

SGSI - Gestione delle Non Conformità e Azioni Correttive

Agenzia delle Entrate-Riscossione

INDICE DEI CONTENUTI

1. REVISIONI DEL DOCUMENTO	3
2. INTRODUZIONE.....	3
3. DEFINIZIONI DELLE NON CONFORMITÀ E DELLE AZIONI CORRETTIVE	3
3.1 Definizione di Non Conformità.....	3
3.2 Definizione di Azione correttiva	4
4. SEGNALAZIONI DELLE NON CONFORMITÀ	4
5. INDIVIDUAZIONE DELLE AZIONI CORRETTIVE	5
6. ATTUAZIONE DELL'AZIONE CORRETTIVA.....	6
7. VALUTAZIONE DELL'AZIONE CORRETTIVA	6
8. MATRICE DELLE RESPONSABILITÀ.....	7
9. APPENDICE – COMPILAZIONE DEI MODULI	8
9.1 Modulo “Segnalazione Non Conformità”	8
9.2 Modulo “Azione Correttiva”	10

1. REVISIONI DEL DOCUMENTO

Titolo	Gestione Non Conformità e Azioni Correttive	Data	09/10/2019
Autore	Gestore SGSI	Riferimento	PGS_SGSI_Gestione Non Conformità e Azioni Correttive_v2.0
Approvato da	Responsabile SGSI	Verificato da	Gestore SGSI

2. INTRODUZIONE

Scopo del documento è descrivere le attività previste per la gestione delle Non Conformità (anche NC) rilevate nell'ambito della sicurezza delle informazioni e delle conseguenti Azioni Correttive (anche AC).

I criteri adottati ed i contenuti riportati nel documento sono in linea con lo standard ISO 27001 e sono, pertanto, attuati nell'ambito del Sistema di Gestione della Sicurezza delle Informazioni (di seguito SGSI o Sistema).

Il documento è rivolto al personale che opera all'interno del Sistema di Gestione della Sicurezza delle Informazioni.

3. DEFINIZIONI DELLE NON CONFORMITÀ E DELLE AZIONI CORRETTIVE

Nei successivi paragrafi, dopo le definizioni di Non Conformità e Azione Correttiva, è riportata la descrizione delle attività relative al processo di Gestione delle Non Conformità e delle Azioni Correttive.

3.1 Definizione di Non Conformità

La Non Conformità consiste nel mancato soddisfacimento di un requisito normativo, ovvero di un'esigenza o aspettativa delle Parti Interessate.

I requisiti possono essere:

- normativi, cogenti (leggi e normativa nazionale e/o comunitaria);
- riferiti alla norma ISO/27001;
- contrattuali;
- riferiti a norme interne all'Ente che delineano modalità operative, organizzative e di controllo inserite nel Sistema Normativo di Agenzia (SNA) o contenute nei documenti del SGSI;
- inerenti alla riservatezza, integrità e disponibilità delle informazioni.

Le NC possono essere:

- NC maggiori (NC1): NC che hanno impatto sulla capacità del Sistema di ottenere i risultati desiderati. Ad esempio, quando sussiste un dubbio significativo che possa essere compromessa l'efficacia del SGSI, quando prodotti/servizi non soddisfano i requisiti del Sistema, oppure nel caso di numerose NC minori riferite al non soddisfacimento del medesimo requisito che potrebbero essere correlate ad un errore sistemico.
- NC minore (NC2): NC che non ha impatto sulla capacità del Sistema di ottenere i risultati desiderati.

3.2 Definizione di Azione correttiva

Un' Azione Correttiva è una azione tesa ad eliminare la **causa** di una Non Conformità rilevata e ad evitare che quest'ultima possa ripresentarsi. Una NC può dipendere da più cause e pertanto potrebbero essere necessarie più AC.

Le Azioni Correttive sono definite ed attuate sulla base di:

- Non Conformità riscontrate negli Audit interni di primo livello e di secondo livello e negli Audit di terza parte (ad esempio Ente di Certificazione);
- decisioni maturate in sede di riesame del SGSI;
- decisioni collegate al riesame dei servizi;
- segnalazioni pervenute dalle Parti Interessate, interne ed esterne, circa il verificarsi di situazioni che impediscono l'attuazione di quanto previsto dalle Politiche di Sicurezza, Procedure, Manuale della Sicurezza, Requisiti cogenti;
- proposte di azioni di miglioramento.

Deve essere mantenuto un registro delle azioni correttive attuate e devono essere registrati i risultati e l'efficacia rispetto alla rimozione/attenuazione delle rispettive cause di Non Conformità.

4. SEGNALAZIONI DELLE NON CONFORMITÀ

Le Non Conformità possono essere rilevate da parte di tutto il personale di Agenzia delle Entrate-Riscossione (di seguito anche Ente). In tal caso può essere inviata una email alla casella funzionale sgsi.governance@agenziariscossione.gov.it con allegato il modulo "MGS_SGSI_Segnalazione Non Conformità", riportato in appendice, appositamente compilato. La casella è presidiata dall'Ufficio SGSI Governance (Gestore SGSI) che, ricevuta la segnalazione, provvede ad indicare le informazioni previste e ad attribuire un identificativo univoco alla Non Conformità.

Qualora la comunicazione avvenga tramite altri canali (telefono, voce, verbali, ecc.) l'Ufficio SGSI Governance provvede alla compilazione del modulo e alla relativa archiviazione e numerazione. Normalmente, le NC scaturiscono a seguito di:

- audit interni di primo e di secondo livello svolti nell'ambito del Programma di audit SGSI annualmente definito;
- audit di terza parte che vengono eseguiti da Enti esterni, per es. Enti di Certificazione;
- risultanze del Riesame di Direzione previsto per il SGSI.

5. INDIVIDUAZIONE DELLE AZIONI CORRETTIVE

A fronte di una Non Conformità l'Ufficio SGSI Governance provvede a:

- inquadrare correttamente la situazione riscontrata;
- verificare l'impatto della NC rispetto agli obiettivi di sicurezza delle informazioni.

A valle di questa analisi il Gestore SGSI decide se dare seguito alla segnalazione.

In caso negativo, il Gestore SGSI chiude la segnalazione di Non Conformità con opportuna motivazione.

In caso affermativo, apre uno o più moduli di Azione Correttiva (utilizzando l'apposito modulo MGS_SGSI_Azione Correttive posto in appendice, assegnando allo stesso un identificativo univoco) e procede alla relativa assegnazione alle Strutture interessate. Nel dettaglio il modulo è composto da sezioni la cui compilazione è in parte a cura del Gestore SGSI che provvede alla descrizione della NC e in parte è a cura della Struttura organizzativa interessata dalla risoluzione che, data la NC, deve valutare l'Azione Correttiva (o più di una) ritenuta più appropriata e la data prevista per il relativo completamento.

Nella compilazione di quanto previsto, la Struttura organizzativa interessata dalla risoluzione della NC procede con l'analisi delle cause della Non Conformità ed in particolare deve:

- verificare la frequenza con cui la situazione segnalata ricorre;
- determinare la gravità del problema segnalato;
- individuare le cause che hanno determinato la NC emersa;
- definire un adeguato piano delle attività (Action Plan) per la rimozione delle cause della Non Conformità.

Dall'analisi condotta sarà possibile classificare la NC (maggiore o minore). È importante sottolineare che le AC devono essere adeguate agli effetti delle NC riscontrate (requisito 10.1 della norma ISO27001).

6. ATTUAZIONE DELL'AZIONE CORRETTIVA

L'attuazione della AC descritta a fronte della NC rilevata è responsabilità della Struttura organizzativa interessata, sia in termini di realizzazione di quanto indicato, sia di rispetto delle tempistiche previste.

A titolo esemplificativo le Azioni Correttive individuate possono comportare:

- adozione di nuovi strumenti a supporto delle attività o di nuove modalità operative;
- aggiornamento o emissione di nuovi regolamenti interni;
- revisione del SGSI in termini di aggiornamento o emissione di nuove procedure;
- attività di formazione per il personale coinvolto nei problemi rilevati.

Il Gestore del SGSI monitora l'attuazione dell'Azione Correttiva.

7. VALUTAZIONE DELLA AZIONE CORRETTIVA

Il Gestore del SGSI ha il compito di valutare i risultati dell'Azione Correttiva. Se i risultati sono ritenuti efficaci, provvede alla chiusura, completando il modulo relativo alla AC delle seguenti informazioni:

- risultati dell'Azione Correttiva;
- valutazione dell'efficacia dell'Azione Correttiva.

Nel caso le azioni attuate siano ritenute non efficaci, il Gestore SGSI provvede a richiedere alla Struttura organizzativa interessata la formulazione di un'ulteriore Azione Correttiva da implementare.

È compito del Gestore del SGSI mantenere le registrazioni delle Non Conformità e delle Azioni Correttive.

8. MATRICE DELLE RESPONSABILITÀ

La tabella seguente riporta l'elenco delle attività precedentemente descritte e relative al processo di Gestione delle Non Conformità e delle Azioni Correttive con il dettaglio degli attori coinvolti ed il ruolo rivestito:

Attività	Segnalatore ¹	Gestore SGSI	Strutture organizzative interessate
Segnalazione delle NC	R	I	
Individuazione delle AC		I	R
Attuazione della AC		P	R
Valutazione della AC		R	I

Legenda:

AC = Azione Correttiva

NC = Non Conformità

R = Responsabile

P = Partecipa

I = Informato

¹ Auditor o dipendente dell'Ente che, a fronte della rilevazione di eventi che impediscono l'attuazione di quanto definito dalle politiche generali di sicurezza e dalle procedure che ne discendono, provvede a segnalare la NC.

9. APPENDICE – COMPILAZIONE DEI MODULI

9.1 Modulo “Segnalazione Non Conformità”

Il modulo viene utilizzato sia per segnalare che per registrare le Non Conformità. Il modulo è suddiviso nelle seguenti tre sezioni.

SEGNALAZIONE

Tale sezione deve essere compilata da chi fa la segnalazione via modulo o da un addetto dell'Ufficio SGSI Governance che riceve la segnalazione.

Devono essere contenute le seguenti informazioni:

- Struttura/e coinvolta/e
- Nome segnalante
- Data
- Descrizione della Non Conformità
- Natura della Non Conformità (maggiore/minore)
- Modalità di Rilevazione
- Documentazione e requisiti normativi di riferimento
- Osservazioni e note
- Allegati (esempio verbale, riesame, rapporto)

REGISTRAZIONE

La compilazione è a cura dell'Ufficio SGSI Governance e prevede:

- Identificativo Non Conformità (progressivo univoco)
- Nominativo di chi effettua la registrazione
- Data di registrazione

RISULTANZE E CHIUSURA

La compilazione è a cura dell'Ufficio SGSI Governance che, a seguito di una prima analisi della segnalazione di Non Conformità, fornisce le seguenti informazioni:

- Necessaria Azioni Correttiva? ☐ SI / ☐ NO
- Note
- Firma Gestore SGSI

- Data chiusura

Modulo: Segnalazione delle Non Conformità		MGS_SGSI_Segnalazione Non Conformità	
Segnalazione			
Struttura/e coinvolta/e:			
Nome segnalante:			
Data:			
Descrizione della Non Conformità			
Natura della Non Conformità			
Modalità di Rilevazione			
Documentazione e requisiti normativi di riferimento			
Osservazione e note			
Allegati			
Registrazione			
Identificativo Non Conformità			
Nome di chi effettua la registrazione		Data di registrazione	
Risultanze e chiusura			
Necessaria Azioni Correttiva?	<input type="checkbox"/> SI <input type="checkbox"/> NO		
Note			
Firma Gestore SGSI		Data chiusura	

9.2 Modulo “Azione Correttiva”

Il presente modulo che viene utilizzato per registrare le Azioni Correttive è formato da quattro sezioni che vengono descritte di seguito.

ESIGENZA E REGISTRAZIONE

Tale sezione deve essere compilata dal Gestore SGSI che effettua la registrazione dell'Azione Correttiva. Devono essere contenute le seguenti informazioni:

- Struttura/e coinvolta/e:
- Nome segnalante:
- Identificativo della Non Conformità registrata
- Descrizione della Non Conformità
- Azione Correttiva N°:
- Nome di chi effettua la registrazione
- Data di compilazione
- Allegati

RIESAME DELLA NON CONFORMITÀ

Questa sezione viene compilata dal Gestore del SGSI. Devono essere contenute le seguenti informazioni:

- Descrizione dell'analisi condotta
- Firma Gestore SGSI
- Data

AZIONE CORRETTIVA

Questa sezione è compilata dal Responsabile della Struttura Organizzativa che deve attuare l'Azione Correttiva. Devono essere contenute le seguenti informazioni:

- Descrizione delle attività (individuate per l'attuazione della AC)
- Responsabile dell'attività
- Data prevista per il termine dell'attività
- Firma e Data devono essere compilati dal Responsabile dell'attività

CHIUSURA E VALUTAZIONE

La sezione è compilata dal Gestore SGSI quando riceve l'informativa dal Responsabile della AC sul relativo completamento. Devono essere contenute le seguenti informazioni:

- Risultati dell'Azione Correttiva
- Valutazione dell'efficacia dell'Azione Correttiva: indicare se l'Azione è stata efficace ed in caso contrario se è necessario impostare una ulteriore Azione Correttiva
- Firma e Data devono essere compilati dal Gestore del SGSI

Modulo: Azioni Correttive			MGS_SGSI_Azioni Correttive
ESIGENZA E REGISTRAZIONE			
Struttura/e coinvolta/e:			
Nome segnalante:			
Identificativo della Non Conformità registrata			
Descrizione della Non Conformità			
Azione Correttiva N°:			
Nome di chi effettua la registrazione		Data di compilazione	
Allegati			
RIESAME DELLA NON CONFORMITÀ			
Descrizione dell'analisi condotta e della proposta di azione			
Firma Gestore SGSI		Data	
AZIONE CORRETTIVA			
Descrizione dell'attività			
Responsabile delle attività		Data prevista per il termine attività	
Firma Responsabile delle attività		Data	
CHIUSURA E VALUTAZIONE			
Risultati dell'Azione Correttiva			
Valutazione dell'efficacia dell'Azione Correttiva			
Firma Gestore SGSI		Data chiusura	

Area Innovazione e Servizi Operativi

II DIRETTORE

Marco Balassi

(Firmato digitalmente)