POLITICA INTEGRATA

PRISMA
improve your business

POLITICA INTEGRATA PER LA QUALITÀ, AMBIENTE, SALUTE E SICUREZZA SUI LUOGHI DI LAVORO E LA SICUREZZA DELLE INFORMAZIONI

Prisma s.r.l. ha implementato un Sistema Gestionale Integrato (SGI) per la qualità, per la salute e sicurezza sui luoghi di lavoro e per la sicurezza delle informazioni conforme alle norme UNI EN ISO 9001:2015, UNI EN ISO 14001:2015, UNI EN ISO 45001:2018 ed UNI CEI ISO/IEC 27001:2017.
Prisma s.r.l. è impegnata in un processo di continuo miglioramento finalizzato al raggiungimento di obiettivi di qualità, ambiente, salute e sicurezza sui luoghi di lavoro e di sicurezza delle informazioni di livello sempre più elevato. Ogni risorsa interna è impegnata a soddisfare costantemente le esigenze esplicite ed implicite di tutti gli utenti, i servizi erogati e le attività svolte da ciascuno devono conformarsi sempre e totalmente ai requisiti prescritti.

La presente Politica per la Qualità, Ambiente, Salute e Sicurezza sui luoghi di lavoro e di Sicurezza delle Informazioni è stabilità ed attuata per soddisfare i requisiti applicabili delle norme di riferimento, proteggere, per quanto possibile e comunque ad un livello ottimale e ad un costo compatibile con le specificità dell'organizzazione, il proprio SGI, da eventi intesi come minacce o incidenti, esterni e/o interni, oggettivi e/o soggettivi, che possano compromettere l'erogazione dei servizi nonché la riservatezza, l'integrità, la disponibilità e l'autenticità dei dati e delle informazioni gestite.
Lo scopo del presente documento è quello di descrivere la Politica per la Qualità, Ambiente, della Salute e Sicurezza sui luoghi di lavoro e di Sicurezza delle Informazioni appropriate alle finalità del contesto dell'organizzazione.
La PRISMA s.r.l. considera il proprio SGI, per il particolare rilievo che ha assunto per il perseguimento dei propri fini istituzionali, parte integrante del proprio patrimonio. È obiettivo di assoluta priorità garantire il miglioramento continuo della qualità dei servizi erogati, degli aspetti ambientali e della gestione della salute e sicurezza dei luoghi di lavoro e salvaguardare la sicurezza del proprio sistema informativo e tutelarne la riservatezza, l'integrità, l'autenticità e la disponibilità delle informazioni prodotte, raccolte o comunque trattate, da ogni minaccia intenzionale o accidentale, interna o esterna.

La PRISMA s.r.l. pone a base della propria Politica Integrata, una idonea analisi delle minacce e delle opportunità di tutte le risorse che costituiscono il proprio SGI, al fine poterne cogliere i vantaggi per il miglioramento continuo e di comprendere le possibili vulnerabilità, valutare le minacce e di predisporre le necessarie contromisure. La consapevolezza che non è possibile ottenere, in ambito informatico come del resto in natura, una condizione di sicurezza assoluta, comporta che lo scopo della propria Politica per la Qualità, Ambiente e di Sicurezza delle Informazioni è quello di gestire il rischio ad un livello accettabile attraverso la progettazione, l'attuazione ed il mantenimento di un SGI.
L'Alta Direzione cura la diffusione al suo interno della presente Politica Integrata a tutto il personale, tale politica viene inserita all'interno di una cartella condivisa accessibile al personale ed a tutte le funzioni organizzative oltre che presente sul sito aziendale.
La Direzione si impegna, altresì, attraverso specifici momenti di formazione al proprio personale, affinché la presente politica sia compresa e condivisa da tutto il personale.

POLITICA INTEGRATA PER LA QUALITÀ, AMBIENTE, SALUTE E SICUREZZA SUI LUOGHI DI LAVORO E LA SICUREZZA DELLE INFORMAZIONI

La presente Politica Integrata viene riesaminata ed eventualmente sottoposta a revisione almeno una volta all'anno in occasione del periodico riesame da parte della direzione ovvero in occasione di significative modifiche organizzative e/o tecnologiche rilevanti per il SGI.

La PRISMA s.r.l. intende continuare ad innalzare e standardizzare la qualità delle proprie attività, al fine di soddisfare nel miglior modo possibile le esigenze degli utenti e di raggiungere la propria piena soddisfazione, garantendo il rispetto di quei valori di riferimento che ne hanno caratterizzato l'azione in termini di etica, moralità, trasparenza, professionalità, investendo nella formazione e fornendo motivazioni per svolgere bene il proprio lavoro.

Nell'ambito lavorativo tali principi sono considerati, dalla Direzione, parte integrante delle strategie messe in atto per garantire un adeguato livello di efficienza dei sevizi resi all'interno del contesto in cui svolge le proprie attività.

Un punto saliente per le strategie aziendali è la sicurezza delle informazioni trattate e gestite, garantita da un sistema gestionale che ha come punto di partenza il pieno rispetto dei requisiti della normativa cogente.

È ferma convinzione della Direzione che la revisione delle procedure di gestione e controllo di tutto il sistema organizzativo garantisca un ambiente di lavoro sereno ed efficiente.

A tale scopo cui la PRISMA s.r.l. ha prima identificato i seguenti processi principali:

- pianificazione ed erogazione dei servizi;
- gestione dei controlli sui servizi erogati;
- approvvigionamento di beni e servizi;
- miglioramento continuo.

Successivamente ha definito i seguenti obiettivi generali finalizzati a garantire l'impegno a soddisfare tutti i requisiti applicabili e l'impegno per il miglioramento continuo del SGI:

- Ottenere e mantenere le certificazioni del proprio Sistema Integrato in conformità delle norme UNI EN ISO 9001:2015, UNI EN ISO 45001:2018 e UNI CEI ISO/IEC 27001:2017.
- ottimizzare e razionalizzare i processi di erogazione dei servizi perseguendo l'efficienza e la sicurezza e garantendo un elevato standard di qualità nei controlli;
- garantire la conformità dei processi e dei servizi erogati ai requisiti cogenti e ai requisiti specificati;
- garantire l'efficacia del sistema gestionale integrato e la sicurezza delle informazioni;
- garantire la soddisfazione degli utenti relativamente alla qualità e alla conformità dei processi e dei servizi erogati;
- Soddisfare gli obblighi di conformità legislativa, determinando gli obblighi di conformità, assicurando che le operazioni siano effettuate in conformità a tali obblighi, valutando l'adempimento degli stessi, correggendo le non conformità;
- Eliminare i pericoli e ridurre i rischi per la salute e sicurezza.

Per soddisfare tali obiettivi la PRISMA s.r.l. s'impegna a:

- tenere sotto controllo tutti i processi, identificando ogni problema e gestendo gli scostamenti dagli standard previsti attraverso adeguate azioni correttive e verificandone l'attuazione;
- fornire agli utenti, ai fornitori ed alle terze parti interessate esaurienti e credibili informazioni sulle attività svolte;
- garantire al personale una adeguata conoscenza e grado di consapevolezza dei problemi connessi con la sicurezza delle informazioni, al fine di acquisire sufficiente coscienza delle loro responsabilità in merito al trattamento;
- accertare che i fornitori esterni, che svolgono attività con impatto sulla qualità e sulla sicurezza delle informazioni, abbiano consapevolezza delle problematiche di sicurezza delle informazioni aziendali e rispettino la politica adottata dall'organizzazione;
- stabilire le procedure e sistemi per la gestione della sicurezza delle informazioni, garantendo che tutto il personale e tutte le terze parti interessate abbiano consapevolezza delle regole tecniche ed organizzative nell'utilizzo dei sistemi informativi;
- proteggere i lavoratori dalle ritorsioni a seguito della segnalazione di incidenti, pericoli, rischi ed opportunità;
- assicurare che l'organizzazione stabilisca ed implementi un processo per la consultazione e la partecipazione dei lavoratori;

Per fare ciò la Direzione garantisce l'informazione, la sensibilizzazione e il coinvolgimento costante tutto il personale attraverso opportuni interventi mirati a rafforzare la competenza e la consapevolezza. La Direzione si impegna inoltre a riesaminare ed adeguare costantemente tutto il Sistema Gestionale Integrato e la documentazione ad esso collegata, compresa la presente Politica, ponendosi sempre nuovi obiettivi da raggiungere.

Gli obiettivi generali enunciati nel presente documento vengono tradotti operativamente con frequenza almeno annuale in obiettivi di dettaglio ed indicatori relativi all'efficacia dei processi individuati, garantendo la misurabilità degli sforzi che l'organizzazione si propone di effettuare nel tempo.

Gli obiettivi di dettaglio relativi ai processi individuati, gli indicatori, le azioni da attuare, le risorse da dedicare e le relative responsabilità, i tempi entro i quali raggiungerli e i metodi di misurazione degli indicatori vengono riportati all'interno dei periodici verbali di riesame della direzione.

Uso dei sistemi di elaborazione delle informazioni

La PRISMA s.r.l. considera i sistemi di elaborazione delle informazioni gestiti, come strumenti di lavoro ed il loro uso, da parte di coloro che vi operano, a qualunque livello e a qualsiasi rapporto.

Gli strumenti messi a disposizione devono essere utilizzati per lo svolgimento dell'attività lavorativa in modo strettamente pertinente alle specifiche finalità della propria attività, nel rispetto delle esigenze di funzionalità e sicurezza dei sistemi stessi e della rete.

Conformemente alle regole del documento Allegato 5 "Norme generali per l'accesso e l'uso delle risorse aziendali", le risorse informatiche ed i servizi di rete sono risorse essenziali che l'azienda mette a disposizione esclusivamente per lo

svolgimento delle proprie attività. Il contributo di tutti gli utenti autorizzati a servirsene è fondamentale affinché ne venga preservata la integrità ed il buon funzionamento.

Sono pertanto vietate:

- attività contrarie alle leggi o proibite dai regolamenti e dalle consuetudini d'uso delle reti e dei servizi acceduti;
- attività commerciali non autorizzate;
- attività comunque idonee a compromettere la sicurezza delle risorse o dirette a cagionare danni a terzi.

Ogni condotta contraria a norme di legge o posta in essere in violazione dei contenuti del documento Allegato 5 "Norme generali per l'accesso e l'uso delle risorse aziendali", oltre a produrre eventuali conseguenze penali, civili o disciplinari, determinerà la sospensione dell'accesso alle risorse informatiche.

Organizzazione e responsabilità della sicurezza delle informazioni

È relativa all'individuazione delle procedure dirette alla gestione e controllo delle misure di sicurezza delle informazioni adottate e si concretizza nell'individuazione di ruoli, funzioni e responsabilità coinvolte nella realizzazione e gestione del SGI.

Assicurare che il personale della PRISMA s.r.l., in una visione che la sicurezza delle informazioni è una responsabilità comune, sia adeguatamente informato e formato sul ruolo che può svolgere al fine di minimizzare i rischi derivanti dalle minacce alla sicurezza delle informazioni.

Al gruppo "Information Security" e al suo responsabile competono la gestione delle risorse informatiche, i collegamenti in rete, nonché la cura, l'installazione e lo sviluppo delle stesse e l'assistenza agli utenti per l'accesso alle risorse ed alla rete; ha inoltre competenza in materia di sicurezza su ogni risorsa informatica.

Il Responsabile Information Security ha il compito di sovrintendere alle risorse del sistema operativo di una infrastruttura e di consentirne l'utilizzazione.

Scambio di informazioni

L'obiettivo è gestire gli scambi di informazioni con determinate strutture esterne, enti e/o organizzazioni pubbliche e private, senza compromettere l'integrità e la riservatezza delle informazioni e, nel contempo, garantire la sicurezza e la correttezza dell'operatività dei sistemi di elaborazione e di comunicazione.

La PRISMA s.r.l. garantisce lo scambio di informazioni con soggetti esterni; tali scambi di informazioni avvengono sulla base di norme di legge, accordi o protocolli d'intesa.

I flussi informativi con i soggetti esterni all'organizzazione sono caratterizzati dalla conformità alle regole concordate al fine di preservare l'integrità, la riservatezza, l'autenticità delle informazioni scambiate e la sicurezza dei sistemi di elaborazione nel rispetto della normativa, nazionale e comunitaria, vigente.

Gestione dei rischi

POLITICA INTEGRATA PER LA QUALITÀ, AMBIENTE, SALUTE E SICUREZZA SUI LUOGHI DI LAVORO E LA SICUREZZA DELLE INFORMAZIONI

L'obiettivo è identificare e contrastare le possibili minacce alla sicurezza dei sistemi e delle informazioni della PRISMA s.r.l., al fine di predisporre adeguate misure di prevenzione e protezione.

La riduzione dei rischi connessi all'interruzione dei servizi è messa in pratica da una costante e continua azione di formazione ed informazione dei dipendenti, come previsto nei piani di formazione, circa le procedure di emergenza, il backup e la conservazione dei dati.

La politica di sicurezza delle informazioni della PRISMA s.r.l. è orientata alla protezione efficace da minacce provenienti da soggetti interni e/o esterni non autorizzati ad accedere ai sistemi di gestione delle informazioni, rendendo meno probabile l'intrusione e l'illecita sottrazione e utilizzazione illegale di informazioni.

Viene effettuato il costante controllo degli aggiornamenti dei sistemi operativi e delle applicazioni software utilizzate, in modo da prevenire errori durante il loro utilizzo con conseguente aumento della qualità dei dati trattati e dell'efficienza operativa del personale.

La riduzione delle possibilità di furti informatici è perseguita tramite il controllo degli accessi fisici ai locali ove sono svolte le attività aziendali, le cui procedure e misure di sicurezza sono descritte nei documenti del SGI.

Uno dei grandi rischi per la sicurezza delle informazioni di una organizzazione è rappresentato dal "codice malevolo" (malware: Virus, trojan, ecc.). I rischi connessi al software malevolo sono affrontati con una politica di formazione ed informazione di personale ed utenti sui danni legati all'utilizzo di software diversi da quelli in dotazione.

Contestualmente la struttura informatica è tutelata contro le minacce derivanti dal malware, dall'aggiornamento continuo dei programmi specifici per la sua rilevazione ed eliminazione e dall'attuazione di specifiche procedure.

La strategia di PRISMA s.r.l. per la riduzione di questo rischio si basa su una serie di contromisure di natura preventiva, difensiva e di intervento per il contenimento del danno.

Le misure preventive adottate sono:

- Utulizzo di sistemi operativi progettati per la sicurezza, come GNU/Linux, Apple macOS, Microsoft Windows dalla versione 10 in poi.
- Mantenere aggiornati i sistemi operativi con l'ultimo livello di patch disponibile presso fonti affidabili e aggiornamenti automatici per macOS e Windows.

Le misure difensive adottate sono:

- Utilizzare e mantenere aggiornata la soluzione antivirus aziendale;

Le misure di intervento per il contenimento del danno sono:

- Isolare immediatamente i dispositivi su cui venga rilevato malware/virus.
- Disattivare le credenziali degli utenti potenzialmente violate a causa della compromissione del dispositivo.
- Ripristinare completamente il dispositivo compromesso evitando operazioni di recupero.

POLITICA INTEGRATA PER LA QUALITÀ, AMBIENTE, SALUTE E SICUREZZA SUI LUOGHI DI LAVORO E LA SICUREZZA DELLE INFORMAZIONI

Business Continuity

La responsabilità della Business Continuity delle attività svolte da PRISMA s.r.l. è del Responsabile Information Security.

Allo scopo è stato predisposto e mantenuto aggiornato un apposito piano di business continuity, inteso come indicazione delle attività organizzative e tecnologiche, finalizzate alla continuità operativa.

L'obiettivo è garantire il ripristino di una situazione di normalità entro un tempo prestabilito e rendere minimi gli impatti sui servizi erogati dall'organizzazione dovuti all'interruzione delle attività successive ad un guasto o disastro.

La PRISMA s.r.l. ritiene che possono presentarsi degli eventi che possano portare all'interruzione dei servizi erogati e cerca, con le precauzioni contenute nel piano di continuità operativa di contenere l'impatto di tali eventi sulle proprie attività.

La PRISMA s.r.l. ritiene che i sistemi di elaborazione delle informazioni sono elementi di criticità per la corretta erogazione dei servizi e una loro prolungata indisponibilità risulta dannosa per l'operatività dell'organizzazione e dei clienti.

Le metodologie che consentono di redigere, realizzare e mantenere il piano di continuità operativa sono diverse e fanno riferimento a standard organizzativi riconosciuti. Gli elementi comuni a tali standard sono:

- identificazione delle strutture di coordinamento della strategia di ripristino;
- valutazione dei risultati dell'Analisi dei Rischi per l'individuazione dei processi e dei servizi critici e delle priorità di intervento;
- predisposizione delle procedure da applicare in caso di attuazione del piano di continuità operativa; tali procedure sono definite nei documenti del SGI;
- sviluppo, documentazione e verifica del piano di business continuity.

La verifica del piano di Business Continuity è annuale, e comunque conseguente a significativi cambiamenti degli elementi che lo compongono.

Assett Inventary

L'Asset Inventary delle risorse è necessario per monitorare l'obsolescenza delle risorse utilizzate, pianificare il loro ammodernamento, e programmare gli investimenti in tecnologie dell'informazione.

L'obiettivo è identificare, classificare e registrare le risorse fisiche, hardware e software utilizzate dall'organizzazione, al fine di tracciare l'intero "ciclo di vita": acquisizione, assegnazione, aggiornamento, manutenzione, dismissione.

La PRISMA s.r.l. è dotato di un inventario informatizzato delle risorse che compongono la dotazione funzionale del servizio, la responsabilità della sua gestione è affidata al Responsabile Information Security.

Le risorse fisiche sono identificate e classificate e per ciascuna di esse sono registrate le informazioni in esse contenute per la loro corretta gestione reperimento, aggiornamento e/o dismissione.

Le risorse hardware sono classificate e per ciascuna di esse sono registrate le informazioni necessarie per la loro corretta gestione ed efficace manutenzione e/o aggiornamento.

I programmi software sono classificati e per ciascuno di essi vengono registrate le informazioni per una corretta gestione, controllo ed efficace manutenzione e/o aggiornamento.

Sicurezza fisica ed ambientale

La sicurezza fisica ed ambientale costituisce la forma di tutela che attiene alla protezione dei sistemi di elaborazione delle informazioni e si manifesta con misure fisiche dirette a garantire i controlli contro accessi non autorizzati ai locali ove sono ubicati i sistemi di gestione delle informazioni.

Preserva l'integrità e la disponibilità dei sistemi di gestione ed elaborazione delle informazioni per mezzo di misure atte ad impedire l'accesso non autorizzato ai locali ove sono ubicati.

L'obiettivo è minimizzare gli impatti delle minacce ai sistemi di gestione ed elaborazione delle informazioni dovuti a danni o intrusioni.

Le aree che comprendono i locali ove risiedono le informazioni sono dotate di punti di accesso controllati.

I locali sono dotati di sistemi atti a garantire e mantenere la sicurezza e l'integrità delle attrezzature, apparecchiature e degli impianti, al fine di evitare guasti che possono causare interruzione fisica al funzionamento delle attività inerenti l'erogazione dei servizi.

Tutti i sistemi e apparecchiature di rete sono ubicati in aree sicure e con accesso controllato. In particolare, i locali ove risiedono i sistemi server e le apparecchiature di rete sono "aree ad accesso ristretto" e l'ammissione è consentita solo in presenza di personale interno dell'organizzazione autorizzato.

Il personale di PRISMA s.r.l. al fine di garantire un adeguato grado di sicurezza, adotta la politica di "schermo e scrivania puliti" relativamente ai documenti ed ai supporti di memorizzazione gestiti, e di schermo pulito relativamente ai PC fissi ed ai PC portatili utilizzati.

"Schermo e scrivania puliti" significa trattare gli spazi di lavoro in modo tale per cui non siano mai visibili informazioni sensibili, anche in maniera accidentale. Al fine di proteggere tutti i dati sensibili e confidenziali PRISMA s.r.l. indica ai suoi dipendenti quali accorgimenti utilizzare affinché gli spazi di lavoro non rendano visibili informazioni sensibili. La postazione di lavoro è intesa come desktop, ma anche come scrivania, nel caso siano presenti documenti cartacei, e più in generale qualsiasi luogo nel quale siano contenute informazioni sensibili relative a PRISMA s.r.l., siano esse di proprietà dell'azienda, relative ai dipendenti, ai clienti o ai fornitori.

- La zona di lavoro deve essere costantemente presidiata, e resa sicura al termine della giornata di lavoro.
- Le postazioni computer devono essere bloccate o spente quando non utilizzate.
- I dati cartacei devono essere resi inaccessibili a terzi quanto non si è presenti alla postazione.
- Nel caso dei dati, in qualsiasi forma, vengano conservati in luoghi chiusi a chiave, le chiavi non devono mai essere lasciate incustodite.
- Le password non vanno mai scritte su foglietti lasciati accanto alla postazione di lavoro, e non vanno conservate in una posizione accessibile (anche un file sul computer non criptato è considerato accessibile).

- I computer vanno impostati in modo che automaticamente si blocchino e richiedano la password dopo più di cinque minuti di inutilizzo.
- Nel caso il proprio cellulare o altri dispositivi siano connessi ad attività aziendali (es. email) le regole per la postazione si applicano anche a loro.

Sicurezza logica

L'obiettivo è impedire accessi non autorizzati, tramite procedure di controllo, del personale della PRISMA s.r.l. e di soggetti appartenenti a organizzazioni esterne che, in forza di titolo (delega, contratto, accordo, convenzione o autorizzazione), accedono alle risorse dell'organizzazione.

Ulteriore obiettivo è proteggere le informazioni ed i sistemi di elaborazione e di comunicazione con misure tecnologiche ed organizzative atte a garantire il controllo degli accessi, la qualità delle informazioni, nonché la loro riservatezza ed integrità.

Il personale della PRISMA s.r.l. deve accedere solo ai sistemi a cui sono stati autorizzati. Ogni abuso di accesso a sistemi diversi da quelli autorizzati, è perseguito ai sensi dell'articolo 615-ter del Codice Penale "Accesso abusivo ad un sistema informatico o telematico", così come modificato dalla Legge 23 dicembre 1993 n. 547 "Modificazioni ed integrazioni delle norme del codice penale e del codice di procedura penale in tema di criminalità informatica".

Qualora gli utenti dovessero accedere in modo incidentale a sistemi o ad applicazioni della PRISMA s.r.l. senza autorizzazione, sono tenuti a disconnettersi e segnalare l'anomalia al Responsabile Information Security.

Il Responsabile Information Security o in generale il gruppo Information Security dota il proprio personale all'atto dell'insediamento, e i soggetti appartenenti a strutture esterne che, in forza di titolo (delega, contratto, accordo, convenzione o autorizzazione), della credenziale d'accesso alla rete.

Il gruppo Information Security abilita il proprio personale ed i soggetti appartenenti ad enti o organizzazioni con i quali è in essere un rapporto, ad essere autorizzati come utenti dei propri sistemi di elaborazione delle informazioni.

La PRISMA s.r.l. adotta la profilazione degli utenti, sia interni che esterni, per la concessione della credenziale d'accesso alle applicazioni ed utilizza a tal fine una procedura formale, mantenendo documentazione cartacea ed elettronica, delle autorizzazioni concesse.

Il Responsabile Information Security per le proprie competenze controlla almeno una volta all'anno, la validità di tutte le autorizzazioni attive per l'accesso alle applicazioni dell'organizzazione.

La revoca all'accesso ai sistemi di elaborazione delle informazioni del*la PRISMA s.r.l.*, viene attuata qualora decadano le caratteristiche di abilitazione di un utente.

La PRISMA s.r.l. considera la password, conformemente alle norme di sicurezza informatica, come una "informazione confidenziale di autenticazione composta da una serie di caratteri e/o simboli", utilizzata per l'accesso ai sistemi di elaborazione dell'informazione.

La struttura delle password individuata dall'utente presenta le seguenti caratteristiche informative e gestionali:

- obbligo di modifica al primo accesso;

- lunghezza minima di 8 caratteri;
- composizione con caratteri comprendenti almeno una lettera maiuscole, un carattere speciale e un numero;
- validità massima minore di 180 gg;
- non ripetibilità delle tre password precedenti;
- disattivazione automatica dopo 180 gg di non utilizzo.

La PRISMA s.r.l. consente l'uso solo di software autorizzato installato sui sistemi all'atto della loro consegna e raccomanda agli utenti l'utilizzo della pila software autorizzata. Software diverso da quello in dotazione standard e comunque conforme alla politica di sicurezza, deve essere richiesto a Responsabile Information Security, dopo aver riconosciuto la necessità funzionale.

La PRISMA s.r.l. proibisce che sui sistemi dati in dotazione ai propri dipendenti sia installato software non autorizzato e non ricompreso nel documento "M753 – Asset inventory" e considera illegale, ai sensi del D.Lgs. 9 aprile 2003 n. 68 "Attuazione della direttiva 2001/29/CE sull'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione", l'uso di software acquisito ed utilizzato senza regolare licenza d'uso.

Backup dei dati ed uso dei dispositivi di memorizzazione

Eventi dannosi o dovuti ad errori accidentali possono comportare perdita di dati conservati sul computer personale con ripercussioni anche gravi sull'attività lavorativa e sull'erogazione dei servizi.

Al fine di evitare il rischio di perdita di dati importanti la PRISMA s.r.l. effettua il backup dei dati e delle informazioni gestite.

Il personale di PRISMA s.r.l. deve salvare periodicamente i dati residenti sul personal computer, nelle apposite cartelle di sistema o sui supporti messi a disposizione dall'organizzazione.

I supporti rimovibili che contengono o hanno contenuto dati personali, possono essere riutilizzati o ceduti solo se debitamente e previamente cancellati in modo tale che, in modo permanente, non sia tecnicamente possibile il recupero di tali dati. In particolare dovrà essere utilizzato un software, anche open source, conforme allo standard "US Department of Defense DoD 5220.22-M (E)".

Sicurezza delle reti delle telecomunicazioni

Per garantire la sicurezza delle reti e delle comunicazioni occorre prevenire l'accesso alle reti e l'utilizzo illegale di informazioni, da parte di soggetti non autorizzati al fine di preservare la riservatezza dei dati e la disponibilità del servizio.

I documenti del SGI contengono le raccomandazioni sulla sicurezza della rete interna, le regole per la navigazione in Internet e le indicazioni per l'uso appropriato della posta elettronica e la protezione contro il software malevolo.

Gestione degli incidenti informatici

Un incidente, nell'ambito della sicurezza dell'informazione, è un evento sospetto o una vulnerabilità tale da violare l'integrità, la riservatezza e/o la disponibilità delle applicazioni, dei dati e/o dei sistemi di elaborazione delle informazioni.

POLITICA INTEGRATA PER LA QUALITÀ, AMBIENTE, SALUTE E SICUREZZA SUI LUOGHI DI LAVORO E LA SICUREZZA DELLE INFORMAZIONI

Tutti devono attenersi alle indicazioni ricevute in materia di sicurezza delle informazioni e contenute nei documenti del SGI.

Chiunque individua o abbiano il sospetto di un possibile incidente riguardante la sicurezza delle informazioni, deve segnalarlo al Responsabile Information Security.

Approvazione ed emissione

Alta Direzione

(Dott. Salvatore Ribaudo)

Prisma S.r.l.
Amministratore Unico
Dr. Salvatore Ribaudo