VERIFICA: GIOVANNI ZANVETTOR **APPROVA**: CARMINE CERRUTI

REV	NOTE DI MODIFICA	DATA
0	Prima emissione	16-06-2021

QUESTO DOCUMENTO È DISTRIBUITO			
	COPIA CONTROLLATA		COPIA NON CONTROLLATA
DESTINATARIO			

INDICE

1. Scopo e Validità

Scopo del presente Regolamento Tecnico è definire e stabilire l'iter e le regole per la gestione, il rilascio, la sorveglianza della Certificazione dei Sistemi di Gestione per la Sicurezza Informatica.

Il presente documento è da considerarsi supplementare, e quindi non sostitutivo, a quanto definito nel "Regolamento Generale di Certificazione"

Ai fini dell'accettazione del presente Regolamento è necessario che il Legale Rappresentante dell'Organizzazione firmi l'apposita parte prevista sull'offerta economica e, nel caso di offerta emessa dal Business Partner, sul contratto, anche mediante l'utilizzo della propria firma elettronica.

2. Modifiche del presente Regolamento

Eventuali variazioni delle norme di riferimento, delle prescrizioni degli Organismi di Accreditamento, del presente Regolamento, saranno comunicate da SI Cert all'Organizzazione certificata, che avrà la facoltà di adeguarsi alle nuove prescrizioni entro i tempi e con le modalità definiti nella comunicazione o di rinunciare alla Certificazione in accordo con quanto previsto nel Regolamento Generale.

Qualora l'Organizzazione certificata non rifiuti formalmente di adeguarsi, le nuove prescrizioni si intenderanno accettate. L'eventuale rifiuto deve essere inviato per iscritto con conferma di ricezione (o a mezzo PEC) entro quindici giorni dal ricevimento della comunicazione delle variazioni.

Eventuali variazioni del presente regolamento entreranno in vigore secondo una procedura che preveda tempi e modalità tali da garantire l'imparzialità.

SI Cert, nel caso di variazioni delle norme di riferimento, si riserva il diritto di verificare la conformità dell'adeguatezza dell'Organizzazione alle nuove prescrizioni della normativa attraverso un Audit.

3. Definizioni, Acronimi e Sinonimi

Le definizioni utilizzate dal presente Regolamento sono quelle riportate nelle norme di riferimento.

In generale nel proseguo del presente documento saranno usati questi Acronimi e Sigle:

- SGSI (ISMS): acronimo di Sistema di Gestione per la Sicurezza Informatica (Information Security management System)
- SI Cert: sinonimo di SI CERT ITALI srl
- OdA: acronimo di Organismi di Accreditamento o Organismo di Accreditamento
- Sistema di Certificazione: sinonimo di certificazione del sistema di gestione, certificazione di prodotto/Servizio, certificazione di Processo
- EA: Acronimo di European co-operation for Accreditation, è un'associazione senza scopo di lucro, registrata nei Paesi Bassi. È formalmente nominato dalla Commissione europea nel regolamento (CE) n. 765/2008 per sviluppare e mantenere un accordo multilaterale di riconoscimento reciproco, l'EA MLA, basato su un'infrastruttura di accreditamento armonizzata.
- IAF: acronimo di International Accreditation Forum è l'associazione mondiale che raggruppa gli organismi che svolgono l'accreditamento della valutazione di conformità e altri organismi interessati alla valutazione di conformità per quanto riguarda sistemi di gestione, prodotti, servizi, risorse umane ed altri ambiti similari.

Laddove necessario, ai fini di una migliore comprensione del presente Regolamento, talune altre definizioni o significati di alcuni termini e/o locuzione, sono riportate contestualmente all'utilizzo del termine o della locuzione stessa.

4. Campo di Applicazione

Il campo di applicazione del presente Regolamento si riferisce alla certificazione dei Sistemi di Gestione per la Sicurezza Informatica secondo la norma:

ISO/IEC 27001 Sistema di Gestione Sicurezza Informatica

E le relative line guida

ISO/IEC 27701 Sistema di Gestione Sicurezza delle informazioni sulla privacy

ISO/IEC 27017 Sistema di Gestione Sicurezza Informatica per i servizi cloud

ISO/IEC 27018 Sistema di Gestione Sicurezza Informatica PRIVACY nel cloud

Nelle edizioni correnti e descrive le procedure applicate da SI Cert per la Certificazione dei SGSI

5. Generalita'

5.1. Requisiti per la Certificazione

L'Organizzazione richiedente la Certificazione deve:

a) avere un Sistema di Gestione per la Sicurezza delle Informazioni attivo da almeno tre mesi che rispetti i requisiti della normativa di riferimento e delle eventuali prescrizioni particolari stabilite di legge per tipologia di prodotto/processo/servizio incluso nel campo di applicazione;
b) avere effettuato un ciclo completo di Verifiche Ispettive Interne ed un Riesame della Direzione;
c) mantenere a disposizione di SI Cert le registrazioni di tutti i reclami ricevuti e delle relative azioni conseguenti;

d) mantenere aggiornata la raccolta delle norme, leggi e regolamenti cogenti applicabili all'attività, processo, servizio, prodotto incluso nel campo di applicazione della Certificazione.

5.2. Emissione e Validità del Certificato

Il Certificato è emesso a fronte del completamento, con esito positivo, dell'Audit Iniziale, il mantenimento della sua validità è subordinato al superamento degli Audit di Sorveglianza periodici annuali e ad una completa rivalutazione (Audit di Rinnovo) ogni 3 anni entro il termine della scadenza.

5.3. Subentro ad altro Ente

Qualora la richiesta di Certificazione provenga da Organizzazioni già certificate e con Certificato in corso di validità, SI Cert subentra nelle attività in accordo con quanto previsto nel Regolamento Generale.

5.4. Modalità di conduzione degli Audit

Gli Audit preferibilmente debbono essere condotti "in campo" (ossia presso la sede dell'Organizzazione) ma, se la situazione lo richiede, possono essere eseguiti in toto o in parte da remoto in accordo con quanto già previsto nel relativo paragrafo del Regolamento Generale.

Prima dell'esecuzione di ogni Audit, SI Cert comunica all'Organizzazione i nomi del Gruppo di Audit che condurrà la valutazione e nello stesso momento indica l'eventuale documentazione che dovrà essere resa disponibile al Gruppo.

L'Organizzazione per la corretta esecuzione dell'Audit deve assicurare la presenza del Personale avente responsabilità per le Aree/Funzioni oggetto di Audit che hanno rilevanza nell'efficace funzionamento dei processi e delle attività rilevanti del Sistema stesso.

Per ogni Audit sono previste:

- una riunione iniziale tra il Gruppo di Audit e l'Organizzazione finalizzata alla presentazione delle parti e all'illustrazione delle procedure di Audit
- l'Audit in campo ed a campione della conformità del Sistema di Gestione dell'Organizzazione ai requisiti della norma di riferimento e della presa in carico delle prescrizioni legali riferibili al campo di applicazione della Certificazione
- la redazione del rapporto finale (Audit Report) con i risultati e le conclusioni della verifica e l'eventuale pianificazione delle attività successive
- una riunione di chiusura tra il Gruppo di Audit e l'Organizzazione per illustrare l'esito della verifica e consegnare l'Audit Report.

Durante la riunione di chiusura, ove lo ritenesse necessario, l'Organizzazione può confrontarsi con il GA sui contenuti del documento, sul prosieguo delle attività e sulle azioni da intraprendere. Alla riunione di chiusura per conto dell'Organizzazione deve essere sempre presente la Direzione e tutti i Responsabili di Area/Funzione/Processo che hanno rilevanza nell'efficace funzionamento dei processi e delle attività rilevanti del Sistema stesso.

Il contenuto della registrazione dell'Audit lasciata dal GA è da considerarsi come comunicazione ufficiale dei risultati dell'Audit da parte della Direzione di SI Cert (a meno che la stessa non faccia pervenire comunicazioni contrarie entro il termine temporale indicato sul documento stesso).

L'Organizzazione, entro il giorno successivo al termine delle attività di Audit, deve inoltrare via fax o e-mail a SI Cert, la registrazione dell'Audit lasciata dal GA al termine della riunione di chiusura dell'Audit, allegando, qualora previsto, la documentazione richiesta.

Eventuali Rilievi che dovessero emergere al termine dell'Audit devono essere prese in carico dall'Organizzazione e la loro gestione comunicata a SI Cert (tramite le modalità indicate nell'Audit Report in funzione della tipologia del Rilievo).

Quest'ultimo deve essere approvato dal Responsabile del Gruppo di Audit prima di proseguire con le successive fasi del processo di Certificazione.

Nell'eventualità l'Organizzazione intenda avvalersi della possibilità di formulare proprie riserve, l'iter di certificazione si sospende fino alla ricezione delle riserve ed alla risoluzione positiva o negativa delle stesse.

L'intenzione di formulare riserve sull'operato del GA o sui contenuti dei documenti dallo stesso redatti e letti all'Organizzazione (Rapporto di Audit), deve essere comunicata al RGA al termine della lettura del documento. L'Organizzazione può formulare le proprie riserve entro 15 giorni dalla fine delle attività di Audit o dalla ricezione di eventuali comunicazioni da parte di SI Cert.

L'iter di certificazione si chiude negativamente nel caso l'esito delle attività di Audit sia negativo, o nel caso di "risoluzione negativa" delle riserve esposte dall'Organizzazione.

Nel corso dell'Audit sono anche verificati l'uso del Marchio SI Cert e degli OdA qualora fossero già nelle disponibilità dell'Organizzazione in accordo a quanto previsto nel Regolamento uso del Marchio.

6. Audit Preliminare

Prima dell'Audit Iniziale è possibile effettuare un Audit preliminare (Pre-Audit), indipendente dall'iter di certificazione.

Questo tipo di Audit è facoltativo e mira a verificare il grado di implementazione del Sistema di Gestione dell'Organizzazione prima dell'Audit di

Certificazione dello stesso, in relazione ai requisiti della norma e di identificare quelle situazioni che potrebbero compromettere il buon esito dell'Initial Audit. È effettuato soltanto dopo espressa richiesta dell'Organizzazione alle condizioni riportate nell'offerta appositamente emessa, ed è sempre erogato/eseguito a titolo oneroso.
Può essere condotto un solo Pre-Audit per ogni Richiesta di Certificazione avente una durata proporzionale alle dimensioni dell'Organizzazione

7. AUDIT INIZIALE

L'audit Iniziale è suddiviso in due momenti di valutazione la cui durata ed estensione dipendono dalle dimensioni e dalle caratteristiche dell'Organizzazione nonché dalla presenza di eventuali sedi secondarie o cantieri (così come previsto dai requisiti degli OdA):

- Stage 1 Audit finalizzato alla verifica della documentazione e della pianificazione del Sistema di Gestione per la Sicurezza nonché alla programmazione dello Stage 2
- Stage 2 Audit avente come scopo la valutazione dell'adeguatezza e conformità del Sistema di Gestione per la Sicurezza.

Lo Stage 2 può essere effettuato solo dopo il completamento dello Stage 1 e deve aver luogo entro e non oltre nove mesi dalla prima verifica altrimenti questa deve essere ripetuta.
Nel caso di integrazione alla ISO/IEC 27017 ("servizi cloud") oppure alle ISO/IEC27017 e ISO/IEC 27018 ("Privacy nel cloud") prima del rilascio della certificazione, salvo diverse disposizioni degli OdA, devono essere verificati tutti i Data Center presso cui sono dislocati i server che gestiscono il cloud; qualora i Data Center utilizzati per le attività "cloud" siano in outsourcing presso fornitori in possesso di certificazioni ISO/IEC 27001, ISO/IEC 27017 (e ISO/IEC 27018) accreditate e riconosciute a livello MLA, o nel caso di Data Center in possesso di certificazioni TIER III o TIER IV ove non fosse possibile svolgere un audit diretto, potrà essere utilizzata la sola valutazione documentale degli aspetti contrattuali e di controllo operativo con tali fornitori.
Nel caso di integrazioni alla ISO/IEC 27701 ("Privacy Information Management System") prima del rilascio della certificazione, salvo diverse disposizioni degli OdA, si dovrà 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).

7.1. AUDIT DI PRIMO STAGE (S1)

Questo Audit viene effettuato, generalmente presso la sede dell'Organizzazione, secondo la comunicazione inviata da SI Cert e ha lo scopo di verificare la correttezza dei dati forniti dall'Organizzazione, predisporre in sintonia con l'Organizzazione il successivo Audit di Certificazione (Audit di Secondo Stage S2) e fornire al Gruppo di Audit un'esatta situazione delle attività e dei siti da sottoporre a certificazione con particolare attenzione a verificare che:

- esistano eventuali processi o aree che necessitano di particolari attenzioni;
- la corretta stesura e applicazione del Sistema di Gestione per la Sicurezza delle Informazioni in conformità alla norma e alle eventuali relative linee guida che l'Organizzazione intende adottare (o alle norme prese a riferimento nel caso di Sistemi di Gestione Integrati);
- i dati forniti dall'Organizzazione in fase di richiesta di offerta economica, al fine di pianificare correttamente le successive attività di Secondo Stage (ad esempio: sedi dichiarate, dimensioni in termini di forza lavoro che ha incidenza sul Sistema o sul prodotto/servizio realizzato, incluse eventuali attività di outsourcing, numero siti produttivi e/o unità produttive o operative, e/o cantieri, orari e/o turni di lavoro);
- la Dichiarazione relativa al "Campo di Applicazione" definisca in modo chiaro, completo e circoscritto l'ambiente fisico (uffici e/o edifici e/o siti etc), il dominio logico (lan, campus, wan e relative apparecchiature) e la struttura organizzativa (processi/attività interne e/o svolte dai fornitori) rispetto al quale si richieda la certificazione;
- la Politica e gli Obiettivi per la Sicurezza definiti siano appropriati all'organizzazione e ai suoi traguardi di business, sia legali sia contrattuali; Politica ed Obiettivi siano approvati dalla Direzione ed inoltre siano attuati opportuni meccanismi per il loro riesame e aggiornamento
- esista e sia applicata la procedura di valutazione e gestione dei rischi; così come previsto dallo standard di riferimento
- la Dichiarazione di Applicabilità sia documentata, congruente con la politica, il campo di applicazione e i risultati della Gestione del Rischio;
- siano motivate e documentate le decisioni riguardanti la scelta di implementare o escludere alcuni dei controlli elencati nella norma di riferimento nonché l'esistenza di collegamenti con documenti di attuazione;
- siano fissate le responsabilità e le interfacce tra i processi interni ed esterni al campo di applicazione (compresi quelli messi in atto da eventuali fornitori) nonché gli accordi sui livelli di servizio garantiti;
- siano elencate e prese in carico dall'organizzazione le norme, e leggi e i regolamenti applicabili (comprese autorizzazioni, implicazioni normative o regolamenti aggiuntivi/inusuali per il settore siano essi volontari ovvero imposti dai propri clienti);
- sia documentata la configurazione di rete;
- esista la planimetria del sito che identifichi le aree sicure e che sia, preferibilmente, comprensiva degli impianti elettrici e meccanici di supporto;

- esistano adeguati obiettivi per la Sicurezza e questi siano supportati da una programmazione e, ove possibile, da una pianificazione tecnica e finanziaria;
- gli obiettivi per la sicurezza e relativi indicatori siano coerenti con la valutazione dei rischi e con la politica per la sicurezza per l'esercizio dell'attività l'Organizzazione sia in possesso di tutte le necessarie licenze relative al software applicativo impiegato;
- gli Audit interni e il Riesame da parte della Direzione siano stati pianificati almeno con cadenza annuale, eseguiti e che il livello di attuazione del Sistema di Gestione fornisca l'evidenza che l'Organizzazione è pronta per lo Stage 2 Audit;
- il Sistema di Gestione tenga traccia e risponda alle principali istanze delle parti interessate riguardo la Sicurezza delle Informazioni;
- ad ogni operatore significativo per la sicurezza delle informazioni sia stato affidato un ruolo chiaro, ben definito e noto, con la chiara definizione delle relative responsabilità per la Sicurezza delle Informazioni;
- il piano di formazione ed informazione delle risorse umane sia definito in base alla relativa analisi delle esigenze ed attuato (o ne sia stata prevista l'attuazione);
- sia stata definita una Procedura per l'analisi delle Non Conformità, degli eventi e delle azioni che potrebbero avere un impatto sull'efficacia e/o sulle prestazioni del sistema di gestione e che tale procedura sia idonea a determinare le cause degli stessi eventi, al fine di predisporre, ove necessario, le opportune Azioni Correttive.

Nel caso di estensione alla/e ISO/IEC 27017 ("servizi cloud") oppure alle ISO/IEC27017 e ISO/IEC 27018 ("Privacy nel cloud")

- la presenza di accordi contrattuali con gli eventuali outsorcers a cui sono appoggiati i servizi Cloud e le relative certificazioni possedute.

Nel caso di estensione alla ISO/IEC 27701 ("Privacy Information Management System"):

- la presenza di rapporti di Vulnerability Assessement e Penetretion Test e le qualifiche dei laboratori che li hanno condotti;
- la presenza di accordi contrattuali con gli eventuali outsorcers fornitori dei Data Center e le relative certificazioni possedute.

Di estrema importanza, in questa fase, verificare che non esistano eventuali registrazioni del SGSI o siti inclusi nello scopo che non possono essere rese/i disponibili per la verifica da parte del Gruppo di Verifica perché contengono informazioni riservate o sensibili ovvero per motivi di sicurezza. In caso si dovrà stabilire se il sistema di gestione potrà essere adeguatamente verificato anche nel caso di assenza di accesso a questi record/siti. Qualora si concluda che non sia possibile verificare adeguatamente il SGSI, si informerà l'organizzazione che l'audit di certificazione non potrà aver luogo se non verranno concesse modalità di accesso adeguate oppure apportando modifiche al campo di applicazione.

Le risultanze dello Stage 1 Audit saranno documentate nell'Audit Report e comunicate all'Organizzazione dal Gruppo di Audit, compresa l'identificazione di ogni rilievo che nello Stage 2 Audit potrebbe essere classificato come Non Conformità) e quindi, concordare/pianificare con l'Organizzazione il prosieguo delle attività, definendo in particolare la data per l'esecuzione dell'Audit S2 ed individuando i turni di lavoro, le eventuali sedi e gli eventuali siti operativi esterni coinvolti dall'Audit S2 e scelti tra quelli comunicati dall'Organizzazione in fase di richiesta/accettazione offerta economica.

7.2. Audit di Secondo Stage (S2) o di Certificazione

L'Audit di Secondo Stage (S2) è eseguito soltanto in caso di esito positivo dell'Audit S1 ed è effettuato secondo la pianificazione concordata con l'Organizzazione alla fine dell'Audit S1 ed ha lo scopo di valutare il grado di adeguatezza ed applicazione dell'intero SGSI implementato dall'Organizzazione.

Durante lo Stage 2 Audit è prevista la valutazione che:

- siano stati presi in carico e risolti i Rilievi emersi durante lo Stage 1 Audit
- l'Organizzazione attui le proprie politiche, obiettivi e procedure;
- il Sistema di Gestione sia conforme a tutti i requisiti dello standard di riferimento (e alle eventuali linee guida che si è deciso di integrare), agisca nel rispetto delle prescrizioni legali applicabili e stia raggiungendo gli obiettivi di politica dell'Organizzazione
- il comportamento dell'Organizzazione, nell'ambito di eventuali iter autorizzativi o prescrizioni che non siano risultati completati al momento dello Stage 1 Audit
- le informazioni che consentano di confermare il campo di applicazione
- l'Organizzazione tenga sotto controllo i processi compresi nel campo di applica.zione e applichi i controlli selezionati
- gli Audit interni ed il Riesame della Direzione siano stati effettuati

La pratica è sottoposta all'analisi della Funzione Deliberante per la decisione sulla certificabilità o meno del Sistema di Gestione dell'Organizzazione in accordo con quanto previsto nel Regolamento Generale, soltanto dopo che eventuali NC (maggiori o minori) sono risolte ed in seguito alla comunicazione/conferma all'Organizzazione dell'accettazione dei contenuti riportati sui documenti di Audit da parte della Direzione Tecnica o suo incaricato.

8. Certificato

Il certificato ha valdità triennale a partire dalla data della decisione per la certificazione e durante il periodo di validità è sottoposto, secondo le

modalità di seguito riportate, a 2 verifiche, denominate Audit di Sorveglianza, sulle condizioni di mantenimento della relativa validità.
Alla scadenza è eseguito uno specifico Audit (audit di rinnovo) per rinnovare la certificazione per un ulteriore triennio. Tale Audit di Rinnovo è effettuato se l'Organizzazione intende rinnovare con SI CERT ITALY srl la propria certificazione per un ulteriore trienno, fatto salvo previsto dal presente Regolamente in materia di recesso contrattuale.

9. AUDIT DI SORVEGLIANZA

Gli Audit di Sorveglianza consistono:

- 1° Audit , successivo alla certificazione iniziale o Rinnovo, entro 12 mesi dalla data decisione sulla certificazione;
- 2° Audit di Sorveglianza entro 24 mesi dalla data decisione della certificazione, salvo casi particolari di volta in volta esaminati da SI CERT ITALY srl come di seguito riportato.

Il 1° Audit di sorveglianza successivo alla certificazione iniziale deve essere effettuato tassativamente entro massimo 12 mesi dalla data decisione sulla certificazione.
La modifica delle frequenze, della numerosità e dell'estensione degli Audit di Sorveglianza può essere dovuta a richieste, opportunamente motivate, da parte dell'Organizzazione (le quali sono esaminate dalla Direzione Tecnica ed eventualmente dalla Funzione Deliberante di SI Cert per approvazione) oppure richieste da SI Cert.
In entrambi i casi SI Cert da comunicazione formale delle decisioni prese all'Organizzazione. Nel caso quest'ultima non sia concorde con la decisione presa, può fare ricorso, rinunciare alla certificazione o vedersi il certificato sospeso/revocato d'ufficio (si vedano paragrafi specifici nel Regolamento Generale).
Per le casistiche, modalità e costi fare riferimento al Regolamento Generale paragrafi "Audit Supplementari" e "Reclami, Ricorsi e Contenziosi".
Ciascun Audit di Sorveglianza riguarda una parte del Sistema di Gestione interessato, ed i 2 Audit di Sorveglianza nel loro insieme assicurano il riesame completo del Sistema di Gestione nel triennio successivo alla certificazione.
L'Audit di Sorveglianza è eseguito secondo la pianificazione in precedenza comunicata all'Organizzazione, che tiene conto della necessità di verificare la risoluzione delle NC minori rilevate durante l'Audit precedente e l'efficacia delle relative azioni correttive, a cui si aggiunge la verifica degli elementi necessari per il mantenimento della certificazione secondo il piano già in possesso dell'Organizzazione:
Nell'eventualità lo ritenga necessario, il GA durante lo svolgimento della Audit di Sorveglianza può andare a verificare anche requisiti e/o aspetti non previsti nel programma iniziale o nella pianificazione comunicata all'Organizzazione.

10. AUDIT DI RINNOVO

La validità del Certificato è confermata a seguito dell'esito positivo di una verifica completa (Audit di Rinnovo o Re-Audit) condotta con gli stessi criteri dello Stage 2 Audit.
La verifica di rinnovo può non prevedere l'esecuzione dello Stage 1 Audit salvo che non siano intervenute modifiche importanti all'Organizzazione o al suo Sistema di Gestione tali da richiederne l'effettuazione.
L'audit di Rinnovo deve essere effettuato entro la data di scadenza del certificato in vigore e con anticipo sufficiente per poter gestire anche la possibilità che, in caso di Non Conformità Maggiori, rimanga il tempo necessario per valutare l'efficacia del trattamento e deliberarne il rinnovo.
Qualora non si riesca a completare l'iter entro i tempi previsti, si procederà con la Revoca del Certificato. In quest'ultimo caso l'Organizzazione che desideri nuovamente ottenere la Certificazione dovrà riattivare l'iter effettuando un nuovo Audit Iniziale.
Eventuali eccezioni a quanto sopra riportato saranno gestite da SI Cert in rispetto delle disposizioni e direttive degli Organismi di Accreditamento e in conformità ai documenti EA/IAF applicabili al presente schema di certificazione.

11. AUDIT SUPPLEMENTARI

Gli Audit Supplementari (così come già definiti all'omonimo paragrafo del Regolamento Contrattuale) è eseguito con le stesse modalità dello Stage 2 Audit. Qualora l'Audit Supplementare effettuato per la verifica dell'efficacia del trattamento delle Non Conformità Maggiori abbia esito negativo, la Certificazione sarà sospesa fino a che non sia stata valutata l'efficacia del nuovo trattamento, e comunque per un periodo massimo di sei mesi, trascorsi i quali la Sospensione si trasformerà in Revoca (Regolamento Contrattuale paragrafi "Sospensione" e "Revoca").

12. CLASSIFICAZIONE E GESTIONE RILIEVI

Durante l'esecuzione degli Audit possono essere riscontrati i seguenti rilievi

12.1. NON CONFORMITÀ MAGGIORI

Sono tutte quelle anomalie che scaturiscono da un mancato soddisfacimento, completo o parziale, di un requisito della norma di riferimento (assoluta mancanza della documentazione e/o non applicazione) oppure di un requisito legislativo o di un requisito contrattuale del Committente, riscontrate con evidenze oggettive, che influiscono in modo significativo sulla conformità del Sistema di Gestione, cioè che impediscono in modo costante e continuativo la sistematica e corretta applicazione della parte di Sistema risultata carente, ma soprattutto che

non permettano il soddisfacimento dei requisiti relativi al prodotto/processo/servizio, siano tecnici sia legali.

L'Organizzazione deve provvedere quindi a definire le modalità di correzione di tali NC maggiori e le azioni intraprese come azioni correttive per eliminare le cause che le hanno determinato con le relative tempistiche, compilando la modulistica prevista. In particolare il termine entro cui presentare la proposta di risoluzione è al massimo di 10 giorni lavorativi. Infine, l'Organizzazione deve inoltrare secondo le modalità e tempistiche concordate con il RGA al termine dell'Audit, tutta la documentazione necessaria attestante l'avvenuto trattamento delle NC e l'efficacia delle azioni correttive attuate. Il termine entro cui chiudere le NC maggiori è al massimo di 3 mesi.

Le NC maggiori riscontrate durante l'Audit di Certificazione determinano la mancata presentazione del fascicolo dell'Organizzazione alla Funzione Deliberante fintanto che queste non sono risolte, mentre, per quelle riscontrate in fase di Audit di Sorveglianza se, scaduto il termine di 3 mesi per la loro risoluzione, queste non sono chiuse, scatta la sospensione del certificato per 6 mesi, oppure, nel caso le NC maggiori siano chiuse prima, fino al momento della loro effettiva chiusura. Trascorsi inutilmente i 6 mesi il certificato viene revocato.

L'Audit della risoluzione (correzione) delle NC maggiori può avvenire:

- su base documentale,
- mediante apposito Audit Supplementare che viene effettuato alle condizioni economiche riportate in Offerta.

Per l'Audit della correzione delle NC maggiori su base documentale, il RGA valuta la documentazione inviata dall'Organizzazione per dimostrare la completa correzione delle NC maggiori e, nel non fosse ritenuta soddisfacente, il RGA provvede alla richiesta di integrazioni all'Organizzazione. Solo alla ricezione di documentazione ritenuta soddisfacente che dia piena confidenza della correzione delle NC maggiori, il RGA provvede al completamento delle apposite sezioni dei documenti utilizzati per questa attività e all'inoltro degli stessi alla Direzione Tecnica di SI Cert che, dopo averli verificati ed averne accettato i contenuti, provvede all'invio degli stessi all'Organizzazione.

Per l'Audit della correzione delle NC maggiori mediante Audit Supplementare, SI Cert provvede ad eseguire l'Audit secondo quanto indicato dal GA nei propri documenti e concordato con l'Organizzazione al termine dell'Audit (ad esempio: Audit limitato alle sole NC maggiori o Audit su tutti i requisiti del Sistema di Gestione) ed alle condizioni economiche riportate in Offerta.

12.2. Non Conformità Minori

Sono tutte quelle anomalie riscontrate con evidenze oggettive che influiscono in modo non significativo sulla conformità del Sistema di Gestione e che non inficiano il prosieguo dell'iter di certificazione e/o il mantenimento della stessa. Tali anomalie, che generalmente sono casuali, non ripetitive e non strutturali, non impediscono la sistematica e corretta applicazione della parte di sistema risultata carente.

Per le NC minori riscontrate durante le attività di Audit, il RGA al termine dell'Audit concorda con l'Organizzazione la tempistica e la modalità per la correzione delle stesse. L'Organizzazione deve provvedere quindi a definire le modalità di correzione di tali NC maggiori e le azioni intraprese come azioni correttive per eliminare le cause che le hanno determinato con le relative tempistiche, compilando la modulistica prevista. In particolare, il termine entro cui presentare la proposta di risoluzione delle stesse è al massimo di 30 giorni solari.

La verifica della correzione delle NC minori può avvenire:

- tramite accettazione della proposta di risoluzione da parte del RGA e quindi verifica della effettiva attuazione ed efficacia durante il successivo Audit di Sorveglianza,
- mediante apposito Audit Supplementare, nel caso durante gli Audit dovessero essere rilevate un numero elevato di NC minori.

Per la verifica della correzione delle NC minori tramite la sola proposta di risoluzione, il RGA valuta la/le proposta/e di correzione inviata/e dall'Organizzazione e, nel non fosse/fossero ritenuta/e soddisfacente/i, il RGA provvede alla richiesta di integrazioni all'Organizzazione. Solo alla ricezione di documentazione ritenuta soddisfacente, il RGA provvede al completamento delle apposite sezioni dei documenti utilizzati per questa attività e all'inoltro degli stessi alla Direzione Tecnica di SI Cert che, dopo averli verificati ed averne accettato i contenuti, provvede all'invio degli stessi all'Organizzazione.

Durante il successivo Audit di Sorveglianza e/o Rinnovo, il GA provvede a verificare l'effettiva chiusura delle NC minori. Nel caso queste non siano state trattate o chiuse efficacemente, sono rilanciate aumentandole di peso (NC maggiore), mentre nel caso in cui siano parzialmente chiuse o non efficacemente chiuse, sono rilanciate con lo stesso peso.

Per la verifica della correzione delle NC minori mediante Audit supplementare, SI Cert provvede ad eseguire l'Audit secondo quanto indicato dal GA nei propri documenti e concordato con l'Organizzazione al termine dell'Audit (ad esempio Audit limitato alle sole NC minori o Audit su tutti i requisiti del Sistema di Gestione) ed alle condizioni economiche riportate in Offerta.

Nel caso queste non siano state trattate o chiuse efficacemente, sono rilanciate aumentandole di peso (NC maggiore), mentre nel caso in cui siano parzialmente chiuse o non efficacemente chiuse, sono rilanciate con lo stesso peso

12.3. Raccomandazioni

Sono quei rilievi che non possono essere considerati NC minori, ma che possono dare un apporto migliorativo all'efficacia del Sistema di Gestione implementato dall'Organizzazione e alla sua capacità di soddisfare in modo efficace ed efficiente i requisiti generali della norma di riferimento.

L'Organizzazione non ha l'obbligo di recepire le raccomandazioni formulate dal GA, ma deve dare evidenza, tramite un riesame delle stesse in forma documentata ed entro breve temine dalla fine dell'Audit (massimo 1 mese), di averle analizzate. Nel caso in cui non dovesse ritenere necessario recepire le raccomandazioni, l'Organizzazione, nella registrazione del riesame delle stesse, deve spiegare i motivi di tale decisione. Durante il successivo Audit di Sorveglianza e/o Rinnovo, il GA provvede a verificare l'effettiva analisi delle raccomandazioni. Per quelle raccomandazioni che l'Organizzazione ha recepito, il GA provvede a verificare l'effettiva applicazione della decisione intrapresa. Nel caso in cui questa non sia stata applicata o chiusa, la raccomandazione è rilanciata aumentandola di peso in NC minore. Nel caso in cui sia parzialmente applicata e/o chiusa la raccomandazione viene rilanciata con lo stesso peso.