

# **SGSI – Valutazione e trattamento del rischio di sicurezza delle informazioni Agenzia delle entrate-Riscossione**

## Sommario

1.	PREMESSA.....	6
2.	PROCESSO DI GESTIONE DEL RISCHIO .....	6
3.	ANALISI DEL CONTESTO.....	9
	<b>3.1 Analisi del contesto esterno .....</b>	<b>9</b>
	<b>3.2 Analisi del contesto interno .....</b>	<b>9</b>
4.	VALUTAZIONE DEL RISCHIO.....	10
	<b>4.1 Valutazione di impatto in termini di RID delle informazioni.....</b>	<b>12</b>
	<b>4.2 Identificazione e valutazione delle vulnerabilità e minacce .....</b>	<b>13</b>
	<b>4.3 Determinazione del valore di Rischio intrinseco .....</b>	<b>14</b>
	<b>4.4 Identificazione e valutazione dei controlli.....</b>	<b>15</b>
	<b>4.5 Determinazione del valore di Rischio residuo.....</b>	<b>16</b>
	<b>4.6 Redazione del Rapporto di Assessment del Rischio residuo .....</b>	<b>18</b>
5.	TRATTAMENTO DEL RISCHIO RESIDUO .....	18
	<b>5.1 Selezione delle opzioni di trattamento del rischio.....</b>	<b>19</b>
	<b>5.2 Redazione del Piano di Trattamento del Rischio.....</b>	<b>22</b>
	<b>5.3 Verifica del PTR.....</b>	<b>23</b>
	<b>5.4 Approvazione del PTR .....</b>	<b>24</b>
	<b>5.5 Accettazione del Rischio residuo .....</b>	<b>24</b>
6.	COMUNICAZIONE DEL RISCHIO, MONITORAGGIO E REVIEW .....	24

## DEFINIZIONI

<b>Ente o AeR</b>	Agenzia delle Entrate-Riscossione.
<b>SGSI</b>	Sistema di Gestione della Sicurezza delle Informazioni.
<b>Destinatari</b>	Il personale di Agenzia delle Entrate-Riscossione, il Presidente e i membri del Comitato di Gestione, i collaboratori esterni e tutti i soggetti aventi rapporti contrattuali con Agenzia delle Entrate- Riscossione.
<b>Informazione</b>	Bene immateriale che deve essere protetto in quanto costituisce un valore per l'organizzazione. L'informazione è protetta quando sono garantiti i requisiti di Riservatezza, Integrità e Disponibilità (RID).
<b>Riservatezza</b>	Proprietà di una informazione che la rende non disponibile a individui, entità e processi non autorizzati.
<b>Integrità</b>	Proprietà di una informazione che la rende protetta in termini di accuratezza e completezza.
<b>Disponibilità</b>	Proprietà di una informazione che la rende disponibile a individui, entità e processi autorizzati.
<b>Perimetro</b>	Rappresenta l'ambito dell'analisi di sicurezza del SGSI. Ad un perimetro sono associate le informazioni e i componenti che le trattano e/o ne influenzano la sicurezza. Per ogni perimetro definito si individua il "Risk Owner" <sup>1</sup> .
<b>Componente</b>	Insieme di risorse che trattano l'informazione (la elaborano, la memorizzano o la comunicano) e/o ne influenzano il livello di sicurezza. Il componente deve proteggere adeguatamente le informazioni contrastando le principali minacce che possono sfruttare le vulnerabilità presenti nel componente stesso. Per ogni componente è individuato il Gestore del componente <sup>2</sup> .

<sup>1</sup> Il Risk Owner è uno dei ruoli previsti nell'organizzazione del SGSI. Uno dei compiti principali è occuparsi nello specifico della sicurezza relativa ai Servizi di propria competenza anche con l'ausilio dei gestori dei componenti. Per la descrizione di dettaglio si rimanda la Manuale SGSI [5].

<sup>2</sup> Il Gestore del componente è uno dei ruoli previsti nell'organizzazione del SGSI. Uno dei compiti principali è amministrare una risorsa che tratta le informazioni e/o ne influenza la sicurezza curando altresì i controlli di sicurezza. Per la descrizione di dettaglio si rimanda la Manuale SGSI [5].

<b>Vulnerabilità</b>	Rappresenta la debolezza di un componente, o di un controllo, che può essere sfruttata da una minaccia.
<b>Minaccia</b>	È la causa potenziale di un evento non desiderato, che può produrre un danno per il SGSI e per l'Ente. Le minacce possono essere originate da azioni/ eventi accidentali o deliberati, che sfruttano punti deboli del sistema (vulnerabilità).
<b>Controllo</b>	Si intendono le pratiche, le procedure o i meccanismi volti alla mitigazione degli effetti delle azioni di minaccia sul componente. I controlli sono orientati alla riduzione delle vulnerabilità o alla limitazione dell'impatto di un incidente. Per i controlli si utilizza la tassonomia prevista nell'allegato A dello standard UNI CEI ISO/IEC 27001:2014 [3].
<b>GdR</b>	Grado di Robustezza di un controllo. È la capacità dei controlli applicati ad un componente di contrastare l'effetto delle minacce. È dichiarato dal Gestore del componente.
<b>Rischio intrinseco e residuo</b>	<p>La norma ISO 31000:2009 "Risk management" definisce il rischio come "l'effetto dell'incertezza sugli obiettivi".</p> <p>In particolare, il rischio di sicurezza è dato dalla relazione tra la probabilità che una minaccia possa sfruttare le vulnerabilità di un componente per compromettere le informazioni (in termini di RID) e l'entità delle conseguenze dannose per l'organizzazione (impatto). La probabilità di accadimento dell'evento dannoso è funzione del livello di esposizione del componente alla minaccia e della presenza e robustezza dei controlli di sicurezza applicati.</p> <p>Si parla di livello di Rischio intrinseco (RI) se il valore del rischio è determinato al netto della considerazione di azioni mitigatrici (o controlli) volte all'abbattimento degli effetti delle minacce sui componenti, altrimenti, si parla di Rischio residuo (RR) per identificare ciò che rimane dopo aver attivato una risposta al rischio.</p>
<b>GAR</b>	Il Grado di Abbattimento è un valore percentuale che esprime quanto il Rischio intrinseco viene abbattuto per effetto delle azioni di controllo attuate nel perimetro di analisi esaminato.

## RIFERIMENTI NORMATIVI E DOCUMENTALI

- [1] AeR – Determinazione del Presidente n.17 del 22 dicembre 2017 “Documento per la progressiva implementazione del Sistema di gestione della sicurezza delle informazioni (SGSI)”.
- [2] ISO/IEC 27002:2017 “Tecnologie Informatiche – Tecniche di sicurezza - Codice di pratica per la gestione della sicurezza delle informazioni”.
- [3] UNI CEI ISO/IEC 27001:2014 “Tecnologia delle Informazioni – Tecniche di Sicurezza – Sistemi di gestione della sicurezza delle informazioni – Requisiti”.
- [4] ISO/IEC 27005:2011 “Information technology – Security techniques – Information security risk management”.
- [5] AeR - DIS\_SGSI\_Manuale SGSI.
- [6] ISO 31000:2009 "Risk management"
- [7] AeR - Manuale unico La Sicurezza
- [8] AeR - Disciplinare per l'utilizzo degli strumenti elettronici e l'accesso alle risorse e ai dati

## 1. PREMESSA

Scopo del presente documento è descrivere la metodologia adottata dall'Ente per la valutazione ed il trattamento del rischio nell'ambito del SGSI, intesa come insieme di attività coordinate volte alla valutazione e al monitoraggio dei rischi connessi alla gestione della sicurezza delle informazioni.

Come indicato nella Determinazione del Presidente n.17 del 22 dicembre 2017 "Documento per la progressiva implementazione del Sistema di gestione della sicurezza delle informazioni (SGSI)" [1], l'Ente intende intraprendere un percorso finalizzato all'adozione del 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 SGSI seguirà un approccio di tipo modulare a partire dall'analisi delle informazioni trattate nell'ambito dei Data Center allocati presso le sedi di Roma e di Torino, fino ad estendersi progressivamente a tutte le informazioni gestite dall'Ente.

Il primo passo di tale percorso d'implementazione è costituito proprio dalla redazione di un'accurata analisi per la valutazione e il trattamento del rischio.

Nel SGSI il rischio può essere definito come l'effetto delle incertezze sugli obiettivi di sicurezza del sistema implementato [6]. Una gestione strutturata e sistematica dei rischi permette di identificare, valutare, comunicare e controllare le incertezze, migliorando la capacità di raggiungere gli obiettivi di sicurezza stabiliti.

Le attività previste per la valutazione ed il trattamento dei rischi definiscono un approccio comune, sistematico e ripetibile in maniera che i rischi possano essere identificati, gestiti e comunicati in maniera chiara e non ambigua alle parti interessate, con particolare riferimento al vertice dell'Ente.

La metodologia proposta si basa su quanto indicato dalle norme UNI CEI ISO/IEC 27001:2014 [3] e ISO/IEC 27005:2011 [4] e a quanto espresso nel Manuale SGSI [5], in particolare in relazione alla organizzazione, ai ruoli e alle responsabilità previste.

## 2. PROCESSO DI GESTIONE DEL RISCHIO

In questo paragrafo è descritta la metodologia generale di gestione del rischio adottata per il SGSI. In una prima fase la metodologia è applicata all'ambito previsto nel documento di emanazione [1], ma la scalabilità del metodo permette di essere in linea con l'approccio implementativo di tipo modulare scelto per il SGSI per il quale seguiranno ulteriori fasi di progressivo ampliamento del perimetro.

In termini generali, l'analisi dei rischi è un elemento fondante del SGSI e, sin dalla fase di progettazione, deve prevedere l'implementazione di adeguati e proporzionati controlli di sicurezza per mitigare il rischio portandolo ad un livello accettabile. In tal senso, il presupposto del processo di gestione della sicurezza delle informazioni consiste nella rilevazione delle esigenze e delle aspettative di sicurezza dei dati da parte dei Data Owner<sup>3</sup>.

L'Ente intende adottare un Sistema di Gestione della Sicurezza delle Informazioni coerente con le prescrizioni dello standard UNI CEI ISO/IEC 27001:2014 [3] che garantisce il governo della sicurezza delle informazioni della organizzazione in relazione ai rischi. Infatti, lo standard prevede che il sistema sia, già nella fase di progettazione, pensato per garantire la selezione di controlli di sicurezza adeguati e proporzionati rispetto al Rischio residuo considerato accettabile. Lo standard, inoltre, consente di monitorare i processi stessi di sicurezza; in questo modo è possibile:

1. accrescere i livelli di protezione delle informazioni e del valore del business;
2. minimizzare i possibili danni derivanti da eventuali incidenti di sicurezza;
3. assicurare alle parti interessate il rispetto dei loro interessi e della loro privacy.

L'approccio adottato, basato sulla norma in materia [4], prevede che il processo di gestione del rischio sia realizzato mediante le seguenti fasi:

1. **Analisi del contesto:** in questa fase viene effettuata l'analisi del contesto esterno ed interno in cui opera l'Ente al fine di comprendere gli elementi di interesse per l'analisi del rischio per l'ambito individuato.
2. **Valutazione dei rischi:** in questa fase si deve individuare la metodologia per la identificazione dei rischi di sicurezza (ad esempio: evidenze e dati storici; metodi sistematici con somministrazione di indagini e questionari; tecniche induttive), analizzare i rischi al fine di determinare le conseguenze (impatti) e le relative probabilità, valutare le evidenze ottenute. Questa fase è basata su:
  - o l'impatto o danno che potrà derivare all'Ente dalla perdita di Riservatezza, Integrità, Disponibilità delle informazioni; tale gravità è espressa con il livello di criticità delle informazioni stimato, analizzando il relativo impatto;
  - o la probabilità che una minaccia si concretizzi in un attacco sfruttando le vulnerabilità presenti nei componenti che trattano le informazioni;
  - o la robustezza dei controlli applicati per la mitigazione degli effetti delle minacce sui componenti nel perimetro.

---

<sup>3</sup> Il Data Owner è uno dei ruoli previsti nell'organizzazione del SGSI. Uno dei compiti principali è la classificazione del dato in funzione del livello di impatto causato dalla perdita di Riservatezza, di Integrità o di Disponibilità. Per la descrizione di dettaglio si rimanda la Manuale SGSI [5].

All'esito della fase, è prodotto il documento denominato Rapporto di Risk Assessment (RAR) per il quale sono previste le attività di formalizzazione e definitiva approvazione da parte delle figure indicate nel Manuale SGSI [5].

3. **Trattamento dei rischi:** eseguito l'assessment del Rischio nel perimetro, la fase di trattamento prevede l'eventuale identificazione e progettazione delle azioni di mitigazione dei rischi. Questa fase non può non prescindere dalla verifica dell'applicazione dei controlli previsti dallo standard [3] la cui conformità garantisce, ai componenti del sistema, protezioni commisurate alla criticità delle informazioni trattate. All'esito della fase, è prodotto il documento denominato Piano di Trattamento del Rischio (PTR) per il quale la fase di Accettazione del rischio prevede le attività di formalizzazione e definitiva approvazione da parte delle figure indicate nel Manuale SGSI [5].

Inoltre, in osservanza del principio del miglioramento continuo, saranno svolte ciclicamente le fasi di **Comunicazione** e di **Monitoraggio e Review del rischio**.

Nello schema seguente sono rappresentate le relazioni tra le fasi descritte.

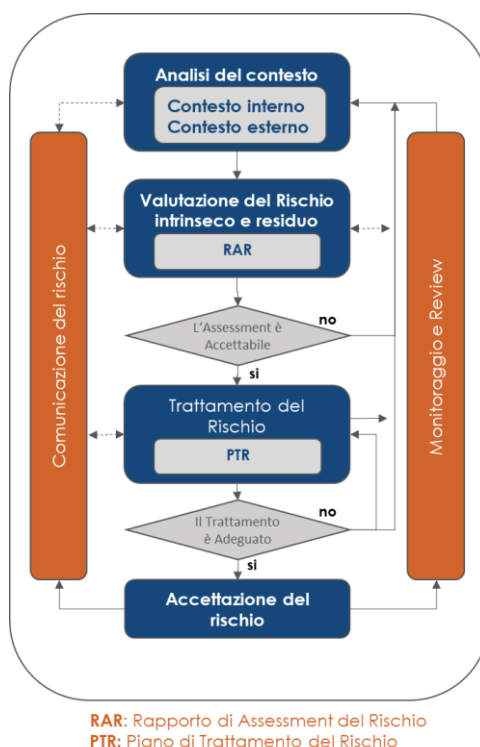


Figura 1: Schema di gestione del rischio.



### 3. ANALISI DEL CONTESTO

Prerequisito per l'attivazione delle fasi di valutazione e trattamento del rischio è aver definito il perimetro di intervento in termini di:

- eventuali scenari di rischio specifici;
- informazioni trattate dai componenti;
- componenti che partecipano all'erogazione ed alla messa in sicurezza dei servizi;
- confini, assunzioni e interfacce dell'ambito oggetto dell'analisi.

#### 3.1 Analisi del contesto esterno

L'analisi del contesto esterno in cui opera l'Ente – organizzato centralmente in Aree/Direzioni Centrali e sul territorio in Reti territoriali, Direzioni regionali e Aree territoriali – deve innanzitutto partire dalla peculiarità dell'attività esercitata, incentrata sulla riscossione di tributi, contributi e sanzioni. Su un piano generale, quindi, è evidente che l'attività di recupero di tributi e contributi non pagati espone al rischio che vengano poste in essere azioni da parte di attori esterni volte ad ottenere informazioni riservate di pertinenza dell'Ente a scopo fraudolento.

D'altra parte è importante evidenziare che l'Ente opera in un contesto normativo già orientato al mantenimento della sicurezza delle informazioni, sia a livello europeo che nazionale. Ad esempio, nello specifico ambito ICT, AeR opera di concerto con le indicazioni del CERT-PA (Computer Emergency Response Team - Pubblica Amministrazione) e del CERT-MEF (organismo dicasteriale avente lo scopo di potenziare la prevenzione degli incidenti di sicurezza informatica e migliorare le capacità di reazione alle minacce cibernetiche all'interno della PA). Queste strutture sono preposte, sia ad interventi di analisi e indirizzo in materia di incidenti di sicurezza informatica nel dominio costituito dalle pubbliche amministrazioni, sia alla condivisione di eventi occorsi o segnalati che richiedono da parte delle PA l'analisi e la valutazione delle azioni da porre in essere, per minimizzare il rischio di attacchi alla sicurezza delle informazioni.

#### 3.2 Analisi del contesto interno

L'analisi del contesto interno è basata sull'esame dell'organizzazione e gestione dell'Ente, con particolare riguardo a:

- governance e assetto organizzativo;
- sistemi, flussi informativi e cultura organizzativa;
- cultura dell'etica.

Per quanto riguarda la specifica Regolamentazione interna in materia di sicurezza, l'Ente ha già previsto l'emanazione di procedure mirate alla Sicurezza delle Informazioni come la regolamentazione dell'accesso ai locali fisici [7] e le norme di buona condotta relative alla gestione degli strumenti informatici [8].

Inoltre, nel documento "Modello di organizzazione, gestione e controllo" del Modello 231 adottato dall'Ente sono esplicitati i modelli, i regolamenti, i sistemi sui quali si basa il sistema di controllo interno (Codice Etico, Regolamento di Contabilità, Prevenzione della Corruzione e della Trasparenza per citarne alcuni) e che sono orientati a garantire il raggiungimento dei seguenti obiettivi:

- efficacia ed efficienza nell'impiego delle risorse, protezione dalle perdite e salvaguardia del patrimonio dell'Ente;
- rispetto delle leggi e dei regolamenti applicabili in tutte le operazioni ed azioni dell'Ente;
- affidabilità delle informazioni, da intendersi come comunicazioni tempestive ed affidabili a garanzia del corretto svolgimento di ogni processo decisionale.

L'applicazione nell'Ente del Modello 231 rappresenta per il SGSI un importante supporto all'analisi del contesto interno in relazione alla valutazione delle capacità, dei flussi di informazione, delle parti interessate interne, degli obiettivi e delle strategie messe in atto per raggiungerli, nonché delle norme e dei modelli di riferimento adottati dall'organizzazione.

## **4. VALUTAZIONE DEL RISCHIO**

La fase di Valutazione del rischio ha come obiettivo la misurazione del rischio di sicurezza (intrinseco e residuo) connesso alla possibile perdita dei requisiti RID delle informazioni nel perimetro, ossia nell'ambito di analisi. Secondo quanto previsto dalla norma [4] la fase prevede l'esecuzione di tre passi principali ossia l'identificazione, la misurazione e la ponderazione del rischio.

L'identificazione dei rischi considera il contesto interno ed esterno in cui opera l'Ente e prevede la consultazione e il confronto tra i vari soggetti rilevanti per l'analisi (ruoli del SGSI [5]), tenendo presenti le specificità di ciascun componente che tratta le specifiche informazioni.

La misurazione del rischio prevede come primo passo la determinazione del valore di Rischio intrinseco (RI) calcolato in funzione della probabilità che, nel perimetro di analisi, una o più minacce sfruttino le vulnerabilità dei componenti e dell'impatto rispetto alla

perdita dei requisiti RID delle informazioni, determinato dal concretizzarsi delle minacce. Ottenuto il valore RI, la misurazione del rischio prevede quindi, il calcolo del Rischio residuo (RR) determinato in funzione del Rischio intrinseco e dell'efficacia dell'attuazione dei controlli sui componenti nel contrasto alle minacce. Pertanto il Rischio intrinseco e residuo sono determinati come segue:

$$\text{Rischio intrinseco} = \text{Probabilità} * \text{Impatto}$$

$$\text{Rischio residuo} = \text{Rischio intrinseco} * \text{GAR}$$

dove per GAR si intende il Grado di Abbattimento del Rischio intrinseco derivato in funzione del Grado di Robustezza (GdR) dei controlli applicati espresso dai Gestori dei componenti.

La ponderazione del Rischio residuo ha lo scopo di stabilire le priorità di trattamento dei rischi considerando gli obiettivi dell'Ente e il contesto in cui opera.

La metodologia adottata prevede che per la valutazione del Rischio di sicurezza sia utilizzato un metodo di calcolo definito "qualitativo" secondo il quale per la determinazione della probabilità, dell'impatto e del GdR dei controlli, siano adottate delle scale di valori discrete, la cui valorizzazione sia ottenuta tramite un metodo di rilevazione sistematico basato su questionari, o schede di rilevazione.

Nello schema seguente sono rappresentate le macro attività previste per la fase di Valutazione del rischio, i ruoli coinvolti ed i relativi prodotti risultanti. Nei sotto paragrafi successivi viene riportato il dettaglio della metodologia adottata.

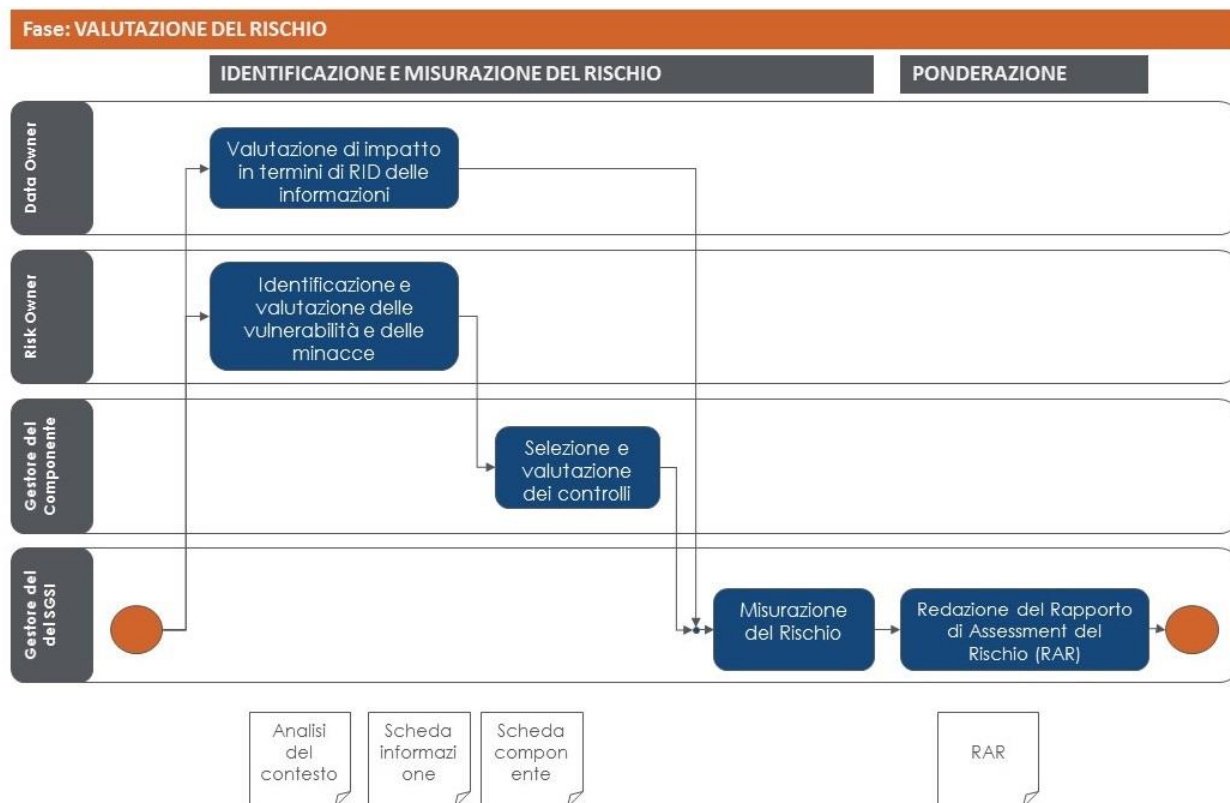


Figura 2: Schema di Valutazione del rischio.

Al termine della fase di Valutazione del rischio il Gestore SGSI<sup>4</sup> e il Risk Owner devono valutare se i risultati ottenuti sono adeguati, altrimenti, devono rivedere quanto svolto nell'Analisi del contesto.

Gli esiti della fase sono utilizzati allo scopo della Comunicazione del rischio e per lo svolgimento della fase di Monitoraggio e review del SGSI.

#### 4.1 Valutazione di impatto in termini di RID delle informazioni

Per la determinazione dell'impatto in termini di RID delle informazioni, si è scelto un metodo di rilevazione basato su questionari o Schede informazione. In particolare, il Gestore SGSI provvede, per ogni informazione, alla predisposizione dei questionari per la valutazione della criticità in termini di RID. I questionari sono distribuiti ai Data Owner rispetto alle informazioni gestite nel perimetro. I Data Owner con la compilazione delle schede consentono di determinare la criticità delle informazioni in termini di RID ossia

<sup>4</sup> Il Gestore SGSI è uno dei ruoli previsti nell'organizzazione del SGSI. Uno dei compiti principali è raccogliere le informazioni utili al monitoraggio e riesaminare periodicamente i risultati del SGSI. Per la descrizione di dettaglio si rimanda la Manuale SGSI [5].

rispetto alla severità dei danni che l'Ente subisce nel caso che le informazioni perdano la propria Riservatezza, Integrità o Disponibilità.

Per le valutazioni della criticità RID delle informazioni che rientrano nella classificazione di "dati personali", secondo quanto previsto dal Regolamento UE 2016/679 per la protezione dei dati personali (GDPR), i questionari sono integrati da uno specifico controllo per la rilevazione dell'impatto sui diritti e sulle libertà dell'interessato.

Una volta compilati dai Data Owner, i questionari sono restituiti al Gestore del SGSI e al Risk Owner per l'opportuna analisi.

Il Gestore SGSI, ove previsto, provvede a sottomettere gli esiti della valutazione anche al Responsabile della protezione dei dati (RPD), nominato ai sensi dell'art. 37 del predetto Regolamento, al fine che possa effettuare una valutazione tra quanto indicato dal Data Owner e quanto richiesto dalla normativa in materia di trattamento dei dati personali.

Nell'ambito della prima implementazione del SGSI, considerando che nel Data Center sono trattate tutte le informazioni dell'Ente, è stata considerata una sola informazione aggregata (tutto il patrimonio informativo) alla quale è stata attribuita la massima gravità rispetto a tutte le dimensioni RID in una scala di valori da 1 (impatto non significativo) a 5 (gravità estremamente alta con significativa perdita economica, reputazionale o di identità).

## **4.2 Identificazione e valutazione delle vulnerabilità e minacce**

Come per la determinazione dell'Impatto, anche per la determinazione del valore della probabilità è proposto un metodo di rilevazione basato sulla somministrazione di questionari, o schede di rilevazione.

In questa fase, sono prodotte dal Gestore SGSI le Schede componente che sono condivise con il Risk Owner affinché siano opportunamente distribuite ai Gestori dei componenti nel perimetro. In particolare, questa fase di identificazione e valutazione è basata sui seguenti passi:

- per ogni tipologia di componente è definito un profilo di vulnerabilità e di minacce pertinenti;
- per ogni componente definito nell'ambito del perimetro, il Gestore del componente stima in maniera qualitativa il Livello di Esposizione (LE) del componente ad una minaccia. In sostanza l'attività consiste nella verifica e nell'eventuale adeguamento del profilo di vulnerabilità del componente;
- la stima di cui al punto precedente viene effettuata senza considerare i controlli di sicurezza per ciascun componente.

Nel dettaglio, il Livello di Esposizione ad una minaccia in uno specifico componente è il risultato della considerazione di due fattori:

- la probabilità di occorrenza della minaccia ovvero della frequenza con cui un attacco/incidente può realizzare la minaccia in un determinato arco temporale (ad esempio un anno), indipendentemente dal suo successo (Frequenza della minaccia);
- la facilità con cui la minaccia può sfruttare una o più vulnerabilità intrinseche del componente (Livello di sfruttamento della minaccia).

I Gestori dei componenti, compilano le Schede Componenti indicando il Livello di Esposizione (LE) del componente alle minacce in una scala di valori condivisa, quindi sottopongono le schede compilate al Gestore SGSI per le opportune valutazioni.

Nell'ambito della prima implementazione del SGSI, è stato considerato un insieme di minacce ispirate a quanto presente nella tassonomia proposta dall'agenzia europea per la sicurezza delle reti e dell'informazione, ENISA (European Network and Information Security Agency). Per ogni minaccia sono stati determinati gli effetti rispetto ai requisiti di RID (ad esempio la minaccia Denial of Service –DOS- agisce solo sulla disponibilità della informazione).

Le minacce, suddivise in nove classi e settantasei minacce di dettaglio, sono associate ai componenti nel perimetro da parte del Gestore del SGSI e vengono sottoposte alla verifica dei Gestori del componente per la valutazione e conferma dei LE proposti, espressi in una scala da 0 a 5 (0 non significativo a 5 altamente frequente -3/4 volte al mese).

### **4.3 Determinazione del valore di Rischio intrinseco**

Il valore del Rischio intrinseco costituisce un indice di quanto è opportuno proteggere, nei confronti della minaccia in esame, la Riservatezza, l'Integrità e la Disponibilità dell'informazione più critica associata al componente.

Tale valore, è ottenuto sulla base dei valori di probabilità rilevati dalle Schede componente compilate a cura dei Gestori del componente e dei valori di impatto rilevati tramite le Schede informazione compilate a cura dei Data Owner.

In particolare, il Gestore SGSI determina, nel perimetro di analisi, il valore del Rischio intrinseco come prodotto matriciale dei Livelli di Esposizione dei componenti alle minacce e degli impatti sulle informazioni.

Il RI considera solo le minacce e la criticità del componente, non prende in considerazione le eventuali misure di protezione in essere. Il valore del Rischio intrinseco è pertanto calcolato come segue:

<b>valore stimato della probabilità</b>	<b>X</b>	<b>valore stimato dell'impatto</b>
---	----------	--

**VALORI E FREQUENZA DELLA PROBABILITÀ**

Valori in una scala da 0 a 5

**VALORI E IMPORTANZA DELL'IMPATTO**

Valori in una scala da 1 a 5

Il valore del Rischio intrinseco è, dunque, esprimibile in un range di valori tra 0 e 25. Più nel dettaglio, il Rischio Intrinseco (RI) è calcolabile come segue:

Dati,

*m = minaccia*

*c = componente*

*I = informazione*

*LE(m, c) = Livello di Esposizione del componente c alla minaccia m*

*IMP (I) = impatto sull'Ente della perdita dei requisiti RID della informazione I*

Si ha,

$$RI(m, c, I) = \frac{\sum_{z=(RID)} (LE(m, c) \cdot z(m) \cdot z(c) \cdot IMP(I) \cdot z(I))}{\sum_{z=(RID)} (z(m) \cdot z(c))}$$

Nel caso il perimetro sia riferito a più di una informazione, il valore di Rischio intrinseco nel perimetro può essere determinato come valore medio dei *RI (m, c, I)*.

#### **4.4 Identificazione e valutazione dei controlli**

Ottenuto il valore di Rischio intrinseco, è possibile determinare il Rischio residuo tenendo conto delle azioni attuate in risposta al rischio.



Nell'ottica della certificazione del SGSI, al fine del calcolo del Rischio residuo, il Gestore del SGSI predispone una scheda, da compilare a cura del Gestore del componente, avente lo scopo di valutare, per ogni componente, il grado di attuazione dei controlli previsti nell'allegato A del UNI CEI ISO/IEC 27001:2014 [3] in modo da poter stimare il Grado di Robustezza (GdR) dei controlli in essere.

Per ogni componente sono selezionati e proposti nella scheda solo i controlli pertinenti alla tipologia di componente analizzato. Il Gestore del componente deve verificare tale profilo di controlli e valutare il relativo Grado di Robustezza.

Le varie istanze di controllo (protezioni) pertinenti un componente possono essere realizzate con diversi gradi di robustezza, ovvero con diverse capacità di:

- resistere ad attacchi più o meno sofisticati;
- resistere ad azioni di aggiramento o di riduzione della loro efficacia;
- assicurare e monitorare la loro efficacia nel tempo.

Una volta compilate le schede, i Gestori dei componenti provvedono alla relativa condivisione con il Gestore SGSI e il Risk Owner.

Nell'ambito della prima implementazione del SGSI, è stato richiesto ai Gestori dei componenti di valutare il GdR in una scala di valori tra 0 (non praticato) a 10 (completamente attuato). A supporto dei Gestori dei componenti, per la valutazione del GdR, è stata fornita la specifica dei controlli [2] e un documento per il supporto nell'autovalutazione del valore.

#### **4.5 Determinazione del valore di Rischio residuo**

Il valore del Rischio residuo (RR) nel perimetro di analisi è, come detto, determinato in funzione del Rischio intrinseco e dell'efficacia dell'attuazione dei controlli sui componenti nel contrasto alle minacce. Pertanto il Rischio residuo è determinato come segue:

$$\text{Rischio residuo} = \text{Rischio intrinseco} * \text{GAR}$$

Dove per GAR si intende il Grado di Abbattimento del Rischio intrinseco.

Il valore del GAR è derivato dai valori dei GdR espressi dai Gestori dei componenti nella Scheda di rilevazione dei controlli ed è calcolato in dettaglio come segue:

Dati,

*m* = minaccia

*c* = componente



$I$  = informazione

$CC$  = controllo

$LE(m, c)$  = Livello di Esposizione del componente  $c$  alla minaccia  $m$

$IMP(I)$  = impatto sull'Ente della perdita dei requisiti RID della informazione  $I$

Si ha,

$$RR(m, c, I, CC) = RI(m, c, I) \cdot GAR(CC)$$

$$GAR(CC) = \frac{\sum_{z=(RID)} GDR \cdot z(CC) \cdot z(m)}{\sum_{z=(RID)} z(m)} \cdot 10$$

Il valore del Rischio residuo calcolato è rappresentato da un valore da 0 a 25 essendo derivato dal valore del Rischio intrinseco abbattuto per effetto della considerazione dei controlli. Nella schematizzazione seguente si riporta un possibile scenario di priorità rispetto al valore di Rischio residuo ottenuto:

<b>IMPATO</b>	<b>5</b> molto alto					
	<b>4</b> alto					
	<b>3</b> medio/alto					
	<b>2</b> medio					
	<b>1</b> basso					
		<b>0-1</b> Improbabile	<b>2</b> poco probabile	<b>3</b> probabile	<b>4</b> molto probabile	<b>5</b> altamente probabile
<b>PROBABILITA'</b>						

La scala di misurazione degli elementi di rischio è strutturata sui seguenti indici di rischio:

- rischio basso per valori inferiori a 6;
- rischio medio per valori compresi tra 6 e 12;
- rischio alto per valori uguali o superiori a 12.

**BASSO**  
**RISCHIO < 6**

**MEDIO**  
**6 ≤ RISCHIO < 12**

**ALTO**  
**RISCHIO ≥ 12**

Il Rischio residuo potrà essere accettato o meno, e in tale caso saranno attuate le opportune opzioni di trattamento.

#### **4.6 Redazione del Rapporto di Assessment del Rischio residuo**

Una volta identificato il livello di Rischio residuo, il Gestore del SGSI si occupa della redazione del documento denominato Rapporto di Assessment del Rischio (RAR).

Il documento RAR include i risultati dell'assessment sia in termini generali sia analitici per componente, controlli e minacce.

Il documento prodotto dal Gestore del SGSI viene verificato dai Data Owner e dai Risk Owner, eventualmente in collaborazione con i Gestori dei componenti per specifiche verifiche. Nell'ambito di questa attività, possono essere considerati anche altre eventuali fonti informative di supporto tra le quali ad esempio i risultati di attività di Vulnerability Assessment, di rapporti di Audit, di rapporti di incidenti, etc.

Nel caso in cui i risultati dell'Assessment non siano ritenuti adeguati dovranno essere riesaminati sia gli esiti dell'Analisi del contesto che della Valutazione del rischio.

Il documento è approvato dal Responsabile del SGSI.

### **5. TRATTAMENTO DEL RISCHIO RESIDUO**

La fase di Trattamento del Rischio residuo, come previsto anche dalla norma [3], prevede che:

- vengano analizzati i risultati della Valutazione dei rischi espressi nel RAR in funzione del perimetro di applicazione del SGSI effettuando uno specifico approfondimento per gli eventi particolarmente rischiosi;
- vengano valutate le priorità di trattamento del rischio.

Il risultato della fase di Trattamento del rischio è la definizione del documento denominato Piano di Trattamento del Rischio (PTR). Per giungere a questo risultato è adottato un procedimento atto a selezionare le opzioni di trattamento del rischio più opportune, a identificare gli interventi di attuazione di tali opzioni e riportarli nel documento PTR, e infine, a formalizzare l'accettazione del rischio residuo. Di seguito le macro attività previste:



Figura 3: Macro attività per l'approvazione del PTR.

Nella matrice che segue sono indicate le responsabilità dei ruoli coinvolti nelle precedenti macro attività:

	Data Owner	Risk Owner	Gestore del componente	Responsabile SGSI <sup>5</sup>	Gestore SGSI
Selezione delle opzioni di trattamento del rischio		R			P
Redazione del Piano di Trattamento del Rischio		P	P		R
Verifica del PTR		P	P		R
Approvazione del PTR	I	I	I	R	P
Accettazione del rischio residuo		R		I	I
Attivazione degli interventi		R	R		P

### Legenda

R = Responsabile

P = Partecipa

I = Informato

## 5.1 Selezione delle opzioni di trattamento del rischio

Il Risk Owner ha il compito di selezionare l'opzione di trattamento del rischio più adeguata e coerente con le aspettative di sicurezza delle informazioni. Le opzioni contemplate per il trattamento del rischio sono:

- **Evitare il rischio:** adottare cambiamenti in maniera che la minaccia non possa più manifestarsi o non generi conseguenze;

<sup>5</sup> Il Responsabile SGSI è uno dei ruoli previsti nell'organizzazione del SGSI. Uno dei compiti principali è definire gli obiettivi e i piani del SGSI da sottoporre all'approvazione del Vertice. Per la descrizione di dettaglio si rimanda la Manuale SGSI

- **Ridurre il verificarsi del rischio:** intervenire proattivamente per ridurre la probabilità che una minaccia si manifesti attuando o irrobustendo opportuni controlli;
- **Attenuare l'effetto del rischio:** attuare o irrobustire controlli per ridurre le conseguenze associate al rischio, per esempio adottando un piano di emergenza;
- **Trasferire il rischio:** far prendere ad una terza parte la responsabilità su parte delle conseguenze finanziarie di una minaccia. Tale opzione, consiste in una forma dell'opzione "riduci" che agisce solamente sulle conseguenze finanziarie di una minaccia;
- **Condividere il rischio:** ovvero concordare con una terza parte la condivisione delle perdite se i costi superano quelli pianificati;
- **Mantenere il rischio:** decidere di non fare nessuna azione e mantenere il rischio così come risulta dal RAR. La scelta di tale opzione deve essere motivata tenendo conto del livello di rischio risultante e della fattibilità e convenienza o meno di intraprendere azioni di mitigazione. In particolare, se il livello di rischio soddisfa i criteri di accettazione del rischio residuo, non vi è alcuna necessità di attuare ulteriori trattamenti e il rischio può essere mantenuto.

Sulla base del valore del Rischio residuo ottenuto nella fase di Valutazione del Rischio è possibile decidere di intraprendere una delle azioni poc'anzi indicate, anche in considerazione dei criteri di accettazione del rischio<sup>6</sup> definiti e riportati nella seguente tabella.

#### Tabella criteri di accettazione del rischio per il SGSI

---

<sup>6</sup> I criteri di accettazione del rischio definiscono le condizioni e l'eventuale processo decisionale per poter selezionare le opzioni di trattamento.

Livelli di accettabilità	Processo decisionale	RR Componente
<b>Accettabile</b>	Il rischio è accettabile così com'è senza necessità di approvazioni selezionando l'opzione di trattamento del rischio "Mantieni il rischio"	0 - 5
<b>Accettabile con riserva</b>	In generale occorre intervenire sul rischio selezionando un'opzione di trattamento diversa da "Mantieni il rischio". Può essere selezionata l'opzione "Mantieni il rischio" solo se approvata da parte del Responsabile del SGSI a seguito di una decisione motivata e verbalizzata da parte del Risk Owner con il Gestore del SGSI	6 - 11
<b>Accettabile con approvazione del Vertice Aziendale</b>	In generale occorre intervenire sul rischio selezionando un'opzione di trattamento diversa da "Mantieni il rischio". Può essere selezionata l'opzione "Mantieni il rischio" esclusivamente se approvata dal Vertice dell'Ente a seguito di una proposta motivata e verbalizzata da parte del Responsabile del SGSI	12 - 17
<b>Inaccettabile</b>	Occorre necessariamente intervenire sul rischio con una opzione di trattamento diversa da "Mantieni il rischio"	18 - 25

Nel caso che il Rischio residuo consenta, in base ai criteri di accettazione del rischio, la scelta dell'opzione "Mantieni il rischio", il PTR deve essere comunque prodotto, ma non necessariamente deve riportare specifici interventi.

Negli altri casi, occorre prima definire l'opzione prescelta per il trattamento e quindi indicare gli interventi previsti in linea con l'opzione prescelta, relativamente ai componenti che hanno, con maggior valore, contribuito alla determinazione del Rischio Residuo complessivo.

Il Gestore del SGSI, sulla base delle informazioni fornite dal Risk Owner inerenti alla selezione delle opzioni del trattamento del rischio provvede a redigere la Dichiarazione di Applicabilità (DDA) che riporta i l'elenco dei controlli dell'Appendice A alla norma ISO/IEC 27001-2014 [3] e le giustificazioni per l'inclusione o per l'esclusione dei controlli. La Dichiarazione di applicabilità deve essere approvata dal Responsabile del SGSI.

## 5.2 Redazione del Piano di Trattamento del Rischio

All'esito della fase precedente viene prodotto il Piano di Trattamento del Rischio (PTR) che identifica gli interventi in termini di attività, responsabilità, tempi e priorità per la mitigazione dei rischi rilevati a seguito della valutazione del rischio.

Obiettivo di ogni intervento è il miglioramento della robustezza di un insieme di istanze di controllo (controllo realizzato da un Componente).

Nella valutazione delle priorità si tiene conto dei seguenti fattori:

- risultati della valutazione del rischio (maggiori Rischi residui portano a maggiore priorità);
- considerazioni in relazione alle altre iniziative dell'Ente con cui gli interventi si devono armonizzare;
- costo stimato della realizzazione, che deve essere commisurato al rischio ovvero all'impatto causato da un evento dannoso e alla probabilità di accadimento di tale evento;
- facilità d'uso del controllo previsto nell'intervento e trasparenza per l'utente;
- selezione del tipo di funzionalità eseguite dal controllo previsto nell'intervento (di prevenzione, di deterrenza, di rilevazione, di limitazione delle conseguenze, di recupero) al fine di avere una protezione più efficace ed efficiente.

Si possono distinguere gli interventi in due categorie, e precisamente:

- interventi trasversali realizzati tramite progetti di AeR che hanno impatto su più componenti. In molti casi tali progetti possono già essere in corso d'opera;
- interventi specifici, realizzati tramite attività dei singoli Gestori dei componenti a cui compete la relativa gestione.

Nel PTR devono essere indicati i seguenti punti:

- sintesi dei risultati della valutazione del rischio;
- analisi di accettabilità per componente;
- punti di forza e aree di miglioramento;
- piano degli interventi.

Rispetto al documento PTR che si intende realizzare saranno ricompresi almeno i seguenti paragrafi.

Il paragrafo "Analisi per componente" riporta la tabella con tutti i componenti ordinati in ordine decrescente di RR.

Componente	RR	Liv. Accett.
Componente 1		Inaccettabile
Componente 2		Accettabile con riserva
Componente 3		Accettabile
Componente 4		

Nel paragrafo “Opzioni di trattamento del rischio” si indicano le opzioni di trattamento del rischio che si vogliono adottare.

Nel paragrafo “Interventi di mitigazione del rischio”, cioè per gli interventi che evitano, riducono o attenuano il rischio, si riporta una tabella in cui per ogni intervento viene indicata:

- il nome dell'area di intervento;
- la priorità in termini di Alta, Media, Bassa;
- la struttura che ha la principale responsabilità gestionale degli interventi;
- la data prevista di conclusione degli interventi;
- gli obiettivi degli interventi;
- i benefici indotti dagli interventi.

Di seguito si riporta un esempio di tale tabella:

Area di interventi	Priorità	Responsabilità	Data conclusione	Obiettivo Interventi	Benefici	Agisce sul controllo
Monitoraggio	Alta		GG/MM/AAA		-	12.04.1
	Media		GG/MM/AAA	–	-	06.01.2

### 5.3 Verifica del PTR

Il Gestore del SGSI, con la collaborazione dei Gestori delle Componenti e del Risk Owner esamina il PTR per verificare che gli interventi previsti siano fattibili e coerenti con gli obiettivi del SGSI e con il piano SGSI. Nella verifica si tengono in conto anche eventuali altri interventi infrastrutturali pianificati che possono coincidere, o essere di supporto a quelli indicati nel PTR. A valle della verifica è il Risk Owner che provvede alla definitiva convalida.

## 5.4 Approvazione del PTR

Il Risk Owner esegue una verifica del PTR valutando se gli interventi previsti nel PTR sono efficaci per la riduzione del rischio e in linea rispetto ai criteri di accettabilità del rischio residuo. Quindi, provvede alla accettazione del documento e lo sottopone al Responsabile SGSI per l'approvazione. In caso di non approvazione, il PTR deve essere rivisto insieme al Gestore SGSI.

## 5.5 Accettazione del Rischio residuo

Il Risk Owner provvede a redigere il "Verbale di accettazione del Rischio residuo" per l'accettazione formale dei Rischi residui e provvede a firmarlo oppure a porlo alla firma del Responsabile SGSI ovvero del Vertice dell'Ente, secondo il relativo livello di accettabilità del rischio.

Il PTR, insieme ai documenti "Perimetro e scenario per il SGSI del Servizio", al RAR e al Verbale di accettazione del Rischio residuo, vengono sottoposti al Responsabile del SGSI per la loro approvazione.

Il Gestore del SGSI riporta gli interventi previsti nel PTR nel "Piano annuale per la sicurezza dell'informazione", sia in termini di obiettivi che di attività.

Per l'attivazione degli interventi previsti sul PTR, il Risk Owner provvede a richiedere ai Gestori dei componenti l'attivazione dei vari interventi tramite le procedure dell'Ente previste allo scopo.

# 6. COMUNICAZIONE DEL RISCHIO, MONITORAGGIO E REVIEW

Queste fasi sono continue rispetto al processo di valutazione e trattamento del rischio.

Periodicamente il Risk Owner informerà il Gestore del SGSI sull'andamento dell'attuazione del PTR e su eventuali criticità rilevate.

L'attività di verifica dell'efficacia del SGSI è continua e costituisce un elemento fondamentale per garantire il principio cardine di un SGSI ossia il miglioramento continuo. Il monitoraggio costituisce un momento di verifica sia del grado di conseguimento degli obiettivi, sia della corretta implementazione delle modalità di gestione prescelte. Ogni deviazione dagli obiettivi e dalle politiche è oggetto di una analisi di dettaglio finalizzata alla identificazione dei fattori ostativi al successo delle soluzioni individuate.

Una volta registrati gli esiti della analisi è avviata la ridefinizione (correttiva) dei programmi di gestione.



Ad un primo livello di analisi, tali attività di verifica sono esplicitate mediante opportune risorse identificate come Lead Auditor interni alla struttura del Gestore del SGSI a seguito di opportuna formazione. Ad un secondo livello, le attività sono deputate alle strutture preposte dalla organizzazione per il monitoraggio specifico di tutte le attività dell'Ente.

Area Innovazione e Servizi Operativi

II DIRETTORE

Marco Balassi

*(Firmato digitalmente)*