



Documento per la progressiva implementazione del Sistema di gestione della sicurezza delle informazioni (SGSI)

22/12/2017

Approvato con Determinazione del Presidente n. 17 del
22/12/2017

1. Premessa

Il corretto esercizio delle attività istituzionali inerenti la riscossione nazionale e l'amministrazione dei processi corporate da parte dell'Agenzia delle entrate-Riscossione (di seguito, anche solo "AeR" o "Ente") è strettamente correlato alla disponibilità, all'integrità e alla riservatezza dei dati contenuti nel proprio sistema informativo.

A tal fine, come evidenziato nel Piano Triennale per l'Informatica nella Pubblica Amministrazione 2017-2019 (di seguito, anche solo "*Piano Triennale ICT 2017-2019*") emanato dall'Agenzia per l'Italia Digitale (di seguito, anche solo "AgID"), la sicurezza informatica riveste un'importanza fondamentale, anche in quanto *"direttamente collegata ai principi di privacy previsti dall'ordinamento giuridico"* (cfr. paragrafo 8 del Piano: "Sicurezza").

Il Piano Triennale ICT 2017-2019, nel definire le attività che le singole amministrazioni hanno realizzato e dovranno realizzare per strutturare, attuare e implementare i propri piani di sicurezza informatica, delinea un processo graduale (essendo la sicurezza informatica *"un'area tecnologica in continua evoluzione, quasi giornaliera"*), così caratterizzato:

1. *"scenario attuale"* (paragrafo 8.1);
2. *"obiettivi strategici"*; (paragrafo 8.2)
3. *"linee di azione"* (paragrafo 8.3).

In particolare, tra le *"linee di azione"* che dovranno essere attuate per il perseguimento degli obiettivi strategici fissati nel Piano Triennale ICT 2017-2019, è previsto che:

"un altro passaggio importante sarà l'emanazione delle Regole Tecniche per la sicurezza ICT delle Pubbliche amministrazioni che forniranno indicazioni sulle misure da adottare in ciascuna componente della Mappa del Modello strategico. Tra queste si anticipano alcune indicazioni relative alle Infrastrutture fisiche:

- *ciascuna Pubblica amministrazione dovrà dotarsi di un Sistema di gestione della sicurezza delle informazioni (SGSI) e della relativa struttura organizzativa;*
- *ciascuna Pubblica amministrazione dovrà, sulla base di una specifica analisi del rischio, individuare il profilo di sicurezza adeguato per la propria infrastruttura e, tenendo anche conto degli aggiornamenti sulle minacce provenienti dal CERT-PA, adottare le misure opportune".*

Ciò premesso, AeR si impegna a promuovere la sicurezza dei dati e delle informazioni gestite, in termini di integrità, disponibilità e riservatezza, attraverso la progressiva implementazione di un Sistema di Gestione della Sicurezza delle Informazioni (SGSI).

Il presente documento ha la finalità di strutturare un processo di gestione del rischio volto a garantire:

- I. la sicurezza delle informazioni;
- II. la sicurezza informatica;
- III. la protezione dei dati personali, mediante specifiche attività di analisi e valutazioni dei rischi condotte congiuntamente con il Data Protection Officer (DPO).

Il SGSI sarà strutturato secondo lo standard UNI CEI ISO/IEC 27001:2014 che prevede l'introduzione di un processo ciclico volto al miglioramento della protezione dei dati e delle informazioni. Il SGSI dovrà essere coerente con gli altri sistemi di gestione già presenti in AeR.

2. Ambito e certificazione ISO 27001

Agenzia delle entrate-Riscossione intende intraprendere un percorso finalizzato all'adozione del Sistema SGSI per tutte le informazioni e i dati gestiti, sia nell'ambito delle attività di riscossione che nell'ambito dei processi amministrativi/corporate.

L'adozione del Sistema SGSI seguirà un approccio di tipo modulare, venendo via via implementato, a partire dalle informazioni e dai dati trattati nell'ambito dei Data Center allocati presso le sedi di Roma e di Torino, fino ad estendersi progressivamente a tutti i dati e le informazioni dell'Ente.

Primo passo di tale percorso d'implementazione sarà costituito dalla redazione di un'accurata analisi per la valutazione del rischio.

Nell'ambito del perimetro iniziale, il documento per la progressiva implementazione del SGSI prevede il completamento di un primo ciclo di attività entro il 2018.

Agenzia delle entrate-Riscossione ha, inoltre, l'obiettivo di conseguire la certificazione UNI CEI/ISO 27001:2014 del proprio SGSI. Secondo il descritto approccio modulare, Agenzia delle entrate-Riscossione ha l'obiettivo di conseguire, già entro il 2019, la certificazione SGSI limitatamente alle informazioni e ai dati trattati nell'ambito dei Data Center allocati presso le sedi di Roma e di Torino.

3. Sicurezza dei dati e delle informazioni

Il presupposto fondante del processo di gestione della sicurezza delle informazioni consiste nella rilevazione delle esigenze e delle aspettative di sicurezza dei dati e delle informazioni gestite da AeR.

L'analisi del rischio consentirà di acquisire la consapevolezza e la visibilità del livello di esposizione al rischio delle informazioni trattate. La valutazione del rischio sarà condotta sulla base:

- del danno che potrà derivare ad AeR dalla perdita di riservatezza, integrità, disponibilità delle informazioni;
- della realistica probabilità che una minaccia si concretizzi in un attacco sfruttando le vulnerabilità presenti.

Sotto il profilo privacy, assume, inoltre, grande rilevanza il Regolamento UE 2016/679 per la protezione dei dati personali (GDPR), pubblicato nella Gazzetta Ufficiale dell'Unione Europea il 4 maggio 2016 ed entrato in vigore il ventesimo giorno successivo alla pubblicazione. Il Regolamento troverà, tuttavia, applicazione a far data dal 25 maggio 2018 (cfr. art. 99 del Regolamento), data entro la quale dovranno essere adottate tutte le misure tecnico-organizzative richieste.

Il Regolamento pone con forza l'accento sulla "Responsabilizzazione" (accountability (cfr. art. 5, paragrafo 2 e considerando n. 74 del Regolamento) di Titolari e Responsabili, ossia sull'adozione di comportamenti proattivi e tali da dimostrare la concreta attuazione di misure finalizzate ad assicurare l'applicazione del medesimo Regolamento.

Principi cardine sono quelli della privacy by design e della privacy by default. La cd. Privacy by design si riferisce alla necessità, per il Titolare del trattamento, di mettere in atto, sia al momento di determinare i mezzi del trattamento (ovvero a monte, prima di procedere al trattamento dei dati vero e proprio) sia all'atto del trattamento stesso, misure tecniche e organizzative adeguate. La cd. Privacy by default fa riferimento al mettere in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita (di default), solo i dati personali necessari per ogni specifica finalità di trattamento.

L'art. 37 del Regolamento, prevede l'individuazione del Data Protection Officer (DPO), figura fulcro del processo di attuazione del principio di "responsabilizzazione" (cd. accountability). Il DPO dovrà essere sempre coinvolto in tutte le questioni relative alla protezione dei dati personali, ivi incluse quelle inerenti il documento programmatico in oggetto e la successiva adozione del Sistema di Gestione della Sicurezza delle Informazioni (SGSI).

Sulla base di quanto sopra, saranno individuate le minacce che possono incidere sulla gestione dei dati e delle informazioni, nonché le eventuali ulteriori misure di sicurezza da implementare per mitigare i relativi rischi.

- informare il Vertice sulle principali evidenze in materia di gestione dei rischi inerenti alla sicurezza delle informazioni.

Tale ruolo sarà attribuito al **Responsabile dell'Area Innovazione e Servizi Operativi**.

4.2 Gestore SGSI

Il Gestore del SGSI avrà il compito di:

- garantire l'applicazione del SGSI e il suo riesame periodico;
- aggiornare il Responsabile del SGSI sui risultati degli Internal Security Audit, sull'andamento generale del SGSI e sulla pianificazione degli interventi previsti;
- gestire il sistema documentale del SGSI;
- tenere sotto controllo gli obiettivi e i piani del SGSI;
- proporre le azioni da intraprendere per il miglioramento della sicurezza delle informazioni e promuovere iniziative di sicurezza delle informazioni;
- supportare il dialogo tra le strutture che realizzano la gestione operativa del SGSI nella valutazione dei rischi e dei livelli di adeguatezza dei controlli di sicurezza previsti, in relazione alle modalità di trattamento dei dati e delle informazioni (c.d. componente);
- definire i requisiti del sistema di indicatori per il monitoraggio del SGSI, nonché raccogliere le informazioni utili al monitoraggio;
- riesaminare periodicamente i risultati del SGSI e analizzare la reportistica sugli incidenti di sicurezza, sugli indicatori di prestazione e sulle verifiche ispettive interne;
- sviluppare la cultura della sicurezza attraverso la promozione di formazione specifica per il personale.

Tale ruolo sarà attribuito all'**Ufficio SGSI Governance**.

4.3 Proprietario dei dati (Data Owner)

Il Proprietario dei dati o Data Owner avrà il compito di esprimere le necessità e le aspettative di sicurezza per le informazioni che gestisce tenendo in considerazione anche le normative vigenti, i contratti, le aspettative di terzi (contribuenti, Enti creditori, ecc.) e il contesto di riferimento.

Tale ruolo sarà attribuito, in relazione alle attività assegnate nel modello organizzativo di AeR, alle Strutture Centrali (Direzioni Centrali e Aree, per il tramite delle proprie articolazioni organizzative) owner dei processi ove sono trattati i dati e le informazioni, anche quali punti di riferimento per le attività svolte dalle Strutture Regionali.

4.4 Gestore del rischio (Risk Owner)

Il Gestore del rischio o Risk Owner avrà il compito di:

- raccogliere le aspettative di sicurezza del Proprietario dei dati in coerenza con le aspettative di contenimento del rischio;
- raccogliere le valutazioni sulle misure di sicurezza presenti o da prevedere da parte del Gestore del componente;
- analizzare le informazioni raccolte per concertare gli interventi sulle misure di sicurezza da realizzare anche tenendo conto dei criteri di accettazione dei rischi definiti dal responsabile del SGSI;
- monitorare e aggiornare le valutazioni di adeguatezza del trattamento dei rischi.

Tale ruolo sarà attribuito, in relazione alle attività assegnate nel modello organizzativo di AeR, alle Strutture di Demand and Delivery della Direzione Tecnologie e Innovazione.

4.5 Gestore del componente

Le tipologie di controllo da gestire al fine di mitigare i rischi di sicurezza dipendono dalle caratteristiche del trattamento effettuato (elaborazione, memorizzazione, comunicazione, ecc.) dei dati e delle informazioni. In particolare, le componenti che possono intervenire nel trattamento del dato e/o dell'informazione sono prevalentemente:

- A. Hardware (server, client, reti, ecc.)
- B. Software (applicazioni, sistemi operativi e sistemi di gestione)
- C. Logistica (locali fisici, impianti infrastrutturali, ecc.)
- D. Personale (competenze)

Ciascuna componente del trattamento presenta tipologie specifiche di minacce e di azioni di protezione.

Il Gestore del componente avrà il compito, con riferimento alla componente di competenza, di:

- valutare il livello di esposizione alle minacce definendo il grado di efficacia delle misure in essere;
- attivare le ulteriori misure necessarie alla riduzione del rischio concordate con il Gestore del rischio;
- assicurare l'effettivo funzionamento delle misure di sicurezza previste.

Tale ruolo sarà attribuito alle strutture di AeR in relazione alle attività assegnate nel modello organizzativo. In particolare, saranno principalmente coinvolte:

- **Direzione Tecnologie e Innovazione – Settore Esercizio Sistemi ICT** (per le componenti A e B);
- **Direzione Approvvigionamenti e Logistica – Settore Logistica Infrastrutture e Security** (per la componente C);
- **Direzione Risorse Umane – Settore Gestione Risorse Umane** (per la componente D).

4.6 Verifiche per il corretto funzionamento del SGSI

Nell'ambito del modello SGSI sarà prevista una specifica fase di verifica (audit di primo livello) al fine di valutare se quanto pianificato ed implementato sia stato effettivamente realizzato, o se debbano essere intraprese ulteriori azioni correttive o di miglioramento per mitigare i rischi. In particolare, in questa fase il responsabile delle verifiche avrà il compito di:

- stabilire la data delle verifiche, in accordo con i responsabili da intervistare, secondo il Piano delle Verifiche;
- eseguire la verifica;
- controllare che siano state risolte le anomalie riscontrate durante le precedenti verifiche;
- esaminare l'efficacia delle azioni correttive implementate;
- definire l'attuazione di nuove misure correttive o delle azioni di miglioramento.

Tale ruolo sarà attribuito all'**Ufficio SGSI Governance**.

L'ufficio Audit ICT e Risk Management, nell'ambito delle competenze attribuite dal funzionigramma dell'Ente, garantirà le verifiche di secondo livello sul SGSI, anche ai fini della eventuale certificazione.

5. Sistema documentale

Il SGSI, in tutte le sue fasi e per tutti gli ambiti di applicazione, includerà la redazione di opportuna e specifica documentazione per regolamentare, in conformità allo standard ISO/27001, le seguenti attività:

- manuale SGSI;
- classificazione delle informazioni per la valutazione del rischio;
- valutazione ed il trattamento del rischio;
- conduzione degli audit interni;
- gestione delle non conformità e delle azioni correttive;
- gestione delle informazioni documentate;
- gestione delle metriche di valutazione e degli indicatori.

Il Responsabile del SGSI curerà l'emanazione dei documenti del SGSI, nel rispetto della normativa vigente e previa condivisione con le competenti strutture dell'Ente.