



Regolamento per la certificazione di Sistemi di Gestione  
della Sicurezza delle Informazioni

# **Regolamento per la certificazione di Sistemi di Gestione della Sicurezza delle Informazioni**

*In vigore dal 01Maggio 2011*

RINA  
Via Corsica 12  
16128 Genova - Italia

tel +39 010 53851  
fax +39 010 5351000  
web site : [www.rina.org](http://www.rina.org)

---

Regolamenti tecnici



RINA

Regolamento per la certificazione di Sistemi di Gestione  
della Sicurezza delle Informazioni

## INDICE

CAPITOLO 1: GENERALITÀ'

CAPITOLO 2: NORMA DI RIFERIMENTO / REQUISITI PER LA CERTIFICAZIONE

CAPITOLO 3: CERTIFICAZIONE INIZIALE

CAPITOLO 6: ESECUZIONE DEGLI AUDIT

CAPITOLO 7: GESTIONE DEI CERTIFICATI DI CONFORMITÀ'

CAPITOLO 9: PARTICOLARITÀ' PER ORGANIZZAZIONI MULTISITO

CAPITOLO 10: TRASFERIMENTO DI CERTIFICATI ACCREDITATI



## **CAPITOLO 1 GENERALITÀ'**

### **1.1**

Nel presente Regolamento sono definite le procedure supplementari, e non sostitutive, applicate da RINA per la certificazione di Sistemi di Gestione della Sicurezza delle Informazioni rispetto a quanto già definito nel:

Regolamento Generale per la certificazione di Sistemi di Gestione

I punti del presente Regolamento si riferiscono (e mantengono la stessa numerazione) ai punti corrispondenti del Regolamento Generale per la Certificazione di Sistemi di Gestione per i quali sono state apportate modifiche e/o integrazioni.

### **1.2**

*Modifica al Regolamento Generale.*

"RINA rilascia la certificazione in accordo ai requisiti della norma ISO/IEC 27006:2007 ad Organizzazioni il cui Sistema di Gestione . . . ."

### **1.7**

*Integrazione al Regolamento Generale*

La terminologia usata nel presente Regolamento è anche quella riportata nella norma UNI ISO/IEC 27001:2005 e CEI EN ISO/IEC 17000:2005.

## **CAPITOLO 2 NORMA DI RIFERIMENTO / REQUISITI PER LA CERTIFICAZIONE**

### **2.2.2**

*Integrazione al Regolamento Generale*

La stesura di un Manuale e' opzionale.

## **CAPITOLO 3 CERTIFICAZIONE INIZIALE**

### **3.1**

*Integrazione al Regolamento Generale*

Le Organizzazioni che desiderino ottenere la certificazione del loro Sistema di Gestione devono fornire a RINA anche i dati essenziali della loro Organizzazione, infrastruttura ICT, attività svolte, informazioni gestite e la localizzazione



In particolare, l'Organizzazione deve anche comunicare a RINAsè il Sistema di Gestione della Sicurezza delle informazioni comprenda documentazione (procedure, registrazioni, ecc.) classificata come "riservata" e/o comunque non disponibile ai fini della certificazione. RINA valuterà conseguentemente la sussistenza delle condizioni per poter proseguire l'iter di certificazione.

### 3.4

#### *Integrazione al Regolamento Generale*

Unitamente alla richiesta di certificazione, o successivamente alla stessa, l'Organizzazione dovrà anche rendere disponibile a RINA le seguente documentazione:

- politiche del sistema di gestione (obiettivi, principi di azione);
- documentazione relativa all'analisi del rischio (compresa la descrizione della metodologia utilizzata);
- criteri di accettazione del rischio e livello di rischio accettabile;
- piani di trattamento del rischio;
- dichiarazione di applicabilità.
- misure di efficacia dei controlli (compresa la descrizione della metodologia di misura)
- architettura della rete e dei sistemi informativi.

La stesura di una Manuale e' facoltativa

## **CAPITOLO 6**

### **ESECUZIONE DEGLI AUDIT**

#### **6.2.1**

##### *Integrazione al Regolamento Generale.*

La finalità dell'audit di fase 1 e' anche di:

- verificare che la valutazione del rischio, il piano di trattamento del rischio e la Dichiarazione di applicabilità (e le eventuali esclusioni dichiarate) siano idonee rispetto al campo di applicazione e le attività dell'organizzazione;
- verificare che le attività esternalizzate siano adeguatamente identificate e tenute sotto controllo, confermando, se del caso, la necessità di effettuare l'audit presso le terze parti.

Lo stage 1 è di norma condotto presso l'azienda, preferibilmente presso la sede o comunque presso un sito compreso nel campo di applicazione della certificazione e in cui sarà svolta la visita di stage 2. Può essere previsto in casi particolari valutati di volta in volta dal RINA che parte dello stage 1 non sia svolto presso l'organizzazione.



## 6.2.2

*Integrazione al Regolamento Generale.*

La stesura di una Manuale e' facoltativa

## CAPITOLO 7 GESTIONE DEI CERTIFICATI DI CONFORMITA'

### 7.1

*Integrazione al Regolamento Generale.*

I certificati rilasciati sotto accreditamento ANAB riportano il riferimento alla Dichiarazione di Applicabilità, la sua versione e la data di emissione, in vigore durante gli audit condotti presso l'organizzazione.

## CAPITOLO 9 PARTICOLARITA' PER ORGANIZZAZIONI MULTISITO

### 9.1

*Integrazione al Regolamento Generale.*

Tra le attività gestite dalla funzione centrale dell'Organizzazione devono rientrare anche:

- definizione e gestione della politica per la sicurezza;
- valutazione, analisi e trattamento dei rischi;
- definizione e gestione dei controlli;
- definizione e gestione della dichiarazione di applicabilità;
- valutazione dell'efficacia dei controlli implementati;

### 9.2

*Modifica al Regolamento Generale:*

“Qualora l'Organizzazione rispetti i requisiti precedenti, RINA verifica comunque la fattibilità di un campionamento su tutti i siti ed eventualmente valuta se limitare tale campionamento sulla base di:

- risultati degli audit interni della sede centrale e dei siti
- i risultati dei riesami della Direzione
- dimensioni dei siti idonei ad un audit multisito



- tipologia di attività svolta dai siti
- complessità del Sistema di gestione della Sicurezza delle Informazioni (variazioni nelle implementazioni locali)
- complessità dell'infrastruttura ICT
- variazioni nelle procedure operative e nelle attività svolte
- interazioni potenziali con sistemi informativi critici o sistemi informativi che gestiscono informazioni sensibili
- differenze nel rispetto dei requisiti legali
- rischi specifici
- presenza di reclami
- modifiche successive all'ultimo audit;
- maturità del sistema di gestione e conoscenza dell'organizzazione;
- differenze di cultura, lingua e requisiti regolamentari;
- distribuzione geografica.

.....“

## **CAPITOLO 10**

### **TRASFERIMENTO DI CERTIFICATI ACCREDITATI**

#### **10.1**

*Integrazione al Regolamento Generale.*

L'organizzazione, in caso di accettazione dell'offerta economica, deve inviare a RINA la “richiesta di certificazione” allegando anche i seguenti documenti:

- copia controllata dell'elenco della documentazione dell'SGSI
- copia controllata del Manuale (opzionale) e della Dichiarazione di applicabilità
- pianta del sito, se non “riservata”
- layout rete, se non “riservata”
- evidenza delle azioni correttive intraprese al fine di risolvere le non conformità rilevate durante le precedenti verifiche o evidenza della verifica della risoluzione delle stesse da parte dell'altro Organismo.
- copia del programma triennale degli audit



RINA

Regolamento per la certificazione di Sistemi di Gestione  
della Sicurezza delle Informazioni

Pubblicazione: RC/C 56

Edizione Italiana

RINA  
Via Corsica 12  
16128 Genova - Italia

tel +39 010 53851  
fax +39 010 5351000  
web site : [www.rina.org](http://www.rina.org)

---

Regolamenti tecnici