Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Ordinanza sulla durata del lavoro e del riposo dei conducenti professionali di veicoli leggeri per il trasporto di persone e di automobili pesanti (OLR 2)

Modifica del …

Il Consiglio federale svizzero
ordina:

I

L'ordinanza del 6 maggio 1981[1] sulla durata del lavoro e del riposo dei conducenti professionali di veicoli leggeri per il trasporto di persone e di automobili pesanti è modificata come segue:

Ingresso

visti gli articoli 25 capoverso 2bis, 56, 103 e 106 della legge federale del 19 dicembre 1958[2] sulla circolazione stradale (LCStr),

Art. 14 lett. a^{bis}

Per controllare se la durata del lavoro, della guida e del riposo sia stata osservata (art. 5–12), bisogna basarsi soprattutto:

a^{bis}. sugli inserimenti nell'applicazione elettronica (art. 16*b*–16*g*);

Art. 16b Applicazione elettronica

L'applicazione elettronica è destinata alla registrazione, all'elaborazione, alla visualizzazione e alla trasmissione di informazioni relative ai periodi di lavoro, di guida e di riposo dei conducenti professionali (dati) mediante un programma software installato su un terminale o utilizzato attraverso una rete di dati.

Art. 16c Requisiti dell'applicazione elettronica

[1] L'applicazione elettronica deve soddisfare i seguenti requisiti:

RS .....
1 RS **822.222**
2 RS **741.01**

a. i dati di cui agli articoli 16*g* e 18 capoversi 5 e 6 devono poter essere registrati e approvati elettronicamente;

b. il momento della registrazione dei dati deve essere visibile;

c. ogni modifica dei dati registrati deve essere visibile, comprensibile e verificabile in modo semplice;

d. i dati devono essere registrati e memorizzati automaticamente subito dopo ciascun inserimento;

e. i dati registrati devono essere immediatamente visibili e consultabili integralmente e illimitatamente per almeno 28 giorni, trascorsi i quali possono essere cancellati o sovrascritti;

f. i dati registrati devono essere accessibili alle autorità di controllo:
   1. nella forma illustrata nell'allegato 1, con la possibilità per le autorità di salvarli in loco con strumenti standardizzati,
   2. online attraverso un URL univoco, ad esempio sotto forma di codice QR;

g. i dati e la loro trasmissione devono essere protetti da manipolazioni e accessi non autorizzati;

h. l'applicazione elettronica deve essere dotata di un numero progressivo per l'identificazione univoca della copia installata presso il conducente nonché dell'identificazione del certificato.

2 L'applicazione elettronica può avere funzioni aggiuntive relative alla corsa, purché ciò non comprometta la conformità con i requisiti di cui al capoverso 1.

Art. 16d Certificazione dell'applicazione elettronica

1 L'applicazione elettronica deve essere presentata per esame e certificazione a un organismo di certificazione secondo l'articolo 16*e*. L'esame è effettuato secondo uno schema di certificazione basato sulle direttive di cui all'allegato 2 numero 2. Se l'applicazione soddisfa i requisiti secondo l'articolo 16*c*, il titolare riceve un certificato. Il certificato è rilasciato per una durata massima di cinque anni.

2 Il titolare del certificato deve:

a. sottoporre qualsiasi modifica sostanziale dell'applicazione all'organismo di certificazione per verifica e approvazione;

b. informare annualmente l'organismo di certificazione degli eventi che indicano possibili malfunzionamenti.

3 Il certificato può essere rinnovato su domanda del titolare, ogni volta al massimo per altri cinque anni, a condizione che i requisiti di cui all'articolo 16*c* continuino a essere soddisfatti. L'organismo di certificazione conduce a tale scopo un audit. La domanda di rinnovo deve essere presentata prima della scadenza del certificato.

4 In caso di controversie di natura contrattuale tra l'organismo di certificazione e il richiedente o il titolare del certificato decide il tribunale civile.

Art. 16e Requisiti dell'organismo di certificazione

La certificazione dell'applicazione elettronica può essere effettuata esclusivamente da organismi:

a. accreditati secondo la norma ISO/IEC 17065:2013, Konformitätsbewertung – Anforderungen an Stellen, die Produkte, Prozesse und Dienstleistungen zertifizieren per i seguenti settori:
   1. crittografia e comunicazione sicura,
   2. protezione dei dati,
   3. sicurezza dell'applicazione mobile; e
b. conformi ai requisiti di cui all'allegato 2.

Art. 16f Condizioni di utilizzo dell'applicazione elettronica

1 L'applicazione elettronica può essere impiegata per veicoli che dispongono di un'iscrizione nella licenza di circolazione secondo l'articolo 80 capoverso 2 dell'ordinanza del 27 ottobre 1976[3] sull'ammissione alla circolazione (OAC) e non sono dotati di tachigrafo.

2 Il conducente di un veicolo deve comunicare all'USTRA il numero di identificazione secondo l'articolo 16*c* capoverso 1 lettera h prima dell'utilizzo dell'applicazione elettronica. Un conducente può impiegare al massimo due applicazioni.

3 Il conducente deve garantire che il terminale:

a. sia sempre aggiornato al fine di proteggerlo da manipolazioni e accessi non autorizzati;
b. sia efficacemente protetto da qualsiasi sollecitazione meccanica e costantemente alimentato con sufficiente energia.

4 Su richiesta, assiste le autorità di controllo nell'accesso ai dati.

Art. 16g Registrazione dei periodi di lavoro, di guida e di riposo nell'applicazione elettronica

1 Il conducente deve registrare i dati di cui all'articolo 18 capoversi 5 e 6 e controllare eventuali inserimenti automatici. Deve effettuare gli inserimenti costantemente. Gli inserimenti non devono essere grafici.

2 Se il conducente professionale utilizza il veicolo per una corsa privata, deve contrassegnarla di conseguenza nell'applicazione elettronica prima di mettersi in viaggio. Deve registrare inizio, fine e chilometraggio della corsa privata.

3 Se il veicolo è utilizzato da terzi per una corsa privata, prima di iniziare la successiva corsa professionale il conducente deve registrare nell'applicazione elettronica la differenza chilometrica corredata dell'indicazione «altro conducente».

3 RS **741.51**

4 Il conducente deve mettere a disposizione del datore di lavoro i dati dell'applicazione elettronica relativi ai periodi di lavoro, di guida e di riposo entro il primo giorno di lavoro della settimana successiva.

Art. 19 cpv. 7

7 Si può omettere la compilazione del libretto di lavoro se i periodi di lavoro, di guida e di riposo sono registrati con un'applicazione elettronica.

Art. 21 cpv. 1, frase introduttiva e 2

1 Ricorrendo ai mezzi disponibili, quali i dischi e le serie di dischi settimanali del tachigrafo, gli inserimenti nell'applicazione elettronica, i fogli settimanali e quotidiani del libretto di lavoro, eventuali rapporti giornalieri ad uso interno dell'azienda e carte di lavoro (art. 19 cpv. 1, art. 25 cpv. 4), il datore di lavoro si accerta in maniera continua che le disposizioni sulla durata del lavoro, della guida e del riposo (art. 5–12) siano osservate. A tale scopo, per ogni conducente riporta in un registro le indicazioni seguenti:

2 Per lavoratori il cui tempo di guida giornaliero, da un controllo sommario dei mezzi di controllo secondo l'articolo 14 lettere a e a^{bis}, è risultato manifestamente inferiore a sette ore non è necessario iscrivere nel registro la durata della guida; basta includerla nella durata totale del lavoro quotidiano (cpv. 1 lett. b).

Art. 22 cpv. 3–5

3 Il datore di lavoro deve mettere a disposizione del conducente il libretto di lavoro nonché le chiavi e i dischi necessari all'uso del tachigrafo oppure l'applicazione elettronica. Il conducente deve informare il prima possibile il datore di lavoro di un eventuale guasto del tachigrafo o dell'applicazione elettronica.

4 Il datore di lavoro deve tenere un elenco contenente i nomi dei conducenti, il loro indirizzo e l'anno di nascita nonché il numero dei rispettivi libretti di lavoro.

5 Deve provvedere affinché i dati personali dei conducenti raccolti in relazione all'esecuzione della presente ordinanza siano utilizzati unicamente ai fini di quest'ultima e siano protetti da accessi non autorizzati.

Art. 23 cpv. 3, frase introduttiva e lett. b^{bis}

3 Devono conservare per due anni, presso la sede dell'azienda:

b^{bis}. gli inserimenti nell'applicazione elettronica (art. 16*f* e 16*g*);

Art. 28 cpv. 2 lett. d, e ed f

2 È punito con la multa chiunque viola le disposizioni sul controllo (art. 15–23), in particolare chi:

d. non registra o non registra debitamente i dati prescritti nell'applicazione elettronica;

e. manipola il sistema globale (applicazione elettronica, terminale e dati salvati nella memoria centrale) in modo da fornire dati errati;

f. utilizza applicazioni elettroniche non certificate.

Art. 32 cpv. 1bis

1bis Aggiorna gli allegati.

II

2 Alla presente ordinanza sono aggiunti gli allegati 1 e 2 secondo la versione qui annessa.

III

La presente ordinanza entra in vigore il ....

… In nome del Consiglio federale svizzero:

La presidente della Confederazione, Karin Keller-Sutter
Il cancelliere della Confederazione, Viktor Rossi

Allegato 1
(art. 16*c* cpv. 1 lett. e)

Moduli per la registrazione dei periodi di lavoro, di guida e di riposo

1. Aspetti generali

I moduli (1.1–1.4) contenenti le indicazioni richieste secondo l'articolo 18 capoversi 5 e 6 sono vincolanti.

1.1 Foglio quotidiano per lavoratori

Campo	**Iscrizione**
Nome, cognome	
Inizio lavoro	
Data	
Targa	
Chilometraggio (iniziale)	
Durata del riposo prima di entrare in servizio in ore e minuti	
Ripartizione oraria/Attività **(inizio e fine lavoro)** (periodi di lavoro e di guida, pause, corse private)	

Fine lavoro	
Chilometraggio (finale)	
Chilometri giornalieri	
Chilometri aggiuntivi per corse private	
Chilometraggio (corse private comprese)	
Durata complessiva per attività	Durata guida:
	Durata lavoro:
	Pausa:
Osservazioni	
Firma	

(Allegato 1.2)

1.2 Foglio settimanale per lavoratori

Nome, cognome								
Settimana								
Ultimo giorno di riposo settimanale								
Giorno della settimana	**LUN**	**MAR**	**MER**	**GIO**	**VEN**	**SAB**	**DOM**	**Totale settimanale**
Targa							-	
Durata del riposo prima dell'inizio in ore e minuti								
Inizio lavoro								
Fine lavoro								
Durata della guida in ore e minuti								
Durata del lavoro in ore e minuti								
Pause in ore e minuti								
Somma durata del lavoro e della guida in ore e minuti								
Giorno di riposo settimanale								
Semigiornata libera settimanale								

Osservazioni	

(Allegato 1.3)

1.3 Foglio quotidiano per conducenti indipendenti

Campo	Iscrizione
Nome, cognome	
Data	
Targa	
Chilometraggio (iniziale)	
Durata del riposo prima di entrare in servizio in ore e minuti	
Ripartizione oraria/Attività (inizio e fine durata della guida)	
Chilometraggio (finale)	
Chilometri giornalieri	
Durata complessiva della guida in ore e min.	
Osservazioni	
Firma	

(Allegato 1.4)

4. Foglio settimanale per conducenti indipendenti

Nome, cognome								
Settimana								
Ultimo giorno di riposo settimanale								
Giorno della settimana	**LUN**	**MAR**	**MER**	**GIO**	**VEN**	**SAB**	**DOM**	**Totale settimanale**
Targa							-	
Durata del riposo prima dell'inizio in ore e minuti								
Inizio attività professionale								
Fine attività professionale								
Durata della guida in ore e minuti								
Giorno di riposo settimanale								
Semigiornata libera settimanale								
Osservazioni								

Allegato 2
(art. 16*d* cpv. 1 e 16*e*)

Requisiti degli organismi di certificazione

1. Aspetti generali

1.1 Organismo di certificazione

Ogni organismo di certificazione deve:

- operare con imparzialità ed evitare conflitti di interesse;
- garantire la riservatezza di informazioni proprietarie, codice sorgente e documentazione di sicurezza;
- applicare lo schema di certificazione in modo coerente;
- tenere traccia di valutazioni e decisioni.

1.2 Schema di certificazione

Per verificare la conformità delle applicazioni elettroniche con i requisiti di cui all'articolo 16*c* capoversi 1 e 2, l'organismo di certificazione predispone uno schema di certificazione tenendo conto delle direttive di cui al numero 2.

Garantisce la conformità con i requisiti della presente ordinanza e con i pertinenti standard internazionali [p. es. norme SN/EN ISO 15408:2023 *Information security, cybersecurity and privacy protection – Evaluation criteria for IT security* (*Common Criteria*), ossia i criteri generali per la valutazione della sicurezza di tecnologie d'informazione, SN/EN IEC 62443-4-1:2018 e 62443-4-2:2019 *IT-Sicherheit für industrielle Automatisierungssysteme*, SN EN ISO/IEC 27034:2023 *Information technology – Security techniques – Application security* e NF EN ETSI 303645:2024 *CYBER – Cybersécurité pour l'Internet des objets grand public: Exigences de base*[4] nonché *Mobile Application Security Verification Standard* (MASVS) v2.1.0 dell'*Open Worldwide Application Security Project* (OWASP)[5]].

Gestisce lo schema di certificazione e all'occorrenza lo aggiorna.

4 Le norme possono essere consultate gratuitamente e ottenute a pagamento presso l'Associazione svizzera di normazione (SNV), Sulzerallee 70, 8404 Winterthur; www.snv.ch (disponibili in tedesco, francese o inglese).
5 Consultabile all'indirizzo: https://mas.owasp.org > MASVS (versione 2.1.0).

2. Direttive per lo schema di certificazione

2.1 Ambito di applicazione e principi delle direttive

Lo schema di certificazione è valido per le applicazioni mobili e i servizi collegati utilizzati per la verifica dei requisiti della presente ordinanza.

I requisiti tecnici derivano dagli obiettivi e requisiti dei *Common Criteria*, dai requisiti della presente ordinanza e dal MASVS (OWASP).

2.2 Pianificazione delle attività

Le diverse fasi devono essere pianificate e concordate dall'organismo di certificazione con il richiedente.

2.3 Verifica degli artefatti di sicurezza pertinenti

Tutti gli artefatti di sicurezza implementati dall'applicazione (p. es. procedure, modelli, strumenti e rapporti di prova) devono essere sottoposti a un controllo documentale.

La tabella 1 «Requisiti di sicurezza» elenca i più importanti artefatti di sicurezza da verificare, sulla base di disposizioni e standard attuali per applicazioni mobili. Sono definiti quattro diversi livelli di valutazione.

Abbreviazione	Descrizione
BE	Verifica di base. L'elemento è verificato mediante semplice lettura. L'obiettivo è quello di comprendere fondamentalmente il testo e capirne il significato. Domande che dovrebbe porsi il revisore: cosa esprime il testo? Quali informazioni ne deduco?
CE	Verifica critica. L'elemento è verificato mediante lettura critica. L'obiettivo è quello di giudicare il funzionamento del testo, analizzarlo, interpretarlo e valutarlo. Domande che dovrebbe porsi il revisore: come funziona il testo? Come si argomenta? Su quali ipotesi si basa il testo? Qual è il significato del testo?
SE	Controllo a campione. L'elemento si compone di diversi documenti o paragrafi, una parte dei quali è verificata attraverso una procedura sistematica di campionamento. Il livello di controllo per gli elementi selezionati corrisponde alla verifica critica. I criteri di selezione si basano sui seguenti principi: viene data la priorità ai documenti con maggiori ripercussioni sulla sicurezza.
NE	Non verificato. L'elemento non è verificato.

Tabella 1: Requisiti di sicurezza

La tabella 2 «Obiettivi di sicurezza» stabilisce gli obiettivi e controlli di sicurezza vincolanti per le applicazioni mobili in base al MASVS (OWASP) e ai *Common Criteria*. Gli obiettivi costituiscono la base per gli audit e devono essere verificati in modo approfondito.

Settore	Requisito principale	PP[6]	MASVS (OWASP)
Crittografia	Codifica, gestione chiavi, protocolli sicuri	FCS[7]	CRYPTO
Protezione dei dati	Codifica dati inattivi, controllo accessi, comunicazione	FDP[8]	STORAGE, NETWORK
Configurazione e gestione	Configurazione sicura, gestione funzioni critiche	FMT[9]	PLATFORM, ARCH
Anti-exploit	Protezione da manipolazioni, controlli integrità, offuscamento del codice, aggiornamenti	FPT[10]	RESILIENCE, ARCH
Canali affidabili	Protezione dei dati durante la trasmissione	FTP[11]	NETWORK
Protezione dei dati	Consenso utente alla trasmissione di PII	FPR[12]	PRIVACY

6 *Protection Profile for Application Software* (profilo di protezione) del NIAP (*National Information Assurance Partnership*)
7 *Functional Class Cryptographic Support* (supporto crittografico)
8 *Functional Class User Data Protection* (protezione dati utente)
9 *Functional Class Security Management* (gestione sicurezza)
10 *Functional Class Protection of the TSF (TOE Security Functions)* (protezione funzioni di sicurezza dell'oggetto di verifica)
11 *Functional Class Trusted Path/Channels* (percorso o canale affidabili)
12 *Functional Class Privacy* (protezione dei dati o della sfera privata)

Rilevamento di rooting/jailbreaking	L'app rileva un ambiente compromesso	n/a[13]	RESILIENCE 1, 2

Tabella 2: Obiettivi di sicurezza

Per requisiti specifici di verifica e prova possono essere utilizzati come base i *Common Criteria* o il MASVS (OWASP).

2.4 Verifica dei processi di supporto – Livello 1

Gli artefatti devono essere riproducibili. A tal fine devono essere definiti processi di supporto nel sistema di gestione del richiedente e deve essere effettuato un controllo documentale dei processi per verificarne completezza e correttezza.

Documento da verificare	Prima verifica / Monitoraggio di modifica sostanziale	Monitoraggio di modifica minore
Manuale per la gestione della cibersicurezza	CE	BE
	BE se ISO27001	BE
Manuale per la gestione del conto	CE	BE
		BE
Rapporto sull'architettura	CE	BE
Rapporto di audit sulla sicurezza	SE	BE
Manuale per la gestione della configurazione	CE	BE
Manuale per la gestione degli eventi	SE	BE
Manuale per i processi di incident response	SE	BE
Manuale per la manutenzione e la gestione di patch	SE	BE
Rapporto sulla protezione da malware	SE	BE
Rapporto sull'accesso a distanza	CE	BE
Manuale di security by design	CE	BE
Manuale per un'implementazione sicura	CE	BE
Manuale per processi di sicurezza	CE	BE
Manuale per aggiornamenti di sicurezza	CE	BE
Rapporto sulla cibersicurezza SIS[14]	CE	BE
Analisi della comunicazione wireless	SE	BE

13 n/a – not applicable (non applicabile)
14 *Secure Internet Service* (servizio Internet sicuro)

Tabella 3: Verifica dei processi

2.5 Test – Livello 2

L'organismo di certificazione può scegliere tre approcci diversi:

- esecuzione di propri test;
- utilizzo di un rapporto su test esterni;
- osservazione di test.

L'ultimo approccio può essere combinato con il secondo se non può essere garantita la reputazione del fornitore di test esterno.

2.5.1 Osservazione di test

In assenza di chiari requisiti per i test negli standard disponibili, deve essere utilizzato l'approccio definito in questo schema, che copre le funzioni di sicurezza tecniche. I test effettuati nei centri di prova del richiedente devono essere osservati secondo lo stato sotto descritto. Per questi test possono essere considerati i risultati della verifica degli artefatti di sicurezza pertinenti.

È possibile effettuare i seguenti test:

a. *Performed by the customer and witness based on sampling* (test P); sono effettuati dal richiedente; una parte è osservata a campione dall'organismo di certificazione;
b. *Performed and fully Witness* (PW); sono validati mediante osservazione.

Test	Prima verifica / Monitoraggio di modifica sostanziale	Monitoraggio di modifica minore
Test di autenticazione (login, sessioni…)	PW	R
Test di autorizzazione (diritti di accesso, elementi non affidabili…)	PW	R
Test di log (avvisi, reminder, protocolli)	PW	PW
Test di robustezza della comunicazione (integrità, conformità protocolli)	PW	PW
Test di interfacce (iniezione di dati, fuzzing, validazione di inserimenti)	PW	R
Test di disponibilità (stress test)	PW	R
Test di penetrazione	PW	R

Tabella 4: Strategia di osservazione di test

2.5.2 Verifica di specifiche e strumenti di prova

Prima di ogni osservazione di test, devono essere presentati al revisore responsabile il piano dei test, le specifiche e le informazioni relative a strumenti e processi di prova del richiedente. Sono valutati:

a. copertura dei test;
b. efficacia dei test;
c. qualità della documentazione di prova;
d. adeguatezza degli strumenti di prova;
e. prove di validazione degli strumenti di prova;
f. competenza del personale;
g. processi aziendali.

2.5.3 Durante l'osservazione di test

Il revisore responsabile deve:

a. osservare la sessione di test, disturbare il meno possibile lo svolgimento, porre tutte le domande o chiedere chiarimenti prima dell'inizio dei test;
b. verificare se i test sono effettuati secondo le procedure concordate, il piano e le specifiche;
c. verificare se i test sono effettuati dagli esaminatori designati nel piano;
d. annotare gli strumenti utilizzati e rispettive versioni, confrontandoli con quelli definiti nelle specifiche.

Il revisore responsabile non può:

a. partecipare attivamente alle attività di prova né assumere ruoli o funzioni spettanti al personale del richiedente;
b. esprimere pareri e proposte né rispondere a domande;
c. influenzare in alcun modo il processo di prova, il centro o i risultati.

Il revisore responsabile può interrompere il test in qualsiasi momento se viene constata una grave non conformità che renderebbe nulli i risultati. In questo caso il richiedente ne è immediatamente informato.

2.5.4 Risultati dell'osservazione di test

Il revisore responsabile deve predisporre un rapporto contenente almeno le seguenti indicazioni:

a. data, ora, luogo;
b. personale coinvolto e relativi ruoli;
c. obiettivo e contesto dei test;
d. versione dei casi di test eseguiti;

e. divergenze tra risultati attesi ed effettivi;

f. valutazione dei risultati da parte di terzi.

2.6 Audit – Livello 3

L'efficacia e la rilevanza degli artefatti di sicurezza e dei relativi processi devono essere valutate e il parere degli stakeholder interessati deve essere confermato. A tale scopo, dopo un esame preliminare degli artefatti di sicurezza e dei relativi processi è condotto un audit formale incentrato su:

- verifica delle funzioni di sicurezza dell'oggetto esaminato;
- valutazione del grado di implementazione e di maturazione dei processi di supporto.

Sono temi dell'audit in particolare:

- organizzazione di sicurezza e competenze;
- processo di miglioramento continuo;
- audit interni sulla cibersicurezza;
- ciclo di vita;
- sistema di gestione della qualità;
- gestione della configurazione;
- gestione delle modifiche;
- valutazione d'impatto;
- verifica;
- struttura della documentazione e modelli;
- gestione dei fornitori;
- processi di post-sviluppo (p. es. monitoraggio dei prodotti, gestione delle vulnerabilità).

2.7 Verifica – Raccomandazione di certificazione

Sulla base dei risultati delle fasi 2.3–2.6, il revisore responsabile deve verificare se sono soddisfatti tutti i requisiti di certificazione.

2.8 Decisione relativa alla certificazione

Sulla base della verifica da parte del revisore responsabile, una commissione indipendente deve verificare la raccomandazione di certificazione. Decide poi in merito al rilascio del certificato.

2.9 Attestazione, licenza

L'organismo di certificazione concede al richiedente il diritto di utilizzare un marchio di certificazione. A tal fine l'organismo di certificazione può riutilizzare un marchio esistente.

2.10 Monitoraggio

Devono essere garantiti gli audit sulla cibersicurezza. A tal fine l'applicazione certificata per applicazioni mobili deve essere costantemente aggiornata e l'organismo di certificazione deve svolgere attività di monitoraggio almeno ogni 12 mesi dalla decisione di certificazione. Le attività di monitoraggio devono comprendere almeno:

- monitoraggio di incidenti: prova che il richiedente monitora la propria applicazione e tratta gli incidenti adeguatamente;
- gestione delle modifiche: modalità di installazione degli aggiornamenti e di garanzia della loro sicurezza;
- audit: colloqui con gli stakeholder interessati in merito alla gestione delle modifiche e per un costante miglioramento.

Tutte le modifiche apportate al prodotto o ai processi di assistenza devono essere classificate sistematicamente in base al loro impatto sugli obiettivi di sicurezza e sul livello di fiducia. Le modifiche sono classificate come minime o sostanziali:

- modifiche minime: modifiche senza influsso sulle funzionalità chiave, sul modello di minaccia e sulla conformità (p. es. aggiornamenti superficiali, ottimizzazioni di performance, miglioramenti della documentazione); di solito richiedono soltanto aggiornamenti della documentazione o una verifica limitata;
- modifiche sostanziali: modifiche riguardanti le funzioni di sicurezza, l'architettura o il profilo di rischio (p. es. nuove funzioni, aggiornamenti rilevanti di meccanismi criptografici, modifiche dello scenario di minaccia); richiedono una valutazione approfondita ed eventualmente una nuova certificazione (parziale).

L'organismo di certificazione è responsabile della classificazione di ogni modifica e dell'applicazione del grado di valutazione adeguato.

2.11 Sospensione

La validità di un certificato può essere temporaneamente sospesa, in particolare se:

- il monitoraggio rivela una non conformità che non richiede il ritiro immediato;
- non sono adottate misure idonee contro l'uso improprio del certificato o del marchio;
- sussistono altre infrazioni allo schema di certificazione o alle procedure di dell'organismo di certificazione.

La sospensione è notificata al richiedente per iscritto. Durante la sospensione l'applicazione può rimanere registrata.

2.12 Ritiro

Un certificato è ritirato se:

- il monitoraggio rivela una grave non conformità;
- sussiste un'infrazione all'accordo tra il richiedente e l'organismo di certificazione;
- non sono adottate misure idonee in caso di sospensione;
- il richiedente non desidera rinnovare il certificato;
- il richiedente non può o non vuole soddisfare i nuovi requisiti derivanti dalla modifica di standard o regole;
- il prodotto non è più fabbricato o il richiedente cessa l'attività.

Il ritiro è notificato per iscritto. Il titolare del certificato deve informare tutti i clienti entro e non oltre dieci giorni dalla notifica, ricordando che l'applicazione non può più essere utilizzata.

3. Modifica dei requisiti dei prodotti

In caso di modifica dei requisiti per i prodotti coperti, l'organismo di certificazione deve informare immediatamente e per iscritto il richiedente sull'entrata in vigore e l'eventuale necessità di una verifica aggiuntiva.