SOMMARIO

INDICE DELLE REVISIONI

DATA	REV.	OGGETTO DI MODIFICA	REDAZIONE	VERIFICA	APPROVAZIONE
05/12/2023	0	NUOVA EMISSIONE	SQA	SQA	AD

1. OBIETTIVO DEL DOCUMENTO

L'obiettivo del documento è quello di definire i principi e le indicazioni della Direzione per approcciare e gestire la sicurezza delle informazioni, con riferimento al contesto delle informazioni aziendali, inclusi i dati personali, sia per l'ambito interno che esterno all'organizzazione.

2. CAMPO DI APPLICAZIONE

La presente procedura si applica alla Società Rekeep. Relativamente ai sistemi informatici tutte le policy di sicurezza si applicano sia agli ambienti fisici e sia agli ambienti virtuali, in funzione dell'applicabilità tecnologica.

3. PROCEDURA

3.1 SICUREZZA BY DESIGN \ BY DEFAULT

Le funzioni aziendali, coinvolte nelle attività di progettazione dei servizi in ambito, devono considerare la sicurezza delle informazioni quale contesto essenziale per la loro gestione, dal punto di vista di:

- Riservatezza
- Integrità
- Disponibilità

I principi applicabili sono:

- Security by Design: il principio prevede che nella gestione di ogni iniziativa che includa la gestione di informazioni, siano messe in atto adeguate misure tecniche ed organizzative volte a garantire la sicurezza di tali informazioni a partire dalle fasi iniziali della progettazione e siano gestite durante tutto il ciclo di vita dell'iniziativa.
- Security by Default: il principio prevede che le misure tecniche ed organizzative applicate ai sistemi di elaborazione delle informazioni siano predisposte nella modalità volta a garantire il maggior livello di sicurezza. A solo titolo di esempio, si riporta il caso delle regole di accesso di un firewall, che nella configurazione di default deve prevedere il blocco di tutte le tipologie di traffico e definire specifiche regole per quello consentito.

3.2 PRIVACY BY DESIGN \ BY DEFAULT

Rekeep considera la tutela della privacy del soggetto diritto fondamentale pertanto, nella gestione del dato personale l'organizzazione si ispira ai seguenti principi chiave:

- Privacy by Design: il principio prevede che in funzione dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del

trattamento, sia all'atto del trattamento stesso, siano in essere misure tecniche e organizzative adeguate, volte ad attuare in modo efficace i principi di protezione dei dati e a integrare nel trattamento le necessarie garanzie al fine di soddisfare e tutelare i diritti degli interessati.

- Privacy by Default: il principio prevede che siano messe in atto misure tecniche e organizzative adeguate a garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento.

  Tale obbligo vale per:

  - la quantità dei dati personali raccolti
  - la portata del trattamento
  - il periodo di conservazione
  - l'accessibilità.

  In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica stessa.

3.3 PROTEZIONE DEI DATI PERSONALI (PII - PERSONAL IDENTIFIABLE INFORMATION)

Citiamo la definizione di Personal Identifiable Information contenuta all'interno del NIST "Special Publication 800-122:
"PII is any information about an individual maintained by an agency, including any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information."
(Le PII sono tutte le informazioni su un individuo conservate da un'organizzazione, comprese le informazioni che possono essere utilizzate per distinguere o rintracciare l'identità di un individuo, come il nome, il codice fiscale riportato sulla tessera sanitaria, la data e il luogo di nascita, il cognome da nubile della madre o i dati biometrici; e qualsiasi altra informazione collegata o collegabile a un individuo, come le informazioni mediche, educative, finanziarie e sull'occupazione).

La seguente lista contiene alcuni esempi, a titolo non esaustivo, di informazioni che vengono considerate PII:

- Nome, cognome, cognome da nubile, cognome da nubile della madre o pseudonimo;
- Numero di identificazione personale, come codice fiscale riportato sulla tessera sanitaria, numero di passaporto, numero di patente di guida, numero di identificazione del contribuente, numero di identificazione del paziente e numero di conto finanziario o di carta di credito;
- Informazioni sull'indirizzo, come l'indirizzo di residenza o l'indirizzo di posta elettronica
- Informazioni sulle risorse, come l'indirizzo IP (Internet Protocol) o MAC (Media Access Control) o un altro identificatore statico persistente specifico per l'host che collega in modo coerente a una persona particolare;
- Numeri di telefono, compresi i numeri di cellulare, di lavoro e personali;

- Caratteristiche personali, comprese immagini fotografiche (in particolare del volto o di altre caratteristiche distintive), radiografie, impronte digitali o altre immagini biometriche o dati di modelli (ad esempio, scansione della retina, firma vocale, geometria facciale)
- Informazioni che identificano beni di proprietà personale, come il numero di immatricolazione del veicolo o il numero del titolo di proprietà e informazioni correlate;
- Informazioni su un individuo che sono collegate o collegabili a uno dei precedenti (ad esempio, data di nascita, luogo di nascita, razza, religione, peso, attività, indicatori geografici, informazioni sull'occupazione, informazioni mediche, informazioni sull'istruzione, informazioni finanziarie).

Rekeep, nell'ambito delle proprie attività, si impegna a garantire la protezione dei dati personali di tutti i soggetti interessati, ponendo particolare attenzione all'utilizzo di servici di cloud pubblici (ovvero nelle infrastrutture controllate da organizzazioni che le rendono disponibili a terzi attraverso la vendita di servizi a consumo).

A tal fine, vi è un impegno continuo a conformarsi alla legislazione applicabile in materia di protezione dei dati personali e ai termini contrattuali concordati con i propri clienti. Rekeep si impegna pertanto a conformarsi alle normative italiane ed europee applicabili in materia di protezione dei dati personali, secondo quanto riportato nell'apposito documento RKP.MOD.PRE.

Nel caso di servizi cloud gli accordi contrattuali stipulati dall'azienda sia con i propri fornitori sia con i propri clienti devono ripartire in modo chiaro le responsabilità tra il responsabile del trattamento dai dati personali nei cloud pubblici, i suoi subappaltatori e il cliente del servizio cloud, tenendo conto del tipo di servizio cloud in questione.

3.4 CLOUD COMPUTING

La politica di sicurezza delle informazioni adottata da Rekeep si basa su principi fondamentali per garantire la protezione delle informazioni e delle risorse nell'ambiente di cloud computing. I seguenti principi sono applicati in modo coerente con i livelli accettabili di rischio per la sicurezza delle informazioni e delle altre risorse dell'organizzazione.

In particolare, Rekeep, sia come fornitore che fruitore di servizi cloud, si impegna a tener conto di quanto segue:

- **Requisiti di sicurezza delle informazioni**: devono essere definiti i requisiti di sicurezza delle informazioni di base che devono essere applicati nella progettazione e nell'implementazione del servizio cloud. Questi requisiti assicurano la protezione dei dati sensibili e delle risorse dell'azienda cliente, garantendo la riservatezza, l'integrità e la disponibilità delle informazioni.
- **Accesso e gestione delle informazioni**: le informazioni archiviate nell'ambiente di cloud computing possono essere soggette ad accesso e gestione da parte del fornitore e del cliente di servizi cloud. Pertanto, sono adottate misure appropriate per garantire la riservatezza, l'integrità e la disponibilità delle informazioni in conformità con le politiche di sicurezza di Rekeep.

- **Protezione delle risorse e dei dati**: le risorse, come i dati, i programmi applicativi e le relative informazioni, possono essere mantenute nell'ambiente di cloud computing. Sono implementate misure di sicurezza per proteggere tali risorse da accessi non autorizzati, modifiche non autorizzate o perdita di dati, al fine di preservarne la disponibilità e l'integrità.
- **Ambiente mono o multi-tenant**: i processi possono essere eseguiti su un servizio cloud virtualizzato e multi-tenant. Nel caso di servizi acquisiti viene verificata la presenza di misure atte a garantire la separazione e l'isolamento logico e/o fisico degli ambienti dedicati a Rekeep rispetto ai dati e/o ai tenant degli altri utenti del servizio cloud. Particolare attenzione viene posta alle tematiche relative alla sicurezza della virtualizzazione.
- **Gestione degli utenti del servizio cloud**: gli utenti del servizio cloud e il contesto in cui utilizzano il servizio cloud sono presi in considerazione per garantire l'adozione di politiche e controlli di sicurezza adeguati. Sono implementati meccanismi di autenticazione, autorizzazione e gestione degli accessi per garantire che solo gli utenti autorizzati possano accedere alle risorse e alle informazioni pertinenti. Il ciclo di vita degli account di Rekeep e dei fornitori del servizio cloud è monitorato al fine di proteggere le informazioni.
- **Privilegi degli amministratori del servizio cloud**: gli amministratori del servizio cloud che hanno accesso privilegiato sono soggetti a controlli specifici. Vengono definiti processi e procedure per gestire l'accesso privilegiato, monitorare le attività degli amministratori e mitigare il rischio di abusi o accessi non autorizzati.
- **Localizzazione dei dati**: le ubicazioni geografiche dell'organizzazione del fornitore di servizi cloud e i Paesi in cui il fornitore di servizi cloud può memorizzare le informazioni sono presi in considerazione. Vengono adottate misure per garantire la conformità alle normative sulla protezione dei dati personali e la protezione delle informazioni sensibili durante la memorizzazione e il trasferimento dei dati all'interno dell'ambiente di cloud computing.

Rekeep si impegna ad applicare questi principi come parte integrante della sua politica di sicurezza delle informazioni, al fine di garantire un livello adeguato di protezione delle informazioni e delle risorse nel contesto del cloud computing sia come fornitore che fruitore di servizi.

3.5 FORMAZIONE E CONSAPEVOLEZZA

L'Information Security passa dalla sicurezza dei comportamenti e delle attività svolte dalle persone, nelle attività lavorative, ma non solo: la persona costituisce un anello importante, spesso il più debole, nel ciclo di vita della sicurezza.

La sicurezza delle informazioni deve, pertanto, basarsi sui concetti di informazione, formazione, e accrescimento della consapevolezza delle risorse umane, intese come:

- Informazione, intesa come il complesso di attività dirette a fornire conoscenze utili alla identificazione, alla riduzione dei rischi per la gestione della sicurezza delle informazioni
- Formazione, intesa come il processo educativo attraverso il quale trasferire a dipendenti e collaboratori e altri soggetti le conoscenze e le procedure utili all'acquisizione di competenze per lo svolgimento sicura dei rispettivi compiti nella gestione delle informazioni (sviluppatori, tecnici ICT, amministrazione, gestione del personale, etc.)

- Consapevolezza, inteso come il complesso di attività dirette a sensibilizzare personale e collaboratori sui potenziali rischi di sicurezza associati a specifici comportamenti e fenomeni (social engineering, phishing, etc.)

Queste attività sono regolamentate tramite opportuni processi aziendali, costantemente revisionati per incrementarne la qualità e l'adeguatezza in funzione della rapida mutevolezza di contesti e scenari di cyber sicurezza.

3.6 STRATEGIA PER LA SICUREZZA E APPROCCIO AL RISCHIO

L'Organizzazione si pone l'obiettivo di gestire la sicurezza delle Informazioni attraverso una strategia adeguata, completa e strutturata, articolata attraverso l'implementazione di iniziative volte ad ottenere i seguenti risultati:

- Raggiungimento degli obiettivi di sicurezza tramite misure ed interventi omogenei e coerenti
- Utilizzo delle valutazioni sul rischio informatico per stabilire l'intensità e l'efficacia dei controlli di sicurezza
- Attribuzione di priorità ai controlli di sicurezza che hanno come scopo la prevenzione delle minacce, rispetto a quelli con finalità di mitigazione degli impatti derivanti dagli incidenti
- Definizione delle misure di sicurezza su una architettura a diversi livelli, così che un'eventuale falla in una linea di difesa sia coperta dalla successiva ("difesa in profondità")
- Verifica che l'implementazione dei controlli di sicurezza includa le modalità ed i meccanismi adeguati a verificarne l'efficacia e la corretta attuazione nel tempo.

3.7 PROCESSO DI GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI

Il perseguimento degli obiettivi aziendali di sicurezza è conseguito attraverso la definizione, l'implementazione e l'aggiornamento periodico di processi facenti parte di un Sistema di Gestione per la sicurezza delle informazioni.

3.8 MODELLO ORGANIZZATIVO PER LA SICUREZZA DELLE INFORMAZIONI

Il perseguimento degli obiettivi aziendali di sicurezza è conseguito attraverso la definizione di un adeguato modello organizzativo per l'attribuzione di ruoli e responsabilità per la sicurezza.

3.9 GESTIONE DEL RISCHIO

La sicurezza delle informazioni è gestita attraverso l'approccio al rischio che permette di valorizzare le informazioni, valutare le minacce e i loro impatti sulle informazioni e identificare le misure tecniche-organizzative (o controlli) adeguate finalizzate a proteggere le informazioni, minimizzando il rischio in maniera efficace ed efficiente, attraverso una pianificazione strategica strutturata.

3.10 SUPPORTO IN TERMINI DI RISORSE UMANE E FINANZIARIE

La sicurezza delle informazioni è garantita attraverso l'impegno della Direzione ad allocare le risorse, umane e finanziarie, necessarie e a garantirne il continuo accrescimento di competenze e consapevolezza in termini di sicurezza delle informazioni.

3.11 COMUNICAZIONE

La sicurezza delle informazioni è garantita attraverso adeguati canali di comunicazione, in funzione delle specifiche esigenze. Tali canali comprendono la pubblicazione di politiche e procedure di sicurezza, la condivisione di principi e requisiti all'interno di offerte e contratti e sui canali istituzionali di comunicazione (sito web, canali social, etc.).

3.12 INTEGRAZIONE NELLE ATTIVITÀ OPERATIVE

La sicurezza delle informazioni è implementata all'interno delle attività operative attraverso la definizione di opportune procedure. L'approccio agli interventi è basato sul concetto di rischio operativo legato a specifici ambiti di controllo per la sicurezza.

3.13 MONITORAGGIO, CONTROLLO E MIGLIORAMENTO CONTINUO

La sicurezza delle informazioni è costantemente monitorata attraverso opportuni strumenti di monitoraggio e controllo volto a valutarne le prestazioni in termini di efficacia ed efficienza. Gli strumenti sono volti anche a identificare le aree di debolezza al fine di comprenderne le cause e poter intervenire con opportune azioni correttive finalizzate al miglioramento continuo.

3.14 MATURITÀ DI PROCESSI CONTROLLI

La gestione della Sicurezza delle Informazioni è finalizzata non solo all'incremento dell'efficacia di processi e controlli, ma anche alla loro maturità, attraverso la produzione di informazioni documentate, cartacee e digitalizzate, di politiche, procedure, processi e registrazioni.

3.15 GESTIONE DEGLI ACCESSI

L'obiettivo di questa policy è di definire l'approccio utilizzato dall'organizzazione per:

- limitare l'accesso alle informazioni ed ai servizi di elaborazione delle informazioni;
- assicurare l'accesso degli utenti autorizzati e prevenire accessi non autorizzati a sistemi e servizi;
- rendere gli utenti responsabili della salvaguardia delle loro informazioni di autenticazione.

La Policy riguarda gli accessi ai sistemi informatici, agli strumenti e alle informazioni.
La responsabilità della applicazione della Policy è attribuita all'Amministratore di Sistema (AdS).

I proprietari delle informazioni e degli asset associati determinano i requisiti di sicurezza delle informazioni e di business relativi al controllo degli accessi.

Le regole di controllo degli accessi sono implementate definendo e mappando i diritti e le restrizioni di accesso appropriati alle entità pertinenti. Un'entità può rappresentare un utente umano così come un elemento tecnico o logico (ad esempio, una macchina, un dispositivo o un servizio).
L'accesso alle informazioni e agli asset associati è assegnato seguendo i seguenti principi:

- need-to-know: a un'entità viene concesso l'accesso solo alle informazioni di cui ha bisogno per svolgere i propri compiti (compiti o ruoli diversi significano informazioni diverse da conoscere e quindi profili di accesso diversi);
- need-to-use: a un'entità viene assegnato l'accesso all'infrastruttura informatica solo se è presente una chiara necessità.

3.16 SEPARAZIONE DEGLI STRUMENTI DI SVILUPPO, DI TEST E OPERATIVI

Gli ambienti di sviluppo e test devono essere separati dagli ambienti operativi al fine di ridurre il rischio di modifiche non autorizzate, volontarie o accidentali, incoerenze e/o incompatibilità tra dati e/o sistemi e in generale preservare l'integrità dei servizi e dei sistemi di produzione.

A questo scopo sono imposti ai diversi fornitori controlli in tal senso, atti ad assicurare la segregazione degli ambienti e la concessione di account separati agli operatori cui, per ragione di servizio è consentito di accedere.

Ove possibile, i dati reali di produzione, in particolar modo se sensibili, sia dal punto di vista privacy che dal punto di vista business, non devono essere utilizzati in ambiente di test se non dopo l'adozione di tecniche di alterazione (es. anonimizzazione, mascheramento etc..). Se ciò non dovesse essere possibile per ragioni riconducibili alle necessità di test dovranno essere adottati controlli secondari, in particolar modo se risultano coinvolte terze parti cui è concesso l'accesso a questi dati.

3.17 SVILUPPO DI SOFTWARE SICURO

Al fine di prevenire vulnerabilità di sicurezza nelle soluzioni applicative è richiesta l'adozione di un ciclo di vita dello sviluppo software maturo, che includa nella filiera di realizzazione dei servizi gli appropriati controlli di sicurezza.

Per le attività di sviluppo software, affidate a fornitori esterni, devono essere imposti dei requisiti di sicurezza allo scopo di ottenere il software più sicuro possibile, in linea con la criticità e riservatezza dei servizi e/o dei dati trattati.

È responsabilità dei Referenti delle diverse linee di servizi, di concerto con il Responsabile IT, mantenere allineate alle esigenze dei clienti, le politiche e i requisiti di sviluppo di software sicuro che impongano di verificare che non siano presenti vulnerabilità prima del rilascio del software in ambiente di esercizio.

3.18 SICUREZZA DELLE COMUNICAZIONI GESTITE ATTRAVERSO LE RETI

Deve essere garantita la protezione delle informazioni gestite attraverso le reti, rispettando tutti i requisiti di sicurezza e gli accordi previsti, in tutte le operazioni di comunicazione di informazioni da e verso l'esterno.

Le funzionalità di protezione, i livelli di servizio e i requisiti di gestione di tutti i servizi di rete devono essere identificati e inclusi in qualsiasi accordo con i fornitori di servizi di rete, in particolar modo in riferimento ai requisiti richiesti nell'ambito dei servizi rivolti al cliente.
Per il trasferimento di informazioni su reti pubbliche devono essere utilizzati canali sicuri (es. HTTPS). In base al livello di classificazione delle informazioni devono essere attivati controlli per verificare l'integrità e la non ripudiabilità dei dati.

- **Segregazione delle Reti**

Le reti di comunicazione devono essere separate fisicamente o logicamente a seconda dei servizi erogati.

- **Configurazione dei dispositivi di rete**

La configurazione dei dispositivi di rete viene definita secondo il principio di disabilitazione dei servizi e delle funzionalità non strettamente necessarie considerando inoltre le migliori pratiche di sicurezza e le raccomandazioni dei rispettivi vendor.
La password degli account di default deve essere modificata e l'account disabilitato.

- **Reti wireless**

Le reti wireless sono protette attraverso l'utilizzo di autenticazione e crittografia in linea con gli standard dell'industria.

- **Accessi da remoto**

L'accesso da remoto ai server deve:

- essere strettamente limitato nel tempo;
- controllato in riferimento a specifiche esigenze;
- avvenire utilizzando canali VPN SSL o IPSEC;
- avvenire solo attraverso endpoint verificati che rispettino le politiche di sicurezza aziendali (Antivirus, aggiornamenti automatici, firewall);
- prevedere la MFA (Multi Factor Autentication)

3.19 BACKUP

L'obiettivo di questa policy è di definire l'approccio utilizzato dall'organizzazione per consentire il recupero in caso di perdita di dati o sistemi.

Strutture di backup adeguate sono state previste al fine di garantire il recupero di tutte le informazioni e i software essenziali in seguito a un incidente, a un guasto o alla perdita dei supporti di memorizzazione. Pertanto, sono stati sviluppati e implementati piani per il backup delle informazioni, del software e dei sistemi dell'organizzazione.

I piani per il backup prevedono la produzione di registrazioni accurate e complete delle copie di backup e delle procedure di ripristino documentate. Esse riflettono i requisiti aziendali dell'organizzazione, i requisiti di sicurezza delle informazioni coinvolte e la criticità delle informazioni per il funzionamento continuo dell'organizzazione e nella frequenza dei backup.

I backup vengono custoditi in un luogo remoto e sicuro, a una distanza sufficiente per evitare i danni di un eventuale disastro nel sito principale, garantendo un livello adeguato di protezione fisica e ambientale, in linea con gli standard applicati al sito principale. Inoltre, mediante crittografia, viene garantita una protezione da rischi relativi alle informazioni la cui confidenzialità è importante.

I supporti di backup vengono testati periodicamente in modo da garantire che si possa fare affidamento su di essi in caso di emergenza. Inoltre, le misure di backup vengono testate regolarmente per garantire che soddisfino gli obiettivi dei piani di risposta agli incidenti e di continuità operativa, con relativo controllo delle procedure di ripristino.

Per i servizi cloud vengono effettuate copie di backup delle informazioni, delle applicazioni e dei sistemi dell'organizzazione nell'ambiente del servizio cloud.

3.20 CRITTOGRAFIA

Al fine di proteggere la riservatezza, l'autenticità e/o l'integrità delle informazioni Rekeep prevede l'utilizzo di idonei controlli crittografici. In particolare, per tutti i dati personali trattati è richiesta la valutazione circa l'adozione di controlli crittografici, in linea con le prescrizioni del GDPR.
Laddove ritenuto necessario, in riferimento all'analisi dei rischi cui sono esposti gli asset contenenti informazioni riservate, sono adottati metodi di crittografia.
Deve essere sempre garantita la crittografia nella trasmissione dei dati su reti pubbliche attraverso l'uso del protocollo HTTPS per la comunicazione sicura.

La robustezza dell'algoritmo di crittografia deve essere selezionata in funzione della riservatezza dei dati, su qualsiasi supporto esse di trovino.
Nella scelta devono essere valutati i rischi di impossibilità di ispezione di dati cifrati e il livello di accuratezza necessario per la gestione delle chiavi crittografiche lungo il loro intero ciclo di vita e le puntuali modalità di generazione delle chiavi, da adottare in caso di danneggiamento o perdita delle chiavi di decifratura. Nel caso in cui tali attività sono affidate a provider esterni, deve essere valutata l'adeguatezza delle procedure adottate in questo ambito dal fornitore.
Particolare attenzione deve essere prestata ai log degli amministratori di sistema e alle password associate ad utenze per l'accesso a sistemi aziendali critici che devono anch'esse essere adeguatamente protette attraverso meccanismi di crittografia.

Nell'implementazione di controlli e/o soluzioni di crittografia Rekeep dovrà tenere conto di:

- verificare se le capacità crittografiche soddisfano i requisiti di Rekeep.
- verificare che tali capacità siano compatibili con altre misure di protezione crittografica già utilizzate
- verificare l'applicazione delle capacità crittografiche che si applicano ai dati in riposo e in transito.

3.21 PROCEDURE DI CANCELLAZIONE DEI DATI

La distruzione dei documenti cartacei contenenti dati personali, il cui trattamento non trova più legittimazione, è assicurato tramite strumenti di tritatura documenti.

La cancellazione sicura dei dati sugli asset aziendali è assicurata mediante l'adozione di appositi tools e in generale secondo le modalità prescritte dai clienti con apposite clausole contrattuali.

3.22 SICUREZZA FISICA E AMBIENTALE

Tutte le risorse fisiche aziendali impiegate per l'elaborazione delle informazioni sensibili sono protette per impedire accessi fisici, danni e interferenze non autorizzate attraverso opportuni contratti di fornitura.
Per la scelta dei luoghi aziendali sono definiti i requisiti di sicurezza fisici e ambientali atti a garantire livelli di sicurezza adeguati. L'accesso ai locali aziendali è consentito solo a persone autorizzate. L'accesso dei dipendenti agli uffici è autorizzato e subordinato all'utilizzo del badge sul sistema automatico di controllo. Tutti i visitatori devono essere identificati da parte del personale Rekeep prima di consentirne l'accesso. Chiunque riceva un visitatore si assume la responsabilità sul suo operato e la sua condotta. I visitatori devono essere sempre accompagnati, in ingresso ed in uscita dalla sede. All'ingresso è depositato un Registro per tracciare gli ingressi dei visitatori.

4. DIFFUSIONE E MODIFICHE ALLA POLITICA

La Politica per la Sicurezza delle Informazioni è definita ed approvata dalla Direzione. Essa è pubblicata, comunicata ed applicata da tutto il personale afferente a Rekeep e dalle rilevanti parti interessate.
La Politica per la Sicurezza delle Informazioni è oggetto di revisione in sede di Riesame della Direzione, al fine di verificarne contenuti e la continua idoneità all'Organizzazione aziendale.

5. ACRONIMI

- ICT INFORMATION AND COMUNICATON TECHNOLOGY
- NIST National Institute of Standards and Technology

6. DOCUMENTI APPLICABILI

- Standard ISO\IEC 27001:2022 - Paragrafi: 5.1, 5.2, 6.2, 7.3
- Standard ISO\IEC 27001:2022 – Appendice A: Controlli: 5.1, 5.4, 5.36, 6.3, 6.4
- Standard ISO\IEC 27017:2015 – Appendice A: Controlli: CLD.9.5, CLD.13.1.4
- RKP.PG.06.18_BACKUP POLICY
- RKP.PG.06.24_GESTIONE DEL CICLO DI VITA DELL'UTENZA
- RKP.PG.04.03 CONTROLLO DELLE INFORMAZIONI DOCUMENTATE E CICLO DI VITA
- RKP.IO.04.06_IS_SICUREZZA DELLE INFORMAZIONI