# Misure di sicurezza dei servizi Welfare e Ticket Restaurant

Manuale di Sicurezza


## Edenred Italia Srl

Via GB Pirelli 18
20124 Milano
Italy
☎ +39 (0) 2 26 904 1
+39 (0) 2 21 309 1
https://www.edenred.it/

| Società | Funzione | Scopo |
|---|---|---|
| Edenred | CISO | Accountable |
| Edenred | CIO | Responsible |

| Revisioni | | | | | |
|---|---|---|---|---|---|
| # | Data | Descrizione | Autore | Rivisto da | Approvato da. |
| 1.0 | 28/08/2025 | Prima stesura del documento | Information Security Consultant | CISO | CISO |

# Sommario

# 1. Introduzione

## 1.1. Scopo del documento

Il documento descrive le informazioni inerenti alle misure di sicurezza tecniche e organizzative adottate da Edenred Italia S.r.l. per i servizi in cloud Welfare e Ticket Restaurant.

# 2. Termini e definizioni

| termine | definizione |
|---|---|
| **Change Management** | Il Change Management è il processo che consente di assicurare mediante controlli e procedure la gestione di tutti i cambiamenti applicativi e di infrastruttura IT, al fine di minimizzare l'impatto degli incidenti nell'ambito dei servizi erogati. |
| **CAB** | Change Advisory Board – Gruppo composto dai capi delle strutture di IT Governance, Architettura, BRM, Sicurezza, Ops & Infr, Workplace Management, Sviluppo e il CIO che ha come compito valutare le CR per approvazione. |
| **Release Management (RM)** | Oggetto Jira creato per segnalare una richiesta di change. |
| **OPIT** | Oggetto Jira correlato alla RM, utilizzato per ingaggiare la struttura di IT Operations che si occupa di eseguire la change richiesta. |

# 3. Misure di sicurezza

Edenred Italia S.r.l. ha stabilito che l'obiettivo principale per la sicurezza delle informazioni e la protezione dei dati personali deve essere quello di supportare l'offerta sul mercato con prodotti con alto profilo di sicurezza, garantendo un appropriato e uniforme livello di protezione. Pertanto, garantisce la sicurezza delle informazioni trattate durante l'erogazione dei propri servizi sotto il profilo della disponibilità, integrità e riservatezza, anche implementando - ove necessari - idonei meccanismi di isolamento dei dati e di tracciatura degli accessi agli ambienti e ai dati. A tal proposito, i servizi si svolgeranno nel rispetto della "*Politica di sicurezza delle informazioni e la protezione dei dati personali*" adottata da Edenred.

## 3.1. Gestione dei diritti di accesso ai servizi cloud

Per quanto riguarda la gestione degli accessi logici, al fine di proteggere i sistemi informativi e i dati, Edenred prevede l'utilizzo di adeguate misure di sicurezza come la segregation of duties, l'accesso limitato ai sistemi (principi del need to know e del least privilege), account non nominali, ecc. Inoltre, svolge l'identificazione e la classificazione delle tipologie di utenti/dipendenti ai fini di una corretta assegnazione delle utenze.

Edenred Italia, garantisce l'indirizzo, il controllo e la gestione delle piattaforme per il trattamento degli accessi privilegiati ai propri sistemi informativi, attraverso logiche e meccanismi di identificazione, autenticazione e tracciamento delle attività svolte dagli amministratori di sistema interni, coerentemente con i requisiti espressi dalla normativa in ambito.

La gestione di tale processo è in capo all'Help Desk che eroga il prodotto nei seguenti giorni/fasce orarie: il prodotto per i clienti sarà erogato, dal lunedì al sabato, durante il normale orario lavorativo (9.00-17.30). Per qualsiasi necessità, di seguito i canali di contatto:

- Form di richiesta di assistenza sul sito https://www.edenred.it/assistenza/contatti/contatti-ticket-restaurant/;
- Numeri telefonici:

  **Beneficiari:** *02.82843701*

  **Aziende clienti:** *02.82843707*.

### 3.2. Gestione dei Log

Edenred ha adottato un processo per la gestione dei log in riferimento a tutte le risorse informatiche di proprietà o utilizzate dalla stessa, le quali devono produrre un log delle loro attività in modo da consentirne il monitoraggio. I log generati vengono trasmessi ai server predisposti alla loro raccolta in un processo di generazione, trasmissione, memorizzazione e dismissione. Al fine di garantire un corretto monitoraggio dei file di log, la gestione dei log è centralizzata mediante l'utilizzo di un sistema di log management, con lo scopo di creare e mantenere un'infrastruttura sicura, bilanciando le performance del sistema e lo spazio di archiviazione, garantendo la conformità alle relative normative vigenti.

La funzione preposta al monitoraggio analizza periodicamente i dati raccolti con l'obiettivo di individuare eventuali incidenti di sicurezza informatica in tempi brevi, limitandosi ad analizzare i log solo per le finalità per i quali sono stati raccolti. Dopo aver identificato un eventuale incidente/problema informatico, la funzione di monitoraggio avvia il relativo processo di gestione e risoluzione.

### 3.3. Gestione delle vulnerabilità tecniche

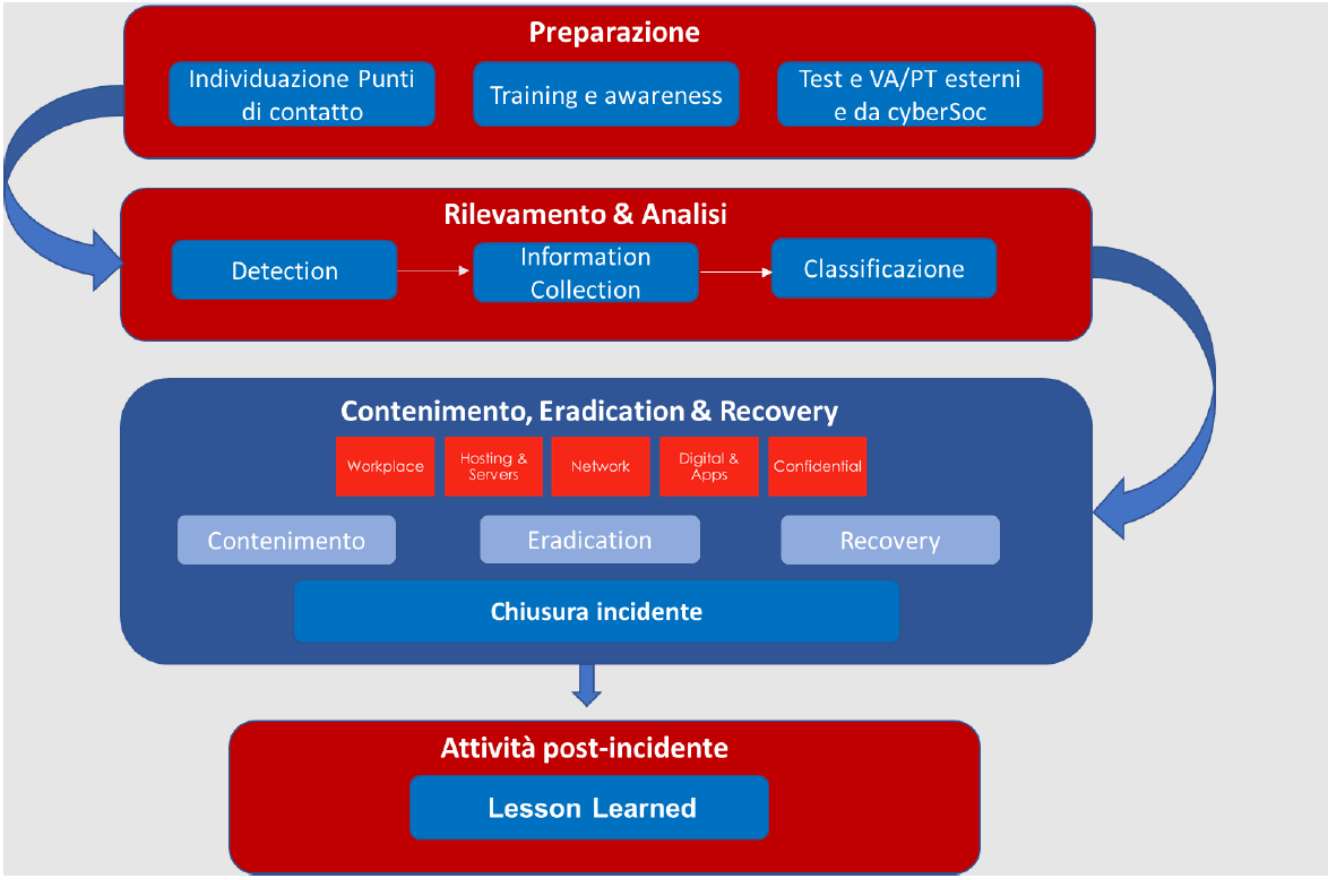
Con lo scopo di garantire la sicurezza delle infrastrutture tecnologiche, Edenred Italia, prevede un processo di identificazione, valutazione, gestione e mitigazione delle vulnerabilità presenti nei sistemi informatici e nell'infrastruttura IT aziendale. Nel proprio processo viene svolto un Vulnerability Assessment annuale completo su tutte le infrastrutture e i servizi, scansioni mensili su infrastrutture, scansioni trimestrali su applicazioni web e scansioni su richiesta.

A valle dell'assessment, le vulnerabilità riscontrate vengono registrate sulla piattaforma di ticketing JIRA sotto il progetto WAPT. Il team di sicurezza supervisiona quindi le vulnerabilità e la relativa mitigazione per tutto il ciclo di vita. Ogni vulnerabilità registrata viene valutata al fine di definire la categoria, ovvero il principale scenario di rischio associato all'incidente ed il suo livello di gravità. Al completamento delle fasi di analisi e classificazione, vengono redatti dei report in cui sono riportate le vulnerabilità e le azioni di remediation. Infine, i report vengono condivisi con il CISO per la validazione.

### 3.4. Gestione degli incidenti di sicurezza

Per rilevare e rispondere in modo appropriato a qualsiasi incidente di sicurezza, Edenred Italia garantisce che gli eventi di sicurezza delle informazioni siano adeguatamente rilevati, classificati e, se necessario, esaminati. In particolare, le attività si articolano nelle diverse fasi della gestione degli incidenti nel corso delle quali verranno coordinate le attività di mitigazione e rimedio. Le fasi prevedono preparazione, rilevamento e analisi, contenimento e rispristino ed, infine, le attività post incidente.

Di seguito una rappresentazione degli step procedurali per la gestione del processo:




La gestione degli incidenti in Edenred coinvolge diversi attori a livello locale e globale, ciascuno con ruoli specifici nel processo di rilevamento, analisi, contenimento e ripristino. La responsabilità complessiva della sicurezza ricade sul CISO supportato dal Senior Cybersecurity Specialist.

Il prodotto viene erogato 7x7 h24 e la segnalazione di un incidente da un cliente può essere effettuata mediante i seguenti canali di contatto:

- Compilando il form di richiesta di assistenza sul sito https://www.edenred.it/assistenza/contatti/contatti-ticket-restaurant/;
- Contattando i seguenti numeri telefonici:

**Beneficiari:** *02.82843701*

**Aziende clienti:** *02.82843707*.

### 3.5. Gestione dei cambiamenti

Le informazioni riportate nel presente documento vengono applicate alle Change Request relative alle modifiche che fanno parte del processo di Change & Release Management di Edenred Italia e si riferiscono alle applicazioni, ai sistemi e ai database.

Il processo di Change & Release Management viene eseguito con cadenza settimanale sulle diverse tipologie di Change Request: standard, normal ed emergency.

Il processo settimanale è il seguente:

- **Venerdì** viene eseguita l'estrazione di RM con data di rilascio settata al mercoledì successivo, l'analisi del Release Management e la verifica dell'esito del test (se eseguito).
- **Lunedì** avviene l'identificazione nel CAB di eventuali **scenari problematici**, di **correlazioni tecniche/funzionali**, verifica dello **stato dei test**, dei **gate approvativi** e del **piano di rollback** della soluzione. Viene svolta una verifica sulla presenza di tutti gli OPIT necessari sulla necessità di supporto tecnico per eventuali correlazioni tra le installazioni. Infine, l'RM viene approvata o ripianificata;
- **Martedì** vengono svolte ulteriori verifiche sulle RM e OPIT;
- **Mercoledì** vengono eseguiti i rilasci alle 21:05 e chiusi gli OPIT, nel caso di problematiche sono previsiti dei rollback e vengono prodotti e condivisi report sull'esito della release;
- **Giovedì** vi è la chiusura delle RM.

### 3.6. Restituzione e rimozione delle risorse

Il processo di restituzione e rimozione delle risorse in cloud viene gestito mediante una piattaforma di ticketing dalla struttura Infrastructure di Edenred Italia. Tale processo prevede una richiesta di dismissione/rimozione di un asset su applicazione Jira mediante l'apertura di un ticket OPIT, includendo la motivazione della richiesta. Il ticket viene preso in carico dal team di competenza che evade la richiesta correlata al Work Item OPIT di riferimento.