REGOLAMENTO TECNICO PER LA CERTIFICAZIONE DI SISTEMI DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI

Dasa - Rägister

INDICE

Dasa - Rägister

1. GENERALITA'

Il presente documento descrive le procedure applicate da Dasa-Rägister per la Certificazione dei Sistemi di Gestione per la Sicurezza delle Informazioni ed è da considerarsi supplementare, e quindi non sostitutivo, a quanto definito nel "Regolamento Contrattuale".

L'Organizzazione richiedente la Certificazione deve:

- avere un Sistema di Gestione per la Sicurezza delle Informazioni che rispetti i requisiti della normativa di riferimento e delle eventuali prescrizioni particolari stabilite per tipologia di prodotto/processo/servizio;
- avere effettuato un ciclo completo di Audit Interni ed un Riesame della Direzione;
- mantenere a disposizione di Dasa-Rägister le registrazioni di tutti i reclami ricevuti e delle relative azioni conseguenti;
- predisporre un programma di miglioramento del proprio Sistema di Gestione;
- mantenere aggiornata la raccolta delle norme, leggi e regolamenti cogenti applicabili all'attività, processo, servizio, prodotto incluso nel campo di applicazione della Certificazione;
- dare evidenza di aver identificato ed analizzato le minacce alla sicurezza dei beni aziendali (Assets) che rientrano nel campo di applicazione previsto dal Sistema di Gestione;
- dimostrare di aver identificato ed analizzato i rischi relativi alla sicurezza delle informazioni nonché identificato ed applicato le opportune misure di sicurezza;
- applicare un monitoraggio delle misure di sicurezza adottate al fine di valutare la loro efficacia nel salvaguardare le informazioni e i servizi erogati dall'organizzazione;
- dimostrare la predisposizione e l'implementazione di un programma di informazione e sensibilizzazione del personale relativamente al problema della sicurezza delle informazioni.

Il Certificato è emesso a fronte del completamento, con esito positivo, dell'Audit Iniziale (Initial Audit), la sua validità è subordinata al superamento degli Audit di Sorveglianza periodici (Surveillance Audit) e ad una completa rivalutazione (Re-Audit) entro il termine della scadenza.

Qualora la richiesta di certificazione provenga da Organizzazioni già certificate da enti accreditati e con certificato in corso di validità, Dasa-Rägister subentra nelle attività in accordo con la pianificazione del precedente ente, recependo eventuali rilievi ed effettuando il relativo Audit secondo le modalità previste dal presente regolamento.

Prima dell'esecuzione di ogni Audit, Dasa-Rägister comunica all'Organizzazione i nomi dei componenti dell'Audit Team che condurrà la valutazione e nello stesso momento indica l'eventuale documentazione che dovrà essere resa disponibile.

Per ogni Audit sono previste:

- una riunione iniziale tra l'Audit Team e l'Organizzazione finalizzata alla presentazione delle parti e all'illustrazione delle procedure di verifica;
- la verifica in campo e 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 (Audit Report) con i risultati e le conclusioni dell'audit e l'eventuale pianificazione delle attività successive;
- una riunione finale tra l'Audit Team e l'Organizzazione per illustrare l'esito dell'audit e consegnare l'Audit Report. In questa fase l'Organizzazione può sollevare e formalizzare eventuali riserve.

Gli Audit potranno essere condotti sia in presenza che a distanza (modalità "da remoto") così come in forma mista.

2. PRE-AUDIT

È possibile effettuare un Audit preliminare (Pre-Audit) prima dell'Audit Iniziale con lo scopo di individuare il grado di preparazione dell'Organizzazione in relazione ai requisiti della norma e di identificare quelle situazioni che potrebbero compromettere il buon esito dell'Initial Audit.

Può essere condotto un solo Pre-Audit per ogni Richiesta di Certificazione.

Dasa - Rägister

3. AUDIT INIZIALE (INITIAL AUDIT)

L'Initial Audit 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 enti di accreditamento):

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

Lo Stage 2 può essere effettuato solo dopo il completamento dello Stage 1 e la presa in carico di eventuali rilievi che, se non risolti, potrebbero comportare Non Conformità Maggiori nello Stage 2. Nel caso in cui nell'intervallo tra i due stage intervengano modifiche significative al Sistema di Gestione, al contesto o alla legislazione applicabile, cambi di sede o altri fattori che rendano il risultato dello Stage 1 non più attuale, occorrerà ripeterlo.

3.1 STAGE 1 AUDIT

Lo Stage 1 Audit viene effettuato presso la sede dell'Organizzazione e prevede le seguenti finalità:

- valutare la documentazione del Sistema di Gestione e che 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;
- valutare che 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;
- che esista e sia applicata la procedura di valutazione e gestione dei rischi; così come previsto dallo standard di riferimento;
- che la Dichiarazione di Applicabilità sia documentata, congruente con la politica, il campo di applicazione e i risultati della Gestione del Rischio;
- che 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;
- che 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;
- che 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);
- che sia documentata la configurazione di rete;
- che esista la planimetria del sito, comprensiva degli impianti elettrici e meccanici di supporto;
- riesaminare lo stato e la comprensione dell'Organizzazione riguardo i requisiti della norma;
- riesaminare l'assegnazione di risorse e concordare con l'Organizzazione i dettagli dello Stage 2 Audit;
- predisporre la pianificazione dello Stage 2 Audit, acquisendo una sufficiente conoscenza del Sistema di Gestione e delle attività del sito dell'Organizzazione, con riferimento ai possibili aspetti significativi;
- valutare se gli Audit interni e il Riesame da parte della Direzione siano in corso di pianificazione ed esecuzione e che il livello di attuazione del Sistema di Gestione fornisca l'evidenza che l'Organizzazione è pronta per lo Stage 2 Audit.

In questa fase dell'iter di certificazione si deve trovare conferma che:

Dasa - Rägister

– sia stata valutata la conformità legislativa e ai requisiti contrattuali e che siano state intraprese le opportune azioni correttive in caso di parziale e/o totale inadempienza;
– esistano adeguati obiettivi per la Sicurezza delle informazioni e questi siano supportati da una programmazione e 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 delle informazioni;
– per l'esercizio dell'attività l'Organizzazione sia in possesso di tutte le necessarie licenze relative al software applicativo impiegato;
– il Sistema di Gestione tenga traccia e risponda alle principali istanze delle parti interessate riguardo la Sicurezza delle Informazioni;
– ad ogni operatore 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.

Le risultanze dello Stage 1 Audit saranno documentate nell'Audit Report e comunicate all'Organizzazione dall'Audit Team, compresa l'identificazione di ogni rilievo che nello Stage 2 Audit potrebbe essere classificato come Non Conformità.

Per eventuali potenziali Non Conformità Maggiori si richiede che l'Organizzazione trasmetta a Dasa-Rägister il trattamento e le eventuali Azioni Correttive per essere certi che queste si possano chiudere entro la data dello Stage 2 Audit.

E' di estrema importanza in questa fase, verificare che non esistano registrazioni del Sistema di Gestione che non possano essere rese disponibili all'Audit Team perché contengono informazioni riservate o sensibili ovvero per motivi di sicurezza. In questo caso, si dovrà stabilire se il Sistema di Gestione potrà essere adeguatamente verificato anche in assenza di accesso a questi record, in caso contrario, si informerà l'Organizzazione che l'audit di certificazione non potrà aver luogo se non verranno concesse modalità di accesso adeguate a tali registrazioni oppore apportando modifiche al campo di applicazione"

3.2. STAGE 2 AUDIT

Lo Stage 2 Audit è programmato in un secondo momento rispetto allo Stage 1 Audit e solo in determinate condizioni possono essere consecutivi.

Lo Stage 2 Audit viene effettuato presso la/e sede/i dell'Organizzazione e prevede la valutazione:
– del Sistema di Gestione dell'Organizzazione e delle prestazioni con riferimento al rispetto delle prescrizioni legali;
– del comportamento dell'Organizzazione nell'ambito di eventuali iter autorizzativi che non siano risultati completati al momento dello Stage 1 Audit;
– dell informazioni ed evidenze circa la conformità a tutti i requisiti della norma o di altro documento normativo applicabile al Sistema di Gestione per la Sicurezza delle Informazioni dell'Organizzazione;
– del monitoraggio, misurazione, rendicontazione e riesame delle prestazioni, con riferimento agli obiettivi e ai traguardi principali;
– del controllo operativo dei processi;
– degli Audit interni e del Riesame della Direzione;
– della responsabilità della Direzione relativamente alle politiche definite;
– dei collegamenti fra i requisiti normativi, la Politica, gli obiettivi ed i traguardi delle prestazioni, tutte le prescrizioni legali applicabili, le responsabilità, la competenza del personale, le attività, le procedure, i dati di prestazioni e le risultanze e le conclusioni degli Audit interni.

Le risultanze dello Stage 2 Audit saranno documentate nell'Audit Report e comunicate all'Organizzazione dall'Audit Team, insieme al Piano delle Sorveglianze (Audit Plan) che riporta la periodicità (solitamente annuale) e i requisiti/processi che saranno verificati durante gli Audit di Sorveglianza.

Eventuali Non Conformità che dovessero emergere al termine dello Stage 2 Audit devono

Dasa - Rägister

essere prese in carico dall'Organizzazione e la loro gestione comunicata a Dasa-Rägister (tramite le modalità indicate nell'Audit Report). Per poter proseguire con le successive fasi del processo di Certificazione, le modalità di trattamento e le eventuali Azioni Correttive definite dall'Organizzazione devono essere approvate dal Lead Auditor.

In caso di Non Conformità Maggiori è necessario verificare l'efficacia del trattamento e delle eventuali Azioni Correttive, che deve avvenire entro sei mesi dalla data dello Stage 2 Audit altrimenti quest'ultimo deve essere ripetuto. La valutazione può avvenire su base documentale o tramite un Follow-Up Audit (par. 5.). In assenza di tale verifica non è possibile proseguire con la fase di Delibera.

3.3. RILASCIO DELLA CERTIFICAZIONE

La Certificazione viene rilasciata a seguito del parere positivo del Comitato di Delibera (Decision Committee) che valuta i documenti relativi all'Audit e prendendo anche in considerazione eventuali informazioni inerenti l'Organizzazione raccolte dal mercato o comunque di pubblico dominio.

In questa fase il Comitato di Delibera:

- può richiedere all'Organizzazione di fornire eventuali informazioni mancanti;
- può disporre un Follow-Up Audit o documentale per integrare eventuali mancanze della verifica.

Il parere positivo del Comitato di Delibera consente:

- l'emissione del Certificato la cui validità è triennale e decorre dalla data della Delibera;
- l'iscrizione e la pubblicazione dei dati dell'Organizzazione nel Registro Certificazioni.

Il Comitato di Delibera può anche disporre Audit di Sorveglianza ad intervalli più frequenti (ad esempio semestrali) a seguito di:

- proposta dell'Audit Team o esito dell'audit tale per cui sia necessario monitorare il Sistema di Gestione con frequenza maggiore rispetto all'anno;
- specifica richiesta dell'Organizzazione.

In caso di non concessione della Certificazione, le ragioni di tale decisione vengono comunicate formalmente all'Organizzazione, precisando gli scostamenti rispetto ai requisiti della norma che la stessa si deve impegnare a correggere entro un termine di tempo proposto e accettato da Dasa-Rägister.

Tale termine non deve in ogni caso essere superiore a sei mesi, superati i quali deve essere ripetuto lo Stage 2 Audit

4. AUDIT DI SORVEGLIANZA (SURVEILLANCE AUDIT)

Al fine di accertare il continuo rispetto di quanto stabilito dalla norma di riferimento, con la periodicità prevista dal Programma di Certificazione vengono effettuati gli Audit di Sorveglianza, durante i quali vengono valutati solo alcuni aspetti del Sistema di Gestione.

L'Audit di Sorveglianza è eseguito con le stesse modalità dello Stage 2 Audit, valutando i requisiti/processi indicati nel Piano delle Sorveglianze. L'Audit può comunque essere condotto anche su altri punti a discrezione del Lead Auditor. L'Audit di Sorveglianza non prevede 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.

Eventuali Non Conformità segnalate all'Organizzazione dovranno essere prese in carico da quest'ultima.

L'efficacia del trattamento e delle eventuali Azioni Correttive viene verificata nel corso del successivo Audit di Sorveglianza salvo i casi in cui, in funzione della gravità e complessità, si ritenga necessaria:

- una verifica documentale supplementare (Follow-Up documentale) con l'invio di documenti da parte dell'Organizzazione a Dasa-Rägister;
- un audit supplementare presso l'Organizzazione (Follow-Up Audit – par. 5.).

Per le Non Conformità Maggiori, Dasa-Rägister definisce un tempo massimo entro il quale effettuare il Follow Up Audit al fine di verificare l'efficacia del trattamento e delle eventuali Azioni Correttive. Qualora questo non abbia luogo nei tempi previsti, la Certificazione verrà sospesa per un periodo massimo di sei mesi trascorsi i quali la Sospensione si trasformerà in Revoca.

La documentazione prodotta durante gli Audit di Sorveglianza viene sottoposta al Comitato

Dasa - Rägister

di Delibera nei seguenti casi:
- siano state rilevate Non Conformità Maggiori;
- sia stato modificato il Programma di Certificazione (per esempio, riduzioni, estensioni...);
- su esplicita richiesta dell'Audit Team, che può segnalare quelle situazioni che possono avere influenza sulla validità del Certificato.

Gli Audit di Sorveglianza hanno quantomeno cadenza annuale ed il primo Audit dopo la certificazione iniziale deve essere effettuato entro i dodici mesi dalla data della delibera del certificato.

5. AUDIT SUPPLEMENTARI (FOLLOW-UP AUDIT)

Il Follow-Up Audit è eseguito con le stesse modalità dello Stage 2 Audit ed ha normalmente come oggetto di verifica le sole parti interessate (per es. correzione Non conformità Maggiori, estensione, scopo,...). La valutazione può comunque essere condotta anche su altri punti a discrezione del Lead Auditor.

Qualora il Follow-Up Audit per la verifica dell'efficacia del trattamento delle Non Conformità Maggiori abbia esito negativo, la Certificazione verrà sospesa fino a che non sia stata valutata l'efficacia del nuovo trattamento e delle eventuali Azioni Correttive, e comunque per un periodo massimo di sei mesi, trascorsi i quali la Sospensione si trasformerà in Revoca.

6. AUDIT DI RINNOVO (RE-AUDIT)

La validità del Certificato è confermata a seguito dell'esito positivo di un audit completo (Re-Audit) condotto con gli stessi criteri dello Stage 2 Audit.

L'Audit di Rinnovo non prevede 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. Eventuali Non Conformità segnalate all'Organizzazione dovranno essere prese in carico da quest'ultima; per le Non Conformità Minori l'efficacia del trattamento e delle eventuali Azioni Correttive viene verificata nel corso del successivo Audit di Sorveglianza salvo i casi in cui, in funzione della gravità e complessità, si ritenga necessaria:
- una verifica documentale supplementare (Follow-Up documentale) con l'invio di documenti da parte dell'Organizzazione a Dasa-Rägister;
- un audit supplementare presso l'Organizzazione (Follow-Up Audit).

In caso di Non Conformità Maggiori è necessario verificare l'efficacia del trattamento e delle eventuali Azioni Correttive entro la data di scadenza in vigore del Certificato.

Entro la medesima data la Certificazione può essere rinnovata a seguito del parere positivo del Comitato di Delibera (Decision Committee) con le stesse modalità del rilascio iniziale (par. 3.3).

Ciò implica che il Re-Audit deve essere effettuato con sufficiente anticipo al fine di permettere la gestione di eventuali Non Conformità.

Qualora non si riesca a completare l'iter entro la data di scadenza del certificato (ad esempio Follow Up), il Comitato di Delibera non potrà procedere con il rinnovo. Se le attività pendenti si riescono a completare entro sei mesi dalla scadenza, il Comitato di Delibera potrà ripristinare il certificato sul quale comparirà il periodo di interruzione della sua validità. Altrimenti, trascorsi sei mesi e non più di un anno dalla scadenza, dovrà essere condotto almeno uno Stage 2 perché il Comitato di Delibera possa ripristinare il certificato. Trascorso un anno si dovrà procedere con un Audit Iniziale (Stage 1+Stage 2) ed il rilascio di un nuovo certificato senza mantenere la storicità della certificazione precedente.

7. CLASSIFICAZIONE DEI RILIEVI

I rilievi riscontrati durante l'Audit sono classificati in Non Conformità Maggiori, Non Conformità Minori e Osservazioni.

Una Non Conformità si definisce "Maggiore" quando si ha:
- assenza o non effettiva implementazione di uno o più degli elementi richiesti dal Sistema di Gestione, o una situazione che genera dubbi significativi circa la capacità di soddisfare i requisiti del prodotto o del servizio;
- un elevato numero di Non Conformità Minori riferite ad un singolo processo/requisito,

che potrebbe comportare la totale inadeguatezza del prodotto o del Sistema di Gestione, oppure una situazione che potrebbe causare il rilascio di un prodotto non conforme o non rispondente a requisiti cogenti;
- la mancata risoluzione di una o più Non Conformità Minori rilevate durante il precedente Audit.

Una Non Conformità si definisce “Minore” quando:
- l’Organizzazione non dimostra di controllare completamente un aspetto del Sistema di Gesione ma fornisce fiducia del controllo del relativo processo;
- un requisito della norma non è stato interpretato o applicato in modo completo e corretto, o non è stato adeguatamente documentato.

L’Audit Team può fornire “Osservazioni” quando identifica aree di miglioramento relative ad attività che comunque risultano essere conformi. Sebbene le Osservazioni non richiedano la formalizzazione né la comunicazione a Dasa-Rägister di alcuna gestione, si richiede in ogni caso all'Organizzazione di fornire evidenza dell'analisi delle stesse in occasione degli audit successivi.

I rilevi che dovessero emergere durante il Pre-Audit non vengono classificati.