PADIGITALE
INNOVAZIONE PER LA PUBBLICA AMMINISTRAZIONE
WEB TECHNOLOGY FOR A REAL INNOVATION

Allegato n. 3 al Manuale del Sistema di Gestione Integrato
aggiornato al 15/02/2022

POLITICA AZIENDALE DELLA SICUREZZA DELLE INFORMAZIONI

Revisione 12 del 15/02/2022

	EMESSO	APPROVATO
Funzione	**Responsabile Gestione Sicurezza delle Informazioni**	**Amministratore Delegato**
Data	15/02/2022	15/02/2022
Firma		

INDICE

1. SCOPO, CAMPO DI APPLICAZIONE E PROFILO AZIENDALE

1.1 Scopo

Scopo della presente Politica Aziendale è descrivere il Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) della società PA DIGITALE S.p.A.

1.2 Campo di Applicazione

Oggetto del Sistema di Gestione per la Sicurezza delle Informazioni:

Analisi, progettazione, sviluppo, produzione, installazione, commercializzazione, distribuzione, manutenzione e assistenza di prodotti software per la Pubblica Amministrazione Locale e Centrale e per il Mercato Privato, erogati in modalità SaaS oppure erogati con installazione in locale (on premise). Erogazione dei servizi professionali connessi ai prodotti software. Erogazione dei servizi SaaS in cloud per la Conservazione Digitale di documenti informatici a Norma e relativo servizio di assistenza.

Tutti i requisiti della Norma UNI CEI EN ISO/IEC 27001:2017 trovano applicazione nell'ambito del Sistema di Gestione della Sicurezza delle Informazioni (SGSI).
Nel Sistema di Gestione per la Sicurezza delle Informazioni di PA Digitale S.p.A. trovano altresì applicazione le Linee Guida ISO/IEC 27017:2015 e ISO/IEC 27018:2019. Infine, nell'ambito del Sistema di Gestione Integrato aziendale, il Sistema di Gestione per la Sicurezza delle Informazioni di PA Digitale S.p.A. è integrato con il Sistema di Gestione per la Qualità (UNI EN ISO 9001:2015) ***e con le seguenti norme in corso di adozione:***

- ***UNI CEI ISO/IEC 20000-1:2020***
- ***UNI EN ISO 22301:2019***
- ***UNI EN ISO 37001:2016***
- ***UNI ISO 45001:2018***

1.3 Profilo aziendale

PA Digitale S.p.A. nasce nel 2009 per rispondere alle necessità di innovazione della Pubblica Amministrazione e alla spinta di accelerazione verso la digitalizzazione.
La completezza dell'offerta, la scelta strategica della tecnologia CLOUD COMPUTING - di seguito Cloud - definita anche SaaS (Software As A Service) o ASP (Application Service Providing), un tipo di approccio che valorizzi le esigenze dei clienti e la capacità di coordinare, gestire e realizzare progetti, permettono a PA Digitale di sviluppare prodotti e servizi di qualità che garantiscono all'ente di disporre di soluzioni software rispondenti all'evoluzione tecnologica e organizzativa della Pubblica Amministrazione e, dal 2014, anche per il mercato privato.
Pur mantenendo una forma giuridica indipendente, PA Digitale S.p.A. è entrata a far parte del Gruppo Buffetti S.p.A., cui fanno capo alcune tra le più rinomate aziende del panorama industriale italiano (Buffetti, Cartiere Pigna, Dylog, Intesi Group, ecc.).
In passato, PA Digitale S.p.A. è stata la prima software house per la Pubblica Amministrazione in Italia ad essere iscritta nell'elenco dei Conservatori di

documenti informatici dell'Agenzia per l'Italia Digitale, e oggi è tra le prime ad essere stata qualificata all'Elenco dei conservatori iscritti al Marketplace dei servizi di conservazione di AgID (https://conservatoriqualificati.agid.gov.it/), ai sensi delle Linee guida di cui all'art 71 del CAD relative alla formazione, gestione e conservazione dei documenti informatici e del Regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici.
L'Azienda è in grado di affiancare imprese, professionisti e pubbliche amministrazioni nei processi di conservazione digitale dei loro documenti informatici con un sistema di conservazione a norma, molto qualificato, governato e gestito da figure professionali capaci di garantire il costante aggiornamento e la conformità dei sistemi e dei processi all'evoluzione normativa e tecnologica.

La struttura organizzativa

Il personale di PA Digitale è altamente qualificato, con un'esperienza professionale ed elevate competenze specifiche nel mercato privato e della Pubblica Amministrazione Locale e Centrale.
L'azienda dispone di una infrastruttura informatica in grado di fornire un efficiente e puntuale supporto alle attività di progettazione, sviluppo, commercializzazione, manutenzione e assistenza dei prodotti software offerti.
PA Digitale è da sempre attenta a offrire servizi efficienti e professionali attraverso una struttura organizzativa che assicura:

- competente supporto pre-vendita (analisi delle esigenze, studio della soluzione, ecc.);
- efficace struttura produttiva di tutto il ciclo di vita del software che, partendo dalle analisi funzionali, implementa con rigore ingegneristico il software medesimo;
- tempestivo e valido servizio post-vendita (installazione, avviamento, assistenza, ecc.);
- puntuale e completa formazione per utilizzare al meglio tutte le potenzialità delle proprie soluzioni;
- costante aggiornamento del software distribuito.

Nei servizi via Internet in modalità Cloud PA Digitale è sinonimo di sicurezza, garantita da un Internet Data Center con Sistema di Gestione della Sicurezza delle Informazioni certificato in conformità alla norma ISO/IEC 27001:2013, che ospita apparecchiature per la trasmissione dati e architetture hardware/software preposte a erogare servizi in condizioni di completa sicurezza informatica e altissima affidabilità.

La rete commerciale

La rete commerciale è composta da un gruppo di funzionari addetti alla vendita diretta, oltre a una propria rete tecnico/commerciale composta da circa 30 partner con strutture complete e distribuite sull'intero territorio nazionale, per servizi commerciali, di avviamento, formazione, installazione e assistenza software.

L'offerta applicativa

PA Digitale vanta più di 1000 procedure software erogate in modalità SaaS oppure on premise presso circa 800 clienti (Ministeri ed enti ministeriali, Regioni, Province, Comuni, Comunità montane, Unioni di Comuni, Consorzi, Enti Socio-Sanitari, Università, Enti Regionali, Soprintendenze, ecc.), e oltre 400.000 applicazioni erogate per clienti del

mercato privato. La quasi totalità di questi clienti utilizza la Conservazione Digitale a Norma erogata da PA Digitale stessa.

Il contesto della presente politica è focalizzato su:

- Erogazione di soluzioni applicative (delle linee Urbi e WebTec) in modalità sia SaaS che on premise (Analisi, progettazione, sviluppo, produzione, installazione, commercializzazione, distribuzione, manutenzione e assistenza di prodotti software per la Pubblica Amministrazione Locale e Centrale e per il mercato privato), comprensiva di erogazione dei servizi professionali.
- Erogazione dei servizi SaaS in Cloud per la Conservazione Digitale di documenti informatici a Norma e relativo servizio di assistenza.

COMPETENZE E ORGANIZZAZIONE

Le strutture della PA DIGITALE S.p.A. sono a:

Italia Nord

- Pieve Fissiraga (LO) - Via Leonardo da Vinci n. 13: Sede Legale, Amministrativa e operativa
  - ***Direzione Generale (Amministratore Delegato)***
  - ***Area Compliance***
  - ***Area Affari Direzionali e Societari***
  - ***Area Osservatorio Normativo - Piattaforme Pubbliche Abilitanti***
  - ***Area Marketing Operativo - Strategia della Comunicazione***
  - ***Area Amministrazione e Contabilità***
  - ***Area Personale - Salute Sicurezza Lavoro - Finanza***
  - ***Area Tecnica***
  - ***Area Sicurezza Informatica***
  - ***Area Offerta Aziende del Gruppo***
  - ***Area Mercato Privato (comprendente Area Commerciale Mercato Privato, Prodotti Mercato Privato, Gestione Clienti Mercato Privato ed Help Desk Clienti Mercato Privato)***
  - ***Area Mercato Pubblica Amministrazione (comprendente Area Commerciale - NORD EST e NORD OVEST, Gestione Gare Pubbliche Mercato Pubblica Amministrazione, Gestione Clienti Mercato Pubblica Amministrazione ed Help Desk Clienti Mercato Pubblica Amministrazione)***
  - ***Area Software Factory***
  - ***Servizio Conservazione Digitale a Norma***
  - ***Sistema Informativo Aziendale (Infrastruttura hardware)***
  - ***Sistema Informativo Aziendale (software gestionale)***

Italia Centro

- Arezzo (AR) - Via Gobetti n. 21: Sede operativa
  - ***Area Mercato Pubblica Amministrazione (comprendente Area Commerciale - CENTRO, Gestione Clienti Mercato Pubblica***

Amministrazione ed Help Desk Clienti Mercato Pubblica Amministrazione)
- ***Area Software Factory***

Roma
- Roma (RM) - Via Filippo Caruso, 23: Sede solo Commerciale*
  - ***Area Mercato Pubblica Amministrazione - Commerciale rivolta alla Pubblica Amministrazione Centrale***

Italia Sud
- Napoli (NA) - Via G. Porzio n. 4 Centro Direzionale Isola E3 - 7° piano: - Sede operativa
  - ***Area Mercato Pubblica Amministrazione (comprendente Area Commerciale - SUD, Gestione Clienti Mercato Pubblica Amministrazione ed Help Desk Clienti Mercato Pubblica Amministrazione)***
  - ***Area Amministrazione Clienti e Contabilità***

La Sede fisica di Roma è l'unica sede non interessata dal Sistema di Gestione della Sicurezza delle Informazioni. Sui processi inerenti il servizio di Conservazione Digitale a Norma (in particolare nel servizio di assistenza) operano addetti in tutte le sedi (Roma esclusa).

2. RIFERIMENTI

La presente politica descrive gli elementi del Sistema di Gestione della Sicurezza delle Informazioni in conformità alla Norma UNI CEI EN ISO/IEC 27001:2017.

3. DEFINIZIONI

Sistema di Gestione per la Sicurezza delle Informazioni (SGSI)
Quella parte del sistema di gestione complessivo, basata su un approccio rivolto al rischio relativo al business, volta a stabilire, attuare, condurre, monitorare, riesaminare, mantenere attivo, aggiornato e migliorare la sicurezza delle informazioni.
Nota: Il sistema di gestione include la struttura organizzativa, le politiche, le attività di pianificazione, le responsabilità, le prassi, le procedure, i processi e le risorse.

Sicurezza delle Informazioni
Conservazione della riservatezza, dell'integrità e della disponibilità delle informazioni; inoltre, possono essere coinvolte altre proprietà quali l'autenticità, la responsabilità, il non ripudio e l'affidabilità.

Disponibilità
Proprietà di essere accessibile e utilizzabile su richiesta di un'entità autorizzata.

Riservatezza
Proprietà per cui l'informazione non è resa disponibile o rivelata a individui, entità o processi non autorizzati

Integrità
Proprietà relativa alla salvaguardia dell'accuratezza e della completezza dei beni.

4. POLITICA AZIENDALE DELLA SICUREZZA DELLE INFORMAZIONI

4.1 Motivazione

PA Digitale S.p.A. è ***un'Azienda che eroga soluzioni legate*** all'Information technology, e in particolare ha realizzato:

- Erogazione di soluzioni applicative in modalità sia SaaS che on premise di prodotti software per la Pubblica Amministrazione Locale e Centrale (della linea Urbi) e per il mercato privato (della linea WebTec)
- un Servizio di Conservazione Digitale a Norma dei Documenti Informatici.

Le soluzioni sopra indicate sono declinate nel Piano di Gestione dei Servizi istituito per la norma UNI CEI ISO/IEC 20000-1:2020, ovvero:

- ***Analisi, progettazione, sviluppo, produzione e manutenzione di Software erogati anche in modalità SaaS***
- ***Assistenza per i Servizi SaaS e Conservazione Digitale a Norma ed erogazione di servizi professionali***
- ***Erogazione del Software come Servizio - SaaS per il Mercato Pubblica Amministrazione e per il Mercato Privato***
- ***Erogazione del Software come Servizio - SaaS di Conservazione Digitale a Norma***
- ***Commercializzazione e distribuzione di Software erogati anche in modalità SaaS***

Data la natura delle proprie attività, e vista la Normativa vigente per quanto concerne l'erogazione di soluzioni applicative in modalità sia SaaS che on premise di prodotti software per la Pubblica Amministrazione Locale e Centrale e Servizi di Conservazione Digitale dei Documenti a Norma per le Pubbliche Amministrazioni e per il mercato privato, PA Digitale S.p.A. considera la sicurezza delle informazioni un fattore irrinunciabile per la protezione del patrimonio informativo dei propri clienti e un fattore di valenza strategica facilmente trasformabile in vantaggio competitivo. Inoltre pone particolare attenzione ai temi riguardanti la sicurezza durante l'erogazione del servizio, che deve essere ritenuto un bene primario dell'azienda. Il SGSI si applica a tutte le attività di:

- Analisi, progettazione, sviluppo, produzione, installazione, commercializzazione, distribuzione, manutenzione e assistenza di prodotti software per la Pubblica Amministrazione Locale e Centrale (della linea Urbi), comprensiva di erogazione dei servizi professionali
- Analisi, progettazione, sviluppo, produzione, installazione, commercializzazione, distribuzione, manutenzione e assistenza di prodotti software per il mercato privato (della linea WebTec), comprensiva di erogazione dei servizi professionali

- Analisi, progettazione, messa in esercizio ed esercizio stesso del Servizio di Conservazione Digitale a Norma e dei dati ad esso collegato, nonché ai servizi di assistenza al cliente.

In particolare cura la tutela dell'accesso ai sistemi sia fisici che logici.
Consapevole del fatto che l'erogazione dei servizi per soggetti esterni può comportare l'affidamento di dati e informazioni critiche, l'unità organizzativa che si occupa della progettazione ed erogazione di tali servizi opera secondo normative di sicurezza internazionalmente riconosciute.
Per questi motivi si intendono adottare le misure, sia tecniche che organizzative, necessarie a garantire al meglio l'integrità, la riservatezza e la disponibilità del patrimonio informativo affidato a PA Digitale S.p.A. dai propri Clienti.
Su tale linea PA Digitale S.p.A. ha deciso di porre in essere un Sistema di Gestione per la Sicurezza delle Informazioni definito secondo regole e criteri previsti dalle "best practice" e dagli standard internazionali di riferimento, in conformità anche alle indicazioni della norma UNI CEI EN ISO/IEC 27001:2017, nonché alle Linee Guida ISO/IEC 27017:2015 e ISO/IEC 27018:2019.

4.2 Obiettivi

L'obiettivo del Sistema di Gestione per la Sicurezza delle Informazioni di PA Digitale è di garantire un adeguato livello di sicurezza dei dati e delle informazioni attraverso l'identificazione, la valutazione e il trattamento dei rischi a cui i propri servizi e le proprie soluzioni sono soggette, nell'ambito del campo di applicazione sopra indicato.
Il Sistema di Gestione per la Sicurezza delle Informazioni di PA Digitale definisce un insieme di misure organizzative, tecniche e procedurali a garanzia del soddisfacimento dei sotto elencati requisiti di sicurezza di base:

- Riservatezza, ovvero la proprietà dell'informazione di essere nota solo a chi ne ha i privilegi;
- Integrità, ovvero la proprietà dell'informazione di essere modificata solo ed esclusivamente da chi ne possiede i privilegi;
- Disponibilità, ovvero la proprietà dell'informazione di essere accessibile e utilizzabile quando richiesto dai processi e dagli utenti che ne godono i privilegi.

Inoltre con la presente politica PA Digitale intende formalizzare i seguenti obiettivi nell'ambito della sicurezza delle informazioni:

- Preservare al meglio l'immagine dell'azienda quale fornitore affidabile e competente;
- Proteggere il patrimonio informativo dei propri clienti;
- Evitare al meglio ritardi nel rilascio dei servizi erogati;
- Adottare le misure atte a garantire la fidelizzazione del personale e la sua crescita professionale;
- Rispondere pienamente alle indicazioni della normativa vigente e cogente;
- Aumentare, nel proprio personale, il livello di sensibilità e la competenza su temi di sicurezza.

4.3 Contenuto della Politica

Il SGSI si applica a tutte le attività di erogazione dei servizi legati:

- all'erogazione di soluzioni applicative in modalità sia SaaS che on premise di prodotti software per la Pubblica Amministrazione Locale e Centrale (della linea Urbi)
- all'erogazione di soluzioni applicative in modalità sia SaaS che on premise di prodotti software per il mercato privato (della linea WebTec)
- al Servizio di Conservazione Digitale a Norma

e ai dati ad essi collegati.

Tutte le informazioni che vengono create o utilizzate dall'Azienda sono da salvaguardare e debbono essere protette, secondo la classificazione attribuita, dalla loro creazione, durante il loro utilizzo, fino alla loro eliminazione. Le informazioni debbono essere gestite in modo sicuro, accurato e affidabile e debbono essere prontamente disponibili per gli usi consentiti. È qui da intendersi con "utilizzo dell'informazione" qualsiasi forma di trattamento che si avvalga di supporti elettronici, cartacei o consenta, in una qualsiasi forma, la comunicazione verbale.

La Politica della Sicurezza delle Informazioni adottata da PA Digitale deve costituire un approccio sistematico alla sicurezza delle informazioni per tutti i componenti dell'organizzazione che - a qualsiasi titolo - possono intervenire su qualsiasi informazione presente all'interno dell'Azienda, nell'ambito del campo di applicazione sopra indicato. Per quanto la Politica della Sicurezza delle Informazioni, essa si basa sui principi fondamentali di seguito descritti.

Per quanto riguarda in modo specifico il trattamento dei dati personali, si rimanda alla Politica in materia di trattamento e protezione dei dati personali.

L'erogazione dei Servizi in modalità Cloud Computing (Servizi SaaS e Servizio di Conservazione Digitale a Norma) è basata sull'infrastruttura fornita da un Internet Data Center gestito da un Fornitore esterno i cui siti risiedono sul territorio nazionale. La Politica Aziendale della Sicurezza di PA Digitale prevede che tale Fornitore abbia a sua volta una certificazione ISO/IEC 27001:2013 (nonché alle Linee Guida ISO/IEC 27017:2015 e ISO/IEC 27018:2019) nell'ambito del servizio di data center fornito a PA Digitale, e che la filiera dei suoi eventuali fornitori sia monitorata.

4.3.1 Coinvolgimento e responsabilità delle risorse umane

Il SGSI deve essere pienamente recepito, accettato e compreso da tutto il personale in organico in azienda, senza alcuna esclusione. Tale coinvolgimento è necessario perché, nell'ambito di azione dell'organizzazione, ogni collaboratore non solo può entrare in contatto con alcune o tutte le informazioni custodite e trattate dall'azienda, ma comunque può prendere visione e conoscere i meccanismi di sicurezza e protezione di PA Digitale nell'ambito del campo di applicazione sopra indicato. PA Digitale adotta pertanto le seguenti linee guida:

- attivazione di processi di formazione periodici per tutto il personale coinvolto, in materia di:

  - riservatezza e confidenzialità delle informazioni;
  - politica aziendale della sicurezza;
  - procedure interne;
  - normative vigenti.
- creazione di un ambiente consapevole dell'importanza della sicurezza e dei rischi relativi, attraverso l'impegno diretto dei responsabili aziendali;
- adozione di strumenti di diffusione e aggiornamento indiretti, tramite l'uso del sistema informatico di bacheca aziendale e del Sistema Documentale interno.

4.3.2 Organizzazione per la sicurezza

Per poter governare il SGSI PA Digitale, nell'ambito del campo di applicazione sopra indicato, definisce e istituisce al proprio interno una specifica organizzazione operativa denominata Comitato di Sicurezza Informatica, composta da almeno un rappresentante delle Aree aziendali che hanno impatto sulla sicurezza delle informazioni:

Presidente del Comitato	Amministratore Delegato
Componente	Responsabile Sicurezza Informatica
Componente	Operatore Area Tecnica
Componente	***Responsabile Produzione Software Factory***
Componente	Responsabile del Servizio di Conservazione
Componente	Responsabile dello Sviluppo del Sistema di Conservazione
Componente	Responsabile per la Gestione della Sicurezza delle Informazioni

L'organizzazione interna ha i seguenti obiettivi:
- controllare la sicurezza delle informazioni in seno all'organizzazione;
- verificare l'attuazione dei controlli selezionati;
- sovrintendere i processi e le attività legate alla sicurezza;
- definire le modalità per il monitoraggio e la revisione del SGSI;
- farsi carico dei processi di mantenimento, evoluzione e miglioramento del sistema.

Le linee guida per la istituzione e l'operatività di tale organizzazione sono:
- individuazione dei componenti della struttura nell'ambito della direzione e delle figure chiave aziendali, anche in base alla preparazione e all'esperienza (Comitato di Sicurezza Informatica, come sopra definito);
- inserimento di almeno un elemento esterno;
- contatto con organizzazioni ed enti di riferimento per la problematica;
- utilizzo costante degli strumenti operativi (riunioni, comunicazioni interne, ecc.) tali da rendere attivo e propositivo il lavoro del gruppo.

4.3.3 Controllo e classificazione delle risorse

Per una corretta attuazione del SGSI è necessaria un'appropriata classificazione delle risorse, in modo da garantirne l'appropriato controllo e la precisa individuazione dei relativi livelli di protezione. La classificazione delle risorse avviene a partire dall'analisi dei processi aziendali, in modo da individuarle e classificarle in base alle informazioni entro-contenute. Tale controllo deve rispettare le seguenti linee guida sotto indicate.

Classificazione delle informazioni trattate in azienda, individuate sulla base dell'analisi dei processi aziendali (segnatamente entro il dominio di applicazione del SGSI), in modo da individuare, controllare e classificare tre tipologie di risorse:

1 Asset Processi Aziendali (principali);
2 Asset informazioni (secondari);
3 Asset fisici (secondari);
4 Asset informatici (secondari);
5 Asset personale (secondari).

Linee guida:

- La classificazione degli Asset è a cura del Responsabile Area Tecnica, del Responsabile della Sicurezza Informatica e del Responsabile Gestione Sicurezza delle Informazioni;
- L'aggiornamento dell'elenco degli Asset deve avvenire ad ogni variazione;
- Il Responsabile Gestione Sicurezza delle Informazioni si assicura che l'elenco degli Asset sia sempre aggiornato.

Il controllo degli Asset deve essere effettuato in maniera incrociata, tra l'analisi dei processi aziendali coinvolti nell'ambito del SGSI e l'inventario diretto dei beni e delle risorse.

4.3.4 Analisi dei rischi

Relativamente all'ambito del SGSI, tale sistema deve prevedere - in conformità alla norma UNI CEI EN ISO/IEC 27001:2017 - che sia condotta con frequenza almeno annuale un'analisi dei rischi, che tenga in considerazione gli obiettivi strategici espressi nella presente politica, degli incidenti occorsi durante tale periodo e dei cambiamenti strategici, di business e tecnologici avvenuti.

Tale analisi sarà ponderata anche rispetto al valore di business degli Asset principali e dovrà identificare chiaramente le azioni da intraprendere che saranno classificate secondo una scala di priorità che rispetti gli obiettivi aziendali, il budget a disposizione e la necessità di mantenere la conformità alle norme e leggi vigenti. Detta analisi dovrà essere effettuata anche a fronte di eventi che possano modificare il profilo di rischio complessivo del sistema.

L'analisi dei rischi viene effettuata sugli Asset principali attraverso l'analisi sugli Asset secondari ad essi collegati.

4.3.5 Sicurezza e responsabilità del personale

Gli obiettivi che PA Digitale intende raggiungere attraverso la responsabilizzazione del personale sono:

- ridurre il rischio di errori umani, furto, frode o uso improprio delle strutture dell'organizzazione coinvolte nell'ambito del SGSI;
- accertarsi che gli utenti interni siano informati sulle minacce alla sicurezza delle informazioni e siano formati a sostenere le politiche di sicurezza aziendali nel corso della propria attività lavorativa;
- minimizzare il danno per incidenti e malfunzionamenti circa la sicurezza e mettere a frutto l'esperienza di avvenimenti precedenti.

Le linee guida sono:

- individuare il personale direttamente coinvolto nei trattamenti delle informazioni, nell'uso e nella gestione delle risorse incluse nel dominio del SGSI;
- selezionare nuove figure, se necessario;
- verificarne l'adeguatezza;
- definire e rendere evidenti a tutte le persone coinvolte le modalità di accesso alle informazioni, i controlli e le registrazioni di tali accessi.

Inoltre, si rende necessario imporre il rispetto delle regole in maniera tassativa, per tutti coloro che in PA Digitale hanno accesso, a qualsiasi titolo, ai dati presenti in azienda e correlati all'ambito di applicazione del SGSI, inclusi quindi gli eventuali responsabili, gli incaricati, o qualsiasi fornitore o terza parte esterna.

4.3.6 Sicurezza materiale e ambientale

Gli obiettivi di PA Digitale sono:

- impedire l'accesso non autorizzato, il danneggiamento e l'interferenza all'interno del flusso delle informazioni di "business";
- impedire la perdita, i danni ai beni del sistema e la interruzione delle attività economiche;
- impedire la manomissione o il furto delle informazioni. Devono essere adottate misure di sicurezza di natura fisica, tecnica ed elettronica delle quali venga resa evidenza nelle procedure attuative del SGSI;
- avvalersi di Certification Authority riconosciute per quanto riguarda soluzioni di crittografia utilizzate per accedere ai dati tramite interfaccia web based.

Per la definizione e l'attuazione di tali misure gli elementi di riferimento adottati sono:

- progettazione e realizzazione di ambienti, impianti e dispositivi di prevenzione rispetto a furti, incendi, calamità, ecc.; a tal fine PA Digitale fa ricorso a progettisti specializzati in materia e/o fornitori esterni anch'essi certificati ISO/IEC 27001:2013;
- rispetto di tutte le normative e regolamenti vigenti in materia;
- definizione di controlli periodici adeguati sugli impianti, sui locali e sui dispositivi tali da garantirne la continuità e il miglioramento nel tempo;
- sistemi di allarme, controllo e autorizzazione degli accessi che permettano la gestione di zone e aree differenziate all'interno dell'organizzazione;
- progettazione e implementazione di sistemi informatici - e uso di appropriati apparati complementari - in grado di garantire continuità di funzionamento anche in caso di guasti improvvisi prevedendo, ad esempio, apparati "fault tolerant", alimentazione ridondante, gruppi di continuità e gruppi elettrogeni. A tal proposito PA Digitale fa sempre ricorso a progettisti e ingegneri qualificati in materia e/o a fornitori esterni anch'essi certificati ISO/IEC 27001:2013.

Le variazioni e le modifiche vengono sempre notificate per tempo a tutti i responsabili coinvolti in modo da generare una adeguata circolazione e condivisione delle modifiche alla struttura e alle misure di sicurezza.

4.3.7 Computer and Network Management

Gli obiettivi e le linee guida adottate sono:

- assicurare il corretto e sicuro funzionamento delle funzioni di elaborazione delle informazioni;
- minimizzare il rischio di guasti dei sistemi;
- proteggere l'integrità del software e delle informazioni;
- gestire l'integrità e la disponibilità dei processi di elaborazione dell'informazione e della comunicazione;
- garantire la salvaguardia delle informazioni in rete e la protezione delle infrastrutture di supporto;
- prevenire i danni ai servizi e le interruzioni alle attività economiche;
- evitare la perdita, modifica o abuso delle informazioni scambiate tra le organizzazioni.

4.3.8 Controllo degli accessi

Gli obiettivi e le linee guida adottate sono:

- controllare l'accesso alle informazioni;
- assicurare la protezione dei servizi in rete;
- prevenire l'accesso non autorizzato ai sistemi;
- rilevare attività non autorizzate;
- garantire la sicurezza delle informazioni quando sono utilizzate dalle postazioni mobili in servizi di rete e telematici.

PA Digitale definisce e organizza al proprio interno articolati sistemi di autenticazione e di gestione dei permessi di accesso ai sistemi, prevedendo il riconoscimento sia delle eventuali postazioni di lavoro usate per l'accesso automatico a tali sistemi sia del personale incaricato dell'attività.
In quest'ambito sono previsti sistemi di documentazione degli accessi che consentano l'identificazione di anomalie e non sono ammessi programmi di utilities potenzialmente in grado di annullare i controlli dei sistemi e delle applicazioni. Inoltre le sessioni inattive sono disattivate automaticamente dopo un determinato periodo di inattività e sono poste limitazioni automatiche ai tempi di connessione per fornire sicurezza aggiuntiva alle applicazioni ad alto rischio che erogano:

- soluzioni applicative di prodotti software per la Pubblica Amministrazione Locale e Centrale (della linea Urbi), erogate anche in modalità SaaS
- soluzioni applicative di prodotti software per la il mercato privato (della linea WebTec), erogate anche in modalità SaaS
- il Servizio di Conservazione Digitale a Norma

4.3.9 Scambio di informazioni

PA Digitale adotta una politica selettiva per lo scambio di informazioni, in particolare verso l'esterno. A tal proposito ha provveduto a classificare le informazioni e a determinare le modalità e gli strumenti di scambio, per ogni classe di informazione. L'obiettivo di tale attività è quello di mantenere la sicurezza delle informazioni e del software scambiati all'interno dell'organizzazioni e con entità esterne. Nell'ambito del Servizio di Conservazione Digitale a Norma non è previsto l'utilizzo di supporti rimovibili. L'accesso alle informazioni avviene tramite sistema web based e anche al termine dei contratti in

essere con i clienti, il materiale può essere scaricato dal sistema, senza l'utilizzo di media rimovibili quali a titolo di esempio CD, DVD o altro.

4.3.10 Sviluppo e manutenzione dei sistemi

Gli obiettivi sono:

- garantire che la sicurezza sia applicata correttamente in tutti sistemi in funzione;
- garantire il corretto uso, dimensionamento, controllo e manutenzione di tutti sistemi in esercizio;
- prevenire la perdita, modifica o cattivo utilizzo dei dati nei sistemi applicativi;
- proteggere la riservatezza, autenticità e integrità dell'informazione;
- assicurare che attività sul software utilizzato per l'erogazione del servizio e attività di supporto siano condotte in modo sicuro;
- gestire la sicurezza del software e dei dati di sistema.

Ai fini della corretta gestione di questa fase, l'azienda implementa procedure organizzative che consentano la regolare applicazione di tutte le idonee soluzioni di sicurezza e di dimensionamento, sia preventive che correttive. Sono inoltre previste politiche di evoluzione del sistema SGSI che definiscono obiettivi e controlli significativi e applicabili all'organizzazione del sistema.

Le linee guida definite in tale area sono:

- analisi e progettazione di architetture e sistemi condivise con tutte le funzioni aziendali coinvolte e con il ricorso a specialisti preventivamente selezionati;
- definizione di adeguate procedure e regole di sicurezza per la gestione dei controlli di accesso ai sistemi dall'interno e dall'esterno della rete, della protezione fisica e logica dei sistemi con tutti gli strumenti disponibili allo stato dell'arte della tecnologia;
- ricorso a politiche di backup complete e diversificate per garantire la ridondanza delle informazioni salvate;
- implementazione di idonee soluzioni di "disaster recovery";
- definizione di adeguate procedure e regole di sicurezza per la gestione dei controlli e della supervisione di reti e sistemi;
- divieto di utilizzo di mobile code;
- azione preventiva per l'individuazione, la definizione e la gestione di procedure di analisi, progettazione, sviluppo e manutenzione del software prodotto internamente alla struttura;
- definizione e impiego di appropriate politiche di screening, valutazione e test per la selezione e l'accettazione di soluzioni software e di sistema;
- definizione e aggiornamento di un piano di capacità del servizio.

4.3.11 Gestione della Business Continuity

È uno dei termini fondamentali e PA Digitale lo recepisce appieno e fa proprio nell'ambito del sistema SGSI, dato che l'azienda deve mantenere pienamente efficienti ed efficaci tutti i servizi a disposizione dei propri Clienti nell'ambito di applicabilità del SGSI medesimo. La Business Continuity è quindi interpretata non solo come strumento per la massimizzazione dei propri risultati economici, ma ancor più come elemento alla base dei servizi erogati ai clienti e pertanto vitale per il funzionamento dell'azienda stessa, oltre che come elemento per ridurre al minimo i possibili rischi di contenzioso legale con i propri clienti. Gli obiettivi

sono di contrastare le interruzioni delle attività di servizio e dei processi di servizio critici, dagli effetti di malfunzionamenti, interruzioni, guasti o disastri.

Per una corretta applicazione della Business Continuity, PA Digitale definisce al proprio interno dei processi per la gestione della medesima (dettati dalle norme UNI EN ISO 22301:2019 e UNI EN ISO 22313:2020), dei piani strategici per l'approccio dei rischi e l'analisi degli impatti, lo sviluppo e il mantenimento di specifici piani di continuità operativa. Infine, definisce le modalità di verifica, correzione e ridefinizione dei piani di business continuity.

4.3.12 Conformità legislativa

Come già esplicitato nei punti precedenti, le linee guida sono:

- garantire il rispetto delle leggi civili, penali, obblighi statutari, regolamentari;
- garantire il rispetto dei termini contrattuali stabiliti con i propri clienti;
- garantire il rispetto di specifiche norme adottate obbligatoriamente o volontariamente da PA Digitale.

La legislazione europea e italiana è stringente soprattutto per tutto ciò che riguarda la gestione della privacy che, nell'ambito in cui opera PA Digitale è intesa sia come gestione della privacy per tutti i dati che riguardano i propri dipendenti, clienti e fornitori, sia per tutti i dati trattati e archiviati in nome e per conto dei propri clienti. Per questo motivo PA Digitale ha predisposto una opportuna Politica in materia di trattamento e protezione dei dati personali, pubblicata sul sito www.padigitale.it.

Rispetto della legge e dei principi di legalità, correttezza e trasparenza
L'azienda intende rispondere all'esigenza di assicurare condizioni di trasparenza nella conduzione della propria attività, alle legittime aspettative dei soci, di tutte le parti interessate e del lavoro dei propri dipendenti, alle necessarie tutele della propria posizione e immagine, mediante l'adozione del Modello di Organizzazione, Gestione e Controllo previsto dal Decreto Legislativo 8 giugno 2001, n 231 e del relativo Codice Etico (conformi alle linee guida di Confindustria) quale espressione dei valori e dei principi che ispirano e guidano l'attività aziendale. Tali strumenti, pubblicati sul sito www.padigitale.it, devono rappresentare validi veicoli di sensibilizzazione di tutti coloro che agiscono in nome o comunque nell'interesse ***dell'Azienda***, affinché, conformando costantemente il loro operare alle prescrizioni ivi previste, ispirino e orientino i loro comportamenti al rispetto della legge e dei principi di legalità, correttezza e trasparenza.

4.4 Responsabilità

- TUTTO IL PERSONALE che, a qualsiasi titolo, collabora con l'azienda, è responsabile dell'osservanza di questa policy e della segnalazione di anomalie di cui dovesse venire a conoscenza, anche non formalmente codificate, al Responsabile del Sistema di Gestione della Sicurezza delle Informazioni.
- DIREZIONE/AMMINISTRATORE DELEGATO. Ha il compito di fissare gli obiettivi, assicurare un indirizzamento chiaro e condiviso con le strategie aziendali e un supporto visibile alle iniziative di sicurezza. Promuove la sicurezza garantendo la

congruità dei singoli budget destinati alla sicurezza coerentemente alle politiche e alle linee strategiche aziendali definite.

- RESPONSABILE DEL SISTEMA DI GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI. Si occupa della progettazione del Sistema di Gestione della Sicurezza delle Informazioni e in particolare di:
  - Assicurare che il sistema sia conforme ai requisiti della norma UNI CEI EN ISO/IEC 27001:2017 esteso alle Linee Guida ISO/IEC 27017:2015 e ISO/IEC 27018:2019;
  - Riferire alla Direzione/Amministratore Delegato sulle prestazioni del Sistema di Gestione per la Sicurezza delle Informazioni.
- TUTTI I SOGGETTI ESTERNI che potrebbero avere accesso alle informazioni riservate devono garantire il rispetto dei requisiti di sicurezza attraverso la sottoscrizione di un "accordo di riservatezza" all'atto del conferimento dell'incarico, allorquando questo tipo di vincolo non sia espressamente citato nel contratto.

4.5 Applicabilità

La presente Politica si applica indistintamente a tutti gli organi dell'Azienda coinvolti:

- nei processi di analisi, progettazione, sviluppo, produzione, installazione, commercializzazione, distribuzione, manutenzione e assistenza di prodotti software per la Pubblica Amministrazione Locale e Centrale (della linea Urbi), comprensiva di erogazione dei servizi professionali;
- nei processi di analisi, progettazione, sviluppo, produzione, installazione, commercializzazione, distribuzione, manutenzione e assistenza di prodotti software per il mercato privato (della linea WebTec), comprensiva di erogazione dei servizi professionali;
- nell'erogazione del Servizio di Conservazione Digitale a Norma e del relativo servizio di assistenza.

L'attuazione della presente Politica è obbligatoria per tutto il personale di PA Digitale.

PA Digitale consente la comunicazione e la diffusione delle informazioni verso l'esterno solo per il corretto svolgimento delle attività aziendali, che devono avvenire nel rispetto delle regole e delle norme cogenti.

4.6 Riesame

PA Digitale verificherà periodicamente l'efficacia e l'efficienza del Sistema di Gestione per la Sicurezza delle Informazioni, garantendo l'adeguato supporto per l'adozione delle necessarie migliorie al fine di consentire l'attivazione di un processo continuo, che deve tenere sotto controllo il variare delle condizioni al contorno o degli obiettivi di business aziendali al fine di garantire il suo corretto adeguamento.
La Politica Aziendale della Sicurezza qui descritta è soggetta a riesame in occasione del Riesame della Direzione e/o a seguito di cambiamenti significativi nel campo di applicabilità del Sistema di Gestione della Sicurezza delle Informazioni in essere. In tale ambito viene verificata la conformità dei processi di elaborazione delle informazioni rispetto alle politiche di sicurezza riportate nel presente documento, alle norme e ad altri requisiti di sicurezza appropriati all'ambito del SGSI.