Regolamento per la certificazione di Sistemi di Gestione della Sicurezza delle Informazioni ed estensione alle linee guida ISO/IEC 27xxx

In vigore dal 20/10/2020

RINA
Via Corsica 12
16128 Genova - Italia

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

Regolamenti tecnici

INDICE

CAPITOLO 1
GENERALITÀ

1.1

Questo Regolamento definisce le procedure aggiuntive e/o 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 dei 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

RINA rilascia la certificazione in accordo ai requisiti delle norme ISO/IEC 17021-1:2015 e ISO/IEC 27006:2015 ad Organizzazioni il cui Sistema di Gestione sia stato riconosciuto conforme a tutti i requisiti previsti dalla norma:

ISO/IEC 27001: 2013 (UNI CEI EN ISO/IEC 27001:2017)

La certificazione è integrabile con le linee guida:

ISO/IEC 27017: 2015
ISO/IEC 27018: 2019
ISO/IEC 27701: 2019

L'estensione alle linee guida deve avvenire a fronte di una certificazione ISO/IEC 27001:2013 (UNI CEI EN ISO/IEC 27001:2017), in corso di validità, accreditata da un Organismo di Accreditamento che aderisce all'accordo di mutuo riconoscimento IAF/MLA (IAF – International Accreditation Forum/MLA - Multilateral Agreements). Lo scopo della certificazione ISO/IEC 27001:2013 deve essere compatibile con i processi delle Linee Guida di cui si chiede l'integrabilità.

Se l'organizzazione è in possesso della certificazione ISO/IEC 27001:2013 emessa da altro Ente di Certificazione con accreditamento MLA, deve richiedere il trasferimento della certificazione a RINA prima dell'estensione alle Linee Guida come descritto al capitolo 10 del Regolamento generale per la certificazione dei Sistemi di Gestione.

Se l'organizzazione non è in possesso della certificazione ISO/IEC 27001:2013 emessa da altro Ente di Certificazione con accreditamento MLA, deve richiedere a Rina una nuova certificazione.

È ammessa l'estensione della certificazione alla linea guida ISO/IEC 27017:2015 da sola, mentre l'estensione alla linea guida ISO/IEC 27018:2019 deve essere sempre preceduta dall'estensione alla ISO/IEC 27017:2015. È ammessa l'estensione contestuale alle linee guida ISO/IEC 27017:2015 e ISO/IEC 27018:2019.

È ammessa l'estensione della certificazione alla linea guida ISO/IEC 27701:2019 da sola.

CAPITOLO 3
CERTIFICAZIONE INIZIALE

3.1

Le Organizzazioni che desiderino ottenere la certificazione del loro Sistema di Gestione della Sicurezza delle Informazione e/o l'estensione alle linee guida devono inviare a RINA oltre al modulo Questionario Informativo anche lo specifico **ALLEGATO AL QUESTIONARIO INFORMATIVO PER OFFERTA ISO/IEC 27001 (ISMS) e ISO/IEC 27XXX:20YY**, disponibile sul sito www.rina.org, compilato in tutte le sue parti.

In particolare, il Questionario informativo richiede che siano fornite informazioni su:

- Datacenter presso cui sono dislocati i server che gestiscono il servizio / Siti ove sono ubicati asset critici;
- Fattori relativi all'attività svolta e all'organizzazione;
- Fattori relativi all'ambiente IT;
- Fattori che potrebbero determinare riduzioni o incrementi della durata del tempo di audit.

Queste informazioni devono pervenire da un rappresentante autorizzato dell'organizzazione richiedente.

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 la sussistenza delle condizioni per poter proseguire l'iter di certificazione.

3.5

L'audit per l'estensione alle linee guida deve essere svolto interamente presso il sito o i siti dell'Organizzazione compresi i data center presso cui è dislocata l'infrastruttura ICT. Nel caso la tipologia di infrastruttura ICT non permettesse di svolgere un audit on site (es. fornitori come AWS, AZURE), dovranno essere verificati gli accordi contrattuali tra l'Organizzazione e i fornitori e gli aspetti di controllo operativo attuati.

CAPITOLO 5
RICERTIFICAZIONE

5.1

In occasione dell'audit di ricertificazione del Sistema di Gestione, previsto ogni tre anni, l'Organizzazione deve inviare a RINA oltre al modulo Questionario Informativo anche lo specifico **ALLEGATO AL QUESTIONARIO INFORMATIVO PER OFFERTA ISO/IEC 27001 (ISMS) e ISO/IEC 27XXX:20YY**, disponibile sul sito www.rina.org, compilato in tutte le sue parti come descritto al punto 3.1 del presente regolamento.

CAPITOLO 6
ESECUZIONE DEGLI AUDIT

6.1 GENERALITA'

6.1.1

L'audit per l'estensione alle linee guida deve essere svolto interamente presso il sito o i siti dell'Organizzazione compresi i data center presso cui è dislocata l'infrastruttura ICT come descritto al punto 3.5 del presente regolamento.

Il tempo di audit on site non deve essere inferiore al 70% del tempo totale di audit.

CAPITOLO 9
PARTICOLARITA' PER ORGANIZZAZIONI MULTISITO

9.1

Il campionamento dei siti da sottoporre ad audit comprende anche i data center presso cui è dislocata l'infrastruttura ICT. Rina valuta l'applicabilità del campionamento oltre ai criteri definiti nel **Regolamento generale per la certificazione dei Sistemi di Gestione** anche rispetto a:

- i risultati degli audit interni della sede centrale e dei siti o di precedenti audit di certificazione;
- complessità del Sistema di Gestione;
- complessità dei sistemi IT dei diversi siti;
- potenziale interazione con i sistemi IT critici o con i sistemi IT che gestiscono dati sensibili;
- la valutazione del rischio.

La funzione centrale dell'Organizzazione deve inoltre partecipare alla definizione e gestione della politica di sicurezza, valutazione del rischio, analisi e trattamento, definizione, gestione e analisi dei controlli, definizione e gestione della Dichiarazione di Applicabilità.

CAPITOLO 10
TRASFERIMENTO DI CERTIFICATI ACCREDITATI

10.1

Qualora un'Organizzazione con certificazione in corso di validità rilasciata da un altro Organismo di Certificazione di Sistemi di Gestione, accreditato da un Organismo di Accreditamento che aderisce all'accordo di mutuo riconoscimento IAF/MLA, voglia trasferire la propria certificazione a RINA, deve inviare a RINA oltre al modulo Questionario Informativo anche lo specifico **ALLEGATO AL QUESTIONARIO INFORMATIVO PER OFFERTA ISO/IEC 27001 (ISMS) e ISO/IEC 27XXX:20YY**, disponibile sul sito www.rina.org, compilato in tutte le sue parti, come descritto al punto 3.1 del presente regolamento, copia del certificato del Sistema di Gestione e copia del documento Dichiarazione di Applicabilità il cui riferimento è riportato sul certificato.

Regolamento per la Certificazione di
Sistemi di Gestione della Sicurezza delle informazioni
ed estensione alle Linee Guida ISO/IEC 27XXX

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