COMUNE DI PETILIA POLICASTRO
PIANO DELLA SICUREZZA DEL SISTEMA DI GESTIONE INFORMATICA DEI DOCUMENTI

1. PREMESSA - RIFERIMENTI ED ALLEGATI
Il presente Piano della Sicurezza del Sistema di gestione informatica dei documenti (PdS) descrive l'implementazione del Sistema di Gestione della Sicurezza Informatica (SGSI) del Comune di Petilia Policastro per quanto attiene alle attività previste nel Sistema di gestione documentale con riferimento alle Linee Guida AGID sulla formazione, gestione e conservazione dei documenti informatici ed *ex* Codice dell'Amministrazione Digitale, D.Lgs. 7 marzo 2005, n. 82 e successive modificazioni. Ogni indicazione contenuta nel PdS è da intendersi riferita, ove altrimenti non indicato, esclusivamente alle predette attività.
Il PdS si fonda su una serie di documenti, procedure e prassi che per motivi di sicurezza non vengono allegate o proposte in estratto, tra cui le Misure Minime di Sicurezza adottate. Nella stesura del presente Piano di Sicurezza del Sistema di gestione informatica dei documenti si è fatto riferimento alle norme tecniche ISO/IEC 27001, quale linea guida tecniche.

2. NORMATIVA E STANDARD DI RIFERIMENTO
2.1 Normativa di riferimento
- Codice Civile Libro Quinto Del lavoro, Titolo II Del lavoro nell'impresa, Capo III Delle imprese commerciali e delle altre imprese soggette a registrazione, Sezione III Disposizioni particolari per le imprese commerciali, Paragrafo 2 Delle scritture contabili, articolo 2215 bis - Documentazione informatica;
- Legge 7 agosto 1990, n. 241 e s.m.i. – Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi;
- Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e s.m.i. – Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- Decreto Legislativo 30 giugno 2003, n. 196 e s.m.i. – Codice in materia di protezione dei dati personali; ▪ Decreto Legislativo 22 gennaio 2004, n. 42 e s.m.i. – Codice dei Beni Culturali e del Paesaggio;
- Decreto Legislativo 7 marzo 2005 n. 82 e s.m.i. – Codice dell'amministrazione digitale (CAD) e in particolare art. 50 bis;
- Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013 – Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma3, lettera b), 35, comma 2, 36, comma 2, e 71;
- Regolamento (UE) 910/2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno – Regolamento eIDAS;
- Regolamento (UE) 2016/679 del Parlamento europeo (GDPR) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati;
- Circolare AGID 10 aprile 2014, n. 65 - Modalità per l'accreditamento e la vigilanza sui soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici di cui all'articolo 44-bis, comma 1, del decreto legislativo 7 marzo 2005, n. 82;
- Circolare n. 2 del 18 aprile 2017, n. 2/2017 di AGID, recante le misure minime di sicurezza ICT per le pubbliche amministrazioni;
- Circolare n. 2 del 9 aprile 2018, recante i criteri per la qualificazione del Cloud Service Provider per la PA;
- Circolare n. 3 del 9 aprile 2018, recante i criteri per la qualificazione di servizi SaaS per il Cloud della PA;
- Regolamento (UE) 2018/1807, relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea;

2.2 Standard di riferimento
Nella definizione del contesto normativo tramite il quale regolamentare il Sistema di gestione documentale, il legislatore ha provveduto ad identificare alcuni standard tecnologici di valenza internazionale cui riferirsi, al fine sia di recepire ricerche e studi, sia di definire il percorso che consenta agli operatori di rispondere in maniera proattiva alla normativa europea. Segue l'elenco degli standard tecnologici cui si ispira il presente documento:
Formazione e gestione di documenti informatici:
- UNI ISO 15489-1: 2006 Informazione e documentazione - Gestione dei documenti di archivio

- Principi generali sul record management.
- UNI ISO 15489-2: 2007 Informazione e documentazione - Gestione dei documenti di archivio – Linee Guida sul record management.
- ISO/TS 23081-1:2006 Information and documentation - Records management processes – Metadata for records – Part 1 – Principles, Quadro di riferimento per lo sviluppo di un sistema di metadati per la gestione documentale.
- ISO/TS 23081-2:2007 Information and documentation - Records management processes – Metadata for records – Part 2 – Conceptual and implementation issues, Guida pratica per

l'implementazione.

- ISO/TS 16175-1 –(ICA) Information and documentation –Principles and functional requirements for records in electronic office environments–Part 1: Over view and statement of principles.

- ISO/TS 16175-2 –(ICA) Information and documentation –Principles and functionalrequirementsforrecordsinelectronic officeenvironments–Part2:Guidelinesandfunctionalrequirements for digital records management systems.

- ISO/TS 16175-3 –(ICA) Information and documentation –Principles and functionalrequirementsforrecordsinelectronic officeenvironments–Part3:Guidelinesandfunctionalrequirements for records in business system.

- ISO15836:2003-Information anddocumentation -The DublinCoremetadata elementset, Sistema dimetadata del Dublin Core.
- ISO9001–Sistemi d igestione per la qualità–Requisiti.
- ISO30300:2011-Information and documentation–Management system sforre cords–Fundamental sand vocabulary.
- ISO30301:2011-Information and documentation-Management systems for records–Requirements.
- ISO30302:2015-Information and documentation-Management systems for records–Guide lines for implementation.
- ISO/TR23081-3-Informationanddocumentation –Managing metadata for records–Part3: Self-assessment method.
- MoReq2001–Model requirements for the management of electronic records.
- MoReq2–Specification 2008 Model requirements for the management of electronic records–che individua i requisiti funzionali della gestione documentale.
- MoReq2010–Modul arrequirements for records systems. Conservazione di documenti informatici:
- UNI11386–Standard SinCRO–Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali.

- ISO14721:2012OAIS(Open Archival Information System),Sistema informativo aperto per l'archiviazione.

- *ISO15836:2003-Information and documentation-The Dublin Core metadata element set, Sistema di metadata del Dublin Core.*

- *ISO/TR18492–Long-termpreservation of electronic document-base dinformation.*

- *ISO20652–Space data and information transfersystems–Producer-Archive interface–Methodology abstract standard.*

- *ISO20104*–Space data and information transfersystem–Producer-Archive Interface Specification (PAIS).

- ISO/CDTR26102–Requirements for long-termpreservation of electronic records.

- SIARD Software Independent Archiving of Relational Databases2.0.

- ISO/IEC 27001:2013, Information technology-Security techniques-Information security management systems–Requirements,Requisitidiun ISMS(Information Security Management System).
- ETSI TS 101 533-1 V 1.3.1 (2012-04) Technical Specification, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 1: Requirements for Implementation and Management. Requisiti per realizzare e gestire sistem isicuri e affidabili per la conservazione elettronica delle informazioni.

- ETSITR101 533-2V1.3.1 (2012-04)Technical Report ,Electronic Signatures and Infrastructures (ESI);Information Preservation Systems Security;Part2:Guide lines for Assessors,Linee guida per valutare sistemi sicuri e affidabili per la conservazione elettronica delle informazioni.

▪METS–Metadata Encodingand Trasmission Standard.
▪PREMIS –PREservation Metadata:Implementation Strategies.
▪EAD(3)/ISAD(G).
▪EAC(CPF)/ISAAR(CPF)/NIERA/(CPF).
▪SCONS2/EAG/ISDIAH. Sicurezza informatica:
▪ISO/IEC 27001 -Information technology-Security techniques-Information security management systems–Requirements, Requisiti di un ISMS (Information Security Management System).
▪Regolamento generale per la protezione dei dati personali2016/679(General Data Protection Regulation o GDPR)-Normativa europea in materia di protezione dei dati personali.
▪ETSITS101533-1V1.2.1–Technical Specification, Electronic Signatures and Infrastructures/ESI); Information Preservation Systems Security.

3.ORGANIZZAZIONE DEL SISTEMA DI GESTIONE DOCUMENTALE

Il paragrafo ha ad oggetto la descrizione dell'organizzazione del Sistema di gestione documentale, sotto il profilo dei ruoli, delle responsabilità e della produzione-diffusione di policy e procedure.

3.1 Ruoli e responsabilità del sistema di gestione documentale

Lo svolgimento delle attività legate al sistema di gestione documentale richiede la presenza di più attori, ognuno dei quali ha la responsabilità di specifiche attività da svolgere. Questi ruoli si inseriscono nell'organigramma generale dell'Ente pubblico, arricchendo i ruoli e le procedure già previste per la gestione dei processi interni. Per ogni figura prevista nel processo di gestione documentale sono richiesti specifici requisiti di onorabilità e di esperienza minima nel ruolo. Peraltro, così com'è previsto che alcune attività possano essere svolte dal medesimo soggetto è, altresì, previsto che alcune funzioni possano essere delegate ad altri soggetti, fermo restando i predetti vincoli di onorabilità e di requisiti di esperienza del delegato. Le attività relative al servizio di gestione documentale coinvolgono vari settori del Comune di Petilia Policastro, che interagiscono tra loro al fine di garantire la gestione di tutte le esigenze del produttore dei documenti. Specificamente, le attività impattano sulle seguenti strutture organizzative:

• *Responsabile del Servizio di gestione documentale*: questi possiede le competenze concernenti la definizione e l'attuazione delle politiche complessive del sistema di gestione documentale, nonché del governo della gestione del sistema. In particolare: a) predispone lo schema del manuale di gestione;

b) propone i tempi, le modalità e le misure organizzative e tecniche;

c) predispone il Piano della Sicurezza del Sistema di gestione informatica dei documenti relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso, alla conservazione dei documenti informatici, in collaborazione con l'U.O. Sistemi informativi;

d) definisce e assicura criteri uniformi di trattamento del documento informatico, di classificazione ed archiviazione, nonché di comunicazione interna.

Questi si appoggia alle seguenti aree del Comune di Petilia Policastro:

• *U.O. Affari Generali - Ufficio Transizione digitale,* che cura l'implementazione, la gestione e la sicurezza dell'infrastruttura ICT;

• *Lo stesso Ufficio Transizione del Digitale:* afferente all'U.O. Affari Generali, che cura la soluzione di problemi tecnici, user oriente d, legati alle infrastrutture digitali telematiche dell'ente;

• *Provider Software applicativo del Protocollo Informatico*: soggetto privato che implementa e gestisce il software applicativo su cui poggia il sistema di Protocollo Informatico in uso nel Comune di Petilia Policastro;

3.2 Ruoli e responsabilità della sicurezza informatica del sistema di gestione documentale

Nell'ambito del personale del Comune di Petilia Policastro destinato alla gestione del sistema documentale per quanto concerne le questioni legate alla Sicurezza informatica, è il Responsabile della gestione documentale si riferisce all'U.O. Sistemi Informativi del Comune di Petilia Policastro.

3.3 Procedure di produzione, diffusione e gestione della documentazione di sicurezza

Le procedure di gestione della documentazione di sicurezza riguardano le attività legate all'acquisizione, produzione, archiviazione e diffusione del materiale relativo alla Sicurezza delle Informazioni.
I principi di Gestione Documentale della Sicurezza, propri del Comune di Petilia Policastro, prevedono la produzione di documenti elaborati e la loro schedulazione di diffusione, in seguito alla fase di analisi dei rischi, da parte del Responsabile della gestione documentale in cooperazione con il Responsabile dell'U.O.. Sistemi Informativi. Scopo dell'attività è offrire uno strumento di condivisione delle procedure di sicurezza con il personale del Comune di Petilia Policastro.

3.4 Procedure per l'acquisto di prodotti e servizi

Sotto il profilo della sicurezza ICT del sistema di gestione documentale, il processo di acquisto dei prodotti e servizi all'interno dell'Ente Pubblico è regolamentato dalle procedure comunali.

3.5 Procedure per l'alienazione degli asset dell'organizzazione

Sotto il profilo della sicurezza ICT del sistema di gestione documentale, il processo di dismissione o alienazione degli asset dell'Ente pubblico viene regolamentato dalle procedure comunali.
Queste sottintendono le seguenti procedure, a seconda della tipologia di oggetti da alienarsi e dei casi d'uso:

- Procedura di **cancellazione** delle informazioni;
- Procedura di **distruzione** dei supporti non riscrivibili utilizzati per la memorizzazione delle informazioni;
- procedura di **cancellazione sicura** dai supporti riscrivibili utilizzati per la memorizzazione delle informazioni;
- procedura di **triturazione** di supporti, quali quelli cartacei e analoghi;
- procedura di custodia e conservazione dei supporti contenenti dati degli utenti (hard disk dei pc) una volta che gli utenti non siano più in comando presso l'Ente – es. pensionamenti, dismissioni volontarie, trasferimenti, aspettative, ecc.

3.6 Piano di formazione del personale

Il Responsabile della Transizione digitale, in cooperazione con il Responsabile per il trattamento dei dati personali e il Responsabile dell'U.O. Affari Generali e Segreteria, organizza, fornisce e gestisce la programmazione della formazione del personale, per quanto concerne i seguenti aspetti:

- policy e tecnica per **l'utilizzo dei sistemi** informatici dell'Ente pubblico e del Protocollo Informatico;
- policy e tecnica per la **sicurezza dei sistemi informatici** dell'Ente pubblico e del Protocollo Informatico;
- policy per la gestione delle **emergenze informatiche** dell'Ente pubblico e del Protocollo Informatico.

3.7 Continuità operativa: Disaster Recovery e procedure di attivazione

Le misure adottate per garantire la continuità operativa dell'accesso all'intero sistema di gestione documentale si fondano sulla strutturazione di procedure di Disaster recovery e Backup delle informazioni, nonché sulla presenza di apparati ridondati e gruppi di continuità UPS, come dettagliato nei paragrafi seguenti.
Le misure concernono:

- il sistema web application per il Protocollo Informatico: mediante policy, procedure e prassi del Provider dell'applicazione;
- il sistema informatico del Comune di Petilia Policastro: attraverso policy, procedure e prassi elaborate secondo le norme concernenti la Tutela dei dati, la Sicurezza dei sistemi, il Codice per l'Amministrazione Digitale e la normativa legata al Sistema di gestione documentale.

In particolare, policy, procedure e prassi concernono:

- il grado di affidabilità dei sistemi hardware/software;
- la programmazione della manutenzione delle apparecchiature e delle infrastrutture di supporto: idrico, elettrico, antintrusione, antifurto, antiallagamento, antincendio, continuità elettrica;
- il controllo sui sistemi al fine di assicurarne la continua disponibilità e integrità.

Il servizio di Disaster Recovery viene garantito sulla base dei dati soggetti a backup periodici effettuati giornalmente ed è declinato in Servizio di Disaster Recovery DATI e Servizio di Disaster Recovery INFRASTRUTTURE applicative, come dettagliato di seguito:

- **Servizio di Disaster recovery DATI** - La soluzione comporta il backup dei dati di tutti i pc presso il server sito nella struttura comunale, il quale giornalmente, effettua il backup di tuti i dati all'interno di un nastro, il quale viene sostituito con cadenza settimanale e inserito in una cassetta ignifuga e antiallagamento. E' intenzione del Comune nei prossimi mesi di implementare un backup in una struttura esterna al Comune, con una riduzione del tempo necessario per il trasporto dei dati e la possibilità di un recovery time piu' veloce. Il sito disporrà di hardware e connettività già funzionante ma su scala inferiore rispetto al sito principale e con

replica costante dei dati. Il backup avverrà in modalità elettronica mediante collegamenti fra i siti tenuto dimensionati tenendo conto della tipologia, quantità e periodicità dei dati, con. - RPO (tempo massimo di delay tra l'ultima copia e il fault dei sistemi) di **4** ore

- RTO (tempo necessario per il ripristino dei sistemi) di **1** ora.

▪ **Servizio di Disaster recovery INFRASTRUTTURE applicative** - la soluzione comporterà la replica delle virtual machine presso il sito secondario, permettendo un recovery time piu' veloce. Il sito disporrà di hardware e connettività già funzionante ma su scala inferiore rispetto al sito principale o ad un sito alternativo sempre disponibile. Il backup avverrà in modalità elettronica mediante collegamenti fra i siti tenuto dimensionati tenendo conto della tipologia, quantità e periodicità dei dati con: - RPO (tempo massimo di delay tra l'ultima copia e il fault dei sistemi) di **24** ore

- RTO (tempo necessario per il ripristino dei sistemi) di **1** ora.

La procedura di Disaster Recovery da attivarsi all'occorrenza lato 'Ente mostra una sua disposizione in fasi, atta ad essere applicata a qualunque evento verificato:

• **Fase di reazione all'emergenza**: 1) ricevimento della segnalazione dell'evento, attraverso sistemi di rilevamento o indicazioni del personale; 2) pre-valutazione della situazione di pericolo e di rischio; 3) indicazione di misure temporanee di emergenza, con possibilità di sospensione del servizio.

• **Fase di gestione dell'emergenza**: 1) identificazione dell'area tecnica da coinvolgere nell'attività;
2) indicazione di misure di emergenza da disporre al fine di risolvere l'evento; 3) supervisione delle attività e adattamento al caso concreto.

• **Fase di riattivazione dei servizi**: 1) osservazione sulle attività svolte in base a principi di buone regole tecniche; 2) test sui servizi soggetti all'evento "off line"; 3) riattivazione graduale dei servizi con controllo dell'efficienza.

• **Fase di ritorno alla normalità**: 1) test dei sistemi online; 2) apertura al personale dei sistemi riattivati con monitoraggio della fruizione; 3) piena operatività dei sistemi e normalità operativa.

La struttura organizzativa di riferimento preposta alla gestione dello stato di emergenza è l'U.O. Sistemi Informativi.

3.8 Piano degli audit del sistema

Il Responsabile della Transizione digitale, in maniera traversale, pianificherà una programmazione di audit periodici sulla base di un cronoprogramma condiviso con i differenti servizi e secondo piani concordati, allo scopo di definire strategie di ottimizzazione applicabili a processi, procedure e infrastrutture.

4. ARCHITETTURA FUNZIONALE

Il sistema di Protocollo Informatico è strutturato secondo le seguenti linee guida:

▪ presenza di un software applicativo centralizzato sull'infrastruttura dell'ente pubblico;

▪ integrazione del sistema e dell'applicativo verso sistema di conservazione sostitutiva;

▪ accesso sicurizzato in VPN al fornitore del software applicativo per manutenzione e adeguamento normativo ai sensi di legge;

▪ integrazione del sistema verso software applicativi verticali utilizzati dall'Ente pubblico, a fini di amministrazione, protocollazione e gestione secondo opportuni workflow.

4.1 Componenti logico-fisiche

La soluzione informatica abilitante il Protocollo Informatico del Comune di Petilia Policastro è rappresentata da un software applicativo erogato in cloud privato in modalità IaaS/PaaS su datacenter di Terze Parti certificato AGID conforme allo standard ISO 27001 e fruibile attraverso l'infrastruttura di rete LAN/MAN dell'Ente.

In via generale, la soluzione software mostra i seguenti profili:

1) Componente logica: • l'architettura applicativa mira a garantire i requisiti di integrità, riservatezza, disponibilità e non ripudio dei dati, delle informazioni e dei messaggi;

• gli utenti usufruiscono dell'applicazione interagendo con l'interfaccia utente per via telematica dalla propria postazione di lavoro e della rete locale del Comune di Petilia Policastro;

• il software e le informazioni gestite risiedono in un sistema centralizzato costituito da server virtuali;

• l'utilizzo dei dispositivi e della rete intranet del Comune di Petilia Policastro è garantito ai soli utenti dotati di apposite credenziali d'accesso al sistema informatico, rilasciate da Sistemi Informativi su indicazione dei ruoli indicati dall' UO Affari Generali e Segreteria – Ufficio Transizione digitale e dai Dirigenti/PO della struttura di appartenenza, con l'utilizzo di password di lunghezza e complessità adeguate e con scadenza e necessità di rinnovo prestabilite;

• il sistema di sicurezza consente agli utenti di collegarsi all'applicazione secondo le modalità d'autorizzazione connesse al proprio ruolo e alle proprie responsabilità;

• l'accesso al sistema è effettuato attraverso dispositivi e reti, nonché sistemi operativi e browser, rilasciati dal Comune di Petilia Policastro e/o certificati dai Sistemi Informativi nel caso di utilizzo di dispositivi di proprietà del singolo utente (BYOD).

2) Componente fisica:

- gli utenti usufruiscono dei dispositivi del Comune di Petilia Policastro per l'accesso e l'utilizzo della piattaforma erogata in cloud;
- l'infrastruttura di rete del Comune include firewall, router e switch sia di core sia di distribuzione ed è soggetta a controlli di sicurezza sia logici sia fisici;
- la sicurezza perimetrale sia on-prem sia cloud viene demandata a Next Generation Firewall in grado di attivare funzionalità di IDS (Intrusion Detection System), IPS (Intrusion Prevention System) ed Antivirus in configurazione di alta affidabilità.
- all'Ente è dedicato ad un Virtual DOMain (VDOM) in modo da garantire il massimo livello di isolamento e protezione del dato, mantenendo sempre massimo il livello di sicurezza informatica fornita;
- il cloud service provider (CSP)* certificato AGID mette a disposizione le risorse della propria piattaforma IaaS/PaaS (risorse computazionali, di rete, di sicurezza,di storage e monitoraggio) implementata dai dispositivi integrati nel proprio cloud (firewall, proxy, web,application e database server, SAN, switch, router,..);
- la componente computazionale è realizzata utilizzando hardware dedicato con server in tecnologia blade e storage SAN/NAS in flash Array dischi SSD e fisici;
- tutti i sistemi sono ridondati in modo da garantire un'alta affidabilità di servizio costante, con servizi di assistenza effettuati e garantiti dal brand produttore stesso. In modo da garantire una continuità di servizio mediante funzionalità di Disater Recovery, con disponibilità dichiarata dal CSP pari a 99,95% su base annuale (con presidio degli impianti con copertura h24 365 giorni annui);
- la disponibilità dell'applicazione dichiarata dal Provider dell'applicativo è del 99% su base annuale.

4.2 Piani di manutenzione delle infrastrutture

L'ecosistema ICT riconducibile nel suo complesso direttamente o indirettamente, al sistema di gestione documentale, è soggetto a manutenzione ordinaria e straordinaria schedulate dal CSP e/o dal Provider dell'applicativo che comunica preventivamente all'Ente le attività manutentive ordinarie e straordinarie, infine dal Responsabile del Servizio di gestione documentale - in quest'ultimo caso in cooperazione con il Responsabile CED - qualora presupponessero impatti limitati all'infrastruttura di LAN/MAN.

4.3 Infrastruttura ICT "on-premise"

Relativamente ai sistemi informatici "on-premise" - cioè fisicamente presenti presso il CED dell'Ente e funzionali alla fruizione in cloud dell'applicazione - le funzionalità sono riconducibili a quelle di server, firewall, switch, router, gruppi di continuità a batteria (UPS).

I sistemi logici di sicurezza sono sia infrastrutturali sia applicativi. La presenza di misure di sicurezza è trasversale ad entrambe le tipologie, quali:

- Server di dominio locale windows 2016 con configurazione Hard Disk in Raid 5
- gestione di copie di backup da server su nastro;
- autenticazione informatica;
- adozione di procedure di gestione delle credenziali di autenticazione;
- utilizzazione di un sistema di autorizzazione;
- gestione dinamica dei permessi ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
- protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
- adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;
- al fine di ottemperare allo smart working è stata effettuata apposita configurazione degli accessi ai pc da remoto da parte dei dipendenti esclusivamente tramite VPN dotata di alti canoni di sicurezza-

4.4 Data Center per l'erogazione del servizio in modalità cloud IaaS/PaaS

I Data Center (primari e di Disaster Recovery) sono situati sul territorio nazionale all'interno di strutture altamente industrializzate, conformi alla normativa vigente dettata dall'A.C.N. (Agenzia per la Cybersicurezza Nazionale).

5. CONFORMITA' AL REG. UE 679/2016 (GDPR)

In ottemperanza la Reg. UE 679/2016 (GDPR), il Provider dell'applicazione agendo in qualità di Responsabile del trattamento, è tenuto a:

- adottare adeguate misure per la sicurezza dei dati personali previste dal GDPR, indicate dal Titolare (Ente Comune di Petilia Policastro, d'ora in avanti "Titolare"), vigilando sulla applicazione delle stesse, in modo da ridurre al minimo i rischi di violazione dei dati medesimi;
- individuare le persone autorizzate al trattamento dei dati personali che operano sotto la propria autorità e garantire che le persone autorizzate assumano idonei obblighi di riservatezza di tali dati, fornendo loro adeguate istruzioni per lo svolgimento delle attività di trattamento e verificandone l'osservanza;
- "conservare direttamente e specificatamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema" esclusivamente per quanto necessario per lo svolgimento di quanto previsto dal Contratto e all'attività di verifica almeno annuale dell'operato di questi amministratori di sistema "in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza, riguardanti i trattamenti dei dati personali, previste dalle norme vigenti" (come previsto dal Provvedimento del Garante sugli "amministratori di sistema" pubblicato in G.U. n. 300 del 24 dicembre 2008 e dalla sua modifica in base al provvedimento del 25 giugno 2009);
- assistere il Titolare nel garantire il rispetto, per quanto di relativa competenza, degli obblighi in tema di sicurezza, notifica all'autorità di eventuali violazioni di dati personali e, se del caso, loro comunicazione agli interessati, nonché di valutazione d'impatto sulla protezione dati ed eventuale consultazione preventiva, ai sensi degli articoli da 32 a 36 del GDPR, tenendo conto della natura del trattamento e delle informazioni a disposizione dello stesso Responsabile;
- comunicare al Titolare per iscritto, senza indebito ritardo, eventuali violazioni di sicurezza che riguardino i dati personali trattati ai fini della fornitura dei Servizi oggetto del Contratto;
- informare tempestivamente il Titolare in caso di ricevimento di richieste di informazioni o documenti, accertamenti ed ispezioni, da parte del Garante per la protezione dei dati personali, quale autorità competente di controllo, o di altre autorità giudiziarie o di polizia giudiziaria, ove attinenti al trattamento dei dati personali connesso alla fornitura dei Servizi oggetto del Contratto, e collaborare con il Titolare alla predisposizione dei correlati riscontri, atti, documenti o comunicazioni;
- cancellare o restituire al Titolare, su richiesta di quest'ultimo, tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancellare le copie esistenti, salvo che la vigente normativa europea o nazionale preveda la conservazione dei dati da parte del Responsabile che, in tal caso, ne darà contestuale attestazione al Titolare.

Il Responsabile si riserva, per la esecuzione di alcune parti delle attività commissionate, di nominare "Altri Responsabili" scelti nel proprio Albo dei Fornitori qualificati e che presentano garanzie sufficienti per mettere in atto misure tecniche e organizzative idonee a garantire il rispetto delle disposizioni della vigente Normativa sulla "Privacy" e si impegna a vincolare contrattualmente gli ulteriori responsabili al rispetto degli stessi obblighi in materia di protezione dei dati personali assunti dalla Società nei confronti del Titolare.
Al Titolare è riservata la facoltà di richiedere l'elenco degli "Altri Responsabili" incaricati e la relativa documentazione di incarico e di idoneità tecnico professionale.
Al Titolare è altresì riservata la facoltà di richiedere le modificazioni e/o integrazioni degli obblighi previsti in capo alla Società quale Responsabile del trattamento che si rendano necessarie a seguito dell'eventuale entrata in vigore di nuove disposizioni di legge, di regolamento ovvero di provvedimenti adottati da autorità amministrative o giudiziali in materia di tutela dei dati personali.
RPD (DPO) della Società
Il Titolare si è avvalso della facoltà prevista dall'art. 37 punto 6 del GDPR per procedere alla nomina di un "Responsabile unico della protezione dei dati" (RPD oppure DPO). Il responsabile della protezione dati assolvere i suoi compiti in base a un contratto di servizi.
Al fine di recepire quanto previsto dal GDPR, il Responsabile CED di concerto con Il Titolare e il DPO, ha adeguato la propria politica della sicurezza delle informazioni e i relativi obiettivi aggiornando il proprio Sistema di Gestione della Sicurezza delle Informazioni (SGSI), riferimento per tutte le procedure e le istruzioni inerenti alla sicurezza delle informazioni e alla protezione dei dati personali. Questa nuova versione del SGSI tende ad una maggiore conformità rispetto alla ISO/IEC 27002:2013.

5.1 "Privacy by design" e "Privacy by default"

In ottemperanza al principio di "responsabilizzazione" ("accountability") previsto nell'art. 5 del Regolamento, devono essere poste "in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento", tra cui quelle previste dall'art. 25, cioè:

- la Privacy by design per rispondere ai principi di protezione dei dati con "Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita"…"tenendo conto dello stato dell'arte e dei costi di attuazione" oltre che del contesto (tipo di dati, finalità, ecc.);

- la Privacy by default per limitare il trattamento ai soli “dati personali necessari”.

Il Responsabile inoltre, in ottemperanza al provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 (pubblicato nella Gazzetta Ufficiale n. 300, 24 Dicembre 2008), modificato in base al provvedimento del 25 giugno 2009, rende disponibile la verifica delle attività degli "Amministratori di Sistema" a beneficio dei Titolari del trattamento dei dati. Il provvedimento richiede - oltre alla valutazione delle caratteristiche soggettive dell’amministratore di sistema, alla sua designazione individuale, al suo inserimento in un elenco e alla verifica del suo operato - anche la registrazione dei suoi accessi (autenticazione informatica) ai sistemi ed agli archivi che contengono dati personali, mediante: monitoraggio delle attività di login e logout degli utenti da sistemi operativi ed ai database;
registrazione in maniera intellegibile ed estrazione su un apposito database per permetterne l ’inalterabilità richiesta dal Garante.
Gli archivi sono conservati e tenuti a disposizione del Titolare del trattamento per almeno sei mesi.

5.2 Identificazione dei rischi

L'infrastruttura ICT sottesa al Protocollo Informatico, nella sua componente legata al software applicativo e all'intera infrastruttura del Comune di Petilia Policastro, può essere così descritta per macro aree:

- reti e apparati di rete;
- elaboratori e software di sistema;
- software applicativo;
- supporti informatici di memorizzazione;
- infrastrutture;
- contenitori/archivi cartacei, archivi informatici di Backup.

Scopo dell'infrastruttura è la gestione del sistema di gestione documentale, garantendo i dati attraverso loro:

- **Riservatezza**: in modo che l'informazione sia resa disponibile solamente ai processi che la devono elaborare ed all'utilizzatore che ne è autorizzato all'uso;
- **Integrità**: in modo che ogni informazione sia realmente quella originariamente immessa nel sistema informativo, ovvero successivamente legittimamente modificata;
- **Disponibilità**: in modo che la reperibilità delle informazioni in funzione delle esigenze di continuità dei processi aziendali ed al fine del rispetto delle norme, tecniche e giuridiche, che ne impongono la conservazione storica.

I rischi cui è esposta l'infrastruttura ICT suindicata, per sua tecnicità e scopo, possono essere ricondotti a cinque macro categorie:

- rischio d’area legato all’accesso non autorizzato nei locali tecnici (cloud e on-prem);
- rischio di guasti tecnici hardware, software, supporti;
- rischio di penetrazione in reti di comunicazione, device e servizi;
- rischio legato ad errori umani;
- rischio d’area per possibili eventi distruttivi.

5.3 Definizione dei rischi

La definizione dei rischi si propone di mostrare i rischi identificati in forma strutturata.
Il **Rischio d’area legato all’accesso non autorizzato nei locali** può essere definito come la possibilità che soggetti non autorizzati accedano ai locali tecnici presso l’Ente (CED) piuttosto che DataCenter (del Cloud Service Provider).
In via indicativa, i rischi possono essere i seguenti:

- accesso ad uffici con collegamento telematico al sistema di gestione documentale;
- accesso al CED e alle aree di Backup;
- accesso alle aree informatiche per la connessione di rete, LAN/MAN e Internet.

Il **Rischio di guasti tecnici hardware, software, supporti**, può essere definito come la possibilità che strumenti fisici e logici si deteriorino o si danneggino, per caso fortuito, incuria o dolo, attraverso attività fisiche e logiche, in modo tale da non consentire la fruizione del sistema di gestione documentale.
In via indicativa, i rischi possono essere i seguenti:

- danneggiamento/deterioramento logico/fisico di supporti di memorizzazione, infrastrutture di rete, device;
- danneggiamento/deterioramento logico/fisico dei device presenti nel CED/DataCenter;
- danneggiamento/deterioramento logico/fisico dei device per il Disaster Recovery e la continuità di accesso ai servizi.

Il **Rischio di penetrazione in reti di comunicazione, device e servizi**, può essere definito come la possibilità che un soggetto non autorizzato abbia accesso alle reti di comunicazione dell'ente, sotto un profilo sia logico sia fisico.
In via indicativa, i rischi possono essere i seguenti:

- accesso alla rete telematica senza autorizzazione;
- violazione di reti e device attraverso attività fisiche;
- attacchi informatici, hacking e cracking;
- interruzione o sviamento del servizio di rete e/o web.

Il **Rischio legato a errori umani** può essere definito come la possibilità che, a causa di incuria o distrazione, il sistema di gestione documentale, o le sue attività, siano messe a rischio sotto il loro profilo logico e fisico.
In via indicativa, i rischi possono essere i seguenti:

- Accesso a device e punti rete incustoditi;
- attacchi d'Ingegneria sociale;
- Sovraccarico della rete e dei servizi per utilizzo anomalo delle console;
- interruzione prolungata di servizi elettrici, incendio e allagamento dei locali tecnici.

Il **Rischio d'area per possibili eventi distruttivi**, infine, può essere definito come la possibilità che, a seguito di eventi naturali di tipo distruttivo, il sistema di gestione documentale possa subire danni od interruzioni del servizio, non dipese dalla volontà del Comune di Petilia Policastro o del fornitore del software applicativo.
In via indicativa, i rischi possono essere i seguenti:

- danneggiamento/distruzione degli edifici e delle connessioni di rete;
- danneggiamento/distruzione dei device, di rete e forniti agli utenti, e dei software applicativi;
- danneggiamento/distruzione delle sale CED e Backup;
- danneggiamento/distruzione degli archivi per la conservazione dei dati in remoto.

5.4 Stima della criticità dei rischi

La stima della criticità dei rischi è effettuata attraverso una ponderazione composta da criteri di probabilità e livello del rischio. In particolare:
Criteri di probabilità:

- basso: improbabile
- medio: possibile
- elevato: altamente possibile Livelli di rischio:
- lieve: evento a basso impatto fisico-logico
- medio: evento a rilevante impatto fisico-logico
- grave: evento ad alto impatto fisico-logico.

5.5 Sviluppo di strategie

In base all'identificazione e alla definizione dei rischi, a seguito di loro stima per criteri di probabilità e livelli di rischio, il Comune di Petilia Policastro sviluppa strategie di contrasto e di mitigazione all'evento, atte a ridurre, eliminare o accettare i rischi individuati.
Le strategie sono elaborate dal Responsabile CED in cooperazione con il D.P.O.

5.6 Mitigazione

Il piano di mitigazione del rischio, ovvero della soluzione prevista, in base alle prerogative di sicurezza del Comune di Petilia Policastro, si fonda su una sua valutazione.
In particolare:

- se il rischio è considerato accettabile: stante le misure di sicurezza minime in essere e le mitigazioni generali performanti, il Comune di Petilia Policastro procedere ad un suo monitoraggio;
- se il rischio non è considerato accettabile: stante le misure di sicurezza minime in essere e le mitigazioni generali performanti, il Comune di Petilia Policastro procede alla revisione delle strategie di sicurezza al fine di individuare mitigazioni ulteriori e sanare il rischio.

5.7 Gestione dei rischi

La gestione dei rischi ICT ha come obiettivo l'analisi circa l'elaborazione di misure atte a modificare il livello di rischio e le strategie di mitigazione, migliorando la sicurezza e la performance dell'infrastruttura ICT.
La gestione del rischio è affidata al Responsabile CED.
Il rischio, in base a policy e procedure del Comune di Petilia Policastro, è differenziato in base al livello di criticità, al fine di affrontare in via principale i rischi più critici e, in via secondaria, i rischi meno critici.

Le misure atte a modificare il livello di rischio e le strategie di mitigazione sono elaborate dal Responsabile della gestione documentale, in cooperazione con il Responsabile CED.

6. POLITICHE DI SICUREZZA

Il paragrafo ha ad oggetto la descrizione delle politiche di sicurezza concernenti il sistema di gestione documentale, in particolare sotto il profilo della gestione dei sistemi, del controllo degli accessi fisici e logici, delle postazioni di lavoro, dei contenuti applicativi, degli apparati e supporti mobili, nonché della rete di comunicazione.

6.1 Politica di gestione della sicurezza dei sistemi

La gestione in sicurezza delle infrastrutture informatiche - recata da policy, procedure e prassi del Comune di Petilia Policastro, ha l'obiettivo di garantire che i sistemi, le postazioni di lavoro, le applicazioni, i servizi di rete, i servizi di elaborazione forniscano le prestazioni tecniche ai livelli e con i requisiti di sicurezza definiti.
I principi generali applicati per la gestione della sicurezza sono così sintetizzabili:

- gestione ed aggiornamento dell'inventario di asset hardware e software;
- applicazione di regole standard per l'installazione e la configurazione dei sistemi;
- configurazioni dei sistemi disegnate tenendo in considerazione le esigenze informatico giuridiche attuali e le possibili attività future;
- configurazioni dei sistemi indirizzate alla sicurezza built-in, atte a facilitare l'installazione di ulteriori misure di sicurezza;
- adozione di procedure standard per la configurazione dei sistemi
- attività regolari di monitoraggio sulle prestazioni dei sistemi per gestire adeguatamente eventi, problemi e incidenti.

6.2 Politica per il controllo degli accessi fisici

La politica per il controllo degli accessi prevede di consentire un accesso ai locali tecnici limitato al personale strettamente necessario autorizzato dal Responsabile dei Sistemi Informativi (personale del Comune di Petilia Policastro, personale di fornitori esterni se accompagnati).

6.3 Politica per l'inserimento dell'utenza e per il controllo degli accessi logici

La creazione dell'utenza è effettuata dal Responsabile CED su comunicazione dell'U.O. Affari Generali e del Personale del Comune di Petilia Policastro, attraverso software applicativo dedicato collegato al database degli accessi al dominio. Il flusso di creazione dell'utenza mostra i seguenti profili:

- indicazione di nuovo componente organico PA all'Ufficio CED;
- inserimento nel dominio ad opera dell'Ufficio CED;
- inserimento nel programma di gestione del personale ad opera dell'Ufficio CED;
- attribuzione dei ruoli specifici per l'applicativo protocollo ad opera dell'Ufficio CED, previa autorizzazione del competente dirigente.

Sono previste altresì dall'Ente procedure di cancellazione su comunicazione dell'U.O. Affari Generali e del Personale e/o di cambio di autorizzazione su comunicazione dei Dirigenti dei servizi competenti.

6.4 Politica di gestione delle postazioni di lavoro

La politica concernente la gestione delle postazioni di lavoro - disposta attraverso differenti policy, procedure e prassi del Comune di Petilia Policastro - mostra i seguenti elementi essenziali:

- provisioning delle postazioni di lavoro;
- regole per l'installazione del software sulle postazioni di lavoro;
- regole per gli aggiornamenti;
- regole per la limitazione della connettività a supporti esterni;
- regole per la modifica delle impostazioni;
- regole tecniche per l'accesso alla rete;
- regole per la creazione dei documenti informatici.

6.5 Politica di gestione del parco applicativo

La politica di gestione del Software si fonda sull'utilizzo di prassi che riguardano:

- la manutenzione dei sistemi;
- il controllo sul contenuto software dei client al fine di verificare la non presenza di codice malevolo sulle postazioni di lavoro;
- la conformità a quanto autorizzato e previsto dalle licenze d'uso.

L'attività è svolta attraverso utilizzo di antivirus/antispam/antimalware costantemente aggiornati, monitoraggio di flussi di rete e analisi preventiva di device, nonché schedulazione di interventi di manutenzione e osservazione delle prestazioni dell'hardware.

6.6 Politica di gestione, dismissione e smaltimento degli apparati e dei supporti

Le politiche di sicurezza del Comune di Petilia Policastro pongono particolare attenzione alla gestione degli apparati mobili, in particolare:

- device: portatili, tablet, smartphone, cellulari, ecc.
- supporti di memoria esterni: HD esterni/CD/DVD/Pen Drive/DAT/LTO, ecc.
- carta stampata: utilizzata e/o prodotta nell'ambito delle attività di protocollazione.

Per quanto concerne device e carta stampata, l'utilizzo è consentito, secondo policy, procedure e prassi dell'Ente pubblico, tali da indicare le modalità di utilizzo e conservazione dei dispositivi, nonché le politiche atte alla loro dismissione/distruzione.

6.7 Politica di gestione dei canali di comunicazione

I canali di comunicazione elettronici che attraversano il confine periferico dell'Ente vengono filtrati da Next Generation Firewall con funzionalità di Intrusion Prevention, Antivirus e Attack Detection per preservare la confidenzialità, e l'integrità, delle informazioni in transito, ed allo stesso tempo evitare abusi del canale elettronico e tentativi di intrusione.

6.8 Manutenzione delle politiche di sicurezza

Il Comune di Petilia Policastro dispone il perfezionamento, la divulgazione e il riesame delle politiche di sicurezza al verificarsi dei seguenti eventi:

- incidenti di sicurezza;
- variazioni tecnologiche significative;
- modifiche all'architettura informatica;
- aggiornamenti delle prescrizioni normative;
- risultati delle eventuali attività di audit interni ed esterni.

7. GESTIONE DEGLI INCIDENT

Si definisce "incidente di sicurezza" qualsiasi evento che comprometta o minacci di compromettere il corretto funzionamento dei sistemi e/o delle reti dell'organizzazione o l'integrità e/o la riservatezza delle informazioni in esse memorizzate od in transito, o che violi le politiche di sicurezza definite o le leggi in vigore. Ciò con particolare riferimento al d.lgs. 196/2003, alla L. 547/1993 ed alla L. 38/2006, al d.p.c.m. 03/12/2013 e al d.l. 2005/82.

Il Comune di Petilia Policastro classifica gli incidenti, definendone la codifica preventiva e la gestione degli stessi. Il processo di gestione degli incidenti è articolato nelle seguenti fasi:

- **Rilevazione/identificazione/classificazione**: sono riconosciuti uno o più eventi di sicurezza come incidente e a ogni incidente ne viene assegnato un livello di gravità. Il rilevamento avviene a valle delle segnalazioni provenienti da strumenti automatici o ancora da segnalazioni del personale dell'amministrazione;
- **Contenimento**: sono attuate le prime contromisure, allo scopo di minimizzare i danni causati dall'incidente. In genere si tratta di azioni temporanee e veloci, di cui effettuare il roll -back dopo la successiva fase di eliminazione;
- **Eliminazione**: sono eliminate le cause che hanno portato al verificarsi dell'incidente;
- **Ripristino**: sono effettuate le operazioni necessarie per riparare i danni causati dall'incidente e si effettua il roll-back delle contromisure di contenimento;
- **Follow-up**: è verificata l'adeguatezza delle procedure di gestione degli incidenti e vengono identificati i possibili punti di miglioramento.

Le procedure di gestione degli incidenti sono demandate, per quanto concerne il sistema di gestione documentale, all'U.O. Sistemi Informativi.

7.1 Processo di gestione degli incident

Più in dettaglio, il modello generale che governa il processo di gestione degli incident deriva dalle migliori pratiche del framework ITIL secondo la seguente metodologia, suscettibile di miglioramenti ed ottimizzazioni in fase di esercizio in funzione di nuove tipologie di minacce nonché della disponibilità di nuove tecnologie e/o evoluzione di quelle presenti atte a contrastarle e mitigarle:

- analisi del contesto;
- ricezione richiesta/segnalazione da parte dell'utente interno all'Ente, oppure rilevazione non sollecitata di una necessità a seguito di controlli periodici o segnalazioni automatiche real-time da strumento di monitoring;

- inserimento nel sistema di ticketing della richiesta/segnalazione/necessità;
- analisi preliminare della richiesta/segnalazione/necessità al fine di limitare inefficienze e problemi per non corrette interpretazioni e/o falsi positivi;
- assegnazione all'intervento di un livello di priorità;
- assegnazione dell'intervento ad un tecnico o gruppo di tecnici in base a complessità;
- pianificazione dell'attività analizzando tutti i fattori ritenuti utili e/o critici (interdipendenze, sinergie tra risorse onsite e/o remote, tempistiche, leveraging esperienziale sulla base di attività analoghe pregresse e di best practice comprovate);
- preparazione dell'intervento attraverso l'analisi di quanto verificatosi in caso di incident/problem, identificazione degli ambiti e degli stakeholder anche esterni, monitoraggio degli SLA, effettuazione di backup delle configurazioni prima dell'intervento;
- attuazione di processi autorizzativi a vari livelli durante l'esecuzione delle attività in base alle classi di intervento concordate e gestione del processo di escalation;
- esecuzione dell'intervento (in loco, o da remoto, etc.) con particolare attenzione alla definizione concordata dei tempi di intervento e minimizzazione dei tempi di disservizio, completezza, efficienza ed efficacia dell'intervento, comunicazione dell'avvenuta esecuzione all'Ente e relativi stakeholder definiti in fase di pianificazione e altri rilevati nel corso dell'intervento, inserimento dello stato avanzamento nel sistema di ticketing, compilazione della documentazione di Knowledge Base quando necessario;
- esecuzione reiterata dell'intervento in caso di mancata risoluzione al primo tentativo con eventuale escalation verso fornitori esterni e/o l'eventuale supporto di figure tecniche specialistiche fino alla completa risoluzione;
- chiusura del caso con comunicazione ai soggetti interessati