

IS13

**Politica del Sistema di Gestione
della Sicurezza delle Informazioni**

Documento rif:	Politica SGSI IS13
Versione:	0
Data della versione:	02.01.2023
Autore:	Ermanno Girelli
Approvato da:	Francesco Crescini
Livello di riservatezza:	Copia controllata

LISTA DISTRIBUZIONE

La presente Politica SGSI è un documento controllato e viene mantenuto sul server in sola lettura. Il rappresentante per la gestione della sicurezza delle informazioni deve garantire che tutte le modifiche siano diffuse e che le copie obsolete siano rimosse e archiviate. Le copie cartacee utilizzate per l'addestramento e l'auditing interno sono controllate e distribuite come segue.

CRONOLOGIA MODIFICHE

Il presente documento viene riesaminato periodicamente, almeno una volta all'anno, e viene conservato per un periodo di cinque anni. Le modifiche e le revisioni sono distribuite ai titolari citati. La cronistoria delle modifiche e la questione delle revisioni sono riportate di seguito.

Data	Modificare. No.	Numero Pagine	Nuovo numero	Motivo del cambiamento	Autorizzato da
02.01.2023	-	7	0	Rilascio iniziale.	Francesco Crescini

Le copie di questo documento diverse da quelle elencate sopra non saranno rivedute; tali copie saranno contrassegnate come **NON CONTROLLATE**.

INTRODUZIONE

VCB Securitas SPA fornisce servizi e funzioni essenziali che si basano su risorse, incluse le informazioni. L'uso delle risorse informative deve essere in linea con le buone pratiche e procedure di lavoro professionali, nonché con i requisiti legali, normativi e contrattuali e deve garantire la riservatezza, l'integrità e la disponibilità di tutte le risorse informative aziendali.

L'informazione è un asset estremamente importante di VCB Securitas Spa e consente alla medesima di adempiere alle proprie funzioni e obblighi commerciali. ISO/IEC 27001:2017, lo standard internazionale di sicurezza per i sistemi di gestione della sicurezza delle informazioni, fornisce i requisiti obbligatori per l'implementazione, la revisione e il miglioramento continuo di un Sistema di Gestione della Sicurezza delle Informazioni (SGSI).

L'SGSI di VCB Securitas Spa garantisce che la stessa soddisfi i requisiti legali, regolamentari e contrattuali in materia di sicurezza delle informazioni, compresi quelli previsti dalla legge sulla protezione dei dati (Reg Ue 2016/679 e D.lgs 101/18).

Il sistema di gestione della sicurezza delle informazioni (SGSI) si applica al controllo delle attività, dei locali e delle risorse di VCB Securitas Spa.

SCOPO

Scopo del presente documento è quello di descrivere i principi generali di Sicurezza delle Informazioni definiti da VCB Securitas al fine di sviluppare un funzionale Sistema di Gestione per la Sicurezza delle Informazioni (SGSI).

CAMPO DI APPLICAZIONE

L'ambito di applicazione di questa politica si estende a tutti i dipartimenti di VCB Securitas Spa, dipendenti, appaltatori, fornitori e agenzie partner che utilizzano/accedono alle risorse informative di VCB Securitas Spa e che collaborano alla gestione delle informazioni ed a tutti i processi, alle risorse coinvolte nella progettazione, realizzazione, avviamento, erogazione, assistenza continuativa nell'ambito dei servizi erogati.

Il campo di applicazione è il seguente:

“Progettazione ed erogazione di servizi di vigilanza fissa, ispettiva, antirapina, telesorveglianza e televigilanza, intervento su allarmi, scorta valori e trasporto valori. Installazione, manutenzione e gestione degli impianti elettrici-elettronici (di allarme e videosorveglianza). Erogazione servizi di portierato, gestione accessi e gestione archivi”.

DICHIARAZIONE POLITICA

La Direzione di VCB SECURITAS ritiene importante il perseguimento da parte di tutta l’organizzazione aziendale degli obiettivi del proprio **Sistema di Gestione della Sicurezza delle Informazioni (SGSI)**, conformemente alla **norma UNI CEI ISO/IEC 27001**.

La gestione della sicurezza delle informazioni è un processo complesso che coinvolge le risorse umane delle unità organizzative all’interno del perimetro di certificazione, definito da VCB SECURITAS nel proprio Manuale per la Sicurezza delle Informazioni.

L’Organizzazione attua la Politica per la Qualità e Sicurezza delle Informazioni perseguendo i seguenti principi:

- adottare l’ISO 27001 come standard per l’implementazione del sistema di gestione della sicurezza dell’informazione e perseguirne la conformità;
- la centralità della figura del cliente e la sua piena soddisfazione anche in termini di Sicurezza delle informazioni trattate nell’ambito dei servizi offerti;
- sensibilizzare tutto il personale interno all’organizzazione ed i collaboratori circa i temi di sicurezza delle informazioni;
- accertare che i fornitori esterni e tutti gli stakeholders abbiano consapevolezza e rispettino la politica di sicurezza adottata da VCB SECURITAS;
- garantire le condizioni di sicurezza in ogni tipologia di attività o fase di trattamento dei dati personali e sensibili;
- garantire l’utilizzo di risorse e tecnologie adeguate.

OBIETTIVI

La Politica per la Sicurezza delle Informazioni di VCB Securitas si orienta ai seguenti obiettivi:

1. garantire all'organizzazione la piena conoscenza delle informazioni gestite e la valutazione della loro criticità, al fine di agevolare l'implementazione degli adeguati livelli di protezione;
2. garantire l'accesso sicuro alle informazioni, in modo da prevenire trattamenti non autorizzati o realizzati senza i diritti necessari;
3. garantire che l'organizzazione e le terze parti collaborino al trattamento delle informazioni adottando procedure volte al rispetto di adeguati livelli di sicurezza;
4. garantire che l'organizzazione e le terze parti che collaborano al trattamento delle informazioni abbiano piena consapevolezza delle problematiche relative alla sicurezza;
5. garantire che le anomalie e gli incidenti aventi ripercussioni sul sistema informativo e sui livelli di sicurezza aziendale siano tempestivamente riconosciuti e correttamente gestiti, attraverso efficienti sistemi di prevenzione, comunicazione e reazione al fine di minimizzare l'impatto sul business;
6. garantire che l'accesso alla sede operativa ed ai locali aziendali avvenga esclusivamente da parte di personale autorizzato, a garanzia della sicurezza delle aree e degli asset presenti;
7. garantire la conformità con i requisiti di legge ed il rispetto degli impegni di sicurezza stabiliti nei contratti con le terze parti;
8. garantire la rilevazione di eventi anomali, incidenti e vulnerabilità dei sistemi informativi al fine di rispettare la sicurezza e la disponibilità dei servizi e delle informazioni;
9. garantire la Continuità Operativa aziendale (Business Continuity) e il Disaster Recovery, attraverso l'applicazione di procedure di sicurezza stabilite.

IMPEGNO DI VCB SECURITAS

Per realizzare tali obiettivi VCB SECURITAS si impegna a:

- migliorare in modo continuo il sistema di gestione per la sicurezza e delle informazioni (SGSI);
- applicare e rispettare i requisiti di legge cogenti e ogni altro requisito/norma/regolamento significativo in ambito sicurezza dei dati e delle informazioni;

- conservare in modo sicuro le informazioni gestite e quindi prevenire gli eventi negativi in materia di sicurezza delle informazioni (es. sottrazione, perdita, violazione del dato). Tale obiettivo viene perseguito seguendo tre principi fondamentali:
 - 1) Integrità dei dati:** ovvero la capacità di mantenere la veridicità dei dati e delle risorse e garantire che non siano in alcun modo modificati o cancellati, se non ad opera di soggetti autorizzati. Integrità significa prendere in considerazione differenti scenari: prevenire modifiche non autorizzate ad informazioni da parte degli utenti, ma anche garantire che le informazioni stesse siano univocamente identificabili e verificabili in tutti i contesti in cui vengono utilizzate.
 - 2) Riservatezza dei dati:** ovvero garantire che i dati e le risorse siano preservati dal possibile utilizzo o accesso da parte di soggetti non autorizzati. La riservatezza deve essere assicurata lungo tutte le fasi di vita del dato stesso.
 - 3) Disponibilità dei dati:** si riferisce alla possibilità, per i soggetti autorizzati, di poter accedere alle risorse di cui hanno bisogno per un tempo stabilito ed in modo ininterrotto. La Disponibilità dei dati impedisce che durante l'intervallo di tempo definito avvengano interruzioni di servizio e allo stesso tempo garantisce che le risorse infrastrutturali siano pronte per la corretta erogazione di quanto richiesto;
- sensibilizzare e formare il personale addetto circa le tematiche di sicurezza delle informazioni;
- fornire un quadro strutturale per stabilire e riesaminare gli obiettivi per la sicurezza delle informazioni;
- classificare le informazioni secondo lo schema definito dall'organizzazione;
- diffondere i principi ed i valori dichiarati nella politica aziendale dall'organizzazione e a rendere attiva ed efficace la comunicazione da e verso le diverse parti interessate affinché sia compresa e partecipata;
- riesaminare periodicamente la propria politica ed obiettivi, almeno annualmente e comunque ogni qual volta ve ne sia l'esigenza a seguito dell'attuazione di modifiche che la influenzano, per accertarne la continua idoneità e rendere effettivo il proprio impegno al miglioramento.

Tutte le figure professionali devono operare per il raggiungimento degli obiettivi di sicurezza nella gestione delle informazioni.

L'applicazione del sistema di gestione richiede pertanto piena partecipazione, impegno ed efficace interazione di tutto il personale.

La Direzione è impegnata ad attuare, sostenere e verificare periodicamente la Politica ed a divulgarla a tutti i soggetti che lavorano per l'azienda o per conto di essa.

GESTIONE DOCUMENTALE

Il presente documento è valido a partire dal 02 gennaio 2023, è pubblico e disponibile per la consultazione da parte di tutte le parti interessate.

Il presente documento viene periodicamente rivisto e comunque con cadenza almeno annuale al fine di garantire il rispetto dei seguenti criteri previsti:

- conformità ai requisiti della norma ISO 27001:2017;
- requisiti legislativi definiti dalla legge.

La Politica per la Sicurezza delle Informazioni è formalizzata nel SGSI e viene costantemente aggiornata per assicurare il suo continuo miglioramento ed è condivisa con l'organizzazione, le terze parti ed i clienti, attraverso specifici canali di comunicazione.