# Politica per la Sicurezza delle Informazioni

(UNI EN ISO 27001:2014)

GPI
The Healthcare Partner

ARGENTEA

# La Sicurezza delle Informazioni

*riguarda la pianificazione, l'implementazione e il continuo miglioramento dei controlli di sicurezza e delle misure a tutela del dato personale che permettono di proteggere la riservatezza, l'integrità e la disponibilità delle risorse informative e dei relativi sistemi di informazione*.

Riservatezza: l'informazione deve essere nota solo a chi ne ha diritto

Integrità*:* l'informazione deve essere resa disponibile integra e senza modifiche effettuate da parte di persone non autorizzate

Disponibilità*:* l'informazione deve essere disponibile quando richiesta dalle persone autorizzate

Conformità*:* l'informazione deve essere trattata secondo le leggi in tema di sicurezza

# I nostri principi

# I nostri principi

Accurata **SELEZIONE DEL PERSONALE** addetto alla progettazione, sviluppo ed esercizio dei sistemi.

Mantenimento delle attività di analisi e gestione del **RISCHIO** allineate alle evoluzioni organizzative e tecnologiche dei sistemi e dei servizi.

Adesione alle politiche di salvaguardia dell'ambiente per lo smaltimento delle apparecchiature informatiche dismesse.

Presenza di **REGOLE, PROCEDURE E ATTIVITÀ DI CONTROLLO** interno riferite alla sicurezza dei dati gestiti e al rispetto delle procedure stesse.

Accurata selezione e monitoraggio dei **FORNITORI DI TECNOLOGIA** e di **SERVIZI CORRELATI ALL'EROGAZIONE/GESTIONE** dei sistemi e dei servizi.

Scelta di **STANDARD TECNOLOGICI** adeguati ed affidabili per la corretta protezione delle informazioni e della qualità delle attività.

Impegno e supporto per essere **CONFORMI** alla legislazione applicabile in materia di protezione delle informazioni e rispettare i termini contrattuali con i propri clienti.

Rispetto delle **NORME** che a qualsiasi titolo prescrivono specifici requisiti di sicurezza delle informazioni finalizzati alla tutela del dato personale - quali ad esempio il D.Lgs. 196/2003, il Regolamento UE 2016/679, il D.Lgs. 101/2018 e le norme ISO-IEC 270xx.

# Incident Management

# Incidenti di Sicurezza

**EVENTO E INCIDENTE**

Un **evento** relativo alla sicurezza delle informazioni è un evento che indica una possibile violazione della sicurezza delle informazioni o fallimento dei controlli.

Un **incidente** relativo alla sicurezza delle informazioni è l'insieme di uno o più eventi di sicurezza delle informazioni correlati e identificati che possono danneggiare i sistemi di informazione e/o le risorse di dati o comprometterne le funzionalità. In generale sono eventi di sicurezza delle informazioni che hanno impatti più o meno gravi per il business aziendale.

**ARGENTEA CONSIDERA GLI INCIDENTI DI SICUREZZA UN IMPORTANTE RISCHIO PER IL PROPRIO BUSINESS E PERTANTO HA:**

- implementato un piano di gestione degli incidenti e le procedure per affrontare le necessarie indagini di follow-up;
- individuato la struttura organizzativa per la gestione degli eventi e degli incidenti, definendo i componenti, le competenze e le modalità operative per il risoluzione del problema e l'eventuale ingaggio dell'ECAB Emergency Change Advisory Board (ECAB).

Questo al fine di evitare, per quanto possibile, l'accadimento di incidenti e, nel caso questi accadessero, di essere in grado di gestirli e di individuare le azioni necessarie per ridurre il rischio del ri-verificarsi dell'incidente.

Gli incidenti di sicurezza si verificano a causa di eventi imprevedibili e dirompenti. Nei casi in cui gli eventi di sicurezza compromettano la continuità aziendale o creino rischi di sicurezza dei dati, la Funzione di Sicurezza deve attivare il piano di gestione degli incidenti per:

**identificare, gestire, registrare ed analizzare**

minacce, attacchi o incidenti di sicurezza in tempo reale, così come descritto all'interno della procedura di gestione degli incidenti.

# Dichiarazione e Responsabilità

# Dichiarazione e Responsabilità

**INFORMAZIONI COME RISORSA AZIENDALE**

Argentea considera le informazioni una risorsa aziendale che deve essere **PROTETTA** in quanto costituiscono parte essenziale per lo svolgimento dell'attività aziendale. Data la tipologia di attività svolta e la natura dei dati trattati, ritiene di importanza fondamentale la tutela dei dati personali. Tutti i dati e le relative elaborazioni per la gestione delle attività devono essere protetti per garantire che giungano **INTEGRI** a chi deve utilizzarli, che **NON VADANO DISPERSI** o che **NON VENGANO DIVULGATI** a soggetti non autorizzati.

Argentea ha impostato un sistema efficiente di sicurezza delle informazioni, atto a ridurre i rischi e le probabilità che si verifichino danni ad un livello ed un costo eccessivi. Questo permette all'azienda di assicurare la continuità delle proprie attività, minimizzare i rischi, garantire il ritorno degli investimenti, le opportunità di business, il rispetto delle leggi e la redditività. Attraverso la valutazione dei rischi, Argentea si propone di rispondere ad ogni minaccia al proprio patrimonio informativo con misure di sicurezza più adeguate, **STANZIANDO PER QUESTE UN BUDGET SUFFICIENTE**.

La sicurezza delle informazioni e la tutela dei dati personali costituiscono un processo sia tecnologico che organizzativo, e di conseguenza Argentea, con la collaborazione del Gruppo GPI, ha predisposto una serie di procedure operative standard unitamente ad attività formativa rivolta al proprio personale addetto. Le politiche di sicurezza, le procedure operative e la valutazione dei rischi sono rivedute ed eventualmente aggiornate con periodicità almeno annuale, per riflettere nuovi indirizzi, evoluzioni e normative pertinenti.

È stato implementato il **SISTEMA DI GESTIONE DI SICUREZZA DELLE INFORMAZIONI**, in conformità alla Norma UNI CEI ISO/IEC 27001:2014, e alle linee guida UNI CEI ISO/IEC 27017 e UNI CEI ISO/IEC 27018, cioè un sistema di operazioni e di controlli per gestire il rischio.

# Dichiarazione e Responsabilità

In particolare, con l'implementazione di questo sistema:

- Vengono **ANALIZZATI I RISCHI**, sulla base dei principi di **riservatezza**, **disponibilità** e **integrità**, al fine di garantire una adeguata **tutela dei dati personali**;
- Vengono **TRATTATI I RISCHI** sulla base di criteri di accettazione dei rischi stessi, in ogni caso non compromettendo il rispetto delle leggi dello Stato ed i requisiti contrattuali;
- Vengono **RESI CONSAPEVOLI** tutte le risorse e i dipendenti della necessità di operare responsabilmente mediante formazione a tutti i livelli;
- Vengono introdotte specifiche **ATTIVITÀ DI CONTROLLO** e vengono prese precauzioni contro i disastri;
- Vengono presi adeguati **PROVVEDIMENTI** ogni qualvolta si verificheranno delle violazioni;
- Nell'ambito di questo sistema sono assegnate le seguenti responsabilità:

- Alla **Direzione** per definire il dominio degli Asset da proteggere;
- Al **Responsabile SGSI** per valutare i rischi cui possono essere esposti i vari Asset;
- Al **Responsabili SGSI e ai Responsabili dei vari Servizi**, per impostare i controlli, implementarli e monitorarli;
- Al **Responsabile SGSI** per registrare tutte le minacce verificatesi, pianificare e implementare nuovi controlli;
- Ad **ogni dipendente**, perché si attenga alle autorizzazioni prescritte e segnali al Responsabile SGSI eventuali minacce riscontrate;
- Alla **Direzione** di riesaminare periodicamente lo stato di sicurezza delle informazioni e l'efficacia della presente politica;
- Alla **Direzione**, al **Responsabile SGSI e Qualità**, e ad **ogni dipendente** di intraprendere azioni di miglioramento.

# POLITICA PER LA SICUREZZA DELLE INFORMAZIONI (UNI EN ISO 27001:2014)

**CODIFICA DOCUMENTO**

000.POL.0012.1.0-POLITICA PER SICUREZZA DELLE INFORMAZONI

**LISTA DI DISTRIBUZIONE**

Tutti i dipendenti di Argentea
CDA Argentea
Responsabile Sicurezza Sistemi
Responsabile ASA Tecnologici
Responsabile Qualità GPI

**TABELLA AGGIORNAMENTO**

| STATO | REDATTO AGGIORNATO DA | RIVISTO E APPROVATO DA | VALIDATO DA UFF. QUALITA' |
|---|---|---|---|
| Prima Emissione | F.Cherotti | M.Torresani | NO |
| | 30/08/2021 | 06/09/2021 | |

**STORIA DELLE MODIFICHE APPORTATE**

| VERSIONE | DATA | PARAGRAFO | MODIFICHE |
|---|---|---|---|
| 1.0 | 06/09/2021 | - | Prima emissione |