

1 SCOPO

LO SCOPO DELLA POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

Lo scopo del presente documento è quello di descrivere i principi generali di sicurezza delle informazioni definiti da **DOMARC SRL** al fine di sviluppare un efficiente e sicuro Sistema di Gestione della Sicurezza delle Informazioni (SGSI).

2 DESCRIZIONE

Per DOMARC SRL, la sicurezza delle informazioni rappresenta una priorità fondamentale, mirata alla protezione dei dati e delle informazioni, nonché delle infrastrutture tecnologiche, fisiche, logiche e organizzative che ne garantiscono la gestione.

Questo significa ottenere e mantenere un sistema di gestione sicura delle informazioni, nell'ambito del campo di applicazione definito per il SGSI, attraverso il rispetto delle seguenti proprietà:

1. **Riservatezza:** assicurare che l'informazione sia accessibile solamente ai soggetti e/o ai processi debitamente autorizzati;
2. **Integrità:** salvaguardare la consistenza dell'informazione da modifiche non autorizzate;
3. **Disponibilità:** assicurare che gli utenti autorizzati abbiano accesso alle informazioni e agli elementi architetturali associati quando ne fanno richiesta;
4. **Controllo:** assicurare che la gestione dei dati avvenga sempre attraverso processi e strumenti sicuri e testati;
5. **Autenticità:** garantire una provenienza affidabile dell'informazione;
6. **Privacy:** garantire la protezione ed il controllo dei dati personali.

Nell'ambito della gestione dei servizi offerti da DOMARC SRL, nella gestione dell'infrastruttura tecnologica, attraverso i propri sistemi, l'osservanza dei livelli di sicurezza stabiliti attraverso l'implementazione del SGSI, assicura:

- la garanzia di aver incaricato implementato procedure e policy che possano garantire un'alta resilienza dei servizi e di disponibilità riservatezza ed integrità delle informazioni;
- selezionare, quando necessario, partner affidabili al trattamento del proprio patrimonio informativo;
- un'elevata immagine aziendale volta alla sicurezza dei clienti;
- la completa osservanza negli accordi stabiliti con i clienti;
- la soddisfazione del cliente;
- il rispetto delle normative vigenti e degli standard internazionali di sicurezza e di privacy.

Per questo motivo DOMARC SRL ha sviluppato un sistema di gestione sicura delle informazioni seguendo i requisiti specificati della Norma ISO 27001:2022 e delle leggi cogenti come mezzo per gestire la sicurezza delle informazioni nell'ambito della propria infrastruttura tecnologica e delle piattaforme applicative gestite sia direttamente sia per terzi.

3 AMBITO DI APPLICAZIONE

La politica per la sicurezza delle informazioni di DOMARC SRL si applica a tutto il personale interno ed alle terze parti che collaborano alla gestione delle informazioni ed a tutti i processi e risorse coinvolte nel campo di applicazione del sistema di gestione che risulta definito nel seguente campo di applicazione:

Progettazione, installazione, consulenza, gestione e assistenza di sistemi e infrastrutture informatiche.

4 POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

MOD-520

La politica della sicurezza di Domarc srl rappresenta l'impegno dell'organizzazione nei confronti di clienti e terze parti a garantire la sicurezza delle informazioni, degli strumenti fisici, logici e organizzativi atti al trattamento delle informazioni in tutte le attività. La politica della sicurezza delle informazioni di DOMARC SRL si ispira ai seguenti principi:

- a. 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.
- b. Garantire l'accesso sicuro alle informazioni, in modo da prevenire trattamenti non autorizzati o realizzati senza i diritti necessari.
- c. Garantire che l'organizzazione e le terze parti collaborino al trattamento delle informazioni adottando procedure volte al rispetto di adeguati livelli di sicurezza.
- d. Garantire che l'organizzazione e le terze parti che collaborano al trattamento delle informazioni, abbiano piena consapevolezza delle problematiche relative alla sicurezza.
- e. 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.
- f. Garantire che l'accesso alle sedi ed ai singoli locali aziendali avvenga esclusivamente da personale autorizzato, a garanzia della sicurezza delle aree e degli asset presenti.
- g. Garantire la conformità con i requisiti di legge ed il rispetto degli impegni di sicurezza stabiliti nei contratti con le terze parti.
- h. 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.
- i. Garantire la business continuity aziendale e il disaster recovery, attraverso l'applicazione di procedure di sicurezza stabilite.
- j. Stabilire un quadro di responsabilità e azioni necessarie per soddisfare i requisiti normativi e le linee guida di sicurezza.
- k. Definire procedure per l'utilizzo sicuro dei beni aziendali e delle informazioni, includendo gli aspetti di sicurezza anche in tutte le fasi di progettazione, sviluppo, esercizio, manutenzione, assistenza e dismissione dei sistemi e dei servizi informatici.

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

5 RESPONSABILITÀ DELLA POLITICA DI SICUREZZA DELLE INFORMAZIONI

La Direzione è responsabile del sistema di gestione sicura delle informazioni, in coerenza con l'evoluzione del contesto aziendale e di mercato, valutando eventuali azioni da intraprendere a fronte di eventi come:

- evoluzioni significative del business;
- nuove minacce rispetto a quelle considerate nell'attività di analisi del rischio;
- significativi incidenti di sicurezza;
- nuovi requisiti e pressioni da parte dei mercati di riferimento;
- evoluzione del contesto normativo o legislativo in materia di trattamento sicuro delle informazioni.

6 DICHIARAZIONE DI IMPEGNO

Domarc Srl si impegna a garantire:

- **la riservatezza delle informazioni** attraverso la definizione puntuale delle responsabilità interne per la gestione dei servizi e delle informazioni ad essi connesse; il controllo degli accessi fisici e logici agli archivi elettronici e cartacei esclusivamente da parte di personale autorizzato e competente;
- **l'integrità delle informazioni** attraverso il controllo degli accessi fisici e logici agli archivi elettronici esclusivamente da parte di personale autorizzato e competente e la gestione dei back-up dei dati e delle configurazioni dei sistemi informativi;
- **la disponibilità delle informazioni** attraverso l'identificazione dei ruoli e delle funzioni, i diritti di accesso alle informazioni e agli assets aziendali per la gestione dei servizi al Cliente;
- che dipendenti, fornitori, partner e ogni altra terza parte coinvolta con il trattamento di informazioni che rientrano nel campo di applicazione del Sistema di Gestione della Sicurezza delle Informazioni, accettino **gli obblighi e le responsabilità** di propria pertinenza, al fine di proteggere le informazioni, i beni e le risorse di Domarc Srl;
- che ogni **accesso**, di tipo fisico o informatico, sia **autorizzato, controllato** e monitorato sulla base dei seguenti criteri: (a) l'accesso è autorizzato al personale abilitato solo per le informazioni necessarie (principio della conoscenza minima o necessità di sapere); (b) l'accesso è autorizzato al personale abilitato solo per le informazioni relative alle attività specifiche (funzione di lavoro-correlati); (c) l'accesso alla struttura e ai locali è autorizzato al personale abilitato. L'accesso ai locali di Domarc Srl è autorizzato, controllato e monitorato in linea con la politica aziendale;
- che ogni dipendente, fornitore, imprenditore e terza parte sia **consapevole** del proprio ruolo e dell'impatto delle proprie azioni sulla sicurezza delle informazioni;
- che ogni risorsa sia adeguatamente **formata e addestrata** sulle politiche e sulle procedure relative alla gestione della sicurezza delle informazioni;
- che i trattamenti delle informazioni, delle attività, delle risorse e delle soluzioni inerenti alla protezione delle informazioni di Domarc o gestiti dalla stessa per conto dei propri clienti sono conformi alle leggi e ai regolamenti applicabili di natura cogente, contrattuale e volontaria;
- che ogni attività e risorsa di Domarc o affidata da questa a terze parti, nonché ogni informazione pertinente l'ambito del SGSI, è protetta contro i problemi legati alla riservatezza, l'integrità e la disponibilità, in proporzione al loro valore e nel rispetto delle leggi vigenti;
- che tutto il **personale** Domarc Srl sia **responsabilizzato** all'obbligo di: (a) garantire il rispetto delle norme, leggi e regolamenti vigenti, di natura cogente, contrattuale e volontaria rese applicabili negli ambiti del SGSI; (b) proteggere la riservatezza, l'integrità e la disponibilità delle informazioni gestite da Domarc Srl, la proprietà intellettuale e il patrimonio di Domarc Srl o da questa affidati a terze parti; (c) aver cura dei beni materiali, i sistemi e le risorse di Domarc Srl; (d) salvaguardare e gestire in modo appropriato ogni informazione e dato afferenti le attività di propria competenza; (e) contattare la Direzione, il Responsabile della Sicurezza delle informazioni e/o altre autorità competenti in caso di effettive o sospette violazioni della sicurezza; (f) segnalare qualsiasi necessità di modifiche alle procedure relative alla gestione della sicurezza delle informazioni. | Compatibilmente con le autorità assegnate nella gestione della sicurezza ciascuno deve: (g) garantire la conformità con la politica di sicurezza, requisiti, standard e/o procedure definiti; (h) individuare e definire i diritti di accesso agli assets per le loro specifiche attività e responsabilità; (i) richiedere alle terze parti di essere formalmente in linea con gli accordi di riservatezza; (l) operare in conformità ai livelli di rischio che sono stati definiti per il proprio ambito di pertinenza.

- che tutto il **personale** cui sono assegnate responsabilità specifiche nella gestione della sicurezza delle informazioni **ha altresì il dovere** di: (m) implementare la sicurezza sulla base delle politiche di sicurezza della Domarc Srl; (n) garantire e monitorare il rispetto delle politiche di sicurezza delle informazioni, requisiti, norme e procedure definiti da Domarc Srl nell'ambito del SGSI; (o) monitorare gli assets aziendali, al fine di garantire il rispetto del livello di controllo previsto per l'asset da proteggere ed il rispetto delle leggi e regolamenti applicabili; (p) rendere effettive l'insieme di regole, funzioni, strumenti, oggetti e controlli, resi coerenti e funzionali agli scopi dell'organizzazione e coerenti con gli ambiti del SGSI, che garantiscano che nella struttura, organizzazione, ambiente informatico, singolo elaboratore, sia costantemente osservato il rispetto dei requisiti del SGSI; (q) garantire che il personale di Domarc Srl e i terzi siano formati e informati circa la politica, i requisiti, standard e/o procedure per la gestione della sicurezza delle informazioni, nonché resi consapevoli delle conseguenze in caso di mancato rispetto della politica e requisiti stabiliti in tali ambiti; (r) sostenere l'adozione di misure adeguate a garantire il controllo sugli aspetti che hanno impatto sulla sicurezza delle informazioni; (s) contenere il livello di rischio negli ambiti di pertinenza; (t) mantenere attive le misure da adottarsi in caso di incidenti derivanti dal verificarsi di condizioni anomale e di emergenza, garantire l'adozione dei piani di continuità in conformità ai requisiti definiti dal SGSI;
- inoltre, che i **sogetti terzi** che gestiscono in modo diretto o indiretto gli assets sensibili di Domarc Srl e dei Clienti, sono **obbligati**, nello svolgimento di processi/attività, a: (u) formalizzare il proprio impegno alla riservatezza e non divulgazione delle informazioni tratte negli ambiti di competenza; (v) proteggere le risorse e le informazioni fisiche e intellettuali a cui possono accedere nella effettuazione delle attività assegnate; (z) garantire la piena osservanza ai requisiti del SGSI nei comportamenti e nell'operatività.

In conclusione, Domarc Srl si impegna a:

- **adottare un sistema di gestione sicura delle informazioni conforme ai requisiti specificati delle Norme UNI CEI EN ISO/IEC 27001:2022**
- **mantenere costantemente monitorato il grado di conformità del sistema alle norme e leggi applicabili di natura cogente e volontaria, e gli obblighi contrattuali pertinenti l'ambito di applicazione del SGSI;**
- **garantire mezzi e risorse idonee al suo mantenimento e miglioramento continuo, in particolare per quanto attiene la mitigazione/riduzione dei livelli di rischio sulla sicurezza delle informazioni e l'adozione di misure idonee a prevenire - ovvero gestire adeguatamente - situazioni anomale e di emergenza;**
- **rendere consapevoli tutte le persone che dell'organizzazione degli obblighi e delle responsabilità di ciascuno nella gestione della sicurezza delle informazioni e delle conseguenze in caso di eventi, dolosi e colposi, relativi all'utilizzazione non autorizzata, modifica o distruzione di informazioni critiche**