MOTIVAZIONE

La mancanza di controllo da parte delle aziende su come i dati e le informazioni vengono generati, dove sono conservati e a quali soggetti sono trasmessi comporta il rischio di incidenti in materia di sicurezza e di conformità alle normative che possono avere un impatto negativo sul business stesso. La sicurezza delle informazioni, infatti, è un bene primario dell'azienda e il predisporre misure efficaci può costituire una strategia che alla lunga si trasforma in un vantaggio competitivo.

Per questo motivo DOS GROUP SA, che è un'azienda attiva da anni nella progettazione e realizzazione di applicazioni software e sistemi di emergenza, è da sempre in prima linea sui temi della data protection. Una misura fondamentale in tal senso è stata l'aver impostato un Sistema di Gestione per la Sicurezza delle Informazioni SGSI, un insieme di processi organizzativi, tecnici e procedurali che si fondano sulle "best practice" e sugli standard di riferimento in conformità anche alle direttive della norma internazionale UNI CEI EN ISO/IEC 27001:2017.

OBIETTIVI

L'obiettivo del Sistema di Gestione per la Sicurezza delle Informazioni di DOS GROUP SA è di garantire un livello di protezione e di sicurezza adeguato alla circolazione delle informazioni all'interno dell'organizzazione in modo da espletare al meglio la progettazione, lo sviluppo e l'erogazione dei servizi aziendali.

Senza procedure di identificazione, valutazione e analisi dei rischi, infatti, i pericoli in materia di sicurezza a cui i servizi e le procedure aziendali sono quotidianamente sottoposti possono inficiare il loro corretto funzionamento, con ricadute anche economiche.

L'insieme di misure organizzative, tecniche e procedurali predisposto dal Sistema di Gestione per la Sicurezza per le Informazioni di DOS GROUP SA soddisfa i seguenti requisiti di sicurezza di base:

- Riservatezza: l'accesso all'informazione è consentito solo a chi ne ha i privilegi
- Integrità: la gestione delle informazioni (e quindi anche la loro modifica) è sottoposta a vincoli precisi settati dalla governance aziendale
- Disponibilità: chi detiene i diritti può accedere liberamente alle informazioni nel momento stesso in cui avverte la necessità di utilizzarle all'interno dei processi operativi e il recupero avviene in maniera veloce e intuitiva

Con la centralizzazione dei sistemi abilitata dal cloud, DOS GROUP SA vuole proporsi nell'ambito della sicurezza delle informazioni come:

- Un fornitore affidabile e competente nel preservare al meglio l'immagine dell'azienda
- Un hub in cui il patrimonio informativo aziendale è conservato, tutelato e protetto
- Un facilitatore della continuità dei processi operativi
- Uno strumento ligio alle indicazioni della normativa vigente e cogente, con la conseguente crescita di competenze aziendali in materia di sicurezza

CONTENUTO DELLA POLITICA

Qualsiasi informazione necessaria per lo svolgimento delle attività interne, dai dati relativi ai prodotti/servizi alla loro configurazione, necessita di essere tutelata nel suo ciclo di vita, dalla creazione all'utilizzo fino all'eliminazione. Il SGSI si inserisce in questo processo, abilitando una gestione delle informazioni sicura, accurata, affidabile e un recupero tempestivo delle stesse.

In accordo con la vigente normativa UNI CEI EN ISO/IEC 27001:2017, tra le misure preventive richieste dal SGSI c'è l'obbligatorietà di una valutazione dei rischi per la sicurezza e dei loro potenziali impatti sull'azienda che deve essere eseguita periodicamente dal Responsabile per la Sicurezza delle Informazioni. Egli, infatti, deve valutare se vengono rispettati i requisiti di sicurezza citati prima, analizzare i fattori critici che hanno portato al verificarsi di incidenti e inserirli in un contesto più ampio di cambiamenti strategici, di business e tecnologici già effettuati o da effettuarsi.

Questa analisi ha lo scopo di valutare il rischio associato ad ogni asset da proteggere rispetto alle minacce individuate. La procedura adottata dal Responsabile della Sicurezza delle Informazioni nel compiere questa valutazione è condivisa con la Direzione, che deve approvare il documento relativo alla metodologia da applicare. Inoltre, è sempre la Direzione a concorrere alla definizione dei parametri che definiscono il valore del rischio. Una volta che il Responsabile ha portato a termine la sua elaborazione, i risultati ottenuti vengono vagliati congiuntamente con la Direzione, che considera accettabile o meno la soglia di rischio in base alle metriche stabilite in precedenza. In conclusione, si definiscono i trattamenti di mitigazione del rischio se ritenuti necessari e le azioni da intraprendere per migliorare la sicurezza del sistema, in base alle priorità e al budget aziendale e alla necessità di essere conformi alle normative vigenti. Il tutto sarà ponderato tenendo in considerazione anche il valore delle informazioni da tutelare e la presenza di eventi che possano avere un impatto significativo sulla sicurezza del sistema.

RESPONSABILITÁ

Le responsabilità sono così distribuite tra:

- il PERSONALE che è responsabile dell'osservanza della privacy policy concordata e che deve segnalare al responsabile, ove le riscontri, eventuali anomalie
- il COMITATO DELLA SICUREZZA DELLE INFORMAZIONI che si incontra con cadenza almeno semestrale. A comporlo il Presidente del Consiglio di amministrazione e il Responsabile della Sicurezza delle Informazioni ma non si esclude il coinvolgimento di chi in azienda ha le competenze tecniche necessarie per la valutazione di aspetti specifici. Come già accennato, la Direzione si occupa di stabilire le priorità e di promuovere le iniziative a favore della sicurezza, assicurandosi di rispettare le strategie aziendali e i budget destinati al progetto.
- il RESPONSABILE DELLA SICUREZZA DELLE INFORMAZIONI: suo è il compito di occuparsi della redazione e progettazione del Sistema di Gestione della Sicurezza delle Informazioni.

Nello specifico effettua l'analisi e la gestione del rischio individuando i criteri e le metodologie più indicate e si occupa di curare la normativa necessaria, tra cui anche quella riguardante la classificazione dei documenti, in modo che l'azienda possa procedere in maniera snella e sicura nello svolgimento delle sue attività. La valutazione comporta anche la proposta da parte del Responsabile di misure di sicurezza idonee e la verifica degli incidenti avvenuti, da sanare con le relative contromisure. Si impegna, inoltre,

a promuovere la cultura relativa alla sicurezza delle informazioni e a proporre percorsi formativi per il personale.
- I SOGGETTI ESTERNI che sono in contatto con DOS GROUP SA devono rispettare i principi di sicurezza indicati e sottoscrivere quando non esplicitato chiaramente nel contratto un "patto di riservatezza" a incarico conferito.

APPLICABILITÀ

La presente privacy policy si applica a tutti gli organi interni ed esterni dell'azienda ed è valevole per tutto il personale DOS GROUP SA. Essa viene applicata anche nei confronti di qualsiasi soggetto esterno che venga a conoscenza delle informazioni gestite in azienda e questo richiede una preventiva regolamentazione degli accordi in modo che la comunicazione verso l'esterno avvenga nel rispetto delle regole e delle norme vigenti.

RIESAME

DOS GROUP SA si assicurerà della verifica periodica dell'efficacia e dell'efficienza del Sistema di Governo per la Sicurezza delle Informazioni. Si occuperà ove necessario e adeguatamente al contesto e agli obiettivi di business di adottare le misure necessarie per migliorare le politiche di sicurezza e il loro corretto adeguamento in modo da garantire lo svolgimento continuo e sicuro di tutti i processi aziendali.

Mendrisio, 30/01/2020

Stefano Doninelli

DOS GROUP SA
Via Rime 38
CH-6850 Mendrisio
T. +41 (0)91 630 20 11
F. +41 (0)91 630 20 12
info@dos-group.com
www.dos-group.com