C.A.A. CONFAGRICOLTURA TOSCANA s.r.l.

POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

PRESENTAZIONE

La Confagricoltura Toscana per agevolare il perseguimento delle proprie finalità statutarie ha costituito il CAA Confagricoltura Toscana (Centro di Assistenza Agricola).

C.A.A. Confagricoltura Toscana, Centro Autorizzato di Assistenza Agricola autorizzato dalla Regione Toscana con decreto della Giunta regionale toscana n. 2375 del 18/04/2003 e modificato con decreto n. 150 28/01/2013, gestisce per conto dei propri utenti le attività previste da apposite convenzioni con organismi pagatori o Amministrazioni Regionali, in particolare:

- costituzione e tenuta del fascicolo aziendale;
- ricezione domande presentate alla pubblica amministrazione;
- assistenza alla compilazione.

Confagricoltura Toscana o "Federazione Toscana degli Agricoltori" è formata dalle Unioni Provinciali Agricoltori della Toscana. Concorre a costituire la Confederazione Generale dell'Agricoltura Italiana che nel riconoscere nell'imprenditore agricolo il protagonista della produzione, persegue gli obiettivi generali dello sviluppo economico, sociale e tecnologico dell'agricoltura.

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 C.A.A. Confagricoltura Toscana e delle sedi dislocate sul territorio regionale 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

Al fine di affrontare le sfide emergenti, salvaguardare gli interessi dei nostri stakeholders e conseguire gli obiettivi strategici con la presente politica manifestiamo l'impegno per la tutela della sicurezza del patrimonio informativo adottando un Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) conforme allo standard internazionale ISO/IEC 27001:2022.

Tale sistema è finalizzato a:

- Garantire alle parti interessate un'adeguata tutela delle informazioni.

- Migliorare la sicurezza delle informazioni gestite, anche tramite il controllo degli incidenti e delle vulnerabilità.
- Regolamentare efficacemente i rapporti con fornitori e outsourcer.
- Monitorare e migliorare la sicurezza dei servizi erogati.
- Mantenere un quadro strutturato e completo per:
    1. l'identificazione e la valutazione dei rischi per la sicurezza delle informazioni
    2. la selezione e l'applicazione di controlli applicabili
    3. la misurazione e il miglioramento della loro efficacia
- raggiungere efficacemente la conformità legale e normativa

IMPEGNO DELL'ORGANIZZAZIONE

Ci impegniamo a:

- Soddisfare la piena conformità ai requisiti normativi, a quelli contrattuali, ai requisiti dei propri stakeholders e alle regolamentazioni interne.
- Integrare i principi fondamentali della sicurezza delle informazioni nei processi aziendali e nella strategia d'impresa.
- Definire processi e misure per attuare la politica di sicurezza delle informazioni.
- Coinvolgere e sensibilizzare il personale, promuovendo la leadership, la motivazione e la partecipazione attiva, e assicurando la formazione continua.
- Proteggere i dati aziendali e personali, salvaguardando il patrimonio informativo e garantire un adeguato livello di protezione delle informazioni e dei servizi informativi, attraverso la tutela della:
    - **Riservatezza:** Protezione delle informazioni da accessi impropri e utilizzo solo da parte di soggetti autorizzati.
    - **Integrità**: Assicurare l'accuratezza e la legittimità delle modifiche ai dati.
    - **Disponibilità:** Garantire l'accesso alle informazioni in base alle esigenze operative e normative.
- Favorire la collaborazione con le parti interessate, condividendo principi e strategie per la sicurezza.
- Gestire e mitigare i rischi, proteggendo la riservatezza, l'integrità e la disponibilità delle informazioni.
- Analizzare, gestire e apprendere dagli incidenti di sicurezza, sviluppando risposte efficaci.
- Migliorare continuamente il SGSI, adottando misure preventive e correttive in base alle vulnerabilità identificate.

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.

Lì 18/3/2025

La Direzione