

MANUALE DEL SISTEMA DI GESTIONE DELLA SICUREZZA DEI DATI

**Redatto in conformità alla Norma
ISO/IEC 27001:2013**

di proprietà della Ditta

MATER SOC. CONS. A R.L.

P.IVA 7010400633

**Sede Legale e Operativa:
via Brecce a S.Erasmo 112/114
80146 Napoli**

Il presente Documento è di proprietà di *Mater scarl* e non può essere riprodotto o divulgato senza l'autorizzazione scritta della Direzione.

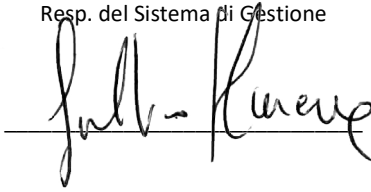
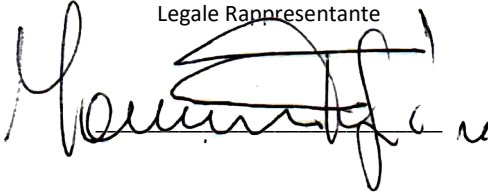
Gestione del documentoIl documento si trova in **Ed. 01 Rev. 00**

Redazione	Consulente Esterno	My Advisor s.r.l.	
Verifica ed Emissione	RSGSD	Fulvio Mancuso	
Approvazione	Legale Rappresentante	Massimo Foglia	

Sottoscrizione del documento

Con l'apposizione della propria firma si attesta di aver preso atto del contenuto del presente documento.

Legale Rappresentante Resp. del Sistema di Gestione

**Elenco delle Edizioni e Revisioni**

Edizione	Revisione	Data	Oggetto della Revisione
01	00	02.02.2018	Prima Stesura

Sommario

1	SCOPO E CAMPO DI APPLICAZIONE DEL SGSD	5
2	I RIFERIMENTI NORMATIVI E LEGISLATIVI DEL SGSD	7
3.	TERMINI E DEFINIZIONI	9
3.1	TERMINI, DEFINIZIONI E SIGLE	9
4	CONTESTO DELL'ORGANIZZAZIONE	12
4.1	L'ORGANIZZAZIONE E IL SUO CONTESTO	12
4.2	COMPRESIONE DELLE ESIGENZE E DELLE ASPETTATIVE DELLE PARTI INTERESSATE	16
4.3	IL CAMPO DI APPLICAZIONE DEL SISTEMA DI GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI	17
4.4	IL SISTEMA DI GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI ED I SUOI PROCESSI	17
4.4.1	DETERMINAZIONE DEI PROCESSI NECESSARI PER IL SISTEMA DI GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI	17
5	LEADERSHIP	20
5.1	LEADERSHIP E IMPEGNO	20
5.2	POLITICA DEL SISTEMA DI GESTIONE	20
5.3	RUOLI, RESPONSABILITÀ E AUTORITÀ NELL'ORGANIZZAZIONE	21
6	PIANIFICAZIONE	23
6.1	PIANO PER AFFRONTARE RISCHI ED OPPORTUNITÀ	23
6.1.1	GENERALITÀ	23
6.1.2	VALUTAZIONE DEL RISCHIO RELATIVO ALLA SICUREZZA DELLE INFORMAZIONI	23
6.1.3	TRATTAMENTO DEL RISCHIO RELATIVO ALLA SICUREZZA DELLE INFORMAZIONI	24
6.2	OBIETTIVI PER LA SICUREZZA DELLE INFORMAZIONI E PIANIFICAZIONE PER IL LORO RAGGIUNGIMENTO	24
7	SUPPORTO	27
7.1	RISORSE	27
7.2	COMPETENZA	27
7.3	CONSAPEVOLEZZA	27
7.4	COMUNICAZIONE	27
7.5	INFORMAZIONI DOCUMENTATE	28
7.5.1	MANUALE DEL SISTEMA DI GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI	29
7.5.2	CREAZIONE E AGGIORNAMENTO	31
7.5.3	CONTROLLO DELLE INFORMAZIONI DOCUMENTATE	31
8	ATTIVITA' OPERATIVE	33
8.1	PIANIFICAZIONE E CONTROLLO OPERATIVI	33
8.2	VALUTAZIONE DEL RISCHIO RELATIVO ALLA SICUREZZA DELLE INFORMAZIONI	33
8.3	TRATTAMENTO DEL RISCHIO RELATIVO ALLA SICUREZZA DELLE INFORMAZIONI	33
9	VALUTAZIONE DELLE PRESTAZIONI	34
9.1	MONITORAGGIO, MISURAZIONE, ANALISI E VALUTAZIONE	34
9.2	AUDIT INTERNI	34
9.3	RIESAME DELLA DIREZIONE	35
10	MIGLIORAMENTO	38
10.1	NON CONFORMITÀ E AZIONI CORRETTIVE	38

10.2 MIGLIORAMENTO CONTINUO	40
-----------------------------------	----

1 SCOPO E CAMPO DI APPLICAZIONE DEL SGSD

La Mater scarl, fondata nel 1996, opera nel settore della progettazione e sviluppo di software.

La Mater scarl si avvale da sempre della collaborazione di professionisti in grado di erogare servizi nel rispetto delle specifiche e delle normative. E' interesse della ns. impresa mantenere un livello qualitativo di fornitura omogeneo e costante per tutta la gamma di servizi offerti.

Siamo inoltre molto attenti alla formazione del personale che collabora con la nostra azienda, attraverso corsi ed aggiornamenti costanti, facendo di tutto ciò un impegno costante atto a garantire un livello qualitativo adeguato alla nostra clientela.

Il Vertice dell'organizzazione aziendale cosciente del livello di importanza assunto dal fattore Sistema di Gestione Sicurezza dei Dati ha riconosciuto la necessità di istituire al proprio interno un Sistema di Gestione Sicurezza dei Dati documentato, nel pieno rispetto di quanto richiesto dalla norma ISO/IEC 27001:2013.

Il presente Manuale Sistema di Gestione Sicurezza dei Dati definisce e documenta gli elementi base e caratteristici del Sistema Sistema di Gestione Sicurezza dei Dati Aziendale adottato; il Vertice di Mater scarl incarica e demanda al Responsabile Sistema di Gestione Sicurezza dei Dati il compito di renderlo organico, rispondente ai requisiti della norma prescelta ed alle proprie necessità e soprattutto applicato.

Il Manuale Sistema di Gestione Sicurezza dei Dati rappresenta, sia per il Personale aziendale sia per i Clienti o per altri che ne facessero richiesta, la guida ed il riferimento dell'applicazione sistematica e della verifica dell'adeguatezza del Sistema Sistema di Gestione Sicurezza dei Dati aziendale; inoltre vuole essere una guida di valutazione per ogni organismo di certificazione.

Il SGSD adottato dalla Mater scarl stabilisce i requisiti di gestione che consentono di formulare la politica aziendale e stabilire obiettivi che permettano di ottenere il miglioramento continuo delle prestazioni aziendali, nonché obiettivi che permettano all'organizzazione di individuare, gestire i rischi aziendali e migliorarne le prestazioni.

Il SGSD stabilisce, documenta, attua, mantiene e migliora in modo continuo il sistema di gestione aziendale, in accordo con i requisiti delle Norme Internazionali ISO/IEC 27001:2013.

Nell'**Allegato 4 – Processi del Sistema di Gestione** sono rappresentati nel dettaglio i processi fondamentali su cui la norma ISO/IEC 27001:2013 si basa con le relative procedure di riferimento.

L'organizzazione, attraverso l'implementazione del sistema di gestione della Sicurezza delle Informazioni:

- a) dimostra la propria capacità di fornire con regolarità prodotti o servizi che soddisfano i requisiti del cliente e i requisiti cogenti applicabili assicurando la sicurezza delle dati;
- b) mira ad accrescere la soddisfazione del cliente tramite l'applicazione efficace del sistema, compresi i processi per migliorare il sistema stesso e assicurare la conformità ai requisiti del cliente e ai requisiti cogenti applicabili.
- c) tiene sotto controllo tutti gli aspetti legati alla Sicurezza dei dati.

Il presente Manuale è stato realizzato nell'ottica di fornire alle parti interessate (interne ed esterne all'Azienda) un'immagine chiara ancorché sintetica dell'approccio di Mater scrl alla gestione della sicurezza dei dati illustrandone gli aspetti salienti e gli elementi necessari a consentire al lettore di comprendere le modalità con le quali l'azienda ha recepito e tradotto in termini operativi i requisiti dello standard ISO/IEC 27001.

Il presente documento è uno dei capisaldi, assieme alla Politica per la Sicurezza delle informazioni, dell'impegno preso nei confronti dei Clienti, della comunità, dei soci e delle autorità amministrative e di controllo.

2 I RIFERIMENTI NORMATIVI E LEGISLATIVI DEL SGSD

Mater scarl ha sviluppato il proprio sistema di gestione della Sicurezza delle Informazioni in accordo con le seguenti norme:

- il modello della norma UNI CEI ISO/IEC 27001:2014 – Tecniche per la sicurezza – Sistemi di gestione per la sicurezza delle informazioni - Requisiti;
- ISO/IEC 27000 — Information security management systems — Overview and vocabulary
- ISO/IEC 27003 — Information security management system implementation guidance
- ISO/IEC 27004 — Information security management — Measurement
- ISO/IEC 27005 — Information security risk management
- ISO 19011:2018, Linee Guida per l’audit dei sistemi di gestione

Per ciò che attiene i riferimenti legislativi si riportano i seguenti:

- Provvedimenti del Garante
- Reg. UE 679/2016 (GDPR)
- D.Lgs. 196/03 e S.m.i.

Di norma la legislazione pertinente viene reperita dietro consultazione degli organi di stampa meglio documentati o di comunicazione aziendale o tramite consulenti. Questo documento è anche il normale riferimento per i testi da consultare ed è disponibile in rete al personale interessato.

Altre fonti

Per completare l’esame iniziale delle normative, è possibile consultare le seguenti fonti:

- data base legislativo;
- informative interne aziendali (notiziario legislativo)
- uffici comunali o Ufficio regionale del Bollettino;
- associazioni o gruppi di industriali;
- bollettini di studi legali;
- associazioni di professionisti;
- rapporti di verifica interna o esterna;
- avvisi di violazione emessi da un’autorità;

La procedura di gestione è la **PR 2.1 – Gestione della documentazione Normativa e Legislativa**.

3. TERMINI E DEFINIZIONI

3.1 Termini, definizioni e sigle

Erogazione del servizio: Insieme di attività svolte che definiscono il servizio erogato dall'organizzazione in termini di efficienza, economicità, rispetto delle normative di sicurezza, comfort per il cliente, salvaguardia ambientale e sicurezza nella gestione dei dati

Vendita del prodotto: Insieme di attività svolte che intercorrono dalla ricezione di un ordinativo di un cliente/committente all'effettiva consegna dei prodotti

Cliente/Committente: Ente, istituto, azienda o privato che affida all'organizzazione il compito di svolgere un servizio oppure effettua un ordinativo di uno specifico prodotto o insieme di prodotti e servizi

Controllo Sistema di Gestione Sicurezza dei Dati servizio: Verifica effettuata in azienda al fine di valutare, secondo i criteri oggettivi predefiniti, che l'organizzazione del servizio sia rispondente alle norme contrattuali e/o agli standard aziendali a monte definiti

Controllo Sistema di Gestione Sicurezza dei Dati prodotto: Insieme delle operazioni di verifica effettuate in azienda al fine di valutare che il prodotto trasformato o venduto sia conforme alle norme contrattuali o comunque agli standard aziendali definiti a monte

Sistema di gestione per la sicurezza dei dati: Sistema per stabilire una politica per la sicurezza dei dati e gli obiettivi per la sicurezza dei dati al fine di conseguire codesti obiettivi

Prodotto: Risultato di uno specifico processo

Processo: Attività che utilizza risorse per trasformare elementi in ingresso in elementi in uscita

Soddisfazione del cliente: Opinione del cliente sul grado in cui una transazione ha soddisfatto le esigenze e le aspettative del cliente stesso

Cliente: Organizzazione o persona che riceve un prodotto o un servizio

Fornitore: Organizzazione o persona che fornisce un prodotto o servizio

Procedura: Modo specificato per svolgere un'attività o un processo

Non conformità: Non ottemperanza ad uno specifico requisito

Conformità: Ottemperanza ad uno specifico requisito

Reclamo: Espressione di una qualsiasi insoddisfazione del cliente

Azione correttiva: Azione adottata per eliminare la causa effettiva di una non conformità rilevata

Azione preventiva: Azione adottata per eliminare la possibile causa di una potenziale non conformità

Audit: Processo sistematico, indipendente e documentato per ottenere evidenza e valutarla con obiettività al fine di stabilire in quale misura si è ottemperato ai criteri della verifica ispettiva

Sistema di Gestione Sicurezza dei Dati: Grado in cui un insieme di caratteristiche intrinseche soddisfa i requisiti

Verifica ispettiva per la sicurezza dei dati: Esame sistematico indipendente mirato a stabilire se le attività svolte per la sicurezza dei dati ed i risultati ottenuti siano in accordo con quanto stabilito e se quanto stabilito viene attuato efficacemente e risulta idoneo al conseguimento degli obiettivi

Miglioramento continuo: Attività ricorrente mirata ad accrescere la capacità di soddisfare i requisiti

Requisito: Esigenza o aspettativa che può essere espressa o usualmente implicita o obbligatoria

Organizzazione: Insieme di persone e di mezzi, con definite responsabilità, autorità ed interrelazioni

Politica della sicurezza dei dati: Obiettivi ed indirizzi generali di una organizzazione, relativi alla sicurezza dei dati, espressi in modo formale dall'Alta Direzione

Rintracciabilità: Capacità di risalire alla storia, all'utilizzazione o all'ubicazione di ciò che si sta considerando

Pianificazione della sicurezza dei dati: Parte della gestione per la sicurezza dei dati mirata a stabilire gli obiettivi ed a specificare i processi operativi e le relative risorse necessarie per conseguire tali obiettivi

Registrazione: Documento che riporta i risultati ottenuti o fornisce evidenza delle attività svolte

Validazione: Conferma a seguito di controllo di quanto si è in possesso (esempio dati), sostenuta da evidenze oggettive verificabili, tangibili, che i requisiti specifici previsti relativi ad un utilizzo o ad un'applicazione, sono soddisfatti

Efficacia: Grado di realizzazione delle attività pianificate e di conseguimento dei risultati pianificati

Efficienza: Rapporto tra i risultato ottenuti e le risorse utilizzate per ottenerle

Infrastruttura: Base organizzativa di tipo materiale (spazi di lavoro, attrezzature, strumentazione) o immateriale (know how, software etc.,) legata alla realizzazione di un determinato servizio

Ambiente di lavoro:Insieme di condizioni in cui opera una persona

Outsourcing: Risorsa esterna

Piano della sicurezza dei dati: Documento che per uno specifico progetto, prodotto, processo o contratto, specifica quali procedure e risorse associate devono essere utilizzate, e da chi e quando

Dichiarazione di applicabilità: dichiarazione in cui l'organizzazione definisce (i) i controlli selezionati come necessari con relativa giustificazione per l'inclusione, (ii) i controlli presenti nell'appendice A eventualmente esclusi con le relative giustificazioni di esclusione, (iii) i controlli selezionati applicati dall'organizzazione.

Piano di trattamento dei rischi della sicurezza delle informazioni: Piano che determina in modo oggettivo i rischi relativi alle informazioni con evidenza di accettazione dei rischi residui che si è deciso di non trattare.

Di seguito sono riportate le sigle identificative degli enti funzionali come da organigramma.

DGE	Direzione Generale per il Sistema
RSGSD	Servizio Sistema di Gestione Sicurezza dei Dati/Responsabile Sistema di Gestione
AMM	Servizio Amministrazione /Resp. Amministrazione
ACQ	Servizio Acquisti
SER	Servizi Erogati
RSPP	Responsabile Servizio di Prevenzione e Protezione

Nel testo sono ricorrenti le seguenti abbreviazioni;

SGSD	Sistema di gestione della Sicurezza delle Informazioni
MSGSD	Manuale del Sistema di gestione della Sicurezza delle Informazioni
PR	Procedura Operativa SGSD
IO	Istruzione Operativa SGSD

4 CONTESTO DELL'ORGANIZZAZIONE

4.1 L'organizzazione e il suo contesto

L'organizzazione ha determinato i fattori esterni e interni rilevanti per le sue finalità e gli indirizzi strategici e che influenzano la sua capacità di conseguire il(i) risultato(i) atteso(i) per il proprio sistema di gestione della Sicurezza delle Informazioni.

I fattori riguardano ambienti legale, tecnologico, competitivo, di mercato, culturale, sociale ed economico.

Lo scopo e la direzione strategica del nostro top management è di conformarsi alle leggi relative alla sicurezza delle informazioni mantenendo la nostra immagine sul mercato, la leadership e aumentando il margine lordo di contribuzione.

Implementando il sistema di gestione della Sicurezza delle Informazioni, abbiamo intenzione di incrementare il nostro fatturato commerciale ottimizzando l'utilizzo delle nostre risorse.

Questo impegno viene tradotto negli obiettivi quantificabili indicati in questo manuale nella forma di informazioni documentate. Abbiamo elencato di seguito gli aspetti interni ed esterni considerati per implementare il sistema di gestione della Sicurezza delle Informazioni.

Aspetti Interni / Esterni

Descrizione aspetto	Tipologia
<ul style="list-style-type: none">• Governance. Chiarezza di intenti. Si punta su servizi strategici che possano garantire un buon margine di contribuzione e una Sistema di Gestione Sicurezza dei Dati del servizio in termini di affidabilità riferita alla capacità di risoluzione delle problematiche. Focus sull'innovazione tecnologica per migliorare le performance dei propri prodotti.	Interni
<ul style="list-style-type: none">• Politica Commerciale. Le proposte di intervento vengono strutturate sulla base delle specifiche del cliente tenendo in conto delle singole attività, delle tempistiche di consegna e delle ore massime stimate per le attività richieste.	Interni
<ul style="list-style-type: none">• Struttura organizzativa, ruoli e responsabilità. L'azienda si è organizzata per funzioni. Per ogni funzione c'è una chiara	Interni

<p>attribuzione di responsabilità in capo ai primi livelli aziendali che vengono scelti sulla scorta delle competenze sia tecniche che manageriali rispetto all'esperienza acquisita sul campo. L'organigramma è chiaramente definito e i lavoratori conoscono esattamente le interdipendenze funzionali.</p>	
<ul style="list-style-type: none"> Fornitori. I fornitori principali dell'azienda sono tipicamente quelli che rogano servizi si staff quali: Medico Competente, Commercialista, Consulente Paghe, Consulente Sicurezza sui Luoghi di Lavoro, Connettività, Data center, Posta elettronica e Repository. 	Interni
<ul style="list-style-type: none"> Outsourcing. I processi affidati all'esterno sono legati allo sviluppo del codice sorgente Project Objects India. 	Interni
<ul style="list-style-type: none"> Ubicazioni Fisiche. L'azienda ha una sede legale ed operativa in Via Brecce a S.Erasmo 112/114 80146 Napoli 	Interni
<ul style="list-style-type: none"> Informazioni Trattate. Le informazioni trattate sono quelle relative ai clienti, ai fornitori, al personale e ai prodotti. Per l'azienda è di fondamentale importanza garantire la riservatezza delle informazioni sui clienti, sui fornitori e sui lavoratori aziendali; per il rispetto della normativa vigente in materia di Privacy risulta di particolare importanza trattare correttamente i dati personali sia con gli strumenti informatici che cartacei. 	Interni
<ul style="list-style-type: none"> Sistema Informatico. Da un punto di vista sistemistico, l'architettura si basa su sistemi Windows e Linux in parte virtualizzati per i server e sistemi Windows per i pc. Le applicazioni ed i servizi più importanti sono: Sistema di posta elettronica, file server, Outlook, SO di rete. 	Interni
<ul style="list-style-type: none"> Dispositivi portatili. I dispositivi portatili in uso in azienda sono rappresentati da: Lap top (2 Apple, 14 Windows) e Hard Disk esterni (2). 	Interni
<ul style="list-style-type: none"> Archivi Cartacei. Alcuni dati possono essere in copie cartacee, archiviate in sede in appositi archivi, limitatamente ai dati di tipo contabile, amministrativo e relativi alla idoneità alla mansione. I dati in formato cartaceo sono conferiti anche allo studio del commercialista e del consulente paghe. 	Interni
<ul style="list-style-type: none"> Personale interno. Composto da 14 impiegati con competenze medie sull'utilizzo dei sistemi informatici. Le risorse umane si attendono di lavorare in un posto di lavoro rispettoso della normativa vigente in particolare dello statuto 	Interni

dei lavoratori e della normativa sulla Privacy. Si attendono il rispetto del pagamento dei propri emolumenti. Allo stato attuale, il clima aziendale è buono e non si sono mai registrate contestazioni rilevanti.	
<ul style="list-style-type: none"> La policy della Sicurezza dei dati. La policy è espressa compiutamente rispetto agli obiettivi strategici a cui vuole tendere l'organizzazione. La policy ha un visione di medio periodo. 	Interni
<ul style="list-style-type: none"> Obiettivi. Definizione degli obiettivi e delle strategie per la sicurezza dei dati. L'azienda ha identificato gli obiettivi da raggiungere ed ha predisposto un action plan dettagliato per il raggiungimento degli obiettivi strategici. 	Interni
<ul style="list-style-type: none"> Infrastrutture e Attrezzature. In tema di infrastrutture ed attrezzature l'azienda pone sotto controllo con manutenzioni preventive e controlli mirati il proprio parco infrastrutture ed attrezzature prodigandosi a sostituire attrezzature e/o mezzi obsoleti. Gli HW informatici (PC assegnati ai lavoratori) vengono sostituiti mediamente ogni 4 anni. 	Interni
<ul style="list-style-type: none"> Le competenze delle Risorse Umane. Per ciò che attiene le competenze, in tema di formazione l'organizzazione effettua periodicamente una gap analysis sui propri collaboratori al fine di accrescere il più possibile le competenze sia tecniche che organizzative/manageriali per stare al passo con le richieste provenienti dal mercato con particolare attenzione alla sicurezza delle informazioni. In particolare il responsabile, il System Administrator e gli incaricati al trattamento dei dati personali sono periodicamente sottoposti ad addestramento. 	Interni
<ul style="list-style-type: none"> Compliance. L'azienda per tenere sotto controllo il rispetto delle norme imperative e delle Leggi cogenti alle proprie attività è dotata di una struttura di servizi consulenziali che abbracciano i seguenti ambiti: Fiscale e Tributario, Consulente del lavoro, Medico competente, Sicurezza sui luoghi del lavoro, Contrattualistica, Consulenza Sistemi di Gestione, Privacy e tutela dei dati personali. Gli aspetti di cui sopra sono valutati di volta in volta con i vari consulenti durante le riunioni di follow-up. 	Interno
<ul style="list-style-type: none"> Standard adottati dall'organizzazione. L'organizzazione ha deciso di dotarsi di un sistema di gestione della Sicurezza delle Informazioni per tener meglio sotto controllo gli aspetti 	Interno

relativi alla compliance, ai requisiti cliente e requisiti normativi e legislativi applicabili in materia.	
<ul style="list-style-type: none"> • Reputazione. La nostra organizzazione è dal xxx sul mercato e gode di esperienza e reputazione per soddisfare tutti i requisiti in materia di Sistema di Gestione Sicurezza dei Dati e di Sicurezza dei Dati. Non sussistono problemi reputazionali dell'azienda. 	Interni/Esterni
<ul style="list-style-type: none"> • Soddisfazione clienti interni ed esterni. Il nostro valore è di fornire piena soddisfazione a tutte le parti interessate e siamo impegnati a conformarci a tutti i requisiti giuridici richiesti dalle direttive e norme applicabili. 	Interni/Esterni
<ul style="list-style-type: none"> • Impatti ambientali e Sicurezza sul lavoro. La natura delle attività è tale che essa non generi impatti di natura ambientale significativa né rischi per la sicurezza importanti. 	Interni
<ul style="list-style-type: none"> • I concorrenti. La concorrenza è molto sentita nel settore. La riservatezza gioca un ruolo fondamentale per evitare attività di migrazione di dati verso la potenziale concorrenza. 	Esterno
<ul style="list-style-type: none"> • I Clienti. I clienti richiedono il rispetto delle scadenze e la Sistema di Gestione Sicurezza dei Dati dei prodotti, in linea con i contratti stipulati e la normativa vigente. 	Esterno
<ul style="list-style-type: none"> • I Fornitori. I fornitori sono relativi a servizi consulenziali, e si attendono di veder apprezzati i loro sforzi per soddisfare le richieste dell'azienda e di essere pagati secondo le scadenze pattuite. 	Esterno
<ul style="list-style-type: none"> • Situazione economica attuale e prevista. In Italia è prevista una fase di crescita economica molto limitata. 	Esterno
<ul style="list-style-type: none"> • Clima politico e sociale. Allo stato, il clima politico in Italia è tale da generare incertezze sullo sviluppo economico del Paese. 	Esterno
<ul style="list-style-type: none"> • Risk management. L'azienda si è dotata di un piano di Business Continuity & Recovery Disaster. [Polizza Incendi RCT] 	Interno/Esterno

Questa è la lista degli aspetti interni/esterni che il RSGSD deve aggiornare e discutere con management.

L'organizzazione si avvale di un sistema di monitoraggio e di riesame delle informazioni che riguardano tali fattori esterni e interni.

Il SGSD adottato dalla Mater scarl permette all'Azienda di:

- stabilire una politica adatta alla propria realtà aziendale;
- identificare le prescrizioni legislative e normative applicabili;
- definire obiettivi e traguardi appropriati e la conseguente strategia per il raggiungimento degli stessi;
- pianificare, gestire, controllare e verificare l'applicazione del sistema di gestione della Sicurezza delle Informazioni in modo tale da assicurare l'adeguatezza dello stesso alla politica di gestione;
- identificare i pericoli connessi alla gestione dei dati elaborati presso l'organizzazione;
- adeguarsi ad eventuali cambiamenti aziendali.

4.2 Comprensione delle esigenze e delle aspettative delle parti interessate

Dato il loro effetto, o effetto potenziale, sulla capacità dell'organizzazione di fornire con regolarità prodotti e servizi che soddisfino i requisiti del cliente e quelli cogenti applicabili, l'organizzazione determina:

- a) le parti interessate rilevanti per il sistema di gestione della Sicurezza delle Informazioni;
- b) i requisiti di tali parti interessate che sono rilevanti per il sistema di gestione della Sicurezza delle Informazioni.

L'elenco di tutte le parti interessate sono identificate e sono elencate di seguito.

1. Clienti diretti
2. Legislatori, autorità competenti nazionali e europei
3. Fornitori
4. I Soci
5. Istituti di credito
6. Lavoratori

I requisiti di tutte le parti interessate pertinenti per il SGSD sono identificati in vari modi come elencato di seguito.

1. I clienti si attendono di ricevere prodotti e servizi conformi con il rispetto e la tutela della Privacy con dati gestiti dai prodotti integri e sempre disponibili.
2. Le autorità competenti si aspettano che l'azienda adotti un modello di gestione conforme alla normativa italiana al D. Lgs. 231/01 ed in particolare per la sicurezza delle informazioni che

adotti tutte le misure minime di sicurezza e le prescrizioni contenute nei Provvedimenti del Garante ad essa applicabili e al Reg. UE 2016/679.

3. I Fornitori si attendono di ricevere contratti chiari dal punto di vista della gestione dei dati ed in particolare, per quelli che trattano in nome e per conto dell'azienda dati personali in modo elettronico, anche la nomina diretta di responsabili del trattamento.

4. I Soci si attendono dall'azienda la Massimizzazione del ROE nel medio-lungo termine dal punto di vista economico e dal punto di vista della sicurezza dei dati il rispetto delle prescrizioni contenute nel sistema di gestione implementato in conformità alle leggi vigenti in materia.

5. Gli istituti di credito si attendono dall'azienda la capacità di riscuotere i propri crediti dai clienti da un lato assicurando il puntuale controllo degli scadenzari clienti.

6. Le risorse umane si attendono di lavorare in un posto di lavoro rispettoso della normativa vigente in particolare dello statuto dei lavoratori e della normativa sulla Privacy. Si attendono il rispetto del pagamento dei propri emolumenti.

L'organizzazione monitora e riesamina le informazioni che riguardano tali parti interessate e i loro requisiti rilevanti.

4.3 Il campo di applicazione del sistema di gestione della Sicurezza delle Informazioni

Il Sistema di gestione della Sicurezza delle Informazioni descritto nel presente Manuale si applica all'attività dell' Mater scarl riferita a:

[INSERIRE LO SCOPO]

L'organizzazione applica tutti i requisiti della presente norma internazionale se essi sono applicabili nell'ambito del campo di applicazione determinato del suo sistema di gestione della Sicurezza delle Informazioni.

4.4 Il sistema di gestione della Sicurezza delle Informazioni ed i suoi processi

4.4.1 Determinazione dei processi necessari per il sistema di gestione della Sicurezza delle Informazioni

L'organizzazione determina i processi necessari per il sistema di gestione della Sicurezza delle Informazioni e la loro applicazione nell'ambito di tutta l'organizzazione e:

- a) determina gli input necessari e gli output attesi da tali processi;
- b) determina la sequenza e l'interazione di tali processi;
- c) determina e applica i criteri e i metodi (compresi il monitoraggio, le misurazioni e gli indicatori di prestazione correlati), necessari 'ad assicurare l'efficace funzionamento e la tenuta sotto controllo di tali processi;
- d) determina le risorse necessarie per tali processi e assicurarne la disponibilità;

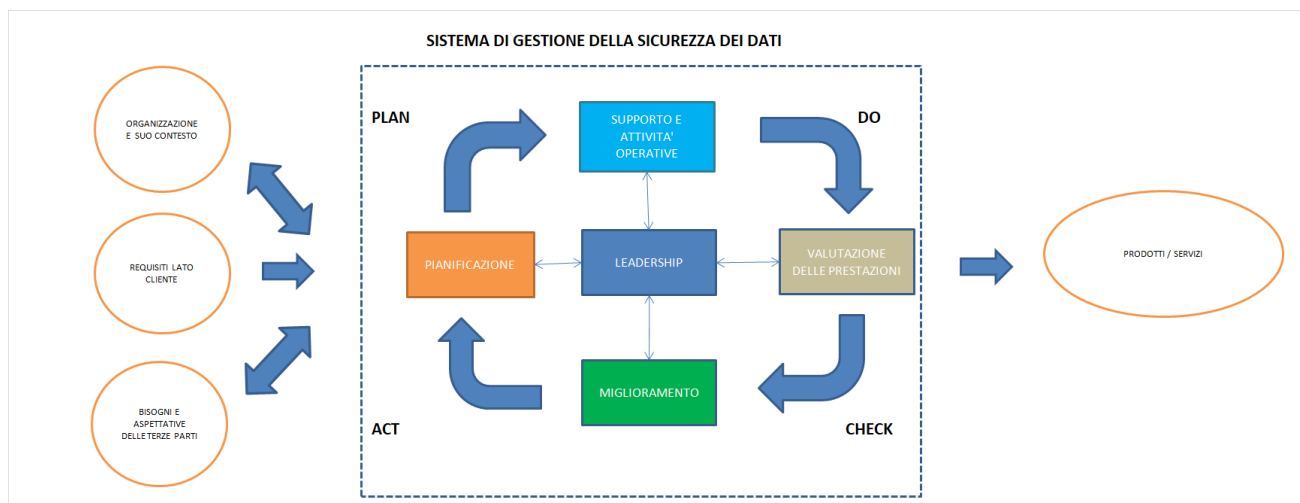
- e) attribuisce le responsabilità e le autorità per tali processi;
- f) affronta i rischi e le opportunità come determinati in conformità ai requisiti di cui al punto 6.1;
- g) valuta tali processi e attuare ogni modifica necessaria per assicurare che tali processi conseguano i risultati attesi;
- h) migliora i processi e il sistema di gestione della Sicurezza delle Informazioni.

Il SGSD messo in atto permette di identificare i processi che impattano sulla funzionalità dell'azienda, di stabilirne il corretto flusso e la loro interazione, gestendoli attraverso opportuni controlli ed indicatori.

Per processo si intende un qualsiasi "sistema di attività che utilizza risorse per trasformare elementi in ingresso in elementi in uscita. ...I processi in una organizzazione sono di regola pianificati ed eseguiti in condizioni controllate al fine di aggiungere valore".

Nell'Allegato 4 – **Processi del Sistema di Gestione** sono rappresentati nel dettaglio i processi fondamentali su cui le norme ISO/IEC 27001:2013 si basano.

Di seguito vengono presentate le tabelle relative ai processi aziendali per la realizzazione del prodotto conformemente a quanto prescritto nella ISO 27001:2013.



Di seguito vengono indicati i Macro Processi Aziendali, i processi di Dettaglio e le Procedure operative di riferimento descrittive dei processi di dettaglio.

Blocchi SGSD	Macro processo	Processi di Dettaglio	ID	Nome Procedura
LEADERSHIP	PROCESSO DIREZIONALE	PROCESSO DI ANALISI DEL CONTESTO	-	-
	PROCESSO DIREZIONALE	PROCESSO DI DEFINIZIONE DELL'ORGANIGRAMMA, RUOLI E RESPONSABILITA'	-	-
PIANIFICAZIONE	PROCESSO DIREZIONALE	VALUTAZIONE DEL RISCHIO RELATIVO ALLA SICUREZZA DELLE INFORMAZIONI	PR. 6.1.1	VALUTAZIONE DEI RISCHI E DELLE OPPORTUNITA'
	PROCESSO DIREZIONALE	TRATTAMENTO DEL RISCHIO RELATIVO ALLA SICUREZZE DELLE INFORMAZIONI	PR. 6.1.3	PIANO DI TRATTAMENTO DEL RISCHIO
	PROCESSO DIREZIONALE	DEFINIZIONE DELLA POLITICA, DEGLI OBIETTIVI AZIENDALI E GESTIONE DEI RIESAMI	PR. 9.3	MODALITA' DEFIN. POLITICHE E OBIETTIVI AZIENDALI - GESTIONE DEI RIESAMI
SUPPORTO	PROCESSO DIREZIONALE	GESTIONE DELLA DOCUMENTAZIONE	PR. 7.5	GESTIONE DOCUMENTAZ. SISTEMA GEST. E DOCUMENTI REGISTRAZIONE
			PR. 2.1	GESTIONE DELLA DOCUMENTAZIONE NORMATIVA E LEGISLATIVA
	PROCESSO GESTIONE RISORSE	GESTIONE DELLE RISORSE UMANE	PR. 7.2.1	GESTIONE DELLE RISORSE UMANE
ATTIVITA' OPERATIVE	PROCESSO DI REALIZZAZIONE DEL PRODOTTO/SERVIZIO	APPROVVIGIONAMENTO	PR. 8.4	GESTIONE APPROVVIGIONAMENTI
VALUTAZIONE DELLE PRESTAZIONI	MONITORAGGIO, MISURAZIONE, ANALISI E VALUTAZIONE	MONITORAGGI, ANALISI DEI DATI E TECNICHE STATISTICHE	PR. 9.1	MONITORAGGI, ANALISI DEI DATI E TECNICHE STATISTICHE
	CONFORMITA DEL SISTEMA DI GESTIONE	GESTIONE DEGLI AUDIT	PR. 9.2	GESTIONE AUDIT
	CONFORMITA DEL SISTEMA DI GESTIONE	NON CONFORMITA' E AZIONI CORRETTIVE	PR. 10.1	GESTIONE DELLE NON CONFORMITA' E AZIONI CORRETTIVE
MIGLIORAMENTO	MIGLIORAMENTO CONTINUO	GESTIONE DEL MIGLIORAMENTO CONTINUO	PR. 10.2	AZIONI DI MIGLIORAMENTO

5 LEADERSHIP

5.1 Leadership e impegno

L'alta direzione dimostra la necessaria leadership e impegno nei riguardi del sistema di gestione della Sicurezza delle Informazioni.

La Direzione:

- a) si assume la responsabilità dell'efficacia del sistema di gestione della Sicurezza delle Informazioni;
- b) stabilisce la politica e gli obiettivi per la Sistema di Gestione Sicurezza dei Dati relativi al sistema di gestione della Sicurezza delle Informazioni e verifica che essi siano compatibili con il contesto e con gli indirizzi strategici dell'organizzazione;
- c) assicura l'integrazione dei requisiti del sistema di gestione della Sicurezza delle Informazioni nei processi di business dell'organizzazione;
- d) promuove l'utilizzo dell'approccio per processi e del *risk-based thinking*;
- e) assicura la disponibilità delle risorse necessarie al sistema di gestione della Sicurezza delle Informazioni;
- f) comunica la politica e l'importanza di una gestione della Sicurezza delle Informazioni efficace, e della conformità ai requisiti del sistema di gestione della Sicurezza delle Informazioni;
- g) assicura che il sistema di gestione della Sicurezza delle Informazioni consegua i risultati attesi;
- h) facilitando la partecipazione attiva, guidando e sostenendo le persone affinché contribuiscano all'efficacia del sistema di gestione della Sicurezza delle Informazioni;
- i) promuove il miglioramento;
- j) fornisce il sostegno agli altri pertinenti ruoli gestionali per dimostrare la loro leadership, come essa si applica alle rispettive aree di responsabilità.

L'alta direzione dimostra anche leadership e impegno riguardo alla focalizzazione sul cliente, assicurando che:

- a) siano determinati, compresi e soddisfatti con regolarità i requisiti del cliente e i requisiti cogenti applicabili;
- b) siano determinati e affrontati i rischi e le opportunità che possono influenzare la conformità dei prodotti e servizi e la capacità di accrescere la soddisfazione del cliente;
- c) sia mantenuta la focalizzazione sull'aumento della soddisfazione del cliente.

5.2 Politica del Sistema di gestione

L'alta direzione ha stabilito, attuato e mantenuto una politica per la Sicurezza delle Informazioni che:

- a) è appropriata alle finalità e al contesto dell'organizzazione e supporta gli indirizzi strategici;
- b) costituisce un quadro di riferimento per fissare gli obiettivi della Sicurezza delle Informazioni;
- c) comprende un impegno a soddisfare i requisiti applicabili;

d) comprende un impegno per il miglioramento continuo del sistema di gestione della Sicurezza delle Informazioni.

L'Organizzazione, con la collaborazione delle parti interessate, ha definito la politica garantendo che:

- sia facilmente comprensibile dalle parti interessate, sia interne che esterne all'Azienda;
- sia comunicata all'interno e alle parti interessate;
- sia adeguata alla natura e alla tipologia di rischi per la Sicurezza delle Informazioni;
- sia adottata e periodicamente riesaminata alla luce degli audit interni e ne sia valutata periodicamente la congruenza con la realtà aziendale;
- fornisca il quadro di riferimento per riesaminare gli obiettivi e i traguardi aziendali;
- includa un impegno al rispetto della legislazione applicabile e ad eventuali accordi volontari sottoscritti dalla ditta;
- includa un impegno continuativo del sistema adottato;

La politica della Sicurezza delle Informazioni è:

- a) resa disponibile e mantenuta come informazione documentata;
- b) comunicata, compresa e applicata all'interno dell'organizzazione tramite affissione in bacheca e condivisione interna sulla rete aziendale;
- c) disponibile alle parti interessate rilevanti, per quanto appropriato tramite il sito web aziendale.

La Direzione ha determinato le parti interessate a cui comunicare la politica:

- Potenziali clienti (che la richiedono per decidere se stipulare o meno un contratto);
- I fornitori (affinchè vi si adeguino);
- Gli auditor o ispettori esterni.

La Direzione della Mater scarl verifica, almeno una volta l'anno, se la Politica è valida tramite il periodico Riesame della Direzione.

Si vedano gli allegati: **All 1 Politica SGSD.**

5.3 Ruoli, responsabilità e autorità nell'organizzazione

L'alta direzione assicura che le responsabilità e le autorità per i ruoli pertinenti siano assegnate, comunicate e comprese all'interno dell'organizzazione.

L'alta direzione assegna le responsabilità e autorità per:

- a) assicurare che il sistema di gestione della Sicurezza delle Informazioni sia conforme ai requisiti della presente norma internazionale;
- b) assicurare che i processi stiano producendo gli output attesi;
- c) riferire, in particolare all'alta direzione, sulle prestazioni del sistema di gestione della Sicurezza delle Informazioni e sulle opportunità di miglioramento;
- d) assicurare che l'integrità del sistema di gestione della Sicurezza delle Informazioni sia mantenuta, quando vengono pianificate e attuate modifiche al sistema stesso.

Al fine di garantire l'efficiente funzionamento del SGSD, sono identificati i ruoli, le responsabilità, i compiti e i rapporti reciproci di tutto il personale che dirige, svolge e controlla le attività che hanno un impatto sulla sicurezza delle informazioni (si vedano **AII 2 – MANSIONARIO AZIENDALE, AII 3A – ORGANIGRAMMA AZIENDALE FUNZIONALE, AII 3B – ORGANIGRAMMA AZIENDALE PRIVACY**).

Le responsabilità sono specificate nel mansionario aziendale **AII 2 – MANSIONARIO AZIENDALE**.

La struttura specifica per la gestione del sistema di gestione delle informazioni, è rappresentata dall'Organigramma Aziendale (si Veda **AII 3A – ORGANIGRAMMA AZIENDALE FUNZIONALE**) che da una chiara specifica sui ruoli.

6 PIANIFICAZIONE

6.1 Piano per affrontare rischi ed opportunità

6.1.1 Generalità

Nel pianificare il sistema di gestione della Sicurezza delle Informazioni, l'organizzazione deve considerare i fattori di cui al punto 4.1 e i requisiti di cui al punto 4.2 e determinare i rischi e le opportunità che è necessario affrontare per:

- a) fornire assicurazione che il sistema di gestione della Sicurezza delle Informazioni possa conseguire il risultato(i) atteso(i);
- b) accrescere gli effetti desiderati;
- c) prevenire, o ridurre, gli effetti indesiderati;
- d) conseguire il miglioramento.

L'organizzazione pianifica:

- a) le azioni per affrontare questi rischi e opportunità;
- b) le modalità per:
 - 1) integrare e attuare le azioni nei processi del proprio sistema di gestione (vedere punto 4.4);
 - 2) valutare l'efficacia di tali azioni.

L'azienda pone in essere tre tipi di pianificazione:

- Pianificazione strategica che comprende le scelte generali relative al sistema di gestione, la preparazione e la pubblicazione della politica per la sicurezza delle informazioni, la scelta degli obiettivi strategici, l'individuazione dei processi e dei controlli del sistema di gestione, le loro caratteristiche generali e le loro relazioni;
- Pianificazione tattica che stabilisce i dettagli dei processi e dei controlli di sicurezza da attuare, i loro obiettivi, le risorse necessarie per realizzare quanto pianificato, le attività che compongono i processi e la loro frequenza o scadenza;
- Pianificazione operativa che stabilisce quando effettuare le attività tra cui: manutenzione degli impianti, riesami delle utenze, esecuzione delle prove di ripristino, esecuzione dei test di continuità operativa, esecuzione dei vulnerabilità assessment, acquisizione delle risorse materiali, reperimento delle persone, formalizzazione dei contratti con i fornitori.

6.1.2 Valutazione del rischio relativo alla sicurezza delle informazioni

L'organizzazione determina una sia una valutazione dei rischi relativi al sistema di gestione delle informazioni che sono originati dai fattori interni ed esterni che compongono il contesto della organizzazione che vengono identificati e valutati che una valutazione del rischio relativo alla sicurezza delle informazioni.

In ogni caso, l'organizzazione:

- a) Stabilisce e mantiene i criteri di rischio che includano:
 1. I criteri per l'accettazione del rischio;

2. I criteri per effettuare valutazioni del rischio relativo alla sicurezza delle informazioni;
- b) Assicura che le ripetute valutazioni del rischio producano risultati coerenti, validi e confrontabili tra di loro;
 - c) Identifica i rischi relativi alla sicurezza delle informazioni, associando i rischi alla potenziale perdita di riservatezza, integrità e disponibilità delle informazioni ed identificando un responsabile per ciascun rischio identificato;
 - d) Analizza i rischi relativi alla sicurezza delle informazioni, determinandone il livello di rischio sulla base della valutazione delle loro conseguenze e probabilità;
 - e) Pondera i rischi confrontandoli con i criteri di rischio e li ordina per dare la corretta priorità per il loro trattamento.

L'azienda ha strutturato una procedura operativa per la valutazione dei rischi e la determinazione delle opportunità denominata **PR 6.1.1 – Valutazione dei rischi e delle opportunità**.

6.1.3 Trattamento del rischio relativo alla sicurezza delle informazioni

L'organizzazione determina e applica un processo di trattamento del rischio per:

- a) individuare le opzioni per il trattamento del rischio tenendo in considerazione i risultati della valutazione del rischio;
- b) determinare tutti i controlli necessari per attuare le opzioni selezionate per il trattamento del rischio relativo alla sicurezza delle informazioni;
- c) confrontare i controlli individuati con quelli dell'Appendice A della norma e verificare che non siano omessi controlli necessari;
- d) redigere il documento "Dichiarazione di Applicabilità" che riporta i controlli necessari e le giustificazioni per l'inclusione e l'esclusione di alcuni controlli;
- e) formulare un piano di trattamento del rischio;
- f) ottenere l'approvazione del piano di trattamento del rischio e l'accettazione dei rischi residui relativi alla sicurezza delle informazioni da parte dei responsabili dei rischi.

L'Azienda ha strutturato una procedura per il trattamento del rischio relativo alla sicurezza delle informazioni denominata opportunità denominata **PR 6.1.3 – Piano di trattamento del rischio**.

6.2 Obiettivi per la sicurezza delle informazioni e pianificazione per il loro raggiungimento

L'organizzazione stabilisce gli obiettivi per la sicurezza delle informazioni relativi alle funzioni, ai livelli e ai processi pertinenti, necessari per il sistema di gestione della Sicurezza delle Informazioni.

Gli obiettivi per la sicurezza delle informazioni:

- a) sono coerenti con la politica;
- b) sono misurabili;
- c) tengono in considerazione i requisiti applicabili e i risultati della valutazione dei rischi e del trattamento dei rischi;

- d) sono comunicati;
- e) sono aggiornati per quanto appropriato.

Gli obiettivi per la sicurezza delle informazioni sono documentati.

Nel pianificare come raggiungere i propri obiettivi per la sicurezza delle informazioni, l'organizzazione determina:

- a) cosa sarà fatto;
- b) quali risorse saranno richieste;
- c) chi ne sarà responsabile;
- d) quando sarà completato;
- e) come saranno valutati i risultati.

Gli Obiettivi e il loro riesame, vengono definiti da parte del DGE con l'assistenza del RSGSD. La direzione della Mater scarl garantisce che gli obiettivi relativi alla Sistema di Gestione Sicurezza dei Dati siano stabiliti per le funzioni ed i livelli aziendali pertinenti.

I principi generali della gestione della sicurezza delle informazioni abbracciano vari aspetti:

- 1- Deve esistere un catalogo costantemente aggiornato degli asset aziendali rilevanti ai fini della gestione delle informazioni e per ciascuno deve essere individuato un responsabile. Le informazioni devono essere classificate in base al loro livello di criticità, in modo da essere gestite con livelli di riservatezza ed integrità coerenti ed appropriati.
- 2- Per garantire la sicurezza delle informazioni, ogni accesso ai sistemi deve essere sottoposto a una procedura d'identificazione e autenticazione. Le autorizzazioni di accesso alle informazioni devono essere differenziate in base al ruolo ed agli incarichi ricoperti dai singoli individui, in modo che ogni utente possa accedere alle sole informazioni di cui necessita, e devono essere periodicamente sottoposte a revisione.
- 3- Devono essere definite delle procedure per l'utilizzo sicuro dei beni aziendali e delle informazioni e dei loro sistemi di gestione.
- 4- Deve essere incoraggiata la piena consapevolezza delle problematiche relative alla sicurezza delle informazioni in tutto il personale (dipendenti e collaboratori) a partire dal momento della selezione e per tutta la durata del rapporto di lavoro.
- 5- Per poter gestire in modo tempestivo gli incidenti, tutti devono notificare qualsiasi problema relativo alla sicurezza. Ogni incidente deve essere gestito come indicato nelle procedure.
- 6- È necessario prevenire l'accesso non autorizzato alle sedi e ai singoli locali aziendali dove sono gestite le informazioni e deve essere garantita la sicurezza delle apparecchiature.
- 7- Deve essere assicurata la conformità con i requisiti legali e con i principi legati alla sicurezza delle informazioni nei contratti con le terze parti.
- 8- Deve essere predisposto un piano di continuità che permetta all'azienda di affrontare efficacemente un evento imprevisto, garantendo il ripristino dei servizi critici in tempi e con modalità che limitino le conseguenze negative sulla missione aziendale.
- 9- Gli aspetti di sicurezza devono essere inclusi in tutte le fasi di progettazione, sviluppo, esercizio, manutenzione, assistenza e dismissione dei sistemi e dei servizi informatici.

10- Devono essere garantiti il rispetto delle disposizioni di legge, di statuti, regolamenti o obblighi contrattuali e di ogni requisito inerente la sicurezza delle informazioni, riducendo al minimo il rischio di sanzioni legali o amministrative, di perdite rilevanti o danni alla reputazione.

Gli obiettivi e traguardi relativi ad ogni aspetto ritenuto significativo da parte della Mater scrl sono specifici e, dove possibile, misurabili, coerenti con la politica, includendo l'impegno per il miglioramento continuativo e il mantenimento della conformità normativa.

La definizione degli Obiettivi e il loro riesame, avviene, di norma, in seguito ad un riesame dei contenuti della politica aziendale, all'analisi delle normative vigenti emanate a livello nazionale e, quando applicabili, a livello internazionale (es. per quanto concerne le normative in materia ambientale e di salute e sicurezza sul lavoro sono previsti a livello di sistema di gestione della Sicurezza delle Informazioni appositi documenti di registrazione delle modifiche normative aggiornato con periodicità trimestrale), all'analisi dei contenuti del documento di valutazione dei rischi, nonché dei risultati degli audit interni ed esterni condotti da terze parti.

Gli obiettivi individuati, tengono in considerazione delle risorse economiche e finanziarie a disposizione della Mater scrl e la migliore tecnologia disponibile.

Gli obiettivi periodici sono portati a conoscenza di tutte le parti interessate con apposito documento emesso dalla direzione.

Il Programma di Gestione, è il documento attraverso il quale [NOME_AZIENDA], rende operative le azioni pianificate per il mantenimento della conformità normativa e il miglioramento continuo delle prestazioni aziendali in termini di Sistema di Gestione Sicurezza dei Dati e salute e sicurezza sul lavoro.

Nel programma di Gestione, sono individuati gli indicatori prestazionali, le singole azioni adottate per raggiungere gli obiettivi. Per ogni singola azione, viene individuato il responsabile della sua attuazione, il tempo di realizzazione e le relative risorse.

Se ritenuto necessario, nel Programma di Gestione, sono definiti i traguardi intermedi che permettono il controllo progressivo delle azioni rispetto agli Obiettivi da raggiungere. La realizzazione di tali traguardi, viene sorvegliata ad intervalli stabiliti e nel caso di inadeguatezza del loro livello di realizzazione, si interverrà con Azioni Correttive.

Se un progetto riguarda nuovi sviluppi, oppure attività, prodotti o servizi nuovi o modificati, i programmi devono essere rivisti, ove è necessario, per garantire che ad essi si applichi un corretto SGSD.

La procedura di riferimento è la **PR 9.3 – Modalità di definizione delle politiche e degli obiettivi aziendali e gestione dei Riesami.**

7 SUPPORTO

7.1 Risorse

L'organizzazione determina e fornisce le risorse necessarie per l'istituzione, l'attuazione, il mantenimento e il miglioramento continuo del sistema di gestione della Sicurezza delle Informazioni.

7.2 Competenza

L'organizzazione:

- a) determina le competenze richieste e necessarie per le persone che lavorano e che influenzano le prestazioni della Sicurezza delle Informazioni;
- b) assicura che le persone siano competenti sulla scorta delle attività di istruzione, formazione e addestramento o esperienza maturata sul campo documentabile;
- c) pianifica e realizza azioni per disporre delle competenze mancanti attraverso corsi di formazione, affiancamenti, assunzioni di personale skillato o inserimento di consulenti esperti in azienda;
- d) valuta l'efficacia delle azioni intraprese.

La procedura di riferimento è la **PR 7.2.1 - Gestione delle Risorse Umane**.

7.3 Consapevolezza

L'organizzazione determina attraverso un processo di sensibilizzazione un adeguato livello di consapevolezza su:

- a) Politica della sicurezza delle informazioni;
- b) Come ciascuno possa contribuire all'efficacia del sistema di gestione della sicurezza delle informazioni;
- c) I benefici di un sistema di gestione efficace;
- d) Le conseguenze del mancato adeguamento ai requisiti del sistema di gestione.

La procedura di riferimento è la **PR 7.2.1 - Gestione delle Risorse Umane**.

7.4 Comunicazione

L'organizzazione determina le necessità per le comunicazioni interne ed esterne indicando:

- a) Cosa comunicare;
- b) Quando comunicare;
- c) Chi deve comunicare;
- d) Chi sono gli interlocutori interni ed esterni all'organizzazione con cui comunicare.

Le comunicazioni possono riguardare processi direzionali o di pubbliche relazioni esterne (aventi ad oggetto Politiche, incidenti, ecc.), relazioni interne (politiche, incidenti, organigramma, mansionari,

procedure operative, ecc.), processi operativi (aggiornamento dei sistemi informatici, incidenti, audit interni, audit di terza parte, ecc.).

Le comunicazioni interne hanno lo scopo di rendere partecipi gli interessati al SGSD e possono essere gestite:

- mediante comunicazione verbale;
- mediante comunicazione scritta e consegnata personalmente;
- mediante posta elettronica;
- mediante comunicazione scritta affissa nella bacheca aziendale;
- attraverso riunioni periodiche che permettono il confronto e la discussione sulle problematiche aziendali;
- mediante le bacheche aziendali.

Inoltre, Mater scarl garantisce che l'organizzazione risponda adeguatamente alle richieste provenienti dalle parti interessate esterne (Clienti, fornitori, Enti di Controllo e Pubbliche Autorità, associazioni ambientaliste, abitanti, ecc.), in relazione ai suoi aspetti legati alla sicurezza delle informazioni.

Tutte le funzioni aziendali possano convocare ed indire riunioni per analizzare e valutare situazioni particolari in merito soprattutto ad attività di interazione tra una funzione e l'altra; dall'esito di tali incontri possono scaturire modifiche alle descrizioni dei processi aziendali sia per migliorare la trasmissione di informazioni sia per adeguamento ai cambiamenti.

Mater scarl mantiene registrazioni delle decisioni assunte in merito a procedimenti di comunicazione esterna e delle comunicazioni effettuate.

La procedura di riferimento è la **PR 7.2.1 - Gestione delle Risorse Umane**.

7.5 Informazioni documentate

Il Sistema di gestione della Sicurezza delle Informazioni della Mater scarl si basa sulla seguente documentazione:

- dichiarazioni sulla politica aziendale, sugli obiettivi e traguardi prefissati;
- il presente manuale di Gestione della Sicurezza delle Informazioni;

- le procedure documentate richieste dalla norma internazionale e dal manuale stesso;
- le istruzioni operative e i documenti di registrazione;
- i documenti necessari all'organizzazione per assicurare l'efficace pianificazione, funzionamento e controllo dei suoi processi.

Per ciò che attiene i documenti di attuazione, il Sistema di gestione della Sicurezza delle Informazioni è documentato attraverso i documenti che includono:

- Campo di applicazione (punto della norma 4.3) → Nel Manuale nel par. 4.3;
- Gestione della documentazione normativa e legislativa → Nella Procedura 2.1;
- Politica per la sicurezza delle informazioni (5.2) → Nell'Allegato 1 al Manuale;
- Processo di valutazione del rischio relativo alla sicurezza delle informazioni (6.1.2) → Nella Procedura 6.1.1.;
- Dichiarazione di Applicabilità dei controlli (Appendice A della Norma) (6.1.3 d) → Nella Procedura 6.1.3;
- Piano di trattamento del rischio (6.1.3 e) → Nella Procedura 6.1.3;
- Obiettivi per la sicurezza delle informazioni (6.2) → Nella Procedura 9.3;
- Competenze delle Risorse Umane (7.2) → Nella Procedura 7.2.1;
- Gestione della documentazione del Sistema di gestione → Nella Procedura 7.5;
- Processi interni ed affidati all'esterno (8.1) → Nel Manuale nel par. 8.1;
- Gestione dei processi relativi al cliente (8.1) → Nel Manuale nel par. 8.1;
- Progettazione (8.1) → Nel Manuale nel par. 8.1;
- Approvvigionamento (8.1) → Nella Procedura 8.4;
- Gestione del Processo (8.1) → Nella Manuale par 8.1;
- Monitoraggi e Misurazioni (9.1) → Nella Procedura 9.1;
- Programma di Audit e Risultati di Audit (9.2) → Nella Procedura 9.2;
- Risultati del Riesame della Direzione (9.3) → Nella Procedura 9.3;
- Natura delle non conformità e azioni intraprese (10.1 f) → Nella Procedura 10.1;
- Risultati di ogni azione correttiva (10.1 g) → Nella Procedura 10.1
- Miglioramento Continuo (10.2) → Nella Procedura 10.2

7.5.1 Manuale del Sistema di gestione della Sicurezza delle Informazioni

Il Manuale del Sistema di gestione della Sicurezza delle Informazioni è il documento di riferimento nell'ambito del SGSD e richiama le procedure sviluppate per soddisfare, a livello operativo, i requisiti delle norme tecniche di riferimento.

Il Manuale è stato articolato in Paragrafi direttamente corrispondenti alla **struttura della Norma ISO/IEC 27001:2013**.

Il Manuale del SGSD rappresenta il primo livello della documentazione di Sistema e descrive:

il campo di applicazione del sistema di gestione;

il riferimento alle procedure predisposte per il sistema di gestione;

le modalità generali di applicazione dei requisiti espressi dalla norma di riferimento e le relative responsabilità.

Il Manuale del SGSD è un documento soggetto a controllo e le regole di redazione, verifica e approvazione le cui regole sono indicate nella **PR 7.5 Gestione della Documentazione del Sistema di gestione della Sicurezza delle Informazioni e Documenti di Registrazione**

Lo stato di aggiornamento dei vari capitoli del Manuale è riportato nella seconda pagina di copertina e l'aggiornamento di un solo capitolo del MSGSD comporta l'aggiornamento dello stato di revisione generale riportato in copertina.

MANUALE (MSGSD)

É il documento che descrive il Sistema di gestione della Sicurezza delle Informazioni come riferimento permanente e ne costituisce la raccolta delle prescrizioni generali.

Esso contiene:

- la Politica e gli obiettivi per la Sicurezza delle Informazioni;
- la struttura organizzativa e le relative responsabilità;
- le modalità gestionali ed operative per la Sicurezza delle Informazioni adottate dall'azienda, dettagliate oltre che nelle sezioni anche nelle Procedure e nelle Istruzioni;
- la strutturazione e la distribuzione della documentazione del Sistema di gestione della Sicurezza delle Informazioni.

PROCEDURE (PR)

Le Procedure, di tipo Gestionale e Operativo, sono documenti in generale derivati da una sezione che regolamentano in modo dettagliato, le modalità di applicazione; impongono responsabilità, relazioni funzionali, modi ed eventualmente tempi di esecuzione attività e i riferimenti circa la raccolta e la conservazione della documentazione di registrazione della Sistema di Gestione Sicurezza dei Dati generatasi.

Le PR sono indicate con la sigla:

PR XX, ove XX indica la sezione di riferimento alla norma.

ISTRUZIONI (IS)

Qualora il dettaglio operativo di una procedura risulti troppo complesso e articolato è conveniente esplodere lo stesso in una o più Istruzioni che definiscono sinteticamente le modalità di svolgimento dell'attività.

Le IS sono identificate con la sigla:

IS XXY ove XXY è il riferimento alla sezione o alla procedura dalla quale prendono spunto.

MODULISTICA

Nello svolgimento delle singole mansioni e nel rispetto delle procedure e istruzioni previste, a volte è necessaria la compilazione di appositi moduli, al fine di registrare dati ed informazioni e documentare determinati eventi affinché ne resti traccia oggettivamente riscontrabile.

Tutti i moduli sono indicati con la sigla Mod XX, ove XX ha il significato visto in precedenza per le Procedure.

7.5.2 Creazione e aggiornamento

L'attività viene condotta secondo quanto previsto dalla procedura **PR 7.5 Gestione della Documentazione del Sistema di gestione della Sicurezza delle Informazioni e Documenti di Registrazione** al fine di assicurare che le edizioni aggiornate della documentazione siano disponibili dove servono ed accessibili a chi ne faccia richiesta, fermo restando gli eventuali limiti stabiliti dalla Direzione.

Il Manuale è redatto, revisionato e distribuito secondo quanto indicato nella suddetta procedura nella quale sono dettagliate le responsabilità per la preparazione, modifica, verifica ed approvazione dei documenti.

Il Manuale, le Procedure, le Istruzioni di Lavoro sono a disposizione del personale in apposite cartelle del sistema informatico aziendale, visibili, in lettura, a tutti gli utenti.

7.5.3 Controllo delle informazioni documentate

L'attività viene condotta secondo quanto previsto dalla procedura **PR 7.5 Gestione della Documentazione del Sistema di gestione della Sicurezza delle Informazioni e Documenti di Registrazione**.

I documenti di gestione, i documenti tecnici e i documenti di registrazione sono tutti quei documenti citati nel presente Manuale, nelle Procedure, nelle Istruzioni Operative ed eventuali altri documenti necessari a dimostrare la conformità dei prodotti/servizi erogati dall'azienda ai requisiti vigenti o volontari stabiliti dall'Organizzazione.

È cura di tutto il personale dell'azienda rispettare le prescrizioni del presente Manuale e gestire correttamente (compresa la compilazione) i documenti di registrazione ivi richiamati.

Le registrazioni prodotte dalla Mater scarl dimostrano l'evidenza oggettiva di:

- attività formative eseguite;

- risultati ottenuti durante la conduzione degli audit (prima, seconda e terza parte);
- riesami aziendali che garantiscano l'adeguatezza e efficacia del SGSD;
- registrazione delle NC, AC e AP, incidenti, mancati incidenti ed infortuni;
- informazioni sulla preparazione delle emergenze e sulle risposte (Business Continuity & Recovery Disaster);
- informazioni sugli aspetti di Sistema di Gestione Sicurezza dei Dati legati ai processi e ai rischi aziendali individuati;
- Dichiarazioni di applicabilità
- Piano dei trattamenti dei rischi
- leggi, norme applicabili e autorizzazioni.

Le registrazioni devono essere leggibili, identificabili e riconducibili all'attività, al prodotto o al servizio cui si riferiscono.

Devono inoltre essere archiviate e conservate in modo da essere facilmente rintracciate e protette contro danneggiamenti, deterioramenti e perdite. La durata di conservazione deve essere preventivamente stabilita e documentata.

La documentazione viene raccolta, controllata, registrata, elencata e conservata in un apposito archivio, nel quale si trovano

Tali documenti, scritti o memorizzati su supporto informatico, permettono di ricavare dati di tendenza e migliorare l'attuazione e l'efficacia del SGSD.

La Mater scarl mantiene sotto controllo il processo di gestione delle registrazioni durante tutte le sue fasi: identificazione delle registrazioni, definizione dei loro contenuti, conservazione e protezione, rintracciabilità, archiviazione e distruzione.

8 ATTIVITA' OPERATIVE

8.1 Pianificazione e controllo operativi

Mater scarl pianifica, attua e tiene sotto controllo i processi necessari per soddisfare i requisiti della sicurezza delle informazioni e per porre in essere le azioni necessarie per affrontare i rischi. Inoltre, l'organizzazione attua i piani per conseguire gli obiettivi per la sicurezza delle informazioni.

In particolare l'azienda ha definito alcune istruzioni operative specifiche per il controllo operativo derivanti dall'applicazione o meno dei controlli previsti dall'annex A.

La procedura di riferimento è la **PR 6.1.3 TRATTAMENTO DEL RISCHIO SICUREZZA DELLE INFORMAZIONI**.

L'azienda gestisce e monitora le azioni intraprese valutandone l'efficacia e gestisce le non conformità e le azioni correttive.

Allo stato, l'azienda ha processi in outsourcing che tiene sotto controllo attraverso audit di seconda parte.

8.2 Valutazione del rischio relativo alla sicurezza delle informazioni

L'azienda ha determinato la frequenza di valutazione del rischio relativo alla sicurezza delle informazioni:

- Ogni anno in conseguenza del riesame della direzione, in assenza di non conformità;
- Al verificarsi di una non conformità;
- Al verificarsi di un cambiamento significativo degli asset aziendali;
- Al verificarsi di un cambiamento significativo delle condizioni al contorno (Contesto interno/esterno).

8.3 Trattamento del rischio relativo alla sicurezza delle informazioni

L'organizzazione attua il piano di trattamento del rischio relativo alla sicurezza delle informazioni che viene riesaminato secondo la seguente periodicità:

- Ogni anno in conseguenza del riesame della direzione, in assenza di non conformità;
- Al verificarsi di una non conformità;
- Al verificarsi di un cambiamento significativo degli asset aziendali;
- Al verificarsi di un cambiamento significativo delle condizioni al contorno (Contesto interno/esterno).

9 VALUTAZIONE DELLE PRESTAZIONI

9.1 Monitoraggio, misurazione, analisi e valutazione

Mater scarl valuta le prestazioni della sicurezza delle informazioni e la relativa efficacia del sistema di gestione implementato.

L'organizzazione in tema di monitoraggio identifica:

- La programmazione delle attività quali audit, verifica dei ripristini dei back-up, test di continuità;
- La rilevazione degli eventi sui sistemi informatici;
- I tempi di indisponibilità dei sistemi e delle loro componenti;
- I tempi di risoluzione degli incidenti;
- Il numero di difetti (Bug) rilevati nei software sviluppati;
- Il numero dei reclami dei clienti pertinenti la sicurezza delle informazioni;
- L'incidenza delle penali riguardanti la sicurezza delle informazioni sul fatturato;
- Intrusioni / attacchi esterni.

L'organizzazione in tema di misurazioni rileva:

- I tempi di indisponibilità dei sistemi e delle loro componenti;
- I tempi di risoluzione degli incidenti;
- Il numero di difetti (Bug) rilevati nei software sviluppati;
- Il numero dei reclami dei clienti pertinenti la sicurezza delle informazioni;
- L'incidenza delle penali riguardanti la sicurezza delle informazioni sul fatturato;
- Il numero di intrusioni / attacchi esterni.

Il monitoraggio e le misurazioni devono essere effettuate continuamente con report mensili. Il RSGSD è responsabile di collezionare tutti i dati dei rilevamenti e di riferirli a DGE.

I Dati vengono analizzati su base mensile a cura di DGE.

Ad ogni misurazione viene associato uno specifico obiettivo.

Le registrazioni e le elaborazioni dei dati, sono poi sottoposti al DGE per le ulteriori analisi, in concomitanza delle attività di riesame della direzione (vedi procedura **PR 9.3 Modalità di definizione delle politiche e degli obiettivi aziendali e gestione dei riesami**)

La procedura di riferimento per la gestione dell'analisi dei dati è la **PR 9.1 – MONITORAGGI, ANALISI DEI DATI E TECNICHE STATISTICHE**.

9.2 Audit Interni

Mater scarl esegue audit di prima parte programmati al fine di monitorare il SGSD, per verificare che esso sia attuato conformemente alle norme di riferimento ed alla politica aziendale, nonché risulti efficacemente attuato e mantenuto aggiornato per il raggiungimento degli obiettivi

definiti dalla Direzione nonché valutare la conformità o meno delle attività di gestione ai Programmi di Sicurezza della Informazioni e la relativa efficacia di applicazione.

La funzione RSGSD pianifica gli Audit di prima parte in funzione della criticità delle aree aziendali, delle anomalie riscontrate nell'area, di eventuali reclami ricevuti dai Clienti in tema di Sicurezza delle informazioni.

Tutte le funzioni aziendali sono comunque sottoposte a verifica almeno una volta l'anno.

Per la conduzione degli Audit di prima parte, RSGSD può avvalersi di "Liste di Riscontro" che permettono di non omettere alcun punto di verifica e registrare le evidenze oggettive trovate. La "Lista di Riscontro" debitamente compilata, oppure il report finale, sono firmati dai partecipanti alla verifica ispettiva (valutatori e valutati) per accettazione dei risultati della verifica stessa.

Sono stabiliti i criteri, l'estensione, la frequenza e le modalità degli Audit di prima parte. I risultati delle verifiche ispettive sono documentate tramite apposite registrazioni che vengono comunicate alle funzioni verificate. A fronte delle carenze riscontrate sono prontamente intrapresi adeguati provvedimenti correttivi secondo la procedura **PR 9.2 – Gestione degli Audit**.

L'attuazione e l'efficacia delle azioni intraprese è accertata nelle successive verifiche ispettive ed opportunamente registrata.

La scelta dei Valutatori e la conduzione delle Verifiche Ispettive assicurano l'obiettività e l'imparzialità del processo di Audit di prima parte nonché la competenza.

I Valutatori non effettuano Audit di prima parte sul proprio lavoro.

9.3 Riesame della Direzione

Il SGSD viene riesaminato periodicamente per garantirne l'idoneità, l'adeguatezza e l'efficacia nel tempo. Oggetto del riesame è anche la valutazione della necessità di cambiamenti del sistema dell'organizzazione, incluse la politica e gli obiettivi. Il riesame del SGSD avviene, di norma, con periodicità almeno annuale.

Durante il Riesame vengono esaminati i seguenti elementi attinenti alla Sicurezza delle informazioni:

- i risultati delle verifiche ispettive interne e delle valutazioni sul rispetto delle prescrizioni legali e eventuali prescrizioni sottoscritte dalla Mater scarl
- il monitoraggio delle prestazioni e il grado di raggiungimento degli obiettivi e traguardi;
- la valutazione dei rischi ed il relativo piano dei trattamenti;

- lo stato delle azioni preventive e correttive;
- le azioni susseguenti ai precedenti riesami da parte della direzione;
- le raccomandazioni per il miglioramento;
- le circostanze derivanti da cambiamenti, comprese le modifiche alle prescrizioni legali e eventuali prescrizioni sottoscritte dalla [NOME_AZIENDA];
- lo stato delle attività relative alla gestione delle risorse;
- le comunicazioni provenienti dalle parti interessate, compresi gli eventuali reclami del Cliente;
- le comunicazioni pertinenti da parti interessate interne all'organizzazione, compresi i reclami;
- progresso nell'attuazione dei programmi di formazione.

L'oggetto del Riesame viene formalizzato in un apposito Verbale (si veda la procedura **PR 9.3 Modalità di definizione delle politiche e degli obiettivi aziendali e gestione dei riesami**) i cui contenuti sintetizzano la convocazione della riunione, i partecipanti, i documenti di input considerati, gli argomenti trattati e le azioni decise.

In tale verbale vengono discussi i seguenti punti:

- a) Lo stato delle azioni derivanti dai precedenti riesami della Direzione;
- b) I cambiamenti dei fattori esterni ed interni che hanno attinenza con il sistema di gestione per la sicurezza delle informazioni;
- c) Le informazioni di ritorno sulle prestazioni relative alla sicurezza delle informazioni compresi gli andamenti:
 1. Delle non conformità e azioni correttive;
 2. Dei risultati del monitoraggio e della misurazione;
 3. Dei risultati degli audit;
 4. Del raggiungimento degli obiettivi per la sicurezza delle informazioni;
- d) Le informazioni di ritorno dalle parti interessate;
- e) I risultati della valutazione del rischio e lo stato del piano di trattamento del rischio;
- f) Le opportunità per il miglioramento continuo.

Gli elementi in uscita dal riesame comprendono decisioni relative a:

1. Opportunità per il miglioramento continuo;
2. Ogni necessità di modifiche al sistema di gestione della sicurezza delle informazioni.

Tra le opportunità relative al miglioramento continuo si individuano:

- necessità di nuovi audit di prima parte e di eventuali audit di seconda parte sui fornitori più critici;
- necessità di adottare opportune Azioni Correttive/Preventive;
- necessità di nuove risorse e piani di formazione;
- revisione degli obiettivi di miglioramento del SGSD.

Il verbale di riesame e gli obiettivi di miglioramento vengono presentati in un incontro tra la Direzione e le funzioni interessate al fine di esporne i contenuti. Nel corso di tale incontro possono essere effettuate modifiche agli obiettivi purché approvate dalla Direzione.

Il Verbale di Riesame costituisce una registrazione del sistema.

La procedura di riferimento è la **PR 9.3 Modalità di definizione delle politiche e degli obiettivi aziendali e gestione dei riesami.**

10 MIGLIORAMENTO

10.1 Non Conformità e Azioni Correttive

Quando si verifica una non conformità, comprese quelle che emergono dai reclami, l'azienda è organizzata per:

a) reagire alla non conformità e, per quanto applicabile:

- 1) intraprendere azioni per tenerla sotto controllo e correggerla;
- 2) affrontarne le conseguenze;

b) valutare l'esigenza di azioni per eliminare la(e) causa(e) della non conformità, in modo che non si ripeta o non si verifichi altrove:

- 1) riesaminando e analizzando la non conformità;
- 2) determinando le cause della non conformità;
- 3) determinando se esistono o potrebbero verificarsi non conformità simili;

c) attuare ogni azione necessaria;

d) riesaminare l'efficacia di ogni azione correttiva intrapresa;

e) aggiornare, se necessario, i rischi e le opportunità determinati nel corso della pianificazione;

f) effettuare, se necessario, modifiche al sistema di gestione per la sicurezza delle informazioni.

In caso di non conformità, l'azienda stabilisce se e quale azione correttiva o preventiva sia necessaria per eliminare le cause della Non Conformità.

Ogni Azione Correttiva può essere intrapresa a seguito di:

1. emissione di uno o una serie di Rapporti di Non Conformità;
2. Reclami e Proteste dei clienti e del personale interno;
3. risultati di Audit di prima parte o Visite Ispettive da parte di Clienti;
4. risultati di Verifiche Ispettive da parte di Organismi di Certificazione;
5. Riesami della Direzione;
6. Segnalazione da parte di terze parti;
7. Attacchi esterni sui sistemi;
8. Eventi incidentali che impattano sui sistemi informativi;
9. Bug che si riscontrano sui software in produzione.

E' compito di DGE, in seguito agli "input" descritti sopra, valutare e stabilire le necessità relative alla delibera di un'Azione Correttiva, analizzarne le cause e stabilire le modalità di attuazione, le responsabilità coinvolte per l'esecuzione, il termine dell'azione correttiva.

Il Responsabile dell'Area interessata all'Azione Correttiva ha il compito di eseguire o di far eseguire al personale interessato le azioni necessarie e deliberate, verificandone la corretta attuazione nei tempi stabiliti.

Ogni Azione Correttiva deve correggere efficacemente le cause di Non Conformità o di anomalia che l'hanno generata.

La corretta esecuzione di un'Azione Correttiva e la valutazione dell'efficacia della stessa sono verificate al termine dei tempi indicati per l'attuazione. Valutati i risultati, RSGSD chiude l'azione eseguita.

Nel caso in cui azioni correttive coinvolgano fornitori nella loro attuazione, questi vengono informati dell'inconveniente riscontrato mediante trasmissione di apposito modulo. Viene quindi chiesto al fornitore di comunicare l'azione correttiva che intende attuare e le relative tempistiche.

Tutte queste attività sono registrate in appositi documenti.

In concomitanza dei Riesami della Direzione, RSGSD raccoglie le Azioni Correttive di periodo e le sottopone all'attenzione della Direzione (vedi **PR 9.3 - Modalità di definizione delle politiche e degli obiettivi aziendali e gestione dei riesami**).

La procedura di riferimento per la gestione delle Azioni Correttive è la procedura **PR 10.1 – Gestione Non Conformità e Reclami Cliente**.

Le Azioni Preventive scaturiscono dalle attività di riesame da parte della direzione, in seguito a valutazioni di risultati, riepiloghi analitici provenienti dalle diverse aree aziendali, in relazione a potenziali cause di non conformità.

E' compito di DGE gestire le attività di definizione delle Azione Preventive, individuandone le cause, e stabilire le modalità di attuazione, le responsabilità coinvolte per l'esecuzione e i termini temporali.

Ogni Azione Preventiva deve quindi essere intrapresa nei tempi stabiliti dal responsabile incaricato dell'esecuzione.

Al termine dei tempi previsti per la sua attuazione, l'azione effettuata è riesaminata dal DGE che ne valutano i risultati in ordine agli obiettivi che ci si erano posti.

Queste attività sono tutte registrate in appositi documenti, che vengono poi consegnati a RSGSD. In concomitanza dei Riesami della Direzione, RSGSD raccoglie le Azioni Preventive di periodo e le sottopone all'attenzione della Direzione (vedi **PR 9.3 Modalità di definizione delle politiche e degli obiettivi aziendali e gestione dei riesami**).

La procedura di riferimento per la gestione delle Azioni Preventive è la procedura **PR 10.1 – Gestione Non Conformità e Reclami Cliente**.

10.2 Miglioramento Continuo

Il vertice aziendale, nella persona del DGE, in coerenza con la missione e la politica aziendale ha la responsabilità di pianificare e gestire i processi necessari per il miglioramento continuo del sistema di gestione per la sicurezza delle informazioni; si struttura quindi un sistema di gestione delle azioni di miglioramento.

Le Azioni di miglioramento adottate dall'organizzazione sono costituite da Azioni Correttive (AC) ed Azioni Preventive (AP) che vengono attuate per migliorare e risolvere Non Conformità, prassi aziendali errate e/o non coerenti, anche potenzialmente, con la politica e gli obiettivi definiti dal vertice, per adeguarsi a segnalazioni e tendenze in arrivo dal mercato.

Le Azioni Correttive hanno un'ottica reattiva di risposta e risoluzione ad anomalie e non conformità in generale, mentre le Azioni Preventive consentono di agire in maniera proattiva, prima che si verifichino eventi potenzialmente problematici.

Caratteristica di entrambe, che le contraddistingue dalle azioni di correzione delle non conformità che si concentrano sull'eliminazione dell'effetto indesiderato, è che esse si concentrano, in maniera appropriata, sulle cause delle situazioni anomale o potenzialmente anomale al fine di prevenirne il loro ripetersi.

Gli strumenti e i supporti da utilizzare per l'attività di gestione del miglioramento sono la politica per la sicurezza delle informazioni e gli obiettivi formalizzati e misurabili, le registrazioni relative ai risultati delle verifiche ispettive interne, le registrazioni riferite all'analisi dei dati, le registrazioni circa la gestione delle non conformità e la gestione delle azioni correttive e preventive e i verbali di registrazione dei riesami della direzione.

La procedura di riferimento è la **PR 10.2 – Azioni di Miglioramento**.