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
4	00	29/06/18	Unificazione Sistemi Gestione SICIV-APAVE CERTIFICATION ITALIA	**Roma** S. Bertini	**Brescia** F. Donati	**Roma** D. Venditti	**Brescia** S. Citroni	Urbano Strada
4	01	28/06/19	Adeguamento alle Code of Practice ISO/IEC 27017 e ISO/IEC 27018	**Roma** S. Bertini	**Brescia** F. Donati	**Roma** D. Venditti	**Brescia** S. Citroni	Urbano Strada
4	02	03/09/19	Valutazione documentale Accredia Code of Practice ISO/IEC 27017 e ISO/IEC 27018	**Roma** S. Bertini	**Brescia** F. Donati	**Roma** D. Venditti	**Brescia** S. Citroni	Urbano Strada
4	03	06/03/20	Adeguamento alla Estensione ISO/IEC 27701	**Roma** S. Bertini	**Brescia** F. Donati	**Roma** D. Venditti	**Brescia** 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.

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 e ISO/IEC 27018:2019, rispettivamente "*Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services" e "Information technology -- Security techniques -- Requirements for bodies providing audit and certification of information security management systems",* e le condizioni per la certificazione della norma (Extension) ISO/IEC 27701:2019 "*Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – requirements and guidelines"*

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. 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 e con l'eventuale l'integrazione alle linee guida ISO/IEC 27017:2015 e/o ISO/IEC 27018:2019 e/o ISO/IEC 27701:2019. La 27017:2015 può 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 27017:2015 dovrà essere integrata con la ISO/IEC 27018:2019. Non è ammessa l'estensione alla sola ISO/IEC 27018:2019. La 27701:2019 può essere oggetto di estensione della certificazione anche da sola.

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 27001:2017 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.

Le due norme ISO/IEC 27017 e ISO/IEC 27018 fanno entrambe specifico riferimento ad un set di controlli ulteriori introdotti per quanto attiene le attività in cloud e si vanno ad aggiungere e/o a modificare quanto riportato nella norma ISO/IEC 27001:2013.

La Norma 27017:2015 può 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 Norma ISO/IEC 27017:2015 dovrà essere integrata con la Norma ISO/IEC 27018:2019.

Le due norme ISO/IEC 27701 fa specifico riferimento ad un set di controlli ulteriori introdotti per quanto attiene le attività per la protezione dei dati personali (privacy) e si vanno ad aggiungere e/o a modificare quanto riportato nella norma ISO/IEC 27001:2013.

La Norma 27017:2015 può essere oggetto di estensione della certificazione anche da sola. Ove si intenda considerare tale estensione anche in ottica di Protezione Dati Personali in cloud, l'estensione alla Norma ISO/IEC 27017:2015 dovrà essere integrata con la Norma ISO/IEC 27018:2019.

Ai fini della integrazione di un certificato ISO/IEC 27001 esistente, a fronte delle Linee Guida ISO/IEC 27017 e ISO/IEC 27018, valgono i seguenti criteri:

a) L'estensione può essere garantita solo dopo una verifica che dovrà essere eseguita presso il sito/i siti interessati dell'organizzazione.

b) Se l'organizzazione è già in possesso di una certificazione ISO/IEC 27001, emessa da Apave Certification Italia e con uno scopo di certificazione compatibile con i processi coperti dalle Norme ISO/IEC 27017 e 27018, l'audit di estensione sarà condotto in un'unica fase, integralmente svolta presso la sede dell'organizzazione. La durata dell'audit di estensione dovrà essere di almeno il 30% del tempo di audit di un rinnovo di certificazione ISO/IEC 27001 (tempo necessario all'audit di ogni linea guida), con una durata minima di una giornata per il sito principale e mezza giornata per ogni sito interessato dall'estensione.

c) Se l'organizzazione è in possesso di altra certificazione ISO/IEC 27001 sotto MLA, dovrà richiedere il trasferimento della stessa ad Apave Certification Italia (vedasi paragrafo Trasferimento nel regolamento Generale SG 01), per consentire l'emissione del certificato integrato.

d) Se l'organizzazione non è già in possesso di una certificazione valida e riconosciuta sotto accreditamento per la Norma ISO/IEC 27001, l'audit sarà svolto secondo i criteri di una nuova certificazione a fronte delle Norme ISO/IEC 27001, con l'aggiunta per la 27017 e 27018 di un incremento minimo del tempo di audit non inferiore al 30% del tempo per una prima certificazione ISO/IEC 27001 (tempo necessario per ogni linea guida; quindi per due linee guida il tempo sarà il doppio) e, comunque, non inferiore a un giorno per il sito principale e mezza giornata per ogni sito aggiuntivo campionato.

e) Per le sorveglianze, si applica sempre l'aumento di almeno mezza giornata per il sito principale e mezza giornata per ogni sito campionato, per linea guida.

Prima del rilascio della certificazione devono essere verificati tutti i data center presso cui sono dislocati i server che gestiscono il cloud.

Estensioni incrementali:

Ove l'organizzazione richieda l'estensione della certificazione alle due Norme ISO/IEC 27017:2015 e ISO/IEC 27018:2019 separatamente, l'iter deve prevedere che la prima estensione sia alla Norma (linea guida) ISO/IEC 27017.

Non è ammessa l'estensione alla Norma (linea guida) ISO/IEC 27018:2019 senza il supporto della ISO/IEC 27017:2015.

La norma ISO/IEC 27701 fa specifico riferimento ad un set di controlli ulteriori introdotti per quanto attiene le attività per la protezione dei dati personali e si vanno ad aggiungere e/o a modificare quanto riportato nella norma ISO/IEC 27001:2013.

La Norma ISO/IEC 27701 può essere oggetto di estensione della certificazione anche da sola, ma occorre che l'organizzazione sia già certificata a fronte della Norma ISO/IEC 27001, sotto accreditamento, anche da un differente organismo.

a) Ai fini della integrazione di un certificato ISO/IEC 27001 esistenti a fronte della norma ISO/IEC 27701, valgono i seguenti criteri:

1. L'estensione può essere garantita solo dopo una verifica che dovrà essere eseguita presso il sito/i siti interessati dell'organizzazione.

2. Se l'organizzazione è già in possesso di una certificazione ISO/IEC 27001, emessa dallo stesso CAB e con uno scopo di certificazione compatibile con i processi coperti dalle Norma ISO/IEC 27701, l'audit di estensione sarà condotto in un'unica fase, integralmente svolta presso la sede dovrà essere di almeno il 30% del tempo di audit di un rinnovo di certificazione ISO/IEC 27001 (tempo necessario all'audit di ogni linea guida), con una durata minima di una giornata per il sito principale e mezza giornata per ogni sito interessato dall'estensione.

3. Se l'organizzazione è in possesso di altra certificazione ISO/IEC 27001 sotto MLA, dovrà richiedere il trasferimento della stessa al CAB accreditato ACCREDIA, per consentire l'emissione del certificato integrato.

4. Se l'organizzazione non è già in possesso di una certificazione valida e riconosciuta sotto accreditamento per la Norma ISO/IEC 27001, l'audit sarà svolto secondo i criteri di una nuova certificazione a fronte delle Norme ISO/IEC 27001, con l'aggiunta per la ISO/IEC 27701 di un incremento minimo del tempo di audit non inferiore al 30% del tempo per una prima certificazione ISO/IEC 27001 (tempo necessario per ogni linea guida che viene adottata per lo schema afferente alla protezione dati; quindi per organizzazioni che operano utilizzando servizi erogati con modalità "cloud" il tempo sarà quello relativo alle tre linee guida applicabili e mandatorie) e, comunque, non inferiore a un giorno per il sito principale e mezza giornata per ogni sito aggiuntivo campionato.

5. Per le sorveglianze, si applica sempre l'aumento di almeno una giornata per il sito principale e mezza giornata per ogni sito campionato, per linea guida. Se vengono adottati servizi "cloud" si sommano anche i tempi per le sorveglianze sulle linee guida ISO/IEC 27017 e 27018.

6. Le modalità di auditing dovranno sempre prevedere la registrazione delle evidenze necessarie a garantire la completa ed esaustiva applicazione sia dei requisiti della Norma ISO/IEC 27001, sia dei requisiti aggiuntivi pertinenti alla ISO/IEC 27701.

7. Si dovrà inoltre verificare se l'organizzazione si sottopone periodicamente a vulnerability assessment / penetration test, e con quali modalità (es. vulnerability assessment condotti da LAB accreditati, penetration test condotti da LAB che abbiano caratteristiche organizzative e gestionali equivalenti ai requisiti della Norma ISO/IEC 17025).

8. Occorre inoltre prevedere la verifica dell'adeguatezza dei data center attraverso, ad esempio, la verifica diretta dell'ambiente fisico, garanzie messe a disposizione da eventuali fornitori, rapporti di audit di prima o di seconda parte. Le modalità di auditing dovranno prevedere, inoltre, la verifica del mantenimento dei criteri adottati per la valutazione dell'adeguatezza dei data center.

b) Estensioni incrementali:

1. Non è ammessa l'estensione alla ISO/IEC 27701, per organizzazioni che utilizzano servizi erogati con modalità "cloud", senza il supporto della ISO/IEC 27017:2015 e della ISO/IEC 27018.

2. È comunque possibile che una organizzazione, già certificata ISO/IEC 27001, richieda l'estensione della certificazione alla ISO/IEC 27701 separatamente da una verifica di sorveglianza o rinnovo ISO/IEC 27001.

c) Audit di sorveglianza e rinnovo:

1. Tali audit saranno condotti sempre su tutte le Norme

   applicabili di estensione alla ISO/IEC 27001:2013, prevedendo:

2. Sorveglianza: un incremento minimo del tempo di audit non inferiore al 30% del tempo di una sorveglianza (tempo necessario all'audit di ogni linea guida, pertanto per tre linee guida il tempo aggiuntivo sarà almeno tre volte il 30%) e non inferiore a mezza giornata per ogni sito aggiuntivo campionato ove adottata una sola linea guida o una giornata per le tre linee guida.

3. Rinnovo: dovrà prevedere un incremento minimo del tempo di audit non inferiore al 30% del tempo di una ricertificativa (tempo necessario all'audit di ogni linea guida, pertanto per tre linee guida il tempo aggiuntivo sarà almeno tre volte il 30%) e una mezza giornata per ogni sito aggiuntivo campionato ove adottata una sola linea guida o una giornata per le tre linee guida.

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 per lo schema SSI è condotto in due fasi nel caso della ISO/IEC27001 ed in unica fase (fase_2) nel caso delle norme ISO/IEC 27017, ISO/IEC 27018 e ISO27701.

- 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 e/o dei controlli aggiuntivi propri delle norme specifiche.

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 27001:2017.

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 dello scopo flessibile ISO/IEC 270xx.

Nella 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.

Nel corso dell'audit per le due norme riferibili al Cloud, l'Organizzazione deve dimostrare di avere implementato il set di controlli previsti dalle norme stesse in aggiunta alla norma di riferimento ISO/IEC 27001, Annex A.

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 documento SoA con i dati identificativi dello stesso (data, revisione, ecc.).

Per quanto riguarda le linee guida 27017 e 27018, il certificato deve fare sempre riferimento alla Norma ISO/IEC 27001 citando l'utilizzo della linea guida ISO/IEC 270XX nella sua applicazione. Saranno indicati i prodotti / servizi / applicazioni / processi coperti dalla certificazione.

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.