ISO/IEC 27001:2022

"Sicurezza delle informazioni, cybersecurity e protezione della privacy - Sistemi di gestione per la sicurezza delle informazioni - Requisiti"

MOD-520-SI

Politica della Sicurezza delle Informazioni

Master	√
Copia controllata	X
Copia non controllata	√
Numero della copia	**01**
Etichetta	**0**

Stato di aggiornamento della Politica

Rev.	Data	Pagine modificate	Autore modifica	Revisionato	Approvato
00	25/08/2023	Prima stesura	Francesca Bucci	Francesca Bucci (RSGQ)	Di Florio Claudio (DG)

Indice generale della Politica

Politica per la Sicurezza delle Informazioni

1. Premessa generale

Arpes Srl è una Consulting e Tech Company operante sul mercato dal 1970. Inizialmente focalizzata sulla Consulenza Strategica, con focus nel settore agricolo e agroindustriale, ha nel corso degli anni ampliato il proprio business introducendo gradualmente attività di progettazione e sviluppo software, a cui si sono aggiunti recentemente servizi per la gestione ambientale e del territorio basati su tecnologie ICT.

La Mission aziendale è la piena condivisione dei progetti di sviluppo di imprese e pubblica amministrazione, la meticolosa realizzazione degli obiettivi concordati e la capacità di seguire i clienti con impegno, entusiasmo e creatività.

Considerato l'ambito di attività, l'Alta Direzione di Arpes srl riconosce l'importanza della Sicurezza delle Informazioni poiché costituisce un elemento cruciale per assicurare il rispetto e la massima soddisfazione dei Clienti, nonché di tutte le altre parti interessate.

A tal fine, Arpes srl ha formulato la propria "Politica per la Sicurezza delle Informazioni", sottolineando che ***la sicurezza delle informazioni e la protezione dei dati personali rappresenta una responsabilità prioritaria nei confronti di tutti gli Stakeholder***.

L'impegno della leadership nei confronti del Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) è integrato in ogni aspetto delle attività dell'organizzazione ed è esteso a tutte le fasi coinvolte nella fornitura dei propri prodotti e servizi.

2. Scopo

L'azienda Arpes srl, già certificata secondo gli standard UNI EN ISO 9001:2015 e UNI EN ISO 14001:2015, ha deciso di istituire un Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) conforme ai requisiti espressi dalla norma ISO/IEC 27001:2022 al fine di garantire e proteggere i dati e le informazioni dalle possibili minacce, attraverso un processo continuo di valutazione e gestione dei rischi e delle opportunità.

Attraverso l'attuazione di questa politica per la sicurezza delle informazioni Arpes intende ottemperare all'impegno di conformità alla normativa ISO/IEC 27001:2022 nonché a conseguire e mantenere tale certificazione.

Lo scopo del presente documento è quello di descrivere i principi generali di sicurezza delle informazioni definiti da Arpes srl al fine di sviluppare un efficiente e sicuro Sistema di gestione della Sicurezza delle informazioni (SGSI), nonché stabilire il quadro di riferimento per gli obiettivi da perseguire e l'impegno della Direzione al soddisfacimento dei requisiti applicabili e al miglioramento continuo delle prestazioni.

3. Ambito di applicazione

La politica per la sicurezza delle informazioni si applica a tutto il personale interno, alle terze parti che collaborano alla gestione delle informazioni e a tutti i processi e risorse coinvolte nella progettazione, realizzazione, avviamento ed erogazione continuativa dei seguenti prodotti/servizi aziendali:

- ✓ Consulting strategico ed economico-finanziario
- ✓ Consulenza IT, progettazione e sviluppo software, assistenza e manutenzione
- ✓ Servizi di analisi ambientale e pianificazione territoriale

4. Principi generali di sicurezza delle informazioni

La politica per la sicurezza delle informazioni adottata da Arpes srl rappresenta l'impegno dell'organizzazione nei confronti di clienti e terze parti a garantire la sicurezza delle informazioni e dei dati personali, degli strumenti fisici, logici e organizzativi atti al trattamento delle informazioni in tutte le attività aziendali.

Pertanto, tutte le persone che lavorano e/o collaborano con Arpes srl sono impegnate a rispettare i seguenti principi:

1. **Riservatezza**: assicurare che l'informazione sia accessibile solamente ai soggetti e/o ai processi debitamente autorizzati;
2. **Integrità**: salvaguardare la consistenza dell'informazione da modifiche non autorizzate e garantire che l'informazione non subisca modifiche o cancellazioni a seguito di errori o di azioni volontarie, ma anche a seguito di malfunzionamenti o danni dei sistemi tecnologici;
3. **Disponibilità**: assicurare che gli utenti autorizzati abbiano accesso alle informazioni quando ne fanno richiesta;
4. **Controllo**: assicurare che la gestione dei dati avvenga sempre attraverso processi e strumenti sicuri e testati;
5. **Autenticità**: garantire una provenienza affidabile dell'informazione;
6. **Privacy**: garantire la protezione e di controllo dei dati personali.

La Direzione è fortemente impegnata a una grande responsabilizzazione di tutte le persone che lavorano per e con Arpes nel garantire la rigorosità del proprio operato per adempiere, con la massima attenzione, ai compiti assegnati.

La responsabilità finale della sicurezza delle informazioni ricade sulla Direzione che ha delegato il Responsabile del sistema di gestione della sicurezza delle informazioni, il Responsabile IT ed i referenti di ciascuna unità organizzativa coinvolta ad attuare quanto necessario.

5. Obiettivi del sistema di gestione delle informazioni

Arpes srl è convinta che garantire la protezione dei dati e la tutela del patrimonio informativo dell'azienda è essenziale per gestire correttamente i rapporti con i Clienti e con le persone fisiche di cui si trattano i dati personali. Per questo motivo le Informazioni devono essere adeguatamente protette equilibrando il livello di rischio accettato con il grado di protezione richiesto. In questo modo, si tutela il valore delle Informazioni e si assicura l'efficienza, l'efficacia e la continuità dei processi aziendali.

A tal fine, la Direzione definisce il seguente quadro di riferimento per determinare gli obiettivi per la sicurezza delle informazioni:

1. garantire all'organizzazione la piena conoscenza delle informazioni da esse gestite e la valutazione della loro criticità, al fine di agevolare l'implementazione degli adeguati livelli di protezione;
2. garantire l'accesso sicuro alle informazioni, al fine di prevenire trattamenti non autorizzati o realizzati senza i diritti necessari;
3. garantire che l'organizzazione e le terze parti collaborino al trattamento delle informazioni adottando procedure volte al rispetto di adeguati livelli di sicurezza;
4. garantire che l'organizzazione e le terze parti che collaborano al trattamento delle informazioni abbiano piena consapevolezza delle problematiche relative alla sicurezza;
5. garantire che le anomalie e gli incidenti aventi ripercussioni sul sistema informativo e sui livelli di sicurezza aziendale siano tempestivamente riconosciuti e correttamente gestiti, attraverso efficienti sistemi di prevenzione, comunicazione e reazione al fine di minimizzare l'impatto sul business;
6. garantire la conformità con i requisiti di legge ed il rispetto degli impegni di sicurezza stabiliti nei contratti con le terze parti;
7. garantire la rilevazione di eventi anomali, incidenti e vulnerabilità dei sistemi informativi in modo da rispettare la sicurezza e la disponibilità dei servizi e delle informazioni.
8. Garantire la business continuity aziendale e il disaster recovery, attraverso l'applicazione di procedure di sicurezza stabilite.

6. Conformità al Regolamento GDPR e Codice Privacy

Arpes considera cruciale garantire il rispetto dei principi di legge sulla protezione dei dati personali, come stabilito dal Regolamento GDPR e dal Codice Privacy per fornire alla propria clientela servizi basati sulla "privacy by design", affrontando le principali questioni giuridiche, sia di natura legale che contrattuale, legate alla gestione dei Dati Personali.

Arpes mira a offrire ai propri clienti prodotti e servizi del più alto livello sia in termini di qualità che di sicurezza delle informazioni e Dati Personali garantendo la loro protezione da tutte le minacce, che possano essere interne o esterne, intenzionali o accidentali. In questo contesto, perseguire la conformità con le leggi sulla protezione dei dati è una parte integrante della missione di Arpes che contribuisce significativamente alla sicurezza e all'affidabilità delle operazioni svolte per il Cliente.

7. Standard di Riferimento

Basandosi sui propri obiettivi aziendali, Arpes ha scelto di proteggere le proprie Informazioni e quelle affidatele dai clienti seguendo standard riconosciuti, metodologie consolidate, leggi e regolamenti. La protezione delle Informazioni si può ottenere applicando misure tecniche ed impostando con costanza ed efficacia politiche, processi e procedure aziendali.

Partendo da queste convinzioni, Arpes ha deciso l'implementazione di un Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) in conformità ai seguenti standard volontari:

- **Norma ISO 27001**, la norma internazionale che stabilisce i requisiti per un Sistema di Gestione della Sicurezza delle Informazioni (SGSI)**.** Un SGSI è un insieme di politiche, procedure e controlli che

un'organizzazione utilizza per proteggere le proprie Informazioni da una vasta gamma di minacce, tra cui furti, violazioni dei dati e attacchi informatici.

- **Linee guida ISO 27002** che forniscono una raccolta di "best practices" che possono essere adottate per soddisfare i requisiti della norma ISO 27001 al fine di proteggere le risorse informative.

- Norma ISO 9001 che stabilisce i requisiti per un sistema di gestione per la qualità. Un sistema di gestione per la qualità è un insieme di processi, procedure e risorse che un'organizzazione utilizza per garantire che i propri prodotti e servizi soddisfino i requisiti dei Clienti e le normative applicabili

- Regolamento (UE) 2016/679 (GDPR) che stabilisce i requisiti per un sistema di gestione del trattamento dei dati personali relativi alle persone nell'UE, da parte di persone, società o organizzazioni.

8. Leadership

La Direzione è responsabile del sistema di gestione sicura delle informazioni e dei dati personali, in coerenza con l'evoluzione del contesto aziendale e di mercato, valutando eventuali azioni da intraprendere a fronte di eventi come:

- ✓ Evoluzioni del business significative
- ✓ Nuove minacce o opportunità rispetto a quelle già individuate e riportate nell'Analisi dei rischi per la sicurezza
- ✓ Significativi incidenti di sicurezza
- ✓ Evoluzione del contesto normativo o legislativo in materia di trattamento sicuro delle informazioni e dei dati personali

La Direzione si impegna attivamente integrando il Sistema di Gestione nella cultura aziendale, stabilendo obiettivi e politiche, assegnando responsabilità e assicurandosi che gli obiettivi pianificati siano compatibili con il contesto e gli indirizzi strategici dell'organizzazione.

Si impegna a fornire le risorse necessarie per l'implementazione e il mantenimento del sistema di gestione, inclusa la formazione del personale e l'infrastruttura.

Si impegna inoltre a comunicare l'importanza del SGSI e a coinvolgere attivamente tutte le parti interessate, coordinandole, sostenendole e impegnandosi a definire e diffondere informazioni documentate chiare, atte ad assicurare un funzionamento efficace ed efficiente dei processi.

La Direzione, infine, è responsabile del monitoraggio costante delle performance del sistema di gestione, prendendo decisioni basate sui dati e impegnandosi nel miglioramento continuo.

9. Miglioramento Continuo

La Direzione sottopone periodicamente a riesame i risultati raggiunti in relazione agli obiettivi e alle politiche stabilite. Queste revisioni comprendono analisi dei dati, audit interni, feedback dei clienti e altre valutazioni.

Nel caso emergessero opportunità di miglioramento durante il monitoraggio, l'organizzazione si impegna ad attuare misure correttive e preventive per garantire un costante ed efficace miglioramento del proprio Sistema di Gestione della Sicurezza delle Informazioni.

La leadership dell'organizzazione gioca un ruolo chiave nel promuovere l'impegno per il miglioramento continuo. Questo coinvolgimento può tradursi nella definizione di obiettivi chiari, nell'allocazione di risorse e nel sostegno attivo alle iniziative di miglioramento.

10. Diffusione e comunicazione della Politica

La Direzione si impegna a far comprendere e attua la presente politica non solo tra il personale interno, ma anche tra collaboratori, consulenti e fornitori, con particolare attenzione a chiunque sia in qualsiasi modo coinvolto nel trattamento delle Informazioni e dei dati personali che rientrano nel campo di applicazione del Sistema di Gestione della Sicurezza delle Informazioni di Arpes.

La politica della sicurezza delle informazioni è, dunque, formalizzata nel SGSI e viene costantemente revisionata per assicurare il suo continuo miglioramento e per garantire la sua idoneità alle attività e alle capacità dell'azienda di soddisfare Clienti e parti interessate.

Essa è condivisa con l'organizzazione, le terze parti ed i clienti, attraverso un sistema di condivisione interna (Google drive) e specifici canali di comunicazione.

11. Impegni della Politica di sicurezza delle informazioni

Tutto il personale di Arpes si impegna a:

- ✓ Rispettare tutte le leggi applicabili in materia di tutela delle informazioni e dei dati personali ed ottemperare agli altri obblighi di conformità di parti interessate;
- ✓ Mantenere costantemente monitorato e aggiornato il sistema di gestione della Sicurezza delle Informazioni;
- ✓ Assicurare la conformità dei comportamenti alle norme e leggi di natura cogente e volontaria in materia di tutela e sicurezza delle informazioni e dati;
- ✓ Adottare dei comportamenti allineati alle linee guida stabilite dalla Direzione, al fine di ridurre il rischio di condivisione e diffusione del patrimonio informativo aziendale;
- ✓ Perseguire il miglioramento continuo e gli obiettivi stabiliti dalla Direzione.

Isernia, 25 Agosto 2023

La Direzione