REGOLAMENTO PARTICOLARE PER LA CERTIFICAZIONE DEI SISTEMI DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI

REGOLAMENTO PARTICOLARE PER LA CERTIFICAZIONE DEI SISTEMI DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI

ED.	REV.	DATA	MOTIVAZIONI DELLE MODIFICHE ALLA PRECEDENTE REVISIONE	REDATTO RSQ		VERIFICATO DO		APPROVATO DG
				Roma	Brescia	Roma	Brescia	
4	00	29/06/18	Unificazione Sistemi Gestione SICIV-APAVE CERTIFICATION ITALIA	S. Bertini	F. Donati	D. Venditti	S. Citroni	Urbano Strada

Indice

1. PRESENTAZIONE APAVE CERTIFICATION ITALIA

Nessuna integrazione rispetto a RG -01 parte generale in revisione corrente.

2. ACCREDITAMENTI APAVE CERTIFICATION ITALIA

Nessuna integrazione rispetto a RG -01 parte generale in revisione corrente.

3. SCOPO E CAMPO DI APPLICAZIONE DEL REGOLAMENTO

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.

Per tutti gli argomenti non esplicitamente citati o descritti in questo Regolamento Particolare, vale quanto descritto nel Regolamento di Certificazione Apave Certification Italia S.r.l.. In caso di disposizioni non omogenee prevale il presente regolamento e in caso di ulteriori dubbi si fa riferimento allo Standard di riferimento ISO/IEC 27001:2013 per le organizzazioni e ISO/IEC 27006:2015 per Apave Certification Italia S.r.l..

Nel presente Regolamento vengono definiti i rapporti tra APAVE CERTIFICATION ITALIA S.R.L. 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 27001:2013.

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 disponibile sul sito www.apave-certification.it o richiedibile a:

APAVE CERTIFICATION ITALIA SRL – SEDE OPERATIVA ROMA

viale Battista Bardanzellu, 94 – Roma – 00155 (RM) – ITALIA - tel. 06/33270123 - fax 06/3320293

e-mail: info.certification.it@apave.com - sito internet www.apave-certification.it

posta elettronica certificata (PEC): info@pec.apave-certification.it

4. TERMINI, DEFINIZIONI, ABBREVIAZIONI

Valgono termini, definizioni e abbreviazioni riportate in RG-01 parte generale in revisione corrente.

5. RESPONSABILITÀ

Nessuna integrazione rispetto a RG -01 parte generale in revisione corrente.

5.1 DIRITTI E DOVERI DI APAVE CERTIFICATION ITALIA-SEDE DI ROMA

Nessuna integrazione rispetto a RG -01 parte generale in revisione corrente.

5.1.1 RISERVATEZZA

Nessuna integrazione rispetto a RG -01 parte generale in revisione corrente.

5.1.2 MODIFICHE AL REGOLAMENTO

Nessuna integrazione rispetto a RG -01 parte generale in revisione corrente.

5.2 DIRITTI E DOVERI DELL'ORGANIZZAZIONE

Nessuna integrazione rispetto a RG -01 parte generale in revisione corrente

5.2.1 ASPETTI GENERALI DEL RAPPORTO ORGANIZZAZIONE/APAVE CERTIFICATION ITALIA-SEDE DI ROMA

Nessuna integrazione rispetto a RG -01 parte generale in revisione corrente.

5.2.2 USO DEL MARCHIO, DEL LOGO E DEL CERTIFICATO

Nessuna integrazione rispetto a RG -01 parte generale in revisione corrente.

5.2.3 MODIFICHE AL SGA DELL'ORGANIZZAZIONE

Nessuna integrazione rispetto a RG -01 parte generale in revisione corrente.

5.2.4 ACCESSO ALLE REGISTRAZIONI DEI RECLAMI

Oltre a quanto prescritto nel corrispondente paragrafo del RG-01 parte generale, APAVE CERTIFICATION ITALIA - SEDE OPERATIVA ROMA richiede all'organizzazione di rendere disponibile a APAVE CERTIFICATION ITALIA - SEDE OPERATIVA ROMA un elenco aggiornato degli eventuali reclami ricevuti relativi agli impatti di natura ambientale quali, a titolo di esempio: sanzioni, procedimenti penali in corso, esposti, azioni volte al risarcimento per danni ambientali, altro.

Qualora una organizzazione richiedente certificazione sia coinvolta in procedimenti legali in corso o con sentenza passata in giudicato, APAVE CERTIFICATION ITALIA - SEDE OPERATIVA ROMA effettua adeguata e sistematica sorveglianza del problema specifico sia durante audit di certificazione (Fase1 e Fase2), sia in audit di mantenimento e rinnovo. Il GA APAVE CERTIFICATION ITALIA - SEDE OPERATIVA ROMA deve raccogliere evidenze oggettive significative, necessarie a dimostrare che per l'oggetto della condanna o del procedimento, non è ancora in essere la violazione contestato al momento dell'audit. APAVE CERTIFICATION ITALIA - SEDE OPERATIVA ROMA si riserva il diritto di effettuare Audit Supplementari o anticipare a 6 mesi l'audit di primo mantenimento sull'organizzazione.

L'organizzazione si impegna a tenere aggiornato APAVE CERTIFICATION ITALIA - SEDE OPERATIVA ROMA di tutti gli sviluppi dei procedimenti in essere.

APAVE CERTIFICATION ITALIA - SEDE OPERATIVA ROMA precisa che l'esistenza di procedimenti penali in corso è collegata ad una ipotesi di reato ma non dimostra la colpevolezza del rappresentante legale dell'organizzazione (o di altra persona fisica operante per conto dell'organizzazione) fino a sentenza definitiva passata in giudicato e che l'eventuale condanna (reclusione, ammenda, altro) prevista della legislazione vigente porta alla espiazione della pena.

Nel caso in cui aree, attività, impianti compresi nello scopo del certificato rilasciato da APAVE CERTIFICATION ITALIA - SEDE OPERATIVA ROMA siano oggetto di sequestro, APAVE CERTIFICATION ITALIA - SEDE OPERATIVA ROMA valuta se il sequestro renda impossibile verificare che il sistema di gestione continui ad essere conforme ed efficacemente attuato e, in caso negativo, sospende il certificato, dopo avere effettuato un Audit Supplementare.

5.2.5 PRESENZA PRESSO L'ORGANIZZAZIONE DI ISPETTORI ED OSSERVATORI

Nessuna integrazione rispetto a RG -01 parte generale in revisione corrente.

5.2.6 COMUNICAZIONI

Qualora l'organizzazione venisse ad essere interessata da provvedimenti sanzionatori, sospensione di autorizzazioni o altro che abbia impatto diretto sul sistema di gestione di sicurezza delle informazioni, queste devono essere tempestivamente comunicate a APAVE CERTIFICATION ITALIA - SEDE OPERATIVA ROMA via mai/pec/fax/raccomandata, che tramite il RSSSI potrà decidere di programmare un audit straordinario e/o anticipare audit di mantenimento e/o altro.

6. Condizioni relative al possesso delle autorizzazioni

APAVE CERTIFICATION ITALIA - SEDE OPERATIVA ROMA verifica che l'organizzazione abbia stabilito un'efficace procedura per identificare ed avere accesso ai requisiti di legge relativi alla sicurezza delle informazioni pertinenti allo scopo del SGSI, tra cui quelli legati al trattamento dei dati personali e a quelli specifici del settore in cui opera l'Organizzazione. Il

mantenimento e la valutazione della conformità ai requisiti cogenti ricadono sotto la responsabilità dell'organizzazione che gestisce il SGSI e che rilascia apposita attestazione, APAVE CERTIFICATION ITALIA - SEDE OPERATIVA ROMA si limita ad eseguire le verifiche a campione per acquisire la fiducia che il SGSI 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.

Particolari situazioni di eccezionalità che possano far proseguire nell'iter di certificazione nonostante quanto appena precisato, saranno valutate da APAVE CERTIFICATION ITALIA - SEDE OPERATIVA ROMA e trattate secondo quanto definito dalle prescrizioni integrative per l'accreditamento delle certificazioni di sistemi di gestione della sicurezza definite dall'Ente di Accreditamento.

L'organizzazione rimane comunque pienamente responsabile dal punto di vista penale ed amministrativo dell'eventuale scelta di operare in assenza delle necessarie autorizzazioni.

7. Attività di valutazione

A seguito dell'accettazione dell'offerta APAVE CERTIFICATION ITALIA - SEDE OPERATIVA ROMA concorda con l'Organizzazione il periodo di effettuazione dell'audit.

L'accettazione del contratto non presuppone né indirettamente né direttamente l'obbligo di rilascio della certificazione da parte di APAVE CERTIFICATION ITALIA - SEDE OPERATIVA ROMA.

Prima dell'audit l'Organizzazione deve comunicare a APAVE CERTIFICATION ITALIA - SEDE OPERATIVA ROMA o al valutatore incaricato della verifica, se ritiene che uno o più documenti del SGSI non possano essere resi disponibili per la verifica. APAVE CERTIFICATION ITALIA - SEDE OPERATIVA ROMA valuta se è possibile condurre una verifica completa a fronte della norma di riferimento anche in assenza di tali documenti.

In tali casi lo scopo di certificazione potrà comprendere solamente i processi che sono stati sottoposti ad audit.

La norma UNI CEI ISO/IEC 27001:2014 riporta nelle sezioni da 4 a 10 (comprese) una serie di requisiti obbligatori per il SGSI, che non possono essere cioè oggetto di esclusione.

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 APAVE CERTIFICATION ITALIA - SEDE OPERATIVA ROMA, quale organismo di certificazione del SGSI, ha il compito di valutare la documentazione ed attuazione di tutti i requisiti delle sezioni da 4 a 10 (comprese), e dei paragrafi dell'"Appendice A" che l'organizzazione ha dichiarato applicabili nel SoA riservandosi la facoltà di giudicare l'adeguatezza delle scelte operate dall'organizzazione.

APAVE CERTIFICATION ITALIA - SEDE OPERATIVA ROMA valuta inoltre la congruenza tra la valutazione dei rischi eseguita e fornita dall'organizzazione, valutando le minacce e le vulnerabilità considerate o applicabili. L'analisi del contesto nel quale opera l'organizzazione e la valutazione di altri eventuali controlli oltre quanto indicato nell'Annex A, sono necessari per la corretta valutazione del SGSI dell'organizzazione e APAVE CERTIFICATION ITALIA - SEDE OPERATIVA ROMA deve valutarle.

7.1 Audit iniziale di certificazione

L'audit iniziale di certificazione è condotto in due fasi:

- fase 1, presso l'Organizzazione, finalizzato alla valutazione della documentazione del sistema SGSI e del grado di preparazione dell'Organizzazione per l'effettuazione dello fase 2 .
- fase 2, presso l'Organizzazione, finalizzato alla valutazione dell'applicazione e dell'efficacia del SGSI.

7.1.1 Audit di fase 1

Prima dell'audit di Fase 1 l'Organizzazione deve:

- mettere a disposizione del valutatore di APAVE CERTIFICATION ITALIA - SEDE OPERATIVA ROMA le informazioni generali relative al SGSI e al campo di applicazione e la documentazione del SGSI;

- indicare al valutatore eventuali esigenze che richiedano che la valutazione documentale venga effettuata in un luogo diverso dalla sede oggetto della certificazione.

Al termine dello Fase 1 il GA definisce i tempi per l'effettuazione dello fase 2.

Tra fase 1 e fase 2 non possono trascorrere più di tre mesi. Trascorso tale termine l'audit di Fase 1 deve essere ripetuto.

APAVE CERTIFICATION ITALIA - SEDE OPERATIVA ROMA valuta i casi eccezionali in cui sussistono le condizioni per mantenere validi i risultati dello Fase 1.

Nella fase 1 il GA procede all'esame della documentazione del SGSI dell'Organizzazione che deve essere costituito dai documenti richiamati al par 7.5 della UNI CEI ISO/IEC 27001:2014.

L'organizzazione deve garantire che lo scopo dell'SGSI, i documenti relativi alla valutazione ed al trattamento dei rischi, e lo Statement of Applicability, le policy e le procedure per la sicurezza delle informazioni siano gestiti sempre in forma controllata.

Vanno evidenziate anche le interrelazioni e le interfacce con processi ed asset non compresi nel SGSI, segnalando in particolari tra questi i processi e/o asset che utilizzino i medesimi siti ed infrastrutture informatiche.

7.1.2 Audit di fase 2

La verifica di valutazione di fase 2 ha lo scopo di:

- confermare che l'organizzazione opera secondo quanto ha stabilito nelle proprie procedure e obiettivi.
- Confermare che il SGSI è conforme ai requisiti della norma ISO/IEC 27001:2013.

Nello fase 2 l'Organizzazione deve dimostrare che il SGSI impostato sia rilevante ed adeguato rispetto alle attività dell'Organizzazione stessa e alle minacce, alle vulnerabilità e agli impatti individuati.

Nel corso dell'audit l'Organizzazione deve inoltre dimostrare di avere un sistema di gestione in grado di assicurare la conformità alle leggi e regolamenti applicabili alla sicurezza delle informazioni.

7.2 Esame degli esiti della valutazione

Vale quanto descritto nel Regolamento Generale di APAVE CERTIFICATION ITALIA - SEDE OPERATIVA ROMA, inoltre nella classificazione dei rilievi, si ritiene "non conformità" il mancato rispetto dei requisiti di legge, il mancato rispetto di requisiti contrattuali concordati con il partner o clienti relativamente alla sicurezza delle informazioni e per i quali il certificato può essere interpretato come garanzia della presa in carico, la palese evidenza di un immediato rischio per le informazioni incluse nello scopo dell'SGSI, nessuna evidenza oggettiva disponibile in relazione alla gestione degli incidenti o la mancanza di un Business Continuity Plan, la non esecuzione di riesami della direzione nei 12-15 mesi precedenti l'audit.

7.3 Rilascio della certificazione

Vale quanto descritto nel Regolamento Generale di APAVE CERTIFICATION ITALIA - SEDE OPERATIVA ROMA. Il certificato di conformità riporterà anche il riferimento al SoA con i dati identificativi dello stesso (data, revisione, ecc.).

7.4 Attività di valutazione in sorveglianza

Vale quanto descritto nel Regolamento Generale di APAVE CERTIFICATION ITALIA - SEDE OPERATIVA ROMA. Al momento dell'audit di sorveglianza l'organizzazione deve dare evidenza dell'esecuzione del riesame della direzione e di un ciclo completo di audit interni secondo quanto previsto dalla sezione 9 della ISO/IEC 27001:2013 con frequenza almeno annuale.

7.5 Rinnovo della certificazione

Vale quanto descritto nel Regolamento Generale di APAVE CERTIFICATION ITALIA - SEDE OPERATIVA ROMA. Al momento dell'audit di sorveglianza l'organizzazione deve dare evidenza dell'esecuzione del riesame della direzione e di un ciclo completo di audit interni secondo quanto previsto dalla sezione 9 della ISO/IEC 27001:2013 con frequenza almeno annuale.

7.6 Diritti e doveri dell'organizzazione in possesso di certificazione

Oltre a quanto descritto nel Regolamento Generale di APAVE CERTIFICATION ITALIA - SEDE OPERATIVA ROMA, l'Organizzazione certificata è tenuta a comunicare a Apave Certification Italia S.r.l. ogni modifica apportata al documento "SoA - Statement of Applicability".

8. AUDIT STRAORDINARI

Nessuna integrazione rispetto a RG -01 parte generale in revisione corrente.

9. PROCEDURA DI RINNOVO

Nessuna integrazione rispetto a RG -01 parte generale in revisione corrente.

10. ESTENSIONE/RIDUZIONE DELLA CERTIFICAZIONE

Nessuna integrazione rispetto a RG -01 parte generale in revisione corrente.

11. SOSPENSIONE DELLA CERTIFICAZIONE

Nessuna integrazione rispetto a RG -01 parte generale in revisione corrente.

12. REVOCA DELLA CERTIFICAZIONE

Nessuna integrazione rispetto a RG -01 parte generale in revisione corrente.

13. RINUNCIA ALLA CERTIFICAZIONE

Nessuna integrazione rispetto a RG -01 parte generale in revisione corrente.

14. TRASFERIMENTO DELLA CERTIFICAZIONE DA ALTRI ODC.

Nessuna integrazione rispetto a RG -01 parte generale in revisione corrente.

14.1 Riesame Preliminare

Nessuna integrazione rispetto a RG -01 parte generale in revisione corrente.

14.2 Certificazione

Nessuna integrazione rispetto a RG -01 parte generale in revisione corrente.

14.3 Clausole contrattuali

Nessuna integrazione rispetto a RG -01 parte generale in revisione corrente.

15. RICORSI

Nessuna integrazione rispetto a RG -01 parte generale in revisione corrente.

16. RECLAMI

Nessuna integrazione rispetto a RG -01 parte generale in revisione corrente.

17. CONTENZIOSI

Nessuna integrazione rispetto a RG -01 parte generale in revisione corrente.

18. GESTIONE DEL CONTRATTO APAVE CERTIFICATION ITALIA - SEDE OPERATIVA BRESCIA-ORGANIZZAZIONE

Nessuna integrazione rispetto a RG -01 parte generale in revisione corrente.

18.1 Quotazione Contrattuale

Nessuna integrazione rispetto a RG -01 parte generale in revisione corrente.

18.2 Fatturazione

Nessuna integrazione rispetto a RG -01 parte generale in revisione corrente.