Regolamento di certificazione per la certificazione di sistemi di gestione per la sicurezza delle informazioni

STATO DELLE REVISIONI

Revisione	Data	Descrizione	Redatto	Approvato DIR
02	18/5/2022	Transizione alla ISO 27001	F. Lubrano (RGQ)	S. Scutiero
01	13/3/2020	Aggiornamento documentazione in seguito all'esito dell'analisi documentale per audit di accreditamento	Lucia Esca (RGQ)	Francesco Lubrano di Scorpaniello
00	05/2/2020	PRIMA EMISSIONE	Lucia Esca (RGQ)	Francesco Lubrano di Scorpaniello

Copia controllata n._____1_____

Copia non controllata n._____0_____

Certifica S.r.l.
Organismo di Certificazione
Via Petrarca, 15 – 80070 Bacoli
p.i. 08654031213 – tel. e fax 081 5237021
info@certificasistemi.com

INDICE

Certifica S.r.l.
Organismo di Certificazione
Via Petrarca, 15 – 80070 Bacoli
p.i. 08654031213 – tel. e fax 081 5237021
info@certificasistemi.com

Certifica S.r.l.
Organismo di Certificazione
Via Petrarca, 15 – 80070 Bacoli
p.i. 08654031213 – tel. e fax 081 5237021
info@certificasistemi.com

Certifica S.r.l.
Organismo di Certificazione
Via Petrarca, 15 – 80070 Bacoli
p.i. 08654031213 – tel. e fax 081 5237021
info@certificasistemi.com

1 DESCRIZIONE DELLA SOCIETA'

Nessuna integrazione rispetto a Regolamento Generale per la Certificazione di Sistemi di Gestione Aziendale RdC in revisione corrente.

2 SCOPO E CAMPO DI APPLICAZIONE

Questo documento specifica e dettaglia alcune condizioni aggiuntive specifiche relative all'iter di certificazione dei sistemi di gestione per la sicurezza delle Informazioni, secondo la norma ISO/IEC 27001.

Oltre alla norma di riferimento ISO/IEC 27001 sono qui descritte le attività e le condizioni per la certificazione delle due norme (Code of Practice) ISO/IEC 27017:2015, rispettivamente code of practice for information security controls based on ISO/IEC 27002 for cloud services" e ISO/IEC 27018:2019 Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors.

Per tutti gli argomenti non esplicitamente citati o descritti in questo Regolamento Particolare, vale quanto descritto nel Regolamento di Certificazione Generale per la Certificazione di Sistemi di Gestione Aziendale RdC

Nel presente Regolamento vengono definiti i rapporti tra CERTIFICA S.r.l. e le Organizzazioni che intendono ottenere e far registrare la Certificazione del proprio Sistema di Gestione della Sicurezza delle Informazioni in conformità allo Standard di riferimento ISO/IEC 27001 e con l'eventuale l'integrazione alle linee guida ISO/IEC 27017 e/o ISO/IEC 27018.

La 27017può essere oggetto di estensione della certificazione anche da sola. Ove si intenda considerare tale estensione anche in ottica di Protezione Dati Personali, l'estensione alla ISO/IEC 27017 dovrà essere integrata con la ISO/IEC 27018. Non è ammessa l'estensione alla sola ISO/IEC 27018.

Sull'applicazione del presente Regolamento sorveglia il Comitato Rappresentativo Parti per la salvaguardia dell'imparzialità nel quale sono rappresentate le parti interessate alla certificazione.

La certificazione può essere rilasciata sul sistema informativo aziendale nella sua interezza o in specifiche aree ed applicazioni di particolare criticità.

Il presente regolamento è consultabili sul sito www.certificasistemi.com e per qualsiasi variazione allo stesso viene immediatamente data comunicazione alle aziende certificate.

I documenti di certificazione possono fare riferimento a standard nazionali e internazionali come fonte/i di controllo impostato per i controlli che sono determinati come necessari nella Dichiarazione di Applicabilità dell'organizzazione in conformità con ISO/IEC 27001:2013, 6.1.3 d).
Il riferimento sui documenti di certificazione deve essere chiaramente indicato come solo una fonte di controllo per i controlli applicati nella Dichiarazione di Applicabilità e non una certificazione della stessa

Certifica S.r.l.
Organismo di Certificazione
Via Petrarca, 15 – 80070 Bacoli
p.i. 08654031213 – tel. e fax 081 5237021
info@certificasistemi.com

3 RIFERIMENTI

– Linea guida ISO/IEC 27002 "Information technology- Security techniques – Code of practice for information security controls", o la sua versione italiana UNI CEI EN ISO/IEC 27002.
– Linea guida ISO/IEC 27017 "Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services".
– Linea guida ISO/IEC 27018 "Information technology - Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors".
– Inoltre sono riferimento obbligatorio per l'accreditamento i documenti emessi da ACCREDIA e reperibili nel sito www.accredia.it :
• Regolamento per l'accreditamento degli Organismi di certificazione ed ispezione RG-01
• Regolamento per l'accreditamento degli Organismi di certificazione del sistema di gestione RG-01-01
• Regolamento Tecnico RT-37 rev.00 "Prescrizioni per l'accreditamento con scopo di accreditamento flessibile"
• Circolare n. 02/2018 "Informativa in merito all'accreditamento per lo schema di certificazione ISO/IEC 27001:2013 con integrazione delle linee guida ISO/IEC 270XX:20YY "Information Technology, Security techniques, Code of practice"
• Circolare n. 01/2019 "Accreditamento schema di certificazione ISO/IEC 27001:2013 con integrazione delle linee guida ISO/IEC 27017:2015 e ISO/IEC 27018:2014 - Information Technology, Security techniques, Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors"
• Altre Disposizioni e Regolamenti in materia di accreditamento.

4 PRIORITÀ DI VALIDITÀ

Nessuna integrazione rispetto a Regolamento Generale per la Certificazione di Sistemi di Gestione Aziendale RdC in revisione corrente.

5 TERMINI E DEFINIZIONI

- ISMS (Information Security Management System), equivalente a "Sistema di Gestione per la Sicurezza delle Informazioni" (SGSI)
- SoA (Statement of Applicability) equivalente a "Dichiarazione di Applicabilità" (DdA)

6 CONDIZIONI GENERALI

Nessuna integrazione rispetto a Regolamento Generale per la Certificazione di Sistemi di Gestione Aziendale RdC in revisione corrente.

Certifica S.r.l.
Organismo di Certificazione
Via Petrarca, 15 – 80070 Bacoli
p.i. 08654031213 – tel. e fax 081 5237021
info@certificasistemi.com

7 DOVERI E DIRITTI

7.1 Doveri dell'Organizzazione

7.1.1 Doveri Generali

Nessuna integrazione rispetto a Regolamento Generale per la Certificazione di Sistemi di Gestione Aziendale RdC in revisione corrente.

7.1.2 Doveri relativi all'Uso della Certificazione e dei Marchi di Certifica S.r.l.

Nessuna integrazione rispetto a Regolamento Generale per la Certificazione di Sistemi di Gestione Aziendale RdC in revisione corrente.

7.1.3 Doveri Relativi all'Audit

Nessuna integrazione rispetto a Regolamento Generale per la Certificazione di Sistemi di Gestione Aziendale RdC in revisione corrente.

7.1.4 Doveri specifici aggiuntivi per ISO 27001

L'organizzazione, all'atto della richiesta di certificazione, è tenuta a comunicare se intende avvalersi della facoltà di negare al team di audit l'accesso a documenti che contengano informazioni considerate riservate o sensibili (per esempio informazioni relative al personale, ai clienti, ai fornitori, a proprietà intellettuale, alla sicurezza nazionale); in tale caso il Certifica srl valuterà se le informazioni cui può avere accesso sono sufficienti ai fini della valutazione del SGSI; se non lo fossero, l'organizzazione ed Certifica srl devono raggiungere – ove possibile – un accordo sulle modalità di accesso a tutte le informazioni indispensabili per la valutazione del SGSI; se l'accordo non può essere raggiunto, l'iter di certificazione non viene iniziato. Detto accordo può consistere nel fatto che l'organizzazione autorizzi il team di audit ad accedere ad informazioni, riservate o sensibili, solo per il tempo dell'audit e in base a modalità concordate.
In caso di sistemi di gestione multipli (riferiti cioè a più di una norma certificabile), l'audit può essere eseguito e condurre al rilascio della certificazione, purché tutti i requisiti della norma di riferimento per gli SGSI siano stati soddisfatti, ed inoltre tutte le informazioni documentate siano disponibili, conformi ai requisiti citati, e siano identificate le interfacce con gli altri sistemi di gestione.

7.2 Diritti dell'Organizzazione

Nessuna integrazione rispetto a Regolamento Generale per la Certificazione di Sistemi di Gestione Aziendale RdC in revisione corrente.

7.3 Doveri di Certifica S.r.l.

Nessuna integrazione rispetto a Regolamento Generale per la Certificazione di Sistemi di Gestione Aziendale RdC in revisione corrente.

7.4 Diritti di Certifica S.r.l.

Nessuna integrazione rispetto a Regolamento Generale per la Certificazione di Sistemi di Gestione Aziendale RdC in revisione corrente.

Certifica S.r.l.
Organismo di Certificazione
Via Petrarca, 15 – 80070 Bacoli
p.i. 08654031213 – tel. e fax 081 5237021
info@certificasistemi.com

8 PROCEDURA DI CERTIFICAZIONE

8.1 Domanda di Certificazione

L'Organizzazione interessata alla Certificazione riceve dall'Organismo il "Questionario Informativo" F01-01. Il Documento è altresì disponibile sul sito internet dell'Istituto (www.certificasistemi.com), pertanto il cliente può inviare il Questionario anche autonomamente.
Sulla base di tutte le informazioni, Certifica S.r.l.formula ed invia una offerta economica personalizzata redatta sulla base del tariffario in vigore. Tale documento identifica il settore IAF di appartenenza dell'Organizzazione e definisce il campo di applicazione (scopo) della Certificazione.
A seguito del Riesame della domanda, l'Organismo può decidere di accettare o respingere la Domanda di certificazione. Nel caso che la richiesta venga respinta, l'Organizzazione viene informata delle motivazioni.

Per la norma UNI CEI EN ISO/IEC 27001: La durata dell'audit, sia che coinvolga un sito singolo, che più siti rientranti nel campo di applicazione del SGSI, sarà determinata da Certifica srl in base alle prescrizioni della norma di accreditamento ISO/IEC 27006 in edizione vigente.
Per audit multisito e audit integrati si fa riferimento rispettivamente ai documenti IAF MD 1 e IAF MD 11.
In caso di audit i cui criteri sono estesi a linee guida incluse nello scopo di accreditamento flessibile (es.: ISO/IEC 27017 e/o ISO /IEC 27018), la durata dell'audit sarà determinata anche in base alle ~~Disposizioni Accredia pertinenti~~. **Circolari di accredia**:

- **Circolare Informativa N° 01/2019 Accreditamento schema di certificazione ISO/IEC 27001:2013 con integrazione delle linee guida ISO/IEC 27017:2015 e ISO/IEC 27018:2014 - Information Technology, Security techniques, Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors**
- **Circolare DC N° 13/2017 – Informativa in merito all'accreditamento per lo schema di certificazione ISO/IEC 27001:2013 con integrazione della linea guida ISO/IEC 27018:2014**
- **Programma di audit con relativi controlli**

Nel caso di Organizzazioni Multisito, Certifica S.r.l.valuta l'applicabilità del IAF MD1 MandatoryDocument for the Certification of Multiple SitesBased on Sampling, identificando con la collaborazione dell'Organizzazione, e prima dell'emissione dell'Offerta, la complessità e la scala delle attività oggetto di certificazione e le differenze tra i vari siti per determinare il livello di campionamento.
Le sedi operative diverse dalla sede principale sono campionate e/o scelte conformemente alle prescrizioni IAF (MD1). Certifica S.r.l. sviluppa un programma di campionamento atto a garantire un audit adeguato del sistema di gestione. La motivazione del piano di campionamento viene consegnata ai clienti.

Per le aziende multi sito il numero di giornate di audit on site totali calcolato in base allo scopo come definito all'interno dell'istruzione operativa denominata "IO 01 Determinazione del tempo di audit "sarà distribuito tra i diversi siti in base alla rilevanza del sito per il sistema di gestione e ai rischi individuati.

La giustificazione della distribuzione è registrata all'interno della documentazione di audit.

Il tempo totale impiegato per l'audit e la sorveglianza iniziali è la somma totale del tempo trascorso in ciascun sito più l'ufficio centrale e non deve mai essere inferiore a quello che sarebbe stato calcolato per l'entità e la complessità dell'operazione se tutto il lavoro fosse stato svolto in un unico sito (cioè, con tutti i dipendenti dell'azienda nello stesso sito).

Certifica S.r.l.
Organismo di Certificazione
Via Petrarca, 15 – 80070 Bacoli
p.i. 08654031213 – tel. e fax 081 5237021
info@certificasistemi.com

8.2 Restituzione dell'offerta e conferma d'ordine

Nessuna integrazione rispetto a Regolamento Generale per la Certificazione di Sistemi di Gestione Aziendale RdC in revisione corrente.

8.3 Modifiche al contratto

Nessuna integrazione rispetto a Regolamento Generale per la Certificazione di Sistemi di Gestione Aziendale RdC in revisione corrente.

8.4 Audit Preliminare

Nessuna integrazione rispetto a Regolamento Generale per la Certificazione di Sistemi di Gestione Aziendale RdC in revisione corrente.

8.5 Pianificazione della VI

Nessuna integrazione rispetto a Regolamento Generale per la Certificazione di Sistemi di Gestione Aziendale RdC in revisione corrente.

8.6 Audit iniziale di certificazione

Per la UNI CEI EN ISO/IEC 27001 l'audit di 1° stadio sarà eseguito interamente presso l'Organizzazione.
a) Verifica della documentazione del SGSI (1° fase del 1° stadio)
La verifica della documentazione del SGSI viene eseguita sempre, con le eventuali limitazioni dovute ai motivi di riservatezza di cui al paragrafo 7.1.5
Per documentazione del SGSI si intende quanto segue:
• i documenti specificati dalla Norma col termine "informazione documentata" (o "documented information")
• l'elenco dei requisiti cogenti applicabili nell'ambito del SGSI
Tra i documenti specificati nella norma vi sono, in particolare, i documenti relativi alla valutazione ed al trattamento dei rischi, la Dichiarazione di Applicabilità, le policy e le procedure per la sicurezza delle informazioni.
Si sottolinea inoltre che nei suddetti documenti deve essere chiaramente riportato il campo di applicazione del SGSI, nonché il suo "perimetro" fisico (sedi dell'organizzazione incluse nel SGSI) e logico (sistemi e utenze coperte dal SGSI pur se fisicamente non nelle sedi). Eventuali interfacce / interazioni con servizi o attività non completamente inclusi nel campo di applicazione devono essere individuate e comprese nella valutazione dei rischi (per esempio questo potrebbe essere il caso di computer o sistemi di telecomunicazioni condivisi con altre organizzazioni).
L'esame della documentazione è volto ad accertare che essa sia innanzitutto completa, ossia soddisfi tutti i requisiti della Norma e del presente regolamento; inoltre la documentazione deve essere chiara, ossia non deve lasciare adito a dubbi interpretativi, deve essere congruente tra le sue varie parti e deve essere facilmente leggibile

I risultati della fase 1 sono documentati all'interno del documento denominato "F05-07 Rapporto AUDIT SSI STAGE 1".
Una volta eseguito l'audit di fase 1 il Lead auditor provvede alla compilazione del rapporto di stage 1 il quale viene consegnato all'azienda Cliente ed inviato a Certifica, la quale esamina il rapporto e decide se procedere con l'audit di fase 2 o meno. Certifica provvederà inoltre a confermare e/o modificare il gruppo di audit per procedere all'audit di fase 2 in base alle competenze necessarie
; ciò può essere fatto anche dal Lead Auditor, sotto mandato di Certifica, che ha condotto l'audit di fase 1 se ritenuto competente e appropriato.
Il riesame della documentazione di fase 1 è eseguito da una figura indipendente, ovvero non coinvolto nell'iter di certificazione. Chi verifica e delibera la documentazione di stage 1 non esegue la verifica e la delibera della documentazione di stage 2.

b) Visita iniziale (2° fase del 1° stadio)
La visita iniziale viene eseguita sempre e consiste in una verifica in campo presso il sito (o i siti) dell'organizzazione.
Essa consente innanzitutto a Certifica srl di meglio comprendere:
- la dimensione e le caratteristiche del SGSI dell'organizzazione;
- il suo grado di idoneità ad affrontare l'iter di certificazione;
- l'applicabilità di norme e requisiti legislativi relativi alla sicurezza delle informazioni;
- il tipo di esperienza richiesta al team incaricato dell'audit di 2° stadio;
- l'entità delle risorse necessarie per svolgere l'audit di 2° stadio.
Inoltre la visita iniziale consente all'organizzazione di approfondire i seguenti aspetti:
- dettagli dell'iter di certificazione;
- programmazione più precisa dei tempi necessari per giungere alla certificazione;
- definizione esatta del campo di applicazione del SGSI;

Certifica S.r.l.
Organismo di Certificazione
Via Petrarca, 15 – 80070 Bacoli
p.i. 08654031213 – tel. e fax 081 5237021
info@certificasistemi.com

- identificazione di eventuali carenze nella attuazione del SGSI.
Per conseguire le suddette finalità, durante la visita iniziale il team di audit valuta il grado di soddisfacimento dei seguenti punti fondamentali della Norma:
• requisiti delle sezioni da 4 a 10;
• Obiettivi di controllo e controlli di riferimento ai paragrafi A1-A18.
Per ciascuno di tali requisiti, il SGSI deve risultare attuato e devono essere disponibili le corrispondenti registrazioni.
L'esito dell'esame della documentazione è riportato, assieme ai risultati della visita iniziale, in un apposito rapporto, emesso a conclusione dell'audit di 1° stadio. Copia del rapporto viene consegnata anche all'organizzazione; se necessario, esso può essere illustrato al cliente in occasione di un incontro diretto col cliente stesso. Qualora l'attuazione del SGSI risulti carente, il cliente ne viene informato tramite il suddetto rapporto.
Nel caso l'esame della documentazione in Fase 1 abbia evidenziato rilievi queste dovranno essere corrette dall'organizzazione prima dell'audit 2° stadio in quanto l'eventuale permanere di rilievi della documentazione al momento dell'audit 2° stadio sono ostative all'emissione del certificato e renderà necessaria l'effettuazione di un post-audit.

Certifica srl effettuerà un riesame del rapporto di 1° stadio per decidere se ci sono le condizioni per procedere con l'audit di 2° stadio, e per verificare la necessità di competenze particolari per il team di audit di 2° stadio.
Inoltre, qualora emergano scostamenti rispetto a quanto comunicato dall'organizzazione in sede di formulazione offerta, Certifica srl si riserva di valutare la necessità di modificare la propria offerta economica.

Al momento dell'audit di 2° stadio l'ISMS dell'organizzazione deve risultare già operativo; in particolare l'organizzazione deve aver definito obiettivi per la sicurezza delle informazioni misurabili e – ove applicabile - quantificati, deve aver eseguito almeno un riesame della direzione documentato ed un ciclo completo di audit interni secondo i requisiti della sezione 9 della Norma.
L'audit viene effettuato sulla base di un piano di audit concepito in modo da tenere conto dell'esito delle attività già svolte (audit di 1° stadio), dando rilevanza agli elementi del SGSI risultati più significativi (valutazione dei rischi per la sicurezza delle informazioni e relativa consistenza dei risultati, selezione degli obiettivi di controllo e dei controlli basati sui risultati di valutazione dei rischi, riesame dell'efficacia del sistema SGSI e misura dell'efficacia dei controlli, implementazione dei controlli, etc.); pertanto il piano comprende, in linea di principio, tutti i requisiti della norma di riferimento, ma può anche non includere quei requisiti che sono risultati attuati in modo completamente soddisfacente nel corso dell'audit di 1°stadio.
Tale piano viene anticipato all'organizzazione prima dell'audit
L'audit per la certificazione ha lo scopo di accertare che il SGSI sia messo in pratica in accordo alla relativa documentazione (policy, procedure, istruzioni, SoA, requisiti di legge, eventuali altri requisiti cogenti, programmi, ecc.) e in maniera efficace, e soddisfi quindi i requisiti della norma di riferimento.
Inoltre il team di audit ha l'obiettivo di verificare che:
• il top management eserciti la leadership con impegno ed efficacia;
• le esigenze derivanti dalle parti interessate – tra cui gli obblighi normativi - siano adeguatamente tenute in considerazione ed ispirino gli obiettivi per l'information security;
• l'analisi effettuata sui rischi per la sicurezza sia adeguata ai processi dell'organizzazione;
• l'organizzazione abbia stabilito adeguate procedure per l'identificazione, l'esame e la valutazione dei rischi per la sicurezza delle informazioni, e che l'applicazione dei controlli operativi sia coerente con la politica, gli obiettivi ed i target definiti dall'organizzazione stessa;
• la documentazione sia conforme alla norma;
• le misurazioni di efficacia dei controlli siano consistenti.
L'audit è anche volto ad accertare che le interfacce con servizi o attività interamente o parzialmente esterne al campo di applicazione del SGSI siano state considerate e quindi incluse nella valutazione del rischio per la sicurezza delle informazioni.
In caso di certificazione estesa a ISO/IEC 27017 e ISO/IEC 27108, questa può essere rilasciata solo dopo una verifica eseguita presso il sito/i siti interessati dell'organizzazione, e in particolare devono essere verificati tutti i data center presso cui sono dislocati i server che gestiscono il cloud.
Se i Data Center utilizzati per le attività "cloud" sono in outsourcing presso fornitori in possesso di certificazioni ISO/IEC 27001, ISO/IEC 27017 e ISO/IEC 27018 accreditate e riconosciute a livello MLA, si potrà evitare di aggiungere tempo di audit presso tali siti. In tutti gli altri casi, dovrà essere aggiunto tempo per la verifica in campo dei siti in outsourcing. Nel caso di siti ove non fosse possibile svolgere un audit diretto (es. fornitori come AWS, AZURE), dovrà essere utilizzato del tempo aggiuntivo presso il sito centrale per la valutazione degli aspetti contrattuali e di controllo operativo con tali fornitori. Questo ultimo requisito è applicabile solamente nel caso di Data Center in possesso di certificazioni TIER III o TIER IV.

8.7 ESCLUSIONI

La Norma UNI CEI 27001 riporta nelle sezioni da 4 a 10 una serie di requisiti obbligatori per gli SGSI, che non possono essere cioè oggetto di esclusione.
Nell'Appendice A (normativa)" (dedicata ai controlli ed ai relativi obiettivi di controllo, denominata "Annex A" nella versione originale della norma) essa riporta l'elenco dei possibili controlli da impiegare nell'ambito dello specifico SGSI, in funzione dei risultati dei processi di valutazione e di trattamento dei rischi. I controlli descritti nell'"Appendice A", vanno selezionati dall'organizzazione responsabile del SGSI utilizzando criteri documentati che tengano presente le proprie reali esigenze; quindi i controlli ritenuti realmente necessari e dunque "obbligatori" nell'ambito dello specifico SGSI vengono identificati a cura

Certifica S.r.l.
Organismo di Certificazione
Via Petrarca, 15 – 80070 Bacoli
p.i. 08654031213 – tel. e fax 081 5237021
info@certificasistemi.com

dell'organizzazione nel SoA, dove devono essere riportate e giustificate eventuali esclusioni. Sarà cura dell'auditor confrontate ciascun controllo dell'Allegato A con quanto riportato nel SoA, ed eventualmente ritenere accettabile l'esclusione da parte dell'organlzzazione.

L'elenco dei possibili controlli richiamati nell' "Appendice A (normativa)" da impiegare nell'ambito dello specifico SGSI, in funzione dei risultati dei processi di valutazione e di trattamento dei rischi non sono tutti obbligatori per tutti i SGSI, ma vanno selezionati dall'organizzazione responsabile del SGSI utilizzando criteri documentati che tengano presente le proprie reali esigenze; quindi i controlli ritenuti realmente necessari e dunque "obbligatori" nell'ambito dello specifico SGSI vengono identificati a cura dell'organizzazione nella Dichiarazione di Applicabilità (SoA – Statement of Applicability), dove devono essere riportate giustificale eventuali esclusioni.

Da quanto sopra deriva che Certifica srl, quale organismo di certificazione degli SGSI, ha il compito di valutare la documentazione ed attuazione di tutti i requisiti delle sezioni da 4 a 10 (comprese), nonché dei controlli dell'"Appendice A" che l'organizzazione ha dichiarato applicabili nel SoA; Certifica srl si riserva la facoltà di giudicare l'adeguatezza delle scelte operate dall'organizzazione
Nell'esecuzione delle proprie verifiche Certifica srl esamina inoltre l'esistenza e la congruenza dei collegamenti tra i diversi elementi del SGSI quali: la politica, i risultati della valutazione dei rischi, gli obiettivi generali e di dettaglio, le strategie di trattamento dei rischi, le responsabilità, i programmi, le procedure, i riesami interni sulla sicurezza, ecc.
Per quanto concerne il rispetto dei requisiti cogenti (per disposizione di leggi, regolamenti, direttive, ecc.), il principio generale è che il mantenimento e la valutazione della conformità ai suddetti requisiti cogenti ricadono sotto la responsabilità dell'organizzazione che gestisce l'ISMS,Certifica srl si limita ad eseguire verifiche a campione per acquisire fiducia che l'ISMS sia efficace sotto questo punto di vista e che – nell'eventualità di non conformità rispetto ai requisiti cogenti – l'organizzazione metta in atto idonee azioni correttive.
Può accadere che l'organizzazione gestisca reti di informazioni che ricadono sotto il controllo di un unico SGSI ma che siano ramificate in luoghi geografici diversi, ossia in più siti; in tale situazione Certifica srl può emettere un unico certificato, ma si riserva la decisione di verificare ogni singolo sito o campionarne alcuni e verificare solo questi (Certifica srl prende tale decisione sulla base delle apposite prescrizioni e raccomandazioni degli standard ISO/IEC 27006 e ISO/IEC 17021-1 in edizione vigente, nonché dei Regolamenti emessi da ACCREDIA).
La certificazione secondo ISO/IEC 27001 può essere integrata dalle linee guida ISO/IEC 27017 e ISO/IEC 27018 su richiesta dell'Organizzazione, nel caso in cui il campo d'applicazione del sistema di gestione preveda l'erogazione di servizi in modalità "cloud", e se vengono trattati dati personali in detta modalità. Si precisa che l'integrazione può riguardare la sola linea guida ISO/IEC 27017 o l'abbinamento con la ISO/IEC 27018, ma non la sola ISO/IEC 27018. In particolare, tale integrazione può essere eseguita sia in caso di nuova certificazione, sia in presenza di una certificazione ISO/IEC 27001 già in vigore, purché emessa da Certifica srl (in caso contrario, è richiesto il preventivo trasferimento della stessa a Certifica srl).

Certifica S.r.l.
Organismo di Certificazione
Via Petrarca, 15 – 80070 Bacoli
p.i. 08654031213 – tel. e fax 081 5237021
info@certificasistemi.com

9 RILASCIO DEL CERTIFICATO DI CONFORMITÀ

9.1 Funzione Tecnica di Delibera (Comitato di Delibera)

Vale quanto descritto nel Regolamento Generale per la Certificazione di Sistemi di Gestione Aziendale RdC in revisione corrente inoltre In caso di certificazione estesa a ISO/IEC 27017 e ISO/IEC 27108, Il certificato riporterà il riferimento alla Dichiarazione di Applicabilità (SoA) con la relativa data, edizione e/o revisione.

Il certificato dovrà essere riemesso anche in fase di sorveglianza, riportando i nuovi riferimenti al SoA, qualora da quest'ultimo documento emerga che è cambiata la copertura dei controlli di cui all'Appendice A della norma.

9.2 Funzione dell'Imparzialità, di Indirizzo e Supervisione delle Attività di Certificazione

Nessuna integrazione rispetto a Regolamento Generale per la Certificazione di Sistemi di Gestione Aziendale RdC in revisione corrente.

9.3 Iscrizione dell'Azienda nell'Elenco delle Organizzazioni Certificate da Certifica S.r.l.

Nessuna integrazione rispetto a Regolamento Generale per la Certificazione di Sistemi di Gestione Aziendale RdC in revisione corrente.

Certifica S.r.l.
Organismo di Certificazione
Via Petrarca, 15 – 80070 Bacoli
p.i. 08654031213 – tel. e fax 081 5237021
info@certificasistemi.com

10 ATTIVITÀ DI SORVEGLIANZA (STANDARD E SUPPLEMENTARE)

10.1Audit di Sorveglianza

Vale quanto descritto nel Regolamento Generale per la Certificazione di Sistemi di Gestione Aziendale RdC in revisione corrente inoltre per la UNI CEI ISO /IEC 27001 ognuno degli audit di sorveglianza è relativo a parti del SGSI: esso comprende sempre, in linea di principio, alcuni elementi fissi del SGSI secondo la Norma (le sezioni da 4 a 10 e Annex A) più ulteriori elementi; tuttavia, nel caso degli eventuali audit di sorveglianza "aggiuntivi", gli elementi fissi citati possono non essere oggetto di verifica a giudizio del team di audit; comunque complessivamente gli audit di sorveglianza del triennio coprono almeno una volta l'intero SGSI.
Al momento di tale audit l'ISMS dell'organizzazione deve dare evidenza dell'esecuzione del riesame della direzione e di un ciclo di audit interni secondo i requisiti della sezione 9 della Norma con una frequenza almeno annuale.
Inoltre come minimo, oltre a quanto stabilito nel RGSG, l'audit di sorveglianza ha l'obiettivo di riesaminare:
• l'efficacia del SGSI con riferimento al raggiungimento degli obiettivi stabiliti nella politica per la sicurezza delle informazioni;
• il funzionamento delle procedure per la valutazione periodica della conformità legislativa e normativa;
• le azioni intraprese a fronte di situazioni non conformi rilevate nel precedente audit;
•eventuali cambiamenti nella copertura dei controlli di cui all'Appendice A della norma, e le conseguenti modifiche alla Dichiarazione di Applicabilità;
• l'implementazione e l'efficacia dei controlli secondo il programma di audit;
• la gestione di reclami proposti dalle parti interessate all'attenzione di Certifica srl;
• il programma di audit in funzione delle modifiche intervenute (inclusi elementi di contesto, rischi, aspetti legislativi, richieste o segnalazioni dalle parti interessate);
• l'uso appropriato del certificato.

10.2 Mantenimento della certificazione

Nessuna integrazione rispetto a Regolamento Generale per la Certificazione di Sistemi di Gestione Aziendale RdC in revisione corrente

10.3 Verifiche ispettive supplementari

Nessuna integrazione rispetto a Regolamento Generale per la Certificazione di Sistemi di Gestione Aziendale RdC in revisione corrente

Certifica S.r.l.
Organismo di Certificazione
Via Petrarca, 15 – 80070 Bacoli
p.i. 08654031213 – tel. e fax 081 5237021
info@certificasistemi.com

11 RINNOVO DELLA CERTIFICAZIONE

11.1 Pianificazione dell'Audit Rinnovo della Certificazione

Nessuna integrazione rispetto a Regolamento Generale per la Certificazione di Sistemi di Gestione Aziendale RdC in revisione corrente

11.2 Audit di Rinnovo

Vale quanto descritto nel Regolamento Generale per la Certificazione di Sistemi di Gestione Aziendale RdC in revisione corrente inoltre
Per Audit di rinnovo secondo la UNI CEI ISO /IEC 27001
Al momento di tale audit l'ISMS dell'organizzazione deve dare evidenza dell'esecuzione del riesame della direzione e di un ciclo di audit interni secondo i requisiti della sezione 9 della Norma

11.3 Informazioni per il Rilascio del Rinnovo della Certificazione

Nessuna integrazione rispetto a Regolamento Generale per la Certificazione di Sistemi di Gestione Aziendale RdC in revisione corrente.

Certifica S.r.l.
Organismo di Certificazione
Via Petrarca, 15 – 80070 Bacoli
p.i. 08654031213 – tel. e fax 081 5237021
info@certificasistemi.com

12 AUDIT SPECIALI

12.1 Estensione del campo di applicazione

Nessuna integrazione rispetto a Regolamento Generale per la Certificazione di Sistemi di Gestione Aziendale RdC in revisione corrente.

12.2 Audit con breve preavviso

Nessuna integrazione rispetto a Regolamento Generale per la Certificazione di Sistemi di Gestione Aziendale RdC in revisione corrente.

13 SOSPENSIONE, REVOCA O RIDUZIONE DELLO SCOPO DI CERTIFICAZIONE

13.1 Sospensione della Certificazione

Nessuna integrazione rispetto a Regolamento Generale per la Certificazione di Sistemi di Gestione Aziendale RdC in revisione corrente.

13.2 Revoca

Nessuna integrazione rispetto a Regolamento Generale per la Certificazione di Sistemi di Gestione Aziendale RdC in revisione corrente.

13.3 Riduzione

Nessuna integrazione rispetto a Regolamento Generale per la Certificazione di Sistemi di Gestione Aziendale RdC in revisione corrente.

13.4 Rinuncia della certificazione

Nessuna integrazione rispetto a Regolamento Generale per la Certificazione di Sistemi di Gestione Aziendale RdC in revisione corrente.

Certifica S.r.l.
Organismo di Certificazione
Via Petrarca, 15 – 80070 Bacoli
p.i. 08654031213 – tel. e fax 081 5237021
info@certificasistemi.com

14 MODIFICHE ALLA CERTIFICAZIONE

14.1 Notifica di Modifiche alle Norme per la Certificazione dei Sistemi di Gestione da Parte di Certifica S.r.l.

Nessuna integrazione rispetto a Regolamento Generale per la Certificazione di Sistemi di Gestione Aziendale RdC in revisione corrente.

14.2 Notifica di Modifiche al Regolamento da Parte di Certifica S.r.l.

Nessuna integrazione rispetto a Regolamento Generale per la Certificazione di Sistemi di Gestione Aziendale RdC in revisione corrente.

14.3 Notifica di Modifiche Apportate dall'Organizzazione Certificata

Nessuna integrazione rispetto a Regolamento Generale per la Certificazione di Sistemi di Gestione Aziendale RdC in revisione corrente.

15 TRASFERIMENTO DELLE CERTIFICAZIONI

Nessuna integrazione rispetto a Regolamento Generale per la Certificazione di Sistemi di Gestione Aziendale RdC in revisione corrente.

16 TARIFFE E CONDIZIONI DI PAGAMENTO

16.1 Tariffe

Nessuna integrazione rispetto a Regolamento Generale per la Certificazione di Sistemi di Gestione Aziendale RdC in revisione corrente.

16.2 Condizioni di pagamento

Nessuna integrazione rispetto a Regolamento Generale per la Certificazione di Sistemi di Gestione Aziendale RdC in revisione corrente.

17 USO DEL MARCHIO E DEL CERTIFICATO

Nessuna integrazione rispetto a Regolamento Generale per la Certificazione di Sistemi di Gestione Aziendale RdC in revisione corrente.

Certifica S.r.l.
Organismo di Certificazione
Via Petrarca, 15 – 80070 Bacoli
p.i. 08654031213 – tel. e fax 081 5237021
info@certificasistemi.com

18 RISERVATEZZA

Nessuna integrazione rispetto a Regolamento Generale per la Certificazione di Sistemi di Gestione Aziendale RdC in revisione corrente.

19 RICORSI, RECLAMI E CONTENZIOSI

19.1 Ricorsi

Nessuna integrazione rispetto a Regolamento Generale per la Certificazione di Sistemi di Gestione Aziendale RdC in revisione corrente.

19.2 Reclami e segnalazioni

Nessuna integrazione rispetto a Regolamento Generale per la Certificazione di Sistemi di Gestione Aziendale RdC in revisione corrente.

19.3 Contenziosi

Nessuna integrazione rispetto a Regolamento Generale per la Certificazione di Sistemi di Gestione Aziendale RdC in revisione corrente.

Relativamente ai contenziosi, la notifica è registrata nella pratica di certificazione dell'Organizzazione e copia della stessa è inviata al Comitato per la Salvaguardia dell'Imparzialità.
Per tutte le altre controversie che dovessero insorgere tra Certifica S.r.l.e soggetti differenti dalle Organizzazioni licenziatarie, è competente in via esclusiva il Foro di Napoli.

20 GESTIONE DI CASI PARTICOLARI

Nessuna integrazione rispetto a Regolamento Generale per la Certificazione di Sistemi di Gestione Aziendale RdC in revisione corrente.

20.1 Cessione di Ramo d'Azienda

Nessuna integrazione rispetto a Regolamento Generale per la Certificazione di Sistemi di Gestione Aziendale RdC in revisione corrente.

20.2 Conferimento in Toto d'Azienda

Nessuna integrazione rispetto a Regolamento Generale per la Certificazione di Sistemi di Gestione Aziendale RdC in revisione corrente.

20.3 Variazioni di scarsa rilevanza sulla certificazione

20.3.1 Cambio di denominazione sociale

Nessuna integrazione rispetto a Regolamento Generale per la Certificazione di Sistemi di Gestione Aziendale RdC in revisione corrente.

Trasformazione

Certifica S.r.l.
Organismo di Certificazione
Via Petrarca, 15 – 80070 Bacoli
p.i. 08654031213 – tel. e fax 081 5237021
info@certificasistemi.com

Nessuna integrazione rispetto a Regolamento Generale per la Certificazione di Sistemi di Gestione Aziendale RdC in revisione corrente.

20.3.2 Cambio di Sede

Nessuna integrazione rispetto a Regolamento Generale per la Certificazione di Sistemi di Gestione Aziendale RdC in revisione corrente.

Cambio di Sede Legale

Nessuna integrazione rispetto a Regolamento Generale per la Certificazione di Sistemi di Gestione Aziendale RdC in revisione corrente.

Cambio di Sede Operativa

Nessuna integrazione rispetto a Regolamento Generale per la Certificazione di Sistemi di Gestione Aziendale RdC in revisione corrente.

Certifica S.r.l.
Organismo di Certificazione
Via Petrarca, 15 – 80070 Bacoli
p.i. 08654031213 – tel. e fax 081 5237021
info@certificasistemi.com