



REGIONE BASILICATA

DIREZIONE GENERALE
AMMINISTRAZIONE DIGITALE

Via Vincenzo Verrastro 6, 85100, Potenza (PZ)

0971 668335

dg.transizionedigitale@cert.regione.basilicata.it



REGIONE BASILICATA

Direzione Generale Amministrazione Digitale

Manuale di gestione della sicurezza informatica

SOMMARIO

1. CONTESTO DI RIFERIMENTO	3
2. OBIETTIVI DEL DOCUMENTO	4
3. DEFINIZIONI E ACRONIMI	5
3.1. DEFINIZIONI	5
3.2. ACRONIMI	6
4. RIFERIMENTI	7
4.1. RIFERIMENTI NORMATIVI	7
4.2. STANDARD DI SETTORE	8
5. MANUALE DI SICUREZZA INFORMATICA	9
5.1. SERVIZI CLOUD OFFERTI DALLA REGIONE	10
5.2. MATRICE DELLA RESPONSABILITA'	10
5.3. GOVERNANCE DELLA SICUREZZA INFORMATICA	11
5.4. ENTERPRISE RISK MANAGEMENT (ERM) PER LA SICUREZZA INFORMATICA ..	12
5.5. GESTIONE DEGLI ASSET INFORMATIVI E DELLE INFORMAZIONI	12
5.6. GESTIONE DEL RISCHIO NELLA CATENA DI FORNITURA	17
5.7. TECNOLOGIE DI PROTEZIONE	17
5.8. GESTIONE DELLE IDENTITA', AUTENTICAZIONE E CONTROLLO ACCESSI	19
6.8.1 SICUREZZA FISICA E AMBIENTE	19
6.8.2 SICUREZZA ATTIVITÀ OPERATIVA	20
5.9. CONSAPEVOLEZZA E FORMAZIONE IN SICUREZZA INFORMATICA	23
5.10. SICUREZZA DEI DATI	24
5.11. MANUTENZIONE E GESTIONE DEL CAMBIAMENTO	26
5.12. MONITORAGGIO CONTINUO DELLA SICUREZZA, GESTIONE ANOMALIE ED EVENTI	26
5.13. GESTIONE DEGLI INCIDENTI E DELLE VULNERABILITA'	27
5.14. GESTIONE DEI BACKUP	29
5.15. BUSINESS CONTINUITY E DISASTER RECOVERY	29
5.16. GESTIONE AUDIT	29

1. CONTESTO DI RIFERIMENTO

La Regione Basilicata ha recentemente potenziato il proprio Data Center per renderlo conforme ai modelli di qualificazione delle infrastrutture e dei servizi cloud emanati dall'Agenzia per la Cybersicurezza Nazionale (ACN). Oggi, tale infrastruttura, certificata secondo lo standard ANSI/TIA-942 (Livello 3), è in grado di offrire servizi cloud a tutti gli enti e le strutture subregionali connesse alla GigaRUPAR (Rete Unitaria della Pubblica Amministrazione Regionale) con livelli di sicurezza coerenti con le linee guida ACN. Elemento centrale di questa infrastruttura è la piattaforma Cloud regionale, in grado di erogare servizi Hosting, IaaS, PaaS, SaaS, in un'ottica Cloud First. La Politica per la sicurezza informatica è adottata e attuata da tutti gli utenti e dalle terze parti coinvolte nella gestione delle informazioni e dei servizi del Data Center regionale.

Il presente documento, in attuazione della Deliberazione della Giunta Regionale (DGR) n.43 del 01/02/2023 ed in conformità al Regolamento (UE) 2016/679, alla Direttiva (UE) 2022/2555 (NIS2), ai requisiti ed al Regolamento per le Infrastrutture Digitali e per i Servizi Cloud per la Pubblica Amministrazione emanati dall'Agenzia per la Cybersicurezza Nazionale, descrive in maniera sintetica le misure di sicurezza messe in atto dalla Regione Basilicata attraverso l'adozione di un proprio Sistema di Gestione della Sicurezza Informatica (SGSI).

Gli enti che intendano richiedere l'accesso ai servizi cloud del Data Center regionale dovranno farlo nel rispetto del suddetto sistema.

2. OBIETTIVI DEL DOCUMENTO

Il presente documento sintetizza i livelli minimi di sicurezza informatica relativi all'infrastruttura ed ai servizi Cloud e le politiche di sicurezza informatica applicabili ai sistemi informativi della Regione Basilicata. La sua finalità è di supportare gli indirizzi strategici regionali e costituire un quadro di riferimento per stabilire gli obiettivi di sicurezza, promuovendo un approccio di miglioramento continuo basato sul rischio, volto a garantire la conformità normativa, la resilienza dei servizi essenziali e la tutela dei diritti e delle libertà fondamentali degli interessati, in coerenza con i principi di accountability e security by design e by default.

3. DEFINIZIONI E ACRONIMI

3.1. DEFINIZIONI

Termine	Descrizione
Policy di Sicurezza Informatica	Insieme di principi, regole e linee guida che regolano la protezione delle informazioni, delle infrastrutture e dei servizi IT, con l'obiettivo di garantirne riservatezza, integrità e disponibilità.
Sistema di Gestione della Sicurezza Informatica (SGSI)	Framework organizzativo e tecnico, conforme alla ISO/IEC 27001, adottato per pianificare, attuare, monitorare e migliorare la sicurezza delle informazioni a tutti i livelli.
ISO/IEC 27001	Standard internazionale che specifica i requisiti per l'implementazione di un SGSI efficace.
Business Impact Analysis (BIA)	Processo per identificare e valutare gli effetti che un'interruzione dei processi critici può avere sull'organizzazione.
Piano di Continuità Operativa (BCP)	Documento che descrive le strategie e le misure per garantire la continuità dei servizi aziendali durante eventi critici.
Piano di Disaster Recovery (DRP)	Strategia e insieme di procedure per il ripristino dei sistemi IT in caso di gravi incidenti.
Inventario degli Asset	Elenco aggiornato di tutti gli asset informatici (hardware, software, dati, persone) per gestirne il ciclo di vita in modo sicuro.
Controllo Accessi	Meccanismi tecnici e procedurali per limitare l'accesso a dati e sistemi solo a utenti autorizzati.
Audit di Sicurezza	Verifiche periodiche per valutare la conformità delle pratiche di sicurezza a politiche e normative vigenti.
Shared Security Responsibility Model (SSRM)	Modello che definisce le responsabilità condivise tra cliente e fornitore nella protezione di dati e infrastrutture, tipico dei servizi Cloud.
Traffic Light Protocol (TLP)	Schema di classificazione dei dati sensibili per comunicare i limiti di condivisione delle informazioni (es. TLP: (LIMITATO)GREEN, TLP: (CONFIDENZIALE)AMBER).
Firewall	Dispositivo o software che controlla il traffico di rete in entrata e uscita per bloccare accessi non autorizzati.
Intrusion Prevention System (IPS)	Sistema che rileva e previene attività malevole nella rete, bloccando gli attacchi in tempo reale.
Indicatori di Compromissione (IoC)	Elementi osservabili (es. file sospetti, IP dannosi) che indicano la presenza di una minaccia.
Web Application Firewall (WAF)	Firewall specifico per proteggere applicazioni web da attacchi comuni come SQL injection e cross-site scripting.
VPN (Virtual Private Network)	Rete privata virtuale che consente connessioni sicure a distanza cifrando i dati trasmessi.
Autenticazione Multi-Fattore (MFA)	Metodo di autenticazione che richiede più di un fattore (es. password + OTP) per garantire un accesso sicuro.

Penetration Test / SAST / DAST / Vulnerability Assessment	Tecniche di analisi e test per identificare vulnerabilità nei sistemi informatici prima della messa in esercizio.
Gestione delle Identità e Accessi (IAM)	Insieme di processi e tecnologie per identificare, autenticare e autorizzare utenti, dispositivi e processi.
Active Directory	Servizio di directory usato per la gestione centralizzata di utenti, dispositivi e risorse di rete.
Credential Management	Gestione delle credenziali (userID, password, certificati) per garantire un uso sicuro e tracciabile delle risorse IT.
Offboarding	Processo di disattivazione e revoca degli accessi e degli account di un dipendente al termine del rapporto lavorativo.
Screensaver con Password	Meccanismo di blocco automatico della postazione inattiva, protetto da password, per prevenire accessi non autorizzati.
Controllo Accessi Fisici	Misure di sicurezza per limitare l'accesso agli edifici e data center solo al personale autorizzato, anche tramite badge, registri e videosorveglianza.
Password Policy	Regole sulla creazione e gestione delle password (es. lunghezza minima, complessità, cambio periodico) per aumentare la sicurezza degli accessi.
Logging e Tracciamento	Registrazione e monitoraggio degli accessi e delle attività degli utenti per fini di sicurezza e audit.
Utenze Privilegiate	Account con diritti amministrativi che devono essere gestiti e monitorati attentamente per ridurre il rischio di abuso o compromissione.
Utente	Personale dipendente interno e personale dipendente esterno.
Denylist/Allowlist	Liste di siti o indirizzi IP bloccati (Denylist) o autorizzati (Allowlist) utilizzate per filtrare il traffico di rete o email.

3.2. ACRONIMI

Termine	Descrizione
ACN	Agenzia per la Cybersicurezza Nazionale
AES	Advanced Encryption Standard
ATC	Assistenza tecnica computer
BIOS	Basic Input/Output System (Sistema di Input/Output di Base)
CEF	Common Event Format
CIE	Carta di Identità Elettronica
COC	Cloud Operation Center - Centro Operativo per i servizi cloud.
CSIRT	Computer Security Incident Response Team
CSV	Comma Separated Values
CTI	Cyber Threat Intelligence
EDR	Endpoint Detection and Response
GDPR	General Data Protection Regulation
IDS	Intrusion Detection System
IP	Internet Protocol

IPS	Intrusion Prevention System
JSON	JavaScript Object Notation
MAC	Media Access Control
MFA	Multi-Factor Authentication
PEC	Posta Elettronica Certificata
RBAC	Role Based Access Control
SAST	Static Application Security Testing
SIEM	Security Information and Event Management
SNMP	Simple Network Management Protocol
SOAR	Security Orchestration, Automation and Response
SLA	Service Level Agreement
SPID	Sistema Pubblico di Identità Digitale
SysLog	System Log
TLP	Traffic Light Protocol
TLS	Transport Layer Security
UEBA	User Entity and Behavior Analytics
VLAN	Virtual LAN
VPN	Virtual Private Network
WAF	Web Application Firewall
XML	eXtensible Markup Language

4. RIFERIMENTI

4.1. RIFERIMENTI NORMATIVI

- **Framework AgID per la Pubblica Amministrazione:** linee guida e raccomandazioni per l'adozione di standard e pratiche volte a garantire la sicurezza informatica e la protezione dei dati;
- **Regolamento UE 2016/679 o GDPR (General Data Protection Regulation):** misure tecniche e organizzative adeguate a garantire la sicurezza dei dati che le aziende devono implementare;
- **Decreto Legislativo 10 agosto 2018, n. 101 (D.Lgs. 196/2003, noto come Codice in materia di protezione dei dati personali):** principale legge italiana che regola il trattamento dei dati personali per adeguarlo al Regolamento (UE) 2016/679 (GDPR - General Data Protection Regulation), entrato in vigore il 25 maggio 2018;
- **Direttiva NIS2:** ufficialmente conosciuta come **Direttiva (UE) 2022/2555**, revisione e ampliamento della **Direttiva NIS** (Network and Information Security) del 2016. La direttiva mira a rafforzare ulteriormente la resilienza e la sicurezza informatica all'interno dell'UE, affrontando le crescenti minacce cyber nei settori critici;

- **Il Regolamento unico per le infrastrutture digitali e i servizi cloud della Pubblica Amministrazione** è stato adottato dall'Agenzia per la Cybersicurezza Nazionale (ACN) il 27 giugno 2024 (prot. n. 0021007.27-06-2024.I).
- **Decreto Legislativo 4 settembre 2024, n. 138:** recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cybersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148. (24G00155);
- **D. Lgs. 82/2005 e ss.mm.ii.,** "Codice dell'Amministrazione digitale";
- **D. Lgs. 81/2008 e ss.mm.ii.,** "Testo Unico sulla sicurezza";
- **D.P.R. 62/2013** "Codice di comportamento dei dipendenti della pubblica Amministrazione";
- **D.G.R. n°44 del 01 febbraio 2023:** Art. 54 del D. Lgs. n. 165/2001 - Approvazione aggiornamento del Codice di comportamento dei dipendenti della Giunta regionale;
- Contratto Collettivo Nazionale di Lavoro e Contratto Collettivo Decentrato Integrativo
- **Provvedimento del Garante 27 novembre 2008:** misure di sicurezza che devono essere adottate per la gestione dei Log degli amministratori di sistema.
- **Provvedimento del Garante n. 209/2021** sulla procedura telematica per la notifica dei data breach.
- **Deliberazione D.G.R. n. 43 del 01/02/2023,** la Regione Basilicata ha aderito al modello di qualificazione della ACN (Agenzia per la Cybersicurezza Nazionale) n. 307 del 18 gennaio 2022 e n. 29 del 2 gennaio 2023 e con decreto direttoriale n. 21007/24 del 27 giugno 2024 (regolamento unico per le infrastrutture e i servizi cloud per la PA).
- **Deliberazione D.G.R. n. 483 del 10/08/2023,** ha ammesso a finanziamento il potenziamento dei servizi di Disaster Recovery, a seguito delle nuove linee guida ACN.
- **Con D.D. n.16BJ.2024/D.01076 del 27/12/2024** è stato istituito un centro di competenze per la risposta agli incidenti informatici con il compito di pianificare ed eseguire attività di sicurezza proattive e reattive volte a prevenire e rispondere attacchi informatici all'interno del territorio regionale.
- **Deliberazione D.G.R. n. 722 del 27/11/2025** "Approvazione disciplinare sull'utilizzo delle dotazioni informatiche della Giunta della Regione Basilicata".
- **Deliberazione D.G.R. n. 724 del 27/11/2025** "Governance delle infrastrutture e dei servizi digitali della Regione Basilicata".

4.2. STANDARD DI SETTORE

- **NIST SP800-92 - Guide to Computer Security Log Management:** pubblicazione riconosciuta a livello internazionale che fornisce raccomandazioni e linee guida per la gestione dei log di sicurezza informatica;

- **ISO/IEC 27001:2022:** standard internazionale pubblicato dall'**International Organization for Standardization (ISO)** e dall'**International Electrotechnical Commission (IEC)** che definisce i requisiti per un **Sistema di Gestione della Sicurezza delle Informazioni (ISMS, Information Security Management System)**. La versione 2022 aggiorna la precedente ISO/IEC 27001:2013. Questo standard richiede che le organizzazioni adottino controlli per la protezione delle informazioni, tra cui l'uso di meccanismi crittografici per garantire la riservatezza, l'integrità e la disponibilità dei dati;
- **ISO/IEC 27002:2022:** standard internazionale complementare a ISO/IEC 27001 fornisce linee guida dettagliate per l'implementazione delle misure di sicurezza dell'informazione. Offre una serie di raccomandazioni e best practice per applicare i controlli di sicurezza previsti da ISO/IEC 27001, inclusi quelli relativi alla gestione dei Log (Log management);
- **COBIT "Control Objectives for Information and related Technology" (modello di riferimento per il governo dell'IT):** framework progettato per la governance e la gestione dell'IT, che include la gestione della sicurezza delle informazioni.

5. MANUALE DI SICUREZZA INFORMATICA

Il presente documento definisce una sintesi sulle linee di indirizzo e i principi generali per la gestione dei livelli minimi di sicurezza informatica relativi all'infrastruttura tecnologica e ai servizi Cloud, in conformità alla normativa vigente e alle linee guida emanate dalle Autorità competenti.

Tali misure sono adottate al fine di garantire la continuità operativa dei servizi erogati, assicurandone l'efficacia e l'efficienza, nonché di tutelare:

- la riservatezza dei dati e delle informazioni, sia residenti sui sistemi sia in fase di trasmissione, prevenendo accessi non autorizzati;
- l'integrità dei dati e delle informazioni, sia residenti sui sistemi sia in transito, mediante l'adozione di misure tecniche e organizzative idonee a prevenire alterazioni intenzionali o accidentali;
- la disponibilità dei dati e delle informazioni, sia residenti sui sistemi sia in transito, garantendone l'accessibilità e la fruibilità continua e proteggendoli da eventi che possano comprometterne l'operatività;
- la protezione dei dati personali, nel rispetto della normativa vigente in materia di protezione dei dati personali, assicurando adeguate misure di sicurezza volte a prevenire perdite, distruzioni, alterazioni o trattamenti non autorizzati, sia intenzionali sia accidentali.

Le politiche, i processi e le procedure di sicurezza sono oggetto di aggiornamento periodico, con cadenza prestabilita, e comunque a seguito di modifiche rilevanti di carattere normativo, tecnologico o organizzativo, al fine di garantirne nel tempo la perdurante idoneità, adeguatezza ed efficacia.

5.1. SERVIZI CLOUD OFFERTI DALLA REGIONE

La Regione offre servizi cloud progettati per assicurare autonomia tecnologica, controllo diretto sul dato, cyber-resilienza, conformità ai requisiti di classificazione del dato (allineamento alle direttive ACN). Inoltre, offre soluzioni cloud più adatte a garantire innovazione ma anche privacy, sicurezza, compliance, efficienza e sovranità del dato come si evince dalla seguente figura:

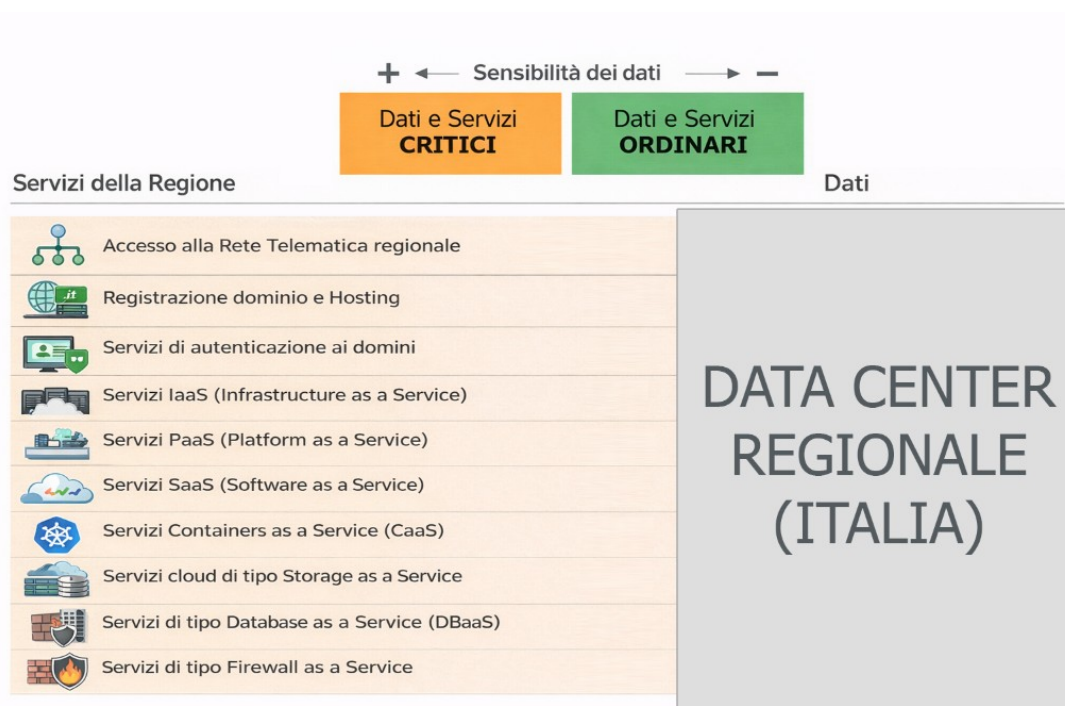


Figura n.1 Caratteristiche dei servizi cloud regionali

5.2. MATRICE DELLA RESPONSABILITA'

Le responsabilità di sicurezza fra Direzione/Ente/Azienda e provider sono formalizzate da un'apposita Matrice di Responsabilità Condivisa di sicurezza:

IaaS	CaaS	SaaS	PaaS	BaaS
Data	Data	Data	Data	Data
Applications	Applications	Applications	Applications	Applications
Operating System	Operating System	Operating System	Operating System	Operating System
Virtual Machine	Virtual Machine	Virtual Machine	Virtual Machine	Virtual Machine
Hardware	Hardware	Hardware	Hardware	Hardware
Network	Network	Network	Network	Network
Physical	Physical	Physical	Physical	Physical

Regione
Direzione/Ente/Azienda
Direzione/Ente/Azienda/Regione previa autorizzazione

Tabella n.1 Matrice di Responsabilità

Ruoli di sicurezza:

Ruolo	Responsabilità
Referente NIS2	Garantire la conformità alla Direttiva NIS2; Coordinare misure di sicurezza; Gestire valutazioni dei rischi; Rapporti con autorità; Audit e miglioramento; Definizione di policy e procedure
Supporto al Referente NIS2	Supporto operativo al referente; Gestione evidenze; Aggiornamento documentazione; Monitoraggio misure di sicurezza; Coordinamento team; Supporto audit
Referente CSIRT	Gestione rapporto con CSIRT nazionale; Coordinamento incident response; Raccolta e trasmissione dati; Notifica incidenti; Aggiornamento procedure; Formazione del personale
DPO	Garantire la conformità al GDPR; Sorvegliare l'applicazione delle norme sulla protezione dei dati; Gestire relazioni con il Garante; Supervisionare valutazioni di impatto (DPIA); Fornire consulenza interna; Monitorare processi di trattamento dei dati

Tabella n.2 Matrice Ruoli Sicurezza

5.3. GOVERNANCE DELLA SICUREZZA INFORMATICA

La Regione Basilicata definisce la propria struttura organizzativa (organigramma consultabile all'interno del sito istituzionale), la mappa dei processi e le procedure fondamentali per garantire la conformità ai requisiti normativi, legali, contrattuali delle parti interessate in materia di sicurezza informatica, il tutto come specificamente dettagliato nel framework Sistema di Gestione della Sicurezza Informatica (SGSI) adottato in conformità alla norma ISO 27001. La Regione individua gli obiettivi di sicurezza informatica in linea con la politica e la strategia regionale, li assegna ai pertinenti processi e ne monitora le prestazioni attraverso un apposito cruscotto di indicatori.

Tale sistema disciplina la pianificazione, l'implementazione, la valutazione e il miglioramento continuo della sicurezza informatica a tutti i livelli organizzativi, coinvolgendo l'utente nonché, considerando il ruolo e le responsabilità ricoperte all'interno dell'Ente. Le attività del SGSI sono definite in funzione dei rischi per la sicurezza e la privacy dell'infrastruttura, dell'Analisi di Impatto sul Business (BIA), del Piano di Continuità Operativa (BCP) e del Piano di Disaster Recovery (DRP).

La documentazione (policy, processi, procedure) sono pubblicate nella rete interna regionale.

5.4. ENTERPRISE RISK MANAGEMENT (ERM) PER LA SICUREZZA INFORMATICA

La Regione implementa un processo di Enterprise Risk Management (ERM), specificamente orientato a garantire la sicurezza dei dati e dei propri sistemi, utilizzando un processo ciclico e in continua evoluzione, nella consapevolezza che nuovi bisogni, minacce emergenti e obblighi normativi richiedono un aggiornamento costante. Tutti gli interventi vengono pianificati a partire da un'attività strutturata di analisi del rischio, che ha lo scopo di individuare le possibili minacce, valutarne le conseguenze, definire le misure di protezione realmente necessarie e stabilire le priorità di intervento.

Tale processo include le seguenti attività:

- **modellazione del Perimetro:** rappresentazione del perimetro tramite un modello articolato in Sistemi e Componenti (asset)
- **Classificazione:** determinazione dell'importanza (criticità) degli asset e, conseguentemente, della necessità di proteggerli
- **Identificazione e Valutazione dei Rischi:** identificare e valutare regolarmente i rischi per la sicurezza informatica e la protezione dei dati personali.
- **Assegnazione delle Responsabilità:** definire e assegnare le responsabilità per la gestione di ciascun rischio identificato.
- **Selezione delle contromisure pertinenti:** applicare controlli di sicurezza adeguati ed efficaci per mitigare i rischi.
- **Accettazione dei Rischi Residui:** formalizzare l'accettazione consapevole e documentata dei rischi residui.

La valutazione dei rischi di sicurezza informatica è condotta con cadenza annuale, salvo modifiche significative che impattino sul contesto tecnologico regionale. I report finali derivanti dal processo ERM sono oggetto di revisione e approvazione.

5.5. GESTIONE DEGLI ASSET INFORMATIVI e DELLE INFORMAZIONI

La Regione Basilicata adotta misure sistematiche per la gestione efficace degli asset informativi, comprendenti dati, utenti, dispositivi, sistemi e infrastrutture. L'obiettivo primario è controllare l'introduzione di nuovi asset, gestire la loro rimozione o aggiornamento e prevenire utilizzi non autorizzati. Questo è realizzato attraverso i seguenti processi fondamentali:

- **Inventario degli Asset:** Viene mantenuto un inventario dettagliato e aggiornato di tutti gli asset informativi, inclusi sistemi, apparati fisici, piattaforme software, applicazioni, dispositivi portatili e fissi, e supporti di archiviazione di massa in uso

presso la Regione Basilicata. A tal fine, si utilizzano piattaforme software e politiche di sicurezza su dispositivi, server e workstation, che consentono di implementare il Catalogo Applicativo e l'inventario digitale dei dispositivi e apparati hardware.

- **Classificazione dell'Informazione:** Le informazioni sono gestite e protette in modo proporzionale alla loro importanza e criticità.

La classificazione delle informazioni relative alla documentazione di sicurezza è effettuata dal Titolare dell'Informazione (Information Owner), individuato tra i responsabili delle strutture che producono o gestiscono le informazioni rilevanti per il sistema di sicurezza a seconda dell'area di competenza (IT, DPO, Network, Sicurezza, Cloud). Ogni Titolare assegna il livello TLP appropriato in base alla sensibilità e agli impatti. Il Responsabile della Sicurezza delle Informazioni supporta l'attività e ne verifica la coerenza.

La Regione utilizza lo schema TLP v 2.0 (Traffic Light Protocol) definito dall'Agenzia per la Cybersicurezza Nazionale (ACN). La classificazione è articolata su quattro livelli:

- **Pubblico (livello di sicurezza 1 (CLEAR)).** Si riferisce ad informazioni che non richiedono protezione specifica e la loro libera diffusione all'interno o all'esterno dell'Amministrazione non comporta rischi.
- **Limitato o interno (livello di sicurezza 2 (GREEN)).** Si riferisce ad informazioni la cui diffusione all'interno dell'Amministrazione è libera, mentre all'esterno è consentita solo se la stessa è regolamentata da appositi accordi di riservatezza stipulati con entità esterne. La loro diffusione non autorizzata, la perdita, la manomissione o l'uso indebito, possono arrecare un danno all'Amministrazione. Sono classificati a questo livello, ad esempio:
 - Dati personali, salvo particolari esigenze
 - Documenti e procedure relative al corpus documentale elaborato nell'ambito dell'Amministrazione (es. Policy gestione Documentale SGSI; Gestione delle registrazioni; Programma e procedura di audit; Policy di Incident Management e criteri di classificazione degli incidenti di sicurezza).
- **Confidenziale (livello di sicurezza 3 (AMBER)).** Si riferisce ad informazioni rilevanti ai fini della sicurezza e che pertanto richiedono protezione specifica. La loro diffusione all'interno dell'Amministrazione è ammessa solo a gruppi rientranti nella lista di distribuzione preventivamente condivisa ed autorizzata dall'Amministrazione (ad es. RTI, Amministrazioni, Consip/AgID, ACN); all'esterno è invece vietata. La loro diffusione non autorizzata, la perdita, la manomissione o l'uso indebito, possono arrecare un danno all'Amministrazione. Sono classificati a questo livello, ad esempio:
 - Dati particolari, personali sensibili e giudiziari, salvo esigenze più restrittive

- Documenti e supporti rimovibili contenenti dati appartenenti alle Amministrazioni (salvo diversa indicazione delle Amministrazioni clienti)
- Documenti e procedure relative al corpus documentale elaborato nell'ambito del progetto critici ai fini della sicurezza (specifiche di progettazione, configurazione, di indirizzamento, ecc.)
- Log di sicurezza
- Report dei livelli di servizio
- Documenti oggetto della presente fornitura (Es. Piano di sicurezza del Centro Servizi; Rapporti di Audit; Rapporti sugli Incidenti).
- **Strettamente Confidenziale (livello di sicurezza 4 (AMBER+STRICT))**. Si riferisce ad informazioni di particolare rilevanza la cui diffusione può arrecare un pericolo immediato dal punto di vista della sicurezza od un danno notevole per la conduzione dei sistemi IT. La loro diffusione all'interno dell'Amministrazione è ammessa solo ai nominativi rientranti nella lista di distribuzione (lista ad personam), preventivamente condivisa ed autorizzata dall'Amministrazione, mentre all'esterno è vietata. La loro diffusione non autorizzata, la perdita, la manomissione o l'uso indebito possono arrecare danni gravissimi, in alcuni casi irreversibili, all'Amministrazione. Sono classificati a questo livello:
 - Password e le chiavi di crittografia sono classificate a questo livello.
 - Risultati verifiche di sicurezza (Vulnerability Assessment e Penetration Test)
 - Documenti (Es. Valutazione dei rischi; Riesame del SGSI; Report degli incidenti, Criticità e Malfunzionamenti).

		LIVELLI DI CLASSIFICAZIONE			
		Pubblico/CLEAR	Limitato/GREEN	Confidenziale/AMBER	Strettamente confidenziale/AMBER + STRICT
Tipologia destinataria	Interno all'Amministrazione	Nessuna restrizione	Nessuna restrizione	Lista di distribuzione	Lista di distribuzione nominativa
	Terze parti in rapporto con i fornitori e Amministrazione	Nessuna restrizione	Soggetti identificati	Solo destinatari presenti nella lista di distribuzione	Solo soggetti identificati nominativamente nella lista di distribuzione
	Media / Altri	Nessuna restrizione	Non ammessa	Non ammessa	Non ammessa

- **Gestione degli Accessi:** in conformità con le politiche di controllo degli accessi è consentito l'accesso alle informazioni, ai sistemi IT e alle risorse dell'Amministrazione solo a persone autorizzate, secondo il principio del least privilege e in base al ruolo, alle mansioni e alla reale necessità di utilizzo. Tutti gli accessi logici sono gestiti e controllati dal COC attraverso procedure formali.

In particolare, l'amministrazione garantisce:

- L'accesso ai sistemi informativi da parte dei soli utenti autorizzati secondo procedure formali di registrazione;
 - l'uso di user-id univoche;
 - l'assegnazione e l'uso dei soli privilegi necessari per lo svolgimento delle mansioni affidate;
 - la conduzione di processi formali di revisione dei diritti di accessi degli utenti ad intervalli regolari;
 - l'utilizzo di account personali e l'assegnazione di password attraverso strumenti e processi di gestione formali. In tutti i casi è richiesto il cambio password al primo accesso.
- **Erogazione dei Servizi IT:** L'attivazione e la fornitura dei servizi IT sono gestite in linea con le politiche di sicurezza stabilite.
 - **Crittografia:** La Regione garantisce un uso corretto ed efficace della crittografia, regolando sia i controlli crittografici sia la gestione delle chiavi, con l'obiettivo di proteggere riservatezza, integrità, autenticità e non ripudio delle informazioni. In particolare, applica le seguenti regole:
 - Utilizzo di meccanismi di cifratura adeguati al valore e al livello di classificazione delle informazioni, secondo standard riconosciuti e costantemente aggiornati.
 - Divieto di memorizzare o trasmettere password in forma reversibilmente cifrata: le credenziali utente sono protette tramite funzioni di hashing robuste e non invertibili.
 - Protezione dei dati sia "in transit" sia "at rest" mediante algoritmi crittografici solidi (es. AES-256) e protocolli sicuri (es. TLS nelle versioni supportate), evitando algoritmi deprecati o soluzioni crittografiche personalizzate.
 - Scelta di tecniche e lunghezze delle chiavi proporzionate al livello di rischio e al ciclo di vita delle informazioni da proteggere.
 - **Audit di Sicurezza:** Vengono condotti audit periodici per verificare la conformità alle politiche e alle procedure di sicurezza relative alla gestione degli asset.

L'esecuzione di queste attività è strettamente correlata alla valutazione dei rischi di sicurezza informatica.

I dispositivi informatici forniti dalla Regione Basilicata sono strumenti di lavoro di proprietà dell'Amministrazione e, in quanto tali, sono soggetti alle seguenti disposizioni per garantirne la sicurezza e l'uso appropriato:

- **Custodia e Diligenza:** Ogni dipendente è responsabile della custodia e dell'utilizzo diligente del dispositivo assegnato, adottando tutte le precauzioni

necessarie per prevenirne danni, smarrimento o sottrazione. In particolare, i dispositivi portatili non devono essere lasciati incustoditi in luoghi non sicuri (uffici aperti, sale riunioni, veicoli parcheggiati) e, al termine dell'orario lavorativo o in caso di inutilizzo, devono essere riposti in armadi/locali chiusi a chiave o assicurati con apposito cavetto di sicurezza.

- **Utilizzo Professionale:** I dispositivi informatici devono essere utilizzati esclusivamente per scopi professionali e per l'archiviazione di dati inerenti all'attività lavorativa. Fatto salvo quanto previsto dall'art. 21, punto 2 del Codice di Comportamento dei Dipendenti della Giunta Regionale, è severamente vietato qualsiasi utilizzo non correlato al lavoro, in quanto ciò può causare disservizi, incrementare i costi di manutenzione e, soprattutto, esporre il sistema a minacce per la sicurezza.

- **Configurazione Standard:** Le impostazioni hardware e software dei PC e dei relativi programmi sono preconfigurate dall'ATC in base a criteri e profili definiti dall'Amministrazione, tenendo conto della qualifica, delle mansioni del dipendente e delle politiche di utilizzo degli strumenti IT.

Non è consentita l'installazione autonoma di software proveniente da fonti esterne senza previa ed esplicita autorizzazione del responsabile della sicurezza, al fine di prevenire l'introduzione di virus e altri software dannosi che potrebbero compromettere seriamente la sicurezza informatica.

L'utilizzo di programmi diversi da quelli distribuiti e installati ufficialmente tramite il software center regionale è proibito. La mancata osservanza di questa disposizione può causare danni al sistema per incompatibilità software ed esporre la Regione a responsabilità civili e penali per violazione delle normative sul diritto d'autore.

È vietato agli utenti modificare le configurazioni predefinite del proprio PC senza previa autorizzazione esplicita dell'Ufficio competente. Inoltre, il personal computer deve essere spento al termine dell'orario lavorativo o in caso di assenze prolungate.

Solo il personale autorizzato dell'ATC è abilitato a effettuare interventi tecnici sui dispositivi per garantirne la sicurezza, la salvaguardia e per attività di manutenzione (aggiornamento, sostituzione, implementazione di programmi, manutenzione hardware, ecc.).

L'attivazione di password all'accensione del PC (BIOS) non è consentita senza preventiva autorizzazione dell'ATC. Il personale incaricato dell'ATC ha la facoltà di connettersi e visualizzare in remoto il desktop delle postazioni PC per fornire assistenza tecnica, garantire la normale operatività e assicurare la massima sicurezza contro virus, spyware, malware e altre minacce.

Ogni utente deve prestare la massima attenzione ai supporti di memorizzazione esterni, ove consentiti, e segnalare immediatamente al personale dell'ATC qualsiasi anomalia o sospetto rilevamento di virus.

Per un maggiore dettaglio si rimanda al Disciplinare sull'utilizzo delle dotazioni informatiche della Giunta della Regione Basilicata.

Gli aggiornamenti dell'infrastruttura tecnologica sono eseguiti a seguito di verifiche puntuali del COC, che analizza i bollettini di sicurezza per i vari ambiti e applica le necessarie correzioni e gli aggiornamenti di sicurezza ai sistemi operativi client e server. In caso di rischio valutato come irrilevante, l'attività di manutenzione straordinaria viene programmata; qualora l'impatto sia bloccante per l'operatività dei servizi regionali, si interviene con urgenza.

5.6. GESTIONE DEL RISCHIO NELLA CATENA DI FORNITURA

La Regione Basilicata garantisce che i rapporti con i Fornitori che accedono alle informazioni o agli asset regionali siano gestiti nel rispetto di rigorosi requisiti di sicurezza. In particolare, prevede accordi di riservatezza validi anche dopo la fine del contratto, l'identificazione e la mitigazione dei rischi legati all'accesso di terze parti tramite controlli di sicurezza specifici, e l'informazione del personale sui controlli e sulle norme di sicurezza da rispettare. L'accesso logico e fisico del personale esterno è consentito solo secondo procedure formalizzate, previa identificazione e registrazione. La Regione monitora costantemente il rispetto dei requisiti di sicurezza da parte dei Fornitori attraverso strumenti e processi di gestione adeguati. La Regione Basilicata adotta un approccio strutturato per identificare, valutare e gestire i rischi associati all'intera catena di approvvigionamento di beni e servizi IT. Inoltre, nella selezione dei fornitori, la Regione si attiene alle seguenti norme e principi fondamentali:

- **Codice dei Contratti Pubblici** (D.Lgs. 36/2023).
- **Standard di Qualificazione ACN per Servizi Cloud:** I fornitori di servizi Cloud devono soddisfare gli standard di qualificazione definiti dall'Agenzia per la Cybersicurezza Nazionale (ACN).
- **Conformità allo Standard ISO 27001:** I fornitori devono essere conformi allo standard ISO 27001 nei seguenti casi:
 - Il fornitore è designato come amministratore di sistema.
 - Il fornitore è designato come responsabile del trattamento di categorie particolari di dati personali (ai sensi dell'art. 9 del GDPR).
 - Il fornitore è coinvolto in processi critici a supporto dei servizi erogati dalla Regione.

La qualità dei servizi erogati dai fornitori è soggetta a revisione annuale, salvo modifiche significative del contesto tecnologico regionale che richiedano una revisione anticipata.

5.7. TECNOLOGIE DI PROTEZIONE

La Regione adotta un insieme strutturato di regole e misure di sicurezza volte a garantire la protezione delle informazioni nell'infrastruttura di rete regionale utilizzata

per l'erogazione dei servizi, assicurando la sicurezza dei dati sia nei flussi interni sia nei collegamenti verso le Amministrazioni e gli Enti collegati.

Per garantire un elevato livello di sicurezza dei propri sistemi informatici e dei dati gestiti, la Regione Basilicata implementa i seguenti principi e tecnologie di protezione:

- **Segregazione e Segmentazione di Rete:** Le aree amministrative, di archiviazione dati e di elaborazione sono logicamente separate e segmentate. L'utilizzo di domini virtuali (VDM) definiti sui firewall e la suddivisione a livello di rete realizzata tramite Virtual Local Area Networks (VLAN) consentono la configurazione e l'applicazione di criteri di accesso differenziati in base alla tipologia di utenza.
- **Limitazione e Monitoraggio di Porte, Protocolli e Servizi:** L'utilizzo delle porte di rete, dei protocolli di comunicazione e dei servizi attivi è limitato a quanto strettamente necessario e costantemente monitorato.
- **Firewall e Sistemi di Prevenzione delle Intrusioni (IPS):** I firewall e i sistemi IPS sono mantenuti aggiornati, correttamente configurati e sottoposti a manutenzione continua. Filtri IPS specifici sono applicati ai servizi esposti su Internet, unitamente alla verifica degli Indicatori di Compromissione (IoC), al fine di bloccare attacchi noti prima che raggiungano le applicazioni e registrarli nel sistema di logging centralizzato.
- **Blocco Accessi a Siti Web Pericolosi:** L'accesso a siti web catalogati come fonti di phishing, spam o classificati come pericolosi da database specializzati (denylist) è bloccato.
- **Sistema Antispam per la Posta Elettronica:** È implementato un sistema antispam con configurazioni specifiche per i diversi gruppi di utenti. Tale sistema consulta denylist pubbliche ed esegue controlli preliminari, categorizza e blocca le e-mail SPAM, verificando l'indirizzo IP del mittente, gli URL contenuti, rilevando URL di phishing e la presenza di virus e malware, controllando il checksum delle e-mail, invio limitato di mail-list(max. 5 utenze).
- **WAF (Web Application Firewall):** Le applicazioni WEB pubblicate su Internet sono protette tramite l'implementazione di un Web Application Firewall (WAF) configurato con specifici requisiti di sicurezza anche per prevenire attacchi di tipo DDoS.
- **Filtri Web Reputation e Antivirus per Accesso Internet Client:** L'accesso a Internet dalla rete dei client è protetto tramite l'implementazione di filtri di web reputation e software antivirus.
- **VLAN Segregate con Controlli di Sicurezza:** Sono configurate e mantenute VLAN (Virtual Local Area Networks) segregate con un numero ristretto di host autorizzati. Le VLAN sono connesse al firewall, integrate con switch di centro stella e sulle policy di traffico interno e di navigazione internet sono applicati filtri antivirus, IPS, sistemi di rilevamento e prevenzione da attacchi DoS (Denial of Service). Questa architettura è utilizzata anche per gli accessi da parte degli enti connessi direttamente alla rete regionale. La classe IP utilizzata nella rete regionale è privata

e le pubbliche amministrazioni connesse adottano un piano di indirizzamento IP compatibile.

- **Accesso Remoto Sicuro tramite VPN:** L'accesso remoto per attività lavorative a distanza e per attività di manutenzione è consentito tramite connessioni VPN (Virtual Private Network) che utilizzano l'autenticazione Multi-Fattore (MFA), la cifratura dei dati e il controllo di integrità dei pacchetti di rete.
- **Test di Sicurezza su Sistemi Critici:** In base all'analisi del rischio, sulle piattaforme e sulle applicazioni software ritenute critiche vengono eseguiti penetration test, analisi statica del codice (SAST), analisi dinamica delle applicazioni (DAST) e vulnerability assessment prima della loro messa in esercizio.
- **Crittografia**, pseudonimizzazione, anonimizzazione e scrambling quali misure di sicurezza specifiche per la Data Protection.
- **Threat Intelligence:** Raccolta e analisi di informazioni al fine di caratterizzare possibili minacce cyber dal punto di vista tecnico, di risorse, di motivazioni e di intenti, spesso in relazione a contesti operativi specifici.
- **SIEM, Log Management e SOAR:** Gestione automatizzata analisi log, Windows Event, Database, Application, Syslog e sistema di risposta automatica agli incidenti tramite l'implementazione di playbook.

L'infrastruttura di rete è **documentata in modo completo e costantemente aggiornata**; le informazioni relative alla topologia, alle configurazioni e agli apparati sono protette da accessi non autorizzati e conservate in modo da garantirne l'inalterabilità. La rete regionale è sottoposta a **monitoraggio continuo**, mediante sistemi di discovery e controllo in grado di individuare eventuali dispositivi non autorizzati. La gestione della sicurezza è supportata dalla raccolta, correlazione e analisi dei log generati dagli apparati di rete e di sicurezza. Ogni modifica alle configurazioni hardware e software è effettuata tramite un **processo strutturato di change management**. Le misure tecnologiche, integrate con quelle fisiche e organizzative, assicurano i principi fondamentali di **riservatezza, integrità e disponibilità** delle informazioni e dei servizi. L'architettura di sicurezza regionale è articolata su più livelli e strati di protezione, supportata dall'utilizzo di strumenti di sicurezza enterprise idonei a garantire le principali capacità di sicurezza logica.

5.8. GESTIONE DELLE IDENTITÀ, AUTENTICAZIONE E CONTROLLO ACCESSI

6.8.1 Sicurezza Fisica e Ambiente

Comprende l'insieme delle misure volte a prevenire, rilevare e gestire **minacce esterne ed eventi ambientali**, assicurando la continuità operativa e la tutela delle persone e delle infrastrutture. Tali misure includono sistemi antincendio e antiallagamento, alimentazione elettrica di emergenza, protezione contro le scariche atmosferiche e misure preventive strutturali e organizzative, nel rispetto delle

normative vigenti in materia di salute e sicurezza e conformi agli standard ISO/IEC 27001 e ANSI/TIA-942, con particolare riferimento alla sicurezza fisica e ambientale.

Le misure sono finalizzate a rilevare, segnalare e impedire accessi non autorizzati al sito e alle aree interne sensibili. Il sistema si basa su una combinazione di personale dedicato (guardiania, centrale operativa e reception) e soluzioni tecnologiche avanzate, quali videosorveglianza, sistemi antintrusione perimetrali e interni, recinzioni, varchi controllati e tornelli. L'accesso alle aree sicure è consentito esclusivamente a personale autorizzato tramite badge, mentre visitatori e fornitori sono soggetti a procedure di autorizzazione e registrazione. Le aree critiche e gli impianti IT sono fisicamente segregati e accessibili solo al personale abilitato.

Le porte dei locali tecnici sono di tipo tagliafuoco e si ha accesso tramite strumenti sicuri (es. Badge, OTP). I locali tecnici sono serviti da sensori di rilevamento della temperatura e fumo, da impianti di condizionamento che ne garantiscono l'adeguato livello di temperatura di esercizio, da dispositivi manuale per l'estinzione degli incendi e da pavimento flottante per proteggere gli apparati da eventuali allagamenti di modesta entità.

L'asset dell'Ente regione si distingue in due tipologie:

1. Asset Primario

- Informazioni e dati;
- Processi e attività dell'Ente Regionale

2. Asset di supporto

- Hardware
- Software
- Rete
- Personale
- Siti
- Struttura del Data Center Regionale

6.8.2 Sicurezza attività operativa

Al fine di garantire la continuità e l'affidabilità dei servizi, tutti i sistemi messi in esercizio, dedicati o condivisi, sono sottoposti a valutazioni iniziali e periodiche di efficienza e capacità.

Per la protezione da software dannosi, sono adottate soluzioni anti-malware dedicate e iniziative di sensibilizzazione del personale alla sicurezza informatica. L'utilizzo di dispositivi mobili e/o dispositivi personali è vietato se non espressamente autorizzato. Il monitoraggio degli accessi e dell'uso dei sistemi è assicurato tramite un sistema strutturato di gestione dei log, che prevede la registrazione, conservazione protetta e verifica periodica degli eventi di sicurezza, delle attività degli utenti e degli amministratori di sistema. Questi ultimi, nel rispetto della normativa vigente e dei provvedimenti del Garante per la protezione dei dati personali, sono nominativamente

identificati; le loro attività sono soggette a tracciamento mediante registrazione degli accessi logici (login, logout, tentativi falliti ed eventi rilevanti), assicurando completezza e inalterabilità dei log. Tali registrazioni sono conservate per un periodo non inferiore a sei mesi, così da consentire verifiche sul loro operato e individuare eventuali anomalie di sicurezza.

Per prevenire lo sfruttamento di vulnerabilità tecniche, vengono effettuate verifiche di sicurezza periodiche su tutta l'infrastruttura tecnologica coinvolta nell'erogazione dei servizi.

L'accesso ai sistemi, alle applicazioni e ai dati, avviene tramite il sistema di autenticazione (CIE, eIDAS, SPID e Token), mentre l'accesso alla VPN avviene tramite le credenziali di tipo a fattore multiplo in funzione del principio di segregazione dei ruoli/separazione delle funzioni, in modo che l'accesso amministrativo ai dati, le capacità di crittografia e gestione delle chiavi e le capacità di registrazione siano distinte e separate e commisurate al rischio della transazione.

L'accesso al PC è protetto da codice identificativo e password (credenziali) che devono essere custoditi con la massima diligenza e non divulgate. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente "User ID", associato ad una parola chiave "password", robusta, personale e riservata, nel rispetto dei criteri definiti nelle apposite procedure di accesso e autenticazione.

Le credenziali di autenticazione per l'accesso ai dispositivi ed alla rete vengono predisposte dal centro operativo per il cloud all'atto dell'assunzione del nuovo dipendente in seguito a confacente comunicazione della struttura Gestione Risorse Umane e devono essere obbligatoriamente modificate al primo accesso. Tale utenza viene associata automaticamente a un account di posta elettronica. L'indirizzo e-mail generato sarà utilizzato per tutte le comunicazioni ufficiali, interne ed esterne, e per l'accesso ai servizi digitali forniti dall'organizzazione. L'account di posta elettronica è considerato uno strumento di lavoro ed è soggetto a politiche specifiche sull'uso corretto degli strumenti informatici. L'utente è responsabile della custodia delle proprie credenziali e dell'utilizzo conforme alle normative vigenti in materia di privacy, sicurezza.

La password di accesso alla rete ha un periodo di validità limitato. In caso di non utilizzo prolungato l'account viene bloccato precauzionalmente. In caso di estinzione del rapporto contrattuale con l'utente, la struttura Gestione Risorse Umane aggiorna la data di cessazione, e attraverso l'apposito servizio di notifica, il reparto del COC è informato tempestivamente e provvede a disattivare immediatamente l'account personale dell'utente al fine di garantire la sicurezza degli accessi e la protezione dei dati trattati dall'Amministrazione.

Contestualmente, la casella di posta elettronica associata all'account viene disattivata e configurata con un autorisponditore generico o funzionale, finalizzato a indirizzare i mittenti verso gli uffici competenti. Per garantire il rispetto dei principi di minimizzazione e necessità, non è previsto alcun reindirizzamento automatico verso altre caselle o destinatari.

Qualora, in casi eccezionali e limitati, si renda necessario accedere ai contenuti della casella per assicurare la continuità di un procedimento amministrativo, l'accesso potrà avvenire esclusivamente nell'ambito di una procedura straordinaria, che prevede:

- verifica della base giuridica idonea al trattamento dei dati;
- parere del DPO;
- aggiornamento dell'informativa, ove necessario;
- tracciamento e verbalizzazione delle attività svolte;
- adozione di misure che evitino qualsiasi consultazione massiva o non pertinente.

Tutte le operazioni effettuate sono registrate nei sistemi di tracciamento e sono soggette a verifiche periodiche nell'ambito delle attività di audit.

Le identità personali e le credenziali di accesso per gli utenti, i dispositivi e i processi autorizzati sono amministrate tramite piattaforma informatica centralizzata, registrate e verificate tramite logging (log conservati in modo sicuro e centralizzati, come previsto per legge),

revocate in caso di cambiamenti organizzativi e sottoposte ad audit di sicurezza annuali. Le identità di sistema sono gestite impiegando certificati digitali.

Gli accessi privilegiati vengono limitati ai soli casi essenziali e monitorati. Tra gli accessi privilegiati si configura la manutenzione/riparazione, in loco e da remoto, delle risorse e dei sistemi, che viene approvata, documentata e autorizzata attraverso meccanismi di autenticazione e identificazione e tracciamento degli eventi, di gestione/controllo delle utenze privilegiate in termini di limitazioni temporali e funzionalità. Tutti i log relativi alle sessioni di comunicazione remote sono prodotti e custoditi su sistemi separati da quelli oggetto di intervento e non accessibili dalle utenze remote. La revisione degli accessi ai sistemi regionali avviene con periodicità semestrale.

Inoltre, la figura dell'Amministratore di Sistema è designata formalmente, in conformità ai principi di responsabilità e tracciabilità previsti dalle politiche di sicurezza dell'Ente e dai controlli ISO/IEC 27001 relativi alla gestione degli accessi privilegiati.

La gestione degli Amministratori di Sistema prevede:

- Elenco nominativo aggiornato, contenente i soggetti autorizzati e le relative aree di competenza;
- Definizione del perimetro operativo per ciascun amministratore, comprensivo di sistemi, funzioni e privilegi assegnati;
- Registrazione dettagliata delle attività rilevanti ai fini della sicurezza, conservate in log sicuri e non alterabili;
- Retention dei log per un periodo non inferiore a sei mesi, in conformità ai requisiti normativi applicabili e alle politiche interne;
- Verifiche periodiche sull'adeguatezza dei privilegi assegnati e sulla coerenza con il ruolo e le esigenze operative;
- Informativa interna aggiornata sulle responsabilità, sugli obblighi e sulle modalità di trattamento dei dati connessi alle attività di amministrazione dei sistemi.

La supervisione degli Amministratori di Sistema è svolta attraverso controlli regolari, assicurando trasparenza, tracciabilità e conformità ai principi di minimizzazione, necessità e proporzionalità del trattamento dei dati.

5.9. CONSAPEVOLEZZA E FORMAZIONE IN SICUREZZA INFORMATICA

La Regione Basilicata riconosce l'importanza della consapevolezza e della formazione del personale quale elemento fondamentale per garantire la sicurezza delle informazioni. Tutti gli utenti e le risorse professionali che accedono alle risorse IT e agli asset informativi regionali ricevono una formazione adeguata al proprio ruolo, erogata all'inizio del rapporto di lavoro e periodicamente aggiornata.

La formazione è strutturata per garantire il continuo adeguamento delle competenze in funzione dell'evoluzione tecnologica, organizzativa e normativa ed è realizzata attraverso percorsi formativi sia formali che informali, in modalità e-learning, in aula e tramite attività di training on the job. Le attività formative sono pianificate, gestite e monitorate dall'ufficio competente, che provvede all'identificazione dei fabbisogni formativi, alla pianificazione degli interventi, alla tracciatura della partecipazione e alla verifica dell'efficacia della formazione.

I programmi formativi coprono, in particolare, i seguenti ambiti:

- ruoli e responsabilità in materia di sicurezza informatica, con particolare riferimento ai soggetti che hanno accesso agli asset informativi;
- politiche di accesso a sistemi, asset e risorse IT;
- politiche di gestione delle informazioni e della sicurezza informatica;
- requisiti di riservatezza, non divulgazione e confidenzialità delle informazioni;
- tecnologie e misure di protezione;
- consapevolezza delle principali minacce informatiche (phishing, ransomware, social engineering);
- sicurezza dei dispositivi mobili e del lavoro da remoto (smart working);
- principi applicabili in materia di protezione dei dati personali (GDPR);
- procedure per la restituzione dei beni aziendali al termine del rapporto di lavoro.

La partecipazione alle attività formative è registrata e documentata. L'efficacia dei programmi di formazione e sensibilizzazione è verificata con cadenza almeno annuale e, su richiesta, le informazioni relative alla formazione e all'aggiornamento professionale delle risorse impiegate sono rese disponibili all'Amministrazione mediante apposita reportistica.

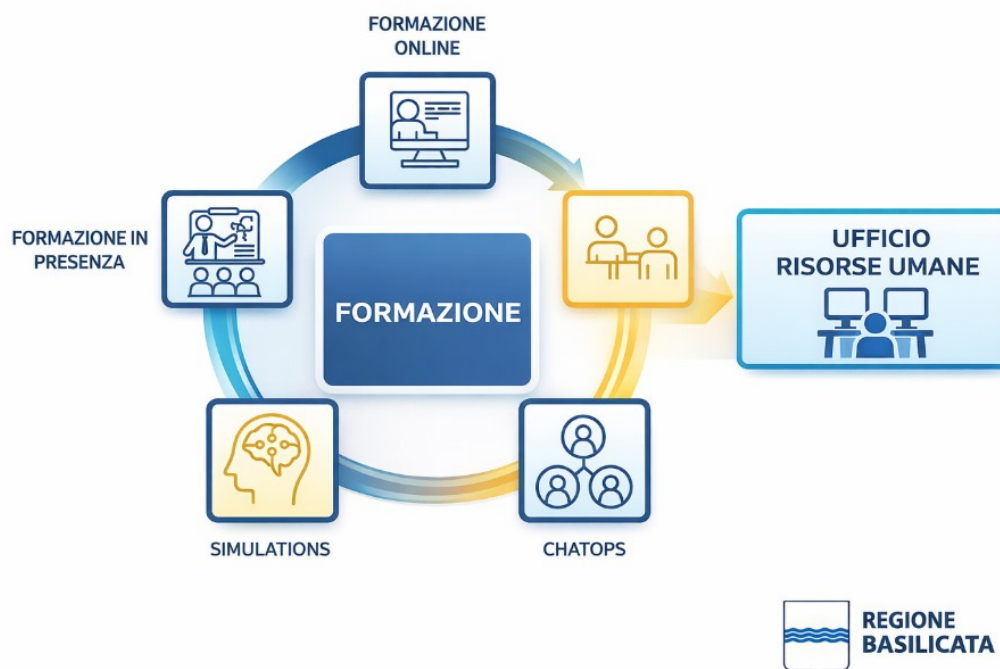


Figura n.2 Formazione

5.10. SICUREZZA DEI DATI

La gestione e la memorizzazione dei dati della Regione Basilicata avvengono in conformità con la strategia di gestione del rischio, al fine di garantirne l'integrità, la riservatezza e la disponibilità ed in applicazione del Regolamento (UE) 2016/679. In presenza di trattamenti che presentano un rischio elevato per i diritti e le libertà degli interessati, è effettuata una Valutazione di Impatto sulla Protezione dei Dati (DPIA), con il coinvolgimento del Responsabile della Protezione dei Dati (DPO).

Gli eventi di violazione dei dati personali (data breach) sono gestiti in conformità a quanto previsto dalla DGR n. 43/2023 "Data Protection Policy" e dalla DD n. 16BJ.2024/D.01076 del 27/12/2024, che istituisce il CSIRT Regionale, nonché dalla relativa documentazione operativa per la gestione degli incidenti.

Sono implementate misure di sicurezza per proteggere i dati da esfiltrazione, utilizzando sistemi EDR/XDR (Endpoint Detection and Response/ Extended Detection and Response), Data Loss Prevention. L'integrità dei dati è assicurata tramite apposite soluzioni e procedure di backup.

La trasmissione e la migrazione di dati, servizi o applicazioni verso ambienti cloud devono avvenire tramite canali cifrati e sicuri (es. HTTPS), in conformità ai controlli ISO/IEC 27001. L'organizzazione adotta misure per la gestione sicura della crittografia e delle chiavi, e regola l'uso dei supporti removibili mediante controlli di accesso.

L'invio tramite posta elettronica e PEC/S-MIME di dati appartenenti alle "categorie particolari" definite dal Regolamento UE 2016/679 deve avvenire allegando il file criptato al messaggio, e non inserendo i dati sensibili nel corpo della mail. Il file allegato deve essere protetto con modalità idonee a impedirne l'accesso non autorizzato o accidentale da parte di soggetti diversi dal destinatario, ad esempio tramite password o chiave crittografica comunicata separatamente agli interessati.

Al fine di Proteggere i dati critici sono implementate policy (DLP - Data Loss Prevention) di blocco per l'invio di email. Non è consentito l'invio o l'inoltro di messaggi non rilevanti per il contesto lavorativo a un numero elevato di destinatari o liste di distribuzione interne.

L'accesso ai dati regionali da parte di entità situate al di fuori dell'Unione Europea non è consentito, ammenoché siano presenti TIA (Impatto sul Trasferimento), SCC (Clausole Contrattuali Standard), misure supplementari che garantiscono i trattamenti da parte di soggetti Extra SEE e autorizzato dal Titolare del trattamento (o dal Responsabile, se designato e nei limiti del mandato) e previa verifica di conformità al GDPR. Eventuali violazioni dei dati personali sono notificate al Garante per la Protezione dei Dati Personali e, se del caso, agli interessati, secondo la normativa vigente.

Il trasferimento fisico, la rimozione e la distruzione dei dispositivi di memorizzazione dati sono gestiti attraverso il processo di asset management, che include procedure per la cancellazione sicura dei dati, anche da remoto.

La sicurezza è integrata in tutto il ciclo di vita dei sistemi informatici, a partire dalla fase di sviluppo. Gli ambienti di sviluppo e test sono mantenuti separati dall'ambiente di produzione. Il software sviluppato è analizzato tramite lo strumento di analisi statica del codice sorgente (SAST) per identificare e correggere potenziali vulnerabilità prima della sua messa in esercizio.

È fatto assoluto divieto di comunicare a terze informazioni riservate (confidenziali), segrete o comunque rilevanti per la Regione e le sue attività, nonché qualsiasi informazione di natura riservata appresa o di cui il dipendente sia venuto a conoscenza durante lo svolgimento delle proprie mansioni. Tale divieto è posto a tutela dell'obbligo di fedeltà e correttezza a carico dei dipendenti e include, a titolo esemplificativo ma non esaustivo, piani strategici, informazioni relative a due diligence e dati personali. È altresì vietato divulgare notizie, dati e qualsiasi altra informazione appresa in occasione della ricezione o dell'invio di posta elettronica, in quanto coperti dal segreto professionale.

Al fine di proteggere il sistema informatico dal rischio di introduzione di codice malevolo e/o di alterazione delle funzionalità delle applicazioni software esistenti, è vietato a chiunque utilizzi computer regionali scaricare dalla rete Internet (installare e/o eseguire) software non autorizzato. L'utilizzo di programmi diversi da quelli ufficialmente approvati è proibito.

5.11. MANUTENZIONE E GESTIONE DEL CAMBIAMENTO

La manutenzione e la riparazione delle risorse e dei sistemi IT regionali sono eseguite e registrate tramite strumenti controllati e autorizzati tramite il sistema di trouble ticketing.

In base all'analisi del rischio, ogni aggiornamento hardware o software di componenti ritenuti critici è verificato in un ambiente di test prima dell'implementazione nell'ambiente operativo, al fine di valutarne anche gli aspetti di sicurezza. Sono fatte salve esigenze di tempestività motivate da impellenti necessità di sicurezza. Il codice sorgente degli aggiornamenti è custodito in un repository regionale ed è responsabilità del fornitore mantenerlo aggiornato all'ultima versione.

Tutti i log relativi alle attività di manutenzione e aggiornamento sono generati e conservati su sistemi separati da quelli oggetto di intervento e non sono accessibili agli utenti che eseguono tali attività.

La manutenzione remota ordinaria dei dispositivi IT viene effettuata, previa autorizzazione degli utenti, tramite piattaforme dedicate e autorizzate dalla regione; la stessa, inoltre, è documentata garantendo la registrazione dei log, la limitazione temporale degli accessi, delle funzionalità amministrative e delle utenze privilegiate.

Le attività di manutenzione straordinaria sono pianificate e documentate, eseguite e monitorate nell'ambito del processo di gestione del cambiamento approvato per i sistemi regionali.

Inoltre, ogni Direzione/Ente/Azienda è responsabile del mantenimento e dell'aggiornamento delle proprie piattaforme. Tale obbligo garantisce la continuità operativa e la conformità agli standard di sicurezza regionali.

5.12. MONITORAGGIO CONTINUO DELLA SICUREZZA, GESTIONE ANOMALIE ED EVENTI

La Regione Basilicata svolge un monitoraggio continuo della propria rete informatica al fine di rilevare potenziali eventi di cybersecurity a livello di applicazioni e infrastruttura. Questo include l'analisi e la correlazione degli eventi provenienti da sensori e diverse sorgenti identificate. I risultati di tale monitoraggio sono conservati secondo quanto definito nella policy di data retention, in conformità alle disposizioni normative vigenti, garantendo integrità, riservatezza, non ripudio e accessibilità per finalità di sicurezza, audit e investigazione.

Il traffico di rete in ingresso e in uscita, le attività dei sistemi perimetrali (router e firewall), gli eventi amministrativi rilevanti e gli accessi (riusciti o falliti) alle risorse di rete e alle postazioni terminali sono monitorati e correlati per identificare e gestire eventi di cybersecurity. A tal fine, vengono utilizzati software specializzati (SIEM, Analyzer, Firewall, EDR, SOAR) mantenuti aggiornati, mantenuti e correttamente configurati.

È inoltre attivo un monitoraggio per rilevare la presenza fisica o logica di utenti, connessioni, dispositivi o software non autorizzati, attraverso l'impiego di sistemi di sorveglianza e controllo degli accessi, nonché scansioni periodiche per l'identificazione di vulnerabilità. I requisiti tecnici per le configurazioni dei sistemi a supporto della conservazione dei log e del monitoraggio degli eventi di sicurezza sono definiti nella specifica politica regionale per la gestione del monitoraggio degli eventi.

La manutenzione remota dei dispositivi IT in caso di rilevazioni di eventi anomali viene effettuata dal COC tramite piattaforme dedicate e autorizzate dalla regione per fronteggiare eventuali minacce informatiche; tale tipologia di attività è documentata garantendo la registrazione dei log, la limitazione temporale degli accessi, delle funzionalità amministrative e delle utenze privilegiate.

5.13. GESTIONE DEGLI INCIDENTI E DELLE VULNERABILITA'

La Regione Basilicata dispone di un processo strutturato per la gestione tempestiva degli incidenti di sicurezza e delle vulnerabilità (segnalate da fonti interne ed esterne). Tale processo coinvolge lo CSIRT regionale e in caso di necessità anche le parti interessate e lo CSIRT Italia.

La documentazione a supporto della gestione degli incidenti è gestita dallo CSIRT regionale attraverso un apposito framework documentale.

La gestione degli incidenti prevede una fase iniziale di identificazione e analisi, basata sulle segnalazioni provenienti dalle Amministrazioni, nonché sugli allarmi generati dagli strumenti di monitoraggio (SIEM, EDR, XDR, SOAR, ecc).

In tale fase, le strutture tecniche del Centro Servizi Regionale svolgono le attività di investigazione preliminare per verificare l'effettiva natura dell'evento, distinguendo gli incidenti reali dai falsi positivi, e producono un documento contenente i primi elementi di analisi, la natura dell'incidente e il relativo livello di gravità.

Gli incidenti sono classificati secondo livelli di severità predefiniti. La trasmissione del documento di analisi preliminare avviene entro tempi massimi differenziati in funzione della gravità dell'incidente.

Livello di Gravità	denominazione	Descrizione
Livello 1	Alto	Incidenti con perdita di riservatezza, integrità o disponibilità dei dati, compromissione di credenziali o chiavi crittografiche, escalation di privilegi, persistenza di codice malevolo, elusione dei sistemi di sicurezza, comunicazioni non autorizzate verso l'esterno, movimenti laterali o esfiltrazione di dati.

Livello 2	Medio	Incidenti che comportano compromissione di server o degrado delle prestazioni dei servizi, con impatti sulla produttività degli utenti. Possibile indisponibilità parziale o intermittente dei servizi critici per periodi limitati, senza compromettere la continuità complessiva del servizio.
Livello 3	Basso	Incidenti senza compromissione di asset o servizi critici, con impatti limitati e temporanei, quali brevi interruzioni operative per un numero ristretto di utenti o infezioni da malware prontamente rilevate e contenute.
Livello 4	Nessuno	Nessun effetto sulla capacità dell'organizzazione di erogare i servizi agli utenti; nessuna informazione è stata oggetto di accesso non autorizzato, esfiltrazione, modifica o cancellazione;

La seconda fase del processo ha lo scopo di individuare le azioni di contenimento necessarie per contrastare l'attacco in corso e impedirne la propagazione. In questo momento si definiscono gli interventi correttivi di breve periodo considerati urgenti, che vengono immediatamente comunicati all'ufficio competente per mettere in sicurezza i sistemi coinvolti.

La fase successiva riguarda la notifica e la raccolta delle evidenze digitali. In quest'ottica si mira a trasmettere rapidamente le informazioni utili e a reperire ogni elemento che possa contribuire alla ricostruzione accurata dell'incidente. Le evidenze raccolte possono riguardare accessi non autorizzati, attività illecite compiute attraverso i sistemi dell'Amministrazione, violazioni della privacy o qualunque altro comportamento anomalo rilevante ai fini investigativi.

Segue poi la fase di risposta e ripristino dei sistemi e delle applicazioni, che ha l'obiettivo di individuare e attuare gli interventi necessari per riportare i sistemi compromessi a un livello adeguato di sicurezza. In questa fase si procede alla rimozione definitiva del problema o della vulnerabilità sfruttata dall'attaccante, garantendo il pieno recupero dell'operatività.

Infine, una volta concluse tutte le attività di risposta, avviene la valutazione a posteriori dell'incidente, orientata al miglioramento continuo. Team CSIRT regionale provvede a notificare la chiusura dell'incidente tramite il sistema di ticketing e produce la documentazione di reporting. Successivamente vengono analizzate le operazioni svolte e le criticità riscontrate, così da trarre insegnamenti utili e proporre soluzioni che aumentino il livello di sicurezza dei servizi offerti. Questa fase permette di

capitalizzare l'esperienza maturata, contribuendo all'evoluzione del sistema di gestione della sicurezza e alla prevenzione di futuri incidenti.

5.14. GESTIONE DEI BACKUP

I dati e le applicazioni della Regione Basilicata sono sottoposti regolarmente a procedure di backup tramite software dedicati. Le copie di backup sono protette con crittografia robusta e l'accesso è limitato all'utente autorizzato. L'integrità delle copie di backup è verificata in modalità continua dal COC in conformità alle procedure di sicurezza per l'accesso ai sistemi e alle applicazioni, garantendo la conservazione dei backup in un formato non cancellabile e inalterabile (WORM: Write Once, Read Many) al fine di garantirne l'autenticità. La regione mette a disposizione dell'utente una piattaforma che consente il salvataggio dei propri dati in modalità cloud.

5.15. BUSINESS CONTINUTY E DISASTER RECOVERY

Il Disaster Recovery "as-a-Service" (DRaaS) è il servizio di cloud computing che consente il ripristino dei dati e dell'infrastruttura IT di un ambiente completo di sistemi e relativi dati. Ciò consente di ripristinare l'accesso e la funzionalità dell'infrastruttura IT dopo un evento disastroso.

Al fine di garantire la resilienza dei propri servizi IT, la Regione Basilicata implementa processi e tecnologie per la Business Continuity in linea con lo standard ISO 22301.

In relazione ai risultati dell'analisi del rischio, sono stati implementati i seguenti meccanismi:

- Meccanismi per soddisfare i requisiti di resilienza sia durante il normale esercizio che in situazioni avverse.
- Architetture di rete, connettività e applicazioni ridondate. I dispositivi e gli apparati che gestiscono servizi e flussi di dati.

5.16. GESTIONE AUDIT

La conformità alla seguente politica ed altri requisiti di sicurezza informatica applicabili è verificata con periodicità definite all'interno del piano audit di sicurezza informatica. A garanzia dell'indipendenza dei risultati di audit, le responsabilità per queste attività sono conferite garantendo la segregazione delle responsabilità, evitando conflitti di interessi e assicurando che siano eseguite da esperti certificati (LEAD Auditor ISO 27001 ed estensioni 27017 e 27018) con comprovate esperienze.

Letto, confermato e sottoscritto digitalmente.

Lì,

L'Utente

.....