SISTEMA di GESTIONE della SICUREZZA delle INFORMAZIONI (SGSI)

Information Security Policy

POLI01PUB

In ottemperanza allo Standard Internazionale ISO/IEC 27001, il presente documento è classificato con il livello USO PUBBLICO.

Elenco delle revisioni

REV	DATA	REDATTORE	BREVE DESCRIZIONE
00	04/04/2019		Prima emissione
01	02/04/2021		
02	02/03/2022		Versione uso pubblico

Indice

1. Scopo e campo di applicazione 5
2. Ruoli e responsabilità per la sicurezza informazioni 5
2.1 Comitato SGSI 6
2.2 Separazione dei compiti 6
3. Sicurezza nei comportamenti del personale 6
3.1 Competenze e formazione sulla sicurezza delle informazioni 7
3.2 Accordo di riservatezza 7
3.3 Utilizzo dei beni informatici 7
3.4 Teleworking e Smartworking 7
3.5 Clear desk 8
4. Gestione e protezione degli asset 8
4.1 Classificazione e protezione delle informazioni 8
4.2 Trasferimento e condivisione di informazioni verso aziende terze 9
4.3 Supporti di memorizzazione e dispositivi mobili 9
5. Sicurezza fisica 10
6. Controllo accessi logici 10
7. Gestione dei sistemi informativi 11
8. Sviluppo e manutenzione del software 11
8.1 Change Management Applicativo 11
8.2 Requisiti di sicurezza 12
8.3 Gestione della configurazione 12
8.4 Protezione del codice sorgente e degli ambienti di sviluppo 12
8.5 Dati di test 12
9. Gestione degli incidenti e dei problemi 12
10. Gestione della Business Continuity 13

11. Gestione dei fornitori 14
12. Compliance e Audit 14

1. Scopo e campo di applicazione

La presente Information Security Policy è stata predisposta nel rispetto dei requisiti dello standard internazionale ISO 27001 e rappresenta il quadro di riferimento dei principi, delle linee guida e delle regole che devono essere adottate per la sicurezza del patrimonio informativo di s.d.i. s.p.a.
I principi, le linee guida e le regole qui riportate sono di natura generale, dedicate ai vari aspetti della sicurezza delle informazioni e articolate secondo la struttura suggerita dallo standard internazionale ISO 27001 e delle "buone pratiche" a esso correlate. In particolare:

- Standard ISO/IEC 27001 - Information security management systems;
- Standard ISO/IEC 27002 - Code of practice for information security controls;

E per il processo di analisi dei rischi:

- Standard ISO/IEC 27005 - Information security risk management;
- Standard ISO/IEC 31000 – Risk management principles and guidelines;

Finalità specifiche del presente documento sono:

- Stabilire la normativa generale e i principi base per la corretta gestione e protezione delle informazioni e dei beni informatici dell'Azienda;
- Adempiere agli obblighi imposti dalle leggi in tema di sicurezza delle informazioni;
- Fornire una base comune di linee guida e regole per lo sviluppo e l'attuazione delle procedure operative per la gestione della sicurezza delle informazioni;
- Definire ruoli e responsabilità, generali e specifiche, per tutti gli aspetti legati alla sicurezza delle informazioni e dei beni informatici dell'Azienda.

La Information Security Policy è destinata ai dipendenti s.d.i. s.p.a. e a tutti gli stakeholders interessati (es. Clienti, Fornitori e altre Parti terze).
L'ambito di applicazione della Information Security Policy coincide con il perimetro del Sistema di Gestione della Sicurezza delle Informazioni. La rivisitazione del presente documento è prevista con cadenza almeno annuale e comunque, in occasione di variazioni significative di elementi che hanno impatti sul Sistema di Gestione della Sicurezza delle Informazioni e sulla sicurezza delle informazioni in azienda, al fine di garantirne l'adeguatezza rispetto al contesto.

2. Ruoli e responsabilità per la sicurezza informazioni

s.d.i. s.p.a., in relazione alla struttura organizzativa aziendale e conformemente alle dimensioni interfunzionali della sicurezza delle informazioni, ha individuato i seguenti ruoli per la gestione del Sistema di Gestione della Sicurezza delle Informazioni (SGSI):

- Responsabile SGSI (Direttore Tecnico);
- Coordinatore SGSI (Responsabile ICT);
- Comitato SGSI.

A integrazione dei ruoli e degli organi in precedenza citati, l'organizzazione del Sistema di Gestione della Sicurezza delle Informazioni prevede inoltre le seguenti figure:

- Responsabile Sicurezza Fisica (Responsabile Servizi Generali);
- Responsabile Sicurezza Logica (Responsabile ICT).

2.1 Comitato SGSI

Il Comitato SGSI è costituito dai seguenti membri permanenti:

- Responsabile SGSI (presiede il Comitato SGSI);
- Coordinatore SGSI;
- Responsabile Sicurezza Fisica;
- Responsabile Sicurezza Logica,
- Responsabile Qualità e HSE
- Eventuali altre Funzioni, coinvolte se necessario, aventi ruolo nella sicurezza delle informazioni e/o professionisti esterni, a supporto del Responsabile Information Security per le attività necessarie all'impostazione, mantenimento e miglioramento continuo del Sistema di Gestione della Sicurezza delle Informazioni.

È prevista per il Comitato SGSI una frequenza di convocazione almeno semestrale. Le riunioni del Comitato SGSI sono precedute da un ordine del giorno e sono verbalizzate.

2.2 Separazione dei compiti

s.d.i. s.p.a. applica il principio della separazione dei compiti e delle responsabilità ove appropriato, in modo da ridurre il rischio di negligenze o di un uso improprio dei sistemi. Tale principio deve essere attuato quando opportuno, tenendo conto delle specificità della situazione aziendale, in modo da ridurre le possibilità per una persona di effettuare modifiche non autorizzate o di utilizzare irregolarmente dati e/o servizi aziendali.

3. Sicurezza nei comportamenti del personale

Tutti i dipendenti, i collaboratori e le Parti terze coinvolte, sono responsabili della tutela delle informazioni della strumentazione informatica di proprietà di s.d.i. s.p.a. a essi affidata.
I dipendenti, i collaboratori e le Parti terze devono applicare le policies, le regole e le procedure aziendali in tema di sicurezza delle informazioni, per quanto di rispettiva competenza.
Il management di s.d.i. s.p.a. si impegna inoltre a:

- Richiedere il rispetto delle policies, delle regole e delle procedure del Sistema di Gestione della Sicurezza delle Informazioni da parte dei dipendenti, dei collaboratori e delle Parti terze coinvolte;
- Favorire in azienda la diffusione della cultura della sicurezza delle informazioni mediante la conoscenza e l'adozione della presente policy e di tutte le regole del Sistema di Gestione della Sicurezza delle Informazioni da parte dei dipendenti, dei collaboratori e delle Parti terze coinvolte;
- Supportare gli organi di gestione del Sistema di Gestione della Sicurezza delle Informazioni nelle fasi di valutazione dei rischi e individuazione di soluzioni adeguate nella propria area di competenza;

- Attuare, nel rispetto dell'ambito di propria competenza, le azioni di mitigazione del rischio approvate nel rispetto della pianificazione definita.

3.1 Competenze e formazione sulla sicurezza delle informazioni

s.d.i. s.p.a. assicura l'opportuna formazione, informazione e sensibilizzazione dei dipendenti, e dei collaboratori ove necessario, per garantire l'acquisizione delle conoscenze necessarie per mantenere la sicurezza del patrimonio aziendale (beni e informazioni) nell'esercizio delle mansioni ad essi affidate.
Il management di s.d.i. s.p.a. s'impegna affinché:

- Sia garantito l'appropriato livello di competenza dei singoli dipendenti in tema di sicurezza delle informazioni, rispetto alle specificità delle mansioni assegnate;
- Siano promosse le opportune azioni di miglioramento di tali competenze, in condivisione con Responsabile SGSI.

3.2 Accordo di riservatezza

Tutti i soggetti che entrano in possesso di dati e informazioni di s.d.i. s.p.a. e del suo business sono tenuti a mantenere la massima riservatezza, come richiesto dalle regole e dalle procedure aziendali:

- I dipendenti, firmando, all'inizio del rapporto di lavoro, l"Accordo relativo a Informazioni confidenziali, proprietà industriale, intellettuale e beni materiali".
- le Parti Terze, quando ritenuto opportuno, firmando contratti che comprendono le condizioni sulla riservatezza "Non-Disclosure Agreement" ed eventualmente anche "Confidentiality and Non-Competition Agreement".

Le eventuali forme di collaborazione con s.d.i. s.p.a. non incluse nelle casistiche già citate devono comunque sottostare alle regole di riservatezza.

3.3 Utilizzo dei beni informatici

L'utilizzo dei beni e dei sistemi informatici, così come il trattamento dei dati e delle informazioni aziendali, deve avvenire per soli scopi lavorativi. Pertanto, ogni uso dei beni, sistemi, dati e informazioni s.d.i. s.p.a. che non sia per tali scopi, può essere considerato come improprio, a meno che non sia stato esplicitamente autorizzato dal management di s.d.i. s.p.a. Tutti i dipendenti e collaboratori di s.d.i. s.p.a. sono responsabili della tutela dei beni e degli strumenti informatici a loro affidati, nel rispetto delle regole aziendali. L'utilizzo del personal computer, della rete, dei supporti, dei notebook, dei dispositivi mobili, della posta elettronica e di internet, sono specificamente regolamentati.

3.4 Teleworking e Smartworking

È possibile il collegamento alla rete aziendale e lo svolgimento dell'attività lavorativa da remoto. Gli accessi da ubicazioni differenti dalle sedi aziendali sono protetti tramite connessione sicura (es. VPN).

3.5 Clear desk

Ai fini della sicurezza delle informazioni aziendali, tutti i dipendenti e collaboratori s.d.i. s.p.a. adottano una modalità di “scrivania sgombra”, per ridurre il rischio di accessi non autorizzati:

- Ai dati aziendali contenuti nel proprio PC (o altri dispositivi), attraverso l’applicazione di uno screen saver temporizzato dotato di blocco automatico con richiesta di password per l’accesso;
- Ai documenti classificati come “riservati” o “confidenziali” che si trovano nel proprio ufficio, attraverso l’utilizzo di cassetti e armadi con chiave.

Analoga attenzione è posta nell’uso di aree comuni (es. sale riunioni) e dei dispositivi condivisi (es. stampanti, fotocopiatrici).

4. Gestione e protezione degli asset

Al fine di garantire il livello adeguato di protezione delle informazioni, tutto il patrimonio informativo aziendale è catalogato e gestito da un tool di asset management.
Ciascun asset (informatico o di produzione) è inventariato ed è attribuito ad una Funzione aziendale.
Il Responsabile della Funzione definisce le misure di sicurezza appropriate per la protezione degli asset di sua competenza. L’assegnatario è tenuto all’applicazione delle misure di sicurezza definite dal Responsabile della Funzione.

4.1 Classificazione e protezione delle informazioni

s.d.i. s.p.a. adotta la classificazione delle informazioni, con particolare riferimento ai documenti elettronici e cartacei presenti in azienda, sulla base della loro criticità in termini di riservatezza, integrità e disponibilità.
Il trattamento delle informazioni deve avvenire in coerenza con le regole definite nella presente Information Security Policy.
La classificazione di tutte le pagine dei documenti prodotti internamente deve essere eseguita dall’autore apponendo relativa etichetta del livello di classificazione, in particolare:

- USO INTERNO
- Confidenziale;
- Altamente confidenziale.

In tal modo si intende che i documenti che non presentano l’etichetta con il livello di classificazione sono da considerarsi “Non classificati” e quindi accessibili a tutti indistintamente, sia all’interno che all’esterno dell’azienda.
I documenti presenti in Azienda ma non prodotti internamente, quindi non etichettabili, devono essere comunque classificati e sottostare alle modalità di gestione indicate precedentemente, in funzione della criticità dei contenuti.

4.2 Trasferimento e condivisione di informazioni verso aziende terze

s.d.i. ha definito le regole per la condivisione di documenti contenenti informazioni aziendali con aziende terze. Tali regole tengono in considerazione la criticità delle informazioni di business oggetto di condivisione.

I documenti condivisi con aziende terze classificati, Altamente Confidenziale s.d.i., Confidenziale s.d.i., devono indicare anche il nome dell'azienda con la quale è condivisa la documentazione in oggetto (es. Classificazione: Altamente Confidenziale s.d.i. - Fornitore XY / Classificazione: Confidenziale s.d.i. – Cliente YZ).

Inoltre, in ogni documento condiviso con aziende terze deve essere riportato, a seconda dei casi, il seguente passaggio:

Livello di Classificazione: Altamente Confidenziale / Confidenziale

In ottemperanza allo Standard Internazionale ISO/IEC 27001, i dati e le informazioni contenute in tutte le pagine del presente documento sono classificate con il livello Altamente Confidenziale/Confidenziale/USO INTERNO s.d.i.-[NOME DEL CLIENTE/FORNITORE].

Onde evitare accessi non autorizzati alle informazioni condivise Vi preghiamo di attenerVi ad una scrupolosa gestione del documento.

*In caso di diffusione non autorizzata delle informazioni (avvenuta o sospetta), deve essere data **tempestiva comunicazione** alla Direzione s.d.i.*

I documenti condivisi con aziende terze classificati come USO INTERNO s.d.i. conterranno invece la seguente dicitura:

Livello di Classificazione: Uso Interno s.d.i.

In ottemperanza allo Standard Internazionale ISO/IEC 27001, il presente documento è classificato con il livello USO INTERNO SDI; pertanto non può essere da Terzi riprodotto, alterato o divulgato.

4.3 Supporti di memorizzazione e dispositivi mobili

E' definito un processo per la gestione, l'assegnazione, la sostituzione e la distruzione dei PC, dei computer portatili, dei dispositivi removibili, degli smartphone e di ogni dispositivo che possa contenere dati al fine di evitare l'uso improprio degli stessi e l'eventuale divulgazione non autorizzata di informazioni. I supporti di memorizzazione non più in uso devono essere conservati, eliminati o distrutti in maniera sicura (es. formattazione di basso livello).
La movimentazione di supporti contenenti dati deve avvenire in modo controllato per evitare l'accesso non autorizzato o la manomissione delle informazioni in essi contenuti.
I dispositivi mobili devono essere adeguatamente protetti da accessi non autorizzati. In particolare i supporti removibili devono essere crittografati. La assegnazione dei dispositivi è censita all'interno di un apposito registro: tali dispositivi devono essere custoditi dagli assegnatari con la massima diligenza per evitare la perdita di informazioni.

5. Sicurezza fisica

Sono individuate ed applicate specifiche ed adeguate misure per garantire la sicurezza fisica, tra cui:

- Controllo fisico degli accessi (es. controllo degli ingressi da parte della reception, registro ingressi, controllo passo carrabile, ecc.);
- Sistemi antintrusione e sistema di videosorveglianza;
- Impianti di alimentazione elettrica protetti (es. cabine elettriche, cablaggi, UPS, ecc.);
- Sistemi antincendio (es. estintori, rilevazione fumi, ecc.).
- Ridondanza dati su Server fisicamente ubicati in edifici separati e protetti da eventi naturali o accidentali (es. incendi).
- Ridondanza della rete dati (Connessione in fibra ottica ridondata in rame con differenti percorsi verso il gestore).

L'individuazione delle misure da applicare si basa sulla valutazione della criticità delle risorse da proteggere. È assicurata la corretta e periodica manutenzione degli impianti per garantire il loro funzionamento ottimale ed il rispetto delle prescrizioni di legge. L'individuazione e la gestione delle misure di sicurezza fisica, così come la loro documentazione tecnica, è assicurata dal Responsabile della Sicurezza Fisica, con l'eventuale collaborazione del Responsabile della Sicurezza Logica.

6. Controllo accessi logici

s.d.i. s.p.a. adotta procedure formali per controllare la distribuzione dei diritti di accesso ai sistemi informativi aziendali e per la gestione degli account utente, in tutte le fasi del loro "ciclo di vita": dalla creazione dell'account utente, alla sua modifica, aggiornamento, eliminazione.
I diritti di accesso alle reti, ai sistemi, alle applicazioni, ai dati e alle informazioni aziendali sono definiti in base al ruolo, alle mansioni svolte e alle effettive necessità lavorative (criterio del "need to know").
I diritti di accesso con profilo di amministrazione dei sistemi, delle reti e dei database, sono limitati e controllati e, ove applicabile anche rispetto alle normative vigenti (Provvedimento del Garante della Privacy sugli Amministratori di Sistema). Le utenze e i profili di accesso ai sistemi sono periodicamente controllati per verificarne l'adeguatezza nel tempo e per sanare eventuali situazioni non conformi.
La metodologia utilizzata da s.d.i. s.p.a. per l'autenticazione di ciascun utente che accede ai sistemi informatici è commisurata alla criticità dei dati contenuti nei sistemi, in base a cui deve essere valutata l'opportunità di utilizzo di metodi di autenticazione più vincolanti (es. strong authentication).
Di norma è utilizzata la combinazione di user-ID e password ed è garantita la robustezza delle credenziali segrete di autenticazione mediante il rispetto di criteri di lunghezza, composizione e scadenza periodica.
E' definito e attuato un processo che garantisca la tempestiva disattivazione delle utenze non più autorizzate ad accedere ai sistemi e alle informazioni di s.d.i. s.p.a.
L'individuazione e la gestione delle misure di sicurezza logica, così come la loro documentazione tecnica, è assicurata dal Responsabile della Sicurezza Logica.

Per gli accessi da remoto alla rete aziendale sono utilizzate connessioni VPN criptate con accesso tramite autenticazione dell'utente e MFA basata sul possesso del proprio cellulare. Lo stesso livello di autenticazione con MFA è previsto per l'accesso ai servizi cloud.

7. Gestione dei sistemi informativi

Al fine di garantire la gestione in sicurezza di tutti i sistemi e infrastrutture aziendali, è necessario che siano documentate le regole e le responsabilità in merito a:

- Installazione del software nei Server, nei PC e negli altri dispositivi aziendali;
- Adeguamento della capacità delle risorse computazionali;
- Gestione delle vulnerabilità tecniche e relative patch;
- Gestione delle minacce alla sicurezza (Security Threats Management);
- Backup dei sistemi;
- Raccolta e protezione dei LOG;
- Gestione delle comunicazioni elettroniche e cartacee;
- Trasmissione dei dati;
- Crittografia dei dati, delle trasmissioni e comunicazioni nei casi previsti..

8. Sviluppo e manutenzione del software

I processi di sviluppo e manutenzione del software devono essere opportunamente regolamentati, documentati e gestiti, non solo nell'intento di perseguire la massima qualità di servizio, efficacia e efficienza operativa, ma anche nell'ottica di garantire che il software rispetti i requisiti di sicurezza necessari.

8.1 Change Management Applicativo

Le modalità e le responsabilità di gestione delle attività che riguardano lo sviluppo e la manutenzione del software sono dettagliate in specifiche procedure. ~~In particolare:~~
Lungo tutto il processo di change del software deve essere tracciata e controllata l'applicazione dei requisiti di sicurezza definiti. Il software deve essere testato. I test devono accertare il funzionamento regolare delle funzioni di sicurezza e l'assenza di vulnerabilità.
Inoltre, deve essere realizzata la separazione degli ambienti di sviluppo, test (eventualmente, di integrazione) e produzione, anche attraverso la differenziazione dei privilegi di accesso ai diversi ambienti, ove necessario.
Nel caso di servizi di sviluppo/manutenzione software affidati a terzi, devono essere utilizzate le stesse modalità di gestione dello sviluppo/manutenzione ed applicati requisiti di sicurezza del software analogamente a quanto fatto per gli sviluppi interni
In caso di sviluppi effettuati da Parti terze, devono inoltre essere definiti i criteri di accettazione del software.

8.2 Requisiti di sicurezza

I requisiti di sicurezza relativi allo sviluppo software e alle modifiche ai sistemi devono essere definiti già nelle fasi iniziali dei progetti e documentati.

8.3 Gestione della configurazione

Deve essere gestita la conservazione ed il versionamento del software per tenere traccia del livello di aggiornamento dei sistemi e delle applicazioni installate nei vari ambienti. Le precedenti versioni del software devono essere conservate come misura preventiva in caso di malfunzionamento della nuova versione.

8.4 Protezione del codice sorgente e degli ambienti di sviluppo

Il codice sorgente dei programmi deve essere conservato e protetto da accessi non autorizzati e perdite accidentali. L'accesso al codice sorgente e agli ambienti di sviluppo deve essere limitato alle sole persone incaricate delle modifiche alle applicazioni, secondo il principio del "need to know".

8.5 Dati di test

I dati di test devono essere protetti qualora essi siano copie complete o parziali dei dati di produzione o nel caso siano critici. Per tale ragione l'accesso agli ambienti di sviluppo deve essere controllato e limitato, in particolare se essi sono accessibili da terze parti.

9. Gestione degli incidenti e dei problemi

Gli incidenti devono essere gestiti tempestivamente e appropriatamente, al fine di minimizzare danni ulteriori e di ripristinare al più presto e in modo ottimale le normali condizioni operative.
In particolare, è necessario individuati gli incidenti di sicurezza che possono mettere a repentaglio la riservatezza, l'integrità e la disponibilità delle informazioni. Per questo deve essere definito, documentato ed adottato un processo per la gestione degli incidenti che preveda almeno:

- La classificazione degli incidenti in base alla loro priorità;
- La registrazione degli incidenti;
- Opportune modalità di gestione in relazione alla classificazione;
- L'individuazione dei responsabili della risoluzione degli incidenti;
- I riferimenti per l'eventuale escalation;
- L'analisi delle problematiche segnalate;
- L'uso di uno strumento per la tracciatura degli incidenti;
- La predisposizione di opportuna reportistica;

- Il riesame periodico degli incidenti principali.

Tutti i dipendenti e le Parti terze sono tenuti a segnalare gli incidenti relativi alla sicurezza delle informazioni s.d.i. s.p.a. tramite i canali e gli strumenti adottati in azienda.

10. Gestione della Business Continuity

Devono essere adottate strategie e piani per la continuità operativa e della sicurezza che tengano conto:

- Dei servizi aziendali valutati critici per il business;
- Dei requisiti minimi di ripristino;
- Dei principali scenari incidentali derivati dalle best practices internazionali;
- Degli impatti dei suddetti scenari sull'azienda e dei conseguenti livelli di rischio.

Il Responsabile SGSI deve assicurare la definizione e l'aggiornamento:

- Dell'elenco dei servizi critici;
- Dei requisiti minimi di ripristino;
- Degli scenari di rischio;
- Degli impatti sull'azienda;
- Delle strategie di ripristino;
- Dei piani e delle procedure di continuità;
- Delle misure che consentono la ripresa del servizio.

Inoltre, il Responsabile SGSI si impegna per garantire:

- La diffusione, all'interno e all'esterno dell'azienda (per quanto necessario), dei piani e delle procedure da adottare per assicurare la continuità del business;
- L'adeguatezza degli accordi contrattuali con i Fornitori in merito alla gestione (tempi e modi) delle situazioni di disastro, a seconda del loro coinvolgimento nell'erogazione di servizi critici;
- L'esistenza, l'aggiornamento ed il test periodico dei piani di continuità operativa e le relative responsabilità per la gestione della reazione all'incidente e il rispristino del servizio secondo i requisiti minimi definiti, da condividere tra tutte le funzioni coinvolte;
- L'adeguatezza delle soluzioni per la continuità operativa (es. ridondanze dei sistemi, resilienza degli impianti, disponibilità di sedi alternative, distribuzione delle competenze critiche, ecc.)

I requisiti di sicurezza informazioni da applicare nelle situazioni di crisi/disastro (es. autorizzazioni all'accesso dei dati, etc.) sono gli stessi che valgono durante la normale operatività.
Analogamente, anche i ruoli e le responsabilità definiti e assegnati per la gestione della sicurezza informazioni durante la normale operatività sono gli stessi che garantiscono la continuità della gestione della sicurezza informazioni anche durante le situazioni di crisi/disastro.

11. Gestione dei fornitori

Il livello di sicurezza garantito dalle Parti terze (es. Fornitori IT, outsourcers, partners, ecc.) deve essere conforme al livello di sicurezza applicato da s.d.i. s.p.a., per evitare che i prodotti/servizi acquisiti dall'esterno costituiscano un elemento di debolezza per la sicurezza delle informazioni.
Deve essere svolta, in via preventiva una valutazione dei rischi delle Parti terze e devono essere definite e inserite nel contratto le responsabilità, le condizioni specifiche, i requisiti di sicurezza e gli SLA (coerenti con le valutazioni di rischio) che le Parti terze sono tenute a rispettare, in particolare nel caso di fornitori/outsourcers ICT.

12. Compliance e Audit

s.d.i. s.p.a. opera nel rispetto delle leggi nazionali e internazionali applicabili, dei regolamenti interni, delle normative volontarie adottate, dei contratti con le controparti esterne. Inoltre, s.d.i. s.p.a. garantisce l'adeguata disponibilità di documentazione e di risorse per consentire le attività degli Auditor interni ed esterni.

Le norme adottate aziendalmente da s.d.i. s.p.a. sono:

- UNI EN ISO 9001
- UNI EN ISO 14001
- ISO/IEC 27001
- BS OHSAS 18001.

Le norme relative alla Cyber Security di riferimento nello sviluppo dei prodotti s.d.i. (sistemi SCADA e apparati di automazione e controllo) sono:

- IEC 62351
- IEC 62541
- IEC 61784-3
- IEC 62443

Vengono tenute inoltre in considerazione le norme:

- NIST SP 800-82
- NIST SP 800-53
- NIST SP 800-57

In particolare, per sistemi Functional Safety, viene adottata la normativa:

- IEC61508:2010

I principali riferimenti normativi cogenti corrispondono a:

- Normativa Privacy (Regolamento (UE) 679/2016 e Codice Privacy armonizzato con il Regolamento);
- Provvedimenti del Garante della Privacy applicabili all'Azienda~~, in particolare:~~
- D.Lgs 81/2008 (Testo Unico sulla Sicurezza sul Lavoro) e successive modificazioni;
- D.Lgs. 231/2001 (Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica) e successive modificazioni.

Oltre alle normative di cui sopra, per quanto riguarda specificatamente gli apparati elettronici prodotti ed i quadri elettrici forniti, i riferimenti sono:

- Marcatura CE: applicazione delle procedure per la verifica di conformità e realizzazione del prodotto munito della documentazione e manualistica necessaria, apposizione della marcatura CE nei casi previsti, predisposizione della dichiarazione di conformità previo superamento con esito positivo dei controlli e collaudi finali comprensivi delle prove funzionali e dei test elettrici condotti con le apposite apparecchiature certificate.
- Certificazione UL (cULus): marchio di certificazione volontario relativo agli standard di sicurezza dei prodotti, riconosciuto nel Nord America (Stati Uniti e Canada).

Per assicurare il recepimento degli aggiornamenti normativi, s.d.i. s.p.a. si avvale di professionalità interne esperte. All'occorrenza, s.d.i. s.p.a. si serve di consulenti esterni che supportano l'azienda su tematiche specifiche relative alla normativa di settore.

I Responsabili di Funzione di s.d.i. s.p.a. analizzano le implicazioni delle novità normative sull'area di propria pertinenza e ne assicurano l'applicazione per quanto di competenza.

Il Responsabile SGSI pianifica i controlli periodici interni per verificare il rispetto ed il corretto recepimento della presente policy e delle procedure del Sistema di Gestione della Sicurezza delle Informazioni, concordando l'eventuale necessità e la pianificazione di audit esterni con le Funzioni aziendali interessate.