



SECURITY ARCHITECT SRL

C.F. e P.IVA: 06385990723

SEDE LEGALE ED OPERATIVA: Via Salvatore Matarrese, 36 70124 - BARI

DOCUMENTO	POLITICA E OBIETTIVI PER LA GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI
RIFERIMENTI	SGSI ISO 27001; Regolamento Europeo 679/2016
REVISIONE	Rev. 1 del 22.12.2023

CONTROLLO DEL DOCUMENTO

TABELLA DI CONTROLLO DELLE REVISIONI		
REV.	DATA	CAUSALE
00	23.12.2022	Prima emissione
01	22.12.2023	Riesame delle politiche per la sicurezza delle informazioni

TABELLA DI CONTROLLO DELL'EMISSIONE	
REDAZIONE	Responsabile Sistema di Gestione per la Sicurezza delle Informazioni
VERIFICA	RIT
VERIFICA APPROVAZIONE	Direttore Generale - RTD

TABELLA DI CONTROLLO DELLA DISTRIBUZIONE DELLE COPIE CONTROLLATE	
NR	SOGGETTI DESTINATARI
1	Direttore Generale - RTD
2	Responsabile Sistema di Gestione Sistema Integrato
3	Responsabile Sistema di Gestione per la Sicurezza delle Informazioni - RIT
4	Responsabili trattamento delle informazioni ai sensi del Regolamento Europeo 679/2016
5	Ente di Certificazione
6	Dipendenti Area Tecnica

TABELLA DI CONTROLLO DELL'AGGIORNAMENTO
<p>L'ultima versione di questo documento può essere scaricata dai destinatari autorizzati dalla intranet aziendale o può essere ottenuto mediante richiesta indirizzata tramite email al Responsabile del Sistema di Gestione per la Sicurezza delle Informazioni.</p> <p>L'aggiornamento della copia cartacea è a cura del destinatario, essendo la versione elettronica il documento oggetto di controllo della revisione.</p>

SOMMARIO

0.INTRODUZIONE.....	0
1.SCOPO E CAMPO DI APPLICAZIONE	0
1.1 SCOPO	0
1.2 CAMPO DI APPLICAZIONE.....	0
2.NORMATIVA DI RIFERIMENTO	1
3.TERMINI E DEFINIZIONI	1
4.CONTESTO DI RIFERIMENTO PER LA DEFINIZIONE DI POLITICA E OBIETTIVI	4
5.PROGRAMMAZIONE E CONTROLLO DEGLI OBIETTIVI	5
5.1 OBIETTIVI STRATEGICI E OBIETTIVI PER LA GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI.....	5
5.1.1 OBIETTIVI ECONOMICO FINANZIARI E OBIETTIVI PER LA GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI.....	5
5.1.2 OBIETTIVI COMPETITIVI E OBIETTIVI PER LA GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI.....	5
5.1.3 OBIETTIVI RELAZIONALI E OBIETTIVI PER LA GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI.....	6
5.2 OBIETTIVI DEL SISTEMA DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI.....	6
5.2.1 OBIETTIVI PER LA GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI.....	6
5.2.2 OBIETTIVI DI CONTROLLO OPERATIVO PER LA SICUREZZA DELLE INFORMAZIONI.....	7
5.3 OBIETTIVI PER LA SICUREZZA DELLE INFORMAZIONI E OBIETTIVI A LIVELLO DI PROCESSI E DI RISORSE	7
5.3.1 OBIETTIVI DI PROCESSO.....	7
5.3.2 OBIETTIVI DI RISORSE.....	8
5.4 OBIETTIVI DEL SISTEMA DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI E OBIETTIVI DI ALTRI SISTEMI GESTIONALI	8
5.4.1 OBIETTIVI PER LA GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI E OBIETTIVI PER LA PROTEZIONE DEI DATI PERSONALI AI SENSI DEL D.LGS. 196/03 "PRIVACY"	8
5.4.2 OBIETTIVI PER LA GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI E OBIETTIVI PER LA GESTIONE DELLA QUALITA' ISO 9001. 8	
5.5 PROGRAMMAZIONE E CONTROLLO DEGLI OBIETTIVI	9
6.REQUISITI PER LA SICUREZZA DELLE INFORMAZIONI E DETERMINAZIONE DI POLITICA E OBIETTIVI	9
6.1 REQUISITI E OBIETTIVI DI GOVERNANCE.....	9



6.2	REQUISITI E OBIETTIVI DI COMPLIANCE	9
6.3	REQUISITI E OBIETTIVI DI RISK MANAGEMENT	9
7.	POLITICA E OBIETTIVI PER IL MIGLIORAMENTO CONTINUO	10
7.1	MIGLIORAMENTO DELLE PRESTAZIONI DEL SISTEMA DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI	10
7.2	MIGLIORAMENTO DEL SISTEMA DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI	10
7.2.1	<i>MIGLIORAMENTO DELLA PIANIFICAZIONE DEL SGSI</i>	<i>10</i>
7.2.2	<i>MIGLIORAMENTO DELL'ATTUAZIONE DEL SGSI</i>	<i>10</i>
7.2.3	<i>MIGLIORAMENTO DEL CONTROLLO DEL SGSI</i>	<i>11</i>
8.	COMUNICAZIONE E SENSIBILIZZAZIONE DI POLITICA E OBIETTIVI	11
8.1	COMUNICAZIONE	11
8.2	SENSIBILIZZAZIONE	11
9.	POLITICA DI CONTROLLO OPERATIVO PER LA SICUREZZA DELLE INFORMAZIONI	11
10.	DICHIARAZIONE D'IMPEGNO	12

0.INTRODUZIONE

SECURITY ARCHITECT SRL (di seguito: "Azienda") ha come **missione strategica l'erogazione di servizi SOC (Security Operation Center), servizi NOC (Network Operation Center), servizi Cloud, servizi e soluzioni di Cyber Security, servizio di gestione e manutenzione dei sistemi tecnologici ICT Hardware e Software, Consulenza informatica, formazione specialistica informatica.**

In funzione della propria missione strategica, l'Azienda ha pianificato il proprio assetto organizzando una struttura che include l'adozione di specifici sistemi di gestione. In considerazione della missione strategica sopra delineata, assume particolare rilevanza l'adozione di un sistema di gestione per la sicurezza delle informazioni in conformità allo standard ISO 27001. Con l'utilizzo di un moderno sistema di gestione per la sicurezza delle informazioni l'Azienda intende infatti perseguire i seguenti obiettivi:

- assicurare, anche con riferimento al sistema di gestione per la qualità adottato, la conformità ai requisiti di sicurezza applicabili ai servizi erogati ai propri clienti;
- assicurare, anche con riferimento ai requisiti in materia di protezione dei dati personali, la conformità alle disposizioni del Regolamento Europeo 679/2016 "privacy".

Nell'ambito del sistema di gestione per la sicurezza delle informazioni adottato dall'Azienda assume particolare rilevanza la definizione, la formalizzazione e l'approvazione da parte della Direzione della politica e degli obiettivi per la sicurezza delle informazioni.

1.SCOPO E CAMPO DI APPLICAZIONE

1.1 SCOPO

Il presente piano descrive la politica per la gestione della sicurezza delle informazioni adottata dall'Azienda ed i relativi obiettivi. Per quanto concerne in particolare questi ultimi, il presente documento costituisce altresì il quadro di riferimento per assicurare che gli obiettivi per la sicurezza delle informazioni:

- a) siano congruenti con gli indirizzi espressi dalla presente politica e da correlate politiche di taglio maggiormente operativo;
- b) siano resi misurabili, dove possibile e/o pertinente;
- c) prendano in considerazione i requisiti per la sicurezza delle informazioni e i risultati della valutazione e del trattamento dei rischi;
- d) siano comunicati;
- e) siano aggiornati in modo appropriato.

1.2 CAMPO DI APPLICAZIONE

Il presente piano si applica ed è quindi richiamato dai seguenti sistemi di gestione adottati dall'Azienda:

- Sistema di Gestione per la Sicurezza delle Informazioni ISO 27001 e del Regolamento Europeo 679/2016 "privacy";
- Sistema di Gestione dei Rischi in conformità allo standard ISO 31000;

2. NORMATIVA DI RIFERIMENTO

Il presente documento fa riferimento alle seguenti norme:

- standard UNI EN ISO IEC 27001:2014 “Tecnologia per l'Informazione – Tecniche per la Sicurezza – Sistemi di Gestione per la Sicurezza delle Informazioni – Requisiti”;
- Standard ISO IEC 27004:2016 “Information technology — Security techniques — Information security management — Monitoring, Measurement, analysis and evaluation”;
- Standard UNI ISO 31000:2010 “Gestione del rischio – principi e linee guida”;
- Standard ISO IEC 27005:2011 “Information technology – Security techniques - Information security risk Management”;
- Standard UNI CEI ISO / IEC 20000-1:2012 “Tecnologie dell'informazione – Gestione dei servizi – Parte 1: Specifiche - Requisiti per un sistema di gestione del servizio”;
- Standard ISO 22301:2012 “Societal security — Business continuity management systems — Requirements”;
- Regolamento Europeo 679/2016 “privacy

3. TERMINI E DEFINIZIONI

Si riporta la definizione degli acronimi utilizzati nel presente documento:

- SGSI: Sistema di Gestione per la Sicurezza delle Informazioni (secondo lo standard ISO 27001);
- IT: Information Technology.

Si riporta la definizione dei termini utilizzati nel presente documento relativi alla sicurezza delle informazioni:

- processo: insieme di attività correlate o interagenti che trasformano elementi in ingresso in elementi in uscita (ISO 9000).
Nota 1: gli elementi in ingresso in un processo provengono generalmente dagli elementi in uscita da altri processi.
Nota 2: i processi in un'organizzazione sono generalmente pianificati ed eseguiti in condizioni controllate al fine di aggiungere valore.
Nota 3: è spesso chiamato "processo speciale" un processo in cui la conformità del prodotto risultante non può essere verificata prontamente o economicamente;
- informazione: dati significativi (ISO 9000);
- sistema di gestione per la sicurezza delle informazioni: quella parte di sistema di gestione globale, basata su un approccio al rischio aziendale, per istituire, attuare, operare, monitorare, riesaminare, mantenere e migliorare la sicurezza delle informazioni (ISO 27000).
Nota: il sistema di gestione comprende la struttura, le politiche, le attività di pianificazione, le responsabilità, le prassi, le procedure, i processi e le risorse dell'organizzazione;
- efficacia: grado di realizzazione delle attività pianificate e di conseguimento dei risultati pianificati (ISO 9000);
- efficienza: rapporto tra i risultati ottenuti e le risorse utilizzate per ottenerli (ISO 9000);

- sicurezza delle informazioni: preservazione di riservatezza, integrità e disponibilità delle informazioni. In aggiunta possono essere coinvolte anche altre proprietà quali autenticità, responsabilità, non ripudiabilità e affidabilità (ISO 27000);
- disponibilità: la proprietà di essere accessibile e utilizzabile su richiesta di un'entità autorizzata (ISO 27000);
- riservatezza: la proprietà per la quale le informazioni non sono rese disponibili o divulgate a individui, entità, o processi non autorizzati (ISO 27000);
- integrità: la proprietà di salvaguardare l'accuratezza e la completezza dei beni (ISO 27000);
- autenticità: la proprietà che un'entità è ciò che afferma di essere (ISO 27000);
- responsabilità: la responsabilità di un'entità per le sue azioni e decisioni (ISO 27000);
- non ripudiabilità: capacità di dimostrare il verificarsi di un evento o di una azione e la sua entità originaria, al fine di risolvere le controversie circa il verificarsi o non verificarsi dell'evento o dell'azione e il coinvolgimento delle entità dell'evento (ISO 27000);
- affidabilità: proprietà di comportamento previsto coerente ai risultati (ISO 27000).

Si riporta la definizione dei termini utilizzati nel presente documento relativi alla gestione del rischio:

- bene: tutto ciò che ha valore per l'organizzazione (ISO 27000).
Nota: ci sono molti tipi di beni, tra cui:
 - a) informazioni;
 - b) software, come un programma informatico;
 - c) fisici, quali un PC;
 - d) servizi;
 - e) persone, le loro qualifiche, le competenze e l'esperienza;
 - f) beni immateriali, come la reputazione e l'immagine;
- beni sotto forma di informazioni: conoscenze o dati che hanno valore per l'organizzazione (ISO 27000);
- gestione del rischio: attività coordinate per dirigere e controllare un'organizzazione per quanto riguarda il rischio (ISO 27000);
- rischio: combinazione della probabilità di un evento e delle sue conseguenze (ISO 27000);
- rischio sulla sicurezza delle informazioni: potenzialità che una minaccia possa sfruttare una vulnerabilità di un bene o di un gruppo di beni e quindi possa danneggiare l'organizzazione (ISO 27000);
- evento: verificarsi di un particolare insieme di circostanze (ISO 27000);
- vulnerabilità: debolezza di un bene o di un controllo che può essere sfruttata da una minaccia (ISO 27000);
- minaccia: potenziale causa di un incidente indesiderato, che può provocare danni al sistema o all'organizzazione (ISO 27000);
- incidente inerente alla sicurezza delle informazioni: singolo evento inerente alla sicurezza delle informazioni, o una serie di tali eventi, che ha una probabilità significativa di compromettere le operazioni aziendali e di minacciare la sicurezza delle informazioni (ISO 27000);

- trattamento del rischio: processo per modificare il rischio (ISO 31000);
- dichiarazione di applicabilità: dichiarazione documentata che descrive gli obiettivi del controllo e i controlli che sono pertinenti e applicabili al SGSI dell'organizzazione.
Nota: gli obiettivi del controllo e i controlli si basano sui risultati e sulle conclusioni dei processi di valutazione del rischio e di trattamento del rischio, nonché su requisiti legali o cogenti, su obblighi contrattuali e sui requisiti aziendali dell'organizzazione per la sicurezza delle informazioni;
- obiettivo di controllo: dichiarazione descrittiva ciò che deve essere raggiunto a seguito di controlli da implementare (ISO 27000);
- controllo: mezzi di gestione del rischio comprese le politiche, le procedure, le linee guida, le prassi o le strutture organizzative, che possono essere amministrative, tecniche, di gestione o di natura legale (ISO 27000).
Nota: controllo è usato anche come sinonimo di salvaguardia o di contromisura;
- rischio residuo: rischio che rimane dopo il trattamento del rischio (ISO 31000).

Si riporta la definizione dei termini utilizzati nel presente documento relativi alla documentazione:

- documento: informazioni con il loro mezzo di supporto (ISO 9000);
- politica: indirizzi gestionali formalmente espressi dalla Direzione (ISO 27000);
- procedura: modo specificato per svolgere un processo o un'attività (ISO 27000);
- istruzioni operative: descrizioni dettagliate su come eseguire dei compiti e tenere le relative registrazioni (UNI 10999).
Nota 1: le istruzioni operative possono essere documentate o no.
Nota 2: le istruzioni operative possono essere, per esempio, dettagliate in descrizioni scritte, diagrammi di flusso, schemi, modelli, note tecniche inserite nei disegni, specifiche, manuali di istruzioni per apparecchiature, figure, video, liste di controllo o una loro combinazione. Le istruzioni operative dovrebbero descrivere ogni materiale, apparecchiatura e documentazione da utilizzare. Quando applicabile, le istruzioni operative includono i criteri di accettazione;
- registrazione: documento che riporta i risultati ottenuti o fornisce evidenza delle attività svolte (ISO 9000).
Nota 1: le registrazioni possono essere utilizzate, per esempio, per documentare la rintracciabilità e per fornire evidenza delle verifiche, delle azioni preventive e delle azioni correttive.
Nota 2: le registrazioni, generalmente, non richiedono un controllo di revisione.

Si riporta la definizione dei termini utilizzati nel presente documento relativi agli indicatori e alle misurazioni:

- indicatore: misura che fornisce una stima o una valutazione di attributi specifici derivati da un modello analitico con rispetto delle esigenze di informazione definite (ISO 27004);
- misura: variabile alla quale viene assegnato un valore come risultato di misurazione (ISO 27004);
- misurazione: processo di ottenimento di informazioni circa l'efficacia del SGSI e controlli utilizzando un metodo di misurazione, una funzione di misura, un modello analitico e criteri decisionali (ISO 27004).

4.CONTESTO DI RIFERIMENTO PER LA DEFINIZIONE DI POLITICA E OBIETTIVI

La politica e gli obiettivi per la sicurezza delle informazioni sono definiti in funzione del contesto di riferimento aziendale così come descritto nel *Manuale di Gestione del Rischio*, documento a cui si rimanda. Questo al fine di assicurare in modo particolare che la politica e gli obiettivi per la gestione della sicurezza delle informazioni siano allineati e congruenti con la missione strategica aziendale e con il relativo modello di business.

La politica della sicurezza delle informazioni di SECURITY ARCHITECT SRL rappresenta l'impegno dell'organizzazione nei confronti di clienti e terze parti a garantire la sicurezza delle informazioni, degli strumenti fisici, logici e organizzativi atti al trattamento delle informazioni in tutte le attività.

La politica della sicurezza delle informazioni di SECURITY ARCHITECT SRL garantisce:

- La piena conoscenza delle informazioni gestite e la valutazione della loro criticità, al fine di agevolare l'implementazione degli adeguati livelli di protezione.
- L'accesso sicuro alle informazioni, in modo da prevenire trattamenti non autorizzati o realizzati senza i diritti necessari.
- Che la documentazione dei clienti viene salvata in formato elettronico in un sistema che ne garantisce la conservazione e l'integrità.
- Che l'organizzazione e le terze parti collaborino al trattamento delle informazioni adottando procedure volte al rispetto di adeguati livelli di sicurezza.
- Che l'accesso alla sede ed ai singoli locali aziendali avvenga esclusivamente da personale autorizzato, a garanzia della sicurezza delle aree e degli asset presenti.
- Che i collaboratori esterni e gli ospiti siano accreditati e accompagnati all'interno dell'azienda dal nostro personale.
- Che a nessuno è consentito l'accesso durante gli orari di chiusura se non alla Direzione.
- Che le anomalie e gli incidenti aventi ripercussioni sul sistema informativo e sui livelli di sicurezza aziendale siano tempestivamente riconosciuti e correttamente gestiti attraverso efficienti sistemi di prevenzione, comunicazione e reazione al fine di minimizzare l'impatto sul business.
- La rilevazione di eventi anomali, incidenti e vulnerabilità dei sistemi informativi al fine di rispettare la sicurezza e la disponibilità dei servizi e delle informazioni. A tale scopo vengono eseguiti penetration test periodici, controlli sul firewall, controlli per verificare il funzionamento del software e di tutte le nuove funzionalità implementate.
- Che adotta un efficace sistema di Business Continuity e Disaster Recovery comprensivo di sistemi di ticketing e back-up periodici.
- La conformità con i requisiti di legge ed il rispetto degli impegni di sicurezza stabiliti nei contratti con le terze parti.
- L'utilizzo di crittografia e policy di accessi con privilegi.

- Che i trattamenti dei dati personali, sia nei casi in cui Security Architect srl operi in qualità di Titolare che nei casi in cui operi per conto terzi in qualità di Responsabile del Trattamento, avvenga nel rispetto del Regolamento Europeo sulla Protezione dei Dati Personali GDPR 679/2016.

La politica della sicurezza delle informazioni viene costantemente aggiornata per assicurare il suo continuo miglioramento ed è condivisa con l'organizzazione, le terze parti ed i clienti, attraverso un sistema telematico e specifici canali di comunicazione.

5.PROGRAMMAZIONE E CONTROLLO DEGLI OBIETTIVI

5.1 OBIETTIVI STRATEGICI E OBIETTIVI PER LA GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI

Gli obiettivi strategici aziendali correlati al modello di business adottato si declinano in obiettivi di ordine economico finanziario, competitivo e relazionale (soddisfazione delle attese dei portatori di interesse quali proprietà, finanziatori, etc.).

Il perseguimento sistematico e puntuale degli obiettivi strategici richiede in tutto o in parte il perseguimento di specifici obiettivi gestionali, tra cui assumono particolare rilevanza gli obiettivi per la gestione della sicurezza delle informazioni.

5.1.1 OBIETTIVI ECONOMICO FINANZIARI E OBIETTIVI PER LA GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI

Il perseguimento di obiettivi per la sicurezza delle informazioni consente di evitare impatti negativi sul business (business impact analysis) in termini di perdite economiche e finanziarie. Tali perdite possono derivare dalle seguenti fonti:

- costi operativi interni per il recupero delle informazioni;
- costi dei premi assicurativi a fronte di incidenti;
- costi derivanti da mancato rispetto dei requisiti contrattuali stabiliti con i clienti;
- esborsi finanziari da risarcimento danno a terzi per trattamenti illeciti o errati dei dati di loro pertinenza o di utilizzo di diritti di proprietà intellettuale.

5.1.2 OBIETTIVI COMPETITIVI E OBIETTIVI PER LA GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI

Il perseguimento di obiettivi per la sicurezza delle informazioni consente di evitare impatti negativi sul business (business impact analysis) in termini di perdita di competitività. Tali perdite possono derivare dalle seguenti fonti:

- perdita di vantaggio competitivo dovuto alla perdita di *know how* tecnico e commerciale;
- perdita di reputazione e di immagine di mercato;
- perdita di affidabilità nei confronti dei clienti per il mancato rispetto di requisiti applicabili ai servizi erogati, anche in termini di standard level agreement;
- perdita di soddisfazione dei clienti relativamente ai servizi erogati (customer satisfaction);
- perdita di capacità di gestire la filiera di fornitura ("supply chain") e di competitività nei rapporti con i fornitori critici.

5.1.3 OBIETTIVI RELAZIONALI E OBIETTIVI PER LA GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI

Il perseguimento di obiettivi per la sicurezza delle informazioni consente di evitare impatti negativi sul business (business impact analysis) in termini di capacità di soddisfare le attese dei portatori di interesse. Tali perdite possono derivare dalle seguenti fonti:

- per la proprietà: perdita di valore dell'Azienda relativamente alla capacità di generare flussi di reddito e di mantenimento dei beni patrimoniali;
- per la Direzione (organi amministrativi e di controllo): conseguenze legali civili e penali relative al mancato rispetto di requisiti cogenti in materia di sicurezza delle informazioni, inclusa la perdita e l'alterazione di informazioni contabili ed amministrative;
- per soggetti finanziatori: perdita di affidabilità dell'Azienda relativamente alla capacità di assicurare adeguati livelli di protezione dei beni patrimoniali, informazioni incluse;
- per soggetti assicuratori: perdita di affidabilità dell'Azienda relativamente alla capacità di controllare e prevenire i rischi correlati al verificarsi di incidenti in materia di sicurezza delle informazioni.

5.2 OBIETTIVI DEL SISTEMA DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI

5.2.1 OBIETTIVI PER LA GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI

Mediante l'adozione di un sistema di gestione per la sicurezza delle informazioni, l'Azienda persegue i seguenti fondamentali obiettivi:

1. **Riservatezza:** per assicurare che l'informazione sia accessibile solamente ai soggetti e/o ai processi debitamente autorizzati e che le informazioni non siano rese disponibili o divulgate a persone o entità non autorizzate;
2. **Integrità:** per salvaguardare la consistenza dell'informazione da modifiche non autorizzate e garantire che l'informazione non subisca modifiche o cancellazioni a seguito di errori o di azioni volontarie, ma anche a seguito di malfunzionamenti o danni dei sistemi tecnologici;
3. **Disponibilità:** per assicurare che gli utenti autorizzati abbiano accesso alle informazioni e agli elementi architettonici associati quando ne fanno richiesta e salvaguardia quindi il patrimonio informativo nella garanzia di accesso, usabilità e confidenzialità dei dati, riducendo i rischi connessi all'accesso alle informazioni (intrusioni, furto di dati, ecc.);
4. **Controllo:** per assicurare che la gestione dei dati avvenga sempre attraverso processi e strumenti sicuri e testati;

5. **Autenticità:** per garantire una provenienza affidabile dell'informazione;
6. **Privacy:** per garantire la protezione ed il controllo dei dati personali.

Questo per tutte le informazioni che rientrano nel perimetro di sicurezza definito dall'Azienda.

In aggiunta a tali obiettivi fondamentali, l'Azienda può altresì individuare a fronte di casi specifici i seguenti obiettivi complementari:

- obiettivo di responsabilità;
- obiettivo di non misconoscimento;
- obiettivo di affidabilità.

Le definizioni dei termini sopra utilizzati sono riportate nel capitolo 3 del presente documento.

Gli obiettivi per la gestione della sicurezza delle informazioni possono a loro volta essere correlati al perseguimento di obiettivi propri di altri sistemi di gestione adottati dall'Azienda come di seguito descritto.

5.2.2 OBIETTIVI DI CONTROLLO OPERATIVO PER LA SICUREZZA DELLE INFORMAZIONI

Il perseguimento degli obiettivi per la gestione della sicurezza delle informazioni richiede l'adozione di una serie di controlli operativi associati al trattamento di specifici rischi. Tali obiettivi di controllo operativo costituiscono obiettivi di secondo livello rispetto agli obiettivi di gestione per la sicurezza. In particolare, gli obiettivi di controllo operativo perseguiti dall'Azienda sono tratti da quelli riportati nell'Appendice A dello standard ISO 27001. Tra questi, in funzione della valutazione del rischio svolta, l'Azienda individua gli obiettivi di controllo applicabili al proprio contesto di riferimento. Gli obiettivi di controllo operativo valutati come "applicabili" sono elencati nel documento "Dichiarazione di Applicabilità", documento a cui si rimanda.

5.3 OBIETTIVI PER LA SICUREZZA DELLE INFORMAZIONI E OBIETTIVI A LIVELLO DI PROCESSI E DI RISORSE

Gli obiettivi per la sicurezza delle informazioni possono essere correlati a specifici obiettivi definiti a livello di singolo processo o di sviluppo e/o utilizzo di singola risorsa. Tali obiettivi sono finalizzati ad assicurare che i processi e le risorse del sistema di gestione per la sicurezza delle informazioni rispettino criteri aziendali di efficienza, efficacia ed economicità.

5.3.1 OBIETTIVI DI PROCESSO

Obiettivi di processo possono essere definiti con riferimento allo svolgimento dei singoli processi in cui si articola il sistema di gestione per la sicurezza delle informazioni. In genere tali obiettivi sono direttamente riferibili a obiettivi di controllo operativo come definiti con puntualità nell'appendice A della norma ISO 27001.

5.3.2 OBIETTIVI DI RISORSE

Obiettivi di risorse attengono alla messa a disposizione oppure al corretto utilizzo di risorse umane, infrastrutturali ed economiche assegnate al sistema di gestione per la sicurezza delle informazioni ovvero ai processi in cui questo si articola.

5.4 OBIETTIVI DEL SISTEMA DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI E OBIETTIVI DI ALTRI SISTEMI GESTIONALI

5.4.1 OBIETTIVI PER LA GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI E OBIETTIVI PER LA PROTEZIONE DEI DATI PERSONALI AI SENSI DEL D.LGS. 196/03 “PRIVACY”

La gestione della sicurezza dei dati personali ai sensi del Regolamento Europeo 679/2016 “privacy” costituisce un sottoinsieme del più generale sistema di gestione per la sicurezza delle informazioni adottato dall’Azienda. Mediante l’adozione di un sistema di gestione per la sicurezza delle informazioni, l’Azienda persegue i seguenti obiettivi di “governance”, “compliance” e “risk management”:

1. definizione dei ruoli e delle responsabilità (“governance”) per il trattamento dei dati personali di soggetti terzi;
2. conformità (“compliance”) ai requisiti posti dal Regolamento Europeo 679/2016 “privacy relativamente alla liceità e alle modalità del trattamento dei dati personali di soggetti terzi;
3. valutazione dei rischi (“risk management”) e adozione delle misure minime di sicurezza per il trattamento dei Regolamento Europeo 679/2016 “privacy.

5.4.2 OBIETTIVI PER LA GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI E OBIETTIVI PER LA GESTIONE DELLA QUALITA’ ISO 9001.

La gestione della qualità ha come obiettivi fondamentali, descritti dalla relativa politica a cui si rimanda, il perseguimento della conformità dei servizi erogati dall’Azienda ai relativi clienti al fine di mantenere ed accrescere la loro soddisfazione. Mediante l’adozione di un sistema di gestione per la sicurezza delle informazioni, l’Azienda persegue i seguenti obiettivi di “governance”, “compliance” e “risk management”:

1. definizione dei ruoli e delle responsabilità (“governance”) per il trattamento delle informazioni di proprietà dei clienti.
2. conformità (“compliance”) ai requisiti in materia di sicurezza delle informazioni applicabili ai servizi erogati ai clienti ed ai relativi processi, siano tali requisiti di ordine contrattuale (inclusi service level agreement), cogenti, di buona tecnica e aziendali;
3. valutazione dei rischi (“risk management”) e adozione dei relativi controlli applicabili nell’erogazione dei servizi ai clienti, con particolare riferimento alla continuità operativa del servizio nonché alla capacità dell’infrastruttura IT di supportare il servizio erogato sotto il profilo operativo ed economico nel rispetto della sicurezza delle informazioni trattate.

5.5 PROGRAMMAZIONE E CONTROLLO DEGLI OBIETTIVI

L'Azienda stabilisce una specifica procedura di programmazione e controllo per assicurare che gli obiettivi per la sicurezza delle informazioni siano sistematicamente e regolarmente attuati. Tale procedura si articola come segue:

- a) che cosa sarà fatto;
- b) quali risorse saranno utilizzate;
- c) chi sarà responsabile del perseguimento dell'obiettivo;
- d) quando sarà completato;
- e) come i risultati saranno valutati.

In particolare, ogni obiettivo oggetto di programmazione e controllo è reso misurabile mediante definizione di opportuni indicatori e valori soglia. A tale scopo viene fatto riferimento alle linee guida dello standard ISO 27004.

6. REQUISITI PER LA SICUREZZA DELLE INFORMAZIONI E DETERMINAZIONE DI POLITICA E OBIETTIVI

6.1 REQUISITI E OBIETTIVI DI GOVERNANCE

La politica aziendale stabilisce l'attribuzione ai vari livelli della struttura organizzativa e ad eventuali terze parti esterne coinvolte, degli obiettivi per la gestione della sicurezza delle informazioni e per il controllo operativo. Questo con particolare riferimento ai requisiti derivanti dalle prescrizioni normative applicabili in materia di sicurezza delle informazioni.

6.2 REQUISITI E OBIETTIVI DI COMPLIANCE

La politica aziendale stabilisce il mantenimento sistematico e puntuale della conformità ai requisiti normativi applicabili alla sicurezza delle informazioni, relativamente alle informazioni trattate ed alle relative infrastrutture utilizzate per il trattamento. A tale proposito la politica aziendale persegue i seguenti obiettivi:

- monitoraggio sistematico di tutti i requisiti in materia di sicurezza delle informazioni applicabili al contesto aziendale;
- individuazione, in funzione del contesto di riferimento aziendale, dei requisiti applicabili;
- riesame di politica e obiettivi per la gestione della sicurezza delle informazioni e per il controllo operativo al fine di renderli allineati con i requisiti applicabili.

6.3 REQUISITI E OBIETTIVI DI RISK MANAGEMENT

La politica aziendale stabilisce che la gestione del rischio sia specificatamente approvata dalla Direzione, con particolare riferimento all'accettazione del rischio residuo. A tale proposito la politica aziendale persegue i seguenti obiettivi:

- tutti i rischi associati al mancato rispetto dei requisiti applicabili al contesto aziendale, in materia di sicurezza delle informazioni, siano oggetto di valutazione;
- tutti i rischi stimati come "non accettabili" debbano essere trattati fino a ridurre il rischio residuo entro livelli stimati come "accettabili";

- i rischi stimati come “accettabili” siano egualmente oggetto di trattamento, in ottica migliorativa, previa analisi dei costi e dei benefici associati al trattamento.

7. POLITICA E OBIETTIVI PER IL MIGLIORAMENTO CONTINUO

7.1 MIGLIORAMENTO DELLE PRESTAZIONI DEL SISTEMA DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI

L'Azienda ha stabilito un processo di miglioramento continuo finalizzato a individuare le opportunità di miglioramento in termini di efficacia, efficienza ed economicità delle prestazioni del sistema di gestione adottato per la sicurezza delle informazioni. Le prestazioni del sistema di gestione per la sicurezza delle informazioni sono principalmente correlate al grado di perseguimento degli obiettivi per la gestione della sicurezza delle informazioni, a loro volta correlati agli obiettivi di controllo operativo per la sicurezza delle informazioni, anche in ottica di riduzione del livello di rischio residuo.

7.2 MIGLIORAMENTO DEL SISTEMA DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI

Il miglioramento delle prestazioni del sistema di gestione per la sicurezza delle informazioni può essere correlato al miglioramento dello stesso sistema di gestione per la sicurezza delle informazioni con riferimento a:

1. obiettivi di miglioramento della pianificazione del SGSI;
2. obiettivi di miglioramento dell'attuazione del SGSI;
3. obiettivi di miglioramento del controllo del SGSI.

7.2.1 MIGLIORAMENTO DELLA PIANIFICAZIONE DEL SGSI

Il miglioramento della pianificazione del SGSI si correla ai seguenti obiettivi di adeguamento del sistema documentale (politiche, procedure, istruzioni operative, piani, etc.):

1. requisiti contrattuali in materia di sicurezza delle informazioni;
2. requisiti cogenti in materia di sicurezza delle informazioni;
3. requisiti tecnici in materia di sicurezza delle informazioni, incluso l'adeguamento alle variazioni degli standard ISO di riferimento;
4. requisiti aziendali in materia di sicurezza delle informazioni, incluso l'adeguamento a seguito di rilievi derivanti da audit interni e da riesami della Direzione.

7.2.2 MIGLIORAMENTO DELL'ATTUAZIONE DEL SGSI

Il miglioramento della pianificazione del SGSI si correla ai seguenti obiettivi:

1. obiettivi di formazione delle risorse umane in materia di sicurezza delle informazioni, con particolare riferimento allo sviluppo delle competenze gestionali, tecniche ed operative richieste per la corretta applicazione dei controlli operativi adottati dall'Azienda;

2. obiettivi di sensibilizzazione delle risorse umane e di terze parti in merito ai rischi ed al sicuro svolgimento dei processi e delle attività di loro competenza, nonché al rispetto di politiche, procedure e controlli operativi;
3. obiettivi di messa a disposizione di risorse per il perseguimento degli obiettivi di controllo operativo e più in generale per il mantenimento del SGSI;
4. obiettivi di adeguamento del perimetro di sicurezza delle informazioni nella dimensione organizzativa, fisica e logico-informatica;
5. obiettivi di conformità relativamente alla corretta applicazione di politiche, procedure, istruzioni operative e controlli operativi.

7.2.3 MIGLIORAMENTO DEL CONTROLLO DEL SGSI

Il miglioramento della pianificazione del SGSI si correla ai seguenti obiettivi fondamentali:

1. obiettivi di programmazione di adeguati cicli di audit interni sul SGSI o su specifiche componenti;
2. obiettivi di pianificazione delle attività di monitoraggio del perseguimento degli obiettivi di controllo operativo.

8.COMUNICAZIONE E SENSIBILIZZAZIONE DI POLITICA E OBIETTIVI

8.1 COMUNICAZIONE

La politica e gli obiettivi per la gestione della sicurezza delle informazioni ed i correlati obiettivi di controllo operativi, sono comunicati dalla Direzione ai vari livelli della struttura organizzativa aziendale, nonché a terze parti esterne eventualmente coinvolte.

Variazioni nella politica e negli obiettivi sopra citati sono parimenti oggetto di specifica comunicazione.

8.2 SENSIBILIZZAZIONE

La politica e gli obiettivi per la gestione della sicurezza delle informazioni ed i correlati obiettivi di controllo operativi, sono oggetto di specifici programmi di sensibilizzazione e cyber security awareness finalizzati a mantenere e ad accrescere la consapevolezza da parte dei destinatari in merito al sistematico rispetto e perseguimento degli obiettivi di sicurezza di cui l'Azienda è anche promotrice.

9.POLITICA DI CONTROLLO OPERATIVO PER LA SICUREZZA DELLE INFORMAZIONI

Il presente documento definisce la politica per la gestione della sicurezza delle informazioni. In tale ottica, il presente documento può richiamare uno o più documenti di politica di controllo operativo che riportano gli indirizzi definiti dalla Direzione, relativamente a specifiche tematiche per la sicurezza delle informazioni. Tali politiche di controllo operativo sono in genere associate all'implementazione dei controlli previsti dall'Appendice A dello standard ISO 27001 e richiamate dal Piano di Trattamento dei Rischi, documento a cui si rimanda.

10. DICHIARAZIONE D'IMPEGNO

L'Azienda si impegna a garantire:

- **la riservatezza delle informazioni** attraverso la definizione puntuale delle responsabilità interne, come descritte nell'Organigramma Nominale e nei moduli Mansionari, per la gestione dei servizi e delle informazioni ad essi connesse; il controllo degli accessi fisici e logici agli archivi elettronici e cartacei esclusivamente da parte di personale autorizzato e competente;
- **l'integrità delle informazioni** attraverso il controllo degli accessi fisici e logici esclusivamente da parte di personale autorizzato e competente e la gestione dei back-up dei dati e delle configurazioni dei sistemi informativi esclusivamente dal personale interno;
- **la disponibilità delle informazioni** attraverso l'identificazione dei ruoli e delle funzioni, i diritti di accesso alle informazioni e agli assets aziendali per la gestione dei servizi al Cliente;
- che dipendenti, fornitori, partner, appaltatori e ogni altra terza parte coinvolta con il trattamento di informazioni che rientrano nel campo di applicazione del Sistema di Gestione della Sicurezza delle Informazioni, accettino **gli obblighi e le responsabilità** di propria pertinenza;
- che ogni **accesso**, di tipo fisico o informatico, sia autorizzato, **controllato** e monitorato sulla base dei seguenti criteri:
 - l'accesso è autorizzato al personale abilitato solo per le informazioni necessarie (principio della conoscenza minima o necessità di sapere);
 - l'accesso è autorizzato al personale abilitato solo per le informazioni relative alle attività specifiche (funzione di lavoro-correlati);
 - l'accesso alla struttura e ai locali è autorizzato al personale interno e a fornitori autorizzati. L'accesso ai locali è ridotto al minimo, autorizzato, controllato e monitorato in linea con la politica aziendale;
- che ogni dipendente, fornitore, partner e terza parte sia **consapevole** del proprio ruolo e dell'impatto delle proprie azioni sulla sicurezza delle informazioni;
- che ogni risorsa sia adeguatamente **formata** sulle politiche e sulle procedure relative alla gestione della sicurezza delle informazioni;
- che i trattamenti delle informazioni, delle attività, delle risorse e delle soluzioni inerenti alla protezione delle informazioni o gestiti dalla stessa per conto dei propri clienti sono conformi alle leggi e ai regolamenti applicabili di natura cogente, contrattuale e volontaria;

- che ogni attività e risorsa di proprietà dell'Azienda o affidata da questa a terze parti, nonché ogni informazione pertinente l'ambito del SGSI, è protetta dai problemi legati alla riservatezza, l'integrità e la disponibilità, in proporzione al loro valore e nel rispetto delle leggi vigenti;
- che tutto il **personale** sia **responsabilizzato** all'obbligo di:
 - garantire il rispetto delle norme, leggi e regolamenti vigenti, di natura cogente, contrattuale e volontaria rese applicabili negli ambiti del SGSI;
 - proteggere la riservatezza, l'integrità e la disponibilità delle informazioni gestite da SA, la proprietà intellettuale e il patrimonio dell'Azienda o da questa affidati a terze parti;
 - aver cura dei beni materiali, dei sistemi e delle risorse nel rispetto delle POI;
 - salvaguardare e gestire in modo appropriato ogni informazione e dato afferente alle attività di propria competenza;
 - contattare la Direzione, il RIT, RSGI e/o altre autorità competenti in caso di effettive o sospette violazioni della sicurezza;
 - segnalare qualsiasi necessità di modifiche alle procedure relative alla gestione della sicurezza delle informazioni.
 - Compatibilmente con le autorità assegnate nella gestione della sicurezza ciascuno deve:
 - garantire la conformità con la politica di sicurezza, requisiti, standard e/o procedure definiti;
 - individuare e definire i diritti di accesso agli assets per le loro specifiche attività e responsabilità;
 - richiedere alle terze parti di essere formalmente in linea con gli accordi di riservatezza e/o in possesso di certificazioni relative alla sicurezza delle informazioni;
 - operare in conformità ai livelli di rischio che sono stati definiti per il proprio ambito di pertinenza.
- che tutto il **personale** cui sono assegnate responsabilità specifiche nella gestione della sicurezza delle informazioni **ha altresì il dovere** di:
 - implementare la sicurezza sulla base delle politiche di sicurezza ivi stabilite;
 - garantire e monitorare il rispetto delle politiche di sicurezza delle informazioni, requisiti, norme e procedure definiti nell'ambito del SGSI;

- monitorare gli assets aziendali, al fine di garantire il rispetto del livello di controllo previsto per l'asset da proteggere ed il rispetto delle leggi e regolamenti applicabili;
- rendere effettive l'insieme di regole, funzioni, strumenti, moduli e controlli, resi coerenti e funzionali agli scopi dell'organizzazione e coerenti con gli ambiti del SGSI, che garantiscano che nella struttura, organizzazione, ambiente informatico, singolo elaboratore, sia costantemente osservato il rispetto dei requisiti del SGSI;
- garantire che il personale e i terzi siano formati e informati circa la politica, i requisiti, standard e/o procedure per la gestione della sicurezza delle informazioni, nonché resi consapevoli delle conseguenze in caso di mancato rispetto della politica e requisiti stabiliti in tali ambiti;
- sostenere l'adozione di misure adeguate a garantire il controllo sugli aspetti che hanno impatto sulla sicurezza delle informazioni;
- contenere il livello di rischio negli ambiti di pertinenza;
- mantenere attive le misure da adottarsi in caso di incidenti derivanti dal verificarsi di condizioni anomale e di emergenza, garantire l'adozione dei piani di continuità e di disaster recovery in conformità ai requisiti definiti dal SGSI;
- inoltre, che i **soggetti terzi** che gestiscono in modo diretto o indiretto gli assets sensibili dei Clienti, **sono obbligati**, nello svolgimento di processi/attività, a:
 - formalizzare il proprio impegno alla riservatezza e non divulgazione delle informazioni tratte negli ambiti di competenza;
 - proteggere le risorse e le informazioni fisiche e intellettuali a cui possono accedere nella effettuazione delle attività assegnate;
 - garantire la piena osservanza ai requisiti del SGSI nei comportamenti e nell'operatività e/o essere in possesso di certificazioni aggiornate riguardo la sicurezza delle informazioni.

Fine del documento