POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

La presente Politica per la Sicurezza delle Informazioni stabilisce i principi generali sulla cui base si stabiliscono i requisiti organizzativi per conseguire, e mantenere nel tempo, la Sicurezza delle Informazioni.

Premessa

Per "Sicurezza delle Informazioni" si intende la condizione in cui una organizzazione è in grado di perseguire, e di mantenere nel tempo, un livello di riservatezza, integrità e disponibilità delle informazioni conforme ai requisiti stabiliti da:

a) Legislazione vigente (in particolare protezione della privacy e della proprietà intellettuale);

b) Requisiti contrattuali dei Clienti;

c) Eventuali ulteriori requisiti stabiliti autonomamente da Palladio Group.

La "riservatezza" indica la proprietà dell'informazione di non essere accessibile a soggetti non autorizzati; l'"integrità" dell'informazione indica la proprietà dell'informazione di non essere modificabile, o cancellabile, se non da soggetti autorizzati; e la "disponibilità" indica la proprietà dell'informazione di essere accessibile, su richiesta di un soggetto autorizzato, entro tempi certi.

Generalità

Palladio Group ha la necessità, come parte delle proprie attività di business, di accedere a, ed elaborare in vario modo, informazioni che possono riguardare: progetti di Clienti, dati personali dei Dipendenti e dei Collaboratori, dati amministrativi e contabili prodotti e conservati allo scopo di ottemperare ad adempimenti legislativi.

La Direzione di Palladio Group ritiene, a questo proposito, che l'adozione di un modello organizzativo orientato alla sicurezza delle informazioni sia una decisione strategica e necessaria per mettere l'Organizzazione in condizione di:

a) Produrre, utilizzare e conservare in modo corretto le informazioni che sono necessarie per ottemperare a obblighi normativi o contrattuali;

b) Utilizzare in modo efficiente le risorse disponibili, attraverso una opportuna classificazione di criticità delle informazioni;

c) Generare, e conservare nel tempo, la fiducia degli stakeholder di Palladio Group nei confronti dell'affidabilità dell'Azienda nel salvaguardare le informazioni che genera e utilizza.

PRINCIPI

La sicurezza delle informazioni è una decisione strategica

La consapevolezza dell'importanza di generare, utilizzare e conservare le informazioni in modo corretto deve diventare parte dell'operato quotidiano a tutti i livelli. L'ideale a cui tendere è che tutti i processi decisionali ed esecutivi di Palladio Group che presuppongano la produzione, l'accesso o l'elaborazione di informazioni debbano essere strutturati in modo da perseguire la sicurezza di tali informazioni.

La sicurezza delle informazioni è basata su un approccio al rischio

Nel perseguire la sicurezza delle informazioni non esistono "ricette magiche" o "best practices" valide per qualunque situazione: il modo in cui l'Azienda affronta la sicurezza delle informazioni è intimamente legato alle minacce ed opportunità a cui l'Organizzazione ritiene di essere esposta. La disciplina del risk-based thinking è lo strumento che aiuta a identificare e dare una corretta priorità alle varie minacce ed opportunità: questo strumento deve quindi diventare parte dell'operato quotidiano di tutti i soggetti a cui sono affidati processi decisionali in Palladio Group.

La sicurezza delle informazioni inizia dal rispetto delle regole

Per garantire la sicurezza delle informazioni è fondamentale avere particolare attenzione alla conoscenza, e al rispetto, dei requisiti legislativi e contrattuali applicabili. Se in generale le decisioni in materia di sicurezza delle informazioni devono essere prese con un approccio risk-based, cioè attraverso una valutazione di costi e benefici, i requisiti legislativi e contrattuali devono sempre essere considerati un "rischio puro", cioè esclusivamente come una fonte di minacce (legate al mancato rispetto della legislazione o delle clausole contrattuali) e mai come una opportunità. L'organizzazione deve pertanto impegnarsi a tutti i livelli nell'identificare, comprendere e rispettare i requisiti legislativi e contrattuali in materia di sicurezza delle informazioni.

In particolare, deve esserci la consapevolezza a tutti i livelli dell'Organizzazione che il modello organizzativo adottato da Palladio Group per la sicurezza delle informazioni è definito e attuato in conformità alla Norma UNI CEI ISO/IEC 27001:2014. Pertanto, ai vari livelli organizzativi è richiesta consapevolezza dei requisiti stabiliti da tale Norma e dell'importanza del loro rispetto.

La sicurezza delle informazioni necessita di lavorare per obiettivi

Per avere una adeguata fiducia che la sicurezza delle informazioni verrà realizzata e mantenuta nel tempo è necessario fissare un percorso, scandito dalla presenza ai vari livelli organizzativi di opportuni obiettivi.

Se la definizione dei contenuti specifici degli obiettivi è lasciata ai vari livelli direzionali, in linea generale è necessario che tali obiettivi siano:

a) Espressi in termini misurabili, nei limiti del praticabile;

b) Compatibili con, e commisurati a, le risorse disponibili all'Organizzazione;

c) Corredati da opportune scadenze temporali, in assenza delle quali un obiettivo non può ritenersi tale;

d) Periodicamente monitorati.

La sicurezza delle informazioni è miglioramento continuo

Il contesto dell'Organizzazione (il mercato, la società, le esigenze e le aspettative dei Clienti, …) muta in continuazione. In questa condizione è impossibile che una qualsiasi Organizzazione riesca a sopravvivere, se non rimette periodicamente in discussione i suoi valori e le sue pratiche al fine di assicurarsi che siano ancora adeguati per affrontare i cambiamenti che inevitabilmente intervengono.

Amministratore Delegato
Dott. Mauro Marchi