Ministero della Salute

DIREZIONE GENERALE DELLE RISORSE UMANE E DEL BILANCIO
Ufficio 1 – Affari generali, organizzazione e relazioni sindacali

ACCORDO IN MATERIA DI SISTEMI DI POSTA ELETTRONICA, DI ACCOUNT MICROSOFT 365 E DEL SERVIZIO DI NAVIGAZIONE IN INTERNET

In data _____, alle ore _____, in Roma, viale Giorgio Ribotta n. 5, nella stanza R303, si riuniscono le Parti sindacali e le Parti pubbliche, come di seguito rappresentate, ai sensi e per gli effetti dell'art. 4 della legge n. 300/1970 e della disciplina in materia di trattamento dei dati, per la stipula dell'accordo in materia di funzionamento del sistema di posta elettronica, dell'account Microsoft 365 e del servizio di navigazione in Internet del Ministero, nel rispetto delle garanzie previste a tutela dei diritti dei lavoratori.

VISTO

- la legge 20 maggio 1970, n. 300, recante "Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale, nei luoghi di lavoro e norme sul collocamento" e s.m.i., in particolare l'art. 4, rubricato "Impianti audiovisivi e altri strumenti di controllo";
- il decreto legislativo 7 marzo 2005, n. 82, recante "Codice dell'amministrazione digitale" e s.m.i.;
- il decreto legislativo 30 giugno 2003, n. 196, recante "Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE" e s.m.i.;
- il Regolamento UE 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, recante "Regolamento generale sulla protezione dei dati";
- il Provvedimento del Garante per la protezione dei dati personali del 6 giugno 2024, recante "Documento di indirizzo. Programmi e servizi informatici di gestione della posta elettronica nel contesto lavorativo e trattamento dei metadati", in particolare il paragrafo 3 relativo alla disciplina di settore in materia di controlli a distanza;

CONSIDERATO CHE

- che il Ministero della salute gestisce dati e informazioni a carattere riservato, anche relativi alla salute pubblica, alla sicurezza sanitaria e alle attività di coordinamento nazionale in materia di prevenzione e tratta quotidianamente dati particolari, riservati e critici, il cui accesso non autorizzato, alterazione o indisponibilità potrebbe determinare gravi impatti negativi sulla tutela della salute pubblica e individuale, sulla continuità operativa delle funzioni istituzionali, sulla fiducia dei cittadini e degli stakeholders nei confronti dell'Amministrazione, nonché potenziali violazioni della normativa in materia di protezione dei dati personali e sicurezza delle informazioni;
- che il Ministero della salute, per lo svolgimento delle proprie attività istituzionali, all'interno di un processo di digitalizzazione dei processi della pubblica amministrazione:
  - assegna ai dipendenti, sulla base di provvedimenti periodicamente aggiornati, attrezzature,

strumenti informatici e servizi infotelematici e, in particolare, fornisce a tutto il personale almeno un personal computer, un account Microsoft, una casella di posta elettronica aziendale nominativa, l'accesso alla rete interna/Intranet e alla rete Internet, nonché a seconda delle mansioni svolte dal dipendente, ulteriori strumentazioni e servizi e l'accesso a programmi, servizi e banche dati ICT, in base al ruolo ricoperto nell'organizzazione e necessari per lo svolgimento delle attività assegnate (di seguito complessivamente indicati come Strumenti e servizi infotelematici);
- gestisce gli Strumenti e servizi infotelematici anche tramite contratti con operatori economici qualificati, tra cui INAIL, Microsoft, Accenture e Avanade;
- tali Strumenti e servizi infotelematici generano, anche in via automatica, log tecnici per la funzionalità o log di sicurezza per la salvaguardia dei sistemi informativi;

- che l'uso degli Strumenti e servizi infotelematici è consentito secondo quanto previsto dalla disciplina vigente in materia di protezione dei dati personali e di sicurezza informatica, nonché dai provvedimenti e linee guida del Garante per la protezione dei dati personali e dell'Agenzia per la Cybersicurezza Nazionale;
- che l'utilizzo dei suddetti Strumenti e servizi infotelematici, pur obbligatorio e indispensabile, necessità di azioni e interventi a presidio della cyber sicurezza e della riservatezza;
- che tali azioni sono necessarie e obbligatorie, in quanto imposte dalla digitalizzazione in analogia con gli accessi fisici alla sede di lavoro e che a tal fine il Ministero della salute si è dotato di un Disciplinare interno per l'uso degli strumenti e servizi informatici, periodicamente aggiornato e pubblicato nella Intranet nella sezione "Infrastruttura ICT";
- che per il medesimo fine il Ministero si è, altresì, dotato di ulteriori documenti tecnici contenenti i criteri e le regole relative al corretto utilizzo degli Strumenti/servizi ICT nell'Amministrazione, nonché le misure e le procedure atte a garantire la sicurezza ed il corretto funzionamento del sistema informatico del Ministero, anche con l'eventuale monitoraggio e controllo dei metadati o log tecnici, generati automaticamente dai relativi strumenti o servizi utilizzati, volti a:
  a) garantire la sicurezza informatica, ad esempio individuando eventuali agenti automatici malevoli (virus, worm, trojan, ecc..) presenti nella rete interna dell'Amministrazione o prevenendo potenziali minacce informatiche (siti di phishing, truffe informatiche, ecc.);
  b) riscontrare le richieste dell'Autorità Giudiziaria;
  c) assicurare la risoluzione di problemi tecnici;
  d) identificare situazioni anomale;
  e) monitorare il funzionamento e le prestazioni dei servizi informatici;
  f) per eseguire analisi statistiche in forma aggregata ed anonima;
- tali attività sono effettuate esclusivamente per finalità di sicurezza informatica e di corretto funzionamento dei sistemi informativi e non comportano analisi individuali dell'attività lavorativa del personale;
- che tali disposizioni possono essere modificate dall'Amministrazione in base alle mutate esigenze organizzative e sono pubblicate nella citata sezione della Intranet, a disposizione di tutto il personale;
- che tali dati di log e metadati possono configurarsi come dati personali riguardanti lavoratori, identificati o identificabili, il cui trattamento è necessario e obbligatorio per le finalità sopra descritte, nonché per il corretto funzionamento dei sistemi informatici e per consentire al dipendente l'erogazione della prestazione lavorativa;
- che in base all'articolo 4 della legge 20 maggio 1970, n. 300, concernente il c.d. "*Statuto dei lavoratori"*, è consentito l'impiego del sistema volto a garantire l'integrità del patrimonio informativo e la sicurezza informatica, nonché il corretto funzionamento tecnico-informatico del servizio di posta elettronica e nonché la sua integrità e sicurezza;
- che il Ministero della salute assicura che mediante i suddetti Strumenti e servizi infotelematici non sono svolti controlli preordinati alla verifica dell'osservanza dei doveri di diligenza stabiliti

per il rispetto dell'orario di lavoro (esclusi i sistemi di rilevamento delle presenze) e la correttezza della prestazione lavorativa;

- che il trattamento dei dati di monitoraggio automatico è svolto solo da soggetti preposti (Amministratori di sistema, autorizzati al trattamento, e dipendenti del Fornitore dei servizi, formalmente designato quale responsabile del trattamento del Ministero della salute), tenendo conto della normativa sulla protezione dei dati e, se pertinente, del principio di segretezza della corrispondenza, essendo, peraltro, escluso un controllo diretto del contenuto della posta elettronica da parte degli Amministratori di sistema e degli altri incaricati del trattamento;
- che per le richiamate finalità e in considerazione delle caratteristiche non modificabili degli Strumenti e dei servizi infotelematici l'Amministrazione conserva i relativi metadati e dati di log per un periodo pari a 90 giorni;
- partecipa alle riunioni il direttore generale dell'UMPNRR in qualità di Titolare del trattamento dei dati per il servizio di navigazione in Internet e il Responsabile della Protezione dei Dati;

Tutto ciò premesso, le parti

CONVENGONO CHE

- il Ministero della salute ha comunicato alla parte sindacale le ragioni tecnico funzionali a sostegno della conservazione delle predette informazioni, necessarie a garantire il funzionamento del sistema di posta elettronica, dell'account Microsoft 365 e del servizio di navigazione in Internet
- la parte sindacale prende atto delle ragioni poste dal Ministero a fondamento dell'operatività dei servizi in conformità alla normativa vigente, comprese le modalità e i tempi di conservazione dei metadati e dei dati di log.
- la parte sindacale, conseguentemente, prende atto della necessità della conservazione dei metadati registrati nel sistema di posta elettronica, dell'account Microsoft 365 e del servizio di navigazione in Internet per un periodo di 90 giorni;
- l'accesso ai suddetti dati è consentito esclusivamente per le finalità indicate nel presente accordo, da parte di soggetti formalmente autorizzati e secondo procedure interne che ne garantiscano la tracciabilità, nel rispetto della normativa vigente e dei provvedimenti del Garante per la protezione dei dati personali nelle materie oggetto del presente accordo;
- l'accesso a tali dati può avvenire solo nei casi previsti dalle vigenti disposizioni normative o su richiesta dell'autorità giudiziaria;
- tali dati, inoltre, non potranno essere utilizzati in caso di contestazioni disciplinari nei confronti dei lavoratori, salvo azione intenzionale del dipendente a danno dell'Amministrazione;
- il Ministero della salute conferma l'esclusione di qualsiasi finalità di controllo a distanza dell'attività lavorativa attraverso i suddetti sistema/servizi e che non è previsto alcun sistema di monitoraggio attivo e/o rilevazione di dati utilizzati in tempo reale durante lo svolgimento dell'attività lavorativa dei dipendenti;
- le parti del presente accordo sono tenute alla massima riservatezza verso i terzi delle informazioni e della documentazione istruttoria ricevuta inerenti alle misure tecniche adottate per garantire la sicurezza del lavoro, nonché la tutela del patrimonio informativo dell'Amministrazione.

Tutto ciò considerato e concordato, le parti ritengono il presente accordo valido ed efficace dalla data della sottoscrizione.

Roma, _____

PER LE OO.SS.:

PER LA PARTE PUBBLICA:

Per il personale del Comparto:

…….

CISL FP

……

..…….

FP CGIL

……

..…….

UIL PA

……

CONFSAL UNSA

……

FLP

……..

USB PI

……..

CONFINTESA FP

……..

Per il personale della Dirigenza:

FLEPAR

……

CISL FP

……..

ANMI ASSOMED SIVEMP FPM

……..

CIDA FC

……

UIL PA

…….

UNADIS

…….

DIRSTAT FIALP UNSA

……..

FP CGIL

……..

ANAI INPS

……..

ANMI-FEMEPA

……..

Ministero della salute

Dipartimento dell'amministrazione generale, delle risorse umane e del bilancio
Unità di Missione per l'attuazione degli interventi del Piano Nazionale di Ripresa e di Resilienza
Ufficio 5 - Cybersicurezza e infrastrutture ICT

Policy per la gestione della Sicurezza Informatica

REV.	DATA	DESCRIZIONE DELLE REVISIONI
00	Giugno 2020	Prima stesura
01	Marzo 2022	Prima revisione
02	Gennaio 2024	Aggiornamenti riferiti a DPCM 30.10.2023
03	Settembre 2025	Aggiornamenti riferiti a nuova riorganizzazione ministeriale, DDL Cyber e NIS 2

Redazione:	Revisione:	Approvazione:
Gruppo Sicurezza Informatica Ufficio V - Unità di Missione per l'attuazione degli interventi del PNRR	Giuseppe Ignazio Bellifemine Dirigente Ufficio V - Unità di Missione per l'attuazione degli interventi del PNRR	Achille Iachino Direttore Generale - Unità di Missione per l'attuazione degli interventi del PNRR

Firmato digitalmente
da GIUSEPPE IGNAZIO BELLIFEMINE
in data 10/10/2025

2025.10.13 15:03:54
MINISTERO DELLA SALUTE
UMPNRR
Il Direttore Generale
Dott. Achille Iachino

Sommario

1. SCOPO

Lo scopo della presente Policy è stabilire i principi generali per la sicurezza delle informazioni validi per il Ministero della Salute (MdS), nonché gli indirizzi strategici e la struttura organizzativa posta a governo del Sistema di Gestione per la Sicurezza delle Informazioni.

Il presente documento costituisce il principale riferimento di Linee Guida, Standard, Procedure e Istruzioni Operative adottate dallo stesso Ministero con l'obiettivo di rafforzare i principi per la sicurezza delle informazioni e per la protezione dei dati.

2. APPLICABILITA'

Questo documento è destinato a tutto il personale del Ministero e del Comando Carabinieri per la tutela della salute e a tutti coloro che hanno un qualsiasi rapporto di collaborazione con il Ministero stesso.
È inoltre destinato a tutti i fornitori che hanno contratti di natura informatica stipulati con l'Amministrazione e a chiunque utilizzi i sistemi informatici del Ministero della Salute.

3. DOCUMENTI CORRELATI

- RI-01 Disciplinare interno per l'uso degli strumenti e dei servizi informatici;
- PRSI-04 Procedura di gestione degli incidenti di sicurezza delle informazioni;
  - PRSI-04-IO01 - Istruzioni operative per i soggetti coinvolti in eventi\incidenti di sicurezza delle informazioni;
  - PRSI-04-IO01 - All 1 - Guida alla richiesta di informazioni Service Desk;
  - PRSI-04-IO03 - Modalità aggiornamento registro incidenti;
- PRSI-09 Procedura di gestione dei Vulnerability Assessment e Penetration Test;
- PRSI-12 Procedura per la gestione delle attività di sensibilizzazione e formazione Cyber;
- PRSI-13 Procedura di analisi dei rischi;
- PRSI-14 Procedura di Business Impact Analysis;
- PRSI-15 Procedura di gestione del rischio derivante dalle terze parti – Supply Chain Security;
- LGSI-03 Linee Guida di gestione degli accessi logici;
  - (LGSI-03) Istruzioni Operative – 01 Gestione Credenziali Enti Esterni – Machine to Machine;
- LSGI-08 Linee Guida sull'utilizzo della crittografia.

Il sistema inoltre è regolato dalla legislazione vigente in materia di sicurezza, o che impatti sui processi inerenti alla sicurezza informatica, tra cui in particolare:

- Legge 28 giugno 2024, n. 90 - con particolare riferimento all'Articolo 14 - Disciplina dei contratti pubblici di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici;
- D.lgs. 4 settembre 2024, n. 138 – Recepimento della direttiva (UE) 2022/2555 (NIS2), relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, e successive determine;
- Decreto del Ministro della Salute 21 novembre 2024 - Individuazione degli uffici di livello dirigenziale non generale del Ministero della Salute (pubblicato sulla Gazzetta Ufficiale n. 294 del 16 dicembre 2024);
- Framework Nazionale per la Cybersecurity e la Data Protection ver.2.0 del 2024;
- DPCM 30 ottobre 2023, n.196 recante Regolamento di organizzazione del Ministero della Salute;
- Norma UNI CEI EN ISO/IEC 27001:2022 "Information security, cybersecurity and privacy protection - Information security management systems - Requirements";
- Decreto Legislativo 18/05/2018, n. 65 (recepimento della Direttiva NIS) e successivi aggiornamenti;
- D.lgs. 10 agosto 2018, n. 101 e successive modifiche (recepimento del Regolamento UE 2016/679 GDPR);
- D.lgs 13 dicembre 2017, n. 217 "Disposizioni integrative e correttive al decreto legislativo 26 agosto 2016, n. 179, concernente modifiche ed integrazioni al Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, ai sensi dell'articolo 1 della legge 7 agosto 2015, n. 124, in materia di riorganizzazione delle amministrazioni pubbliche";
- Linee guida per lo sviluppo di software sicuro dell'Agenzia per l'Italia Digitale (AgID) AgID del 21 Novembre 2017 e successivi aggiornamenti;
- Misure minime di sicurezza emanate da AgID con Circolare 18 aprile 2017, n. 2/2017 ed applicate in data 31 dicembre 2017;
- Prescrizioni del Regolamento Europeo 2016:679 in termini di obblighi per la sicurezza nel trattamento di dati personali;
- Norma UNI EN ISO 9001:2015 "Requisiti per i Sistemi di Gestione per la Qualità (SGQ)"; Testo unico sulla salute e la sicurezza sul lavoro, decreto legislativo n° 81/2008 e successive modifiche, integrazioni e revisioni;
- Art. 615 ter e ss. del Codice penale – Accesso abusivo ad un sistema informatico.

4. RESPONSABILITA'

Al fine di garantire l'applicazione della Politica e il raggiungimento degli obiettivi di sicurezza, tutto il personale (interno, esterno e collaboratori) deve essere coinvolto e responsabilizzato nella gestione della sicurezza delle informazioni.
I contenuti della presente Politica saranno diffusi e promossi, fin dalla sua prima emissione e in occasione di eventuali modifiche, aggiornamenti o secondo necessità legate a specifici piani formativi, a cura dell'Ufficio V dell'Unità di missione per l'attuazione degli interventi del PNRR del Ministero della Salute, in collaborazione con gli Uffici e Dipartimenti interessati. Inoltre, al fine di garantire un approccio omogeneo, come descritto nei capitoli seguenti, il Ministero ha individuato e assegnato responsabilità specifiche per la gestione della sicurezza informatica, secondo i principi generali di seguito illustrati.

5. ACRONIMI E DEFINIZIONI

Acronimi	Definizioni
AGID	Agenzia per l'Italia Digitale
Backup	In informatica, operazione attraverso cui si duplica un dato (o un insieme di…) che viene poi archiviato su un supporto di salvataggio diverso da quello di provenienza. In caso di guasto del sistema principale è così possibile ripristinare il dato dall'archivio di riserva
BC	Business Continuity: si definisce come tale la capacità di un'Organizzazione di mantenere la propria operatività e garantire così la continuità dei servizi erogati, pur a seguito di un incidente o evento distruttivo
BIA	Business Impact Analysis
CAD	Codice dell'Amministrazione Digitale
CED	Centro Elaborazione Dati
Collaboration	Le piattaforme di team collaboration abilitano uno spazio di lavoro virtuale che consente la condivisione di documenti e dati necessari alle attività lavorative in un unico repository centralizzato e accessibile nel rispetto dei principi di profilazione
Disciplinare	Disciplinare interno per l'uso delle risorse e dei servizi informatici
DMZ	Una zona demilitarizzata (DMZ) è una rete perimetrale, che protegge la rete locale (LAN) interna di un'organizzazione dal traffico non attendibile. La DMZ indica comunemente una sottorete che si trova tra la rete Internet pubblica e le reti private
DR	Disaster Recovery: ripristino delle funzionalità del CED in luogo diverso da quello che ha subito un evento disastroso
Garante	Organo di controllo sulla protezione dei dati personali, istituito ai sensi dell'art.51 del GDPR
GDPR	General Data Protection Regulation - Regolamento Europeo 2016:679 sulla protezione dei dati personali

Acronimi	Definizioni
Gruppo Sicurezza	Gruppo afferente all'ufficio Ufficio 5 della Unità di Missione per l'attuazione degli interventi del Piano Nazionale di Ripresa e di Resilienza che svolge attività di sicurezza informatica.
Hardening	Insieme di attività specifiche di configurazione di un sistema informatico che mirano a minimizzare i rischi in caso di attacco che sfrutti le vulnerabilità dello stesso
IPS	Un sistema di prevenzione delle intrusioni (Intrusion Prevention System, IPS) aiuta le organizzazioni a identificare il traffico dannoso bloccandolo in modo proattivo per impedire l'accesso alla propria rete. I prodotti che utilizzano la tecnologia IPS possono essere implementati in linea per monitorare e ispezionare il traffico in entrata e rilevare eventuali vulnerabilità ed exploit
Least priviledge	Il principio del privilegio minimo (least priviledge) prevede che a un utente vengano concessi i livelli – o permessi – minimi di accesso necessari a svolgere le proprie mansioni
MdS	Ministero della Salute
NSIS	Nuovo Sistema Informativo Sanitario
Need to know	L'accesso ai dati dovrebbe seguire il principio del cosiddetto "need-to-know", ossia in base alla necessità; tale principio prevede che si debba concedere agli utenti l'accesso ai servizi e ai dati in uso presso il Ministero soltanto nel caso in cui questo sia necessario per poter svolgere il proprio lavoro
Patching	Processo di applicazione e installazione di correzioni o aggiornamenti software per risolvere errori o problemi di sicurezza in un sistema informatico
PdL	Postazione di lavoro
Penetration test	Un attacco informatico autorizzato, eseguito per valutare la sicurezza complessiva dell'infrastruttura informatica e identificare eventuali vulnerabilità
RS	Responsabile Sicurezza Informatica
RSI	Responsabile Sistema Informativo

Acronimi	Definizioni
SGSI	Sistema di Gestione per la Sicurezza delle Informazioni: parte del sistema di gestione complessivo, basata su un approccio rivolto al rischio relativo al business, volta a stabilire, attuare, condurre, monitorare, riesaminare, mantenere attivo, aggiornato e migliorare la sicurezza delle informazioni. Il sistema di gestione deve includere la struttura organizzativa, le politiche, le attività di pianificazione, le responsabilità, le prassi, le procedure, i processi e le risorse
SLA	Service Level Agreement
SPC	Sistema Pubblico di Connettività
SSI	Sistema di Sicurezza Informatica
User Account	Insieme di informazioni che individuano un utente e che lo autorizzano o non lo autorizzano all'accesso ad un dominio, o programma, o piattaforma, ecc
VA	Vulnerability Assessment – Scan del sistema che evidenzia eventuali vulnerabilità

6. POLICY

6.1. Pianificazione e governo del sistema della sicurezza (PLSI-01)

Al fine di garantire un sistema per la sicurezza delle informazioni efficace ed efficiente all'interno del Ministero della Salute, è necessario che siano definiti i ruoli, le responsabilità e la pianificazione puntuale delle attività operative.

L'approccio da adottare nella pianificazione e nel governo della sicurezza è di carattere preventivo e difensivo. Le linee d'azione sono le seguenti:

1. **Resistenza passiva**. Eliminazione dei rischi non necessari.
    a. Investire del tempo nella pianificazione e nelle politiche di sicurezza;
    b. Identificare il ruolo di MdS nell'ambito della definizione delle competenze sulla sicurezza (D.Lgs. 4 settembre 2024, n.138 di recepimento della Direttiva (UE) 2022/2555, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione);
    c. Strutturare la rete in modo da limitare l'accesso dall'esterno;
    d. Installare solo i servizi necessari;
    e. Utilizzare software sicuro e robusto e garantirne il continuo aggiornamento;
    f. Configurare opportunamente tutte le componenti logiche e fisiche (reti, server, file system, software, account utente, ecc..) per poter realizzare un appropriato controllo degli accessi.
2. **Resistenza attiva**. Resistenza ai metodi conosciuti di accesso non autorizzato.
    g. Utilizzare apposite soluzioni tecnologiche per ridurre le esposizioni verso l'esterno;
    h. Utilizzare tecniche di cifratura per dati ritenuti riservati, critici o sottoposti ad obblighi normativi.
3. **Logging e monitoraggio**. Testare le difese e individuare i punti deboli.
    i. Monitorare il traffico di rete (Internet, reti interne, connessioni a provider o ad altre reti esterne, ecc…);
    j. Rilevare e registrare attività sospette sulle diverse componenti tecnologiche del MdS;
    k. Testare le difese tramite attività specifiche e mirate (Vulnerability Assessment, Penetration Test, security awareness, ecc..).
4. **Resilienza**. Preparazione al ripristino dopo un attacco.
    l. Realizzare backup con frequenza periodica e prestabilita;

m. Scrivere e tenere aggiornata la documentazione sulle diverse componenti tecnologiche del MdS;
n. Mantenere procedure scritte, approfondite e testate per il ripristino delle diverse componenti tecnologiche del MdS.

Al fine di garantire una corretta pianificazione del sistema della sicurezza devono essere raccolte tutte le informazioni sulle necessità organizzative, tecnologiche e normative che possano avere impatto su di essa.

Nella pianificazione devono essere coinvolti eventuali fornitori o partner e nei rapporti con quest'ultimi dovranno essere adottate le regole di procurement ICT emanate dall'autorità nazionale in tale materia.

In detta pianificazione si dovrà tenere conto che in tutti i casi, i dati devono essere protetti mediante una serie di azioni che il MdS deve mettere in atto e deve indicare attraverso apposite misure descritte nei paragrafi successivi.

Il governo dei sistemi informatici deve essere effettuato in modo da garantire la sicurezza del patrimonio informativo del MdS. A tal fine è necessario regolamentare i seguenti aspetti:

- ✓ documentazione degli asset autorizzati (apparati hardware, software, protocolli autorizzati, dati trattati, ecc…);
- ✓ documentazione di tutte le procedure operative ed in particolare quelle di gestione operativa per la manutenzione dei sistemi informatici MdS;
- ✓ definizione delle responsabilità;
- ✓ controllo delle operazioni ed in particolare quelle di gestione operativa in termini di pianificazione, monitoraggio ed eventuale ripristino se necessario;
- ✓ gestione degli incidenti in collaborazione con tutti gli attori/soggetti anche terzi coinvolti;
- ✓ separazione dei ruoli;
- ✓ separazione degli ambienti;
- ✓ affidamento della gestione operativa a terzi.

L'insieme dei documenti e dei dati prodotti per la pianificazione ed il governo del sistema della sicurezza dovrà essere riesaminato ogni anno tramite procedure di revisione a cura della struttura del Ministero organizzativamente competente. Il riesame si formalizza mediante un verbale di riesame a cui devono necessariamente essere allegati tutti i documenti che riguardano il governo ed il monitoraggio dei sistemi informativi del MdS.

Il riesame del sistema della sicurezza potrà confluire nel più ampio riesame dei sistemi informativi e potrà essere incluso in un più ampio Piano di miglioramento della sicurezza informatica. Tale riesame dovrà, infine, determinare le azioni che dovranno essere intraprese, come, ad esempio, approvvigionamenti di natura ICT.

6.2. Struttura organizzativa per la Sicurezza informatica (PLSI-02)

I principi di **integrità, confidenzialità e disponibilità** sono i fattori chiave per la gestione in sicurezza dell'informazione.

Il Ministero della Salute, nell'ambito delle proprie attribuzioni, tratta una serie di dati che devono sempre rispettare i principi sopra citati.

I dati vengono trattati, prevalentemente, con mezzi informatici; pertanto, l'Amministrazione dovrà prevedere una struttura con funzioni in materia di sicurezza informatica, in particolare:

- ✓ azione di indirizzo, pianificazione, coordinamento e monitoraggio della sicurezza informatica, relativamente ai sistemi, alle infrastrutture, anche in relazione al sistema pubblico di connettività, nonché ai dati in attuazione della normativa nazionale, europea ed internazionale in materia di protezione dei dati sanitari, anche in collaborazione con l'Agenzia per la cybersicurezza nazionale (ACN) quale autorità nazionale per la cybersicurezza e l'Agenzia per l'Italia digitale (AgID), in coerenza con gli indirizzi stabiliti dal Garante per la protezione dei dati personali e sulla base dei principi tecnici definiti dall'Agenzia nazionale per i servizi sanitari regionali nel ruolo di Agenzia nazionale per la sanità digitale;
- ✓ pianificazione, progettazione, sviluppo e gestione dell'infrastruttura tecnologica e delle reti del Servizio sanitario nazionale e del Ministero;
- ✓ attività della struttura e del referente per la cybersicurezza ai sensi della legge 28 giugno 2024, n. 90;
- ✓ funzioni di «Autorità di settore NIS» in attuazione della direttiva (UE) 2022/2555 e attività di supporto all'Autorità nazionale competente ACN.

Tale struttura, che potrà anche essere in parte gestita in outsourcing, dovrà essere formata da uno o più responsabili per la cybersicurezza e da personale qualificato e specializzato, con aggiunta di personale di supporto per l'espletamento dei compiti sopra citati.

6.3. Categorizzazione delle informazioni (PLSI-03)

Le informazioni gestite dal Ministero della Salute hanno una duplice categorizzazione che tiene conto sia della legislazione relativa alla protezione dei dati (Registro dei trattamenti), sia del grado di riservatezza delle informazioni trattate.
Le informazioni riconducibili alla legislazione relativa alla protezione dei dati sono classificabili in:

- ✓ dati personali;
- ✓ dati particolari (giudiziari, inerenti salute, credo religioso, credo politico, identità di genere, ecc.).

Le informazioni che non rientrano nella suddetta disciplina possono essere raggruppate secondo le categorie di seguito riportate:

- ✓ pubbliche – tutte le informazioni il cui contenuto può essere diffuso all'interno o all'esterno dell'organizzazione in quanto la loro divulgazione non comporta alcun rischio per l'Amministrazione. I dati possono circolare liberamente ed essere pubblicati verso l'esterno, ad esempio sul sito Internet ministeriale;
- ✓ ad uso interno – l'informazione deve essere trattata all'interno del Ministero della Salute, e l'accesso alla stessa è consentito al personale dipendente e non (a titolo esemplificativo personale esterno e/o fornitori) del Ministero. Rientrano in questa categoria tutte le informazioni che non hanno ottenuto l'approvazione alla libera diffusione al di fuori dell'Amministrazione;
- ✓ confidenziali - la diffusione non autorizzata, la perdita, la manomissione o l'uso indebito possono arrecare un danno all'organizzazione, ai suoi dipendenti e/o a terze parti. I dati di tale tipologia possono essere acceduti e/o distribuiti solo a liste ristrette di dipendenti e di terze parti interessate, sotto il controllo di chi ne è responsabile;
- ✓ riservate – sono le informazioni che per ragioni legislative e/o strategiche richiedono la massima attenzione nella loro divulgazione creando gravi danni all'Amministrazione, ai cittadini o a chiunque sia coinvolto. La distribuzione di tali dati deve essere sottoposta a rigidi controlli sia per quanto riguarda i destinatari, sia per le modalità con cui vengono distribuite (controlli crittografici nel caso in cui fossero in formato elettronico, cassaforte o armadio dotato di chiave per il formato cartaceo);
- ✓ classificate - qualsiasi informazione cui sia stata attribuita una classifica di segretezza (es. Riservato, Riservatissimo, Segreto, Segretissimo), secondo la normativa nazionale. Tali informazioni sono trattate solo da personale autorizzato, trasmesse tramite canali governativi approvati, e utilizzate

esclusivamente per gli scopi previsti. Il trasferimento a terzi richiede autorizzazione scritta dell'autorità competente.

Le informazioni ad uso interno, confidenziali e riservate, siano esse in formato elettronico o cartaceo, devono essere debitamente etichettate, in modo che sia sempre chiaro che tipo di informazione si stia trattando. L'etichettatura non deve essere facilmente modificabile.

Le eventuali copie dei dati categorizzati devono essere trattate con le medesime regole di accesso e protezione degli originali.

Il processo di categorizzazione delle informazioni deve essere periodicamente rivisto al fine di garantire un costante allineamento fra il dato trattato e il suo grado di riservatezza. L'eventuale modifica della categorizzazione può avvenire solo attraverso un'apposita procedura di revisione della stessa.

6.4. Asset Management (PLSI-04)

Gli Asset del Ministero della Salute sono categorizzati secondo le seguenti tipologie:

- ✓ Risorse hardware;
- ✓ Risorse software;
- ✓ Dati.

Ogni categoria prevede la definizione del suo livello di sicurezza in termini di priorità e valore. Il livello assegnato deve essere valutato attraverso:

- ✓ la funzione del sistema;
- ✓ la classificazione dei dati trattati in termini di riservatezza, integrità e disponibilità;
- ✓ il valore per il business dell'Organizzazione;
- ✓ la criticità.

L'Asset Management (gestione degli inventari) comprende tutte le attività di raccolta, memorizzazione, aggiornamento e reporting delle informazioni relative alle componenti del sistema informativo del MdS, ove per "componenti del sistema informativo" si intende l'insieme di apparati hardware, di software e di dati, inclusi i sistemi informativi esterni al Ministero.

L'attività di gestione degli asset deve essere effettuata in modo continuo al fine di garantire che a fronte di modifiche (nuovi strumenti hardware o software, nuovi flussi di dati, etc.) i relativi database siano aggiornati, laddove possibile con meccanismi automatici.

L'inventario degli asset creato deve includere tutte le informazioni necessarie alla sua identificazione e categorizzazione.

L'inventario del software deve includere anche le piattaforme applicative e deve indicare su quali apparati è utilizzato.

L'inventario degli asset deve considerare tutti i database in uso presso il Ministero e deve riportare l'indicazione della loro criticità, rilevata in base al tipo di dati in essi contenuti. Tali informazioni devono essere riportate anche nella Business Impact Analysis (BIA) propedeutica alla definizione del Piano di Continuità Operativa e del Disaster Recovery Plan.

La classificazione e l'inventariazione degli asset deve essere effettuata anche nel caso vi siano sistemi gestiti all'esterno dell'Organizzazione.

Al fine di ottemperare alle normative vigenti relative al trattamento di dati personali, i flussi di dati devono essere opportunamente catalogati nel Registro dei trattamenti, compilato ai sensi dell'art.30 del GDPR (Regolamento europeo 679/2016).

In ottemperanza al Decreto Legislativo 138/2024 e alla Direttiva (UE) 2022/2555 (NIS 2), l'inventario degli asset ICT deve essere oggetto di monitoraggio e aggiornamento continuo, al fine di riflettere tempestivamente ogni modifica infrastrutturale, nuova acquisizione o dismissione, garantendo così un controllo costante e puntuale sull'intera infrastruttura digitale.

6.5. Gestione degli accessi (PLSI-05)

L'accesso alla rete di MdS deve essere effettuato da asset autorizzati e presenti nel relativo inventario e da personale interno al Ministero. L'accesso deve avvenire nel modo più sicuro possibile, per esempio, con un'autenticazione a più fattori, in ogni caso attraverso credenziali personali ed univoche, deve essere registrato attraverso un'attività di logging e deve essere oggetto di monitoraggio.

La rilevazione di apparati non autorizzati collegati alla rete del MdS deve essere effettuata preferibilmente con modalità automatiche.

L'accesso da parte di soggetti esterni a qualsiasi asset del patrimonio informativo dell'Amministrazione deve essere opportunamente autorizzato.

Al fine di consentire l'accesso, sia fisico che logico, a persone non appartenenti a MdS, deve essere effettuato un risk assessment, anche informale, per valutare se mettere in atto misure di sicurezza suppletive al fine di garantire riservatezza, integrità e disponibilità dei dati dell'Amministrazione nel rispetto dei principi di "*need to know*" e "*least priviledge*".

I soggetti appartenenti ad enti e organi del Servizio Sanitario Nazionale e ai NAS hanno l'accesso all'ambiente di esercizio degli asset che trattano le informazioni necessarie all'espletamento delle loro attività.

6.5.1 Sicurezza Fisica

Il gestore dei Data Center per conto di MdS è anche responsabile della sicurezza fisica degli stessi e dovrà provvedere alla sicurezza di area, prevenendo accessi fisici non autorizzati, danni ad asset e all'operatività dei servizi e processi informatici, utilizzando, a titolo esemplificativo e non esaustivo:

- ✓ Sistemi di video sorveglianza;
- ✓ Sistemi di allarme perimetrale;
- ✓ Sistemi di allarme interno;
- ✓ Sistemi di vigilanza e di reception.

Il gestore dei Data Center per conto di MdS deve provvedere alla sicurezza delle apparecchiature**,** proteggendole da danneggiamenti accidentali o intenzionali e alla sicurezza ambientale tramite:

- ✓ Sistemi di climatizzazione;
- ✓ Sistemi di rilevamento allarmi ambientali (incendi, allagamenti, ecc,);
- ✓ Impianti di alimentazione elettrica di emergenza (UPS).

L'accesso alle aree riservate dei Data Center per conto di MdS deve essere concesso solo al personale addetto e opportunamente autorizzato. Le autorizzazioni all'accesso devono essere revisionate periodicamente e ogniqualvolta se ne dovesse presentare l'esigenza.

Per quanto riguarda le postazioni di lavoro informatizzate, MdS dovrà avvalersi, ove possibile, di analoghe misure di sicurezza.

6.5.2 Sicurezza Logica

Per poter garantire la sicurezza del patrimonio informatico di MdS è necessario definire quali siano i requisiti necessari per ottenere l'accesso al dominio, alle applicazioni e, più in generale, ai sistemi informativi del Ministero.

Al fine di garantire il corretto allineamento fra attività svolte e profili di accesso ai sistemi devono essere considerati:

- ✓ l'ente di appartenenza;
- ✓ le attività che l'utente deve svolgere (sia esso dipendente o consulente).

La concessione dell'accesso deve rispettare quanto stabilito dalla corrispondente policy in merito alla riservatezza.

Il controllo accessi ai servizi informatizzati MdS deve essere garantito almeno tramite user accounts e user groups e laddove tecnicamente possibile attraverso un sistema più sicuro come, ad esempio, autenticazione a più fattori o riconoscimento biometrico.

Il personale utilizza le risorse informatiche di proprietà di MdS nei limiti del profilo autorizzativo assegnato, in linea con il ruolo ricoperto e le mansioni assegnate, e per esclusive finalità lavorative.

Tale utilizzo deve sempre ispirarsi ai principi di diligenza e correttezza che sono alla base di ogni atto o comportamento posto in essere nell'ambito del rapporto professionale, in coerenza con le vigenti normative.

Devono essere predisposte e diffuse idonee linee guida per il personale del Ministero contenenti indicazioni circa le modalità da osservare sul corretto utilizzo delle risorse e dei servizi informatici nonché le responsabilità, anche civili e penali, derivanti in caso di inosservanza. Devono inoltre essere predisposte linee guida per user account, user groups e utenze amministrative in termini di definizioni e regole d'uso.
L'accesso al dominio può essere effettuato tramite autenticazione con certificato digitale, nel qual caso è necessario che la chiave privata sia adeguatamente protetta, oppure tramite User Account.

Per accedere ai servizi applicativi erogati da MdS, l'utente deve essere in possesso di apposito profilo e credenziali attraverso specifiche autorizzazioni del competente Ufficio MdS.

6.6 Protezione dei Sistemi Informatici (PLSI-06)

La gestione dei sistemi informatici di MdS deve essere svolta da personale qualificato, interno o su contratto, che per esperienza, capacità e affidabilità fornisce garanzia del pieno rispetto delle disposizioni interne e delle normative esterne in materia.

La sicurezza perimetrale deve essere gestita anche con l'ausilio di specifici apparati per effettuare il monitoraggio, prevenire o bloccare eventuali tentativi di intrusione e verificare il corretto utilizzo dei protocolli autorizzati da/verso reti esterne (Internet).

Tutte le operazioni di accesso o amministrazione remota di server, pdl, dispositivi di rete, ecc. devono essere eseguite tramite connessioni sicure e protette.

Devono essere implementati meccanismi che permettono di soddisfare requisiti di resilienza sia durante il normale esercizio che in situazioni avverse.

Al fine di garantirne la protezione, negli ambienti di sviluppo, collaudo, pre-esercizio e produzione devono essere disattivate tutte le funzioni superflue. Tali ambienti devono essere opportunamente aggiornati per ridurre eventuali esposizioni causate da difetti o vulnerabilità emergenti.

L'adeguatezza dei processi di *hardening* e *patching* deve essere periodicamente verificata mediante attività di vulnerability assessment dei sistemi e/o penetration test attraverso idonei strumenti regolarmente aggiornati, analisi mirate e adeguata documentazione. I test di vulnerability assessment devono essere effettuati anche in caso di significativi cambiamenti alla configurazione dei sistemi o delle reti.

Si deve tenere in considerazione, nell'attività di scansione, ogni segnalazione di nuove minacce o vulnerabilità provenienti da servizi appositi (es. bollettini CSIRT, CNAIPIC, servizi di *Early warning*/IOC di terze parti, ecc.)

Devono essere effettuate attività di scanning delle vulnerabilità periodiche, per le quali devono essere archiviati i relativi log e mantenuta tutta la documentazione a supporto dei rilievi identificati e le relative azioni correttive poste in essere.

Gli ambienti di sviluppo non devono contenere dati reali.

I supporti di memorizzazione removibili e i documenti cartacei relativi ai sistemi informatici devono essere adeguatamente protetti per esempio da danneggiamenti casuali o intenzionali, furti, smarrimenti, ecc.

Qualora i dati presenti sui supporti removibili, così come quelli su documenti cartacei, contengano informazioni riservate, sarà necessario prevedere apposite procedure di accesso e custodia in cassaforte o armadi dotati di chiave.

A titolo esemplificativo, possono esserne gestite:

- ✓ la conservazione;
- ✓ l'accesso;
- ✓ la cancellazione (per i supporti);
- ✓ la distruzione.

La cancellazione dei dati memorizzati su supporti mobili di memorizzazione diventa obbligatoria nei casi in cui le corrispondenti informazioni non siano più utili a MdS e non vi sia alcun vincolo legale che ne preveda la conservazione.

La distruzione di tutti i supporti contenenti dati diventa obbligatoria in caso di obsolescenza, numero massimo di riscritture, guasto irreparabile, ecc..; il processo deve tener conto del possibile impatto ambientale preferendo, per tale motivo, il ricorso a ditte specializzate.

6.7 Protezione da software dannoso (PLSI-07)

L'integrità delle informazioni e delle risorse informatiche deve essere preservata dalla possibile compromissione da parte di software dannoso (es. virus, worm, trojan horses, ransomware, software manomessi, ecc..).

A tal fine devono essere previste difese perimetrali idonee (es. antispamming, firewalling, Url filtering, ecc.).

Su tutti i server e su tutte le postazioni di lavoro informatizzate devono essere installate idonee soluzioni antivirus/antimalware, controllate e gestite in modalità automatica e centralizzata, con aggiornamenti automatici rispetto ai periodici rilasci della casa madre e con la capacità di rilevare anomalie di comportamento. Tali soluzioni non devono essere disattivabili dagli utenti. Tutte le operazioni di installazione, disinstallazione, disattivazione, anche temporanea, dei sistemi antimalware devono essere effettuate esclusivamente dall'Amministratore di Sistema.

Deve, inoltre, essere possibile forzare un particolare aggiornamento, tramite la consolle centralizzata, in caso di necessità.

Sulle PdL, ove necessario, devono anche essere attivati firewall e IPS personali.

Tutti gli eventi rilevati dai citati sistemi di sicurezza devono essere registrati ed archiviati in un repository centralizzato; nel caso in cui l'analisi degli eventi dannosi rilevati non sia delegata a soggetti terzi, si dovrà operare su sistemi dedicati e staccati dalla rete.

6.8 Configurazione degli apparati (PLSI-08)

Tutti gli apparati MdS devono essere configurati a partire da configurazioni standard sulle quali è stato implementato l'opportuno *hardening* rispetto alla destinazione d'uso dell'apparato stesso.

Tali configurazioni devono essere oggetto di backup, segregate su postazioni non collegate alla rete o, se su supporti portatili, custodite in armadi chiusi a chiave, e periodicamente validate da MdS.

Le postazioni di lavoro informatizzate devono essere configurate secondo le necessità, opportunamente documentate, legate alle mansioni che l'utente dovrà svolgere; l'assegnazione agli utenti deve prevedere apposita procedura.

In caso di sistemi sui quali siano memorizzati dati con un grado di particolare criticità o riservatezza si devono valutare misure di sicurezza aggiuntive come, ad esempio:

- ✓ L'isolamento dalla rete;
- ✓ L'introduzione di opportune whitelist;

- ✓ L'inibizione delle porte USB;
- ✓ L'inibizione dell'accesso a persone non autorizzate.

Il ciclo di vita di tutti i sistemi hardware e software deve essere standardizzato e documentato.

6.9 Applicazioni e Servizi interni (PLSI-09)

MdS mette a disposizione dei propri utenti interni applicazioni, servizi e strumenti di supporto, comunicazione e *collaboration* omogenei adottando opportune misure di sicurezza. Tali servizi vengono descritti nell'apposito Disciplinare a cui si rimanda per le regole di dettaglio.

6.9.1 Navigazione web

Al fine di garantire una adeguata protezione dei sistemi informativi dell'amministrazione, devono essere implementate adeguate misure di sicurezza per la navigazione web. Il traffico web deve essere limitato ai siti inerenti all'attività lavorativa e comunque a siti "sicuri". Deve essere bloccato l'accesso a siti illegali, e a quelli "pericolosi" attraverso le opportune funzioni di filtering sul firewall.

6.9.2 Posta elettronica

Per garantire la sicurezza del sistema informativo del Ministero, devono essere poste in essere tutte le azioni necessarie al filtraggio della posta elettronica attraverso sistemi antispam e antivirus. Inoltre, dovrà essere bloccata la spedizione e la ricezione di allegati con estensioni non strettamente connesse all'attività lavorativa e potenzialmente pericolose.

6.9.3 Cloud

I repository per il cloud devono risiedere nell'ambito dello Spazio Economico Europeo (SEE).

L'accesso ai servizi cloud deve avvenire con le stesse credenziali usate per l'accesso alla rete del Ministero.

Il gestore del cloud deve garantire il rispetto di tutte le policy di sicurezza e di quelle per la Continuità Operativa riportate nelle presenti policy.

6.9.4 WiFi

Il servizio WI-FI deve essere configurato in linea con le misure di sicurezza previste per la rete LAN ed in particolare per la navigazione web. La rete wireless aziendale deve prevedere opportuni meccanismi di autenticazione in grado di garantire l'accesso ai

soli utenti autorizzati evitando l'utilizzo di protocolli notoriamente non sicuri (WEP, WPA, ecc…).

Il nome utente e la password utilizzati devono corrispondere a quelli della rete interna di MdS.

6.10 Gestione della Continuità Operativa (PLSI-10)

MdS, con il supporto di eventuali fornitori in outsourcing, predispone il Piano di Continuità Operativa (Business Continuity Plan) in conformità a quanto previsto dalla normativa vigente e dai principali standard internazionali, tanto al fine di garantire la continuità dei servizi e mitigare il rischio di perdita di informazioni.

Tale piano descrive i processi da mettere in atto, le attrezzature ed il personale per far fronte ad eventi come, a titolo esemplificativo e non esaustivo:

- ✓ catastrofi naturali;
- ✓ incidenti;
- ✓ atti vandalici o terroristici;
- ✓ indisponibilità di attrezzature critiche per il funzionamento di MdS.

La responsabilità della gestione e della manutenzione delle operazioni di backup dei server è di competenza di un apposito Amministratore di sistema.

Le policy di backup adottate devono almeno tener conto dei seguenti elementi:

- ✓ selezione delle informazioni oggetto di backup;
- ✓ controllo dell'esito delle operazioni di backup anche attraverso ripristini di prova;
- ✓ protezione e controllo dei supporti di memorizzazione utilizzati;
- ✓ definizione di frequenza e periodi di retention in base alla classificazione delle informazioni;
- ✓ test di ripristino delle operazioni di back up eseguite.

I supporti utilizzati per le operazioni di backup devono essere protetti da accessi non autorizzati, tramite cifratura o comunque con mezzi idonei a preservarne la riservatezza e l'integrità; è fortemente consigliato archiviare almeno una delle copie di backup su apparati '*stand alone*' non collegati alla rete.

Il ripristino dei dati dovrà essere eseguito a fronte di una richiesta dell'Amministrazione o di propri referenti terzi autorizzati.

Per la minimizzazione dei disservizi, la gestione degli errori e le attività degli operatori devono essere tracciati ed interpretati con l'ausilio di un sistema centralizzato di Log

Management. Tale sistema deve essere correlato ad un sistema di analisi (SIEM) che consenta la correlazione degli eventi e delle operazioni intraprese.

Il Piano di Continuità Operativa deve contenere un Piano di Disaster Recovery in caso di dichiarazione di disastro. Tali piani devono essere periodicamente riesaminati e aggiornati in base a cambiamenti di natura organizzativa o tecnica.

Tutti gli eventi anomali devono essere analizzati e gestiti secondo le tipologie individuate e opportunamente classificati.

Nell'impossibilità di ripristinare i sistemi impattati in tempi brevi, si deve procedere con la mitigazione degli effetti e degli impatti dell'evento.

MdS predispone e aggiorna periodicamente una procedura di gestione degli incidenti che disciplina e dettaglia tutte le fasi di gestione di un incidente, dal momento in cui si verifica fino al completo ripristino dei servizi impattati e follow-up. Inoltre, a seguito dell'entrata in vigore della Direttiva NIS 2, il MdS si impegna a rispettare le tempistiche previste per la notifica degli incidenti, garantendo un primo invio entro 24 ore dalla scoperta di un incidente significativo, in conformità con il flusso operativo e le scadenze stabilite dalle linee guida pubblicate dall'ACN.

6.11 Change Management (PLSI-11)

Tutte le modifiche apportate a sistemi ed applicazioni MdS, ivi incluse quelle alle configurazioni, devono essere oggetto di un processo formale di Change management, al fine di garantirne la correttezza, i test, la documentazione, le autorizzazioni e la tracciatura. Sulla base delle modifiche effettuate e delle minacce alla sicurezza osservate, i test sul sistema oggetto di cambiamento devono essere ripetuti regolarmente e comprendere scenari di attacchi potenziali pertinenti e noti. Il risultato di tali test deve essere condiviso, in automatico, con gli amministratori di sistema.

Se possibile, si deve utilizzare un sistema centralizzato di controllo automatico delle configurazioni che possa rilevare e segnalare modifiche non autorizzate e consentire il ripristino di configurazioni standard.

Deve essere garantito l'aggiornamento di tutte le componenti hardware e software attraverso operazioni di upgrade, *patching* e correzione degli errori applicativi rilasciati dai produttori. Devono essere comprese negli aggiornamenti le corrispondenti procedure di *rollback* per il ripristino delle situazioni ex-ante in caso di problemi.

6.12 Network Management (PLSI-12)

L'infrastruttura di rete deve essere protetta da tutti quei fattori che volontariamente o involontariamente ne possano pregiudicare l'integrità e la disponibilità.

La rete dati deve prevedere meccanismi di segretazione, autenticazione, cifratura e controllo in grado di garantire la sicurezza dei flussi da e verso le diverse risorse informatiche e prevenire accessi non autorizzati.

A tale scopo occorre garantire i seguenti requisiti minimi:

- ✓ La rete dati deve essere opportunamente segregata al fine di minimizzare i rischi di accessi non autorizzati ai servizi e disservizi dovuti a comportamenti volontari o involontari;
- ✓ La rete dati deve essere separata dalle reti esterne e più in generale da internet mediante firewall in grado di oscurare la topologia e l'indirizzamento interno della rete e rendere visibili dall'esterno esclusivamente i servizi pubblicati;
- ✓ i servizi pubblicati su internet devono essere resi accessibili mediante un livello front-end (web server, reverse proxy) in grado di terminare la sessione da internet e re-instaurarla verso le componenti software di business (applicazioni e banche dati);
- ✓ tutti i sistemi di front-end che espongono servizi accessibili da Internet devono risiedere su segmenti di rete ad hoc (DMZ) segregati mediante firewall dai segmenti che ospitano le componenti applicative e i database;
- ✓ tutti i flussi dati che coinvolgono segmenti di rete in cui il livello di sicurezza è al di sotto del livello previsto di "fiducia" (le cosiddette reti "*non trusted*", come ad esempio Internet) devono avvenire utilizzando protocolli (HTTPS, SFTP, SSL/TLS, SSH) in grado di cifrare le credenziali di autenticazione e le comunicazioni. Nel caso di dati critici devono essere adottati meccanismi di cifratura anche del dato. In particolare, tutti gli accessi effettuati da remoto verso risorse all'interno della intranet devono avvenire tramite canali sicuri in grado di proteggere le credenziali di accesso;
- ✓ tutti i segmenti di rete che ospitano sistemi accessibili da Internet devono essere monitorati mediante sistemi IPS;
- ✓ l'accesso a segmenti di rete più critici deve prevedere meccanismi di autenticazione basati su credenziali o certificato.

La struttura organizzativa competente del Ministero in termini di infrastrutture di rete deve garantire il corretto funzionamento di tutti i dispositivi di rete e l'applicazione di sistemi ed accorgimenti che rendano adeguato il livello di sicurezza del patrimonio informativo del Ministero della Salute. A tal fine, coordinando tutti i fornitori coinvolti per la risoluzione di incidenti ed anomalie, devono impegnarsi per la risoluzione dei

problemi riscontrati, in tempi adeguati alla gravità degli stessi ed all'urgenza del ripristino dei servizi coinvolti.

Ogni qual volta, a causa di interventi di manutenzione programmata o straordinaria sull'infrastruttura di rete, si venga a creare una sospensione parziale o totale dei servizi, tutti gli utenti interessati devono essere tempestivamente avvisati attraverso i mezzi di comunicazione, anche elettronici (es. e-mail, intranet), a disposizione dell'Amministrazione. Nelle comunicazioni è necessario indicare i motivi generali dell'intervento, in che modo impatta sull'interruzione dei servizi, e, soprattutto ora e data di inizio e di fine.

6.13 Definizione dei ruoli e responsabilità (PLSI-13)

6.13.1 Definizione dei ruoli e delle responsabilità della Sicurezza Informatica

L'assegnazione delle mansioni al personale dell'Amministrazione deve essere gestita in modo da limitare il rischio legato ad errori umani, furti, frodi o usi delle infrastrutture non conformi alle Policy di sicurezza. A tal fine è necessario regolare i seguenti aspetti:

- ✓ la definizione dei ruoli, termini e condizioni di impiego;
- ✓ la verifica della compatibilità del ruolo;
- ✓ gli accordi di non divulgazione.

In particolare, devono essere definiti e resi noti i ruoli e le responsabilità del personale incaricato della Sicurezza Informatica, indipendentemente dal livello gerarchico occupato, coinvolgendo anche i soggetti terzi che svolgono incarichi chiave per la sicurezza informatica compresi quelli di eventuali fornitori esterni.

6.13.2 Sensibilizzazione degli utenti

Al fine di garantire l'efficacia delle misure di sicurezza è necessaria la collaborazione degli utenti che sono tenuti ad applicare tali misure.

A tal fine l'Amministrazione provvederà ad erogare agli utenti un'adeguata formazione finalizzata alla sensibilizzazione e consapevolezza, entrambe necessarie agli utenti per lo svolgimento delle attività operative nel rispetto del patrimonio informativo dell'Amministrazione. In aggiunta, l'Amministrazione ha la responsabilità di effettuare simulazioni di phishing periodiche, al fine di valutare il livello di esposizione al rischio umano e rafforzare la postura complessiva di sicurezza dell'Ente.

Le società fornitrici di servizi informatici per il Ministero della Salute sono obbligate alla firma di un "patto di riservatezza" contestualmente alla firma del contratto di lavoro.

6.13.3 Responsabilità degli utenti

Gli utenti sono responsabili in prima persona della strumentazione fornita loro per lo svolgimento dell'attività lavorativa.

Il mancato rispetto delle regole riportate nelle Policy e procedure del Ministero, nonché del Disciplinare interno per l'uso degli strumenti e servizi informatici, che il nuovo assunto, firmando il contratto di assunzione, si impegna ad osservare, può comportare l'erogazione di sanzioni disciplinari o, in alcuni casi, in sanzioni a livello giudiziale.

La struttura organizzativa competente del Ministero sulla sicurezza informatica è tenuta ad informare il personale, sia interno che esterno, delle policy emesse perché questi possano applicarle, ciascuno per la propria parte.

I dipendenti sono tenuti al rispetto delle Policy di sicurezza e all'adempimento dei compiti assegnati anche quando svolgono l'attività lavorativa presso luoghi diversi dalle sedi del Ministero della Salute.

La responsabilità degli utenti, dove per utenti si intende il personale interno di MdS, i fornitori, i consulenti o comunque chiunque utilizzi beni o servizi informatici dell'Amministrazione e che abbia accesso ai dati di proprietà del Ministero, si applica alle regole generali di comportamento e ad alcune regole particolari come la gestione delle proprie credenziali, l'obbligo di riservatezza, ecc.

Nel caso in cui un utente sia costretto ad utilizzare una postazione di lavoro che non sia la propria, è tenuto, alla fine dell'utilizzo, a cancellare le informazioni su cui ha lavorato, se queste hanno un alto grado di riservatezza, accertandosi anche che non siano reperibili nel cestino.

Per quanto riguarda il personale appartenente al Gruppo Sicurezza, questo è tenuto a non divulgare le misure di sicurezza applicate per la difesa del Patrimonio Informativo del Ministero della Salute a persone che non ne hanno diritto, sia interne che esterne all'Amministrazione.

6.14 Trasmissione delle informazioni (PLSI-14)

Le informazioni di proprietà MdS possono essere trasferite all'interno o all'esterno dell'Amministrazione, curandone la protezione anche durante gli spostamenti.
Per trasferire le informazioni, risulta obbligatorio verificare:

- ✓ la classificazione (PLSI-03 - Categorizzazione delle informazioni);
- ✓ mittente e destinatario (interno o esterno a MdS);
- ✓ tipo di trasmissione (digitale, cartacea, su supporto di memorizzazione);
- ✓ forma dell'informazione;

- ✓ trasporto dell'informazione;
- ✓ autorizzazione alla trasmissione.

Nel caso in cui sia necessario trasmettere informazioni riservate o nel caso in cui sia necessario trasmettere le informazioni ad uso interno a destinatari esterni, devono essere utilizzate tutte le misure di sicurezza idonee a garantire che siano ricevute e consultate dai soli soggetti autorizzati sia che si tratti di informazioni su documenti cartacei o siano essi salvati su supporti di memorizzazione. Nel caso in cui si tratti di informazioni inviate telematicamente, devono essere utilizzati gli strumenti di autenticazione e crittografia messi a disposizione dall'Amministrazione.

Non è consentito inviare in via telematica informazioni riservate (tra cui dati ex sensibili) o informazioni per uso interno a destinatari non interni se non si dispone di opportuni strumenti di crittografia (compreso l'uso di VPN).

Le informazioni riservate e le informazioni per uso interno trasmesse a destinatari esterni devono essere sempre dotate di un'etichetta che contenga le seguenti informazioni:

- ✓ la classificazione dell'informazione;
- ✓ il mittente;
- ✓ il numero di protocollo;
- ✓ il destinatario.

L'etichetta deve essere applicata, nel caso di documenti cartacei e supporti di memorizzazione, sul documento cartaceo/supporto di memorizzazione stesso e sull'involucro che li contiene. Nel caso di invio telematico, la prima pagina del documento deve contenere esclusivamente l'etichetta (in formato elettronico).

6.15 Monitoraggio dei sistemi e delle reti (PLSI-15)

Il monitoraggio di reti e sistemi ICT ha lo scopo di tenere sotto controllo i fornitori dei servizi e l'infrastruttura informatica, valutandone al contempo efficienza ed efficacia. I corrispondenti processi devono essere definiti, testati e soddisfare tutti i requisiti applicabili, così come devono essere esplicitati ruoli e responsabilità di ogni sistema di monitoraggio.

Tali sistemi devono prevedere la produzione di allarmi in caso di criticità al fine di consentire interventi tempestivi e riduzione dei tempi di disservizio, nonché segnalazione di anomalie rilevate, ad esempio:

- ✓ dalla gestione e dall'analisi dei log (Log Management);
- ✓ dai risultati delle scansioni di VA (infrastrutturale, applicativo, dei DB);

- ✓ dai risultati dei Penetration Test;
- ✓ dalle intercettazioni delle sonde IPS/IDS;
- ✓ dalle intercettazioni dei sistemi di *Data Loss Prevention*.

In ottemperanza al Decreto Legislativo 138/2024 e alla Direttiva (UE) 2022/2555 (NIS 2), per almeno i sistemi informativi e di rete rilevanti, devono essere adottati strumenti tecnici aggiornati e configurati in modo adeguato a garantire il rilevamento tempestivo di incidenti significativi. Tali strumenti includono soluzioni di analisi e filtraggio del traffico in ingresso (inclusa la posta elettronica), il monitoraggio degli accessi da remoto, delle attività dei sistemi perimetrali (es. router e firewall), degli eventi amministrativi rilevanti e degli accessi, riusciti o falliti, alle risorse di rete, terminali e applicativi. Devono inoltre essere definiti, monitorati e documentati parametri quali-quantitativi per rilevare accessi non autorizzati o abusi dei privilegi concessi. I livelli di servizio attesi (SL) dei servizi e delle attività devono essere formalizzati anche ai fini del rilevamento tempestivo degli incidenti. Tutte le attività di monitoraggio devono essere supportate da procedure documentate, in linea con le politiche organizzative, che definiscano ruoli, responsabilità e modalità operative.

Con cadenza periodica, le informazioni acquisite durante il monitoraggio dei sistemi informatici devono essere analizzate per consentire l'individuazione delle eventuali vulnerabilità del sistema, degli eventi anomali o sospetti e degli eventuali errori del sistema di controllo. Qualora vengano riscontrate carenze rispetto ai requisiti di sicurezza prefissati, deve essere avviato un processo di revisione dei sistemi stessi al fine di colmare le lacune evidenziate dall'attività di monitoraggio.

6.16 Uso della crittografia (PLSI -16)

Devono essere formalizzate le regole sull'uso dei controlli crittografici per la protezione delle informazioni e dei dati personali al fine di indirizzare un approccio gestionale da parte dell'Amministrazione in tale ambito, definendo i criteri in base ai quali le informazioni e i dati personali devono essere protetti a seconda della criticità assegnata.
Le regole devono includere le componenti fisiche utilizzate per la crittografia, a titolo esemplificativo gli hardware HSM (Hardware Security Module), nonché le modalità di utilizzo, di protezione e di durata delle chiavi crittografiche per tutto il loro ciclo di vita: generazione, memorizzazione, conservazione, recupero, distribuzione, ritiro e distruzione.
Le regole devono fare esplicito riferimento alla normativa nazionale di settore per ogni tipologia di applicazione crittografica implementata, anche per quanto riguarda l'assegnazione dei ruoli e delle responsabilità. A tal proposito il Ministero recepisce e

attua le Linee guida sulla crittografia emanate dall'Agenzia per la cybersicurezza Nazionale[1].

Devono essere presenti strumenti con servizi idonei a rilevare l'uso di cifrature non autorizzate nelle trasmissioni in entrata ed in uscita dalla rete ministeriale.

6.17 Auditing del sistema di sicurezza (PLSI-17)

L'Amministrazione ha il dovere di accertarsi che le misure di sicurezza previste nelle policy siano applicate e che funzionino.
Tutti gli Asset del sistema informativo del Ministero della Salute, sia all'interno che all'esterno dell'Amministrazione, possono essere oggetto di auditing, in modalità differenti secondo la natura dell'Asset stesso e secondo gli standard di settore riconosciuti.
L'attività di auditing può essere effettuata da personale interno all'Amministrazione oppure data in outsourcing.
Nel caso in cui sia interna, il personale designato deve essere assolutamente estraneo al gruppo di lavoro della sicurezza.
Qualora l'Amministrazione decida di ricorrere a società esterne per l'esecuzione di auditing, dovrà valutare i seguenti aspetti:

- ✓ l'affidabilità e l'esperienza dell'azienda;
- ✓ esito di eventuali rapporti precedenti.

In ogni caso oggetto dell'auditing saranno:

- ✓ il rispetto delle norme comportamentali riportate nelle policy e nelle procedure da parte del personale interno o esterno all'Amministrazione;
- ✓ l'applicazione delle procedure;
- ✓ l'esistenza della strumentazione prevista per la sicurezza informatica;
- ✓ la scansione dei server per la verifica della presenza di dati rilevanti in chiaro o di altre vulnerabilità che deve essere fatta con strumenti automatici.

Il rapporto sull'auditing deve essere presentato dal responsabile dell'attività all'Ufficio V che, nel caso questo evidenziasse delle discrasie rispetto agli obiettivi di sicurezza previsti, provvederà tempestivamente all'analisi e alla possibile risoluzione dei problemi emersi.
Il materiale prodotto durante le ispezioni è riservato e deve quindi godere delle precauzioni descritte all'interno della Policy sulla "Classificazione delle informazioni" (PLSI-02).

[1] https://www.acn.gov.it/agenzia/attivita/certificazione-e-vigilanza/crittografia

6.18 Conformità ai requisiti di legge (PLSI-18)

Per ogni sistema deve essere definita ed opportunamente documentata la presenza di eventuali vincoli dovuti a normativa o leggi vigenti.
Gli elementi di prova, ai fini probatori, devono essere raccolti e tenuti in modo conforme alle regole di ammissibilità in giudizio.
Per garantire la conformità dei sistemi ai requisiti di sicurezza, i responsabili di struttura devono assicurare la corretta ed integrale applicazione delle procedure di sicurezza, all'interno della propria area di competenza. In particolare, si fa riferimento ai vincoli di legge civili e penali, a quelli di origine statutaria, ad obbligazioni contrattuali, ai requisiti di sicurezza, ai diritti di proprietà intellettuale e all'uso del software proprietario.
A tale proposito devono essere effettuate regolari verifiche di conformità. Tutte le informazioni detenute dal Ministero e ritenute strategiche, quali informazioni amministrative e contabili, devono essere protette da perdite, distruzione e falsificazione. Inoltre, la legislazione citata deve essere portata a conoscenza di tutto il personale che opera sugli asset del patrimonio informatico.

Per quanto riguarda la proprietà intellettuale e/o il copyright si veda la policy PLSI-06 - Protezione da software dannoso. Per la protezione dei dati si rimanda alla policy PLSI-03 - Categorizzazione delle informazioni.

6.19 Gestione della documentazione della sicurezza (PLSI-19)

La documentazione è parte integrante del sistema di sicurezza di MdS in quanto riporta le regole per il corretto utilizzo degli Asset al fine di ridurre il rischio di incidenti.

A seguito di modifica della legislazione vigente o dell'introduzione di nuove tecnologie o in base al risultato di un audit che ha evidenziato delle vulnerabilità (vedi PLSI-17 Auditing del sistema di sicurezza) o a seguito di cambiamenti organizzativi, può nascere l'esigenza della modifica della documentazione esistente o della creazione di nuovi documenti.

La creazione e la modifica di un documento sulla sicurezza devono rispettare i seguenti criteri:

- ✓ essere a norma di legge;
- ✓ essere tollerabile l'impatto sulle attività di MdS;
- ✓ essere chiare ed attuabili.

In particolare, le policy devono essere formalmente approvate dall*a struttura organizzativa competente del Ministero in termini di* Responsabile dei Sistemi Informativi e solo dopo tale approvazione possono essere divulgate agli interessati. Le

procedure e gli altri documenti del sistema sicurezza devono invece essere approvati dall*a struttura organizzativa competente del Ministero in termini di* cybersicurezza.

Tutta la documentazione sulla sicurezza, ai sensi della vigente normativa sulla protezione dei dati personali, deve essere revisionata almeno una volta l'anno.

6.20 Analisi del rischio (PLSI-20)

L'analisi dei rischi dovrà essere applicata dal MdS periodicamente e ogni qualvolta venga identificata la potenzialità che un'azione possa generare:

- ✓ un danno ad un elemento dell'infrastruttura informatica;
- ✓ una perdita di dati;
- ✓ un'interruzione di un processo;
- ✓ un evento indesiderato.

Una volta effettuata l'analisi dei rischi, si potrà tracciare un piano di azione conseguente per neutralizzare la minaccia o ridurla al minimo. In questo caso, il rischio residuo dovrà essere monitorato e neutralizzato appena possibile.

6.20.1 Supply Chain Risk Management

Il Ministero della Salute, con la presente policy, si impegna a garantire un adeguato livello di sicurezza delle forniture ed esternalizzazioni di beni ICT e servizi introducendo attività di controllo e valutazione del rischio cyber dei fornitori.

Il processo di gestione delle forniture di prodotti e/o servizi ICT (on-premise e cloud) è parte integrante della gestione della sicurezza delle informazioni e di protezione dei dati personali. Pertanto, è necessario definire specifici requisiti di sicurezza, nel regolamentare gli accordi contrattuali e durante la fase di forniture del servizio / prodotto per monitorare l'attuazione di quanto concordato e valutarne la qualità e l'eventuale trattamento del rischio delle forniture ICT.

La Supply Chain Security fa riferimento a processi, tecnologie e competenze con le quali si gestisce e si regola il rapporto con i fornitori al fine di mitigare i rischi e le minacce di cybersecurity derivanti dalla catena di approvvigionamento dei servizi esternalizzati e affidati a terze parti.

Nell'ambito della gestione dei fornitori di servizi ICT, l'amministrazione deve:

- valutare il rischio connesso alla fornitura coinvolgendo l'Ufficio preposto alla sicurezza informatica per gli aspetti di cybersecurity;

- assicurare un'adeguata diversificazione dei fornitori per garantire la resilienza della catena di approvvigionamento;
- valutare l'affidabilità tecnica dei fornitori utilizzando le best practice in materia e tenendo conto almeno dei seguenti ambiti:
    a. la qualità dei prodotti e delle pratiche di sicurezza cibernetica del fornitore;
    b. la capacità del fornitore e dei partner terzi di garantire l'approvvigionamento, l'assistenza e la manutenzione nel tempo;
- formalizzare e mantenere aggiornato l'elenco dei fornitori;
- in relazione alla criticità della componente software, la valutazione dell'affidabilità tecnica del fornitore deve tenere conto:
    a. della disponibilità del fornitore a condividere il codice sorgente;
    b. di certificazioni o evidenze utili possedute dal fornitore in merito alla qualità del processo di sviluppo del software;
    c. dell'adozione, da parte del produttore, di procedure e strumenti tecnici per garantire l'autenticità e l'integrità del software o firmware installato;
    d. dell'adozione, da parte del produttore, di procedure e strumenti tecnici per garantire una corrispondenza univoca tra il codice sorgente e il codice oggetto installato e eseguito.

Inoltre, l'Amministrazione nell'ambito delle attività esternalizzate deve valutare e indirizzare i seguenti aspetti:

- la gestione del rischio inerente della catena di approvvigionamento cyber al fine di identificare e contrattualizzare le idonee misure di cyber security che il fornitore e partner terzi devono rispettare e implementare al fine di erogare i servizi verso l'amministrazione;
- l'indirizzamento dei requisiti di security e privacy by design nel caso in cui i servizi esternalizzati ne prevedano la definizione e l'implementazione;
- la valutazione periodica dei fornitori e partner terzi attraverso audit, verifiche, o altre forme di valutazione per confermare il rispetto degli obblighi contrattuali nell'ambito degli aspetti di sicurezza concordati;
- il rispetto dei requisiti di continuità operativa rispetto ai servizi critici esternalizzati.

6.20.2 Sicurezza dello sviluppo del software

Tutte le attività, comprese quelle di supporto e di manutenzione dei sistemi, devono essere indirizzate da specifiche linee guida e procedure nel rispetto dei principi di sicurezza emanati dalle autorità nazionali nell'ambito di riferimento.

I requisiti relativi alla sicurezza delle informazioni, nonché alla protezione dei dati personali, devono essere inclusi tra quelli richiesti per l'acquisizione e/o lo sviluppo di nuovi sistemi informativi o per l'aggiornamento di quelli esistenti. Tali requisiti scaturiscono da esigenze di conformità (normativa, regolamenti interni e vincoli contrattuali) e dai risultati dell'analisi dei rischi.

I servizi applicativi che transitano su reti pubbliche devono essere sottoposti ad una dettagliata valutazione del rischio, per individuare idonei controlli di sicurezza, finalizzati a contrastare attività fraudolente, dispute contrattuali, divulgazioni e modifiche non autorizzate. In particolare, l'Amministrazione deve garantire che i dati personali trasmessi su reti pubbliche non affidabili vengano crittografati.

Deve essere definita ed applicata una politica contenente le regole per lo sviluppo sicuro del software e dei sistemi all'interno dell'Amministrazione, che:

- tenga conto della sicurezza dell'ambiente di sviluppo;
- tenga conto dei principi di *privacy by design* e *privacy by default* introdotti dalle normative di riferimento sulla protezione dei dati personali;
- contenga una guida sulla sicurezza nelle fasi di sviluppo del software, con riferimento alla metodologia e/o alla piattaforma di sviluppo e alle linee guida di programmazione sicura conformi ai più diffusi standard di sicurezza in materia, nonché ai principi di Security by Design definiti dalle Linee Guida AgID sulla sicurezza ICT;
- analizzi i requisiti di sicurezza nella fase di progettazione, con riferimenti anche alla gestione delle versioni;
- preveda che le milestone di progetto debbano includere specifici controlli sullo stato di implementazione dei requisiti di sicurezza e sui risultati dei test eseguiti (qualità del software).

Qualora le attività di sviluppo comportino trattamenti di dati personali che possano avere un impatto elevato sui diritti e le libertà degli interessati e che ricadono nell'elenco delle tipologie di trattamenti previsti dal provvedimento del GPDP del 11 ottobre 2018 è necessario condurre una valutazione di impatto per la protezione dei dati (di seguito, per semplicità, DPIA). I risultati dell'attività di DPIA devono essere

tenuti in considerazione per determinare le opportune misure di sicurezza tecniche e organizzative da attuare al fine di mitigare i rischi identificati.

Devono essere definite procedure formali di controllo dei cambiamenti dei sistemi all'interno del loro ciclo di vita. Quando avvengono dei cambiamenti nelle piattaforme operative (software di sistema e middleware), le applicazioni critiche per l'Amministrazione devono essere riesaminate e sottoposte a test per assicurare che non ci siano impatti negativi sulle attività operative o sulla sicurezza.

La modifica dei pacchetti software deve essere disincentivata e limitata ai cambiamenti necessari che devono comunque essere strettamente controllati e, contrariamente, incentivato il riuso.

I principi per l'ingegnerizzazione sicura dei sistemi (fase di progettazione) devono essere stabiliti, documentati, manutenuti e applicati ad ogni implementazione di un sistema informativo. L'Amministrazione deve garantire il rispetto di tali principi anche nel caso in cui lo sviluppo dei sistemi informativi sia affidata, completamente o in parte, a terze parti.

L'Amministrazione deve definire e proteggere in modo appropriato gli ambienti di sviluppo dei sistemi e le informazioni e i dati personali in essi caricati, indicando le linee guida per il mascheramento di quelle non rilevanti ai fini dell'attività.

L'Amministrazione deve supervisionare e monitorare le attività di sviluppo dei sistemi affidate all'esterno.

I test relativi alle funzionalità di sicurezza devono essere effettuati almeno prima dell'avvio della fase di collaudo e sempre prima dell'avvio in produzione, in coerenza con le convenzioni vigenti. I dati di test devono essere scelti con attenzione, protetti e tenuti sotto controllo. In particolare, non devono essere utilizzati, ove possibile, dati personali per l'esecuzione di test: qualora non possa essere evitato l'utilizzo di dati personali a scopo di test, l'Amministrazione deve prevedere l'utilizzo di misure tecniche e organizzative equivalenti a quelle utilizzate nell'ambiente di produzione al fine di ridurre al minimo i rischi connessi ai diritti e alle libertà degli interessati.

I test di accettazione dei sistemi devono includere anche la verifica dei requisiti di protezione dei dati personali.

7. INTERPRETAZIONE DELLE POLICY

La responsabilità dell'interpretazione del presente documento è in carico all'Ufficio V dell'Unità di missione per l'attuazione degli interventi del PNRR.

8. GESTIONE DEL DOCUMENTO

I contenuti di questa policy saranno diffusi e promossi a cura dell'Ufficio V dell'Unità di missione per l'attuazione degli interventi del PNRR, in collaborazione con gli altri uffici e dipartimenti interessati. La policy dovrà essere aggiornata periodicamente, almeno con cadenza annuale, i suoi contenuti saranno diffusi in tutte le occasioni di modifica o aggiornamento, o comunque secondo necessità, in relazione a specifici aggiornamenti del panorama normativo in materia di sicurezza informatica, incidenti significativi, variazioni organizzative o mutamenti dell'esposizione alle minacce e ai relativi rischi. In aggiunta, dovrà essere redatto un registro aggiornato, al fine di censire il riesame della presente politica ed eventuali dettagli in riferimento agli esiti ottenuti.