Statement of Applicability

Linee Guida

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/

Pubblico
Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

Società	Funzione	Scopo
Edenred	Chief Legal Officer	Accountable
Edenred	CISO - Chief Information Security Officer	Responsible
Edenred	CIO - Chief Information Officer	Responsible
Edenred	Head of Employee Relations & Reward	Responsible
Edenred	Head of Legal & Advisory	Responsible
Edenred	DPO & Head of Anti Fraud	Responsible
Edenred	Head of Procurement & Facility	Responsible
Edenred	Test Manager	Responsible

Revisioni

#	Data	Descrizione	Autore	Rivisto da	Approvato da.
1.0	22/10/2018	Prima bozza rilasciata	IT Security	CIO	CIO
1.1	13/03/2019	Aggiunta dei riferimenti dei documenti per ogni controllo	IT Security	CIO	CIO
1.2	23/08/2019	Aggiornamento riferimenti	IT Security	CIO	CIO
1.3	04/10/2019	Aggiornamento documento	Information Security Consultant	IT Security	CIO
1.4	13/12/2019	Aggiornamento documento	Information Security Consultant	IT Security	CIO
2.0	08/01/2021	Aggiornamento documento/Trasposizione su nuovo template/aggiornamento matrice RACI	Information Security Consultant	CISO	CISO
2.1	11/10/2021	Revisione dei contenuti	Information Security Consultant	CISO	CISO
2.2	19/12/2022	Aggiornamento riferimenti	Information Security Consultant	CISO	CISO
2.3	23/01/2023	Integrazione con controlli 27701	Information Security Consultant	DPO	Head of Corporate Compliance & Legal
2.4	20/12/2023	Aggiornamento stato dei controlli	Information Security Consultant	DPO	Head of Corporate Compliance & Legal
3.0	20/09/2024	Aggiornamento stato dei controlli e adeguamento secondo la nuova normativa ISO/IEC 27001:2022	Information Security Consultant	DPO	Chief Legal Officer

Pubblico

Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

3.1	11/10/2024	Aggiornamenti formali	Privacy Specialist	DPO	Chief Legal Officer
3.2	31/01/2025	Revisione dei contenuti	Data Protection Specialist	DPO	
3.3	16/07/2025	Integrazione con controlli ISO/IEC 27017 ed ISO/IEC 27018	Information Security Consultant	DPO	CISO
3.4	26/10/2026	Aggiornamento annuale del Documento	Information Security Consultant	DPO	CISO - Chief Information Security Officer

Pubblico

Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

Sommario

1. Introduzione 5

1.1. Scopo del documento 5

1.2. Termini e definizioni 5

2. Controlli 6

2.1. Controlli ISO 27001:2022 7

2.2. Controlli ISO 27701:2019 46

2.3. Controlli ISO 27017:2015 65

2.4. Controlli ISO 27018:2019 68

Pubblico
Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

1. Introduzione

1.1. Scopo del documento

Il presente documento descrive sia i controlli attuati da Edenred Italia S.r.l., che quelli esclusi perché ritenuti non efficaci per la gestione del rischio relativo alla sicurezza delle informazioni, alla data protection e alla sicurezza per i servizi cloud, adeguatamente mappati con quelli presenti nell'appendice A della norma ISO/IEC 27001 ed estesi da quelli previsti come estensioni degli standard ISO/IEC 27701, ISO/IEC 27017 ed ISO/IEC 27018.

Questo documento sarà mantenuto aggiornato, nel contesto complessivo e secondo le politiche definite da Edenred Italia S.r.l., secondo quanto previsto nella sua **Politica di sicurezza delle informazioni e la protezione dei dati personali.**

1.2. Termini e definizioni

Per le definizioni associate ai termini specialistici utilizzati nel presente documento si faccia riferimento alla norma internazionale ISO/IEC 27000 e ISO/IEC 29100.

Pubblico
Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

2. Controlli

Così come richiesto dalla norma ISO/IEC 27001, dalle estensioni ISO/IEC 27701, ISO/IEC 27017 ed ISO/IEC 27018, di seguito sono riportate le informazioni relative ai controlli del sistema di gestione integrato organizzate in formato tabellare:

Rif. Appendice A	**Controllo Annex A ISO/IEC 27001-Annex A, ISO/IEC 27701-ISO/IEC 27017 ed ISO/IEC 27018** **Obiettivo di controllo Annex A ISO/IEC 27001-Annex A, ISO/IEC 27701-ISO/IEC 27017 ed ISO/IEC 27018**
Controllo	**Dettaglio obiettivo di controllo Annex A ISO/IEC 27001 Annex A ISO/IEC 27701, ISO/IEC 27017 ed ISO/IEC 27018**
Descrizione del Controllo	*Descrizione del controllo secondo quanto riportato nello standard ISO/IEC 27001-ISO/IEC 27701-ISO/IEC 27017, ISO/IEC 27018*
Incluso	Sì/No
Motivazione per l'inclusione / Esclusione	Riporta le motivazioni per le quali un controllo è stato incluso o escluso dal SOA
Livello di Implementazione	Riporta il livello di implementazione di ciascun controllo
Ownership	Riporta la società che è responsabile dell'implementazione del controllo della ISO/IEC 27001-ISO/IEC 27701-ISO/IEC 27017-ISO/IEC 27018; ovvero *Edenred Italia* come soggetto certificato e/o *Edenred SE come entità controllante di Edenred Italia*. L'ownership può appartenere sia ad una singola organizzazione che ad entrambe
Referente	Figure aziendali che si occupano della implementazione dei controlli previste nelle politiche e procedure della organizzazione secondo quanto previsto dallo standard ISO/IEC 27001 e dalle estensioni ISO/IEC 27701-ISO/IEC 27017-ISO/IEC 27018
Documentazione	• Elenco dei documenti sia di Edenred Italia sia di Edenred SE che implementano il controllo della ISO/IEC 27001-ISO/IEC 27017-ISO/IEC 27018 • ERIT-SGI-BCM-Catalogo Documentale
Note	Eventuali commenti legati al controllo della ISO/IEC 27001-ISO/IEC 27701-ISO/IEC 27017-ISO/IEC 27018

Pubblico

Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

2.1. Controlli ISO 27001:2022

Rif. Appendice A ISO/IEC 27001	A.5 Controlli organizzativi
Controllo	**A.5.1 Politiche per la sicurezza delle informazioni**
Descrizione del Controllo	*La politica di sicurezza delle informazioni e le politiche specifiche per ogni argomento devono essere definite, approvate dalla direzione, pubblicate, comunicate e riconosciute dal personale e dalle parti interessate, e riviste a intervalli pianificati e in caso di modifiche significative.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Ritenuto necessario per rendere efficace il SGI
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	CISO
Documentazione	• ERIT-SGI - Politica di sicurezza delle informazioni e la protezione dei dati personali • SEC-POL-025-Server and Cloud Security Policy_2026 version PCI-DSS (CSP, CSC) • SEC-POL-019-Infrastructure Security Policy_202602 (CSP, CSC)
Note	
Controllo	**A.5.2 Ruoli e responsabilità in materia di sicurezza delle informazioni**
Descrizione del Controllo	*I ruoli e le responsabilità in materia di sicurezza delle informazioni devono essere definiti e assegnati in base alle esigenze dell'organizzazione.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Ritenuto necessario per rendere efficace il controllo A.5.1
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	CISO
Documentazione	• ERIT-SGI - Politica di sicurezza delle informazioni e la protezione dei dati personali (CSP, CSC) • ERIT-SGI - Comunicazione (CSP, CSC) • Contratto Microsoft (CSC)

Pubblico

Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

	• Contratto Mulesoft (CSC)
Note	
Controllo	**A.5.3 Segregazione dei compiti**
Descrizione del Controllo	*Le mansioni e le aree di responsabilità in conflitto devono essere separate.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Necessario al corretto svolgimento delle attività.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	Head of Infrastructure & Operations
Documentazione	• ERIT-SGI - Gestione Accessi Logici
Note	
Controllo	**A.5.4 Responsabilità di gestione**
Descrizione del Controllo	*La direzione deve richiedere a tutto il personale di applicare la sicurezza delle informazioni in conformità con la politica di sicurezza delle informazioni, alle politiche e alle procedure specifiche dell'organizzazione.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Necessario al corretto svolgimento delle attività.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	CISO
Documentazione	• ERIT-SGI - Politica di sicurezza delle informazioni e la protezione dei dati personali
Note	
Controllo	**A.5.5 Contatto con le autorità**
Descrizione del Controllo	*L'organizzazione deve stabilire e mantenere i contatti con le autorità competenti.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Requisito di legge.

Pubblico

Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	CISO, DPO, Chief Legal Officer
Documentazione	• ERIT-SGI - Politica di sicurezza delle informazioni e la protezione dei dati personali • ERIT-SGI - Comunicazione (CSC) • ERIT-SGI-Matrice di gestione delle comunicazioni (CSC) • ERIT-SGI - Edenred Italia Descrizione Piattaforma (CSP)
Note	
Controllo	**A.5.6 Contatti con gruppi di interesse specifico**
Descrizione del Controllo	*L'organizzazione deve stabilire e mantenere contatti con gruppi di interesse speciale o altri forum specializzati in materia di sicurezza e associazioni professionali.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Ritenuto necessario per rendere efficace il SGI.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	CISO
Documentazione	• 5.6 - Evidenza Clusit 1 • 5.6 - Evidenza Clusit 2
Note	
Controllo	**A.5.7 Threat intelligence**
Descrizione del Controllo	*Le informazioni relative alle minacce alla sicurezza delle informazioni devono essere raccolte e analizzate per produrre informazioni sulle minacce.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Ritenuto necessario per rendere efficace il SGI.
Livello di Implementazione	Implementato
Ownership	Edenred SE
Referente	CISO, SOC
Documentazione	• SEC-GUI-036-Risk Assessment Guidelines_2026 version

Pubblico

Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

Note	
Controllo	**A.5.8 Information security in project management**
Descrizione del Controllo	*La sicurezza delle informazioni deve essere integrata nella gestione del progetto*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Ritenuto necessario per rendere efficace il SGI.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	CISO
Documentazione	• ERIT-SGI - Politica di sicurezza delle informazioni e la protezione dei dati personali • ERIT-SGI - Procedura Security e Privacy by Design (CSP) • ERIT-SGI - Policy sviluppo sicuro (CSP) • SEC-POL-025-Server and Cloud Security Policy_2026 version PCI-DSS (CSC) • Contratto Microsoft (CSP, CSC) • Contratto Mulesoft (CSP, CSC)
Note	
Controllo	**A.5.9 Inventario delle informazioni e delle altre risorse associate**
Descrizione del Controllo	*È necessario sviluppare e mantenere un inventario delle informazioni e delle altre risorse associate, compresi i proprietari.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Necessaria al corretto svolgimento delle attività.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	Head of Enterprise Architecture, Head of Infrastructure & Operations
Documentazione	• ERIT-SGI - Gestione Attrezzature Inventario HW • ERIT-SGI - Gestione Licenze Software • 5.9 - IT Asset Inventory - App • 5.9 - IT Asset Inventory – PC • ERIT-SGI - Linee Guida Application Catalog (CSP, CSC)

Pubblico

Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

Note	
Controllo	**A.5.10 Uso accettabile delle informazioni e delle altre risorse associate**
Descrizione del Controllo	*Le regole per l'uso accettabile e le procedure per la gestione delle informazioni e delle altre risorse associate devono essere identificate, documentate e implementate.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Necessaria al corretto svolgimento delle attività.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	CISO
Documentazione	• ERIT-SGI-IT Charter
Note	
Controllo	**A.5.11 Ritorno degli Assets**
Descrizione del Controllo	*Il personale e le altre parti interessate, a seconda dei casi, devono restituire tutti i beni dell'organizzazione in loro possesso al momento della modifica o della cessazione del rapporto di lavoro, del contratto o dell'accordo.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Necessaria al corretto svolgimento delle attività.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	Head of Infrastructure & Operations
Documentazione	• ERIT-SGI-IT Charter • 5.11 - Parco PC - Luglio 2024 • 5.11 - Modulo Consegna Materiale IT Vuoto
Note	
Controllo	**A.5.12 Classificazione delle informazioni**
Descrizione del Controllo	*Le informazioni devono essere classificate in base alle esigenze di sicurezza delle informazioni dell'organizzazione, in base alla riservatezza, all'integrità, alla disponibilità e ai requisiti delle parti interessate.*
Incluso	Sì

Pubblico

Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

Motivazione per l'inclusione / Esclusione	Ritenuto necessario per rendere efficace il SGI.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	CIO
Documentazione	• ERIT-SGI - Classificazione delle Informazioni
Note	
Controllo	**A.5.13 Etichettatura delle informazioni**
Descrizione del Controllo	*Un'adeguata serie di procedure per l'etichettatura delle informazioni deve essere sviluppata e implementata in conformità con lo schema di classificazione delle informazioni adottato dall'organizzazione.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Ritenuto necessario per rendere efficace il SGI.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	CIO
Documentazione	• ERIT-SGI - Classificazione delle Informazioni (CSP, CSC)
Note	
Controllo	**A.5.14 Trasferimento di informazioni**
Descrizione del Controllo	*Devono essere in vigore regole, procedure o accordi per il trasferimento delle informazioni per tutti i tipi di strutture di trasferimento all'interno dell'organizzazione e tra l'organizzazione e altre parti.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Ritenuto necessario per rendere efficace il SGI.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	Privacy Manager
Documentazione	• ERIT-SGI - Gestione sicura dei Fornitori • ERIT-SGI - Politica di sicurezza delle informazioni e la protezione dei dati personali

Pubblico

Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

Note	
Controllo	**A.5.15 Controllo degli accessi**
Descrizione del Controllo	*Le regole per controllare l'accesso fisico e logico alle informazioni e alle altre risorse associate devono essere stabilite e implementate in base ai requisiti di business e di sicurezza delle informazioni.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Ritenuto necessario per rendere efficace il SGI.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	Head of Infrastructure & Operations, Head of Procurement & Facility
Documentazione	• ERIT-SGI-Accessi Fisici • ERIT-SGI - Gestione Accessi Logici (CSP, CSC)
Note	
Controllo	**A.5.16 Identity Management**
Descrizione del Controllo	*È necessario gestire l'intero ciclo di vita delle identità.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Ritenuto necessario per rendere efficace il SGI.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	Head of Infrastructure & Operations, Head of Procurement & Facility
Documentazione	• ERIT-SGI - Gestione Utenti (CSP, CSC)
Note	
Controllo	**A.5.17 Informazioni di autenticazione**
Descrizione del Controllo	*L'assegnazione e la gestione delle informazioni di autenticazione devono essere controllate da un processo di gestione, che comprenda la consulenza al personale sulla gestione appropriata delle informazioni di autenticazione.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Ritenuto necessario per rendere efficace il SGI.

Pubblico
Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	Head of Infrastructure & Operations, Head of Procurement & Facility
Documentazione	• ERIT-SGI - Gestione Accessi Logici (CSP) • ERIT-SGI-Accessi Fisici (CSP) • Contratto Microsoft (CSC) • Contratto Mulesoft (CSC)
Note	
Controllo	**A.5.18 Diritti di accesso**
Descrizione del Controllo	*I diritti di accesso alle informazioni e alle altre risorse associate devono essere forniti, rivisti, modificati e rimossi in conformità alla politica e alle regole per il controllo degli accessi specifiche dell'organizzazione.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Ritenuto necessario per rendere efficace il SGI.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	Head of Infrastructure & Operations
Documentazione	• ERIT-SGI - Gestione Accessi Logici (CSP, CSC)
Note	
Controllo	**A.5.19 Sicurezza delle informazioni nelle relazioni con i fornitori**
Descrizione del Controllo	*Occorre definire e implementare processi e procedure per gestire i rischi per la sicurezza delle informazioni associati all'uso dei prodotti o dei servizi del fornitore.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Necessaria al corretto svolgimento delle attività.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	CISO
Documentazione	• ERIT-SGI - Gestione sicura dei Fornitori (CSP, CSC)
Note	

Pubblico
Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

Controllo	**A.5.20 Affrontare la sicurezza delle informazioni negli accordi con i fornitori**
Descrizione del Controllo	*I requisiti di sicurezza delle informazioni pertinenti devono essere stabiliti e concordati con ciascun fornitore in base al tipo di rapporto con lo stesso.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Necessaria al corretto svolgimento delle attività.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	CISO
Documentazione	• ERIT-SGI - Gestione sicura dei Fornitori (CSP, CSC)
Note	
Controllo	**A.5.21 Gestire la sicurezza delle informazioni nella catena di fornitura delle ICT**
Descrizione del Controllo	*Occorre definire e implementare processi e procedure per gestire i rischi per la sicurezza delle informazioni associati alla catena di fornitura di prodotti e servizi ICT.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Necessaria al corretto svolgimento delle attività.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	CISO
Documentazione	• ERIT-SGI - Gestione sicura dei Fornitori (CSP, CSC)
Note	
Controllo	**A.5.22 Monitoraggio, revisione e gestione delle modifiche dei servizi dei fornitori**
Descrizione del Controllo	*L'organizzazione deve monitorare, rivedere, valutare e gestire regolarmente i cambiamenti nelle pratiche di sicurezza delle informazioni e nella fornitura di servizi da parte dei fornitori.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Necessaria al corretto svolgimento delle attività.

Pubblico
Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	CISO
Documentazione	• ERIT-SGI - Gestione sicura dei Fornitori
Note	
Controllo	**A.5.23 Sicurezza delle informazioni per l'utilizzo dei servizi cloud**
Descrizione del Controllo	*I processi per l'acquisizione, l'uso, la gestione e l'uscita dai servizi cloud devono essere stabiliti in conformità ai requisiti di sicurezza delle informazioni dell'organizzazione.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Necessaria al corretto svolgimento delle attività.
Livello di Implementazione	Implementato
Ownership	Edenred SE
Referente	CISO
Documentazione	• 5.23 Contratti cloud
Note	
Controllo	**A.5.24 Pianificazione e preparazione della gestione degli incidenti di sicurezza delle informazioni**
Descrizione del Controllo	*L'organizzazione deve pianificare e prepararsi a gestire gli incidenti di sicurezza delle informazioni definendo, stabilendo e comunicando i processi di gestione degli incidenti di sicurezza delle informazioni, i ruoli e le responsabilità.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Ritenuto necessario per rendere efficace il SGI.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	CISO
Documentazione	• ERIT-SGI - Gestione degli incidenti di sicurezza (CSP, CSC) • ERIT-SEC-22301-Business Continuity Plan (CSP) • ERIT- Misure di sicurezza Welfare e Ticket Restaurant (CSP) • Contratto Microsoft (CSC)

Pubblico
Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

	• Contratto Mulesoft (CSC)
Note	
Controllo	**A.5.25 Valutazione e decisione sugli eventi di sicurezza delle informazioni**
Descrizione del Controllo	*L'organizzazione deve valutare gli eventi di sicurezza delle informazioni e decidere se devono essere classificati come incidenti di sicurezza delle informazioni.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Ritenuto necessario per rendere efficace il SGI.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	CISO
Documentazione	• ERIT-SGI - Gestione dei Log • ERIT-SGI - Gestione degli incidenti di sicurezza
Note	
Controllo	**A.5.26 Risposta agli incidenti di sicurezza delle informazioni**
Descrizione del Controllo	*Gli incidenti di sicurezza delle informazioni devono essere affrontati in conformità alle procedure documentate.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Ritenuto necessario per rendere efficace il SGI.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	CISO
Documentazione	• ERIT-SGI - Gestione degli incidenti di sicurezza
Note	
Controllo	**A.5.27 Imparare dagli incidenti di sicurezza informatica**
Descrizione del Controllo	*Le conoscenze acquisite dagli incidenti di sicurezza delle informazioni devono essere utilizzate per rafforzare e migliorare i controlli di sicurezza delle informazioni.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Ritenuto necessario per rendere efficace il SGI.

Pubblico

Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	CISO
Documentazione	• ERIT-SGI - Gestione degli incidenti di sicurezza
Note	
Controllo	**A.5.28 Raccolta delle prove**
Descrizione del Controllo	*L'organizzazione deve stabilire e implementare procedure per l'identificazione, la raccolta, l'acquisizione e la conservazione delle prove relative agli eventi di sicurezza delle informazioni.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Ritenuto necessario per rendere efficace il SGI.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	Head of Infrastructure & Operations, CISO
Documentazione	• ERIT-SGI - Gestione dei Log (CSP, CSC) • ERIT-SGI - Gestione degli incidenti di sicurezza (CSP, CSC) • Contratto Microsoft (CSP, CSC) • Contratto Mulesoft (CSP, CSC)
Note	
Controllo	**A.5.29 Sicurezza delle informazioni durante le interruzioni**
Descrizione del Controllo	*L'organizzazione deve pianificare come mantenere la sicurezza delle informazioni a un livello adeguato durante le interruzioni.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Ritenuto necessario per rendere efficace il SGI.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	CISO
Documentazione	• ERIT-SEC-22301-Politica di Business Continuity
Note	

Pubblico
Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

Controllo	A.5.30 Prontezza delle ICT per la continuità operativa
Descrizione del Controllo	*La preparazione delle ICT deve essere pianificata, implementata, mantenuta e testata sulla base degli obiettivi di continuità operativa e dei requisiti di continuità delle ICT.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Necessaria al corretto svolgimento delle attività.
Livello di Implementazione	Implementato
Ownership	Edenred Italia, Edenred SE
Referente	CISO
Documentazione	• ERIT-SEC-22301-Politica di Business Continuity • ERIT-SEC-22301-Business Continuity Plan • ERIT-SEC-22301-ValutazioneTrattamentoRischioContinuitàOperativa_2025 • ERIT-SEC-22301-BIA 2025 • EDNR IT - DXC Recovery Guidance New version 09052024
Note	
Controllo	**A.5.31 Requisiti legali, statutari, normativi e contrattuali**
Descrizione del Controllo	*I requisiti legali, statutari, normativi e contrattuali relativi alla sicurezza delle informazioni e l'approccio dell'organizzazione per soddisfare tali requisiti devono essere identificati, documentati e aggiornati.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Requisito di legge.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	Chief Legal Officer
Documentazione	• DPO & DPC Handbook • Edenred Legal Procedures Handbook v2 • PACCHETTO FORNITURA IT • 5.31 - Questionario 2024 • ERIT-SGI - Politica di crittografia (CSP, CSC) • Contratto Microsoft (CSC)

Pubblico
Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

	• SEC-GUI-039-Cryptography & Secure Protocols Guidelines_2026 version (CSC)
Note	
Controllo	**A.5.32 Diritti di proprietà intellettuale**
Descrizione del Controllo	*L'organizzazione deve implementare procedure appropriate per proteggere i diritti di proprietà intellettuale.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Requisito di legge.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	Chief Legal Officer
Documentazione	• ERIT-SGI - Classificazione delle Informazioni • PACCHETTO FORNITURA IT • ERIT-SGI - Gestione Licenze Software (CSP, CSC)
Note	I diritti di proprietà intellettuale sono una conseguenza della classificazione "Riservata" delle informazioni nella Politica di classificazione dei dati.
Controllo	**A.5.33 Protezione dei documenti**
Descrizione del Controllo	*I documenti devono essere protetti da perdita, distruzione, falsificazione, accesso non autorizzato e rilascio non autorizzato.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Necessaria al corretto svolgimento delle attività.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	Head of Infrastructure & Operations
Documentazione	• DLP_EDENRED ITALY_INFORMATIVA PRIVACY • Edenred_DLP PIA_ERIT_10072023 • ERIT-SGI - Gestione Utenti • ERIT-SGI - Gestione dei Log • ERIT- Misure di sicurezza Welfare e Ticket Restaurant (CSP) • ERIT-SGI - Data Masking Procedure (CSP) • Contratto Microsoft (CSP, CSC)

Pubblico

Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

	• Contratto Mulesoft (CSP, CSC)
Note	
Controllo	**A.5.34 Privacy e protezione delle PII**
Descrizione del Controllo	*L'organizzazione deve identificare e soddisfare i requisiti relativi alla conservazione della privacy e alla protezione delle PII in base alle leggi e ai regolamenti applicabili e ai requisiti contrattuali.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Requisito di legge.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	DPO
Documentazione	• ERIT-SGI - Linee Guida sulla Protezione dei Dati Personali
Note	
Controllo	**A.5.35 Revisione indipendente della sicurezza delle informazioni**
Descrizione del Controllo	*L'approccio dell'organizzazione alla gestione della sicurezza delle informazioni e la sua implementazione, comprese le persone, i processi e le tecnologie, devono essere rivisti in modo indipendente a intervalli pianificati o quando si verificano cambiamenti significativi.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Ritenuto necessario per rendere efficace il SGI.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	CISO, DPO
Documentazione	• ERIT-SGI - Politica di sicurezza delle informazioni e la protezione dei dati personali • https://compliance.salesforce.com/en/services/mulesoft • https://servicetrust.microsoft.com/
Note	
Controllo	**A.5.36 Conformità alle politiche, alle regole e agli standard per la sicurezza delle informazioni.**

Pubblico
Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

Descrizione del Controllo	*La conformità alla politica di sicurezza delle informazioni dell'organizzazione, alle politiche, alle regole e agli standard specifici per ogni argomento deve essere verificata regolarmente.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Ritenuto necessario per rendere efficace il SGI.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	CISO, DPO
Documentazione	• ERIT-SGI - Politica di sicurezza delle informazioni e la protezione dei dati personali
Note	
Controllo	**A.5.37 Procedure operative documentate**
Descrizione del Controllo	*Le procedure operative per le strutture di elaborazione delle informazioni devono essere documentate e rese disponibili al personale che ne ha bisogno.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Necessaria al corretto svolgimento delle attività.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	Head of Infrastructure & Operations
Documentazione	
Note	
Rif. Appendice A ISO/IEC 27001	**A.6 Controlli sulle persone**
Controllo	**A.6.1 Screening**
Descrizione del Controllo	*I controlli sui precedenti di tutti i candidati a diventare personale devono essere effettuati prima di entrare a far parte dell'organizzazione e su base continuativa, tenendo conto delle leggi, dei regolamenti e dell'etica applicabili e devono essere proporzionati ai requisiti aziendali, alla classificazione delle informazioni a cui si deve accedere e ai rischi percepiti.*
Incluso	Sì

Pubblico
Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

Motivazione per l'inclusione / Esclusione	Necessaria al corretto svolgimento delle attività.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	Chief People & Sustainability Officer
Documentazione	• RU-001A Selezione e reclutamento Rev. 05 08-09-21
Note	
Controllo	**A.6.2 Termini e condizioni di lavoro**
Descrizione del Controllo	*Gli accordi contrattuali di lavoro devono indicare le responsabilità del personale e dell'organizzazione in materia di sicurezza delle informazioni.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Necessaria al corretto svolgimento delle attività.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	Chief People & Sustainability Officer
Documentazione	• Presa visione e adesione _ICT
Note	
Controllo	**A.6.3 Sensibilizzazione, educazione e formazione sulla sicurezza delle informazioni**
Descrizione del Controllo	*Il personale dell'organizzazione e le parti interessate devono ricevere un'adeguata sensibilizzazione, istruzione e formazione in materia di sicurezza delle informazioni e aggiornamenti periodici della politica di sicurezza delle informazioni dell'organizzazione, delle politiche e delle procedure specifiche per ogni argomento, in base alle funzioni svolte.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Necessaria al corretto svolgimento delle attività.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	CISO, Chief People & Sustainability Officer

Pubblico

Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

Documentazione	• ERIT-SGI - Politica di sicurezza delle informazioni e la protezione dei dati personali (CSP, CSC) • Edenred IT Security Awareness Guidelines (CSC) • Contratto Microsoft (CSC) • Contratto Mulesoft (CSC)
Note	
Controllo	**A.6.4 Processo disciplinare**
Descrizione del Controllo	*È necessario formalizzare e comunicare un processo disciplinare per intraprendere azioni contro il personale e le altre parti interessate che hanno commesso una violazione della politica di sicurezza delle informazioni.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Ritenuto necessario per rendere efficace il SGI.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	CISO
Documentazione	• ERIT-SGI - Politica di sicurezza delle informazioni e la protezione dei dati personali • 6.4 - Allegato A al codice di comportamento
Note	
Controllo	**A.6.5 Responsabilità dopo la cessazione o il cambiamento del rapporto di lavoro**
Descrizione del Controllo	*Le responsabilità e i doveri in materia di sicurezza delle informazioni che rimangono validi anche dopo la cessazione o il cambiamento del rapporto di lavoro devono essere definiti, applicati e comunicati al personale interessato e alle altre parti coinvolte.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Necessaria al corretto svolgimento delle attività.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	Chief People & Sustainability Officer, Head of Infrastructure & Operations
Documentazione	• Impegno di riservatezza
Note	

Pubblico

Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

Controllo	A.6.6 Accordi di riservatezza o di non divulgazione
Descrizione del Controllo	*Gli accordi di riservatezza o di non divulgazione che riflettono le esigenze dell'organizzazione in materia di protezione delle informazioni devono essere identificati, documentati, regolarmente rivisti e firmati dal personale e dalle altre parti interessate.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Necessaria al corretto svolgimento delle attività.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	Chief People & Sustainability Officer, DPO
Documentazione	• ERIT-SGI - Classificazione delle Informazioni • ERIT-SGI - Gestione sicura dei Fornitori • Impegno di riservatezza
Note	
Controllo	**A.6.7 Remote working**
Descrizione del Controllo	*Le misure di sicurezza devono essere implementate quando il personale lavora in remoto per proteggere le informazioni a cui si accede, che vengono elaborate o archiviate al di fuori dei locali dell'organizzazione.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Necessaria al corretto svolgimento delle attività.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	CISO, Head of Infrastructure & Operations
Documentazione	• ERIT-SGI-Policy smartworking
Note	
Controllo	**A.6.8 Segnalazione di eventi di sicurezza informatica**
Descrizione del Controllo	*L'organizzazione deve fornire un meccanismo che consenta al personale di segnalare tempestivamente eventi di sicurezza delle informazioni osservati o sospetti attraverso i canali appropriati.*
Incluso	Sì

Pubblico
Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

Motivazione per l'inclusione / Esclusione	Ritenuto necessario per rendere efficace il SGI.
Livello di Implementazione	Implementato
Ownership	Edenred SE
Referente	CISO, SOC
Documentazione	• SEC-PRO-030-Security monitoring use case creation • ERIT-SGI - Gestione degli incidenti di sicurezza (CSP, CSC) • ERIT-SEC-22301-Business Continuity Plan (CSP) • ERIT- Misure di sicurezza Welfare e Ticket Restaurant (CSP) • Contratto Microsoft (CSC) • Contratto Mulesoft (CSC)
Note	
Rif. Appendice A ISO/IEC 27001	**A.7 Controlli fisici**
Controllo	**A.7.1 Perimetro di sicurezza fisica**
Descrizione del Controllo	*I perimetri di sicurezza devono essere definiti e utilizzati per proteggere le aree che contengono informazioni e altre risorse associate.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Necessaria al corretto svolgimento delle attività.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	Head of Procurement & Facility, Head of Infrastructure & Operations
Documentazione	• ERIT-SGI-Accessi Fisici • ERIT-SGI - Network Security
Note	
Controllo	**A.7.2 Accesso fisico**
Descrizione del Controllo	*Le aree di sicurezza devono essere protette da controlli e punti di accesso adeguati.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Necessaria al corretto svolgimento delle attività.

Pubblico
Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	Head of Procurement & Facility
Documentazione	• ERIT-SGI-Accessi Fisici
Note	
Controllo	**A.7.3 Rendere sicuri uffici, locali e strutture**
Descrizione del Controllo	*Deve essere progettata e applicata la sicurezza fisica agli uffici, ai locali ed agli impianti.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Necessaria al corretto svolgimento delle attività.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	Head of Procurement & Facility
Documentazione	• ERIT-SGI-Accessi Fisici
Note	
Controllo	**A.7.4 Monitoraggio della sicurezza fisica**
Descrizione del Controllo	*I locali devono essere costantemente monitorati per individuare eventuali accessi fisici non autorizzati.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Necessaria al corretto svolgimento delle attività.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	Head of Procurement & Facility
Documentazione	• ERIT-SGI-Accessi Fisici
Note	
Controllo	**A.7.5 Protezione dalle minacce fisiche e ambientali**
Descrizione del Controllo	*La protezione contro le minacce fisiche e ambientali, come i disastri naturali e altre minacce fisiche intenzionali o non intenzionali alle infrastrutture, deve essere progettata e implementata.*

Pubblico

Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

Incluso	Sì
Motivazione per l'inclusione / Esclusione	Necessaria al corretto svolgimento delle attività.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	Head of Procurement & Facility
Documentazione	• ERIT-SGI-Accessi Fisici • ERIT-SGI-22301-Scenari di Indisponibilità e Gestione Operativa
Note	
Controllo	**A.7.6 Lavoro in aree sicure**
Descrizione del Controllo	*Proteggere le informazioni e le altre risorse associate in aree sicure da danni e interferenze non autorizzate da parte del personale che lavora in tali aree.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Necessaria al corretto svolgimento delle attività.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	Head of Infrastructure & Operations
Documentazione	• ERIT-SGI-Accessi Fisici
Note	
Controllo	**A.7.7 Politica di schermo e scrivania puliti**
Descrizione del Controllo	*Devono essere adottate sia una politica di "scrivania pulita" per i documenti ed i supporti di memorizzazione rimovibili, sia una politica di "schermo pulito" per i servizi di elaborazione delle informazioni.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Richiesto dalla valutazione del rischio.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	CISO
Documentazione	• ERIT-SGI-IT Charter

Pubblico

Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

Note	
Controllo	**A.7.8 Disposizione delle apparecchiature e loro protezione**
Descrizione del Controllo	*Le apparecchiature devono essere disposte in modo sicuro e protetto.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Necessaria al corretto svolgimento delle attività
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	CISO, Head of Infrastructure & Operations, Head of Procurement & Facility
Documentazione	• ERIT-SGI-Accessi Fisici
Note	
Controllo	**A.7.9 Sicurezza degli asset all'esterno delle sedi**
Descrizione del Controllo	*Gli asset all'esterno delle sedi devono essere protetti.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Necessaria al corretto svolgimento delle attività
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	CISO, Head of Infrastructure & Operations
Documentazione	• ERIT-SGI-IT Charter
Note	
Controllo	**A.7.10 Supporti di memorizzazione**
Descrizione del Controllo	*I supporti di memorizzazione devono essere gestiti durante il loro ciclo di vita di acquisizione, uso, trasporto e smaltimento in conformità allo schema di classificazione e ai requisiti di gestione dell'organizzazione.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Necessaria al corretto svolgimento delle attività
Livello di Implementazione	Implementato

Pubblico
Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

Ownership	Edenred Italia
Referente	Head of Infrastructure & Operations
Documentazione	• ERIT-SGI-IT Charter
Note	
Controllo	**A.7.11 Infrastrutture di supporto**
Descrizione del Controllo	*Le apparecchiature devono essere protette da malfunzionamenti alla rete elettrica di alimentazione e da altri disservizi causati da malfunzionamenti dei servizi ausiliari.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Necessaria al corretto svolgimento delle attività
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	Head of Procurement & Facility
Documentazione	• ERIT-SGI-Accessi Fisici
Note	
Controllo	**A.7.12 Sicurezza dei cablaggi**
Descrizione del Controllo	*I cavi per l'energia elettrica e le telecomunicazioni adibiti al trasporto di dati o a supporto di servizi informativi devono essere protetti da intercettazioni, interferenze o danneggiamenti.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Necessaria al corretto svolgimento delle attività
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	Head of Infrastructure & Operations, Head of Procurement & Facility
Documentazione	• ERIT-SGI-Accessi Fisici • 7.12 - DVRUF3_EDE01_02102023 • 7.12 - 1 pagina firmata DVR Sede Milano
Note	
Controllo	**A.7.13 Manutenzione delle apparecchiature**

Pubblico
Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

Descrizione del Controllo	*Le apparecchiature devono essere correttamente mantenute per garantire la disponibilità, l'integrità e la riservatezza delle informazioni.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Necessaria al corretto svolgimento delle attività
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	Head of Infrastructure & Operations
Documentazione	• ERIT-SGI - Gestione Attrezzature Inventario HW • 7.13 - BitLocker • 7.13 - Device Overview
Note	
Controllo	**A.7.14 Dismissione sicura o riutilizzo delle apparecchiature**
Descrizione del Controllo	*Le apparecchiature contenenti supporti di memorizzazione devono essere verificate per assicurare che tutti i dati sensibili e il software con licenza siano stati rimossi o sovrascritti in modo sicuro prima dello smaltimento o del riutilizzo.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Richiesto dalla valutazione del rischio
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	Head of Infrastructure & Operations
Documentazione	• ERIT-SGI-IT Charter (CSC) • ERIT- Misure di sicurezza Welfare e Ticket Restaurant (CSP) • Contratto Microsoft (CSC) • Contratto Mulesoft (CSC)
Note	
Rif. Appendice A ISO/IEC 27001	**A.8 Controlli tecnologici**
Controllo	**A.8.1 Dispositivi endpoint dell'utente**
Descrizione del Controllo	*Le informazioni memorizzate, elaborate o accessibili tramite i dispositivi endpoint degli utenti devono essere protette.*
Incluso	Sì

Pubblico

Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

Motivazione per l'inclusione / Esclusione	Richiesto dalla valutazione del rischio.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	Head of Infrastructure & Operations
Documentazione	• ERIT-SGI-IT Charter
Note	
Controllo	**A.8.2 Diritti di accesso privilegiato**
Descrizione del Controllo	*L'assegnazione e l'uso dei diritti di accesso privilegiato devono essere limitati e gestiti.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Richiesto dalla valutazione del rischio.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	Head of Infrastructure & Operations
Documentazione	• ERIT-SGI - Gestione Accessi Logici (CSP) • ERIT-SGI - Gestione Utenti (CSP) • Contratto Microsoft (CSC) • Contratto Mulesoft (CSC)
Note	
Controllo	**A.8.3 Limitazione dell'accesso alle informazioni**
Descrizione del Controllo	*L'accesso alle informazioni e alle altre risorse associate deve essere limitato in conformità alla politica di controllo degli accessi stabilita per ogni argomento.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Necessaria al corretto svolgimento delle attività.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	Head of Infrastructure & Operations
Documentazione	• ERIT-SGI - Gestione Accessi Logici (CSP)

Pubblico

Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

	• ERIT-SGI - Gestione Utenti (CSP) • Contratto Microsoft (CSC) • Contratto Mulesoft (CSC)
Note	
Controllo	**A.8.4 Accesso al codice sorgente**
Descrizione del Controllo	*L'accesso in lettura e scrittura al codice sorgente, agli strumenti di sviluppo e alle librerie software deve essere gestito in modo appropriato.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Necessaria al corretto svolgimento delle attività
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	Head of Core & Digital Solutions
Documentazione	• ERIT-SGI-Policy sviluppo sicuro • Evidenze flusso rilasci - 1 • Evidenze flusso rilasci - 2 • Evidenze flusso rilasci - 3 • 8.4 - Access to source code - 1 • 8.4 - Access to source code - 2
Note	
Controllo	**A.8.5 Autenticazione sicura**
Descrizione del Controllo	*Le tecnologie e le procedure di autenticazione sicura devono essere implementate in base alle informazioni e la politica di controllo degli accessi specifica dell'argomento.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Necessaria al corretto svolgimento delle attività.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	CISO, Head of Infrastructure & Operations
Documentazione	• ERIT-SGI - Gestione Accessi Logici
Note	
Controllo	**A.8.6 Gestione della capacità**

Pubblico

Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

Descrizione del Controllo	*L'uso delle risorse deve essere monitorato e regolato in linea con i requisiti di capacità attuali e previsti.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Necessaria al corretto svolgimento delle attività.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	Head of Infrastructure & Operations, Head of Procurement & Facility
Documentazione	• ERIT-SGI - CapacityManagement (CSP) • SEC-POL-019-Infrastructure Security Policy_202602(CSP) • Contratto Microsoft (CSC) • Contratto Mulesoft (CSC)
Note	
Controllo	**A.8.7 Protezione contro i malware**
Descrizione del Controllo	*La protezione contro le minacce informatiche deve essere implementata e supportata da un'adeguata sensibilizzazione degli utenti.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Necessaria al corretto svolgimento delle attività.
Livello di Implementazione	Implementato
Ownership	Edenred Italia; Edenred SE
Referente	CISO, Head of Infrastructure & Operations
Documentazione	• ERIT-SGI - Network Security • Richiesta svolgimento corsi obbligatori neoassunti
Note	
Controllo	**A.8.8 Gestione delle vulnerabilità tecniche**
Descrizione del Controllo	*È necessario ottenere informazioni sulle vulnerabilità tecniche dei sistemi informativi in uso, valutare l'esposizione dell'organizzazione a tali vulnerabilità e adottare misure adeguate.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Richiesto dalla valutazione del rischio.

Pubblico
Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	CISO, Head of Infrastructure & Operations, Head of Core & Digital Solutions
Documentazione	• ERIT-SGI - Gestione delle Vulnerabilità (CSP, CSC) • ERIT-SGI - Policy sviluppo sicuro (CSP, CSC) • Data Processing Agreement (CSP) • ERIT- Misure di sicurezza Welfare e Ticket Restaurant (CSP) • Contratto Microsoft (CSP, CSC) • Contratto Mulesoft (CSP, CSC)
Note	
Controllo	**A.8.9 Gestione delle configurazioni**
Descrizione del Controllo	*Le configurazioni, comprese quelle di sicurezza, di hardware, software, servizi e reti devono essere stabilite, documentate, implementate, monitorate e riviste.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Necessaria al corretto svolgimento delle attività
Livello di Implementazione	Implementato
Ownership	Edenred SE
Referente	Head of Infrastructure & Operations
Documentazione	• SEC-POL-019-Infrastructure Security Policy_202602
Note	
Controllo	**A.8.10 Cancellazione delle informazioni**
Descrizione del Controllo	*Le informazioni memorizzate nei sistemi informativi, nei dispositivi o in qualsiasi altro supporto di memorizzazione devono essere eliminate quando non sono più necessarie.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Ritenuto necessario per rendere efficace il SGI.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	Head of Infrastructure & Operations, CISO
Documentazione	• ERIT-SGI - Data Retention Policy

Pubblico

Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

Note	
Controllo	**A.8.11 Mascheramento dei dati**
Descrizione del Controllo	*La mascheratura dei dati deve essere utilizzata in conformità alla politica specifica dell'organizzazione sul controllo degli accessi e ad altre politiche specifiche correlate, nonché ai requisiti aziendali, tenendo conto della legislazione applicabile.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Ritenuto necessario per rendere efficace il SGI.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	Head of Test & QA
Documentazione	• ERIT-SGI - Data Masking Procedure
Note	
Controllo	**A.8.12 Prevenzione della fuga di dati**
Descrizione del Controllo	*Le misure di prevenzione delle fughe di dati devono essere applicate ai sistemi, alle reti e a qualsiasi altro dispositivo che elabora, memorizza o trasmette informazioni sensibili.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Necessaria al corretto svolgimento delle attività.
Livello di Implementazione	Implementato
Ownership	Edenred Italia, Edenred SE
Referente	Head of Infrastructure & Operations
Documentazione	• DLP_EDENRED ITALY_INFORMATIVA PRIVACY • Edenred_DLP PIA_ERIT_10072023 • ERIT-SGI-IT Charter • ERIT-SGI-Gestione Data Breach
Note	
Controllo	**A.8.13 Backup delle informazioni**
Descrizione del Controllo	*Le copie di backup delle informazioni, del software e dei sistemi devono essere mantenute e testate periodicamente in conformità con la politica di backup concordata per l'argomento specifico.*
Incluso	Sì

Pubblico

Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

Motivazione per l'inclusione / Esclusione	Necessaria al corretto svolgimento delle attività.
Livello di Implementazione	Implementato
Ownership	Edenred Italia, Edenred SE
Referente	Head of Infrastructure & Operations
Documentazione	• SEC-POL-018- IT Resilience & Backup Policy (CSP, CSC)
Note	
Controllo	**A.8.14 Ridondanza delle strutture di elaborazione delle informazioni**
Descrizione del Controllo	*Le strutture di elaborazione delle informazioni devono essere implementate con una ridondanza sufficiente a soddisfare i requisiti di disponibilità.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Necessaria al corretto svolgimento delle attività.
Livello di Implementazione	Implementato
Ownership	Edenred SE
Referente	Head of Infrastructure & Operations
Documentazione	• EDNR IT - DXC Recovery Guidance New version 09052024
Note	
Controllo	**A.8.15 Registrazione**
Descrizione del Controllo	*I registri che registrano le attività, le eccezioni, i guasti e altri eventi rilevanti devono essere prodotti, archiviati, protetti e analizzati.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Richiesto dalla valutazione del rischio / Requisito di legge.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	Head of Infrastructure & Operations
Documentazione	• ERIT-SGI - Gestione dei Log (CSP) • Data Processing Agreement (CSP) • ERIT- Misure di sicurezza Welfare e Ticket Restaurant (CSP) • Contratto Microsoft (CSP, CSC)

Pubblico

Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

	• Contratto Mulesoft (CSP, CSC)
Note	
Controllo	**A.8.16 Attività di monitoraggio**
Descrizione del Controllo	*Le reti, i sistemi e le applicazioni devono essere monitorati per rilevare comportamenti anomali e devono essere intraprese azioni appropriate per valutare potenziali incidenti di sicurezza delle informazioni.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Ritenuto necessario per rendere efficace il SGI.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	CISO, Head of Infrastructure & Operations, SOC
Documentazione	• ERIT-SGI - Network Security • ERIT-SGI - Gestione degli incidenti di sicurezza
Note	
Controllo	**A.8.17 Sincronizzazione dell'orologio**
Descrizione del Controllo	*Gli orologi dei sistemi di elaborazione delle informazioni utilizzati dall'organizzazione devono essere sincronizzati rispetto a fonti di tempo approvate.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Richiesto dalla valutazione del rischio.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	Head of Infrastructure & Operations
Documentazione	• ERIT-SGI - Gestione dei Log (CSP) • Data Processing Agreement (CSP) • Contratto Microsoft (CSP, CSC) • Contratto Mulesoft (CSP, CSC)
Note	
Controllo	**A.8.18 Utilizzo di programmi di utilità privilegiati**
Descrizione del Controllo	*L'uso di programmi di utilità che possono scavalcare i controlli del sistema e dell'applicazione deve essere limitato e strettamente controllato.*

Pubblico
Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

Incluso	Sì
Motivazione per l'inclusione / Esclusione	Ritenuto necessario per rendere efficace il SGI.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	Head of Infrastructure & Operations
Documentazione	• ERIT-SGI - Gestione Accessi Logici (CSP) • 8.18 - 8.19 Use of privileged utility programs - 1 • 8.18 - 8.19 Use of privileged utility programs - 2
Note	
Controllo	**A.8.19 Installazione di software su sistemi operativi**
Descrizione del Controllo	*È necessario implementare procedure e misure per gestire in modo sicuro l'installazione del software sui sistemi operativi.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Necessaria al corretto svolgimento delle attività.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	Head of Infrastructure & Operations
Documentazione	• ERIT-SGI - Gestione Accessi Logici • 8.18 - 8.19 Use of privileged utility programs - 1 • 8.18 - 8.19 Use of privileged utility programs - 2
Note	
Controllo	**A.8.20 Sicurezza delle reti**
Descrizione del Controllo	*Le reti e i dispositivi di rete devono essere protetti, gestiti e controllati per proteggere le informazioni nei sistemi e nelle applicazioni.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Necessaria al corretto svolgimento delle attività.
Livello di Implementazione	Implementato
Ownership	Edenred Italia

Pubblico
Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

Referente	Head of Infrastructure & Operations
Documentazione	• ERIT-SGI - Network Security
Note	
Controllo	**A.8.21 Sicurezza dei servizi di rete**
Descrizione del Controllo	*I meccanismi di sicurezza, i livelli di servizio e i requisiti di servizio dei servizi di rete devono essere identificati, implementati e monitorati.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Necessaria al corretto svolgimento delle attività.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	Head of Infrastructure & Operations
Documentazione	• ERIT-SGI - Network Security
Note	
Controllo	**A.8.22 Segregazione delle reti**
Descrizione del Controllo	*I gruppi di servizi informativi, gli utenti e i sistemi informativi devono essere segregati nelle reti dell'organizzazione.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Necessaria al corretto svolgimento delle attività.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	Head of Infrastructure & Operations
Documentazione	• ERIT-SGI - Network Security (CSP) • SEC-POL-019-Infrastructure Security Policy_202602(CSC) • Contratto Microsoft (CSC) • Contratto Mulesoft (CSC)
Note	
Controllo	**A.8.23 Filtraggio web**
Descrizione del Controllo	*L'accesso ai siti web esterni deve essere gestito per ridurre l'esposizione a contenuti dannosi.*
Incluso	Sì

Pubblico

Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

Motivazione per l'inclusione / Esclusione	Necessaria al corretto svolgimento delle attività.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	Head of Infrastructure & Operations
Documentazione	• ERIT-SGI-IT Charter
Note	
Controllo	**A.8.24 Utilizzo della crittografia**
Descrizione del Controllo	*Devono essere definite e attuate regole per l'uso efficace della crittografia, compresa la gestione delle chiavi crittografiche.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Richiesto dalla valutazione del rischio.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	Head of Infrastructure & Operations
Documentazione	• ERIT-SGI - Politica di crittografia (CSP, CSC) • SEC-GUI-039-Cryptography & Secure Protocols Guidelines_2026 version (CSC) • Contratto Microsoft (CSC)
Note	
Controllo	**A.8.25 Ciclo di vita dello sviluppo sicuro**
Descrizione del Controllo	*È necessario stabilire e applicare regole per lo sviluppo sicuro di software e sistemi.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Necessaria al corretto svolgimento delle attività.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	CISO
Documentazione	• ERIT-SGI - Policy sviluppo sicuro (CSP)

Pubblico

Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

	• Contratto Microsoft (CSC) • Contratto Mulesoft (CSC)
Note	
Controllo	**A.8.26 Requisiti di sicurezza delle applicazioni**
Descrizione del Controllo	*I requisiti di sicurezza delle informazioni devono essere identificati, specificati e approvati durante lo sviluppo o l'acquisizione di applicazioni.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Necessaria al corretto svolgimento delle attività / Richiesto dalla valutazione del rischio.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	CISO
Documentazione	• ERIT-SGI - Policy sviluppo sicuro • 8.26 - Secure Coding Third Party - Evaluation • 8.26 - Secure Coding Third Party - Matrix • 8.26 - Edenred - Compartiva Payroll HR • [SGSI-633] Valutazione tecnica - Corso Secure Code 2024 - Jira • [SGSI-632] Valutazione tecnica - SonarQube - Local-Cloud e Security • OWASP_MASVS-v1.2-en • SecureCoding - SonarLint Rule IDE - 1 • SecureCoding - SonarLint Rule IDE - 2 • SecureCoding - Pipeline DEVOPS
Note	
Controllo	**A.8.27 Architettura sicura dei sistemi e principi di ingegneria**
Descrizione del Controllo	*I principi per la progettazione di sistemi sicuri devono essere stabiliti, documentati, mantenuti e applicati a tutte le attività di sviluppo di sistemi informativi.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Necessaria al corretto svolgimento delle attività.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	CISO, Head of Core & Digital Solutions, Head of Enterprise Architecture
Documentazione	• ERIT-SGI - Policy sviluppo sicuro

Pubblico

Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

	• PACCHETTO FORNITURA IT • 8.27 - 1.3 PACCHETTO FORNITURA IT - NON IT - LITE
Note	
Controllo	**A.8.28 Secure coding**
Descrizione del Controllo	*I principi di Secure coding devono essere applicati allo sviluppo del software.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Necessaria al corretto svolgimento delle attività.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	CISO, Head of Core & Digital Solutions
Documentazione	• ERIT-SGI - Policy sviluppo sicuro • [SGSI-633] Valutazione tecnica - Corso Secure Code 2024 - Jira • [SGSI-632] Valutazione tecnica - SonarQube - Local-Cloud e Security • OWASP_MASVS-v1.2-en • SecureCoding - SonarLint Rule IDE - 1 • SecureCoding - SonarLint Rule IDE - 2 • SecureCoding - Pipeline DEVOPS • 8.28 - Blocking_Mode_SonarQube • 8.28 - Secure coding PT
Note	
Controllo	**A.8.29 Test di sicurezza in fase di sviluppo**
Descrizione del Controllo	*I processi di verifica della sicurezza devono essere definiti e implementati nel ciclo di vita dello sviluppo.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Necessaria al corretto svolgimento delle attività.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	CISO
Documentazione	• ERIT-SGI - Policy sviluppo sicuro
Note	

Pubblico

Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

Controllo	A.8.30 Sviluppo in outsourcing
Descrizione del Controllo	*L'organizzazione deve dirigere, monitorare e rivedere le attività relative allo sviluppo di sistemi in outsourcing.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Necessaria al corretto svolgimento delle attività.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	CISO
Documentazione	• ERIT-SGI-Policy Sviluppo Software Fornitori
Note	
Controllo	**A.8.31 Separazione degli ambienti di sviluppo, test e produzione**
Descrizione del Controllo	*Gli ambienti di sviluppo, test e produzione devono essere separati e protetti.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Necessaria al corretto svolgimento delle attività
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	Head of Core & Digital Solutions, Head of Enterprise Architecture
Documentazione	• ERIT-SGI - Policy sviluppo sicuro
Note	
Controllo	**A.8.32 Change management**
Descrizione del Controllo	*Le modifiche alle strutture di elaborazione delle informazioni e ai sistemi informativi devono essere soggette a procedure di gestione del cambiamento.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Necessaria al corretto svolgimento delle attività.
Livello di Implementazione	Implementato
Ownership	Edenred Italia

Pubblico
Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

Referente	Head of Enterprise Architecture, Head of Infrastructure & Operations, Head of Core & Digital Solutions
Documentazione	• ERIT-SGI - Change & Release Management Process (CSP, CSC) • 8.1 - Release and deploy management • 8.1 - UAT Refresh Calendar 2024 • 8.1 - Release Calendar 2024 • 8.1 - Release Management Process - V2.4 • 8.1 - Release Management - Change Request v1.1 • Evidenze flusso rilasci - 1 • Evidenze flusso rilasci - 2 • Evidenze flusso rilasci - 3 • 8.32 - Change management • Change Management Confluence • EA-DevOps - GIT Flow Guidelines-220725-092701 • ERIT-SGI-Change Request (CSP) • ERIT- Misure di sicurezza Welfare e Ticket Restaurant (CSP) • Data Processing Agreement (CSP) • Contratto Microsoft (CSC) • Contratto Mulesoft (CSC)
Note	
Controllo	**A.8.33 Informazioni sul test**
Descrizione del Controllo	*Le informazioni di test devono essere selezionate, protette e gestite in modo appropriato.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Necessaria al corretto svolgimento delle attività.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	CISO, Head of Test & QA
Documentazione	• ERIT-SGI - Policy sviluppo sicuro
Note	
Controllo	**A.8.34 Protezione dei sistemi informativi durante le prove di audit**
Descrizione del Controllo	*I test di audit e le altre attività di assurance che comportano la valutazione dei sistemi operativi devono essere pianificati e concordati tra il tester e la direzione competente.*

Pubblico

Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

Incluso	Sì
Motivazione per l'inclusione / Esclusione	Ritenuto necessario per rendere efficace il SGI.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	CISO
Documentazione	• ERIT-SGI-27001-Piano di Audit-2026
Note	

2.2. Controlli ISO 27701:2019

Rif. Appendice A ISO/IEC 27701	**A.1 Obiettivi di controllo e controlli** **A. 7.2 Condizioni per la raccolta e trattamento**
Controllo	**A.7.2.1 Identificare e documentare le finalità**
Descrizione del Controllo	L'organizzazione deve identificare e documentare le finalità specifiche per cui i dati personali saranno trattati.
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Necessaria al corretto svolgimento delle attività.
Ownership	Edenred Italia, Edenred SE
Referente	DPO
Documentazione	• Registro dei trattamenti • Informativa privacy
Note	
Controllo	**A.7.2.2 Identificare la base giuridica**
Descrizione del Controllo	*L'organizzazione deve determinare, documentare e rispettare la base legittima per il trattamento dei dati personali per le finalità identificate.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Necessaria al corretto svolgimento delle attività.
Ownership	Edenred Italia, Edenred SE
Referente	DPO
Documentazione	• Registro dei trattamenti

Pubblico

Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

	• Informativa privacy
Note	
Controllo	**A.7.2.3 Determinare quando e come ottenere il consenso.**
Descrizione del Controllo	*L'organizzazione deve determinare e documentare un processo con cui dimostrare se, come e quando è stato ottenuto il consenso per il trattamento dei dati personali da parte dei soggetti interessati (beneficiari).*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Richiesto dalla valutazione del rischio.
Ownership	Edenred Italia, Edenred SE
Referente	DPO
Documentazione	• ERIT-SGI - Procedura di Gestione dei consensi • ERIT-SGI - Linee Guida sulla Protezione dei Dati Personali • ERIT-SGI - Politica Gestione Diritti interessati
Note	
Controllo	**A.7.2.4 Ottenere e registrare il consenso**
Descrizione del Controllo	*L'organizzazione deve ottenere e registrare il consenso dei soggetti interessati (beneficiari) secondo i processi documentati.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Necessaria al corretto svolgimento delle attività.
Ownership	Edenred Italia, Edenred SE
Referente	DPO
Documentazione	• ERIT-SGI - Procedura di Gestione dei Consensi • ERIT-SGI - Politica Gestione Diritti interessati
Note	
Controllo	**A.7.2.5 Valutazione dell'impatto sulla privacy**
Descrizione del Controllo	*L'organizzazione deve valutare la necessità di una valutazione dell'impatto sulla privacy e implementarla, se necessario, ogni volta che vengano introdotti nuovi trattamenti di dati personali o siano pianificate modifiche ai trattamenti esistenti.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Necessaria al corretto svolgimento delle attività.

Pubblico

Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

Ownership	Edenred Italia, Edenred SE
Referente	DPO
Documentazione	• ERIT-SGI - Linee Guida sulla Protezione dei Dati Personali
Note	
Controllo	**A.7.2.6 Contratti con i responsabili del trattamento dei dati personali**
Descrizione del Controllo	*L'organizzazione deve avere un contratto scritto con qualsiasi responsabile del trattamento dei dati personali che utilizza e deve garantire che i contratti con i responsabili del trattamento dei dati personali prevedano l'attuazione dei controlli appropriati di cui all'Allegato B.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Richiesto dalla valutazione del rischio.
Ownership	Edenred Italia, Edenred SE
Referente	DPO
Documentazione	• Data Processing Agreement • ERIT-SGI - Linee Guida sulla Protezione dei Dati Personali • ERIT-SGI - Procedura Security e Privacy by Design
Note	
Controllo	**A.7.2.7 Contitolare del trattamento dei dati personali**
Descrizione del Controllo	*L'organizzazione deve determinare i rispettivi ruoli e responsabilità per il trattamento dei dati personali (inclusi i requisiti di protezione e sicurezza dei dati personali) con qualsiasi co-titolare dei dati personali.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Richiesto dalla valutazione del rischio.
Ownership	Edenred Italia, Edenred SE
Referente	DPO
Documentazione	Non sono presenti rapporti di contitolarità
Note	
Controllo	**A.7.2.8 Registrazioni relative al trattamento dei dati personali**
Descrizione del Controllo	*L'organizzazione deve determinare e conservare in modo sicuro le registrazioni necessarie a supporto dei propri obblighi per il trattamento dei dati personali.*
Incluso	Sì

Pubblico
Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

Motivazione per l'inclusione / Esclusione	Richiesto dalla valutazione del rischio.
Ownership	Edenred Italia, Edenred SE
Referente	DPO
Documentazione	• Registri dei trattamenti • Informative privacy • ERIT-SGI - Linee Guida sulla Protezione dei Dati Personali
Note	
Rif. Appendice A ISO/IEC 27701	**A.1 Obiettivi di controllo e controlli** **A.7.3 Obblighi nei confronti dei soggetti interessati (beneficiari)**
Controllo	**A.7.3.1 Determinare e adempiere agli obblighi nei confronti dei soggetti interessati**
Descrizione del Controllo	*L'organizzazione deve determinare, documentare e rispettare i propri obblighi legali, normativi e aziendali nei confronti dei soggetti interessati (beneficiari) in relazione al trattamento dei dati personali e fornire i mezzi per soddisfare tali obblighi.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Necessaria al corretto svolgimento delle attività.
Ownership	Edenred Italia, Edenred SE
Referente	DPO
Documentazione	• Registri del trattamento • Informativa privacy • Valutazione del rischio • Autorizzazione al trattamento • Formazione • ERIT-SGI - Politica Gestione Diritti interessati • ERIT-SGI-Procedura Gestione Diritti interessati
Note	
Controllo	**A.7.3.2 Determinare le informazioni da fornire ai soggetti interessati (beneficiari)**
Descrizione del Controllo	*L'organizzazione deve determinare e documentare le informazioni da fornire ai soggetti interessati (beneficiari) in merito al trattamento dei loro dati personali e alle tempistiche di utilizzo*
Incluso	Sì

Pubblico

Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

Motivazione per l'inclusione / Esclusione	Necessaria al corretto svolgimento delle attività.
Ownership	Edenred Italia, Edenred SE
Referente	DPO, Privacy Manager
Documentazione	• Informativa privacy Beneficiari
Note	
Controllo	**A.7.3.3 Fornire informazioni ai soggetti interessati (beneficiari)**
Descrizione del Controllo	*L'organizzazione deve fornire ai soggetti interessati (beneficiari) con chiarezza e facilità di accesso informazioni relative a titolari e responsabile del trattamento dei dati personali*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Richiesto dalla valutazione del rischio.
Ownership	Edenred Italia, Edenred SE
Referente	DPO
Documentazione	• Informativa privacy Beneficiari • Form di Onetrust Edenred
Note	
Controllo	**A.7.3.4 Fornire un meccanismo per modificare o revocare il consenso**
Descrizione del Controllo	*L'organizzazione deve fornire un meccanismo che consenta ai responsabili dei dati personali di modificare o revocare il proprio consenso.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Necessaria al corretto svolgimento delle attività.
Ownership	Edenred Italia, Edenred SE
Referente	DPO, Privacy Manager
Documentazione	• ERIT-SGI - Procedura di Gestione dei Consensi • ERIT-SGI - Politica Gestione Diritti interessati • Portale Beneficiari (sezione modifica consensi) • Form di Onetrust Edenred • Informativa privacy Beneficiari
Note	

Pubblico
Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

Controllo	**A.7.3.5 Fornire un meccanismo per opporsi al trattamento dei dati personali**
Descrizione del Controllo	*L'organizzazione deve fornire un meccanismo che consenta ai soggetti interessati (beneficiari) di opporsi al trattamento dei loro dati personali.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Necessaria al corretto svolgimento delle attività.
Ownership	Edenred Italia, Edenred SE
Referente	DPO, Privacy Manager
Documentazione	• ERIT-SGI - Procedura di Gestione dei Consensi • ERIT-SGI - Politica Gestione Diritti interessati • Form di Onetrust Edenred • Informativa privacy Beneficiari
Note	
Controllo	**A.7.3.6 Accesso, rettifica e/o cancellazione**
Descrizione del Controllo	*L'organizzazione deve implementare politiche, procedure e/o meccanismi per soddisfare i propri obblighi nei confronti dei soggetti interessati (beneficiari) per l'accesso, la rettifica e/o la cancellazione dei dati personali.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Richiesto dalla valutazione del rischio.
Ownership	Edenred Italia, Edenred SE
Referente	DPO
Documentazione	• ERIT-SGI - Politica Gestione Diritti interessati • Form di Onetrust Edenred • ERIT-SGI-Linee Guida Cancellazione dei dati personali
Note	
Controllo	**A.7.3.7 Obblighi dei titolari del trattamento di dati personali di informare terze parti**
Descrizione del Controllo	*L'organizzazione deve implementare politiche, procedure e meccanismi per informare le terze parti con cui sono stati condivisi i dati personali di qualsiasi modifica, ritiro o obiezione relativa ai dati personali condivisi.*
Incluso	Sì

Pubblico
Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

Motivazione per l'inclusione / Esclusione	Necessaria al corretto svolgimento delle attività.
Ownership	Edenred Italia, Edenred SE
Referente	DPO
Documentazione	• Data Processing Agreement • Data Processing Agreement_titolare-titolare
Note	
Controllo	**A.7.3.8 Fornire una copia dei dati personali trattati**
Descrizione del Controllo	*L'organizzazione deve essere in grado di fornire una copia dei dati personali che vengono trattati, su richiesta dei soggetti interessati (beneficiari).*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Richiesto dalla valutazione del rischio.
Ownership	Edenred Italia, Edenred SE
Referente	DPO
Documentazione	• ERIT-SGI - Politica Gestione Diritti interessati • Form di Onetrust Edenred • Informativa privacy Beneficiari
Note	
Controllo	**A.7.3.9 Gestione delle richieste**
Descrizione del Controllo	*L'organizzazione deve definire e documentare le politiche e le procedure per la gestione e la risposta a richieste legittime da parte dei titolari dei dati personali.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Necessaria al corretto svolgimento delle attività.
Ownership	Edenred Italia, Edenred SE
Referente	DPO
Documentazione	• Data Processing Agreement del Cliente • Registro responsabili • Data Processing Agreement
Note	
Controllo	**A.7.3.10 Processo decisionale automatizzato**

Pubblico

Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

Descrizione del Controllo	*L'organizzazione deve identificare e affrontare tutti gli obblighi, compresi quelli legali, nei confronti dei titolari dei dati personali derivanti da decisioni prese dall'organizzazione e relative soggetti interessati (beneficiari) basati esclusivamente sul trattamento automatizzato dei dati personali.*
Incluso	No
Motivazione per l'inclusione / Esclusione	Non sono previsti sistemi automatici per le decisioni relative ai trattamenti dei dati personali
Ownership	Edenred Italia, Edenred SE
Referente	DPO
Documentazione	-
Note	-
Rif. Appendice A ISO/IEC 27701	**A.1 Obiettivi di controllo e controlli**
	A.7.4 Privacy by design and privacy by default
Controllo	**A.7.4.1 Limitare la raccolta**
Descrizione del Controllo	*L'organizzazione deve limitare la raccolta di dati personali al minimo indispensabile che sia pertinente, proporzionale e necessario per gli scopi identificati.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Necessaria al corretto svolgimento delle attività.
Ownership	Edenred Italia, Edenred SE
Referente	DPO
Documentazione	• ERIT-SGI - Linee Guida sulla Protezione dei Dati Personali • ERIT-SGI-Procedura Security e Privacy by Design
Note	
Controllo	**A.7.4.2 Limitare il trattamento**
Descrizione del Controllo	*L'organizzazione deve limitare il trattamento dei dati personali a ciò che è adeguato, pertinente e necessario per gli scopi identificati.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Necessaria al corretto svolgimento delle attività.
Ownership	Edenred Italia, Edenred SE
Referente	DPO

Pubblico
Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

Documentazione	• ERIT-SGI - Linee Guida sulla Protezione dei Dati Personali • ERIT-SGI-Procedura Security e Privacy by Design
Note	
Controllo	**A.7.4.3 Accuratezza e qualità**
Descrizione del Controllo	*L'organizzazione deve garantire e documentare che i dati personali siano accurati, completi e aggiornati quanto necessario per le finalità per le quali devono essere trattati, per tutto il loro ciclo di vita.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Richiesto dalla valutazione del rischio.
Ownership	Edenred Italia, Edenred SE
Referente	DPO
Documentazione	• ERIT-SGI - Linee Guida sulla Protezione dei Dati Personali • ERIT-SGI-Procedura Security e Privacy by Design
Note	
Controllo	**A.7.4.4 Obiettivi di minimizzazione dei dati personali**
Descrizione del Controllo	*L'organizzazione deve definire e documentare gli obiettivi di minimizzazione dei dati e come vengono raggiunti, compresi i meccanismi (come la de-identificazione) utilizzati.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Necessaria al corretto svolgimento delle attività.
Ownership	Edenred Italia, Edenred SE
Referente	DPO
Documentazione	• ERIT-SGI - Linee Guida sulla Protezione dei Dati Personali • ERIT-SGI-Procedura Security e Privacy by Design • ERIT-SGI - Data Masking Procedure • Formazione
Note	
Controllo	**A.7.4.5 De-identificazione e cancellazione dei dati personali al termine del trattamento**
Descrizione del Controllo	*L'organizzazione dovrà cancellare i dati personali o renderli in una forma che non permetta la (ri)identificazione dei soggetti interessati, non appena i dati personali originali non siano più necessari per gli scopi identificati.*

Pubblico
Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

Incluso	Sì
Motivazione per l'inclusione / Esclusione	Necessaria al corretto svolgimento delle attività.
Ownership	Edenred Italia, Edenred SE
Referente	DPO
Documentazione	• ERIT-SGI - Data Retention Policy • ERIT-SGI - Data Masking Procedure • ERIT-SGI-Linee Guida Cancellazione dei dati personali
Note	
Controllo	**A.7.4.6 File temporanei**
Descrizione del Controllo	*L'organizzazione deve assicurarsi che i file temporanei creati come risultato dell'elaborazione dei dati personali siano rimossi secondo procedure documentate entro un determinato periodo di tempo.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Richiesto dalla valutazione del rischio.
Ownership	Edenred Italia, Edenred SE
Referente	DPO
Documentazione	• ERIT-SGI - Procedura Security e Privacy by Design • ERIT-SGI - Linee Guida sulla Protezione dei Dati Personali
Note	
Controllo	**A.7.4.7 Conservazione**
Descrizione del Controllo	*L'organizzazione non deve conservare i dati personali più a lungo di quanto sia necessario per le finalità per le quali i dati personali sono trattati.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Necessaria al corretto svolgimento delle attività.
Ownership	Edenred Italia, Edenred SE
Referente	DPO
Documentazione	• ERIT-SGI - Data Retention Policy
Note	
Controllo	**A.7.4.8 Cancellazione**

Pubblico

Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

Descrizione del Controllo	*L'organizzazione deve disporre di politiche, procedure e/o meccanismi per la cancellazione dei dati personali.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Richiesto dalla valutazione del rischio.
Ownership	Edenred Italia, Edenred SE
Referente	DPO
Documentazione	• ERIT-SGI - Data Retention Policy • ERIT-SGI-Linee Guida Cancellazione dei dati personali
Note	
Controllo	**A.7.4.9 Controlli sulla trasmissione dei dati personali**
Descrizione del Controllo	*L'organizzazione deve sottoporre i dati personali inviati (ad esempio, inviati ad un'altra organizzazione) su una rete di trasmissione dati a controlli appropriati per garantire che i dati raggiungano la destinazione prevista.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Richiesto dalla valutazione del rischio.
Ownership	Edenred Italia, Edenred SE
Referente	DPO
Documentazione	• ERIT-SGI - Classificazione Delle Informazioni • DLP
Note	
Rif. Appendice A ISO/IEC 27701	**A.1 Obiettivi di controllo e controlli**
	A.7.5 Condivisione, trasferimento e divulgazione dei dati personali
Controllo	**A.7.5.1 Identificare la base per il trasferimento dei dati personali tra giurisdizioni.**
Descrizione del Controllo	*L'organizzazione deve identificare e documentare la base pertinente per il trasferimento dei dati personali tra giurisdizioni.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Necessaria al corretto svolgimento delle attività.
Ownership	Edenred Italia, Edenred SE
Referente	DPO

Pubblico
Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

Documentazione	• Transfer Impact Assessment • ERIT-SGI - Politica Trasferimento Dati verso Paesi Terzi
Note	
Controllo	**A.7.5.2 Paesi e organizzazioni internazionali verso cui i dati personali potrebbero essere trasferiti**
Descrizione del Controllo	*L'organizzazione deve specificare e documentare i paesi e le organizzazioni internazionali a cui i dati personali potrebbero essere trasferiti.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Necessaria al corretto svolgimento delle attività.
Ownership	Edenred Italia, Edenred SE
Referente	DPO
Documentazione	• ERIT-SGI - Politica Trasferimento Dati verso Paesi Terzi
Note	
Controllo	**A.7.5.3 Registri del trasferimento dei dati personali**
Descrizione del Controllo	*L'organizzazione deve registrare i trasferimenti dei dati personali da o verso terzi e garantire la cooperazione con tali parti per supportare richieste future relative agli obblighi nei confronti dei soggetti interessati (beneficiari)*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Richiesto dalla valutazione del rischio.
Ownership	Edenred Italia, Edenred SE
Referente	DPO
Documentazione	• Transfer Impact Assessment • Data Processing Agreement • ERIT-SGI - Politica Gestione Diritti interessati
Note	
Controllo	**A.7.5.4 Registrazione della diffusione dei dati personali a terzi**
Descrizione del Controllo	*L'organizzazione deve registrare le diffusioni dei dati personali a terzi, compreso quali informazioni personali sono state diffuse, a chi e in quale momento.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Necessaria al corretto svolgimento delle attività.

Pubblico

Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

Ownership	Edenred Italia, Edenred SE
Referente	DPO
Documentazione	• Registro Fornitori esterni
Note	

Rif. Appendice B ISO/IEC 27701	**B.1 Obiettivi di controllo e controlli** **B.8.2 Condizioni di raccolta e trattamento**
Controllo	**B.8.2.1 Accordo con il cliente**
Descrizione del Controllo	*L'organizzazione deve garantire che il contratto per il trattamento dei dati personali riguardi (laddove pertinente e tenendo conto della natura del trattamento e delle informazioni a disposizione dell'organizzazione) il ruolo dell'organizzazione nel fornire assistenza agli obblighi del cliente*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Necessaria al corretto svolgimento delle attività.
Ownership	Edenred Italia, Edenred SE
Referente	DPO
Documentazione	• Data Processing Agreement • ERIT-SGI - Procedura Gestione Diritti interessati • ERIT-SGI - Politica Gestione Diritti interessati
Note	
Controllo	**B.8.2.2 Finalità dell'organizzazione**
Descrizione del Controllo	*L'organizzazione deve garantire che i dati personali trattati per conto di un cliente non vengano trattati per alcuno scopo indipendentemente dalle istruzioni documentate del cliente.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Necessaria al corretto svolgimento delle attività.
Ownership	Edenred Italia, Edenred SE
Referente	DPO
Documentazione	• Autorizzazione al trattamento • Formazione personale • Data Processing Agreement

Pubblico

Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

Note	
Controllo	**B.8.2.3 Utilizzo per Marketing e pubblicità**
Descrizione del Controllo	*L'organizzazione non deve utilizzare i dati personali elaborati nell'ambito di un contratto per fini di marketing e pubblicità senza il previo consenso del soggetto interessato (beneficiari). L'organizzazione non deve porre tale consenso come condizione per ricevere il servizio.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Richiesto dalla valutazione del rischio.
Ownership	Edenred Italia, Edenred SE
Referente	DPO
Documentazione	• ERIT-SGI-Procedura di Gestione dei Consensi
Note	
Controllo	**B.8.2.4 Istruzioni in violazione della normativa**
Descrizione del Controllo	*L'organizzazione deve informare il cliente se, a suo avviso, un'istruzione di trattamento viola leggi o regolamenti in essere.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Necessaria al corretto svolgimento delle attività.
Ownership	Edenred Italia, Edenred SE
Referente	DPO
Documentazione	• Data Processing Agreement • Autorizzazione al trattamento
Note	
Controllo	**B.8.2.5 Obblighi nei confronti del cliente**
Descrizione del Controllo	*L'organizzazione deve fornire al cliente le informazioni appropriate che consentano di dimostrare la conformità ai propri obblighi.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Necessaria al corretto svolgimento delle attività.
Ownership	Edenred Italia, Edenred SE
Referente	DPO
Documentazione	• Informative

Pubblico

Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

	• ERIT-SGI - Procedura Gestione Diritti interessati • ERIT-SGI - Politica Gestione Diritti interessati • Data Processing Agreement
Note	
Controllo	**B.8.2.6 Registrazioni relative a trattamento dei dati personali**
Descrizione del Controllo	*L'organizzazione deve determinare e conservare la documentazione necessaria a supporto della dimostrazione della conformità ai propri obblighi (come specificato negli accordi in essere) per il trattamento dei dati personali effettuato per conto di un cliente.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Richiesto dalla valutazione del rischio.
Ownership	Edenred Italia, Edenred SE
Referente	DPO
Documentazione	• Registri dei trattamenti • Valutazione del rischio • Autorizzazione al trattamento • Informative • Formazione • Data Processing Agreement
Note	
Rif. Appendice B ISO/IEC 27701	**B.8.3 Obblighi verso i soggetti interessati**
Controllo	**B.8.3.1 Obblighi verso i soggetti interessati**
Descrizione del Controllo	*L'organizzazione deve fornire al cliente i mezzi per adempiere ai propri obblighi verso i soggetti interessati*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Necessaria al corretto svolgimento delle attività.
Ownership	Edenred Italia, Edenred SE
Referente	DPO
Documentazione	• ERIT-SGI - Procedura Gestione Diritti interessati • ERIT-SGI - Politica Gestione Diritti interessati • Informative privacy
Note	

Pubblico

Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

Rif. Appendice B ISO/IEC 27701	B.8.4 Privacy by design and privacy by default
Controllo	**B.8.4.1 File temporanei**
Descrizione del Controllo	*L'organizzazione deve garantire che i file temporanei creati come risultato del trattamento dei dati personali siano cancellati secondo procedure documentate entro un periodo specifico.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Necessaria al corretto svolgimento delle attività.
Ownership	Edenred Italia, Edenred SE
Referente	DPO
Documentazione	• ERIT-SGI - Procedura Security e Privacy by Design • ERIT-SGI - Linee Guida sulla Protezione dei Dati Personali
Note	
Controllo	**B.8.4.2 Restituzione, trasferimento o eliminazione dei dati personali**
Descrizione del Controllo	*L'organizzazione deve fornire le modalità per la restituzione, il trasferimento e/o la cancellazione dei dati personali in modo sicuro e deve mettere a disposizione del cliente la propria politica per l'esercizio di tale funzione.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Richiesto dalla valutazione del rischio.
Ownership	Edenred Italia, Edenred SE
Referente	DPO
Documentazione	• ERIT-SGI - Procedura Gestione Diritti interessati • ERIT-SGI - Politica Gestione Diritti interessati • Data Processing Agreement • ERIT-SGI-Linee Guida Cancellazione dei dati personali • ERIT-SGI-Policy sul trattamento dei dati personali in formato cartaceo
Note	
Controllo	**B.8.4.3 Controlli sulla trasmissione dei dati personali**
Descrizione del Controllo	*L'organizzazione deve sottoporre i dati personali trasmessi attraverso una rete di trasmissione dati gli appropriati controlli per garantire che gli stessi raggiungano la destinazione prevista.*
Incluso	Sì

Pubblico

Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

Motivazione per l'inclusione / Esclusione	Richiesto dalla valutazione del rischio.
Ownership	Edenred Italia, Edenred SE
Referente	DPO
Documentazione	• ERIT-SGI - Classificazione delle Informazioni
Note	
Rif. Appendice B ISO/IEC 27701	**B.8.5 Condivisione, trasferimento e divulgazione dei dati personali**
Controllo	**B.8.5.1 Regole per i trasferimenti di dati personali tra giurisdizioni**
Descrizione del Controllo	*L'organizzazione dovrà informare tempestivamente il cliente sulle regole per il trasferimento dei dati personali tra le varie giurisdizioni e su eventuali modifiche previste in questo ambito, in modo che il cliente abbia la possibilità di opporsi a tali cambiamenti o di rescindere il contratto.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Necessaria al corretto svolgimento delle attività.
Ownership	Edenred Italia, Edenred SE
Referente	DPO
Documentazione	• Informative privacy • Data Processing Agreement
Note	
Controllo	**B.8.5.2 Paesi e organizzazioni internazionali verso i quali i dati personali potrebbero essere trasferiti**
Descrizione del Controllo	*L'organizzazione dovrà specificare e documentare i paesi e le organizzazioni internazionali a cui i dati personali potrebbero essere eventualmente trasferiti.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Richiesto dalla valutazione del rischio.
Ownership	Edenred Italia, Edenred SE
Referente	DPO
Documentazione	• Transfer Impact Assessment • Registro dei trattamenti
Note	
Controllo	**B.8.5.3 Registrazioni della diffusione di dati personali a terzi**

Pubblico

Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

Descrizione del Controllo	*L'organizzazione deve registrare il trasferimento dei dati personali a terze parti, includendo quali dati personali sono stati divulgati, a chi e quando.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Richiesto dalla valutazione del rischio.
Ownership	Edenred Italia, Edenred SE
Referente	DPO
Documentazione	• Data Processing Agreement • Registro dei trattamenti • Informativa privacy
Note	
Controllo	**B.8.5.4 Notifica delle richieste di diffusione di dati personali**
Descrizione del Controllo	*L'organizzazione deve notificare al cliente qualsiasi richiesta legalmente vincolante di divulgazione dei dati personali, a meno che non sia altrimenti vietato dalla legge.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Necessaria al corretto svolgimento delle attività.
Ownership	Edenred Italia, Edenred SE
Referente	DPO
Documentazione	• Informative privacy • Data Processing Agreement
Note	
Controllo	**B.8.5.5 Diffusione dei dati personali legalmente vincolanti**
Descrizione del Controllo	*L'organizzazione deve rifiutare qualsiasi richiesta di diffusione dei dati personali che non sia legalmente vincolante, consultare il cliente corrispondente, ove legalmente consentito, prima di effettuare qualsiasi diffusione dei dati personali e accettare qualsiasi richiesta di diffusione dei dati personali concordata contrattualmente e autorizzata dal cliente corrispondente.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Richiesto dalla valutazione del rischio.
Ownership	Edenred Italia, Edenred SE
Referente	DPO
Documentazione	• Informative privacy

Pubblico

Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

	• Data Processing Agreement
Note	
Controllo	**B.8.5.6 Diffusione dei subappaltatori utilizzati per il trattamento di dati personali**
Descrizione del Controllo	*L'organizzazione deve comunicare al cliente l'eventuale utilizzo di subappaltatori per il trattamento dei dati personali prima dell'uso.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Necessaria al corretto svolgimento delle attività.
Ownership	Edenred Italia, Edenred SE
Referente	DPO
Documentazione	• Elenco fornitori uso esterno • Informative privacy
Note	
Controllo	**B.8.5.7 Incarico di un subappaltatore per il trattamento dei dati personali**
Descrizione del Controllo	*L'organizzazione può incaricare un subappaltatore di trattare dati personali solo se previsto dal contratto stipulato con il cliente.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Necessaria al corretto svolgimento delle attività.
Ownership	Edenred Italia, Edenred SE
Referente	DPO
Documentazione	• Informative privacy • Contratto • Data Processing Agreement
Note	
Controllo	**B.8.5.8 Modifica del subappaltatore per il trattamento dei dati personali**
Descrizione del Controllo	*L'organizzazione deve, nel caso in cui sia in possesso di un'autorizzazione generale scritta, informare il cliente di qualsiasi modifica prevista relativa all'aggiunta o alla sostituzione di subappaltatori per il trattamento dei dati personali, dando al cliente la possibilità di opporsi a tali modifiche.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Richiesto dalla valutazione del rischio.

Pubblico

Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

Ownership	Edenred Italia, Edenred SE
Referente	DPO
Documentazione	• Informative privacy • Data Processing Agreement
Note	

2.3. Controlli ISO 27017:2015

Rif. ISO/IEC 27017	**Annex A controlli aggiuntivi**
Controllo	**CLD 6.3.1 Shared roles and responsibilities within a cloud computing environment**
Descrizione del Controllo	*Responsibilities for shared information security roles in the use of the cloud service should be allocated to identified parties, documented, communicated and implemented by both the cloud service customer and the cloud service provider.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Ritenuto necessario per rendere efficace il controllo 5.1.1.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	CISO
Documentazione	• ERIT-SGI - Politica di sicurezza delle informazioni e la protezione dei dati personali (CSP, CSC) • ERIT-SGI - Comunicazione (CSP, CSC) • Contratto Microsoft (CSC) • Contratto Mulesoft (CSC)
Note	
Controllo	**CLD 8.1.5 Removal of cloud service customer assets**
Descrizione del Controllo	*Assets of the cloud service customer that are on the cloud service provider's premises should be removed, and returned, if necessary, in a timely manner upon termination of the cloud service agreement.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Richiesto dalla valutazione del rischio

Pubblico
Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	CISO
Documentazione	• ERIT-SGI-IT Charter (CSC) • ERIT- Misure di sicurezza Welfare e Ticket Restaurant (CSP) • Contratto Microsoft (CSC) • Contratto Mulesoft (CSC) • Contratti Welfare (CSP)
Note	
Controllo	**CLD 9.5.1 Segregation in virtual computing environments**
Descrizione del Controllo	*A cloud service customer's virtual environment running on a cloud service should be protected from other cloud service customers and unauthorized persons.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Necessaria al corretto svolgimento delle attività.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	Head of Infrastructure & Operations
Documentazione	• ERIT-SGI - Network Security (CSP) • ERIT-SGI - Policy sviluppo sicuro (CSP)
Note	
Controllo	**CLD 9.5.2 Virtual machine hardening**
Descrizione del Controllo	*Virtual machines in a cloud computing environment should be hardened to meet business needs.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Necessaria al corretto svolgimento delle attività.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	Head of Infrastructure & Operations
Documentazione	• SEC-POL-019-Infrastructure Security Policy_202602(CSP, CSC)

Pubblico
Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

	• SEC-GUI-041- Firewall Security Guidelines_2026 version (CSP, CSC)
Note	
Controllo	**CLD 12.1.5 Administrator's operational security**
Descrizione del Controllo	*Procedures for administrative operations of a cloud computing environment should be defined, documented, and monitored.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Necessaria al corretto svolgimento delle attività.
Livello di Implementazione	Implementato
Ownership	Edenred Italia, Edenred SE
Referente	Head of Core & Digital Solutions, Head of Infrastructure & Operations
Documentazione	• ERIT-SGI - Change & Release Management Process (CSP, CSC) • ERIT-SGI - Change Request (CSP, CSC) • SEC-POL-018- IT Resilience & Backup Policy (CSP, CSC) • ERIT-SGI - Risk Management Information Security e Data Protection (CSP, CSC)
Note	
Controllo	**CLD 12.4.5 Monitoring of Cloud Services**
Descrizione del Controllo	*The cloud service customer should have the capability to monitor specified aspects of the operation of the cloud services that the cloud service customer uses.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Necessaria al corretto svolgimento delle attività.
Livello di Implementazione	Implementato
Ownership	Edenred Italia, Edenred SE
Referente	CISO, Head of Infrastructure & Operations, SOC
Documentazione	• Data Processing Agreement (CSP) • ERIT-SGI - CapacityManagement (CSP) • ERIT-SGI - Gestione dei Log (CSP) • Contratto Microsoft (CSP, CSC) • Contratto Mulesoft (CSP, CSC) • ERIT- Misure di sicurezza Welfare e Ticket Restaurant (CSP) • Contratti Welfare (CSP)

Pubblico

Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

	• SEC-POL-025-Server and Cloud Security Policy_2026 version PCI-DSS (CSC)
Note	
Controllo	**CLD 13.1.4 Alignment of security management for virtual and physical networks**
Descrizione del Controllo	*Upon configuration of virtual networks, consistency of configurations between virtual and physical networks should be verified based on the cloud service provider's network security policy.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Necessaria al corretto svolgimento delle attività.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	Head of Infrastructure & Operations
Documentazione	• ERIT-SGI - Network Security (CSP)
Note	

2.4. Controlli ISO 27018:2019

Rif. ISO/IEC 27018	**PII.A.2 Consent and Choice**
Controllo	**A.2.1 Obligation to cooperate regarding PII principal's rights**
Descrizione del Controllo	*The public cloud PII processor should provide the cloud service customer with the means to enable them to fulfil their obligation to facilitate the exercise of PII principals' rights to access, correct and/or erase PII pertaining to them.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Ritenuto necessario per rendere efficace il SGI.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	Privacy Manager, DPO
Documentazione	• Informative privacy • ERIT-SGI - Procedura di Gestione dei Consensi

Pubblico

Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

	• ERIT-SGI - Politica Gestione Diritti interessati • Data Processing Agreement
Note	
Rif. ISO/IEC 27018	**PII.A.3 Purpose legitimacy and specification**
Controllo	**A.3.1 Public cloud PII processor's purpose**
Descrizione del Controllo	*PII to be processed under a contract should not be processed for any purpose independent of the instructions of the cloud service customer.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Ritenuto necessario per rendere efficace il SGI.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	Privacy Manager, DPO
Documentazione	• Data Processing Agreement • Informative privacy • ERIT-SGI - Linee Guida sulla Protezione dei Dati Personali
Note	
Rif. ISO/IEC 27018	**PII.A.3 Purpose legitimacy and specification**
Controllo	**A.3.2 Public cloud PII processor's commercial use**
Descrizione del Controllo	*PII to be processed under a contract should not be processed for any purpose independent of the instructions of the cloud service customer.*
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Ritenuto necessario per rendere efficace il SGI.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	Privacy Manager, DPO
Documentazione	• Registro responsabili • Data Processing Agreement • ERIT-SGI - Linee Guida sulla Protezione dei Dati Personali
Note	

Pubblico
Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

Rif. ISO/IEC 27018	PII.A.5 Data Minimization
Controllo	**A.5.1 Secure erasure of temporary files**
Descrizione del Controllo	Temporary files and documents should be erased or destroyed within a specified, documented period.
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Ritenuto necessario per rendere efficace il SGI.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	Privacy Manager, DPO
Documentazione	• ERIT-SGI - Procedura Security e Privacy by Design • ERIT-SGI - Linee Guida sulla Protezione dei Dati Personali
Note	
Rif. ISO/IEC 27018	**PII.A.6 Use, Retention and Disclosure Limitation**
Controllo	**PII.A.6.1 PII disclosure notification**
Descrizione del Controllo	The contract between the public cloud PII processor and the cloud service customer should require the public cloud PII processor to notify the cloud service customer, in accordance with any procedure and time periods agreed in the contract, of any legally binding request for disclosure of PII by a law enforcement authority, unless such a disclosure is otherwise prohibited.
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Ritenuto necessario per rendere efficace il SGI.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	Privacy Manager, DPO
Documentazione	• Data Processing Agreement • ERIT-SGI - Linee Guida sulla Protezione dei Dati Personali
Note	
Rif. ISO/IEC 27018	**PII.A.6 Use, Retention and Disclosure Limitation**
Controllo	**PII.A.6.2 Recording of PII disclosures**
Descrizione del Controllo	Disclosures of PII to third parties should be recorded, including what PII has been disclosed, to whom and at what time.

Pubblico

Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

Incluso	Sì
Motivazione per l'inclusione / Esclusione	Ritenuto necessario per rendere efficace il SGI.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	Privacy Manager, DPO
Documentazione	• Data Processing Agreement • Informative privacy • ERIT-SGI - Linee Guida sulla Protezione dei Dati Personali
Note	
Rif. ISO/IEC 27018	**PII.A.8 Openness, Transparency and Notice**
Controllo	**PII.A.8.1 Disclosure of sub-contracted PII processing**
Descrizione del Controllo	The use of sub-contractors by the public cloud PII processor to process PII should be disclosed to the relevant cloud service customers before their use.
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Ritenuto necessario per rendere efficace il SGI.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	Privacy Manager, DPO
Documentazione	• Data Processing Agreement • ERIT-SGI - Linee Guida sulla Protezione dei Dati Personali • ERIT-SGI - Gestione sicura dei Fornitori
Note	
Rif. ISO/IEC 27018	**PII.A.10 Accountability**
Controllo	**PII.A.10.1 Notification of a data breach involving PII**
Descrizione del Controllo	The public cloud PII processor should promptly notify the relevant cloud service customer in the event of any unauthorized access to PII or unauthorized access to processing equipment or facilities resulting in loss, disclosure or alteration of PII.
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Ritenuto necessario per rendere efficace il SGI.

Pubblico

Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	Privacy Manager, DPO
Documentazione	• Data Processing Agreement • ERIT-SGI - Linee Guida sulla Protezione dei Dati Personali • ERIT-SGI-Gestione Data Breach
Note	
Rif. ISO/IEC 27018	**PII.A.10 Accountability**
Controllo	**PII.A.10.2 Retention period for administrative security policies and guidelines**
Descrizione del Controllo	Copies of security policies and operating procedures should be retained for a specified, documented period upon replacement (including updating).
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Ritenuto necessario per rendere efficace il SGI.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	Privacy Manager, DPO
Documentazione	• Informative privacy (storico) • ERIT-SGI - Linee Guida sulla Protezione dei Dati Personali
Note	
Rif. ISO/IEC 27018	**PII.A.10 Accountability**
Controllo	**PII.A.10.3 PII return, transfer and disposal**
Descrizione del Controllo	The public cloud PII processor should have a policy in respect of the return, transfer and/or disposal of PII and should make this policy available to the cloud service customer.
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Ritenuto necessario per rendere efficace il SGI.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	Privacy Manager, DPO

Pubblico

Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

Documentazione	• ERIT-SGI - Linee Guida sulla Protezione dei Dati Personali • Data Processing Agreement
Note	
Rif. ISO/IEC 27018	**PII.A.11 Information Security**
Controllo	**PII.A.11.1 Confidentiality or non-disclosure agreements**
Descrizione del Controllo	Individuals under the public cloud PII processor's control with access to PII should be subject to a confidentiality obligation.
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Ritenuto necessario per rendere efficace il SGI.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	Privacy Manager, DPO
Documentazione	• ERIT-SGI - Linee Guida sulla Protezione dei Dati Personali • Data Processing Agreement
Note	
Rif. ISO/IEC 27018	**PII.A.11 Information Security**
Controllo	**PII.A.11.2 Restriction of the creation of hardcopy material**
Descrizione del Controllo	The creation of hardcopy material displaying PII should be restricted.
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Ritenuto necessario per rendere efficace il SGI.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	Privacy Manager, DPO
Documentazione	• ERIT-SGI - Linee Guida sulla Protezione dei Dati Personali • ERIT-SGI-IT Charter
Note	
Rif. ISO/IEC 27018	**PII.A.11 Information Security**
Controllo	**PII.A.11.3 Control and logging of data restoration**

Pubblico
Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

Descrizione del Controllo	There should be a procedure for, and a log of, data restoration efforts.
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Ritenuto necessario per rendere efficace il SGI.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	Privacy Manager, DPO
Documentazione	• ERIT-SGI - Linee Guida sulla Protezione dei Dati Personali • ERIT-SGI - Gestione dei Log
Note	
Rif. ISO/IEC 27018	**PII.A.11 Information Security**
Controllo	**PII.A.11.4 Protecting data on storage media leaving the premises**
Descrizione del Controllo	PII on media leaving the organization's premises should be subject to an authorization procedure and should not be accessible to anyone other than authorized personnel (e.g. by encrypting the data concerned).
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Ritenuto necessario per rendere efficace il SGI.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	Privacy Manager, DPO
Documentazione	• ERIT-SGI - Linee Guida sulla Protezione dei Dati Personali • ERIT-SGI - Gestione Utenti (CSP, CSC) • ERIT-SGI - Gestione Accessi Logici (CSP) • ERIT-SGI - Controllo Accessi Applicativi
Note	
Rif. ISO/IEC 27018	**PII.A.11 Information Security**
Controllo	**PII.A.11.5 Use of unencrypted portable storage media and devices**
Descrizione del Controllo	Portable physical media and portable devices that do not permit encryption should not be used except where it is unavoidable, and any use of such portable media and devices should be documented.
Incluso	Sì

Pubblico

Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

Motivazione per l'inclusione / Esclusione	Ritenuto necessario per rendere efficace il SGI.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	Privacy Manager, DPO
Documentazione	• ERIT-SGI - Linee Guida sulla Protezione dei Dati Personali • ERIT-SGI - Politica di crittografia (CSP, CSC) • SEC-GUI-039-Cryptography & Secure Protocols Guidelines_2026 version (CSC)
Note	
Rif. ISO/IEC 27018	**PII.A.11 Information Security**
Controllo	**PII.A.11.6 Encryption of PII transmitted over public data-transmission networks**
Descrizione del Controllo	PII that is transmitted over public data-transmission networks should be encrypted prior to transmission.
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Ritenuto necessario per rendere efficace il SGI.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	Privacy Manager, DPO
Documentazione	• ERIT-SGI - Linee Guida sulla Protezione dei Dati Personali • ERIT-SGI - Politica di crittografia (CSP, CSC) • Contratto Microsoft (CSC) • SEC-GUI-039-Cryptography & Secure Protocols Guidelines_2026 version (CSC) • ERIT-SGI - Network Security
Note	
Rif. ISO/IEC 27018	**PII.A.11 Information Security**
Controllo	**PII.A.11.7 Secure disposal of hardcopy materials**
Descrizione del Controllo	Where hardcopy materials are destroyed, they should be destroyed securely using mechanisms such as cross-cutting, shredding, incinerating, pulping, etc.
Incluso	Sì

Pubblico

Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

Motivazione per l'inclusione / Esclusione	Ritenuto necessario per rendere efficace il SGI.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	Privacy Manager, DPO
Documentazione	• ERIT-SGI - Politica Gestione Diritti interessati • ERIT-SGI - Linee Guida sulla Protezione dei Dati Personali
Note	
Rif. ISO/IEC 27018	**PII.A.11 Information Security**
Controllo	**PII.A.11.8 Unique use of user Ids**
Descrizione del Controllo	If more than one individual has access to stored PII, then they should each have a distinct user ID for identification, authentication and authorization purposes.
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Ritenuto necessario per rendere efficace il SGI.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	Privacy Manager, DPO
Documentazione	• ERIT-SGI - Gestione Utenti (CSP, CSC) • ERIT-SGI - Gestione Accessi Logici (CSP) • ERIT-SGI - Controllo Accessi Applicativi
Note	
Rif. ISO/IEC 27018	**PII.A.11 Information Security**
Controllo	**PII.A.11.9 Records of authorized users**
Descrizione del Controllo	An up-to-date record of the users or profiles of users who have authorized access to the information system should be maintained.
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Ritenuto necessario per rendere efficace il SGI.
Livello di Implementazione	Implementato
Ownership	Edenred Italia

Pubblico

Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

Referente	Privacy Manager, DPO
Documentazione	• ERIT-SGI - Gestione Utenti (CSP, CSC) • ERIT-SGI - Gestione Accessi Logici (CSP) • ERIT-SGI - Linee Guida sulla Protezione dei Dati Personali
Note	
Rif. ISO/IEC 27018	**PII.A.11 Information Security**
Controllo	**PII.A.11.10 User ID management**
Descrizione del Controllo	De-activated or expired user IDs should not be granted to other individuals.
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Ritenuto necessario per rendere efficace il SGI.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	Privacy Manager, DPO
Documentazione	• ERIT-SGI - Gestione Utenti (CSP, CSC) • ERIT-SGI - Gestione Accessi Logici (CSP) • ERIT-SGI - Linee Guida sulla Protezione dei Dati Personali
Note	
Rif. ISO/IEC 27018	**PII.A.11 Information Security**
Controllo	**PII.A.11.11 Contract measures**
Descrizione del Controllo	Contracts between the cloud service customer and the public cloud PII processor should specify minimum technical and organizational measures to ensure that the contracted security arrangements are in place and that data are not processed for any purpose independent of the instructions of the controller. Such measures should not be subject to unilateral reduction by the public cloud PII processor.
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Ritenuto necessario per rendere efficace il SGI.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	Privacy Manager, DPO
Documentazione	• Contratto Microsoft (CSC)

Pubblico

Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

	• Data Processing Agreement
Note	
Rif. ISO/IEC 27018	**PII.A.11 Information Security**
Controllo	**PII.A.11.12 Sub-contracted PII processing**
Descrizione del Controllo	Contracts between the public cloud PII processor and any sub-contractors that process PII should specify minimum technical and organizational measures that meet the information security and PII protection obligations of the public cloud PII processor. Such measures should not be subject to unilateral reduction by the sub-contractor.
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Ritenuto necessario per rendere efficace il SGI.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	Privacy Manager, DPO
Documentazione	• Data Processing Agreement
Note	
Rif. ISO/IEC 27018	**PII.A.11 Information Security**
Controllo	**PII.A.11.13 Access to data on pre-used data storage space**
Descrizione del Controllo	The public cloud PII processor should ensure that whenever data storage space is assigned to a cloud service customer, any data previously residing on that storage space is not visible to that cloud service customer.
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Ritenuto necessario per rendere efficace il SGI.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	Privacy Manager, DPO
Documentazione	• Data Processing Agreement • Contratto Microsoft (CSC)
Note	
Rif. ISO/IEC 27018	**PII.A.12 Privacy Compliance**
Controllo	**PII.A.12.1 Geographical location of PII**

Pubblico

Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

Descrizione del Controllo	The public cloud PII processor should specify and document the countries in which PII might possibly be stored.
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Ritenuto necessario per rendere efficace il SGI.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	Privacy Manager, DPO
Documentazione	• ERIT-SGI - Edenred Italia Descrizione Piattaforma
Note	
Rif. ISO/IEC 27018	**PII.A.12 Privacy Compliance**
Controllo	**PII.A.12.2 Intended destination of PII**
Descrizione del Controllo	PII transmitted using a data-transmission network should be subject to appropriate controls designed to ensure that data reaches its intended destination.
Incluso	Sì
Motivazione per l'inclusione / Esclusione	Ritenuto necessario per rendere efficace il SGI.
Livello di Implementazione	Implementato
Ownership	Edenred Italia
Referente	Privacy Manager, DPO
Documentazione	• ERIT-SGI - Network Security (CSP) • SEC-POL-019-Infrastructure Security Policy_202602(CSC) • Contratto Microsoft (CSC)
Note	

Pubblico

Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.