direzione Centrale Tecnologia, informatica e innovazione

Politica di Sicurezza Informatica

Versione: 1.0

	Nominativo	Ruolo/Azienda	Data
Approvato da:	Valeria Vittimberga	Direttore Generale	
Verificato da:	Massimiliano D'Angelo	Direttore Centrale Tecnologia, Informatica e Innovazione	12-10-2026
Redatto da:	Area Cybersecurity Area Internal Audit, Risk Management e Compliance IT	DCTII	12-10-2026
Indirizzo di Pubblicazione	Pagina intranet della DCTII		
Stato	approvato		
Classificato	uso interno		

Abstract

La presente Politica definisce i principi e gli indirizzi adottati da INPS per garantire la protezione delle informazioni, dei sistemi informativi e di rete e dei servizi istituzionali, attraverso un approccio basato sulla gestione del rischio e sul miglioramento continuo. Essa costituisce il quadro di riferimento per l'adozione delle misure organizzative, fisiche e tecnologiche necessarie a garantire la sicurezza delle informazioni, la resilienza dei sistemi e la continuità dei servizi, in conformità alla normativa applicabile e agli obiettivi dell'Istituto.

Storico delle Versioni		
Versione	**Data**	**Informazioni sull'aggiornamento**
V 1.0		Prima emissione del documento

Indice

1 Obiettivo 5
2 Definizioni, Abbreviazioni e Acronimi 6
3 Riferimenti 8
4 Politiche di sicurezza informatica 9
4.1 Gestione del rischio 9
4.2 Ruoli e responsabilità 10
4.3 Risorse umane e formazione 11
4.4 Gestione dei rischi della catena di approvvigionamento 11
4.5 Gestione degli asset 12
4.6 Gestione delle vulnerabilità 12
4.7 Continuità operativa, disaster recovery e gestione delle crisi 13
4.8 Gestione dell'autenticazione, delle identità digitali e del controllo accessi 13
4.9 Sicurezza fisica 14
4.10 Sicurezza dei dati 14
4.11 Sviluppo, configurazione, manutenzione e dismissione dei sistemi informativi e di rete 15
4.12 Protezione delle reti e delle comunicazioni 16
4.13 Monitoraggio degli eventi di sicurezza 16
4.14 Risposta agli incidenti e ripristino 17
4.15 Conformità e audit di sicurezza 18
5 Documenti attuativi 19
6 Comunicazione e riesame 20

Indice Tabelle

Tabella 1 - Definizioni, abbreviazioni e acronimi 7

1 Obiettivo

INPS, nella sua qualità di ente di diritto pubblico dotato di personalità giuridica e gestione autonoma, svolge i compiti e le funzioni che ad esso competono, avvalendosi, tra l'altro, di un sistema informativo che utilizza tecnologie informatiche.

Garantire la conformità alle leggi, l'integrità, la disponibilità e l'affidabilità dei servizi erogati, direttamente o tramite terze parti è parte integrante del suo mandato e pertanto pone la sicurezza alla base del proprio sistema informativo.

Il Consiglio di Amministrazione e il Direttore Generale, quali Organi di Amministrazione e Direttivi, riconoscono la sicurezza delle informazioni e la cybersicurezza quali elementi strategici per il perseguimento della missione istituzionale dell'Istituto e si impegnano ad assicurare la disponibilità delle risorse organizzative, economiche e tecnologiche necessarie al mantenimento e al miglioramento continuo del sistema di gestione della sicurezza.

A questo scopo INPS definisce, applica e mantiene un sistema di politiche di sicurezza informatica conforme alla normativa applicabile e volto a proteggere le informazioni contro la perdita, l'indisponibilità, la diffusione incontrollata e l'accesso non autorizzato.

Le politiche per la sicurezza delle informazioni hanno lo scopo di definire gli obiettivi e le regole necessarie alla tutela del patrimonio informativo dell'Istituto; esse rappresentano il mandato e le direttive dell'Istituto a chi, operativamente, è chiamato a trattare le informazioni e, dunque, devono essere osservate da tutto il personale, sia interno che esterno. Tali politiche sono da considerarsi valide per:

- tutte le informazioni trattate (acquisite, modificate, aggregate, archiviate) attraverso supporti fisici o strumenti elettronici per il trattamento delle informazioni;
- tutti i sistemi informativi e di rete a supporto della gestione e dell'archiviazione delle informazioni (es. locali, impianti di energia, impianti di raffreddamento, ecc.);
- le persone che interagiscono con quanto elencato nei punti precedenti.

Eventuali deroghe alle disposizioni della presente Politica devono essere motivate, documentate, temporalmente delimitate e preventivamente autorizzate dal soggetto competente secondo l'assetto organizzativo vigente. La richiesta individua almeno l'ambito della deroga, le ragioni, la durata, i rischi derivanti, le misure compensative e il responsabile del relativo monitoraggio. Le deroghe sono registrate e riesaminate alla scadenza o in caso di variazione del rischio.

Attesa la loro pervasività e la loro trasversalità nei processi operativi d'Istituto, le politiche di sicurezza informatica sottendono alla necessità di assicurare costantemente il raccordo tra le articolazioni interne dell'Istituto stesso le quali concorrono, ognuna per quanto di rispettiva competenza, al concreto mantenimento e progressivo rafforzamento della postura di sicurezza e della resilienza informatica.

2 Definizioni, Abbreviazioni e Acronimi

Termine/Abbreviazione	Definizione
Asset	Risorsa avente valore per l'Istituto, inclusi dati, sistemi, applicazioni, infrastrutture, dispositivi, servizi e componenti tecnologiche.
Audit	Attività di verifica indipendente o strutturata volta ad accertare la conformità a requisiti normativi, procedurali o organizzativi.
Backup	Copia di dati, configurazioni, sistemi o informazioni, predisposta per consentirne il ripristino in caso di perdita, indisponibilità o compromissione.
Cloud	Modello di erogazione di risorse e servizi informatici tramite infrastrutture accessibili da remoto.
CERT	Computer Emergency Response Team; struttura deputata alla gestione, analisi e risposta a eventi, vulnerabilità e incidenti di sicurezza informatica.
CSIRT	Computer Security Incident Response Team; struttura incaricata della gestione e risposta agli incidenti di sicurezza informatica.
Data center	Struttura fisica destinata a ospitare sistemi, apparati, infrastrutture e servizi ICT.
Disaster recovery	Insieme di strategie, piani e procedure finalizzate al ripristino di sistemi, dati e servizi a seguito di eventi disastrosi o gravi indisponibilità.
Endpoint	Dispositivo terminale connesso alla rete, quali postazioni di lavoro, laptop, smartphone, tablet, server o altri dispositivi utilizzati dagli utenti o dai sistemi.
Governance	Sistema di indirizzo, governo, controllo e responsabilità attraverso cui l'Istituto gestisce la sicurezza delle informazioni e la cybersicurezza.
Hardware	Componenti fisiche dei sistemi informativi e di rete, inclusi server, dispositivi, apparati, endpoint e infrastrutture tecnologiche.
ICT	Information and Communication Technology; insieme delle tecnologie dell'informazione e della comunicazione.
Log	Registrazione cronologica di eventi, accessi, attività o operazioni effettuate su sistemi, applicazioni, reti o dispositivi.
Privacy by default	Principio secondo cui, per impostazione predefinita, devono essere trattati solo i dati personali necessari per ciascuna specifica finalità.
Privacy by design	Principio secondo cui la protezione dei dati personali deve essere considerata fin dalla progettazione di processi, sistemi, applicazioni e servizi.
Security by default	Principio secondo cui sistemi, applicazioni e servizi devono essere configurati in modo sicuro per impostazione predefinita.
Security by design	Principio secondo cui la sicurezza deve essere considerata fin dalla progettazione di sistemi, applicazioni, servizi e processi.

Sistemi informativi e di rete rilevanti	Sistemi informativi e di rete rilevanti: sistemi informativi e di rete la cui compromissione comporterebbe un impatto significativo sulla riservatezza, integrità e disponibilità delle attività e dei servizi.
Software	Programmi, applicazioni, sistemi operativi, componenti o codice utilizzati per l'elaborazione, trasmissione o gestione delle informazioni.

Tabella 1 - Definizioni, abbreviazioni e acronimi

3 Riferimenti

Per i riferimenti normativi si rimanda al documento "INPS-SGI-GEN-Requisiti Legali e Regolamentari", redatto e mantenuto dalla Direzione Centrale Tecnologia, Informatica e Innovazione (DCTII) nell'ambito del Sistema di Gestione Integrato certificato ISO.

Di seguito si riportano riferimenti interni specifici del presente documento:

- Organizzazione per la sicurezza informatica.

4 Politiche di sicurezza informatica

4.1 Gestione del rischio

L'Istituto adotta un approccio strutturato alla gestione del rischio per la sicurezza informatica, finalizzato a identificare, analizzare, valutare, trattare e monitorare i rischi che possono incidere sulla riservatezza, integrità e disponibilità delle informazioni e dei sistemi informativi e di rete.

A tal fine, l'Istituto sottopone a valutazione i propri sistemi informativi e di rete e identifica i sistemi informativi e di rete rilevanti, ai fini dell'applicazione delle specifiche misure di sicurezza previste dalla normativa.

La gestione del rischio deve tenere conto del contesto organizzativo, degli asset informativi e tecnologici, delle minacce applicabili, delle vulnerabilità, delle dipendenze da fornitori e dei relativi potenziali impatti.

L'Istituto persegue un approccio multirischio (all-hazards), che considera cioè i rischi derivanti da tutte le tipologie di minaccia ai sistemi informativi e di rete nonché al loro contesto fisico, quali furti, incendi, inondazioni, interruzioni, anche parziali, delle telecomunicazioni e della corrente elettrica, fattore umano, catena di fornitura e in generale accessi fisici non autorizzati.

La valutazione del rischio comprende l'identificazione, l'analisi e la valutazione dei rischi ed è riesaminata a intervalli pianificati e almeno ogni due anni, nonché in caso di incidenti significativi, variazioni organizzative o mutamenti dell'esposizione alle minacce e ai relativi rischi.

I criteri per la valutazione del grado di esposizione al rischio considerano la probabilità che si verifichino incidenti, nonché la loro gravità, compreso il loro impatto sociale ed economico.

Sulla base degli esiti della valutazione del rischio, l'Istituto definisce, attua e monitora un piano di trattamento che individua le misure, le priorità, le responsabilità, le tempistiche e le motivazioni dell'eventuale accettazione del rischio residuo. Qualora, per motivate e documentate ragioni normative o tecniche, non sia possibile attuare specifiche misure applicabili, il piano individua le misure compensative e il relativo rischio residuo.

Le misure adottate, adeguate e proporzionate ai rischi, tengono conto delle conoscenze più aggiornate e dello stato dell'arte in materia nonché dei costi di attuazione.

La valutazione del rischio e il relativo piano di trattamento, inclusa l'eventuale accettazione dei rischi residui, sono sottoposti all'approvazione degli organi di amministrazione e direttivi.

L'intero processo è disciplinato da un piano di gestione dei rischi per la sicurezza informatica, definito, attuato, aggiornato e documentato dall'Istituto a cura delle

Direzioni Centrali competenti, che assicura il coordinamento delle attività di identificazione, analisi, valutazione, trattamento e monitoraggio dei rischi.

Le attività e gli esiti della gestione del rischio di sicurezza informatica costituiscono parte integrante del framework di gestione del rischio dell'Istituto e sono integrati nel più ampio sistema di Enterprise Risk Management (ERM) dell'Istituto.

4.2 Ruoli e responsabilità

La governance della sicurezza informatica costituisce il presidio organizzativo attraverso cui l'Istituto assicura il governo, l'indirizzo, il coordinamento e il monitoraggio delle iniziative di sicurezza informatica.

Nel documento "Organizzazione per la sicurezza informatica", l'Istituto definisce e mantiene un assetto idoneo ad assicurare il governo delle attività di protezione delle informazioni e dei sistemi informativi e di rete. Tale organizzazione prevede l'attribuzione di ruoli e responsabilità coerenti con l'assetto istituzionale, organizzativo e tecnologico dell'Istituto, nonché con gli obblighi previsti dalla normativa applicabile. Tale organizzazione, adottata dal Consiglio di Amministrazione, è resa nota alle strutture dell'Istituto.

La sicurezza informatica è una responsabilità condivisa che coinvolge, secondo le rispettive competenze, gli organi di amministrazione e direttivi, le strutture di gestione, le funzioni tecniche, il personale interno, i collaboratori esterni, gli amministratori di sistema, i fornitori e le terze parti.

Ciascun soggetto è tenuto a operare nel rispetto della presente Politica, dei documenti attuativi e delle istruzioni applicabili, contribuendo alla prevenzione, rilevazione, segnalazione e gestione di eventi o condizioni che possano compromettere la sicurezza informatica.

I ruoli e le responsabilità in materia di sicurezza informatica sono riesaminati e, ove necessario, aggiornati periodicamente e comunque almeno ogni due anni, nonché al verificarsi di incidenti significativi, variazioni organizzative o mutamenti dell'esposizione alle minacce e ai relativi rischi. Gli esiti del riesame e gli eventuali aggiornamenti sono documentati e comunicati alle strutture dell'Istituto.

Ai fini del modello organizzativo di sicurezza informatica, la Direzione Centrale Tecnologia, Informatica e Innovazione assicura, attraverso le proprie articolazioni organizzative competenti, il presidio delle funzioni di cybersicurezza, gestione del rischio ICT e cyber, compliance della sicurezza informatica, monitoraggio delle azioni di trattamento e attuazione tecnica delle misure di sicurezza, in raccordo con le funzioni competenti in materia di audit, assurance e controlli interni.

4.3 Risorse umane e formazione

L'Istituto riconosce il ruolo cruciale del personale interno ed esterno nella protezione delle informazioni e assicura che chiunque vi acceda o le tratti, operi in modo da preservarne la riservatezza, l'integrità e la disponibilità.

Il personale interno è selezionato in accordo alle norme vigenti per le P.A. centrali. Il rapporto di lavoro, ivi incluso il procedimento disciplinare, è regolato dai contratti di lavoro e dall'ordinamento dell'Istituto.

Il personale esterno è selezionato in accordo alla normativa vigente in materia di Contratti Pubblici e la specifica disciplina contrattuale regola l'ingaggio, il monitoraggio e la verifica della prestazione erogata dal personale esterno.

L'Istituto definisce, attua e aggiorna un programma di formazione e sensibilizzazione sulla sicurezza informatica, articolato in funzione dei ruoli, delle attività svolte e dei rischi associati. Il relativo piano, adottato dal Consiglio di Amministrazione, disciplina le attività e i contenuti formativi, includendo iniziative specifiche per il personale neoassunto e per il personale con ruoli specialistici sulla base delle mansioni e del ruolo che ricopre. L'efficacia della formazione è verificata periodicamente e le attività svolte sono documentate in appositi registri.

Gli organi di amministrazione e direttivi seguono una formazione in materia di sicurezza informatica adeguata alle responsabilità loro attribuite e ne promuovono l'offerta periodica al personale.

L'assegnazione di ruoli, incarichi e autorizzazioni di accesso tiene conto delle competenze richieste, delle esigenze di servizio e dei rischi connessi alle informazioni e ai sistemi interessati. Gli accordi applicabili al personale dipendente, ai consulenti, ai fornitori e ai collaboratori esterni disciplinano le responsabilità in materia di sicurezza informatica e, in funzione del rischio, gli obblighi destinati a permanere dopo la cessazione o la modifica del rapporto, inclusi eventuali impegni di riservatezza. L'inosservanza delle istruzioni impartite comporta l'applicazione delle conseguenze previste dall'ordinamento e dagli accordi applicabili.

4.4 Gestione dei rischi della catena di approvvigionamento

L'Istituto governa i rischi per la sicurezza informatica derivanti dalla catena di approvvigionamento, con particolare riferimento ai fornitori e alle terze parti che, per conto dell'Istituto, accedono agli asset, trattano informazioni, erogano servizi ICT o forniscono componenti, applicazioni, infrastrutture o servizi per i sistemi informativi e di rete.

L'Istituto definisce ruoli, responsabilità e modalità di governo delle relazioni con i fornitori, assicurando il coinvolgimento delle funzioni competenti nella valutazione e nella gestione dei rischi connessi alle forniture.

L'Istituto definisce requisiti di sicurezza commisurati al livello di criticità risultante dalla valutazione del rischio della fornitura e coerenti con le misure applicate ai propri sistemi informativi e di rete. Ove pertinenti, tali requisiti riguardano l'affidabilità del fornitore, la sicurezza dei dati, dei sistemi e degli accessi, la continuità operativa, la gestione degli incidenti e gli ulteriori rischi connessi al ciclo di vita della fornitura e alla relativa catena di approvvigionamento. I requisiti sono recepiti nella documentazione di gara e contrattuale e, ove applicabile, estesi ai subfornitori e agli altri soggetti coinvolti.

L'accesso fisico e logico dei fornitori alle informazioni e ai sistemi dell'Istituto è consentito secondo il principio della necessità operativa e nel rispetto dei requisiti di sicurezza definiti. Gli eventuali ruoli e responsabilità in materia di sicurezza informatica attribuiti al personale delle terze parti sono definiti e resi noti alle strutture dell'Istituto.

Inoltre, l'Istituto mantiene un inventario aggiornato dei fornitori relativi a forniture con potenziali impatti sulla sicurezza dei sistemi informativi e di rete, contenente almeno i riferimenti di contatto e la tipologia di fornitura.

La conformità delle forniture ai requisiti di sicurezza contrattualizzati è monitorata, verificata periodicamente e documentata lungo l'intero ciclo di vita del rapporto, incluse le modifiche significative e la cessazione, al fine di individuare eventuali scostamenti e le conseguenti azioni correttive o di miglioramento.

4.5 Gestione degli asset

L'Istituto assicura l'identificazione, il censimento, la classificazione e il monitoraggio degli asset informativi e tecnologici mediante inventari comprendenti, ove applicabile, hardware, software, applicazioni, infrastrutture, componenti di rete, servizi erogati o gestiti da terze parti e risorse umane. Tale gestione viene assicurata durante tutto il ciclo di vita degli asset censiti.

Sono inoltre mantenuti aggiornati l'inventario dei flussi di rete esterni autorizzati, nonché quello dei servizi informatici erogati dai fornitori, inclusi i servizi cloud, al fine di assicurare la conoscenza delle dipendenze rilevanti per la sicurezza e la continuità dei sistemi informativi e di rete.

Gli inventari sono riesaminati e aggiornati periodicamente e in occasione di modifiche rilevanti del contesto organizzativo, tecnologico, contrattuale o architetturale, al fine di garantirne completezza, accuratezza e coerenza e di supportare la gestione dei rischi, delle vulnerabilità, degli accessi, della continuità operativa e degli eventi di sicurezza.

4.6 Gestione delle vulnerabilità

L'Istituto assicura la gestione continua delle vulnerabilità dei sistemi informativi e di rete, delle applicazioni, dei componenti tecnologici e dei servizi, attraverso attività di identificazione, analisi, valutazione, trattamento e monitoraggio basate su fonti interne ed esterne. A tal fine, monitora almeno i canali del CSIRT Italia, nonché, ove pertinenti,

quelli dei CERT, degli Information Sharing and Analysis Centre settoriali e dei fornitori del software ritenuto critico.

Le vulnerabilità individuate sono valutate e prioritizzate in base al livello di rischio e alla criticità degli asset interessati, al fine di definire misure di trattamento proporzionate. Esse sono risolte mediante aggiornamenti di sicurezza o misure di mitigazione, ove disponibili; in alternativa, il rischio è documentato e gestito in coerenza con il piano di trattamento dei rischi per la sicurezza informatica. L'efficacia delle misure adottate è sottoposta a monitoraggio e riesame.

L'intero processo è disciplinato da un piano di gestione delle vulnerabilità, definito, attuato, aggiornato e documentato dall'Istituto, che stabilisce modalità, pianificazione, procedure, ruoli e responsabilità per l'identificazione e la gestione delle vulnerabilità e delle relative informazioni.

4.7 Continuità operativa, disaster recovery e gestione delle crisi

L'Istituto definisce e mantiene presidi di continuità operativa, disaster recovery e gestione delle crisi, finalizzati a garantire la continuità e il ripristino delle attività e dei servizi in caso di eventi avversi. A tal fine, definisce, attua, aggiorna e documenta piani di continuità operativa, ripristino in caso di disastro e gestione delle crisi informatiche, commisurati alla criticità dei servizi e agli esiti della valutazione del rischio.

I piani tengono conto degli asset e delle loro interdipendenze per le finalità istituzionali e definiscono, ove applicabile, finalità e ambito, esigenze di continuità e ripristino, ruoli e responsabilità, modalità di coordinamento e comunicazione interna ed esterna, condizioni di attivazione e disattivazione dei piani stessi e risorse necessarie.

I piani di ripristino in caso di disastro individuano inoltre l'ordine e le procedure di ripristino dei servizi e dei sistemi interessati, nonché i relativi obiettivi di ripristino.

I piani sono adottati dal Consiglio di Amministrazione, comunicati, sottoposti periodicamente a esercitazioni, verifiche o test e riesaminati e, ove opportuno, aggiornati almeno ogni due anni, nonché in caso di incidenti significativi o mutamenti dell'esposizione alle minacce e ai relativi rischi.

4.8 Gestione dell'autenticazione, delle identità digitali e del controllo accessi

L'Istituto assicura che l'accesso alle informazioni e ai sistemi informativi e di rete sia consentito esclusivamente a soggetti autorizzati. Tutte le utenze, incluse quelle con privilegi amministrativi e quelle utilizzate per l'accesso da remoto, sono censite e approvate dai soggetti competenti e, fatte salve motivate e documentate ragioni tecniche, sono di regola personali o il loro utilizzo deve essere sempre attribuibile ad un operatore. Le credenziali sono protette, robuste e aggiornate secondo criteri coerenti con gli esiti della valutazione del rischio. Per almeno i sistemi informativi e di rete

rilevanti, le utenze e le relative autorizzazioni sono verificate periodicamente e aggiornate o revocate in caso di variazioni, quali trasferimenti, modifiche delle mansioni o cessazione del rapporto.

Le modalità di autenticazione sono commisurate al rischio, tenendo conto dei privilegi attribuiti alle utenze, della criticità dei sistemi informativi e di rete e della tipologia di operazioni consentite. Per almeno i sistemi informativi e di rete rilevanti, l'accesso dalla rete esterna richiede modalità di autenticazione multi-fattore.

I permessi e le autorizzazioni sono assegnati secondo i principi del minimo privilegio, della separazione delle funzioni e della necessità di conoscere. Per gli amministratori di sistema, ove possibile, è assicurata la distinzione tra utenze con privilegi amministrativi e utenze prive di tali privilegi.

Per almeno i sistemi informativi e di rete rilevanti, l'Istituto definisce e adotta adeguate misure di sicurezza per l'accesso. È inoltre mantenuto un elenco aggiornato dei sistemi informativi e di rete accessibili da remoto, con la descrizione delle relative modalità di accesso.

4.9 Sicurezza fisica

L'Istituto protegge le proprie sedi, i locali, i data center, le infrastrutture, le apparecchiature, i supporti fisici e le informazioni dai rischi derivanti da accessi non autorizzati, danneggiamenti, eventi accidentali, minacce ambientali e azioni dolose. Le misure di sicurezza fisica e ambientale sono definite in funzione dei rischi, della criticità degli asset e delle esigenze di continuità operativa, al fine di tutelare le persone e assicurare la protezione delle informazioni e dei sistemi informativi e di rete.

Particolare attenzione è riservata ai data center, il cui accesso è consentito esclusivamente ai soggetti autorizzati e gestito secondo modalità formalizzate. Gli accessi di fornitori, visitatori e altri soggetti esterni sono autorizzati, registrati e, ove necessario, supervisionati. Le apparecchiature sono installate, utilizzate e mantenute in ambienti adeguatamente protetti e il loro ciclo di vita è gestito in modo da prevenire perdita di informazioni, accessi non autorizzati o compromissioni della sicurezza.

Le regole di comportamento applicabili nei data center e nelle altre aree ad accesso ristretto sono definite nella documentazione di dettaglio. Le misure e le procedure di sicurezza fisica sono mantenute aggiornate e riesaminate periodicamente in funzione dell'evoluzione dei rischi e del contesto organizzativo, tecnologico e logistico.

4.10 Sicurezza dei dati

L'Istituto protegge i dati e le informazioni durante l'intero ciclo di vita, adottando misure tecniche e organizzative commisurate alla loro classificazione, agli obblighi normativi applicabili e ai rischi derivanti dalla compromissione della riservatezza, dell'integrità o della disponibilità.

La protezione delle informazioni a riposo e in transito è assicurata, in funzione del rischio, anche mediante controlli crittografici e un'adeguata gestione delle relative chiavi. Fatte salve motivate e documentate ragioni normative o tecniche, sono cifrati mediante protocolli e algoritmi considerati sicuri i dati memorizzati su dispositivi portatili e supporti removibili, nonché quelli trasmessi da e verso l'esterno dell'Istituto, inclusi i dati scambiati mediante sistemi di comunicazione vocale, video e testuale. I supporti removibili sono inoltre sottoposti a misure volte a prevenirne l'utilizzo improprio e a rilevare eventuali codici malevoli.

L'Istituto assicura la possibilità di recuperare dati, informazioni, software e configurazioni in caso di indisponibilità o compromissione, effettuando periodicamente le attività di backup in coerenza con le esigenze di continuità operativa e di ripristino. Per almeno i sistemi informativi e di rete rilevanti, sono adottate tecnologie di backup che garantiscono la riservatezza e l'integrità mediante adeguate misure di protezione fisica o crittografica. L'utilizzabilità dei backup è verificata periodicamente mediante test di ripristino effettuati su base campionaria, documentandone gli esiti e le eventuali azioni correttive o di miglioramento.

4.11 Sviluppo, configurazione, manutenzione e dismissione dei sistemi informativi e di rete

L'Istituto assicura che la sicurezza informatica e la protezione dei dati siano considerate durante l'intero ciclo di vita dei sistemi informativi e di rete, dalla definizione dei requisiti fino alla manutenzione, modifica e dismissione. I sistemi sono progettati, sviluppati e configurati secondo i principi di security by design e by default e, ove applicabile, di data protection by design e by default, adottando misure proporzionate ai rischi da gestire. Per almeno i sistemi informativi e di rete rilevanti, sono definite e documentate configurazioni di riferimento sicure.

Gli ambienti di sviluppo, test e produzione sono opportunamente separati e i sistemi, le applicazioni e i componenti tecnologici sono sottoposti a controlli di sicurezza prima della messa in esercizio e in occasione di modifiche rilevanti. Lo sviluppo del software avviene secondo pratiche di sicurezza documentate e coerenti con la criticità delle applicazioni, delle informazioni trattate e dei servizi supportati. Le modifiche a sistemi, applicazioni, infrastrutture e configurazioni sono valutate, autorizzate e tracciate attraverso processi controllati.

L'Istituto assicura inoltre la disponibilità degli aggiornamenti di sicurezza per il software installato e la loro applicazione senza ingiustificato ritardo, in coerenza con la criticità dei sistemi e con il piano di gestione delle vulnerabilità, fatte salve motivate e documentate ragioni normative o tecniche. Gli aggiornamenti del software ritenuto critico sono verificati in ambiente di test prima dell'impiego operativo, salvo motivate e documentate ragioni normative o tecniche.

La manutenzione, la sostituzione, il trasferimento e la dismissione di sistemi, componenti e supporti sono gestiti secondo modalità controllate e documentate, al fine di prevenire perdita di informazioni, accessi non autorizzati, configurazioni non sicure o indisponibilità dei servizi. Per almeno i sistemi informativi e di rete rilevanti, sono adottate procedure per il trasferimento e la dismissione sicura dei dispositivi di memorizzazione e sono mantenuti registri delle manutenzioni hardware effettuate.

4.12 Protezione delle reti e delle comunicazioni

L'Istituto protegge le reti, le comunicazioni elettroniche, gli accessi remoti, il traffico dati e i servizi di rete mediante misure commisurate ai rischi e alle esigenze di continuità e resilienza. A tal fine, le reti e i servizi di comunicazione sono progettati, gestiti e monitorati adottando configurazioni sicure, controlli degli accessi e dei flussi informativi, segregazione degli ambienti e adeguati sistemi di protezione perimetrale, mantenuti aggiornati e correttamente configurati.

Il trasferimento delle informazioni, sia all'interno dell'Istituto sia verso fornitori, partner, amministrazioni e altri soggetti esterni, avviene attraverso modalità coerenti con la classificazione delle informazioni, i rischi associati e i requisiti normativi e contrattuali applicabili. Le comunicazioni elettroniche, inclusi i servizi di posta elettronica, messaggistica e collaborazione, sono protette mediante adeguate misure tecniche e organizzative volte a prevenire accessi non autorizzati, alterazioni, divulgazioni indebite e perdita delle informazioni.

Inoltre, l'Istituto si dota di sistemi di comunicazione di emergenza protetti, idonei a supportare il coordinamento e lo scambio di informazioni in situazioni avverse o di crisi.

Le misure di protezione delle reti e delle comunicazioni sono documentate, mantenute aggiornate e riesaminate periodicamente in funzione dell'evoluzione dei rischi, delle minacce, delle architetture e delle tecnologie utilizzate.

4.13 Monitoraggio degli eventi di sicurezza

L'Istituto assicura il monitoraggio continuo degli eventi di sicurezza mediante strumenti tecnici adeguatamente configurati, aggiornati e mantenuti, nonché attraverso la registrazione, raccolta, protezione, conservazione e analisi delle registrazioni (log) e delle evidenze rilevanti, al fine di rilevare tempestivamente anomalie, accessi non autorizzati, eventi potenzialmente avversi e incidenti significativi.

Ai fini del rilevamento di anomalie e scostamenti rispetto alle condizioni di normale funzionamento, l'Istituto definisce e documenta i livelli di servizio attesi dei propri servizi e delle proprie attività.

I log e le evidenze sono protetti in modo da garantirne riservatezza, integrità e disponibilità limitandone l'accesso al personale autorizzato e assicurando, ove applicabile, la sincronizzazione temporale delle fonti di registrazione. Le tempistiche di

conservazione dei log sono definite e documentate tenendo conto delle esigenze di monitoraggio, investigazione e conformità normativa. Il monitoraggio è definito in funzione del rischio e comprende gli accessi da remoto e le attività effettuate mediante utenze privilegiate. Per almeno i sistemi informativi e di rete rilevanti, comprende inoltre gli accessi, eseguiti o falliti, ai sistemi perimetrali, alle risorse di rete e agli applicativi.

L'Istituto adotta inoltre strumenti per l'analisi e il filtraggio del traffico in ingresso e per la rilevazione e il contrasto di contenuti e codici malevoli. Fatte salve motivate e documentate ragioni normative o tecniche, i sistemi di protezione degli endpoint sono adeguatamente configurati, aggiornati e mantenuti.

Le modalità di monitoraggio, registrazione, analisi, gestione degli alert ed escalation degli eventi di sicurezza sono documentate, mantenute aggiornate e riesaminate periodicamente, in funzione dell'evoluzione delle minacce, degli esiti della valutazione del rischio e degli incidenti occorsi.

4.14 Risposta agli incidenti e ripristino

L'Istituto definisce e attua un processo per la gestione degli incidenti di sicurezza informatica, che disciplini l'intero ciclo di vita degli incidenti che possono compromettere le informazioni, i sistemi informativi e di rete o i servizi erogati.

Il processo è disciplinato e formalizzato nel Piano per la gestione degli incidenti di sicurezza informatica, che definisce le fasi del ciclo di vita dell'incidente, i ruoli e le responsabilità, i canali di segnalazione e comunicazione, i criteri di classificazione e di escalation, le informazioni di contatto e la reportistica necessaria alla documentazione degli incidenti. Nei casi previsti dalla normativa applicabile, l'Istituto assicura le notifiche al CSIRT Italia e le comunicazioni alle altre autorità competenti secondo le modalità e le tempistiche previste.

Il Piano è riesaminato e, ove opportuno, aggiornato periodicamente e comunque almeno ogni due anni, nonché in caso di incidenti significativi o mutamenti dell'esposizione alle minacce e ai relativi rischi, tenendo conto delle lezioni apprese.

L'Istituto assicura la registrazione e l'analisi degli incidenti, l'attuazione delle attività di contenimento e ripristino e la raccolta e protezione delle evidenze rilevanti. Le attività di ripristino e il relativo stato sono comunicati alle articolazioni interne interessate, secondo modalità definite e documentate, al fine di garantire il coordinamento delle attività. Le conoscenze acquisite sono utilizzate per individuare azioni correttive e migliorare le capacità di prevenzione, risposta e resilienza dell'Istituto.

Sono inoltre predisposte procedure per la comunicazione degli incidenti significativi ai destinatari dei servizi, agli altri soggetti interessati e, laddove necessario, al pubblico. Gli incidenti che comportano o possono comportare una violazione dei dati personali sono gestiti in coordinamento con i processi e le procedure applicabili in materia di protezione dei dati personali.

4.15 Conformità e audit di sicurezza

L'Istituto monitora la conformità alle disposizioni normative in materia di sicurezza informatica e ai documenti interni applicabili attraverso attività di verifica, audit, riesame e valutazione dell'efficacia delle misure adottate. Gli esiti di tali attività sono documentati, comunicati ai livelli organizzativi competenti e utilizzati per individuare eventuali scostamenti e le conseguenti azioni di adeguamento.

La presente politica e le relative politiche di dettaglio sono riesaminate annualmente e, ove opportuno, aggiornate in caso di evoluzioni normative, incidenti significativi, variazioni organizzative o mutamenti dell'esposizione alle minacce e ai relativi rischi. Il riesame verifica almeno la conformità delle politiche alla normativa applicabile e i relativi esiti sono formalizzati in un registro aggiornato.

Gli interventi necessari a colmare gli scostamenti rilevati confluiscono in un piano di adeguamento unitario adottato dal Consiglio di Amministrazione, volto a individuare gli interventi necessari ad assicurare l'attuazione delle politiche e il rafforzamento delle misure di sicurezza.

L'Istituto definisce, attua, aggiorna e documenta inoltre un piano per la valutazione dell'efficacia delle misure di gestione del rischio per la sicurezza informatica. Gli organi di amministrazione e direttivi sono informati periodicamente sullo stato di attuazione e sugli esiti del Piano di Adeguamento e del Piano di Valutazione dell'Efficacia, inclusi gli scostamenti e le azioni correttive individuate.

Le risultanze delle attività svolte alimentano il miglioramento continuo della sicurezza informatica e il mantenimento della conformità agli obblighi applicabili.

5 Documenti attuativi

La presente Politica è attuata attraverso un insieme coordinato di documenti di carattere strategico con finalità di governo e di documenti di secondo livello, quali politiche di dettaglio, procedure, piani operativi, linee guida, istruzioni operative e registri, che disciplinano in modo puntuale gli ambiti di sicurezza richiamati nel presente documento. Tali documenti costituiscono il sistema attuativo della Politica e devono essere mantenuti coerenti con l'evoluzione del contesto organizzativo, tecnologico e normativo.

I documenti di carattere tecnico-operativo sono predisposti, adottati, riesaminati e aggiornati dalla Direzione Centrale Tecnologia, Informatica e Innovazione, assicurando tracciabilità delle versioni, disponibilità della documentazione vigente e accessibilità secondo criteri di pertinenza, necessità operativa e necessità di conoscere.

6 Comunicazione e riesame

La presente Politica costituisce il quadro di indirizzo per l'attuazione della sicurezza informatica nell'Istituto attraverso politiche di dettaglio, processi, procedure, linee guida, piani e controlli.

La Politica è comunicata e resa disponibile alle strutture organizzative, al personale e, ove applicabile, ai fornitori, ai partner e alle altre terze parti interessate, secondo criteri di pertinenza e necessità. La comunicazione avviene attraverso i canali previsti dal sistema documentale dell'Istituto.

Direzione Centrale Tecnologia, informatica e innovazione

Piano per la Gestione degli Incidenti di Sicurezza Informatica

Versione: 1.0

	Nominativo	Ruolo/Azienda	Data
Approvato da:	Valeria Vittimberga	Direttore Generale	
Verificato da:	Massimiliano D'Angelo	Direttore Centrale Tecnologia, Informatica e Innovazione	12-10-2026
Redatto da:	Area Cybersecurity	DCTII	12-10-2026
Indirizzo di Pubblicazione	Pagina intranet della DCTII		
Stato	approvato		
Classificato	uso interno		

Abstract

Il presente Piano definisce le modalità con cui l'Istituto indirizza la gestione della risposta agli incidenti di sicurezza che interessano la disponibilità, l'autenticità, l'integrità o la riservatezza delle informazioni, dei sistemi informativi e di rete e dei servizi. Il Piano disciplina l'intero ciclo di vita dell'incidente, dall'identificazione alla chiusura, inclusi il flusso di segnalazione ed escalation e la notifica alle Autorità competenti.

Storico delle Versioni		
Versione	**Data**	**Informazioni sull'aggiornamento**
V 1.0		Prima emissione del documento

Indice

1. Obiettivo 5
2. Definizioni, Abbreviazioni e Acronimi 6
3. Riferimenti 8
4. Principi generali per la gestione degli incidenti 9
5. Ciclo di vita dell'incidente 10
   5.1 Workflow 11
   5.2 Matrice RACI 12
6. Identificazione 13
   6.1 Analisi preliminare ed esiti 14
7. Classificazione 15
8. Notifica ed escalation 16
   8.1 Notifiche alle Autorità competenti 16
   8.2 Comunicazione verso i destinatari dei servizi e al pubblico 17
   8.3 Canali di comunicazione 18
9. Risposta 20
10. Ripristino 21
11. Chiusura, follow-up e miglioramento continuo 22
12. Raccordo con la continuità operativa 23
13. Reportistica e documentazione dell'incidente 24
14. Segnalazione degli incidenti di sicurezza 25
15. Comunicazione e riesame 26

Indice Tabelle

Tabella 1 - Definizioni, Abbreviazioni e Acronimi 7
Tabella 2 - Ciclo di vita dell'incidente 10
Tabella 3 - Legenda Workflow 11
Tabella 4 - Matrice RACI 12
Tabella 5 - Legenda Matrice RACI 12
Tabella 6 - Livelli e Criteri di classificazione degli incidenti di sicurezza 15
Tabella 7 - Obblighi di notifica alle Autorità competenti 17
Tabella 8 - Canali di comunicazione 19
Tabella 9 - Elementi minimi di registrazione dell'incidente 24

Indice Figure

Figura 1 - Workflow 11

1. Obiettivo

Il presente Piano ha l'obiettivo di definire il quadro complessivo di governo del processo di gestione degli incidenti di sicurezza dell'Istituto.

Si rimanda, per i processi e le procedure di dettaglio, alla documentazione predisposta e manutenuta dalla DCTII.

Ai fini del presente Piano, per **incidente di sicurezza** si intende un evento che compromette la disponibilità, l'autenticità, l'integrità o la riservatezza di dati o dei servizi offerti o accessibili attraverso i sistemi informativi e di rete. Il Piano si applica a tutti gli incidenti di sicurezza, indipendentemente dalla natura della minaccia che li ha generati - inclusi, a titolo esemplificativo, attacchi informatici, errori umani, guasti e malfunzionamenti, eventi di natura fisica - nella misura in cui essi compromettano o possano compromettere la sicurezza dei sistemi informativi e di rete, delle informazioni o dei servizi dell'Istituto.

Tutti i dipendenti INPS, i collaboratori, i fornitori e chiunque abbia un obbligo legale nel preservare le informazioni e gli asset dell'Istituto, sono tenuti a riferire qualsiasi evento di sicurezza.

2. Definizioni, Abbreviazioni e Acronimi

Termine/Abbreviazione	Definizione
ACN	Agenzia per la Cybersicurezza Nazionale.
Comitato di Coordinamento	Organo che assume le decisioni di indirizzo e coordinamento in occasione di incidenti di livello importante e valuta l'attivazione del Comitato di Crisi.
Comitato di Crisi	Organo che assume le decisioni di indirizzo e coordinamento in occasione di incidenti di livello grave.
CSIRT Italia	Struttura nazionale istituita presso l'Agenzia per la Cybersicurezza Nazionale, specializzata nella prevenzione, gestione e risposta agli incidenti di sicurezza informatica, nonché nel monitoraggio e nell'analisi di minacce, vulnerabilità e incidenti a livello nazionale.
CSIRT	Computer Security Incident Response Team.
Data Breach	Una violazione di sicurezza che comporta – accidentalmente o in modo illecito – la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.
Dato personale	Qualsiasi informazione riguardante una persona fisica identificata o identificabile; si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.
DPO/RPD	Data Protection Officer / Responsabile per la protezione dei dati personali.
Evento di sicurezza	Situazione relativa allo stato di un sistema, di un servizio, di una rete o di un ambiente che può indicare la compromissione, potenziale o in atto, della disponibilità, dell'autenticità, dell'integrità o della riservatezza delle informazioni o dei servizi, ovvero una possibile violazione dei criteri di sicurezza o un fallimento dei controlli.
Falso positivo	Evento rilevato o segnalato che, all'esito dell'analisi preliminare, non risulta configurare un evento di sicurezza.
Funzione responsabile della gestione dell'incidente	Funzione competente che assicura la conduzione dell'incidente lungo l'intero ciclo di vita, dalla presa in carico fino alla chiusura, indipendentemente da chi materialmente attua le singole attività.
Gestione degli incidenti di sicurezza	Le azioni e le procedure volte a prevenire, rilevare, analizzare, contenere e rispondere a un incidente e le azioni di ripristino.
GPDP	Garante per la Protezione dei Dati Personali

Incidente di sicurezza	Un evento che compromette la disponibilità, l'autenticità, l'integrità o la riservatezza di dati conservati, trasmessi o elaborati o dei servizi offerti dai sistemi informativi e di rete o accessibili attraverso di essi.
Incidente di sicurezza significativo	Un incidente è considerato significativo se: a) ha causato o è in grado di causare una grave perturbazione operativa dei servizi o perdite finanziarie per il soggetto interessato; b) ha avuto ripercussioni o è idoneo a provocare ripercussioni su altre persone fisiche o giuridiche causando perdite materiali o immateriali considerevoli.
Quasi-incidente (cd. near-miss)	Un evento che avrebbe potuto configurare un incidente senza che quest'ultimo si sia tuttavia verificato, ivi incluso il caso in cui l'incidente sia stato efficacemente evitato.
Lezioni apprese	Conoscenze acquisite dall'esperienza maturata nella gestione di un incidente, documentate e rese disponibili a fini di miglioramento.
Referente CSIRT	Figura designata dall'Istituto ai sensi del D.lgs. 138/2024, che cura la predisposizione e la trasmissione delle pre-notifiche, delle notifiche e delle relazioni al CSIRT Italia.

Tabella 1 - Definizioni, Abbreviazioni e Acronimi

3. Riferimenti

Per i riferimenti normativi si rimanda al documento "INPS-SGI-GEN-Requisiti Legali e Regolamentari", redatto e mantenuto dalla Direzione Centrale Tecnologia, Informatica e Innovazione (DCTII) nell'ambito del Sistema di Gestione Integrato certificato ISO.

Di seguito si riportano i riferimenti interni specifici del presente documento:

- Politica di Sicurezza Informatica;
- Organizzazione per la sicurezza informatica.

Per quanto riguarda i riferimenti esterni, si evidenziano le "Linee Guida NIS - Specifiche di base - Definizione del processo di gestione degli incidenti di sicurezza informatica" emanate dall'Agenzia per la Cybersicurezza Nazionale.

4. Principi generali per la gestione degli incidenti

La gestione degli incidenti di sicurezza dell'Istituto si ispira ai seguenti principi:

- **tempestività:** gli incidenti sono rilevati, presi in carico e gestiti nel minor tempo possibile, al fine di contenerne gli impatti;
- **tracciabilità:** tutte le attività di gestione dell'incidente sono documentate e tracciate;
- **miglioramento continuo:** le lezioni apprese dalla gestione degli incidenti alimentano il rafforzamento delle capacità di prevenzione, risposta e resilienza.

5. Ciclo di vita dell'incidente

Il processo di gestione degli incidenti di sicurezza si articola nelle fasi di seguito riportate.

Fase	Finalità
0. Preparazione	Precede il verificarsi di un incidente e costituisce la base per una risposta efficace agli incidenti di sicurezza; include le attività di governo, identificazione (del contesto) e protezione.
1. Identificazione	Rilevazione e presa in carico degli eventi di sicurezza, da fonti interne, esterne e di monitoraggio, e accertamento della loro natura di incidente.
2. Classificazione	Analisi, caratterizzazione e attribuzione del livello di gravità dell'incidente, nonché valutazione della sua significatività ai fini degli obblighi di notifica.
3. Notifica & Escalation	Comunicazione interna, escalation e, ove dovuta, notifica alle Autorità competenti.
4. Risposta	Definizione e attuazione delle strategie di contenimento e risposta.
5. Ripristino	Ripristino del normale funzionamento dei sistemi e dei servizi coinvolti e comunicazione dello stato di ripristino.
6. Chiusura, follow-up e miglioramento continuo	Analisi a posteriori dell'incidente, individuazione delle lezioni apprese e delle azioni di miglioramento.

Tabella 2 - Ciclo di vita dell'incidente

Per un'efficace ed efficiente gestione degli incidenti di sicurezza, è prevista una fase di Preparazione che si articola in un complesso di attività di governo, identificazione e protezione. Tra queste attività troviamo ad esempio la redazione di playbook, l'Identificazione del contesto (l'inventario dei sistemi informativi e di rete e l'individuazione di minacce e vulnerabilità), la Protezione degli asset, per le quali si rimanda alla specifica documentazione predisposta e manutenuta nell'ambito delle articolazioni competenti.

5.1 Workflow

Si riporta una rappresentazione grafica delle attività che compongono il processo. I simboli utilizzati nel flow-chart, con una breve descrizione degli stessi, sono illustrati nella seguente tabella:

Simbolo	Significato	Simbolo	Significato
	Inizio / Fine Processo		Attività
	Snodo decisionale		Direzione del flusso di processo
	Rimando ad altro processo	-	-

Tabella 3 - Legenda Workflow

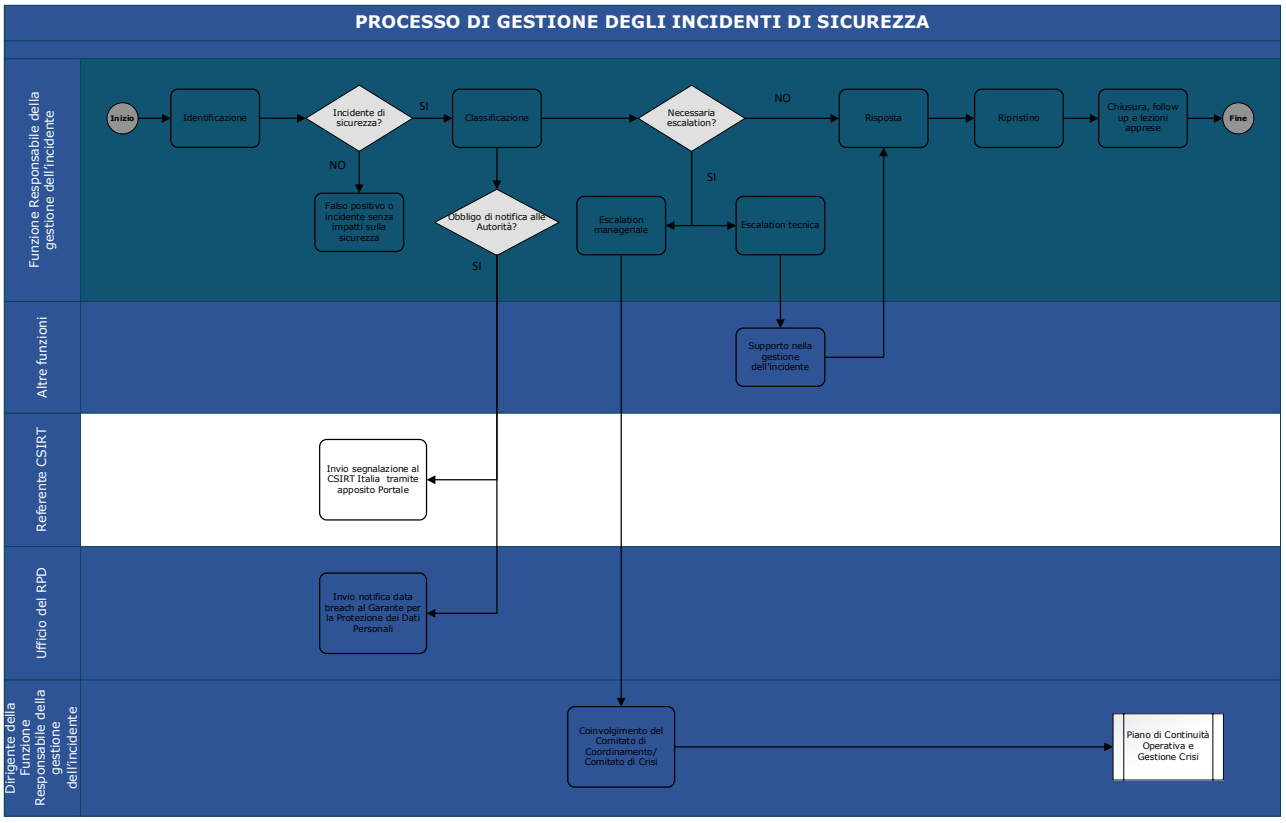


Figura 1 - Workflow

5.2 Matrice RACI

Attività	F. responsabile della Gestione dell' Incidente	Altre funzioni	Dirigente della Funzione Responsabile	Referente CSIRT	Ufficio RPD	Direzione Centrale Comunicazione
Identificazione	A/R	-	-	-	-	-
Classificazione	A/R	-	-	**-**	-	-
Escalation tecnica/manageriale	A/R	-	-	-	-	-
Supporto nella gestione dell'incidente	A	R	-	-	-	-
Notifica al CSIRT Italia	C	-	I	A/R	-	-
Notifica al GPDP	C	-	I	-	A/R	-
Comunicazioni al pubblico e ai destinatari dei servizi	C	-	C	C	C	A/R
Risposta	A/R	-	-	-	-	-
Ripristino	A/R	-	-	-	-	-
Chiusura, follow up e miglioramento continuo	A/R	-	-	-	-	-

Tabella 4 - Matrice RACI

Legenda matrice RACI	
R – **Esegue** l'attività	**C** – È **consultato** durante lo svolgimento dell'attività
A – È **responsabile** del risultato e dell'approvazione dell'attività	**I –** È **informato** sull'attività

Tabella 5 - Legenda Matrice RACI

6. Identificazione

Rappresenta la fase in cui gli eventi di sicurezza sono rilevati, presi in carico e analizzati al fine di accertarne la natura di incidente, assicurando che nessuna segnalazione sia trascurata e che gli incidenti siano individuati tempestivamente.

L'identificazione degli eventi di sicurezza si fonda sui presidi di monitoraggio adottati dall'Istituto, sulle segnalazioni provenienti da fonti interne ed esterne (vd. par. 14), nonché sui processi di natura predittiva finalizzati all'individuazione anticipata di minacce e vulnerabilità.

Eventi rilevati dai presidi di monitoraggio e di rilevazione

Costituiscono fonti di rilevazione diretta:

- il monitoraggio continuo dei sistemi informativi e di rete e dei relativi eventi di sicurezza, mediante strumenti finalizzati alla rilevazione di anomalie, condizioni di rischio e potenziali incidenti;
- l'analisi delle registrazioni di log generate da applicazioni, sistemi, apparati di rete e dispositivi, finalizzata all'individuazione di eventi di sicurezza, comportamenti anomali, accessi non autorizzati e altri elementi rilevanti ai fini dell'identificazione degli incidenti;
- i presidi di sicurezza fisica e ambientale, mediante sistemi e impianti di rilevazione e mediante il personale di vigilanza, per eventi che possano ripercuotersi sulla sicurezza dei sistemi, delle informazioni o dei servizi.

Gli eventi rilevati da tali presidi sono presi in carico dalla funzione che ne cura l'esercizio, la quale procede all'analisi preliminare. Resta ferma l'attivazione delle misure di primo intervento previste per l'ambito interessato.

Eventi segnalati da personale, collaboratori e fornitori

Il personale dipendente, i collaboratori e i fornitori sono tenuti a segnalare tempestivamente gli eventi sospetti o i potenziali incidenti di cui vengano a conoscenza, utilizzando i canali di cui al capitolo "Segnalazione degli incidenti di sicurezza". Le segnalazioni provenienti da soggetti privi di competenza tecnica sull'ambito interessato sono instradate alla funzione competente in ragione della natura dell'evento, che ne assume la presa in carico.

Comunicazioni da fonti esterne

Le comunicazioni provenienti dalle Autorità competenti e da altre fonti esterne, ivi incluse le segnalazioni relative a potenziali violazioni di dati personali, sono sottoposte

a una verifica preliminare di pertinenza rispetto ai sistemi, ai servizi e alle informazioni dell'Istituto, al fine di accertare se l'evento segnalato abbia riscontro nel proprio ambito. Accertata la pertinenza, l'evento è preso in carico dalla funzione competente e trattato secondo quanto previsto nel presente capitolo.

6.1 Analisi preliminare ed esiti

L'evento, preso in carico dalla funzione competente in ragione della natura dell'evento, è oggetto di un'analisi preliminare volta a valutarne l'attendibilità e i possibili impatti. All'esito di tale analisi, l'evento può essere:

- chiuso, qualora risulti un falso positivo, dandone comunque evidenza ai fini della tracciabilità;
- gestito nell'ambito dei processi ordinari di gestione dei malfunzionamenti e dei disservizi, qualora non presenti implicazioni per la sicurezza delle informazioni, dei sistemi e dei servizi;
- qualificato come incidente di sicurezza, con conseguente attivazione delle fasi successive. In tal caso, la funzione che ha assunto la presa in carico assume anche il ruolo di Funzione responsabile della gestione dell'incidente, assicurandone la conduzione lungo l'intero ciclo di vita fino alla chiusura, ovvero, ove la natura dell'incidente lo richieda, tale ruolo è attribuito alla funzione competente per l'ambito interessato.

Gli eventi presi in carico sono registrati a cura della Funzione responsabile della gestione dell'incidente, con l'indicazione della fonte, della data e dell'ora della rilevazione ovvero della ricezione della segnalazione, e degli elementi descrittivi disponibili, assicurandone la tracciabilità sin dal momento della presa in carico.

7. Classificazione

Ogni incidente di sicurezza è classificato dalla Funzione responsabile della gestione dell'incidente secondo un livello di gravità determinato sulla base della valutazione complessiva degli impatti effettivi o potenziali prodotti sull'operatività dell'Istituto. A tal fine sono considerati, ove applicabile, la rilevanza dei sistemi, il numero di servizi coinvolti, l'entità e la durata dell'indisponibilità, la compromissione della disponibilità, dell'integrità, dell'autenticità o della riservatezza delle informazioni, nonché gli eventuali impatti verso soggetti esterni. Il livello di gravità orienta i livelli di escalation.

Di seguito è rappresentata una tabella con i livelli di classificazione e le relative figure coinvolte.

Classificazione Incidente	Figure coinvolte	Descrizione
Lieve	• Funzione responsabile della gestione dell'incidente	Incidenti che coinvolgono l'Istituto soltanto internamente. Possono creare disagi limitati ad uno o più utenti senza coinvolgere l'erogazione dei servizi. L'impatto economico è trascurabile e l'incidente non comporta una compromissione di dati e sistemi. Non si può escludere un danno d'immagine, anche se limitato all'interno dell'ente stesso.
Importante	• Funzione responsabile della gestione dell'incidente • Comitato di Coordinamento • Comitato di Crisi (eventuale)	Incidenti dall'impatto limitato ma che possono comportare ripercussioni anche sull'erogazione dei servizi. L'impatto economico è limitato, ma può esserci una compromissione di dati e sistemi. Può essere presente un eventuale danno d'immagine che coinvolge altre entità e soggetti privati.
Grave	• Funzione responsabile della gestione dell'incidente • Comitato di Coordinamento • Comitato di Crisi • Organi di Amministrazione e Direttivi	Incidente con conseguenze molto rilevanti sull'erogazione di servizi. L'impatto economico può essere significativo. È presente una compromissione di dati e sistemi che può anche causare un sensibile arresto dell'operatività internamente ed esternamente verso altre entità e soggetti privati. È presente un danno d'immagine che può coinvolgere altre entità e soggetti privati.

Tabella 6 - Livelli e Criteri di classificazione degli incidenti di sicurezza

8. Notifica ed escalation

Rappresenta la fase in cui sono attivati i flussi di comunicazione, notifica ed escalation previsti in funzione della natura e della gravità dell'incidente, assicurando il coinvolgimento dei soggetti competenti e l'assolvimento degli eventuali obblighi di comunicazione e notifica applicabili.

Le possibili attività di notifica ed escalation verso altre strutture/funzioni si distinguono nelle seguenti due tipologie:

- **Escalation tecnica**: è attivata qualora, per la gestione dell'incidente, sia necessario, alla luce del principio del *need to know*, il coinvolgimento o il supporto di ulteriori funzioni competenti, in ragione delle conoscenze specialistiche, delle competenze tecniche o delle responsabilità decisionali richieste.
- **Escalation Manageriale**: escalation nei confronti del Dirigente della Funzione responsabile della gestione dell'incidente. Tale tipologia di escalation avviene nel caso in cui l'incidente è di tipologia "importante" o "grave". In tal caso, il Dirigente della Funzione responsabile della gestione dell'incidente coinvolge il Comitato di Coordinamento, che effettua le dovute valutazioni e, se ritenuto necessario, coinvolge il Comitato di Crisi.

8.1 Notifiche alle Autorità competenti

L'Istituto è soggetto a una pluralità di regimi in materia di notifica degli incidenti di sicurezza alle Autorità competenti, i cui obblighi possono coesistere sul medesimo incidente.

La Funzione responsabile della gestione dell'incidente valuta la potenziale rilevanza dell'incidente ai fini degli obblighi di notifica, tenendo conto delle caratteristiche dell'evento e dei criteri previsti dalla normativa applicabile.

Qualora emerga la possibile sussistenza di obblighi di notifica al CSIRT Italia, la Funzione responsabile della gestione dell'incidente coinvolge il Referente CSIRT, fornendo le informazioni necessarie per le valutazioni di competenza.

Ove accertata la sussistenza di uno o più di tali obblighi, le notifiche sono trasmesse dal Referente CSIRT mediante il portale unico di notifica dell'ACN, secondo i criteri e le tempistiche riepilogati dalla normativa applicabile.

Qualora l'incidente comporti o possa comportare una violazione di dati personali, è coinvolto anche l'Ufficio del Responsabile della Protezione dei Dati, ai fini delle valutazioni e degli adempimenti previsti dalla normativa in materia di protezione dei dati personali. La Funzione responsabile della gestione dell'incidente assicura la collaborazione e la trasmissione delle informazioni necessarie.

Restano ferme le competenze dei soggetti individuati dalla disciplina interna dell'Istituto per la segnalazione delle violazioni di dati personali al Responsabile della Protezione dei Dati.

La presente tabella riepiloga i principali obblighi normativi di segnalazione e notifica degli incidenti cyber applicabili all'Istituto. Ulteriori obblighi comunicativi possono derivare da disposizioni normative specifiche, provvedimenti delle Autorità competenti, accordi convenzionali o previsioni contrattuali.

Normativa	Criteri di attivazione dell'obbligo di notifica	Tempistiche di segnalazione e notifica (decorrenti dalla conoscenza dell'evento)
NIS2 (D.lgs. 138/2024)	Incidente significativo secondo le tipologie di incidente significativo di base (Allegato 4 della determinazione ACN 379907/2025).	Pre-notifica entro 24 ore Notifica entro 72 ore; Relazione finale entro 1 mese.
Legge 90/2024	Incidenti riconducibili alla tassonomia adottata con determina ACN n° 28900 del 9 febbraio 2026. Per l'Istituto, soggetto anche al decreto NIS, l'obbligo è assolto tramite la notifica NIS mediante il portale unico ACN.	Si applicano le tempistiche previste per la NIS2
PSNC *DPCM 81/2021*	Incidenti su beni ICT inclusi nel Perimetro di Sicurezza Nazionale Cibernetica.	Notifica entro: - 1 ora, bene ICT (o contiguo) classe ICP-B; - 6 ore, bene ICT (o contiguo) classe ICP–A; - 24 ore, diverso da bene ICT, classe ICP-C.
GDPR Regolamento (UE) 2016/679	Incidenti di sicurezza con impatto su dati personali che possono avere effetti avversi significativi sugli individui, causando danni fisici, materiali o immateriali.	Notifica entro 72 ore (art. 33 GDPR).

Tabella 7 - Obblighi di notifica alle Autorità competenti

8.2 Comunicazione verso i destinatari dei servizi e al pubblico

Ove ritenuto opportuno dall'Istituto e, ove applicabile, qualora richiesto o intimato dall'Autorità competente, l'Istituto provvede, senza ingiustificato ritardo, alle comunicazioni verso l'esterno connesse all'incidente.

Tali comunicazioni sono gestite dalla Direzione Centrale Comunicazione, attivata dalla DCTII e, nei casi che coinvolgano dati personali, con il coinvolgimento dell'Ufficio del Responsabile della Protezione dei Dati, e comprendono:

• la comunicazione ai destinatari dei servizi degli incidenti che possono ripercuotersi sulla fornitura dei servizi, nonché, ai destinatari potenzialmente interessati da una minaccia informatica significativa, della natura della minaccia e delle misure di mitigazione adottabili;

• l'informazione al pubblico sugli incidenti occorsi, qualora intimato dall'Autorità, secondo le modalità e i contenuti indicati dalla stessa.

Le comunicazioni sono conservate come evidenza della gestione dell'incidente.

8.3 Canali di comunicazione

Le comunicazioni interne sono finalizzate a garantire il tempestivo allineamento delle strutture coinvolte e del personale interessato, favorendo la condivisione delle informazioni necessarie alla gestione dell'evento e il coordinamento delle azioni intraprese.

Le comunicazioni esterne e istituzionali sono gestite nel rispetto delle competenze attribuite alle strutture organizzative dell'Istituto; in particolare, per gli aspetti di informazione e comunicazione verso l'esterno, opera la Direzione Centrale Comunicazione.

In relazione alla natura dell'evento e ai soggetti coinvolti, l'Istituto può avvalersi dei seguenti canali di comunicazione, da utilizzare singolarmente o in combinazione, al fine di assicurare tempestività, tracciabilità e coerenza dei flussi informativi.

Canale di comunicazione	Interno/esterno	Regole di utilizzo
Posta elettronica istituzionale	Interno	Utilizzata per comunicazioni operative e informative tra le strutture coinvolte. Le informazioni riservate, le evidenze e gli eventuali allegati contenenti dati sensibili sono trasmessi esclusivamente adottando le misure di protezione previste dalle politiche dell'Istituto. Non è utilizzata qualora vi siano elementi per ritenere compromesso il servizio di posta elettronica.
Piattaforme di collaborazione e videoconferenza	Interno	Utilizzate per il coordinamento delle attività e la condivisione delle informazioni tra soggetti autorizzati. L'accesso è limitato ai partecipanti necessari e le sessioni, le registrazioni e i documenti condivisi sono gestiti secondo il principio della necessità di conoscere.
Intranet aziendale	Interno	Utilizzata per la diffusione di comunicazioni informative rivolte al personale o a specifiche articolazioni organizzative. Non è utilizzata per la pubblicazione di dettagli tecnici, evidenze o informazioni riservate relative all'incidente, salvo che siano

		previste apposite aree ad accesso controllato.
Riunioni e sale di crisi "war room"	Interno	Utilizzate per il coordinamento degli incidenti importanti o gravi. La partecipazione è limitata ai soggetti coinvolti nella gestione e le informazioni condivise sono trattate secondo il principio della necessità di conoscere.
Canali telefonici istituzionali	Interno	Utilizzati per comunicazioni urgenti e per l'attivazione tempestiva delle strutture interessate. Le informazioni riservate o di dettaglio sono successivamente condivise e tracciate attraverso un canale istituzionale adeguatamente protetto.
Portale istituzionale Internet	Esterno	Utilizzato esclusivamente per la pubblicazione delle comunicazioni approvate e destinate al pubblico. Non è utilizzato per lo scambio di informazioni operative o riservate relative all'incidente.
PEC e posta elettronica	Esterno	Utilizzate per le comunicazioni formali verso soggetti esterni, secondo le competenze delle strutture coinvolte. La trasmissione di informazioni riservate o contenenti dati personali avviene adottando le misure di protezione previste dall'Istituto.
Portali e strumenti istituzionali previsti per le comunicazioni verso le Autorità competenti.	Esterno	Utilizzati per la trasmissione di notifiche, segnalazioni, comunicazioni e relazioni verso le Autorità competenti secondo le modalità previste dalla normativa applicabile.

Tabella 8 - Canali di comunicazione

In linea generale, sono sempre privilegiati canali e strumenti di comunicazione istituzionali protetti, in grado di garantire adeguati livelli di riservatezza, integrità, autenticità e disponibilità delle informazioni scambiate, in coerenza con le politiche di sicurezza dell'Istituto e sulla base delle esigenze di sicurezza associate ai servizi coinvolti. La scelta dei canali e degli strumenti di comunicazione è effettuata tenendo conto della natura dell'evento, dei soggetti coinvolti, del livello di criticità e delle eventuali esigenze di continuità delle comunicazioni anche in condizioni di indisponibilità parziale delle infrastrutture ordinarie.

9. Risposta

Rappresenta la fase in cui sono definite e attuate le strategie di contenimento più appropriate, in funzione della natura e della gravità dell'incidente. Le strategie sono definite dalla Funzione responsabile della gestione dell'incidente, con il coinvolgimento delle figure previste in ragione del livello di gravità dell'incidente.

I criteri per la determinazione della corretta strategia di contenimento sono:

- potenziali danni o perdite di risorse;
- necessità di preservare le evidenze;
- impatto sulla disponibilità del servizio;
- tempo e risorse da impiegare per porre in atto la strategia;
- effetto atteso della strategia (risoluzione totale, risoluzione parziale ecc.);
- durata della soluzione prodotta.

A livello operativo, la Funzione responsabile della gestione dell'incidente:

- definisce le strategie di contenimento più appropriate e, ove applicabile, le eventuali azioni per raccogliere le tracce dell'avvenuta violazione;
- attua le azioni di contenimento, avvalendosi ove necessario delle altre funzioni competenti;
- monitora le operazioni di contenimento dell'incidente.

In tutti i casi, la Funzione responsabile della gestione dell'incidente provvede al monitoraggio delle fasi di gestione e contenimento dell'incidente, registrandone i cambiamenti di stato, annotando i dettagli delle comunicazioni avvenute e tracciando le attività svolte, accompagnando formalmente la fase di risposta alla successiva fase di ripristino.

10. Ripristino

Dopo che l'incidente è stato contenuto e ricondotto sotto il pieno controllo dell'organizzazione, sono adottate tutte le misure tecniche e organizzative necessarie a ripristinare la piena funzionalità dei sistemi, dei servizi e degli ambienti coinvolti, riportandoli al livello di sicurezza atteso.

Per azioni di ripristino si intendono tutte le attività che hanno come obiettivo:

- l'eliminazione delle componenti residue dell'incidente occorso e delle relative cause;
- il ripristino dei sistemi, dei dati, delle configurazioni e degli ambienti interessati, anche mediante il recupero da copie di backup ovvero mediante gli interventi di ripristino previsti per l'ambito interessato;
- l'adozione di eventuali azioni di miglioramento attuabili, al fine di ridurre il rischio futuro di incidenti analoghi.

L'identificazione e l'attuazione delle strategie di ripristino sono a cura della Funzione responsabile della gestione dell'incidente, che si avvale ove necessario delle altre funzioni competenti già coinvolte nelle fasi precedenti.

In questa fase e in quella successiva è assicurata la conservazione delle evidenze raccolte, secondo le modalità appropriate alla natura dell'incidente, al fine di salvaguardarne l'integrità anche a fini investigativi o legali.

La Funzione responsabile della gestione dell'incidente monitora e registra lo stato di avanzamento delle operazioni di ripristino e ne comunica l'esito alle strutture interessate, dando evidenza delle eventuali misure temporanee ancora in vigore e delle attività di monitoraggio successive alla chiusura dell'incidente.

11. Chiusura, follow-up e miglioramento continuo

Completate le attività di ripristino e verificato il ritorno alle condizioni di normale funzionamento, la Funzione responsabile della gestione dell'incidente ne dispone la chiusura, dandone evidenza nella registrazione dell'incidente unitamente all'esito finale e alla data di chiusura.

Almeno per gli incidenti di maggiore rilevanza è svolta un'analisi a posteriori volta a esaminare la dinamica dell'evento, stabilirne le cause, le modalità e le conseguenze, nonché a valutare l'efficacia della gestione. Gli esiti dell'analisi sono formalizzati dalla Funzione responsabile della gestione dell'incidente in una relazione, redatta di norma entro quindici giorni dalla risoluzione dell'incidente, che riporta almeno:

- la cronologia degli eventi e le modalità con cui l'incidente è stato rilevato;
- i sistemi, i servizi e gli utenti impattati;
- l'analisi svolta e le evidenze raccolte, ivi inclusa l'individuazione delle cause;
- le soluzioni temporanee adottate e la soluzione definitiva attuata;
- la valutazione di quanto ha funzionato e delle criticità emerse sul piano tecnico, procedurale e di comunicazione;
- le azioni migliorative e di consolidamento individuate.

Le conoscenze acquisite sono raccolte come lezioni apprese nei report finali degli incidenti e rese disponibili alle strutture coinvolte nella gestione degli incidenti, al fine di prevenirne il ripetersi, migliorarne la rilevazione preventiva e ridurne gli effetti. Le lezioni apprese e le azioni di miglioramento alimentano il riesame del presente Piano.

12. Raccordo con la continuità operativa

Qualora un incidente sia classificato come importante o grave, ovvero abbia determinato o possa determinare impatti sulla disponibilità dei servizi erogati, si applicano i livelli di escalation previsti dal presente Piano.

In tale ambito, il Comitato di Coordinamento, ingaggiato dal Dirigente della Funzione Responsabile della gestione dell'incidente, effettua le dovute valutazioni e, se necessario, coinvolge il Comitato di Crisi, secondo quanto previsto dalla documentazione di continuità operativa e gestione della crisi adottata dall'Istituto.

13. Reportistica e documentazione dell'incidente

La tracciatura delle attività di gestione dell'incidente è effettuata dalla Funzione responsabile della gestione dell'incidente mediante gli strumenti in uso in ragione della natura dell'incidente. Indipendentemente dallo strumento utilizzato, la documentazione è mantenuta secondo criteri omogenei, a garanzia dell'uniformità, della completezza e della tracciabilità delle informazioni.

Per ciascun incidente è mantenuta una registrazione che riporta, a titolo esemplificativo e non esaustivo, i seguenti elementi:

Elementi identificativi e descrittivi	Elementi di gestione ed esito
• identificativo univoco dell'incidente • soggetto o fonte segnalante • data e ora della segnalazione e della rilevazione • area, servizio e componenti interessati • descrizione dell'evento e dei sintomi rilevati • origine e natura dell'incidente	• livello di gravità e priorità attribuiti • valutazione di significatività ai fini di notifica • struttura o funzione assegnataria • stato di avanzamento della gestione • azioni di contenimento, risposta e ripristino attuate • esito finale e data di chiusura

Tabella 9 - Elementi minimi di registrazione dell'incidente

La registrazione è aggiornata lungo l'intero ciclo di vita dell'incidente, dando evidenza dei cambiamenti di stato, delle comunicazioni intercorse e delle attività svolte. Il livello di dettaglio della documentazione è proporzionato alla gravità e alla rilevanza dell'incidente.

La documentazione dell'incidente supporta l'analisi a posteriori, l'adempimento degli obblighi di notifica e il processo di miglioramento continuo.

14. Segnalazione degli incidenti di sicurezza

I canali di segnalazione sono individuati in funzione della natura dell'evento e dell'ambito interessato:

- per gli eventi e gli incidenti informatici, la Direzione Centrale Tecnologia Informatica e Innovazione provvede con proprie risorse e canali di comunicazione a raccogliere le segnalazioni in un unico collettore, registrarle e gestirle nell'ambito delle proprie articolazioni in funzione delle procedure interne e dei processi di escalation;
- per gli eventi di natura ambientale o impiantistica, il personale addetto al monitoraggio della sensoristica presso la DG e, ove presente, presso le sedi è preposto alla raccolta e alla trattazione delle segnalazioni secondo le procedure interne indirizzate dal Coordinamento Generale Tecnico Edilizio. Ove l'evento possa avere un potenziale impatto sull'infrastruttura informatica o sull'erogazione dei servizi, la segnalazione viene prontamente inoltrata alla Direzione Centrale Tecnologia, Informatica e Innovazione che la gestisce per quanto di competenza;
- per gli eventi di sicurezza fisica, i presidi di guardiania e vigilanza sono preposti alla raccolta e alla trattazione delle violazioni secondo le procedure interne indirizzate dalla Direzione Centrale Risorse Strumentali e Centrale Unica Acquisti. Ove l'evento possa avere un potenziale impatto sull'infrastruttura informatica o sull'erogazione dei servizi, la segnalazione viene prontamente inoltrata alla Direzione Centrale Tecnologia, Informatica e Innovazione che la gestisce per quanto di competenza;
- la presunta violazione di dati personali riscontrata da qualunque soggetto, ove pervenga a canali diversi dal Responsabile della Protezione dei Dati personali, deve ad esso essere ricondotta con tempestività e completezza di informazioni circa l'evento riscontrato.

Indipendentemente dal canale utilizzato, il destinatario iniziale assicura l'instradamento della segnalazione alla funzione competente e la continuità della presa in carico fino alla corretta assegnazione.

15. Comunicazione e riesame

Il presente Piano è comunicato e reso disponibile alle strutture dell'Istituto e ai soggetti coinvolti nel processo di gestione degli incidenti, secondo criteri di pertinenza e necessità di conoscere. Il Piano è riesaminato e, se opportuno, aggiornato periodicamente e comunque almeno ogni due anni, nonché qualora si verifichino incidenti significativi, integrando le relative lezioni apprese. Gli esiti del riesame e le eventuali proposte di aggiornamento sono formalizzati e documentati.