POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

PRESENTAZIONE

La Confagricoltura Trentina per agevolare il perseguimento delle proprie finalità statutarie ha costituito il CAA Agricoltura Trentina Servizi S.r.l (Centro di Assistenza Agricola).

CAA Agricoltura Trentina Servizi S.r.l, Centro Autorizzato di Assistenza Agricola autorizzato, cura per conto dei propri utenti le attività di servizio previste da apposite convenzioni con l'organismo pagatore provinciale. Agli imprenditori agricoli assicura, con proprio personale qualificato, assistenza per accedere agli aiuti comunitari, nazionali e provinciali, garantisce una informativa costante e aggiornata sulle opportunità e benefici previsti dalla Politica Agricola Comunitaria.

L'obiettivo primario è stato quello di assicurare agli operatori del settore agricolo pronte erogazioni degli aiuti comunitari previsti dalla regolamentazione comunitaria vigente, coprendo sul territorio regionale, sportelli operativi presso i quali l'agricoltore possa inoltrare le specifiche domande.

Attraverso l'operato di CAA Agricoltura Trentina Servizi S.r.l. si garantisce che l'agricoltore che si rivolge presso uno degli sportelli dedicati avrà la certezza di poter usufruire di un servizio erogato rispettando la normativa vigente e caratterizzato da standard di sicurezza delle informazioni elevati.

SICUREZZA DELLE INFORMAZIONI

Per affrontare le sfide in evoluzione, tutelare gli interessi delle nostre parti interessate e raggiungere gli obiettivi strategici, attraverso la presente dichiarazione esprimiamo il nostro impegno a proteggere la sicurezza del patrimonio informativo mediante l'adozione di un Sistema di Gestione della Sicurezza delle Informazioni (SGSI) conforme alla norma internazionale ISO/IEC 27001:2022.

Questo sistema ha l'obiettivo di:

- Assicurare alle parti coinvolte un livello adeguato di protezione dei dati e delle informazioni.
- Potenziare la sicurezza delle informazioni trattate, anche attraverso la gestione degli eventi critici e delle debolezze del sistema.
- Gestire in modo strutturato i rapporti con fornitori esterni e soggetti terzi.
- Sorvegliare e ottimizzare la protezione dei servizi offerti.

Il sistema consente di mantenere un impianto organizzativo solido e completo per:

- individuare e analizzare i rischi legati alla sicurezza delle informazioni
- scegliere ed implementare le misure di sicurezza più idonee
- valutare e accrescere costantemente l'efficacia dei controlli adottati
- garantire il rispetto delle normative e degli obblighi legali applicabili

IMPEGNO DELL'ORGANIZZAZIONE

Il nostro impegno è volto a:

• Rispondere pienamente alle disposizioni normative, agli obblighi contrattuali, alle aspettative degli stakeholder e alle regole interne dell'organizzazione.
• Fondere i principi cardine della protezione delle informazioni all'interno delle attività operative e della visione strategica aziendale.

• Elaborare procedure e strumenti finalizzati all'attuazione concreta della politica di sicurezza informativa.
• Mobilitare e responsabilizzare il personale, valorizzando la leadership, incentivando l'engagement e la partecipazione proattiva, garantendo percorsi di aggiornamento continuo.
• Salvaguardare i dati aziendali e personali, proteggendo il capitale informativo e assicurando un'adeguata difesa delle informazioni e dei sistemi informatici, tutelando:

✓ **Riservatezza**: Evitare accessi non autorizzati e consentire la fruizione dei dati solo a chi ne ha titolo.

✓ **Integrità**: Mantenere l'affidabilità e la correttezza delle modifiche apportate alle informazioni.

✓ **Disponibilità**: Fornire l'accesso ai dati secondo le esigenze operative e le prescrizioni di legge.

• Stimolare il dialogo e la cooperazione con tutte le parti interessate, condividendo valori e approcci comuni in tema di sicurezza.

• Affrontare e contenere i rischi connessi alla sicurezza, preservando la confidenzialità, la coerenza e l'accessibilità delle informazioni.

• Valutare, gestire e trarre vantaggio in termini di apprendimento dagli incidenti informatici, pianificando risposte pronte ed efficaci.

• Accrescere costantemente le prestazioni del SGSI, applicando interventi preventivi e correttivi in base alle criticità individuate.

• Potenziare in modo continuo il Sistema di Gestione della Sicurezza delle Informazioni (SGSI), adottando misure preventive e correttive sulla base delle vulnerabilità rilevate.

PRINCIPI FONDAMENTALI DEL SGSI

Il successo del SGSI si basa sui seguenti principi fondamentali:

1. Consapevolezza della necessità della sicurezza delle informazioni a tutti i livelli organizzativi.
2. Attribuzione chiara delle responsabilità per garantire un'efficace protezione delle informazioni.
3. Impegno del management e allineamento con gli interessi degli stakeholder per promuovere una cultura della sicurezza.
4. Miglioramento continuo dei valori societari, integrando la sicurezza delle informazioni nelle strategie aziendali.
5. Valutazione del rischio per implementare controlli adeguati e mantenere il rischio a livelli accettabili.
6. Sicurezza incorporata come elemento essenziale delle reti informatiche e dei sistemi aziendali.
7. Prevenzione attiva e tempestiva individuazione degli incidenti di sicurezza delle informazioni.
8. Adozione di un approccio globale alla gestione della sicurezza, garantendo coerenza e integrazione con altri processi aziendali.
9. Rivalutazione continua della sicurezza delle informazioni, con aggiornamenti e miglioramenti in base alle necessità e ai contesti.

Per garantire il rispetto dei principi fondamentali, ci siamo dotati di:

- Una struttura organizzativa con attribuzione chiara delle responsabilità per garantire un'efficace protezione delle informazioni.
- Regolamenti interni a garanzia del rispetto del Provvedimento Generale del Garante della Privacy del 10/03/2007 che raccomanda alle imprese l'adozione di un "Regolamento Interno" nel quale siano chiaramente indicate le regole per l'uso di Internet e della posta elettronica, unitamente alle disposizioni in materia di protezione e sicurezza dei dati personali trattati con strumenti elettronici di cui al Regolamento 679/2016 UE (GDPR).

- Procedure per identificare, analizzare, valutare i rischi, selezionare l'opzione di trattamento adeguata e adottare misure di mitigazione efficaci.
- Regole che ciascun utente è tenuto a rispettare, per evitare che comportamenti anche inconsapevoli possano innescare problemi o minacce alla sicurezza del sistema informativo, agli strumenti, ai dispositivi mobili e violazione dei dati personali soggetti a trattamento;
- Politiche per la comunicazione chiara e trasparente nei confronti degli utenti sulle finalità e le modalità dei controlli effettuati dalla Società e sulle specifiche tecnologie adottate per la loro effettuazione.
- Misure per la protezione fisica e organizzativa con l'obiettivo di garantire la sicurezza nei locali aziendali e la protezione delle informazioni anche su supporto cartaceo.
- Procedure per la gestione degli incidenti di sicurezza e dei data-breach, al fine di migliorare su base continua il proprio modello organizzativo e prevenire violazioni, identificare tempestivamente gli eventi critici per la sicurezza e adottare sistemi di prevenzione, monitoraggio e risposta per minimizzare gli impatti, anche in conformità ai requisiti cogenti.

Trento, 07/05/2025 **La Direzione**