ECOCERVED
società consortile a responsabilità limitata

Documento Pubblico

Misure di sicurezza adottate da Ecocerved

Informazioni generali
Ecocerved S.C.A.R.L. Tel: 051 / 63 16 700 contatto DPO/RPD[1]: dpo@ecocerved.it

La sicurezza delle informazioni e la protezione dei dati sono elementi fondamentali per garantire l'integrità, la riservatezza e la disponibilità delle risorse aziendali e dei clienti. Questo documento descrive le misure di sicurezza tecniche e organizzative adottate dalla nostra organizzazione per proteggere i dati e ridurre i rischi associati a potenziali minacce informatiche e operazionali.

Le nostre pratiche si basano su standard internazionali riconosciuti, in particolare:

- **ISO/IEC 27001**: per la gestione della sicurezza delle informazioni, attraverso un approccio strutturato per identificare, prevenire e mitigare i rischi.
- **ISO/IEC 27701**: per la gestione della privacy e la protezione dei dati personali, garantendo conformità ai requisiti normativi e alle migliori pratiche internazionali.

Ecocerved è dotata di un proprio Sistema di gestione integrato in costante aggiornamento in relazione allo stato del progresso tecnico, certificato secondo gli Standard ISO 27001 Sistema di gestione della sicurezza delle informazioni e ISO 9001, periodicamente verificati da un Organismo di Certificazione accreditato.

Il documento illustra anche i principali passi procedurali relativi alla **procedura di gestione degli incidenti**, che definisce i passaggi da seguire in caso di eventi che possano compromettere la sicurezza o la continuità aziendale e il **piano di continuità operativa**, che garantisce la resilienza dell'azienda e la capacità di rispondere rapidamente a situazioni di emergenza o crisi.

[1] Il servizio di Data protection officer affidato alla Società Xifram Srl della quale era stato individuato l'Avv. Riccardo Rocca come DPO di Ecocerved Scarl è terminato. Il servizio è stato affidato dal 25 luglio 2025 ad AIZOON CONSULTING SRL, che ha individuato, quale referente del DPO, Ercole Dalmanzio.

Controlli ISO/IEC 27001

Di seguito viene riportato l'elenco dei controlli relativi alla sicurezza delle informazioni applicati:

Controllo
05.01.01 Politiche per la sicurezza delle informazioni - con estensione ISO/IEC 27701
05.01.02 Politiche per la sicurezza delle informazioni - Riesame
05.02 Ruoli e responsabilità per la sicurezza delle informazioni - con estensione ISO/IEC 27701
05.03 Separazione dei compiti
05.04 Responsabilità della direzione
05.05 Contatti con le autorità
05.06 Contatti con gruppi di interesse
05.07 Monitoraggio delle minacce
05.08 Sicurezza delle informazioni nella gestione dei progetti
05.09.01 Inventario delle informazioni e degli altri asset associati
05.09.02 Inventario - Responsabilità
05.10.01 Uso accettabile delle informazioni e degli altri asset associati
05.10.02 Uso accettabile delle informazioni e degli altri asset associati - Relazioni con la classificazione
05.11 Restituzione degli asset
05.12 Classificazione delle informazioni - con estensione ISO/IEC 27701
05.13 Etichettatura delle informazioni - con estensione ISO/IEC 27701
05.14.01 Trasferimento delle informazioni - Regole interne - con estensione ISO/IEC 27701
05.14.02 Trasferimento delle informazioni - Accordi con altri
05.14.03 Trasferimento delle informazioni - Trasferimento elettronico
05.14.04 Trasferimento delle informazioni - Trasferimento fisico - con estensione ISO/IEC 27701
05.14.05 Trasferimento delle informazioni - Trasferimento orale
05.15.01 Controllo degli accessi
05.15.02 Controllo degli accessi - Servizi di rete
05.16 Gestione delle identità - con estensione ISO/IEC 27701
05.17.01 Informazioni di autenticazione - Allocazione
05.17.02 Informazioni di autenticazione - Responsabilità degli utenti
05.17.03 Informazioni di autenticazione - Sistema di gestione delle password
05.18.01 Diritti di accesso - Assegnazione - con estensione ISO/IEC 27701
05.18.02 Diritti di accesso - Riesame
05.18.03 Diritti di accesso - Cambiamento o cessazione del rapporto di impiego
05.19 Sicurezza delle informazioni nelle relazioni con i fornitori
05.20 Sicurezza delle informazioni negli accordi con i fornitori - con estensione ISO/IEC 27701
05.21 Gestione della sicurezza delle informazioni nella filiera di fornitura per l'ICT
05.22.01 Monitoraggio, riesame e gestione dei cambiamenti dei servizi dei fornitori - Monitoraggio e riesame
05.22.02 Monitoraggio, riesame e gestione dei cambiamenti dei servizi dei fornitori - Cambiamenti
05.23 Sicurezza delle informazioni per l'utilizzo dei servizi cloud
05.24.01 Pianificazione e preparazione per la gestione degli incidenti relativi alla sicurezza delle informazioni - Procedure - con estensione ISO/IEC 27701
05.24.02 Pianificazione e preparazione per la gestione degli incidenti relativi alla sicurezza delle informazioni - Report
05.25 Valutazione e decisione sugli eventi relativi alla sicurezza delle informazioni
05.26 Risposta agli incidenti relativi alla sicurezza delle informazioni - con estensione ISO/IEC 27701
05.27 Apprendimento dagli incidenti relativi alla sicurezza delle informazioni
05.28 Raccolta di prove
05.29.01 Sicurezza delle informazioni durante le interruzioni - BIA

05.29.02 Sicurezza delle informazioni durante le interruzioni - Attuazione
05.29.03 Sicurezza delle informazioni durante le interruzioni - Test
05.30 Prontezza dell'ICT per la continuità operativa
05.31.01 Identificazione dei requisiti legali, statutari, regolamentari e contrattuali - con estensione ISO/IEC 27701
05.31.03 Identificazione dei requisiti legali, statutari, regolamentari e contrattuali - Requisiti contrattuali
05.32 Diritti di proprietà intellettuale
05.33 Protezione delle registrazioni - con estensione ISO/IEC 27701
05.34 Privacy e protezione dei dati personali
05.35.01 Riesame indipendente della sicurezza delle informazioni - con estensione ISO/IEC 27701
05.35.02 Riesame indipendente della sicurezza delle informazioni - Tecnologico - con estensione ISO/IEC 27701
05.36 Conformità alle politiche e alle norme per la sicurezza delle informazioni
05.37 Procedure operative documentate
06.01 Screening
06.02 Termini e condizioni di impiego
06.03 Consapevolezza, istruzione, formazione e addestramento sulla sicurezza delle informazioni - con estensione ISO/IEC 27701
06.04 Processo disciplinare
06.05 Responsabilità dopo la cessazione o variazione del rapporto di lavoro
06.06 Accordi di riservatezza o di non divulgazione - con estensione ISO/IEC 27701
06.07 Lavoro remoto
06.08.01 Segnalazione degli eventi relativi alla sicurezza delle informazioni
06.08.02 Segnalazione degli eventi relativi alla sicurezza delle informazioni - Vulnerabilità
07.01 Perimetri di sicurezza fisica
07.02.01 Controlli di accesso fisico - Generale
07.02.02 Controlli di accesso fisico - Visitatori
07.03 Messa in sicurezza di uffici, locali e strutture
07.04 Monitoraggio della sicurezza fisica
07.05 Protezione dalle minacce fisiche e ambientali
07.07 Schermo e scrivania puliti - con estensione ISO/IEC 27701
07.08 Disposizione delle apparecchiature e loro protezione
07.09 Sicurezza degli asset all'esterno delle sedi
07.10.01 Supporti di memorizzazione - Supporti rimovibili - con estensione ISO/IEC 27701
07.10.02 Supporti di memorizzazione - Riuso ed eliminazione sicuri - con estensione ISO/IEC 27701
07.10.03 Supporti di memorizzazione - Trasferimento
07.11 Infrastrutture di supporto
07.12 Sicurezza dei cablaggi
07.13 Manutenzione delle apparecchiature
07.14 Dismissione sicura o riutilizzo delle apparecchiature - con estensione ISO/IEC 27701
08.01.01 Dispostivi finali degli utenti - con estensione ISO/IEC 27701
08.01.02 Endpoint degli utenti - Dispositivi non presidiati
08.02 Diritti di accesso privilegiato
08.03 Limitazione degli accessi alle informazioni
08.04 Accesso al codice sorgente
08.05 Autenticazione sicura - con estensione ISO/IEC 27701"
08.06 Gestione della capacità
08.07 Protezione dal malware
08.08 Gestione delle vulnerabilità tecniche
08.09 Gestione delle configurazioni sicure e dell'hardening
08.10 Cancellazione delle informazioni
08.11 Mascheramento (e anonimizzazione) dei dati

08.12 Prevenzione di leakage delle informazioni
08.13 Backup delle informazioni - con estensione ISO/IEC 27701
08.14 Ridondanza delle strutture di elaborazione delle informazioni
08.15.01 Raccolta di log - Generale - con estensione ISO/IEC 27701
08.15.02 Raccolta di log - Amministratori e operatori
08.15.03 Raccolta di log - Protezione - con estensione ISO/IEC 27701
08.16 Attività di monitoraggio
08.17 Sincronizzazione degli orologi
08.18 Utilizzo di programmi di utilità privilegiati
08.19.01 Installazione del software sui sistemi di produzione - Accettazione
08.19.02 Installazione del software sui sistemi di produzione - Gestione
08.20 Sicurezza delle reti
08.21 Sicurezza dei servizi di rete
08.22 Segregazione delle reti
08.23 Web filtering
08.24.01 Uso della crittografia - Generale - con estensione ISO/IEC 27701
08.24.02 Uso della crittografia - Gestione delle chiavi
08.25 Ciclo di vita dello sviluppo sicuro
08.26.01 Requisiti di sicurezza delle applicazioni - Generale
08.26.02 Requisiti di sicurezza delle applicazioni - Reti pubbliche - con estensione ISO/IEC 27701
08.26.03 Requisiti di sicurezza delle applicazioni - Servizi transazionali
08.27 Sicurezza dell'architettura dei sistemi e dei principi di ingegnerizzazione - con estensione ISO/IEC 27701
08.28 Sviluppo sicuro (codifica sicura) - con estensione ISO/IEC 27701
08.29 Test di sicurezza in fase di sviluppo e di accettazione
08.30 Sviluppo affidato all'esterno - con estensione ISO/IEC 27701
08.31.01 Separazione degli ambienti di sviluppo, test e produzione
08.31.02 Separazione degli ambienti di sviluppo, test e produzione - Sicurezza degli ambienti
08.32.01 Gestione dei cambiamenti (per sistemi e reti)
08.32.02 Gestione dei cambiamenti (per sistemi e reti) - Riesame delle applicazioni
08.32.03 Gestione dei cambiamenti (per sistemi e reti e applicazioni) - Limitare i cambiamenti ai pacchetti
08.33 Dati di test - con estensione ISO/IEC 27701
08.34 Protezione dei sistemi informativi durante i test di audit

Controlli ISO/IEC 27701

Di seguito viene riportato l'elenco dei controlli privacy applicati:

Controllo
27701-A.07.02.01 (Tit.) Identificare e documentare le finalità
27701-A.07.02.02 (Tit.) Identificare le basi legali del trattamento
27701-A.07.02.03 (Tit.) Determinare quando e come ottenere il consenso
27701-A.07.02.04 (Tit.) Ottenere e registrare i consensi
27701-A.07.02.05 Privacy impact assessment
27701-A.07.02.06 (Tit.) Contratti con i responsabili
27701-A.07.02.07 (Tit.) Co-titolari
27701-A.07.02.08 (Tit.) Registro dei trattamenti
27701-A.07.03.01 (Tit.) Determinare e ottemperare agli obblighi verso gli interessati
27701-A.07.03.02 (Tit.) Impostare le informative
27701-A.07.03.03 (Tit.) Fornire le informative agli interessati
27701-A.07.03.04 (Tit.) Fornire meccanismi per modificare o ritirare il consenso
27701-A.07.03.05 (Tit.) Fornire meccanismi per obiettare al trattamento
27701-A.07.03.06 (Tit.) Accesso, correzione, cancellazione
27701-A.07.03.07 (Tit.) Comunicazione con terze parti delle richieste degli interessati
27701-A.07.03.08 (Tit.) Fornire copia dei dati personali trattati
27701-A.07.03.09 (Tit.) Gestione delle richieste
27701-A.07.03.10 (Tit.) Processi decisionali automatizzati
27701-A.07.04.01 (Tit.) Limitare la raccolta
27701-A.07.04.02 (Tit.) Limitare (minimizzare) i trattamenti
27701-A.07.04.03 (Tit.) Accuratezza e qualità
27701-A.07.04.04 (Tit.) Obiettivi di minimizzazione
27701-A.07.04.05 (Titolare) De-identificazione e cancellazione alla conclusione del trattamento
27701-A.07.04.06 (Tit.) File temporanei
27701-A.07.04.07 (Tit.) Tempi di conservazione
27701-A.07.04.08 Eliminazione
27701-A.07.04.09 (Tit.) Controlli sulle trasmissioni dei dati personali
27701-A.07.05.01 (Tit.) Identificare le basi per il trasferimento dei dati personali.
27701-A.07.05.02 (Tit.) Paesi e organizzazioni internazionali a cui sono trasferiti i dati personali.
27701-A.07.05.03 (Tit.) Registrazioni dei trasferimenti dei dati personali
27701-A.07.05.04 (Tit.) Registrazioni delle comunicazioni di dati personali a terze parti
27701-B.08.02.01 (Resp.) Accordi con i clienti
27701-B.08.02.02 (Resp.) Finalità dei trattamenti
27701-B.08.02.03 (Resp.) Uso dei dati per marketing e pubblicità
27701-B.08.02.04 (Resp.) Segnalazione di istruzioni non-conformi
27701-B.08.02.05 (Resp.) Strumenti per i titolari per poter dimostrare la propria conformità
27701-B.08.02.06 (Resp.) Registro dei trattamenti
27701-B.08.03.01 (Resp.) Strumenti per i diritti degli interessati
27701-B.08.04.01 (Resp.) File temporanei
27701-B.08.04.02 (Responsabile) Restituzione, trasferimento o eliminazione dei dati personali
27701-B.08.04.03 (Resp.) Controlli sulle trasmissioni dei dati personali
27701-B.08.05.01 (Resp.) Comunicazione ai clienti dei trasferimenti di dati personali in altre giurdisdizioni (extra-SEE)

27701-B.08.05.02 (Resp.) Paesi e organizzazioni internazionali a cui sono trasferiti i dati personali
27701-B.08.05.03 (Resp.) Registrazioni delle comunicazioni di dati personali a terze parti
27701-B.08.05.04 (Resp.) Notifica delle richieste di trasferimento di dati personali
27701-B.08.05.05 (Resp.) Trasferimenti di dati personali per legge
27701-B.08.05.06 (Resp.) Dichiarazione dei sub-fornitori
27701-B.08.05.07 (Resp.) Ingaggio dei sub-responsabili
27701-B.08.05.08 (Resp.) Modifica dei sub-responsabili

Gestione Incidenti Applicativi

Di seguito vengono riportati i principali passi procedurali relativi alla procedura di Gestione degli Incidenti applicativi:

Attività	Competenza
Ricezione segnalazione	
➢ Da Cliente / Utente	Cliente Utente
➢ Da monitoraggio applicativo	Assistenza 2° Livello
Valutazione segnalazione	Assistenza 2° Livello Responsabile Tecnico
Valutazione segnalazione per L 90	Assistenza 2° Livello Responsabile Tecnico
Valutazione segnalazione per NIS2	Assistenza 2° Livello Responsabile Tecnico
Coinvolgimento del Direttore Tecnico e Responsabile Prodotto / Servizio	Responsabile Tecnico
Eventuale coinvolgimento del Direttore Generale	Direttore Tecnico Responsabile Prodotto/Servizio
Analisi della soluzione	Assistenza 2° Livello Responsabile Tecnico
Eventuale Segnalazione al Cliente	Responsabile Prodotto/Servizio
Implementazione della soluzione	Assistenza 2° Livello Responsabile Tecnico
Risposta al segnalante	Responsabile Prodotto/Servizio (può delegare la risposta, dando indicazioni chiare sulla risposta)

Piano di continuità operativa

Ecocerved ha predisposto un Piano di Continuità Operativa, il quale descrive le modalità di intervento a fronte di situazioni di emergenza ed eventi critici, (intendendosi eventi anomali ed eccezionali), che impediscono l'erogazione dei servizi in toto o in parte in ambito ICT.

La struttura organizzativa che Ecocerved ha predisposto per la gestione dell'emergenza presenta la seguente articolazione funzionale:

- Comitato di crisi ICT;
- Responsabile di continuità operativa;
- Team di disaster recovery;
- Team del piano di continuità operativa;
- Ufficio Stampa;
- Fornitori ICT;
- Personale operativo

Ecocerved ha predisposto un piano di Disaster Recovery coordinato con Infocamere. I test di Disaster Recovery vengono eseguiti almeno una volta l'anno.

Amministratori di Sistema

Ecocerved ha nominato i propri amministratori di sistema in conformità alla disciplina applicabile (nomina individuale, controllo periodico dell'operato, conservazione dei file di log, ecc.).

Servizio di hosting

Il servizio di hosting viene fornito da Infocamere ScpA.