

**INDICE**

1. SCOPO E CAMPO DI APPLICAZIONE .....	2
2. REQUISITI ESSENZIALI RISPETTO AI QUALI È RICHIESTA LA VALUTAZIONE .....	2
3. REQUISITI ESSENZIALI RELATIVI AL PROCESSO DI VALUTAZIONE .....	2
4. SOSPENSIONE, REVOCA O RIDUZIONE DELLA CERTIFICAZIONE .....	4
5. USO DEL MARCHIO E DEL CERTIFICATO DI CONFORMITÀ .....	5

Convalida: Direzione Generale *Ing. Rodolfo Trippodo* \_\_\_\_\_

Approvazione: Presidente Comitato di Indirizzo e Controllo *Ing. Gianni Rigamonti* \_\_\_\_\_

## 1. SCOPO E CAMPO DI APPLICAZIONE

I requisiti espressi nel presente documento fanno parte integrante del contratto di valutazione della conformità DSC 05 e dell'offerta economica che li richiama.

Tali requisiti, sono riferiti unicamente agli aspetti specificatamente connessi al campo di applicazione della certificazione richiesta.

## 2. REQUISITI ESSENZIALI RISPETTO AI QUALI È RICHIESTA LA VALUTAZIONE

UNI CEI ISO IEC 27001 Tecnologia delle informazioni - Tecniche di sicurezza - Sistemi di Gestione della Sicurezza delle Informazioni - Requisiti

Le prescrizioni riportate nella norma sono da ritenersi tutte vincolanti ed applicabili, a meno che, esclusivamente nell'ambito dell'allegato A, vi siano prescrizioni relative a elementi gestionali non pertinenti alla natura dell'attività del cliente.

## 3. REQUISITI ESSENZIALI RELATIVI AL PROCESSO DI VALUTAZIONE

### 3.1 Premessa

La conformità legislativa sarà considerata da CERMET come un pre-requisito per il rilascio della certificazione del sistema di gestione della sicurezza delle informazioni.

Nella predisposizione del sistema di gestione, l'Organizzazione deve definire in via preliminare la mappatura delle informazioni critiche per i clienti e per la stessa Organizzazione, finalizzata alla definizione degli "asset", destinati a conservare, elaborare o trasmettere tali informazioni, in modo che le modalità di predisposizione della valutazione dei rischi per la sicurezza delle informazioni, trovino il loro punto di partenza dall'analisi dei processi di business e dalla criticità delle informazioni gestite.

#### 3.1.1 Verifica preliminare

Su richiesta dell'Organizzazione, dopo l'attivazione del servizio, è possibile effettuare una pre-verifica (verifica facoltativa), con l'obiettivo di valutare il grado di adeguatezza del sistema di gestione per la sicurezza delle informazioni, rispetto alla norma di riferimento, per i prodotti/servizi per i quali è richiesta la certificazione. I risultati di tale verifica sono espressi solo in termini di non conformità, non comportano da parte dell'Organizzazione la comunicazione a CERMET delle azioni correttive che intende intraprendere e non sono sottoposti ad analisi per il rilascio della certificazione.

#### 3.2 Verifica iniziale di certificazione

La verifica iniziale di certificazione è condotta in due stadi: Stadio 1 e Stadio 2.

##### 3.2.1 Stadio 1 (analisi documentale e verifica di stadio 1)

Tale verifica ha luogo presso la sede dell'Organizzazione, ed ha inizio con l'analisi della documentazione.

La documentazione da sottoporre ad analisi documentale è rappresentata da documenti specificati al cap. 4.3 della UNI CEI ISO IEC 27001.

Da tali documenti deve risultare chiaro ed univoco il campo di applicazione del Sistema di Gestione della Sicurezza delle Informazioni (SGSI); devono essere chiaramente individuate ed essere oggetto di valutazione dei rischi, eventuali interfacce con servizi o attività non pienamente inclusi nel campo di applicazione.

Il cliente deve mantenere per CERMET una copia ad aggiornamento controllato della propria documentazione del SGSI e renderla disponibile su richiesta, per tutto il periodo di validità del contratto e durante le attività di valutazione.

Al termine della verifica ispettiva di stadio 1, il Gruppo di Valutazione CERMET lascia copia del rapporto della verifica ispettiva, che il cliente sottoscrive.

Qualora entro 30 giorni lavorativi dal termine della verifica il cliente non riceva alcuna comunicazione, o in caso di ricezione della notifica di verifica di stadio 2 da parte di CERMET, il rapporto della verifica potrà considerarsi automaticamente confermato. Viceversa, se a seguito di analisi interna, CERMET dovesse ritenere opportune delle modifiche ai contenuti del rapporto, ne darà comunicazione formale all'Organizzazione, fornendo spiegazioni per ogni divergenza e indicazione delle azioni successive.

Per tutte le eventuali non conformità minori verbalizzate, l'Organizzazione deve analizzare e formalizzare le cause che le hanno generate, e definire in modo formale gli opportuni trattamenti e azioni correttive. Le evidenze

della chiusura delle non conformità minori saranno valutate dal CERMET in occasione della verifica di certificazione.

Nel caso di non conformità maggiori, l'Organizzazione deve inviare al CERMET la proposta dei trattamenti e delle azioni correttive entro 10 giorni lavorativi dal termine della verifica, queste dovranno essere risolte entro la fase successiva.

CERMET si riserva di richiedere l'invio del trattamento e del piano di azioni correttive, anche in caso di non conformità minori, in funzione del tipo e numero di non conformità e dei risultati complessivi dell'audit.

### 3.2.2 Verifica ispettiva per la Certificazione (VIC) o di Stadio 2

La verifica di certificazione o di stadio 2 viene sempre eseguita presso i luoghi ove si svolgono le attività oggetto di certificazione. Tale verifica è estesa a tutti i requisiti della norma e a tutti i prodotti/servizi e siti oggetto del presente contratto.

Lo stadio 2 è pianificato ad una distanza di tempo dallo stadio 1 tale da consentire all'Organizzazione la risoluzione dei rilievi emersi in stadio 1 e la corretta pianificazione dello stadio 2 da parte di CERMET.

In casi eccezionali e adeguatamente motivati, stabiliti da CERMET, si potranno organizzare i due stadi in momenti consecutivi, in tali casi qualora l'esito dello stadio 1 fosse negativo (non conformità maggiori), la verifica iniziale di certificazione sarà ugualmente portata a termine, ma si renderà necessaria l'effettuazione di una nuova verifica di stadio 2.

Il tempo massimo che può trascorrere tra lo stadio 1 e lo stadio 2, sarà stabilito da CERMET e deve essere tale da garantire che i risultati dello stadio 1 si mantengano validi, pertanto il sistema, l'Organizzazione, il contesto normativo e legislativo non devono subire variazioni significative tra i due stadi.

Nella fase iniziale della verifica per la concessione della certificazione, viene valutata la risoluzione dei rilievi notificati all'Organizzazione nelle fasi precedenti dell'iter. La chiusura delle eventuali non conformità maggiori costituisce elemento vincolante per la prosecuzione della verifica stessa. Eventuali non conformità minori non risolte devono essere riportate nel rapporto di verifica.

Al termine della verifica ispettiva, il Gruppo di Valutazione CERMET lascia copia del rapporto di verifica ispettiva, che il cliente sottoscrive.

Tale rapporto, viene sottoposto ad analisi ed approvazione interna da parte di CERMET, per la successiva delibera o meno di certificazione.

Nel caso di non conformità maggiori, il cliente deve inviare a CERMET la proposta di risoluzione e le azioni correttive. La pratica non potrà essere analizzata per la delibera, fino a ricezione delle proposte di risoluzione e azioni correttive delle non conformità maggiori. Inoltre prima del rilascio della certificazione, deve essere verificata la soluzione di tutte le non conformità maggiori secondo le modalità di valutazione stabilite da CERMET (verifica ispettiva presso il cliente e/o attraverso evidenze documentali). Tale valutazione deve essere effettuata al massimo entro 6 mesi dalla Verifica di Certificazione; in caso contrario si renderà necessaria l'intera rivalutazione del sistema di gestione per la sicurezza delle informazioni.

Per tutte le eventuali non conformità minori verbalizzate, l'Organizzazione deve analizzare, formalizzare le cause che le hanno generate, e definire in modo formale gli opportuni trattamenti e azioni correttive. Le evidenze della chiusura delle non conformità minori saranno valutate dal CERMET in occasione della verifica successiva.

CERMET si riserva di richiedere l'invio del trattamento e del piano di azioni correttive, anche in caso di non conformità minori, in funzione del tipo e numero di non conformità e dei risultati complessivi dell'audit.

Il periodo di validità del Certificato è di tre anni dalla data di rilascio o ultima riemissione.

Eventuali richieste di modifica dei contenuti del certificato devono essere inviate a CERMET in forma scritta e preventivamente alla prima attività di verifica utile.

### 3.3 Verifiche ispettive di sorveglianza (VIS)

Le verifiche ispettive di sorveglianza, sono effettuate entro e non oltre i 12 mesi dalla verifica precedente<sup>1</sup>. Esse vengono sempre eseguite presso i luoghi ove si svolgono le attività oggetto di certificazione.

Nel corso delle verifiche di sorveglianza è assicurata la valutazione della risoluzione delle non conformità emerse nelle precedenti verifiche, nonché la valutazione dell'attuazione e dell'efficacia delle conseguenti azioni correttive.

<sup>1</sup> La data della prima VIS (cioè la verifica di sorveglianza che segue la VIC) non deve superare i 12 mesi dall'ultimo giorno della VIC

Al termine della verifica ispettiva, il Gruppo di Valutazione CERMET lascia copia del rapporto della verifica ispettiva che il cliente sottoscrive.

Qualora entro 30 giorni lavorativi dal termine della verifica, il cliente non riceva alcuna comunicazione da parte di CERMET, il rapporto della verifica potrà considerarsi automaticamente confermato. Viceversa, se a seguito di analisi interna, CERMET dovesse ritenere opportune delle modifiche ai contenuti del rapporto, ne darà comunicazione formale all'Organizzazione, fornendo spiegazioni per ogni divergenza e indicazioni in merito alle azioni successive.

Per tutte le eventuali non conformità minori verbalizzate, l'Organizzazione deve analizzare, formalizzare le cause che le hanno generate, e definire in modo formale gli opportuni trattamenti e azioni correttive. Le evidenze della chiusura delle non conformità minori saranno valutate da CERMET in occasione della verifica successiva.

Nel caso di non conformità maggiori, l'Organizzazione deve inviare a CERMET la proposta dei trattamenti e delle azioni correttive entro 10 giorni lavorativi dal termine della verifica. CERMET entro 30 giorni lavorativi dal termine della verifica, analizzato il rapporto della verifica per conferma o meno dei suoi contenuti, comunicherà all'Organizzazione le azioni conseguenti (verifica ispettiva presso il cliente e/o verifica attraverso evidenze documentali). Tale verifica deve essere effettuata al massimo entro 6 mesi dalla precedente (CERMET potrà stabilire tempistiche più ristrette in base alla gravità e numero della non conformità verbalizzata).

Scaduti i termini massimi consentiti, se le motivazioni che giustificano l'impossibilità di effettuare la valutazione non influiscono sulla garanzia di conformità ai requisiti essenziali, la certificazione potrà essere sospesa (cfr. § 4), in caso contrario CERMET potrà stabilire la rescissione dal contratto (rif. Contratto di valutazione della conformità DSC 05).

CERMET si riserva di richiedere l'invio del trattamento e del piano di azioni correttive, anche in caso di non conformità minori, in funzione del tipo e numero di non conformità e dei risultati complessivi dell'audit.

Le attività di sorveglianza, oltre alla verifica ispettiva in campo, possono comprendere ad esempio:

- a) richieste al cliente certificato circa aspetti attinenti alla certificazione;
- b) riesame delle dichiarazioni del cliente riguardo le proprie attività (per esempio materiale promozionale, sito web);
- c) richieste al cliente di fornire documenti e registrazioni (su mezzi cartacei o elettronici).

Tali altre forme di monitoraggio possono essere applicate da CERMET, in funzione di: informazioni ricevute dall'esterno, esito delle verifiche, input da parte dell'Organismo di Accreditamento ecc.

### **3.4 Verifica ispettiva di Rinnovo (VIR)**

Entro il terzo anno dalla verifica ispettiva di certificazione CERMET esegue una verifica ispettiva orientata al riesame generale del sistema di gestione per la sicurezza delle informazioni, all'analisi della sua efficacia e delle sue prestazioni nell'arco del periodo di certificazione e comprende anche il riesame dei risultati dei precedenti rapporti di audit di sorveglianza. A tal fine la verifica è estesa a tutti i requisiti della norma e a tutti i prodotti/servizi oggetto del presente contratto. Essa viene sempre eseguita presso i luoghi ove si svolgono le attività oggetto di certificazione.

CERMET decide se rinnovare o meno, sulla base dei risultati dell'audit di rinnovo, dei risultati del riesame delle prestazioni dell'intero sistema nel periodo di certificazione e dei reclami ricevuti dagli utenti della certificazione

La verifica di rinnovo può essere preceduta (a discrezione di CERMET) da una verifica di Stadio 1, qualora si siano verificate modifiche significative al Sistema di Gestione o al contesto legislativo/normativo di riferimento, tale verifica sarà gestita secondo quanto indicato al precedente § 3.2.1.

La gestione dei risultati della verifica avviene secondo le stesse modalità descritte al precedente § 3.4. Nel caso in cui siano state rilevate non conformità maggiori, qualora non sia possibile verificarne la risoluzione entro la scadenza del certificato, CERMET deciderà per la sospensione della certificazione (cfr. § 4) o nei casi più gravi CERMET potrà stabilire la rescissione dal contratto (rif. Contratto di valutazione della conformità DSC 05)

Non è consentito lo slittamento della data della verifica di rinnovo oltre la data di scadenza del certificato.

A seguito del rinnovo viene aggiornata la validità del certificato di conformità.

#### 4. SOSPENSIONE, REVOCA O RIDUZIONE DELLA CERTIFICAZIONE

La Certificazione può essere sospesa, revocata o ridotta:

- su richiesta del cliente;
- su decisione di CERMET, in caso di: mancato rispetto da parte del cliente delle condizioni contrattuali, dei requisiti essenziali, delle condizioni economiche concordate con CERMET, o in caso di variazione dei termini contrattuali attuata senza l'approvazione di CERMET.

Salvo casi eccezionali (stabiliti comunque da CERMET) Il periodo di sospensione non può durare oltre sei mesi, in caso contrario si procede alla rescissione dal contratto (rif. Contratto di valutazione della conformità DSC 05).

Durante il periodo di sospensione il cliente perde il diritto di utilizzo del Marchio di Certificazione CERMET e del certificato e viene cancellato dagli elenchi delle organizzazioni certificate. Le condizioni per il ripristino della certificazione sospesa (comprese le necessarie attività di valutazione della conformità), saranno stabilite da CERMET in base alle motivazioni che hanno portato alla sospensione e in base alla durata della sospensione.

Qualora il cliente non metta in atto le azioni indicate da CERMET per il ripristino della certificazione sospesa, il contratto cesserà di essere valido (rif. DSC 05 - Contratto di valutazione della conformità § 10) e la certificazione sarà revocata ovvero, nei casi possibili, ne sarà ridotto il campo di applicazione.

La riduzione della certificazione comporta la riemissione di un nuovo certificato, indicante il campo di applicazione per cui la certificazione è rimasta valida, e il ritiro del vecchio certificato. Il cliente inoltre dovrà tempestivamente adeguare tutte le forme di comunicazione e pubblicità della certificazione al nuovo campo di applicazione.

A seguito di revoca della certificazione, l'Organizzazione perde il diritto di utilizzo del Marchio di Certificazione CERMET e viene cancellata dall'albo delle Organizzazioni certificate.

CERMET si riserva di comunicare il provvedimento di sospensione, revoca o riduzione agli enti di accreditamento e/o ad altri terzi che ne facciano richiesta, nonché di inserire la notizia sul proprio sito Internet.

#### 5. USO DEL MARCHIO e DEL CERTIFICATO DI CONFORMITÀ

Il cliente con SGSI certificato da CERMET può utilizzare il Marchio di certificazione CERMET presentato in una delle due versioni nelle figure 1 o 2. Il marchio è composto da un logo azzurro CYAN (Marchio depositato).

Nel caso di utilizzo del marchio secondo la versione di figura 2, i due marchi (marchio CERMET e marchio dell'organismo di accreditamento) devono essere adiacenti, la figura 2 mostra un esempio di applicazione.



Fig. 1



Fig. 2

Il marchio di certificazione:

- deve essere riportato unitamente al marchio e/o nome dell'Organizzazione certificata;
- deve essere riportato unitamente al/agli schema/i certificati (la norma deve essere citata con l'anno di edizione). Il cliente può utilizzare il marchio CERMET in riferimento a una o più norme contemporaneamente, purché il sistema di gestione del cliente sia certificato da CERMET rispetto a tutte le norme citate;
- deve essere utilizzato in modo da evitare che la certificazione non sia attribuibile a requisiti essenziali differenti da quelli per i quali è stata effettuata la valutazione, ad esempio la certificazione del SGSI non

deve essere utilizzata in modo da essere scambiata per una certificazione di prodotto, pertanto il marchio non può essere applicato sui prodotti o sul loro imballaggio;

- d) deve essere utilizzato soltanto in riferimento ai prodotti/servizi, siti, oggetto della certificazione concessa;
- e) può essere ingrandito o ridotto, ma deve comunque permettere sempre la lettura delle parole e dei numeri iscritti;
- f) può essere applicato sui sistemi di trasporto/movimentazione dei prodotti purché abbinato al logo/nome dell'Organizzazione certificata;
- g) non può essere riportato dai laboratori di taratura e prova sui propri certificati/rapporti di prova.

Per pubblicizzare la certificazione il cliente può, garantendo il rispetto di quanto sopra, ed evitando di fornire informazioni che possano produrre confusione o malintesi da parte dei propri clienti ed utilizzatori finali, utilizzare la dicitura tipo: *“Organizzazione con Sistema di Gestione per la Sicurezza delle Informazioni Certificato da CERMET secondo UNI CEI ISO IEC 27001:2006”* (o simile). Tale dicitura può essere riportata anche sui prodotti e sui loro imballi.

Il marchio può essere utilizzato a colori, in tal caso dovranno essere rispettati i colori propri del marchio stesso, oppure in versione monocromatica (di qualsiasi colore).

Le presenti prescrizioni si applicano anche nel caso in cui si faccia uso di marchi trasferibili (ad es. adesivi).

Il cliente deve informare il personale che può far uso del marchio, delle sopraindicate prescrizioni.

È possibile la riproduzione (anche a colori) dei certificati di conformità rilasciati da CERMET, purché riproducano integralmente l'originale.