



RINA

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 1/07/2010

RINA
Via Corsica 12
16128 Genova - Italia

tel +39 010 53851
fax +39 010 5351000
web site : www.rina.org

Regolamenti tecnici



RINA

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

INDICE

CAPITOLO 1 GENERALITÀ.....	3
CAPITOLO 2 NORMA DI RIFERIMENTO / REQUISITI PER LA CERTIFICAZIONE.....	3
CAPITOLO 3 CERTIFICAZIONE INIZIALE.....	3
CAPITOLO 4 MANTENIMENTO DELLA CERTIFICAZIONE.....	5
CAPITOLO 8 PARTICOLARITÀ PER ORGANIZZAZIONI MULTISITO	5



RINA

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

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

Modifica al Regolamento Generale:

“La terminologia usata nel presente Regolamento è 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

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 i dati essenziali della loro Organizzazione, infrastruttura ICT, attività svolte, informazioni gestite, e la localizzazione”

In particolare, l'Organizzazione deve comunicare a RINA:



RINA

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

- se 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.

..... "

3.2

Integrazione al Regolamento Generale:

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

- procedure e registrazioni richieste dalla norma;
- procedure e registrazioni adottate dall'Organizzazione;
- politiche del sistema di gestione (obiettivi, principi di azione);
- 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

3.4

Modifica al Regolamento Generale:

".....

L'audit di stage 2 e' effettuato da tecnici qualificati del RINA sulla base del rapporto di audit dello stage 1 e dei documenti predisposti dall'Organizzazione e relativamente a quelli elencati al paragrafo 3.2"



CAPITOLO 4 MANTENIMENTO DELLA CERTIFICAZIONE

4.4

Modifica al Regolamento Generale:

“ contenute nella norma di riferimento secondo cui il Sistema di Gestione e' stato certificato, tenendo conto dei documenti di cui al punto 3.2”

CAPITOLO 8 PARTICOLARITA' PER ORGANIZZAZIONI MULTISITO

8.1

Modifica al Regolamento Generale:

“Qualora un'Organizzazione operi su più siti permanenti e sia richiesta un'unica certificazione, le attività di audit possono essere espletate per campionamento dei siti sottoposti ad audit, purché tutti i siti operino sotto lo stesso Sistema di Gestione della Sicurezza delle Informazioni gestito, verificato e riesaminato da parte della Direzione in modo centrale.

In particolare, oltre a quanto richiesto dal Regolamento per la Certificazione di Sistemi di gestione, almeno le seguenti attività devono essere gestite dalla funzione centrale dell'Organizzazione (o almeno la sede centrale deve dimostrare di essere in grado di sapere raccogliere ed esaminare i dati relativi alle attività stesse da tutti i siti e la sua autorità e la capacità di introdurre cambiamenti organizzativi, se necessario):

- riesame della politica/politiche per la sicurezza;
- riesame dell'analisi dei rischi, dei rischi residui e del livello di rischio accettabile;
- scelta dei controlli;
- riesame della dichiarazione di applicabilità;
- gestione dei processi esternalizzati;
- riesame della conformità ai requisiti di legge;
- riesame da parte della direzione;
- valutazione efficacia delle contromisure implementate;
- registrazioni delle azioni e degli eventi che abbiano un impatto sulla sicurezza delle informazioni.



RINA

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

Prima dell'audit iniziale da parte del RINA, l'Organizzazione deve aver effettuato un audit interno ad ogni sito ed abbia verificato la sua conformità alla norma di riferimento."

8.2

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.

Se i siti in cui si svolgono le attività sottoposte a certificazione non sono tutti pronti contemporaneamente per essere presentati per la certificazione, l'Organizzazione deve comunicare preventivamente a RINA i siti che essa desidera siano inclusi nella certificazione e quelli che ne devono essere esclusi. "



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

Regolamenti tecnici