POLITICA AZIENDALE – PERSEC S.R.L.

È redatto per gli scopi interni all'organizzazione sulla base di informazioni disponibili e secondo le procedure e lo stato di diritto vigente al momento della redazione, nessuna responsabilità può essere riposta in capo al redattore per eventuali imprecisioni o errori che possano emergere successivamente alla sua emissione.

Esso è fornito agli aventi causa in via confidenziale e non deve essere divulgato senza il consenso esplicito della Direzione della Persec s.r.l. che lo ha emesso.

Sommario

Introduzione

L'Azienda Persec s.r.l. è un'azienda che opera in Sicilia nel settore della progettazione, realizzazione, manutenzione e gestione di sistemi integrati in ambito ICT e infrastrutture di reti locali. Inoltre, l'azienda eroga servizi di consulenza, assistenza e gestione su sistemi ICT e di sicurezza informatica. L'obiettivo dell'azienda è quello di conformarsi alle norme UNI EN ISO 9001 e UNI EN ISO 27001 per garantire elevati standard di qualità e sicurezza nei servizi offerti.

Scopo

Il presente documento ha l'obiettivo dichiarare l'impegno della Persec s.r.l. a fornire servizi di alta qualità ai propri clienti attraverso una costante ricerca dell'eccellenza.

Contesto

Persec s.r.l. è nata dalla fusione di aziende attive nel mondo IT da oltre vent'anni. Si differenzia nel panorama dell'innovazione tecnologica grazie alle soluzioni all'avanguardia che hanno raccolto numerosi consensi per merito delle caratteristiche di usabilità e adattabilità alle specifiche esigenze del cliente e alla professionalità dei propri tecnici. Numerose aziende siciliane e nazionali leader nel proprio settore di riferimento hanno scelto Persec s.r.l. come partner tecnologico per le proprie infrastrutture: tutto ciò lo dobbiamo proprio all'affidabilità delle soluzioni IT e informatiche proposte.

La salvaguardia del nostro patrimonio informativo e di quello dei nostri clienti rappresenta un elemento di primaria importanza per il nostro core business, per questo motivo l'intera organizzazione è impegnata a garantire la massima sicurezza durante tutte le fasi del ciclo di vita dei nostri prodotti e servizi, che costituiscono il bene primario dell'azienda.

Al fine di garantire un approccio al miglioramento continuo dei processi organizzativi e di allineare i servizi alle migliori pratiche in materia di sicurezza delle informazioni, la Persec s.r.l. ha deciso di adottare uno standard conforme alla norma ISO/IEC 27001, validato da un Registered Certification Body (RCB) terzo e indipendente. Tale scelta ci consente di garantire un elevato livello di sicurezza delle informazioni e di conformità alle norme in vigore.

Le norme di riferimento utilizzate sono la norma Europea UNI CEI EN ISO/IEC 27001:2022 e la UNI EN ISO 9001:2015.

La nostra Vision

"Non cosa vogliamo essere, ma che problema vogliamo risolvere. È necessario pensare in grande e fuori dagli schemi perché non c'è innovazione senza immaginazione."
I nostri punti di forza sono:

- Reti: Infrastrutture scalabili e performanti;
- SOC/SIEM: Analisi degli attacchi informatici;
- Cyber Security: Proteggiamo la tua infrastruttura;
- Supporto: Assicuriamo un supporto professionale.

La nostra Mission

"Impegno e professionalità!"

Il nostro impegno per il cliente è massimo: questo richiede un lavoro di squadra in cui ciascun membro del gruppo si assume la responsabilità personale di fare la cosa giusta per i nostri clienti, il nostro team e la nostra azienda.

Per guadagnare la fiducia dei nostri clienti, dobbiamo lavorare insieme con rispetto e mantenere un alto livello di eccellenza in ogni aspetto del nostro lavoro. Dalla consulenza preliminare alla progettazione esecutiva, fino alla direzione lavori e alla gestione dell'impianto, ci sforziamo di supportare il manager nelle sue scelte di innovazione tecnologica, sia in ambito strategico che di consolidamento.

Per guidare verso l'eccellenza, dobbiamo migliorare le nostre abilità personali e professionali e mantenere un equilibrio positivo nella vita. Ci impegniamo a fare la differenza nel mercato, fornendo un servizio di alta qualità ai nostri clienti e lavorando insieme con rispetto e responsabilità personale.

Requisiti di protezione delle informazioni

All'interno dell'organizzazione Persec s.r.l., si concorderà e manterrà una definizione chiara dei requisiti per garantire la sicurezza delle informazioni, sia a livello interno che esterno, in modo che tutte le attività del Sistema di Gestione della Sicurezza delle Informazioni (ISMS) si concentrino sul rispetto di tali requisiti.

Saranno documentati tutti i requisiti normativi e contrattuali, che serviranno come input per il processo di pianificazione. Inoltre, i requisiti specifici per quanto riguarda la sicurezza dei nuovi o dei sistemi modificati o dei servizi verranno acquisiti come parte della fase di progettazione di ogni progetto.

Un principio fondamentale del sistema di gestione della sicurezza delle informazioni della Persec s.r.l. è che i controlli implementati siano definiti in opportune procedure e comunicati regolarmente a tutto il personale attraverso incontri di gruppo e documenti informativi.

Quadro per la definizione degli obbiettivi

Per definire gli obiettivi di sicurezza delle informazioni, verrà seguita una procedura parallela al ciclo di pianificazione del budget. Questo garantirà che siano disponibili i finanziamenti adeguati alle attività di miglioramento individuate. La definizione di questi obiettivi sarà basata su una chiara comprensione dei requisiti aziendali, scaturiti dal processo di riesame della direzione, durante il quale verranno considerate le opinioni delle parti interessate pertinenti.

Gli obiettivi di sicurezza delle informazioni saranno documentati e conservati per un periodo di tempo concordato insieme ai piani di dettaglio su come saranno raggiunti. Saranno valutati e monitorati come parte del riesame della direzione per garantire che rimangano validi. Se necessario, gli obiettivi verranno modificati attraverso il processo di gestione del cambiamento.

In conformità con la norma ISO/IEC 27001, Persec s.r.l., se del caso, adotterà i controlli di riferimento descritti nell'allegato A della norma. Questi saranno revisionati regolarmente in base ai risultati delle valutazioni dei rischi e in linea con i piani di trattamento del rischio per la sicurezza delle informazioni. Per maggiori dettagli sui controlli dell'Allegato A implementati e quelli esclusi, consultare la Dichiarazione di Applicabilità.

Inoltre, Persec s.r.l. adotterà e implementerà controlli avanzati e aggiuntivi derivanti dalle seguenti norme, standard e best practice:

- ISO/IEC 27017 - Controlli di Sicurezza per i Servizi Cloud
- ISO/IEC 27018:2019: Codice di condotta per la protezione delle PII (Personally Identifiable Information) nei servizi di public cloud per i cloud provider.
- Standard di programmazione PSR-4 per l'auto loading delle classi PHP
- tecniche best practice OWASP per la qualità del codice nell’ambito della prevenzione di vulnerabilità di sicurezza.

L’adozione di queste norme fornirà ulteriore garanzia ai nostri clienti e contribuirà ulteriormente alla nostra conformità legislativa in materia di protezione dei dati.

Politica

La Persec s.r.l. si impegna a stabilire un insieme di misure organizzative, tecniche e procedurali per garantire il raggiungimento dei requisiti fondamentali di qualità e sicurezza delle informazioni trattate.

Questo impegno si riflette nella progettazione e realizzazione di sistemi ICT avanzati e nelle attività di manutenzione e gestione delle reti locali, garantendo agli utenti finali un'esperienza ottimale e affidabile fondamentali per garantire la sicurezza delle informazioni.

L'azienda offre servizi di consulenza altamente specializzati per assistere i clienti nella scelta delle soluzioni ICT più adatte alle loro esigenze. Questa personalizzazione consente di massimizzare l'efficienza e la sicurezza dei sistemi implementati, aumentando la soddisfazione dei clienti e consolidando le relazioni a lungo termine.

Il Sistema di Gestione per la Sicurezza delle Informazioni si estende a tutte le attività sensibili identificate dall'analisi del contesto organizzativo.

La sicurezza delle informazioni è un aspetto cruciale per il successo dei nostri servizi e prodotti e per il raggiungimento degli obiettivi di business. Il conseguimento e il mantenimento della certificazione ISO 27001 costituiscono una prova tangibile, visibile e valutabile da terze parti dell'impegno di Persec s.r.l. per la sicurezza delle informazioni. La perdita o la sospensione della certificazione rappresenta un grave danno all'immagine e un potenziale rischio per il conseguimento degli obiettivi di business.

Tutte le informazioni e i dati trattati nei processi sono classificati e gestiti in base al loro livello di classificazione lungo tutto il loro ciclo di vita, rispettando le procedure correlate. Persec s.r.l. definisce la propria politica dettagliatamente per ciascuna area di pertinenza relativa alla protezione delle informazioni, con un approccio basato sul rischio e sulla gestione del rischio nel contesto organizzativo, come espresso nei documenti specifici per ciascuna area identificata.

Ciascuno dei criteri è definito e concordato da uno o più esperti nel settore e, una volta formalmente approvato, viene comunicato alle parti interessate interne ed esterne all'organizzazione. L'Allegato "A" elenca le aree individuate all'interno dei confini di applicabilità del sistema e riassume il contenuto di ogni politica e il target di riferimento delle parti interessate, declinando i principi stabiliti in questo documento.

Impegno al miglioramento continuo

Persec s.r.l. si impegna costantemente a migliorare il proprio sistema di gestione e la performance riguardante la sicurezza delle informazioni. Per raggiungere questo obiettivo, adotta il ciclo di Deming (Plan-Do-Check-Act) nei propri processi e si impegna in particolare a:

- Migliorare continuamente l'efficacia del sistema di gestione;
- Migliorare i processi attuali per portarli in linea con la buona pratica definita all'interno delle norme volontarie adottate;
- Ottenere e mantenere le certificazioni di sistema EN UNI ISO 9001 e EN ISO/IEC 27001;
- Aumentare il livello di proattività (e la percentuale degli stakeholder di proattività);
- Misurare la propria performance sulla sicurezza delle informazioni mediante l'adozione di controlli misurabili al fine di fornire una solida base per assumere decisioni informate;
- Riesaminare annualmente i processi di misura per valutare su base storica la loro efficacia e valutarne l'eventuale modifica;
- Ottenere spunti di miglioramento tramite riunioni periodiche e altre forme di comunicazione con le parti interessate, compresi i clienti del cloud service;
- Riesaminare i programmi di miglioramento al fine di riprogrammare le priorità degli interventi e delle assegnazioni delle risorse sulla base dei tempi e benefici ottenibili;
- investire nella formazione continua del proprio personale per garantire competenze e conoscenze aggiornate sulle tecnologie e le best practices del settore ICT

Proposte di miglioramento possono derivare da qualsiasi fonte, incluse risorse interne come dipendenti, personale IT, valutazioni di rischio e rapporti di servizio, nonché risorse esterne come clienti e fornitori. Tali proposte verranno registrate e valutate come parte della gestione del cliente.

Applicazione della Information Security Policy

Il Management di Persec s.r.l. non intende imporre restrizioni che vadano contro la consolidata cultura aziendale di apertura, fiducia e integrità morale, ma piuttosto perseguire l'obiettivo primario di proteggere le informazioni per tutelare tutte le parti interessate. Le dichiarazioni di politica presenti in questo documento e nei documenti di supporto elencati nell' Allegato A sono state esaminate e approvate dall'alta direzione di Persec s.r.l. e devono essere rispettate da tutto il personale dell'organizzazione.

L'omessa o parziale applicazione dei principi espressi nei documenti di politica per la sicurezza delle informazioni da parte di personale dipendente e/o collaboratori può comportare azioni disciplinari intraprese in conformità ai procedimenti disciplinari dell'organizzazione. In caso di domande riguardanti qualsiasi politica di Persec s.r.l., il dipendente deve rivolgersi in primo luogo ai propri manager gerarchici.

Destinatari e distribuzione

La politica per la sicurezza delle informazioni di Persec s.r.l. deve essere comunicata a tutto il personale interno, ai collaboratori, ai fornitori e a tutte le terze parti che vengono a contatto con le informazioni protette dall'ISMS di Persec s.r.l.. Questa politica deve essere compresa e accettata, e i principi in essa contenuti devono essere rispettati integralmente da tutte le parti interessate.

La politica viene distribuita attraverso il sito internet aziendale, dove è disponibile la versione approvata più aggiornata. Si ricorda che qualsiasi copia di questo documento che non sia stata appena scaricata dal sito internet aziendale è da considerarsi non aggiornata. Pertanto, è responsabilità del lettore assicurarsi di ottenere la versione più aggiornata e attuale del documento.

La documentazione aziendale di riferimento viene fornita su richiesta e in linea con il livello di confidenzialità del documento richiesto.

Tabella allegato A

Titolo politica	Area di interesse	Parti interessate
01 - Politica di utilizzo accettabile di internet.	Uso aziendale e personale di internet. Gestione degli account internet. Sicurezza, monitoraggio e usi vietati del servizio internet.	Gli utenti del servizio internet.
02 - Politica per il cloud computing.	Adeguata valutazione, registrazione, configurazione, gestione e rimozione dei servizi di cloud computing.	Dipendenti coinvolti nell'approvvigionamento e nella gestione dei servizi cloud.
03 - Politica per i dispositivi mobili.	Cura e sicurezza dei dispositivi mobili come laptop, tablet e smartphone forniti dall'organizzazione per uso aziendale.	Dipendenti a cui vengono forniti dispositivi mobili dall'azienda.
04 - Politiche per il telelavoro.	Considerazioni sulla sicurezza dell'informazione nella creazione e gestione di un sito di telelavoro, accordi, sicurezza fisica, assicurazioni e attrezzature.	Dirigenti e dipendenti coinvolti nella creazione e manutenzione di un sito di telelavoro.
05 - Politica sui controlli di accesso.	Registrazione e cancellazione dell'utente, fornitura dei diritti di accesso, accesso esterno, revisioni dell'accesso, politica della password, responsabilità dell'utente e controllo dell'accesso al sistema e alle applicazioni.	Dipendenti coinvolti nell'impostazione e nella gestione del controllo degli accessi.
06 - Politiche sulla crittografia.	Valutazione del rischio, selezione della tecnica, implementazione, test e revisione della crittografia e gestione delle chiavi.	Dipendenti coinvolti nell'impostazione e nella gestione dell'uso della tecnologia e delle tecniche crittografiche.
07 - Politiche sulla sicurezza fisica.	Aree sicure, sicurezza sulle carte e delle apparecchiature con relativo ciclo di vita.	Tutti i dipendenti.
08 - Politica anti-malware.	Firewall, antivirus, filtro antispam, installazione e scansione del software, gestione delle vulnerabilità, formazione e consapevolezza degli utenti, monitoraggio e avvisi sulle minacce, revisione tecniche e gestione degli incidenti malware.	Dipendenti responsabili della protezione dell'infrastruttura dell'organizzazione dal malware.
09 - Politiche di backup.	Cicli di backup, backup su cloud, documentazione di archiviazione off-site, test di ripristino e protezione dei supporti di archiviazione	Dipendenti responsabili della progettazione dell'implementazione dei regimi di backup.
10 - Politica di registrazione e monitoraggio.	Impostazioni per la raccolta, protezione e revisione degli eventi.	Dipendenti responsabili della protezione dell'infrastruttura dell'organizzazione dagli attacchi.

11 - Politiche sui software.	Acquisto, registrazione, installazione e rimozione di software. Sviluppo software interno e utilizzo software nel cloud.	Tutti i dipendenti.
12 - Politiche di gestione delle vulnerabilità tecniche.	Definizione delle vulnerabilità, fonti di informazioni, patch e aggiornamenti, valutazione delle vulnerabilità, rafforzamento e formazione sulla consapevolezza.	Dipendenti responsabili della protezione dell'infrastruttura dell'organizzazione dal malware.
13 - Politiche di sicurezza della rete.	Progettazione della sicurezza di rete, inclusa la segregazione della rete, sicurezza perimetrale, reti wireless, accesso remoto; Gestione della sicurezza della rete, inclusi ruoli e responsabilità, registrazione, monitoraggio e modifiche.	Dipendenti responsabili della progettazione, implementazione e gestione delle reti.
14 - Politiche sulla messaggistica elettronica.	Invio e ricezione di messaggi elettronici. Monitoraggio delle strutture di messaggistica elettronica e utilizzo della posta elettronica.	Utenti dei servizi di messaggistica elettronica.
15 - Politica di sviluppo sicuro.	Specifica dei requisiti aziendali, progettazione del sistema, sviluppo e test e uso Di software di terze parti.	Dipendenti responsabili della progettazione, gestione e scrittura di codice per sviluppi software su misura.
16 - Politica di sicurezza dell'informazione relativa alla catena di fornitura.	Adeguata valutazione, contratti con i fornitori, monitoraggio e revisione dei servizi, modifiche, controversie e fine del contratto.	Dipendenti coinvolti nella creazione e gestione dei rapporti con i fornitori.
17 - Politica per la disponibilità delle informazioni.	Requisiti di disponibilità e di progettazione, monitoraggio e reporting, di disponibilità, verifica dei piani di disponibilità e gestione dei cambiamenti.	Dipendenti responsabili della progettazione dei sistemi e della gestione dei servizi di consegna/rilascio.
18 - Politica per la garanzia della proprietà intellettuali e dei copyright.	Protezione delle proprietà intellettuali, legge, sanzioni e gestione dei software.	Tutti i dipendenti.
19 - Politica della protezione e conservazione delle registrazioni.	Tempi di conservazione di specifici tipi di informazioni, scelta e gestione dei supporti da utilizzare, uso della crittografia, accesso ai dati, cancellazione e recupero.	Dipendenti responsabili della creazione e gestione delle informazioni.
20 - Politica sulla privacy e protezione dei dati personali.	Legislazione applicabile sulla protezione dei dati, definizione e requisiti.	Dipendenti responsabili della progettazione e della gestione dei sistemi che utilizzano definizioni e requisiti dei dati personali.

21 - Politica sulla scrivania e sullo schermo puliti.	Sicurezza delle informazioni mostrate sugli schermi, stampate e conservate su supporti rimovibili.	Tutti i dipendenti.
22 - Politica sui social media.	Linee guida su come utilizzare i social media quando si rappresenta l'organizzazione e quando si discutono questioni rilevanti per l'organizzazione.	Tutti i dipendenti.