

Politica Sistema di Gestione per la Sicurezza delle Informazioni

Sommario

1	Proprietà del documento	3
1.1	Revisioni.....	3
1.2	Distribuzione.....	3
1.3	Allegati.....	3
2	Introduzione	4
3	Obiettivi e strategie	4
4	Opportunità	5
5	Normativa cogente - Dichiarazione di conformità	5
6	Le caratteristiche del sistema di gestione della sicurezza delle informazioni.....	6

1 Proprietà del documento

1.1 Revisioni

Edizione	Revisione	Data	Modifiche
01	00	27/03/2019	Prima redazione.

1.2 Distribuzione

Funzioni interne autorizzate	<ul style="list-style-type: none">• Direzione;• Comitato per la Sicurezza delle Informazioni.
Parti esterne, senza limitazioni	<ul style="list-style-type: none">• Autorità competenti.
Parti esterne, previa sottoscrizione di NDA	<ul style="list-style-type: none">• Clienti;• Fornitori.
Canali autorizzati	<ul style="list-style-type: none">• Intranet aziendale;• Posta elettronica
Formati autorizzati	<ul style="list-style-type: none">• Elettronico inalterabile (es. PDF)

1.3 Allegati

Costituiscono allegati al presente documento quelli riportati nella tabella a seguire.

Titolo	Breve descrizione

2 Introduzione

E-Fil considera la sicurezza delle informazioni un aspetto primario per la protezione del proprio business e dei propri clienti, in linea con la nostra consolidata politica della qualità.



L'evoluzione dell'organizzazione e dei suoi prodotti/servizi presenti sul mercato, la stabile collocazione fra i fornitori di servizi in modalità "software as a service" (SaaS) e le grandi quantità di dati forniti da Pubbliche Amministrazioni e aziende private gestiti in cloud, hanno reso indispensabile l'adozione di modelli di sicurezza mirati a proteggere e stabilizzare i processi e le informazioni e la protezione dei dati personali relativa agli utenti dei servizi.

3 Obiettivi e strategie

L'Alta direzione pone il proprio massimo impegno per garantire la sicurezza delle informazioni e dei dati personali trattati nell'ambito dei servizi erogati in accordo con la normativa applicabile ed in particolare secondo i requisiti dettati dalla norma UNI CEI EN ISO/IEC 27001, scelta quale standard di riferimento anche per la corretta connotazione e reputazione dell'organizzazione nei confronti delle Parti interessate.

Per il conseguimento del suddetto obiettivo strategico in tema di sicurezza delle informazioni E-fil si propone di :

- Assicurare una protezione delle informazioni e dei dati personali adeguata in termini di **integrità, disponibilità e riservatezza** attuando un modello strutturato di protezione dell'informazione, orientata ad una efficace **analisi e gestione dei rischi correlati**;
- Coinvolgere allo scopo l'intera organizzazione aziendale ed il personale impegnato nei processi fornendo risorse adeguate al perseguimento del programma di sicurezza.
- Assegnare al proprio interno ruoli e responsabilità ben definiti.
- Provvedere ad un'adeguata formazione al fine di garantire un elevato livello di competenza e consapevolezza delle responsabilità delle proprie risorse impegnate nei processi e trattamenti sulle informazioni ai vari livelli .
- Effettuare un efficace e costante monitoraggio dei processi affidati a partner e fornitori strategici, largamente utilizzati nei servizi erogati da E-Fil, che incidono profondamente nella catena di preservazione della sicurezza e della continuità operativa
- In ogni caso tutelare la sicurezza del personale nella gestione dei casi di emergenza e proteggere l'interesse dei clienti, dei dipendenti e delle terze parti;
- Assicurare la conformità alle leggi e ai regolamenti applicabili in materia di trattamento dei dati personali e di sicurezza dell'informazione;
- Rispondere in modo efficace alle crescenti minacce ai sistemi informativi nello spazio cibernetico;
- Utilizzare in modalità preferenziale le moderne tecnologie di erogazione in Cloud. Adottando l'infrastruttura Azure di Microsoft come infrastruttura centrale per garantire elevati livelli di servizio, scalabilità e sicurezza delle informazioni. L'infrastruttura è stata selezionata anche per gli specifici strumenti gestionali e di monitoraggio nell'ambito della sicurezza delle informazioni. Perseguire politiche formative specifiche per il personale di sviluppo e di

 <p>SOLUZIONI DIGITALI PER IL CICLO DEGLI INCASSI</p> <p>SISTEMA DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI</p>	<p align="center">Politica</p> <p align="center">Per la sicurezza delle informazioni</p> <p align="center">NORMA ISO/IEC 27001</p>	<p>SI-001</p> <p>Ed. 01 Rev.01 del 31/05/2019</p>  <p align="right">Pagina 5 di 6</p>
---	---	--

erogazione.

Sul piano del controllo e della certificazione da parte di soggetti esterni E-Fil si propone :

- Di applicare e certificare un sistema di gestione per la sicurezza delle informazioni conforme ai requisiti della norma UNI CEI EN ISO/IEC 27001, integrando i controlli previsti dalla stessa norma con le linee guida definite:
 - ISO/IEC 27017 – Prassi per i controlli di sicurezza delle informazioni per i servizi in Cloud
 - ISO/IEC 27018 – Prassi per la protezione dei dati personali trattati nei servizi Cloud pubblici
- Di ottemperare ai requisiti richiesti dall’Agenzia per l’Italia Digitale (AgID) per la qualificazione come fornitori CSP e di servizi SaaS per il Cloud della PA, secondo le circolari AgID n. 2 e 3 del 9/04/2018, e per l’inserimento dei servizi SaaS di E-Fil nel Marketplace Cloud previsto nelle circolari stesse.

4 Opportunità

L’adozione del sistema di sicurezza delle informazioni deve puntare a conseguire vantaggi di varia natura ed in particolare:

- Massimizzare gli effetti positivi degli investimenti che l’azienda destina al capitolo della sicurezza delle informazioni e dei dati personali.
- Permettere con il coordinamento dei processi di migliorare l’efficacia nella protezione dei dati personali a tutela della privacy;
- Contribuire a prevenire e mitigare danni di natura economica, legale e/o reputazionale derivanti da incidenti della sicurezza delle informazioni e dati personali.

5 Normativa cogente - Dichiarazione di conformità

E-fil, nell’ambito degli obiettivi di cui al par. 2, si impegna a garantire la conformità alle seguenti norme :

- ISO/IEC 27001 - Sistema di Gestione per la Sicurezza delle Informazioni
- ISO/IEC 27017 - Controlli di sicurezza per servizi cloud
- ISO/IEC 27018 - Cloud e Privacy
- Legge 18 marzo 2008, n. 48 - Ratifica alla Convenzione di Budapest
- Regolamento (UE) 16/679 (GDPR)
- D.lgs. 30 giugno 2003, n. 196 - Codice in materia di protezione dei dati personali (Precedente normativa sulla privacy)
- D.lgs. 101/2018 - Adeguamento della normativa italiana al GDPR (Regolamento UE 2016/679)
- Circolare AgID n. 2 del 9 aprile 2018 - Criteri per la qualificazione dei Cloud Service Provider per la PA

- Circolare AgID n. 3 del 9 aprile 2018 - Criteri per la qualificazione di servizi SaaS per il Cloud della PA

Sono escluse dal campo di applicazione :

- Direttiva UE 2016/1148) “ misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione” – NIS) in quanto le disposizioni non si applicano alle piccole imprese, classifica cui appartiene E-Fil per numero di addetti e fatturato.

6 Le caratteristiche del sistema di gestione della sicurezza delle informazioni

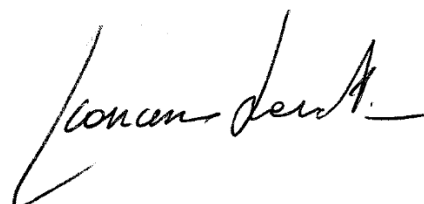
Il sistema di gestione E-Fil mette in stretta relazione le competenze tecniche e le funzioni decisionali, con lo scopo di conseguire efficacia e rapidità nelle decisioni, mediante il “Comitato SGSI” deputato ad affrontare e risolvere le problematiche di carattere operativo che possono insorgere sia nelle attività di definizione e miglioramento del Sistema di Gestione per la Sicurezza delle Informazioni, sia nell’attuazione dello stesso.

L’efficacia del programma di sicurezza delle informazioni si basa sui seguenti punti:

1. Applicare pratiche sistematiche di analisi e valutazione dei rischi;
2. Svolgere attività di intelligence sulle minacce, consentendo una gestione del rischio adeguata allo stesso;
3. Selezionare, progettare e implementare misure di mitigazione dei rischi di sicurezza;
4. Garantire e verificare l’efficacia dei controlli di sicurezza;
5. Riesaminare l’adeguatezza dei controlli e l’efficacia del sistema di protezione dell’informazione per assicurare il suo continuo mantenimento e miglioramento alla luce dell’evolversi della minaccia, del business, del contesto tecnologico e normativo.

Il sistema di gestione della sicurezza delle informazioni si basa sulla documentazione di base che approfondisce e sviluppa i punti di cui sopra, definendo criteri e modalità operative.

Legale Rappresentante
(ing. Francesco Laratta)



FINE DOCUMENTO