MODALITÀ DI VALUTAZIONE PER LA CERTIFICAZIONE INIZIALE E PER IL RINNOVO DELLA CERTIFICAZIONE DEI
ISMS AUDITOR / RESPONSABILI GRUPPO DI AUDIT

Rev.	Data	Motivazioni	Convalida	Approvazione
5	30.08.2017	Rev. Generale	*R.A. Favorito*	*M. Dutto*
4	28.09.2016	Pag. 1	*R.A. Favorito*	*G. Colferai*

INDICE

1.0 SCOPO E CAMPO DI APPLICAZIONE

La presente procedura descrive le modalità operative adottate da CEPAS per l'attività di valutazione e certificazione degli Auditor (AUD) e dei Responsabili Gruppo di Audit (RGA) di Sistemi di Gestione per la Sicurezza delle Informazioni (ISMS).

La procedura si applica nei processi di certificazione delle figure professionali specificate che operano nell'ambito dei Sistemi di Gestione per l'ISMS ed evidenzia le responsabilità delle diverse funzioni CEPAS coinvolte.

2.0 RIFERIMENTI

Tutti i riferimenti a Leggi, Norme e documenti CEPAS richiamati nel presente documento si intendono nella loro ultima edizione vigente

- Riferimenti CEPAS per la certificazione degli ISMS Auditor/Responsabili Gruppo di Audit:
  - Norma UNI CEI EN ISO/IEC 17024:2012
  - Manuale del Sistema di Gestione per la Qualità CEPAS, sez. 5 (MQ01)
  - Schema di Certificazione CEPAS: Regolamento Generale CEPAS (RG01), Codice Deontologico (CD01), Prescrizioni per l'Uso del Marchio (MC01), Modulo richiesta ammissione esame/certificazione (MD08accr), Scheda Requisiti CEPAS SH142, Tariffario e la presente procedura PG30

- Riferimenti normativi per la valutazione degli Audit:
  - UNI EN ISO 19011:2012
  - UNI CEI ISO/IEC 27001:2014
  - ISO/IEC 27005:2011
  - ISO/IEC 27006:2011
  - UNI CEI EN ISO/IEC 17021:2011
- Regolamenti Tecnici emessi da ACCREDIA

3.0 PROCESSO DI VALUTAZIONE

La valutazione di idoneità del Candidato, ai fini del rilascio della certificazione CEPAS, avviene attraverso la sequenza, temporale e vincolante, di ciascuna delle seguenti fasi:

- valutazione della documentazione prodotta dal Candidato eseguita dal Referente CEPAS, che accerta il possesso dei requisiti di cui alla Scheda SH142; nei casi dubbi, l'Operational & Technical Manager può inoltre procedere a:
  - richiesta di informazioni/documenti supplementari al candidato;
  - accertamento, tramite invio di un Commissario appositamente incaricato, dell'attività svolta presso le aziende citate nella documentazione presentata.

Il Candidato dichiara espressamente di accettare le condizioni previste dall'iter di certificazione CEPAS ai sensi e per gli effetti delle disposizioni di cui all'art. 1341 C.C.

ad esito positivo segue:

- revisione del processo di certificazione (CPR) per l'emissione del certificato (a cura del referente di Schema)

ad esito positivo segue:

- approvazione da parte dell'Operational & Technical Manager CEPAS e delibera di iscrizione nel Registro;

ad esito positivo segue:

- comunicazione al Comitato di Imparzialità e di Schema.

Qualora l'esito di una qualsiasi delle suddette fasi sia negativo, CEPAS interrompe il processo di valutazione e informa il Candidato. Per procedere nell'iter sarà necessario prima risolvere le carenze riscontrate nella singola fase, nei tempi indicati da CEPAS.

CEPAS rende disponibile la seguente modulistica, contenente tutte le informazioni necessarie per verificare il possesso dei requisiti richiesti per la certificazione:

- MD71qas: Modulo di registrazione audit
- MD71dich: Modulo fac simile lettera di referenze (per documentare esperienza lavorativa)
- MD71dich_training: Moduli di registrazione audit condotti sotto la direzione e guida di Responsabili Gruppo di Audit certificati da OdC del Personale o qualificati da OdC di Sistema

4.0 ESAME

4.1 Requisiti di ammissione esame di certificazione

I Candidati in possesso dei requisiti di formazione specifica, esperienza lavorativa complessiva, esperienza specifica di audit descritti nella SH142 saranno ammessi all'esame di certificazione CEPAS, presentando formale richiesta attraverso il modulo MD08accr e allegando i documenti nello stesso indicati e di cui alla suddetta Scheda requisiti:

- copia titolo di studio
- curriculum vitae datato, aggiornato e firmato
- evidenze oggettive in merito alla formazione specifica (attestati,…)
- evidenze oggettive in merito agli anni di esperienza lavorativa continuativa complessiva e agli anni di esperienza lavorativa specifica nel campo dei Sistemi di gestione della sicurezza delle informazioni,
- evidenze oggettive in merito agli audit completi UNI CEI ISO/IEC 27001:2006 validi a fini della certificazione,
- evidenze oggettive in merito agli audit completi effettuati sotto la direzione e guida di un Responsabile Gruppo di Audit,
- regolare pagamento delle quote previste per l'ammissione all'esame come da tariffario CEPAS

Per i Candidati non madrelingua italiana, CEPAS si assicura la corretta comprensione della lingua italiana, scritta e orale, e a tal fine può richiedere evidenza di corsi riconosciuti.

La documentazione completa per la richiesta di certificazione deve essere trasmessa a CEPAS entro 10 giorni lavorativi prima della data d'esame.

4.2 Finalità esame

L'esame ha lo scopo di:

- approfondire le informazioni presentate dal Candidato, nell'ambito della sua esperienza professionale, valutando l'adeguatezza della documentazione presentata e la sua congruenza con il/i settore/i di interesse indicato/i dal Candidato;
- accertare il possesso da parte del Candidato delle conoscenze tecniche e metodologiche necessarie a:
  - condurre audit interni e/o esterni per la verifica della conformità e dell'efficacia dei Sistemi di Gestione per la Sicurezza delle Informazioni alle Norme di riferimento, sia ai fini dell'accertamento periodico e sistematico dell'adeguatezza e funzionalità dei Sistemi di Gestione, sia ai fini del rilascio della relativa Certificazione;
  - condurre gli Audit in conformità alle Norme UNI EN ISO 19011 e UNI CEI EN ISO/IEC 17021:2011

Rientrano tra tali conoscenze e abilità:

<u>Area Auditing:</u>

- norma UNI EN ISO 19011, ISO/IEC 27000, UNI CEI ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005, ISO/IEC 27006 e Prescrizioni ACCREDIA applicabili
- Norma UNI EN ISO 19011:
  - principi dell'attività di audit
  - gestione di un programma di audit
  - attività di audit
  - competenza e valutazione degli auditor
- Norma UNI CEI EN ISO/IEC 17021, in particolare cap. 9 e Appendici A, D, E, F
- Tipologie di audit
- Pianificazione dell'audit che deve prevedere:

- comunicazione con l'organizzazione sottoposta ad audit;
- documentazione dell'esame preliminare;
- esame della documentazione;
- selezione del team di audit;
- preparazione dell'audit e riunione del team.

- Cenni sulle finalità di audit preliminari
- Preparazione ed uso (con esempi di modulistica) di checklist durante le fasi di audit
- Preparazioni delle riunioni di audit, con esempi
- Contenuto, programma e conduzione delle riunioni di apertura e chiusura
- Comportamento dell'auditor nello svolgimento dell'audit, incluse le relazioni con l'azienda, l'importanza delle evidenze oggettive; rilevazione, redazione e comunicazione delle anomalie
- Criteri per la formulazione e metodologie per l'identificazione dei rilievi e loro classificazione
- Attività di follow-up
- Cenni sulla gestione del rischio come applicabile nel settore ISMS
- Cenni sul rispetto dei requisiti di legge su salute e sicurezza da parte del Gruppo di Audit
- Elementi di metrologia industriale, tecniche statistiche, tecniche affidabilistiche ("failure analysis") applicabili al settore
- Differenze di ruolo fra Auditor e Responsabili Gruppo di Audit, nella gestione dell'audit e dei membri del team
- inoltre, le conoscenze e abilità riportate, a titolo esemplificativo, nella norma UNI EN ISO 19011:2012 Appendice A.7

Area Legale

- L. 300/1970
- Aspetti legali relativi ai Decreti legislativi e modificazioni successive:
  - Privacy: D. Lgs. 196/03, con i vari allegati, tra cui il B sulle misure minime
  - Diritto d' Autore: L. 633/41 - D. Lgs 518/92 - L. 248/00 - Regol. 338/01 (SIAE)
  - Responsabilità penali delle Persone Giuridiche (pirateria informatica, pedoporno, truffe informatiche ai danni dello stato) D. Lgs. 231/01
  - Commercio elettronico, D. Lgs 70/03
  - Proprietà Industriale, D. Lgs. 30/05
  - Amministrazione Digitale (firme elettroniche etc.) D. Lgs. 82/05
  - Antiterrorismo (pacchetto Pisanu) L. 155/05
  - Violazione reti informatiche, L. 547/93 da leggere con il D. Lgs. 196/03
- Conoscenze degli aspetti normativi sulla tutela del segreto di Stato
- Responsabilità Civili, Penali e Amministrative
- Aspetti contrattuali relativi all'Outsourcing connessi alla Security
- Aspetti contrattuali (security audit) Fornitori, Clienti, Terze Parti
- Aspetti di diritto e procedura penali connessi alla Security
- Iniziative di tipo giuridico e assicurativo a protezione del patrimonio informativo aziendale

Area Tecnologica

- Elementi base dell'ISMS, dei concetti di sistema e delle reti
- Fondamentali dell'Information Security
- Criteri e strumenti di classificazione dei dati trattati
- Tecniche di controllo accesso fisico e logico
- Modalità di protezione delle informazioni ed elementi di crittografia
- Firma elettronica, digitale
- Virus, I-Worms, Programmi maligni, Prodotti e tecniche di prevenzione e di contrasto
- Business Continuity, Disaster Recovery e Crisis Management
- Penetration tests (cenni) e relativi aspetti legali
- Applicazione delle soluzioni individuate delle vulnerabilità e delle minacce

- ITSEC (cenni)
- ISO 15408 Parte 1 - 2 e 3 (*cenni*) (ex Common Criteria)
- Elementi base dei principali rischi per l'ICT Security nei: commercio elettronico, EDI (Elettronic Data Interchange), posta elettronica, operazioni bancarie o di trading remote, sistemi di gestione integrati ERP, sistemi di supporto a e decisioni (DSS), sviluppo e/o acquisto di Sistemi Informativi e di Telecomunicazione, re-ingegnerizzazione dei processi o del relativo sw, gestione della documentazione di sistema.

Area Management

- Aspetti organizzativi dell'Information Technology
- Aspetti organizzativi dell'Information Security
- Gestione delle problematiche complesse
- D.Lgs 231/01, sistemi di controllo ed elementi di Corporate Governance
- D. Lgs 196/2003, D.Lgs 196 del 30 giugno 2003 - Codice in materia di protezione dei dati personali
- Norma ISO/IEC 27000, Information technology -- Security techniques --Information security management systems - Fundamentals and vocabulary
- Norma UNI CEI ISO/IEC 27001 Tecnologie delle informazioni. Tecniche di sicurezza. Sistemi di gestione delle sicurezza delle informazioni – Requisiti
- Norma ISO/IEC 27002, Information Technology - Security techniques - Code of Practice for information security management
- Norma ISO/IEC 27005, Information technology — Security techniques — Information security risk management
- Norma ISO/IEC 27006, Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems
- Definizione della politica dell'ISMS
- Definizione delle strategie dell'ISMS
- Organizzazione della struttura di ISMS
- Risk Assessment: Risk Analysis e Risk Evaluation
- Risk Management
- BS 25999-1: 2006 Business Continuity Management, Part 1: Code of practice
- BS 25999-2: 2007 Business Continuity Management, Part 2: Specification
- Sistemi di misurazione per analisi Costi/Benefici
- Modalità di supporto alle attività delle istituzioni deputate
- Rischi di ICT Security connessi allo sviluppo e/o acquisto di Sistemi Informativi e di Telecomunicazione.
- Rischi ICT Security connessi con la re-ingegnerizzazione dei processi o del relativo sw
- Rischi connessi alla gestione della documentazione di sistema

L'esame è condotto dai Commissari d'esame CEPAS, i quali si accertano, attraverso opportune tecniche, che il Candidato abbia i comportamenti personali idonei allo svolgimento delle attività professionali per le quali richiede la certificazione. La Commissione definirà inoltre, in sede d'esame, l'idoneità allo svolgimento del ruolo richiesto, sulla base della documentazione prodotta e dell'esito dell'esame (ISMS Auditor oppure ISMS Responsabile Gruppo di Audit). I Commissari sono responsabili della valutazione delle prove d'esame del Candidato e per questo ne rispondono a CEPAS; per tutte le attività di valutazione i Commissari garantiscono indipendenza di giudizio, imparzialità, assenza di conflitto di interessi e riservatezza dei dati.

4.3 Modalità svolgimento esame

L'esame si svolge nelle località e secondo le date e il programma comunicati ai candidati da CEPAS.

Alla sessione d'esame CEPAS sono presenti i candidati, la commissione d'esame, il personale CEPAS e, quando previsto, gli ispettori ACCREDIA. Gli ispettori ACCREDIA possono riservarsi di intervistare i presenti nel rispetto, comunque, del programma CEPAS di gestione dell'esame.

Prima dell'inizio delle prove d'esame, i candidati sono tenuti a:
- esibire un documento di identità valido e consegnarne copia a CEPAS,
- firmare il foglio presenze,
- sottoscrivere copia del Codice Deontologico (CD01) e delle Prescrizioni per l'uso del Marchio (MC01), per accettazione delle procedure dell'intero iter di certificazione.
- presentare la ricevuta degli avvenuti pagamenti delle quote previste per la partecipazione all'esame.

4.4 Argomenti e criteri di valutazione

L'esame CEPAS si articola così come di seguito dettagliato, in base al punto della SH142 applicabile.

Per i Candidati in possesso dei requisiti di cui al **punto 1** della Scheda SH142 l'esame consiste in:
- una prova scritta di carattere specifico (capacità di applicare correttamente le norme);
- una prova scritta di carattere generale (conoscenza ed interpretazione delle norme);
- una prova orale (colloquio).

La prova scritta di carattere specifico, caso di studio, riferito ad un audit, è volta ad accertare la conoscenza, da parte del Candidato, delle metodologie di esecuzione delle attività per le quali si è richiesta la Certificazione (ISMS Auditor/Responsabile Gruppo di Audit). Per tale prova è previsto un tempo massimo di 70 minuti.

La prova scritta di carattere generale è volta ad accertare il possesso, da parte del Candidato, delle conoscenze tecniche necessarie a svolgere le attività relative alla domanda di Certificazione presentata. E' composta da:
- un numero minimo di 20 domande, per le quali vengono fornite cinque risposte di cui una sola è sicuramente esatta. Per tale prova è previsto un tempo massimo di 45 minuti.

La prova orale (colloquio) è volta a:
- approfondire il livello di conoscenza degli elementi culturali di base di cui alle prove scritte,
- approfondire nell'ambito della esperienza professionale le informazioni presentate dal Candidato,
- valutare l'adeguatezza, l'estensione ed il grado di aggiornamento delle esperienze specifiche operative,
- verificare il modo di gestire i rapporti interpersonali del Candidato,
- valutare i comportamenti personali attesi previsti dalle Norme di riferimento (UNI EN ISO 19011 e UNI CEI EN ISO/IEC 17021 parti applicabili) in funzione del ruolo di Auditor o di Responsabile Gruppo di Audit,
- valutare la congruenza tra la richiesta di certificazione da parte del Candidato (nel ruolo di AUD o RGA) e lo Schema di Certificazione CEPAS,

La Commissione di Esame procede alla valutazione di idoneità del Candidato a fronte dei criteri e dei parametri di seguito specificati:
- la votazione massima ottenibile è di 80 punti, ed è data dalla sommatoria delle votazioni conseguite dal candidato nelle prove d'esame:
  - alla prova scritta di carattere specifico, viene attribuita una votazione massima di 10 punti.
  - alla prova scritta di carattere generale, viene attribuita una votazione massima di 50 punti.
  - alla prova orale, viene attribuita una votazione massima di 20 punti.

La **soglia minima** per il superamento dell'esame è pari al 70% della sommatoria del massimo punteggio ottenibile nelle prove sostenute dagli stessi (56 punti), tenendo comunque presente che deve essere anche superata la soglia minima fissata per le prove scritte, pari a 36 punti. Pertanto, se il Candidato non supera la soglia minima di 36 punti nelle prove scritte non verrà ammesso alla prova orale e dovrà ripetere l'intero esame (scritto e orale).

******

Per i Candidati in possesso dei requisiti di cui al **punto 2** e **punto 3** della Scheda SH142 l'esame consiste in:

- una prova tecnica specifica orale volta a:
  - approfondire il livello di conoscenza degli elementi culturali di base (rif. prove scritte),
  - approfondire nell'ambito della esperienza professionale le informazioni presentate dal Candidato,
  - valutare l'adeguatezza, l'estensione ed il grado di aggiornamento delle esperienze specifiche operative,
  - verificare il modo di gestire i rapporti interpersonali del Candidato,
  - valutare i comportamenti personali attesi previsti dalle Norme di riferimento (UNI EN ISO 19011 e UNI CEI EN ISO/IEC 17021 parti applicabili) in funzione del ruolo di Auditor o di Responsabile Gruppo di Audit,

- valutare la congruenza tra la richiesta di certificazione da parte del Candidato (nel ruolo di AUD o RGA) e lo Schema di Certificazione CEPAS,

La Commissione di Esame procede alla valutazione di idoneità del Candidato a fronte dei criteri e dei parametri di seguito specificati:

- la votazione massima ottenibile per la prova tecnica specifica orale è di 20 punti.

La **soglia minima** per il superamento dell'esame, pari al 70% del massimo punteggio ottenibile nella prova, è pari a 14 punti. Pertanto, se il Candidato non supera la soglia minima di 14 punti nella prova orale, dovrà ripetere l'esame (orale).

******

Per i Candidati in possesso dei requisiti di cui ai **punti 4 e 5** della Scheda SH142 l'esame consiste in:

1. prima parte della prima prova scritta (caso di studio);
2. prova tecnica specifica orale

La Commissione di Esame procede alla valutazione di idoneità del Candidato a fronte dei criteri e dei parametri di seguito specificati:

- la votazione massima ottenibile è di 30 punti, ed è data dalla sommatoria delle votazioni conseguite dal candidato nelle prove d'esame:
  - alla prova scritta di carattere specifico (caso di audit) viene attribuita una votazione massima di 10 punti.
  - alla prova tecnica specifica orale, viene attribuita una votazione massima di 20 punti.

La **soglia minima** per il superamento dell'esame è pari al 70% della sommatoria del massimo punteggio ottenibile nelle prove sostenute dagli stessi (21 punti), tenendo comunque presente che deve essere anche superata la soglia minima fissata per la prova scritta, pari a 7 punti. Pertanto, se il Candidato non supera la soglia minima di 7 punti nella prova scritta non verrà ammesso alla prova orale e dovrà ripetere l'intero esame (scritto e orale).

******

Per i Candidati in possesso dei requisiti di cui al **punto 6** della Scheda SH142 l'esame consiste in:

- una prova tecnica specifica orale

La Commissione di Esame procede alla valutazione di idoneità del Candidato a fronte dei criteri e dei parametri di seguito specificati:

- la votazione massima ottenibile per la prova tecnica specifica orale è di 20 punti.

La **soglia minima** per il superamento dell'esame, pari al 70% del massimo punteggio ottenibile nella prova, è pari a 14 punti. Pertanto, se il Candidato non supera la soglia minima di 14 punti nella prova orale, dovrà ripetere l'esame (orale).

******

Durante l'intero svolgimento delle prove d'esame, il Candidato può consultare esclusivamente le Norme e le Leggi di riferimento in versione ufficiale o autorizzata, sempre in maniera individuale. La consultazione di documentazione differente (es. materiale didattico di corsi, interpretazioni della Norma, ecc.) e/o lo scambio di informazioni con altri candidati è causa di interruzione dell'esame stesso.

Le prove, nel loro insieme, sono finalizzate a verificare le conoscenze, le capacità applicative delle Norme UNI CEI ISO/IEC 27001, UNI EN ISO 19011 e UNI CEI/EN ISO/IEC 17021, e i comportamenti personali attesi da parte dei candidati (UNI EN ISO 19011 par. 7.2.2 e UNI CEI/EN ISO/IEC 17021 appendice D-E). La valutazione dei comportamenti personali è condotta anche con l'ausilio di opportuni strumenti dedicati (colloquio, questionario ecc.).

I Commissari, al termine dell'esame, comunicano a ciascun candidato l'esito della valutazione delle prove da essi effettuata comprensivo dell'esito circa l'idoneità al ruolo. Il Personale CEPAS quindi informa il candidato circa le fasi successive previste dallo schema di certificazione

La Commissione d'esame, nei casi in cui lo ritenga opportuno, può inoltre richiedere che venga effettuato un supplemento di esame–colloquio integrativo a breve termine, come *conditio sine qua* non ai fini del rilascio/mantenimento della certificazione.

La valutazione di idoneità al ruolo di Responsabile Gruppo di Audit è data dalle evidenze emerse durante la prova orale, in riferimento alla UNI EN ISO 19011 e UNI CEI/EN ISO/IEC 17021.

4.5 Ripetizione esame di certificazione

Se non vengono superate le soglie minime previste, pari al 70% della sommatoria del massimo punteggio ottenibile nelle prove effettivamente sostenute dal candidato, l'esame potrà essere ripetuto. Ogni ripetizione comporta il pagamento della quota prevista dal tariffario vigente.

5.0 CERTIFICAZIONE

5.1 Rilascio del certificato

Il Candidato in possesso di tutti i requisiti richiesti viene proposto per la certificazione all'Operational & Technical Manager CEPAS per l'approvazione. L'Operational & Technical Manager, per i candidati ritenuti idonei, rilascia il Certificato e provvede all'iscrizione nell'apposito Registro e comunica la stessa al Comitato di Schema CEPAS.
Qualora l'esito di una qualsiasi delle suddette fasi sia negativo e/o il Candidato non corrisponda le quote previste dal tariffario, CEPAS interrompe il processo di valutazione e informa il Candidato. Per procedere nell'iter sarà necessario prima risolvere le carenze riscontrate nella singola fase, nei tempi indicati da CEPAS.

5.2 Passaggio di Registro (da ISMS Auditor a ISMS Responsabile Gruppo di Audit)

Il personale certificato CEPAS, in qualità di ISMS Auditor, può richiedere il rilascio del certificato per il livello funzionale successivo e l'iscrizione nel relativo registro, trascorsi almeno 6 mesi dalla prima iscrizione nel Registro, salvo quanto diversamente comunicato al candidato in merito (es. richiesta di colloquio integrativo, integrazioni in merito all'esperienza lavorativa, ecc.). In tal caso il periodo necessario per poter richiedere il passaggio di registro può essere elevato a 12 mesi.

La richiesta di passaggio prevede l'integrazione della documentazione prodotta per la prima certificazione, sulla base di quanto indicato dalla Scheda requisiti CEPAS di riferimento, ed il pagamento della quota secondo tariffario. Nel caso in cui la richiesta di passaggio di registro avvenga a seguito di colloquio integrativo per il rilascio/mantenimento della certificazione (rif. paragrafo 5.4), gli audit necessari dovranno essere successivi al rilascio della prima certificazione.

La valutazione di idoneità del Candidato avviene attraverso la sequenza, temporale e vincolante, di ciascuna delle seguenti fasi:

- valutazione della documentazione prodotta dal Candidato eseguita dal Referente CEPAS, che accerta il possesso dei requisiti per il passaggio di Registro, di cui alla Scheda SH142; nei casi dubbi, l'Operational & Technical Manager può inoltre procedere a:
  - richiesta di informazioni/documenti supplementari al candidato;
  - accertamento, tramite invio di un Commissario appositamente incaricato, dell'attività svolta presso le aziende citate nella documentazione presentata,
  - invitare il Candidato per un colloquio di approfondimento.

ad esito positivo segue:

- revisione del processo di certificazione (CPR) per l'emissione del certificato (a cura del referente di Schema)

ad esito positivo segue:

- approvazione da parte dell'Operational & Technical Manager CEPAS e delibera di iscrizione nel Registro;

ad esito positivo segue:

- comunicazione al Comitato di Imparzialità e di Schema.

Qualora l'esito di una qualsiasi delle suddette fasi sia negativo e/o il Candidato non corrisponda la quota prevista dal tariffario, CEPAS interrompe il processo di valutazione e informa il Candidato. Per procedere nell'iter sarà necessario prima risolvere le carenze riscontrate nella singola fase, nei tempi indicati da CEPAS.

CEPAS infine provvederà all'aggiornamento dei relativi registri e all'emissione del nuovo certificato, chiedendo la restituzione di quello superato. Il passaggio di Registro non comporta la variazione della data di scadenza complessiva.

5.3 Monitoraggio della certificazione

Per tutta la durata della certificazione, nell'ambito del monitoraggio continuo della stessa, CEPAS comunica qualsiasi eventuale esito negativo derivante dall'analisi sistematica delle pratiche. In particolare, a seguito della prima emissione del certificato, durante l'attività di comunicazione al Comitato di Certificazione/Schema, qualora si rilevi un'eventuale carenza grave che osta alla conferma della certificazione, CEPAS comunica al candidato i

passi successivi. Per procedere e/o concludere l'iter di certificazione, sarà necessario prima risolvere la carenza riscontrata, nei tempi indicati da CEPAS. In caso negativo, CEPAS avvierà la procedura di sospensione/rinnovo della certificazione stessa.

6.0 MANTENIMENTO E RINNOVO DELLA CERTIFICAZIONE

La certificazione CEPAS ha una durata quinquennale e si rinnova, in assenza di revoca e/o rinuncia, al termine dei cinque anni di validità.

6.1 Criteri per il mantenimento annuale

Annualmente, l'ISMS Auditor/RGA deve produrre a CEPAS la dichiarazione di assenza reclami ed il pagamento della quota di mantenimento prevista dal tariffario CEPAS in vigore.

6.2 Criteri per il rinnovo quinquennale

Prima della data di scadenza dei cinque anni di validità della certificazione, CEPAS informa l'ISMS Auditor/RGA, regolarmente iscritto nel relativo Registro, della possibilità di chiedere il rinnovo della propria certificazione. La comunicazione relativa al rinnovo e la relativa fattura sono inviate a tutte le persone certificate che non abbiano comunicato, almeno 3 mesi prima della scadenza annuale, l'eventuale disdetta, così come da Regolamento Generale RG01.

Ai fini del rinnovo, l'ISMS Auditor/RGA certificato dovrà produrre adeguata documentazione attestante l'attività professionale svolta nel quinquennio, come di seguito specificato:

⇒ esperienza lavorativa specifica maturata nel settore ISMS:

⇒ per ISMS Auditor: 6 ISMS audit completi (su almeno 3 sistemi diversi), di cui almeno 2 nell'ultimo anno

⇒ per ISMS Responsabili Gruppo di Audit: 8 ISMS audit completi (su almeno 2 sistemi diversi) di cui almeno 2 nell'ultimo anno e di cui almeno 5 condotti in qualità di Responsabile

⇒ aggiornamento professionale specifico nel settore per almeno 40 ore nei precedenti 5 anni;

⇒ richiesta rinnovo certificazione (MD63rin), contenente accettazione documenti CEPAS, dichiarazione Assenza reclami e accettazione clausole contrattuali

⇒ versamento della quota prevista per il mantenimento annuale, come da tariffario vigente

⇒ superamento test online per la verifica dell'aggiornamento delle conoscenze, secondo quanto indicato nella comunicazione di rinnovo.

⇒ dettagliato curriculum vitae, completo di consenso al trattamento dati personali e redatto ai sensi dell'art. 46 e 76 del D.P.R. 445/2000, aggiornato, datato e firmato per esteso;

⇒ fotocopia di un documento di identità in corso di validità;

⇒ versamento della quota prevista per il mantenimento annuale, come da tariffario vigente;

Tutte le evidenze devono essere relative all'attività professionale/aggiornamento professionale svolti nei 5 anni precedenti la scadenza del certificato.

Eventuali aggiornamenti normativi volontari e/o cogenti che dovessero intervenire saranno recepiti dallo schema di certificazione e verrà richiesto l'adeguamento da parte delle persone certificate.

6.3 Sospensione e annullamento

Nel caso la documentazione inviata non sia idonea ai fini del rinnovo e/o non venga presentata entro la data comunicata con il preavviso di scadenza e in caso di mancato pagamento della quota di mantenimento, CEPAS procederà, comunicandolo alla Persona certificata, alla sospensione del certificato e all'aggiornamento del relativo registro senza il nominativo della Persona stessa. Nel caso tale documentazione non venga presentata entro il mese successivo alla scadenza della certificazione, l'Operational & Technical Manager provvederà all'annullamento della certificazione e alla relativa comunicazione al Comitato di Certificazione/Schema, richiedendo la restituzione del certificato e dell'eventuale timbro.

All'ISMS Auditor/RGA che, nell'arco dei cinque anni di validità della certificazione, non ha svolto le attività richieste per il rinnovo e/o non ha fornito a CEPAS adeguata evidenza documentale, non viene rinnovata la certificazione.

L'ISMS Auditor/RGA, qualora non intenda rinnovare la propria certificazione, è tenuto a darne comunicazione, scritta, a CEPAS nel periodo dei tre mesi precedenti la data di scadenza della stessa.

L'annullamento della certificazione comporta, nel caso in cui il Candidato voglia successivamente certificarsi, il ripetersi dell'intero iter di certificazione, come dalla presente procedura CEPAS PG30 vigente.

La persona cui venga sospesa o annullata la certificazione non può far uso del certificato e dell'eventuale timbro CEPAS.