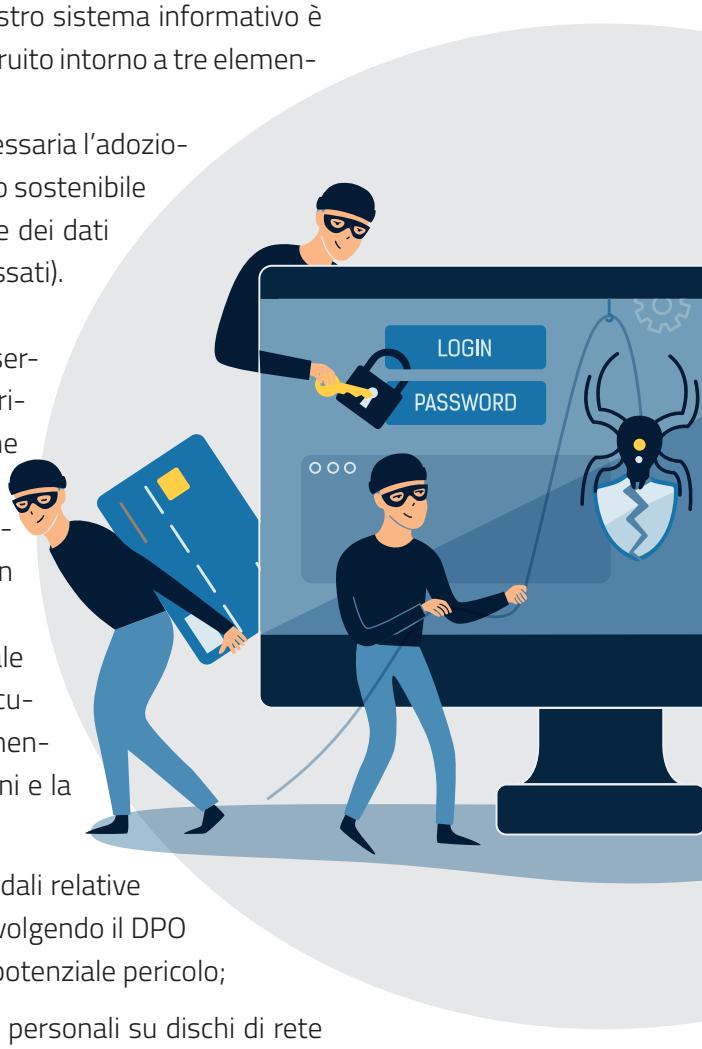
POLITICA SU PRIVACY E SICUREZZA DELLE INFORMAZIONI

La gestione della sicurezza delle informazioni e, conseguentemente, quella dei dati personali, è costituita dall'insieme di: misure tecnologiche, organizzative, procedurali e legali, la cui osservanza ci consente di monitorare e gestire i rischi a cui il nostro sistema informativo è sottoposto e così attuare un modello di sicurezza adeguato e costruito intorno a tre elementi fondamentali ovvero tecnologie, persone e processi.
Digitalizzazione e tecnologie sempre più innovative, rendono necessaria l'adozione di strategie che consentano di coniugare gli obiettivi di sviluppo sostenibile con l'adeguamento della sicurezza informatica e della protezione dei dati personali (anche a garanzia dei diritti e libertà dei soggetti interessati).



Questa Politica fornisce indicazioni e supporto sulle regole da osservare per ottenere una protezione delle informazioni efficace e rispondente ai requisiti di riservatezza, integrità e disponibilità, come anche previsti dal GDPR.
La mancanza di adeguati livelli di sicurezza fisica e logica può causare rilevanti danni sia in termini economici che reputazionali e non consente una condivisione sicura delle informazioni.
Per conseguire gli obiettivi di sicurezza aziendali, è fondamentale l'integrazione tra le risorse che al nostro interno si occupano di sicurezza delle infrastrutture tecnologiche, il DPO e le risorse appartenenti a tutte le altre funzioni aziendali. La sicurezza delle informazioni e la protezione dei dati è garantita grazie al fatto che:

- il personale conosce e applica le Politiche e le procedure aziendali relative alla sicurezza delle informazioni e alla protezione dei dati, coinvolgendo il DPO e gli amministratori di sistema qualora vi fossero situazioni di potenziale pericolo;
- il personale archivia tutte informazioni, le registrazioni e i dati personali su dischi di rete protetti e sottoposti a backup, incluse quelle riguardanti i clienti;
- tutti i software utilizzati dispongono di regolari licenze le cui informazioni sono archiviate dagli amministratori di sistema;
- meccanismi fisici anti-intrusione impediscono l'accesso di personale non autorizzato alle sale dove sono ubicati i server;
- i server sono configurati in modo da fronteggiare le emergenze e gli incidenti, sia naturali sia informatici, e garantire sempre la continuità del servizio; sono inoltre protetti in caso di possibili mancanze di tensione da gruppi di continuità e condizionatori;
- l'accesso logico ai sistemi e alla rete è garantito da adeguati livelli di protezione;

i software sono inoltre costantemente aggiornati per minimizzare il rischio di attacchi esterni:

- l'accesso avviene sempre attraverso login, password e, dove previsto, necessario e consentito dal sistema, tramite doppia autenticazione;
- le applicazioni anti-virus permettono di rilevare e rimuovere eventuali virus informatici senza pregiudicare la continuità del servizio;
- l'integrità dei dati è garantita dall'attività di back-up e da procedure di restore, così come definite nelle procedure dedicate;
- il Business Continuity Plan e la procedura di Disaster Recovery assicurano la corretta gestione degli incidenti e delle emergenze;

> i log registrano ciò che viene intercettato dai sistemi di anti-intrusione (Firewall) al fine di consentire azioni tempestive di prevenzione contro attacchi esterni;

> le informazioni e i dati, a seconda della classificazione e dei supporti, sono archiviate e protette da accessi non autorizzati;

> le connessioni VPN sono sottoposte a un processo di autenticazione, il cui protocollo ne garantisce la sicurezza;

> meccanismi di time-out impediscono la presenza di sessioni di lavoro e/o di interconnessione troppo lunghe;

> ogni cambiamento viene effettuato senza che vi siano perdite di informazioni; gli eventuali incidenti sono inoltre registrati e analizzati onde evitarne il ripetersi e impedire azioni legali di terzi;

> gli impianti ausiliari dei server (gruppi di continuità, condizionatori, ecc.), al pari delle infrastrutture informatiche e degli applicativi di supporto, sono sottoposti a manutenzione al fine di evitare possibili disservizi. Per quanto attiene le informazioni aziendali e del cliente di cui viene a conoscenza nel corso delle proprie attività, tutto il personale è soggetto ai vincoli di riservatezza. Allo stesso modo, eventuali fornitori che dovessero venire a conoscenza di tali tipologie di informazioni sono soggetti ai vincoli di riservatezza imposti in forza del contratto stipulato con l'azienda;

> sono attuate misure organizzative quali nomine, istruzioni, formazione e attività di sensibilizzazione;

> sono attuati con continuità piani di analisi, test, vigilanza e monitoraggio.

La presente Politica è comunicata e diffusa sia all'interno dell'organizzazione, tramite gli strumenti di condivisione disponibili, sia all'esterno tramite la pubblicazione nel sito web e viene revisionata almeno semestralmente.