Certificación de procesos y componentes ciberseguros

Reglamento técnico de Ciberseguridad

CONTROL DE LA DOCUMENTACIÓN

- El presente documento se distribuye como Copia No Controlada.
- No se garantiza que sea la última versión del mismo. Debe consultarse con CERTINALIA, S.L.U. si está en posesión de la versión en vigor.

Contenido

1. INTRODUCCIÓN 3
2. OBJETO Y CAMPO DE APLICACIÓN 3
3. NORMATIVA DE REFERENCIA 5
4. DEFINICIONES 5
5. ESQUEMA DE CERTIFICACIÓN. 6
6. PROCESO DE CERTIFICACIÓN DE CICLO DE VIDA (SPDL) 8
6.1. SOLICITUD DE CERTIFICACION 9
6.2. REVISIÓN DE LA SOLICITUD 9
6.3. PROCESO DE EVALUACIÓN 9
6.4. PLAN DE ACCIONES CORRECTORAS 10
6.5. REVISIÓN Y DECISIÓN 10
6.6. EMISION DEL CERTIFICADO DE CONFORMIDAD 10
6.7. VALIDEZ DEL CERTIFICADO SPDL 11
7. PROCESO DE CERTIFICACIÓN DE COMPONENTE (CSA) 12
7.1. SOLICITUD DE CERTIFICACION 13
7.2. REVISIÓN DE LA SOLICITUD 13
7.3. PROCEDIMIENTOS DE EVALUACIÓN. 13
7.4. PLAN DE ACCIONES CORRECTORAS 14
7.5. REVISIÓN Y DECISIÓN 14
7.6. EMISION DEL CERTIFICADO DE CONFORMIDAD 14
7.7. VALIDEZ DEL CERTIFICADO CSA 14
8. MANTENIMIENTO DEL CERTIFICADO 15
8.1. ACTIVIDADES DE SEGUIMIENTO 15
8.2. CONTROL DE MODIFICACIONES EN LOS COMPONENTES (SI APLICA) 15
8.3. AUDITORIA EN EL CENTRO DE DESARROLLO/PRODUCCIÓN 15
9. AMPLIACIÓN, REDUCCIÓN, SUSPENSIÓN Y RETIRADA DE CERTIFICADOS. 16
9.1. AMPLIACIÓN / REDUCCIÓN DE ALCANCE CERTIFICADO 16
9.2. SUSPENSIÓN DE CERTIFICADOS 16
10. USO DEL CERTIFICADO Y MARCA 17
11. CAMBIOS EN LOS REQUISITOS DE CERTIFICACION 17
12. COMUNICACIÓN DE CAMBIOS POR PARTE DEL CLIENTE 17
13. RECLAMACIONES DIRIGIDAS AL SOLICITANTE 18
14. RECURSOS Y APELACIONES 18
15. CONFIDENCIALIDAD 18
16. INFORMACION PUBLICA 19
17. HISTORICO DE MODIFICACIONES 19
ANEXO I: REQUISITIOS MÍNIMOS NIVEL BÁSICO CERTIFICADO SPDL (EN IEC 62443-4-1) 20
ANEXO II: REQUISITOS MÍNIMOS NIVEL AVANZADO CERTIFICADO SPDL (EN IEC 62443-4-1) 22
ANEXO III: REQUISITOS PARA CERTIFICACION DE COMPONENTE (EN IEC 62443-4-2) 24

1. INTRODUCCIÓN

La norma IEC 62443 es un conjunto de estándares que ofrecen una serie de recomendaciones y mejores prácticas para fortalecer la seguridad de los sistemas de control industrial frente a las amenazas cibernéticas. La norma cubre a múltiples actores que toman parte en los sistemas de control y automatización industrial (Industrial Automation and Control Systems, IACS), desde un fabricante de un componente hasta el usuario final de esos mismos productos.

El estándar diferencia dos familias de normas, con sus correspondientes documentos, para establecer los requerimientos de seguridad en un entorno IACS.

- Por un lado, está la familia de normas IEC 62443-3, que ofrece las pautas para sistemas ciberseguros en entornos IACS.
- Por otro lado, la familia IEC 62443-4, define las pautas relativas a los componentes que tomaran parte en los sistemas IACS.

Dentro de la familia IEC 62443-4, dos normas son relevantes para este esquema de certificación; la norma EN IEC 62443-4-1 y EN IEC 62443-4-2. El documento EN IEC 62443-4-2 define los requerimientos técnicos de seguridad que debe tener un componente. Estos requerimientos serán variables dependiendo de la severidad en el nivel de seguridad que se quiera obtener por parte del proveedor de productos. En cambio, el documento IEC 62443-4- 1 define los requerimientos del ciclo de vida de los procesos de desarrollo de productos ciberseguros.

En la familia IEC 62443-3, se especifican los requisitos de seguridad del sistema completo del que formará parte el componente evaluado. Este esquema de certificación está dirigido a los proveedores de componentes, y, por lo tanto, el certificado se centra en los requerimientos específicos de los componentes y no del componente integrado en un sistema final, dejando a un lado el documento IEC 62443-3-3 y su certificado correspondiente.

2. OBJETO Y CAMPO DE APLICACIÓN

Este documento tiene como objeto definir el procedimiento a seguir por **CERTINALIA** como entidad para la certificación para la emisión de un certificado de conformidad con las normas EN IEC 62443-4-2 y/o EN IEC 62443-4-1.
El alcance reglamentario se define de la siguiente manera:

- **Certificado de Ciclo de Vida (SPDL) conforme EN IEC 62443-4-1**: Define los requerimientos del ciclo de vida para el proceso de desarrollo de productos ciberseguros. La norma define cuatro niveles de madurez (Maturity Level, ML) para poder describir el nivel de desarrollo en el que sus procesos se sitúan respecto a la descripción de los procesos en los requerimientos. Teniendo en cuenta la necesidad de poder certificar productos industriales en el ámbito de la ciberseguridad con la mayor celeridad posible y el esfuerzo que supone el cumplimiento total de los requisitos de ciclo de vida del desarrollo seguro del producto acorde a la EN IEC 62443-4-1, se plantean en el presente esquema de certificación dos tipos de certificación del ciclo de vida para el desarrollo de productos seguros (Secure Product Development Lifecycle, SPDL), el nivel <u>básico</u> y el nivel <u>avanzado</u>.

- **Certificado Componente (CSA) EN IEC 62443-4-2**: Los requerimientos para componentes (component requirements, CRs) que se definen en la norma están dirigidos a cuatro tipos de componente:
    - Aplicaciones de software,
    - dispositivos integrados,
    - dispositivos de red y
    - dispositivos anfitriones.

Además, la norma define **cuatro niveles de seguridad** (Security Level, SL). El solicitante deberá definir el nivel de seguridad objetivo en función de sus necesidades.

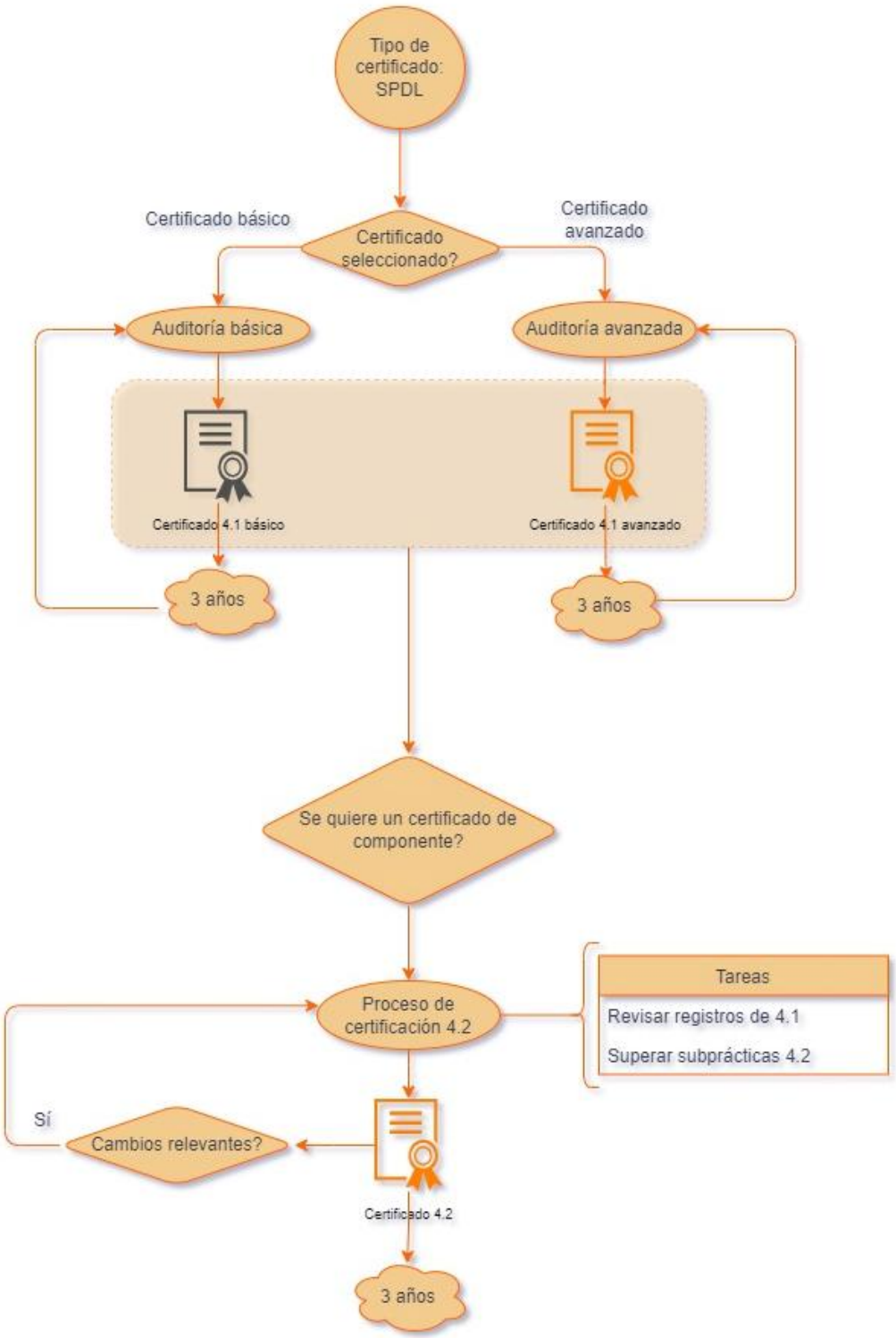

Ilustración 1:Diagrama explicativo del esquema de certificación

3. NORMATIVA DE REFERENCIA

- ISO/IEC 17067:2013. Evaluación de la conformidad. Fundamentos de la certificación de producto y directrices para los esquemas de certificación de producto.
- ISO 17065:2012 - Evaluación de la conformidad. Requisitos para organismos que certifican productos, procesos y servicios
- IEC TS 62443-1-1:2009 Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models
- IEC 62443-3-3:2013 Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels
- EN IEC 62443-4-1:2018 Security for Industrial Automation and Control Systems - Part 4-1: Secure Product Development Lifecycle Requirements
- EN IEC 62443-4-2:2019 Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components

4. DEFINICIONES

- Expediente: Conjunto de documentación que recoge la evaluación realizada al solicitante, solicitud, planes de muestreo, informes de ensayos, decisiones…
- SPDL: Secure Product Development Lifecycle. En castellano, Ciclo de Vida para el Desarrollo Seguro del Producto.
- Componente: Entidad perteneciente a un IACS que manifiesta las características de uno o más dispositivos host, dispositivo de red, aplicación de software o dispositivo integrado. Cuando en la parte 4-2 de la norma se menciona la palabra componente, el cual es el objecto de certificación, se deberá entender que se refiere a un sistema, subsistema o componente individual. Esto se puede ver claramente en la ilustración 2, donde se describen las entidades que pueden ser certificadas bajo la norma EN IEC 62443-4-2.

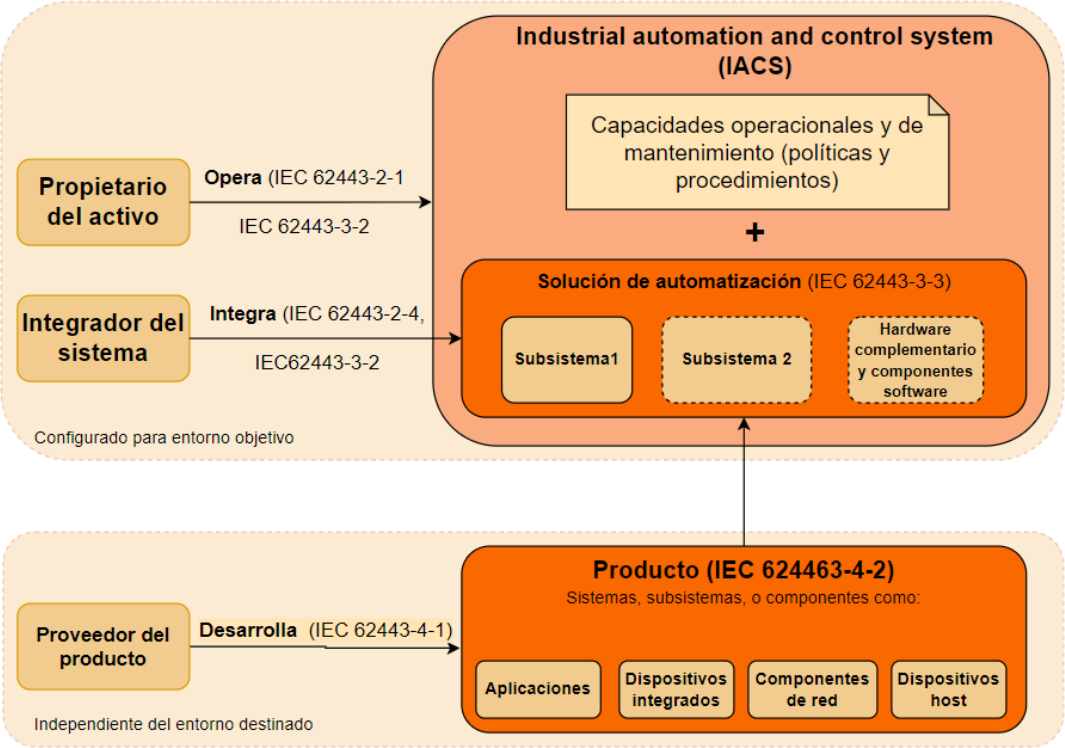

Ilustración 2: Diagrama explicativo de aplicación de la norma IEC 62443

- Dispositivo integrado (ED): Dispositivo de propósito especial diseñado para monitorear o controlar directamente un proceso industrial. También conocidos como dispositivos embebidos. Por ejemplo: los Controladores Lógicos Programables (PLC) o los Dispositivos Electrónicos Inteligentes (IED).
- Dispositivo host (HD): Dispositivo de uso general que ejecuta un sistema operativo (por ejemplo, sistema operativo Microsoft Windows o Linux) capaz de albergar una o más aplicaciones de software, almacenar datos o funciones de uno o más proveedores. Por ejemplo: Estaciones de trabajo del operador (operator workstations) o historiodares de datos (data historians).
- Aplicación Software (SA): Uno o más programas de software y sus dependencias (paquetes de bases de datos, herramientas de generación de informes o cualquier software de código abierto o de terceros) que se utilizan para interactuar con el proceso o el propio sistema de control. Es importante tener en cuenta que las aplicaciones de software típicamente se ejecutan en los dispositivos host y en los dispositivos embebidos.
- Dispositivo de red (ND): Dispositivo que permite el flujo de datos entre dispositivos, o restringe el flujo de datos, pero no puede interactuar directamente con un proceso de control. Por ejemplo: los switches o los terminadores de VPN (Virtual Private Network).

5. ESQUEMA DE CERTIFICACIÓN.

El esquema de certificación incluirá actividades de evaluación que funcionarán de una manera modular, donde el cliente podrá seleccionar el certificado que más se ajuste a sus necesidades, y, por lo tanto, el procedimiento de evaluación que le corresponda. Los procedimientos de evaluación serán las siguientes:

- Concesión del Certificado de Ciclo de Vida (SPDL) conforme a EN IEC 62443-4-1, NIVEL BÁSICO.

Certificado 4.1 básico

- Concesión del Certificado de Ciclo de Vida (SPDL) conforme a EN IEC 62443-4-1, NIVEL AVANZADO.

Certificado 4.1 avanzado

- Concesión de Certificado de Componente (CSA) conforme a EN IEC 62443-4-2

Certificado 4.2

5.1. CERTIFICADO DE CICLO DE VIDA (SPDL). NIVEL BÁSICO.

En el Anexo I de este Reglamento Técnico, se definen los procesos a auditar incluyendo el nivel exigido por requisito para obtener el nivel básico de la certificación de Ciclo de Vida (SPDL).
El nivel básico de certificación requiere el nivel mínimo de ML para todas las 47 subprácticas establecidas por la norma EN IEC 62443-4-1.
Esto garantiza que si en un futuro se desea obtener el Certificado de Componente (CSA), el fabricante no tendrá que someterse a una recertificación ni ampliar el ML en ninguna de las subprácticas. El nivel de madurez (ML) requerido para cada subpráctica varía en función de su importancia para la obtención del Certificado de

Componente (CSA). Las más críticas son clasificadas con un ML de 3 y las menos críticas con un ML de 2. En el Anexo I se detallan todos estos requisitos junto con sus respectivos ML.

Se considera que el cumplimiento de las secciones mencionadas y sus ML en el Anexo I asegura de manera suficiente la continuidad de los requisitos de seguridad ensayados para la norma EN IEC 62443-4-2 pudiendo garantizar su vigencia por el periodo establecido en la duración del certificado.

5.2. CERTIFICADO DE CICLO DE VIDA (SPDL). NIVEL AVANZADO.

En el Anexo II de este Reglamento Técnico, se definen los procesos a auditar incluyendo el nivel exigido por requisito para obtener el nivel avanzado de la certificación de Ciclo de Vida (SPDL).

Para el nivel de certificación avanzado, se exigirá el cumplimiento de todos los requisitos aplicables de la norma EN IEC 62443-4-1 para el ciclo de vida seguro con un ML de 3 o superior. Los requerimientos de la norma para el nivel avanzado y sus ML se encuentran definidos en el Anexo II.

5.3. CERTIFICADO DE COMPONENTE (CSA) CONFORME A EN IEC 62443-4-2.

Para optar por este certificado, será necesario haber obtenido la certificación de Ciclo de vida (SPDL) conforme a este esquema.
Es posible tramitar un proceso de certificación inicial conjuntamente para ambos certificados.

En el caso del Certificado de Componente, la norma está formada por siete bloques llamados requisitos fundamentales (foundational requirements - FR), donde existe una diferenciación por componentes y niveles de seguridad, y un primer bloque común para todos los componentes y todos los niveles.
El bloque común, por un lado, hace referencia a ciertos requisitos de la IEC 62443-3-3, y, por otro, a la necesidad de tener implementados procesos de desarrollo de productos seguros en base al documento EN IEC 62443-4-1.
Los requisitos aplicables para cada componente estarán determinados por el tipo de componente y el nivel de seguridad requerido que se especificará a en la *Solicitud de Certificación de Componente* **(RPO.CIB.01-02)**.

6. PROCESO DE CERTIFICACIÓN DE CICLO DE VIDA (SPDL)

El procedimiento para la concesión del certificado SPDL se plasma en el siguiente diagrama de flujo:

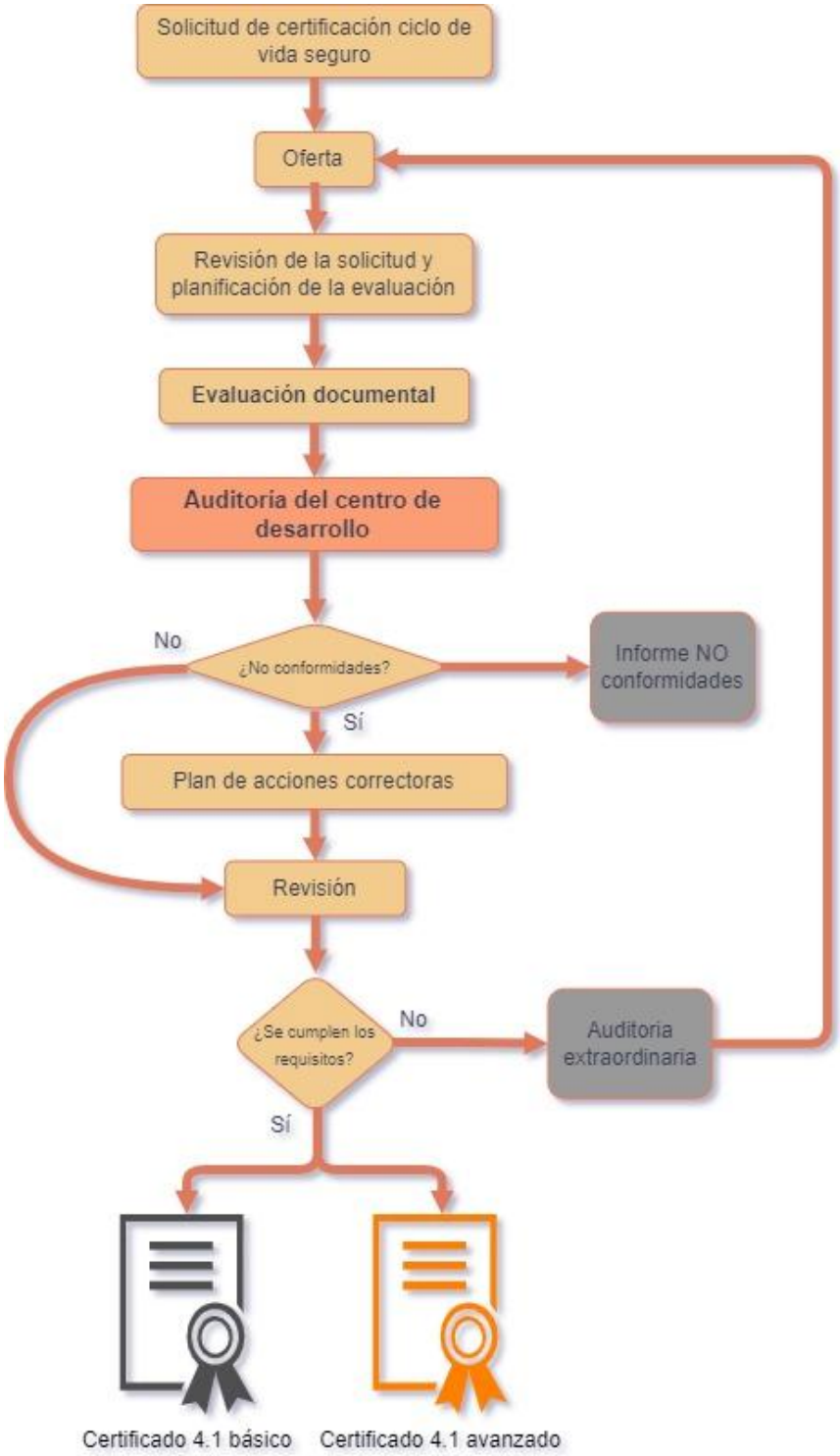

Ilustración 3: proceso de certificación de ciclo de vida seguro

6.1. SOLICITUD DE CERTIFICACION

El solicitante que desee obtener la certificación de ciclo de vida (SPDL) básico o avanzado, en base a la norma EN IEC 62443-4-1 deberá deberá hacer llegar a **CERTINALIA**, debidamente cumplimentado el formulario de solicitud **RPO.CIB.01** ***Solicitud de Certificación de Ciclo de*** Vida junto con información general del fabricante y/o información técnica detallada del alcance a certificar, incluyendo:

- Datos del solicitante.
- Nivel de Certificación EN IEC 62443-4-1 solicitado (básico o avanzado).
- Requisitos EN IEC 62443-4-1 incluidos y sus respectivos ML.
- Información sobre evaluaciones previas realizadas.

Durante la tramitación de la solicitud **CERTINALIA** pondrá a disposición del solicitante toda la información necesaria para conocer el proceso de certificación.

6.2. REVISIÓN DE LA SOLICITUD

CERTINALIA analizará la solicitud enviada por el solicitante asegurando que:

- Se ha recibido el formulario de solicitud correctamente rellenado.
- Se ha definido correctamente el alcance (la familia de producto, exclusiones si las hubiera, referencias incluidas en la serie, referencias comerciales, etc.).
- Si ha definido los emplazamientos y límites de la unidad técnica que se va a evaluar (número de personas, responsabilidades de cada una de ellas, localización de cada una de ellas, organigrama, etc.).
- Cualquier otro documento que sea necesario.

Durante esta etapa se realizarán las oportunas consultas con el cliente hasta definir perfectamente el alcance de la certificación y verificar que se puede proporcionar el servicio solicitado.

CERTINALIA facilita al solicitante un presupuesto a medida en función del contenido de la solicitud y de la carga de trabajo estimada para realizar las tareas de evaluación de la conformidad.

Solamente se procesará la solicitud, y se iniciaran las actividades de evaluación cuando se disponga de la solicitud de certificación, la información completa del producto y el presupuesto aceptado por el solicitante.
La aceptación de la oferta supone la aceptación de todas las condiciones que regulan la certificación y es a todos los efectos, el documento contractual entre los firmantes.

6.3. PROCESO DE EVALUACIÓN

En los Anexo I y II se definen los procesos a auditar incluyendo el nivel exigido por requisito para obtener el nivel básico y el nivel avanzado, de la certificación de Ciclo de Vida (SPDL). Cuando exista alguna excepción por motivos específicos de la empresa y/o componente, estos se justificarán.

CERTINALIA determinará la duración de la auditoría y los centros a visitar y elaborará un plan de auditoría de acuerdo con lo establecido en los procedimientos internos. **CERTINALIA** confirmará por escrito a la empresa con una antelación mínima de 15 días, la fecha de la auditoría y el equipo auditor asignado.

Tanto la fase de evaluación documental como la auditoría del centro de desarrollo podrán realizarse de forma presencial o remota.
La modalidad —presencial o remota— será acordada por las partes interesadas antes del inicio de cada fase, garantizando que los recursos necesarios estén disponibles y que los hitos temporales definidos queden reflejados.

6.3.1 EVALUACIÓN DOCUMENTAL

Previo a la auditoría del centro de desarrollo, se realizará una evaluación documental, donde se examinará la documentación técnica aportada por la empresa. La duración entre la evaluación documental y la auditoría no podrá ser superior a 3 meses.

En esta evaluación documental se evaluarán las prácticas de la norma para el nivel solicitado. **CERTINALIA** elaborará un informe de evaluación y lo enviará al cliente. En función del contenido del informe, se planificará de forma consensuada las fechas de la auditoría.

6.3.2 AUDITORÍA DEL CENTRO DE DESARROLLO

En la auditoría al centro de desarrollo, se revisarán las no conformidades de la evaluación documental y se solicitarán los registros necesarios para evidenciar la puesta en marcha de las prácticas requeridas en la norma. La auditoría se realizará por muestreo profundizando en aquellas prácticas que el equipo de evaluación considera más críticas y aquellas en la que auditoría documental muestre deficiencias.
Durante la auditoría, el equipo auditor verificará, de forma muestral, la gama de productos certificados bajo la norma EN IEC 62443-4-1.
El informe de auditoría indicará las no conformidades detectadas categorizadas como mayores y menores, y un apartado con notas y comentarios del equipo auditor.

6.4. PLAN DE ACCIONES CORRECTORAS

La evaluación documental no requerirá un plan de acciones correctivas, se entregará al cliente un informe con las no conformidades encontradas y estás serán evaluadas en la auditoria del centro de desarrollo.

La auditoría al centro de desarrollo SI requerirá de un Plan de Acciones Correctivas cuando durante la misma se detecten No Conformidades Mayores y/o Menores.

- Las No Conformidades mayores requerirán de propuesta de acción correctiva y evidencia de su implantación
- Las No Conformidades menores requerirán únicamente de propuesta de acción correctiva.

El plazo máximo para el envío del PAC será de 3 meses

CERTINALIA, evaluará el PAC enviado por el solicitante. Las acciones correctivas propuestas deberán ser aceptadas y las evidencias enviadas deberán permitir el cierre de las No Conformidades Mayores.

El plazo máximo establecido para el cierre de la evaluación, incluyendo la solicitud de nuevas acciones correctivas y el envío de nuevas evidencias es de 6 meses.

6.5. REVISIÓN Y DECISIÓN

Un técnico independiente de quien ha participado en le evaluación analizará el expediente correspondiente al solicitante y comprobará que:

- Se ha definido correctamente el alcance de la certificación.
- Las actividades de evaluación se han realizado correctamente.
- El plan de acciones correctivas ha sido evaluado correctamente y aceptado por el equipo de evaluación
- El expediente está completo y aprobado por las personas competentes.

El plazo establecido para la revisión del expediente y la toma de decisión es de 30 días. El resultado de esta revisión técnica será CONCEDER o DENEGAR el certificado de conformidad solicitado: Certificado de Ciclo de Vida (SPDL). La decisión será comunicada al solicitante por escrito.

6.6. EMISION DEL CERTIFICADO DE CONFORMIDAD

Con la decisión favorable de CONCEDER la certificación, **CERTINALIA** emitirá el correspondiente certificado de conformidad: Certificado de Ciclo de Vida (SPDL) nivel BASICO o AVANZADO de conformidad con la norma EN IEC 62443-4-1.

6.7. VALIDEZ DEL CERTIFICADO SPDL

La validez del Certificado de Ciclo de Vida (SPDL) será de 3 años desde su fecha de emisión, con carácter renovable por periodos iguales siempre y cuando el fabricante continúe cumpliendo los criterios establecidos en este reglamento técnico y las obligaciones resultantes de la certificación

7. PROCESO DE CERTIFICACIÓN DE COMPONENTE (CSA)

El procedimiento para la concesión del certificado CSA conforme a EN IEC 62443-4-2 viene plasmado en el siguiente diagrama de flujo:

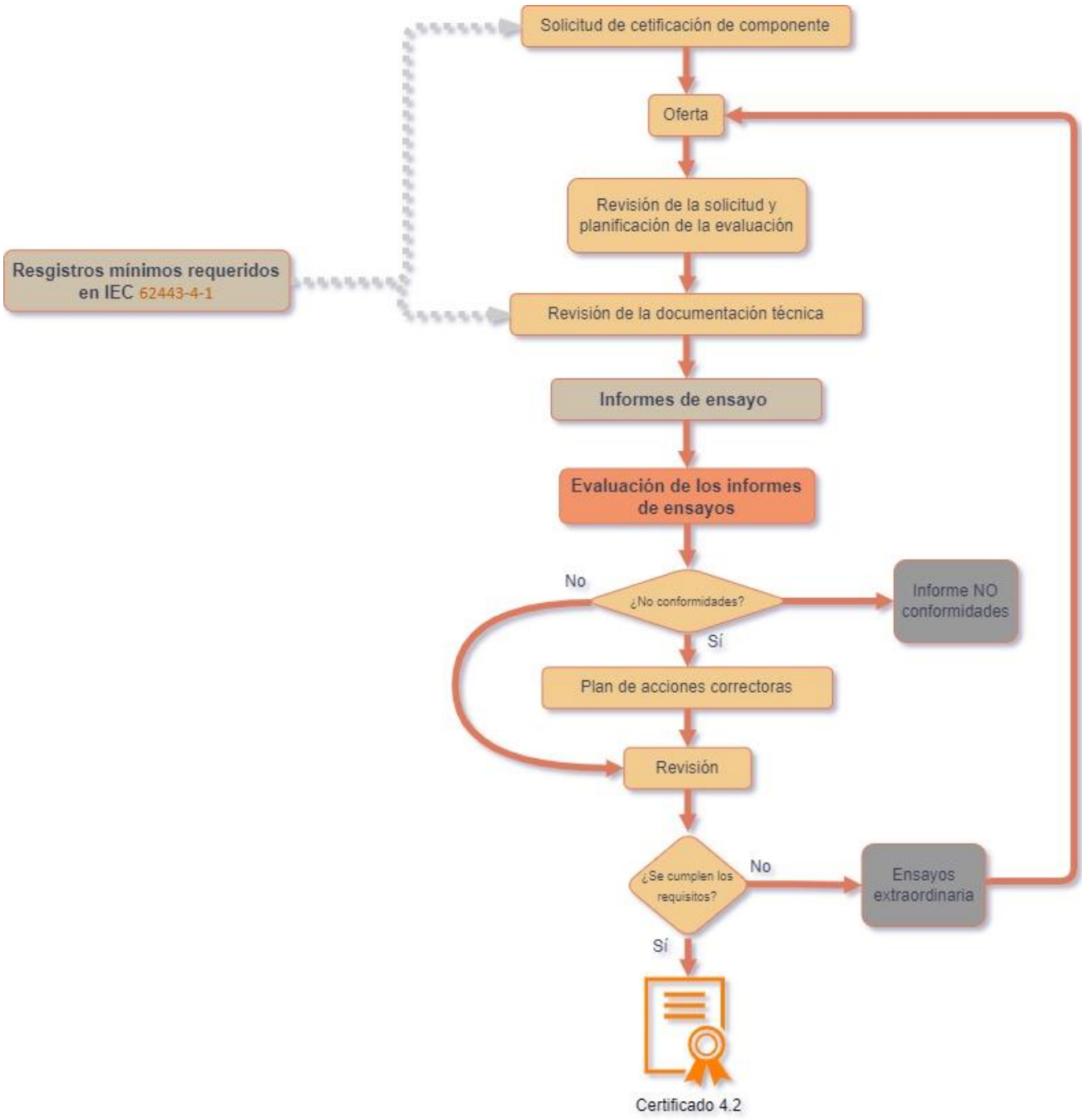

Ilustración 4: proceso de certificación de componente

7.1. SOLICITUD DE CERTIFICACION

El solicitante que desee obtener la certificación de componente (CSA), en base a la norma EN IEC 62443-4-2 deberá deberá hacer llegar a **CERTINALIA**, debidamente cumplimentado el formulario de solicitud **RPO.CIB.02** ***Solicitud de Certificación de Componente*** junto con información general del fabricante y/o información técnica detallada del producto a certificar, incluyendo:

- Datos del solicitante.
- Nivel de SL de EN IEC 62443-4-2 requerido.
- Definición del producto, así como información relevante del producto (tipo de componente, características técnicas, etc.).
- Evaluaciones previas realizadas.
- Registros necesarios para acreditar que el componente ha sido desarrollado siguiendo los pasos EN IEC 62443-4-1 (en Anexo I y Anexo II).
- Número de certificado de EN IEC 62443-4-1.

Durante la tramitación de la solicitud **CERTINALIA** pondrá a disposición del solicitante toda la información necesaria para conocer el proceso de certificación.

7.2. REVISIÓN DE LA SOLICITUD

CERTINALIA analizará la solicitud enviada por el solicitante asegurando que:

- Se ha recibido el formulario de solicitud correctamente rellenado.
- Se ha definido correctamente el alcance (los modelos de los, exclusiones si las hubiera, referencias incluidas en la modelo, referencias comerciales, etc.).
- Se ha recibido la documentación técnica completa con la solicitud:
- Planos del componente.
- Documentación del usuario, características funcionales.
- Especificaciones técnicas del componente.
- Diagrama de bloques descriptivo del hardware
- Registros de las pruebas (test de vulnerabilidades y prácticas IEC62443-4-1).
- Etc.

Durante esta etapa se realizarán las oportunas consultas con el cliente hasta definir perfectamente el alcance de la certificación y verificar que se puede proporcionar el servicio solicitado. En base a la información facilitada se hará una estimación de plan de ensayos.

CERTINALIA facilita al solicitante un presupuesto a medida en función del contenido de la solicitud y de la carga de trabajo estimada para realizar las tareas de evaluación de la conformidad.

Solamente se procesará la solicitud, y se iniciaran las actividades de evaluación cuando se disponga de la solicitud de certificación, la información completa del producto y el presupuesto aceptado por el solicitante.
La aceptación de la oferta supone la aceptación de todas las condiciones que regulan la certificación y es a todos los efectos, el documento contractual entre los firmantes.

7.3. PROCEDIMIENTOS DE EVALUACIÓN

El solicitante deberá proporcionar la información necesaria sobre el componente, como el tipo de componente (aplicaciones de software, dispositivos integrados, dispositivos de red y dispositivos host), el nivel de seguridad (desde SL de 1 a 4), y los registros pertinentes del ciclo de vida seguro (EN IEC 62443-4-1).

TECNALIA analizará la documentación técnica remitida para definir correctamente el alcance de la certificación y para comprobar que se han implantado las prácticas de la norma EN IEC 62443-4-1 requeridas por el esquema de certificación.

Como resultado de la revisión de la documentación técnica, se definirá de forma clara y completa el componente incluido en el alcance de la certificación, el plan de ensayos y las muestras o software necesarios.

Posteriormente, **CERTINALIA** procederá a realizar los ensayos y pruebas previstos de acuerdo con EN IEC 62443-4-2 para verificar el cumplimiento del componente con los requisitos aplicables y comprobar que los informes del cliente eran correctos.

CERTINALIA enviará al fabricante los informes relativos a los ensayos realizados en los laboratorios, incluyendo las NO CONFORMIDADES detectadas tanto en la revisión documental como en los ensayos.

7.4. PLAN DE ACCIONES CORRECTORAS

Todas las No conformidades detectadas en los ensayos de laboratorio requerirán de modificaciones en los componentes y un nuevo plan de ensayos. El plan de ensayos podrá ser completo o parcial en función del problema detectado. En cualquier el proceso de evaluación no continuará hasta disponer de resultados CONFORMES en todos los ensayos incluidos en el plan de muestreo y ensayos.

Cuando las No conformidades están relacionadas con la evaluación documental, se requerirá al solicitante nuevos registros de las prácticas IEC62443-4-1 y/o nueva documentación técnica que permita caracterizar de forma completa el producto.

No se establece plazo máximo para la implementación de las modificaciones de los productos, que dependerán de la gravedad de los problemas detectados, si bien se establece un plazo máximo de 12 meses para el cierre de la evaluación, que únicamente podrá ser ampliado bajo solicitud razonada del solicitante.

7.5. REVISIÓN Y DECISIÓN

Un técnico independiente de quien ha participado en le evaluación analizará el expediente correspondiente al solicitante y comprobará que:

- Se ha definido correctamente el alcance de la certificación.
- Las actividades de evaluación se han realizado correctamente.
- Las acciones correctivas han sido correctamente evaluadas y aceptadas por el equipo de evaluación
- El expediente está completo y aprobado por las personas competentes.

El plazo establecido para la revisión del expediente y la toma de decisión es de 30 días. El resultado de esta revisión técnica será CONCEDER o DENEGAR el certificado de conformidad solicitado: Certificado de Componente (CSA). La decisión será comunicada al solicitante por escrito.

7.6. EMISION DEL CERTIFICADO DE CONFORMIDAD

Con la decisión favorable de CONCEDER la certificación, **CERTINALIA** emitirá un certificado de conformidad: Certificado de Componente (CSA) de conformidad con la norma EN IEC 62443-4-2.

7.7. VALIDEZ DEL CERTIFICADO CSA

La validez del Certificado de Componente (CSA) será de 3 años desde su fecha de emisión, con carácter renovable por periodos iguales siempre y cuando el fabricante continúe cumpliendo los criterios establecidos en este reglamento técnico y las obligaciones resultantes de la certificación.

8. MANTENIMIENTO DEL CERTIFICADO

Durante el periodo de la certificación, el fabricante deberá comunicar todos los cambios relevantes en su organización, razón social, organigrama, personal clave y centros de desarrollo.
En el caso del Certificado Componente (CSA), deberá comunicar todos los cambios relevantes introducidos en los componentes certificados empleando el documento *Cambios y actualizaciones en los componentes* **(RPO.CIB.12)**.

8.1. ACTIVIDADES DE SEGUIMIENTO

El Certificado de Ciclo de Vida (SPDL) requerirá la realización de una auditoría de seguimiento anual para el mantenimiento del certificado durante su periodo de videncia. Cuando el solicitante dispone además de un Certificado de Componente (CSA), la auditoría incluirá necesariamente el análisis de las modificaciones introducidas en el componente.

El Certificado Componente (CSA), no requerirá de actividades de seguimiento durante la vigencia del certificado, siempre y cuando no se hayan introducido modificaciones en el componente certificado.

8.2. CONTROL DE MODIFICACIONES EN LOS COMPONENTES (Si aplica).

Si el fabricante dispone de un Certificado de Componente (CSA), durante la auditoría de seguimiento anual para el Certificado de Ciclo de Vida (SPDL) se comprobará que no se han incluido modificaciones relevantes que afectan al alcance de la certificación:

- Todas las mejoras funcionales (upgrade) han debido ser comunicadas a **CERTINALIA**
- Todas las actualizaciones (update) con riesgos significativos han sido también comunicadas.
- Todas las actualizaciones (update) sin riesgos significativos han sido evaluadas y gestionadas convenientemente.

Se comprobará que en esos casos donde se han realizado cambios no relevantes, los procedimientos y la evaluación de los clientes ha sido correcta.

8.3. AUDITORIA EN EL CENTRO DE DESARROLLO/PRODUCCIÓN

El equipo auditor asignado al expediente se desplazará al centro de desarrollo/producción para evaluar la implantación de los procedimientos e instrucciones del sistema de ciclo de vida y los registros generados como resultado de dichas operaciones.

La auditoría se desarrollará siguiendo la misma sistemática que la auditoría inicial reflejada en el punto 7.3 de este reglamento. Las auditorías de seguimiento serán siempre auditorías completas evaluando todos los requisitos aplicables al esquema.

El plazo para el envío del PAC en el caso de los seguimientos es de 45 días y el plazo para el envío de las evidencias que justifiquen su implantación es de 45 días adicionales. Finalizado este plazo de tiempo se deberá cerrar el expediente.

A continuación, un técnico independiente realizará la revisión del expediente y tomará la decisión de **MANTENER**, **SUSPENDER** o **RETIRAR** el certificado.
El plazo para la elaboración del informe es de 30 días y la decisión será comunicada al cliente.

9. AMPLIACIÓN, REDUCCIÓN, SUSPENSIÓN Y RETIRADA DE CERTIFICADOS.

9.1. AMPLIACIÓN / REDUCCIÓN DE ALCANCE CERTIFICADO

Se trata de la modificación del alcance de la certificación concedida a una empresa. La ampliación está contemplada para la incorporación de nuevos componentes desarrollados por la empresa, la incorporación de nuevas variantes a los componentes ya certificados y/o la mejora en los niveles de madurez de las prácticas definidas en EN IEC 62443-4-1 para pasar de NIVEL BÁSICO a nivel AVANZADO.

La ampliación del alcance necesita un informe de evaluación SATISFACTORIO. Si el componente se considera conforme a la norma EN IEC 62443-4-2, entra a formar parte de los componentes certificados ampliando así el alcance de los certificados ya emitidos, o emitiendo nuevos certificados. Si el Ciclo de Vida se considera conforme a la norma EN IEC 62443-4-1 nivel AVANZADO se emitirá un nuevo certificado.

La reducción del alcance de la certificación está contemplada para posibles descatalogaciones de productos, o cualquier otro argumento comunicado por la empresa solicitante. Para la reducción del alcance de la certificación sólo será necesaria la solicitud por escrito de anulación voluntaria del certificado por parte de la empresa solicitante.

9.2. SUSPENSIÓN DE CERTIFICADOS

La SUSPENSIÓN de la certificación es una medida cautelar y temporal, aunque limitada. Se trata de cancelar o bloquear los procesos de certificación que estén en marcha. La suspensión de la tramitación de la certificación puede ser voluntaria u obligatoria.

Será voluntaria cuando el motivo es una decisión interna de la empresa certificada, comunicada por escrito a **CERTINALIA.**

Será obligatoria, cuando se detecte alguna de las siguientes situaciones:

- El informe de auditoría refleja que el sistema ha dejado de cumplir de forma grave los requisitos de certificación, y recomienda la suspensión.
- El informe de evaluación refleja No Conformidades sin resolver y Planes de Acciones Correctoras inadecuados, y recomienda la suspensión.
- El cliente no permite la realización de las auditorías de seguimiento, de acuerdo con la periodicidad requerida.

La duración máxima de la suspensión no será nunca superior a 12 meses. Si transcurrido ese tiempo persiste la necesidad de suspensión de la certificación se pasará al proceso de RETIRADA de certificado.

Durante el periodo de suspensión, el cliente se debe abstener de publicitar su certificación. A petición de cualquier parte interesada**, CERTINALIA** declarará la condición de certificación del cliente como suspendida.

9.3. RETIRADA DE CERTIFICADOS

La RETIRADA del certificado puede ser voluntaria u obligada, pero tiene carácter definitivo. Se trata de cancelar definitivamente los procesos de certificación que estén en marcha.

La anulación de la certificación puede ser voluntaria, y comunicada por escrita enviada a **CERTINALIA**

La anulación obligatoria, estará ligada a un dictamen técnico, por sanción o como medida ante la reiteración de No-conformidades sin resolver o ante Planes de Acciones Correctoras considerados como no adecuados. Los motivos que pueden provocar la anulación de la certificación son los siguientes:

- El informe de auditoría extraordinaria refleja que el SPDL continúa sin cumplir los requisitos de certificación, tras el periodo de suspensión, y recomienda la anulación o retirada del certificado.
- Tras el periodo de suspensión, las No Conformidades continúan sin resolverse y los Planes de Acciones Correctoras se manifiestan inadecuados.

- Durante el periodo de suspensión, no se resuelve la negativa del cliente a permitir auditorías extraordinarias.

A partir de la comunicación de retirada, el cliente se debe abstener de publicitar su certificación. A petición de cualquier parte interesada, **CERTINALIA** declarará la condición de certificación del cliente como retirada.

Una vez retirada la certificación, para volver a obtenerla será obligatoria una nueva solicitud de concesión e iniciar el proceso desde el principio.

10. USO DEL CERTIFICADO Y MARCA

Tras la decisión favorable de Certificación, el titular de la certificación estará autorizado para usar el certificado y la **marca TECNALIA**, siempre que se cumpla lo establecido en el contrato de derecho de uso de marca y las reglas de uso de logo establecidas.

El certificado puede ser reproducido íntegramente en impresos, catálogos o cualquier otro tipo de documentos técnicos o comerciales.

Ni el certificado, ni la condición de certificado podrán utilizarse en cualquiera de los siguientes casos:

- Cuando la solicitud de certificación esté en fase de tramitación.
- Cuando no se haya concedido el certificado.
- Cuando la certificación haya sido suspendida temporal o definitivamente.
- Cuando se haya solicitado voluntariamente la retirada del certificado.

El solicitante tendrá derecho al uso de la **marca TECNALIA** siempre que claramente se asocie al producto certificado (sobre el propio producto, sobre su embalaje o sobre su documentación comercial de acompañamiento). Nunca se podrá utilizar la marca sobre productos no certificados ni haciendo referencia genérica a la organización.

El logotipo de la entidad de Acreditación ENAC y el de **CERTINALIA,** no podrá ser utilizado bajo ningún concepto.

CERTINALIA se reserva el derecho de impugnar la información y publicidad o promoción de los productos certificados, si estos no cumplieran con los requisitos establecidos.

11. CAMBIOS EN LOS REQUISITOS DE CERTIFICACION

En el caso de que se incorporen cambios substanciales en los requisitos del Esquema de Certificación, **CERTINALIA** informará a los clientes de dichos cambios, estableciendo el plan de transición y acciones necesarias para adaptarse a los nuevos requisitos.

El no cumplimiento de los plazos establecidos por parte del cliente para la adecuación a los cambios podría conllevar a una suspensión o retirada de la certificación.

12. COMUNICACIÓN DE CAMBIOS POR PARTE DEL CLIENTE

El cliente debe mantener el cumplimiento de los requisitos de certificación durante la validez del certificado, informando puntualmente a **CERTINALIA** cualquier modificación que afecte a su capacidad para cumplir con los requisitos, tales como:

- Cambios en la propiedad, incluidas las modificaciones en la denominación legal o el domicilio;
- Cambios de organización y gestión, tal como personal en puestos clave y estructuras organizacionales relacionadas con el alcance de la certificación;
- modificaciones relevantes en relación a los productos, sistemas de gestión y los procesos, cuando corresponda, para el alcance certificado

La decisión tomada por **CERTINALIA** tras el análisis de los cambios y la documentación presentada, será comunicada al cliente, pudiendo concluir la necesidad de actividades de evaluación adicionales (documental o in situ).

13. RECLAMACIONES DIRIGIDAS AL SOLICITANTE

El fabricante certificado deberá analizar y documentar todas las reclamaciones técnicas recibidas de sus clientes y referidas al cumplimiento de los requisitos de certificación y pondrá dichos registros a disposición de la entidad de certificación cuando se le solicita.

La tramitación de dichas reclamaciones incluirá su análisis y aceptación o rechazo, las comunicaciones con el cliente, la identificación de las causas de las no conformidades, la aprobación de acciones correctoras y preventivas, su seguimiento, la evaluación de su eficacia, y el cierre de la reclamación.

Dentro del proceso, el fabricante certificado deberá analizar las posibles consecuencias que la reclamación efectuada pudiera tener con respecto a los productos puestos en el mercado. En el caso de que se detectaran partidas que afecten a la seguridad del producto deberá tomar las medidas oportunas, incluido el cese de la comercialización de los productos y la retirada del mercado de los lotes defectuosos.

14. RECURSOS Y APELACIONES

Tomadas las decisiones relativas al proceso de certificación, y tras la notificación del resultado al solicitante, éste dispondrá de un plazo de un mes natural para APELAR en primera instancia dicha decisión.
CERTINALIA resolverá la APELACIÓN de acuerdo con el procedimiento **PCT.08.07** ***Tratamiento de quejas y apelaciones***, disponible para todos los solicitantes de la certificación.

La resolución de la APELACIÓN se notificará por escrito al solicitante. Tras la resolución en firme de la APELACIÓN, existe posibilidad de RECURRIR ante una segunda instancia. El solicitante dispondrá de un plazo de un mes natural para efectuar dicho recurso.

La tramitación del recurso se realizará también conforme al procedimiento **PCT.08.07** ***Tratamiento de quejas y apelaciones.*** La resolución del RECURSO se notificará al solicitante también por escrito. La decisión del RECURSO se considera definitiva y agota las posibilidades de revisión de la decisión de certificación.

15. CONFIDENCIALIDAD

La información recogida a lo largo del proceso de certificación será considerada como confidencial, conforme a los procedimientos internos de **CERTINALIA**. La información relativa al cliente obtenida de fuentes distintas al cliente (por ejemplo, de una queja, de autoridades reglamentarias) será tratada igualmente como información confidencial.

Todo el personal que participa de alguna forma en las actividades de Certificación tiene firmada una Declaración de Confidencialidad personal, donde se compromete a no revelar a ninguna persona o entidad la información propiedad del cliente a la que ha tenido acceso como consecuencia del proceso de certificación.

Los únicos límites establecidos al apartado anterior tienen que ver con los procesos de acreditación y los requerimientos legales. Durante las auditorías de acreditación por parte de ENAC se deberá mostrar al auditor toda la información referida a los expedientes sin limitación alguna. Cuando se reciba un requerimiento judicial que afecte a información considerada confidencial, se solicitará el consentimiento al cliente, pero se actuará en cualquier caso cumpliendo nuestras obligaciones legales.

Otros requisitos particulares relativos al uso de la información confidencial solicitados en el transcurso del proceso de certificación serán estudiados por **CERTINALIA** e incorporados en la medida de lo posible.

16. INFORMACION PUBLICA

CERTINALIA facilita a todos los usuarios y partes interesadas a través de su página web y sin necesidad de solicitud previa, la siguiente información resumida relativa a los procesos de certificación:

- Consulta sobre la validez de un certificado emitido a través del nº serie de un certificado emitido, incluyendo información sobre el alcance certificado.

17. HISTORICO DE MODIFICACIONES

Nº	FECHA	MOTIVO
00	**10-23**	- Primera edición del documento
01	**03-24**	- Definir los plazos de respuesta a desviaciones de auditorías (aptdo. 6.1.5; aptdo. 6.2.5; aptdo. 7.2.2). - Completar descripción del proceso de revisión y decisión (aptdo.6.1.6; aptdo. 6.2.6). - Incluir en anexos II y III práctica SG-7 " Documentation review)
02	**05-25**	- Referencia **CERTINALIA** - Se reestructuran los apartados del documento diferenciando el procedimiento de la certificación SPDL y la certificación CSA - Se especifica la posibilidad de tramitar una solicitud conjunta de certificados SPDL y CSA. - El proceso de evaluación de la certificación SPDL flexibiliza la posibilidad de realizar el proceso en modalidad remoto.(aptdo.6.3) - Se incluye sistemática aplicable a posibles cambios del esquema o cambios comunicados por el esquema (Capítulo 11; Capítulo 12) - Se incluye capítulo de información pública (Capítulo 16)

ANEXO I: REQUISITIOS MÍNIMOS NIVEL BÁSICO CERTIFICADO SPDL (EN IEC 62443-4-1)

PRÁCTICA 1: Security management

Requerimiento	Genera registros EN IEC 62443-4-2 **(S, £)**	Minimun Maturity Level **(1,2,3,4)**
SM-1: Development Process	S	3
SM-2: Identification of responsibilities	£	2
SM-3: Identification of applicability	£	2
SM-4: Security expertise	£	2
SM-5: Process scoping	£	2
SM-6: File integrity	S	3
SM-7: Development environment security	£	2
SM-8: Controls for private keys	£	2
SM-9: Security requirements for externally provided components	S	3
SM-10: Custom developed components from third-party suppliers	S	3
SM-11: Assessing and addressing security-related issues	£	2
SM-12: Process verification	£	2
SM-13: Continuous improvement	£	2

PRÁCTICA 2: Specifications of security requirements

Requerimiento	Genera registros EN IEC 62443-4-2 **(S, £)**	Minimun Maturity Level **(1,2,3,4)**
SR-1: Product security context	S	3
SR-2: Threat model	£	2
SR-3: Product security requirements	S	3
SR-4: Product security requirements content	£	2
SR-5: Security requirements review	£	2

PRÁCTICA 3: Secure by design

Requerimiento	Genera registros EN IEC 62443-4-2 **(S, £)**	Minimun Maturity Level **(1,2,3,4)**
SD-1: Secure design principles	S	3
SD-2: Defense in depth design	£	2
SD-3: Security design review	S	3
SD-4: Secure design best practices	£	2

PRÁCTICA 4: Secure implementation

Requerimiento	Genera registros EN IEC 62443-4-2 **(S, £)**	Minimun Maturity Level **(1,2,3,4)**
SI-1: Security implementation review	£	2
SI-2: Secure coding standards	£	2

PRÁCTICA 5: Security verification and validation testing		
	Genera registros EN IEC 62443-4-2 **(S, £)**	Minimun Maturity Level **(1,2,3,4)**
Requerimiento		
SVV-1: Security requirements testing	S	3
SVV-2: Threat mitigation testing	S	3
SVV-3: Vulnerability testing	S	3
SVV-4: Penetration testing	S	3
SVV-5: Independence of testers	£	2

PRÁCTICA 6: Management of security-related issues		
	Genera registros EN IEC 62443-4-2 **(S, £)**	Minimun Maturity Level **(1,2,3,4)**
Requerimiento		
DM-1: Receiving notifications of security-related issues	S	3
DM-2: Reviewing security-related issues	S	3
DM-3: Assessing security-related issues	S	3
DM-4: Addressing security-related issues	S	3
DM-5: Disclosing security-related issues	S	3
DM-6: Periodic review of security defect management practice	S	3

PRÁCTICA 7: Security update management		
	Genera registros EN IEC 62443-4-2 **(S, £)**	Minimun Maturity Level **(1,2,3,4)**
Requerimiento		
SUM-1: Security update qualification	S	3
SUM-2: Security update documentation	S	3
SUM-3: Dependent component or operating system security update documentation	S	3
SUM-4: Security update delivery	S	3
SUM-5: Timely delivery of security patches	S	3

PRÁCTICA 8: Security guidelines		
	Genera registros EN IEC 62443-4-2 **(S, £)**	Minimun Maturity Level **(1,2,3,4)**
Requerimiento		
SG-1: Product defense in depth	£	2
SG-2: Defense in depth measures expected in the environment	£	2
SG-3: Security hardening guidelines	£	2
SG-4: Secure disposal guidelines	£	2
SG-5: Secure operation guidelines	S	3
SG-6: Account management guidelines	S	3
SG-7: Documentation review	£	2

ANEXO II: REQUISITOS MÍNIMOS NIVEL AVANZADO CERTIFICADO SPDL (EN IEC 62443-4-1)

PRÁCTICA 1: Security management

Requerimiento	Genera registros EN IEC 62443-4-2 **(S, £)**	Minimun Maturity Level **(1,2,3,4)**
SM-1: Development Process	S	3
SM-2: Identification of responsibilities	£	3
SM-3: Identification of applicability	£	3
SM-4: Security expertise	£	3
SM-5: Process scoping	£	3
SM-6: File integrity	S	3
SM-7: Development environment security	£	3
SM-8: Controls for private keys	£	3
SM-9: Security requirements for externally provided components	S	3
SM-10: Custom developed components from third-party suppliers	S	3
SM-11: Assessing and addressing security-related issues	£	3
SM-12: Process verification	£	3
SM-13: Continuous improvement	£	3

PRÁCTICA 2: Specification of security requirements

Requerimiento	Genera registros EN IEC 62443-4-2 **(S, £)**	Minimun Maturity Level **(1,2,3,4)**
SR-1: Product security context	S	3
SR-2: Threat model	£	3
SR-3: Product security requirements	S	3
SR-4: Product security requirements content	£	3
SR-5: Security requirements review	£	3

PRÁCTICA 3: Secure by design

Requerimiento	Genera registros EN IEC 62443-4-2 **(S, £)**	Minimun Maturity Level **(1,2,3,4)**
SD-1: Secure design principles	S	3
SD-2: Defense in depth design	£	3
SD-3: Security design review	S	3
SD-4: Secure design best practices	£	3

PRÁCTICA 4: Secure implementation

Requerimiento	Genera registros EN IEC 62443-4-2 **(S, £)**	Minimun Maturity Level **(1,2,3,4)**
SI-1: Security implementation review	£	3
SI-2: Secure coding standards	£	3

PRÁCTICA 5: Security verification and validation testing		
	Genera registros EN IEC 62443-4-2 **(S, £)**	Minimun Maturity Level **(1,2,3,4)**
Requerimiento		
SVV-1: Security requirements testing	S	3
SVV-2: Threat mitigation testing	S	3
SVV-3: Vulnerability testing	S	3
SVV-4: Penetration testing	S	3
SVV-5: Independence of testers	£	3

PRÁCTICA 6: Management of security-related issues		
	Genera registros EN IEC 62443-4-2 **(S, £)**	Minimun Maturity Level **(1,2,3,4)**
Requerimiento		
DM-1: Receiving notifications of security-related issues	S	3
DM-2: Reviewing security-related issues	S	3
DM-3: Assessing security-related issues	S	3
DM-4: Addressing security-related issues	S	3
DM-5: Disclosing security-related issues	S	3
DM-6: Periodic review of security defect management practice	S	3

PRÁCTICA 7: Security update management		
	Genera registros EN IEC 62443-4-2 **(S, £)**	Minimun Maturity Level **(1,2,3,4)**
Requerimiento		
SUM-1: Security update qualification	S	3
SUM-2: Security update documentation	S	3
SUM-3: Dependent component or operating system security update documentation	S	3
SUM-4: Security update delivery	S	3
SUM-5: Timely delivery of security patches	S	3

PRÁCTICA 8: Security guidelines		
	Genera registros EN IEC 62443-4-2 **(S, £)**	Minimun Maturity Level **(1,2,3,4)**
Requerimiento		
SG-1: Product defense in depth	£	3
SG-2: Defense in depth measures expected in the environment	£	3
SG-3: Security hardening guidelines	£	3
SG-4: Secure disposal guidelines	£	3
SG-5: Secure operation guidelines	S	3
SG-6: Account management guidelines	S	3
SG-7: Documentation review	£	3

ANEXO III: REQUISITOS PARA CERTIFICACION DE COMPONENTE (EN IEC 62443-4-2)

FR 1 – Identification and authentication control (IAC) / Control de identificación y autenticación

		Nivel de Seguridad (SL 1-4)	**Tipo de componente** (CR, SAR, HDR, NDR, EDR)
	Requisitos		
1.1	Human user identification and authentication	1,2,3,4	CR
	• Unique identification and authentication	2,3,4	
	• Multifactor authentication for all interfaces	3,4	
1.2	Software process and device identification and authentication	2,3,4	CR
	• Unique identification and authentication	3,4	
1.3	Account management	1,2,3,4	CR
1.4	Identifier management	1,2,3,4	CR
1.5	Authenticator management	1,2,3,4	CR
	• Hardware security for authenticators	2,3,4	
1.6	Wireless access management	1,2,3,4	NDR
	• Hardware security for authenticators	2,3,4	
1.7	Strength of password-based authentication	1,2,3,4	CR
	• Password generation and lifetime restrictions for human users	3,4	
	• Password lifetime restrictions for all users (human, software process, or device)	4	
1.8	Public key infrastructure certificates	2,3,4	CR
1.9	• Strength of public key-based authentication	2,3,4	CR
	• Hardware security for public key-based authentication	3,4	
1.10	Authenticator feedback	1,2,3,4	CR
1.11	Unsuccessful login attempts	1,2,3,4	CR
1.12	System use notification	1,2,3,4	CR
1.13	Access via untrusted networks	1,2,3,4	NDR
	• Explicit access request approval	3,4	
1.14	Strength of symmetric key-based authentication	2,3,4	CR
	• Hardware security for symmetric key-based authentication	3,4	

FR 2 – Use control (UC) / Control de uso

		Nivel de Seguridad (SL 1-4)	**Tipo de componente** (CR, SAR, HDR, NDR, EDR)
	Requisitos		
2.1	Authorization enforcement	1,2,3,4	CR
	• Authorization enforcement for all users (humans, software processes and devices)	2,3,4	
	• Permission mapping to roles	2,3,4	
	• Supervisor override	3,4	
	• Dual approval	4	
2.2	Wireless use control	1,2,3,4	CR
2.3	Use control for portable and mobile devices	--	CR
2.4	Mobile code	2,3,4	SAR, EDR, HDR, NDR
	• Mobile code authenticity check	3,4	
2.5	Session lock	1,2,3,4	CR
2.6	Remote session termination	2,3,4	CR
2.7	Concurrent session control	3,4	CR
2.8	Auditable events	1,2,3,4	CR
2.9	Audit storage capacity	1,2,3,4	CR

	• Warn when audit record storage capacity threshold reached	3,4	CR
2.10	Response to audit processing failures	1,2,3,4	CR
2.11	Timestamps	1,2,3,4	CR
	• Time synchronization	2,3,4	
	• Protection of time source integrity	4	
2.12	Non-repudiation	1,2,3,4	CR
	• Non-repudiation for all users	1	
2.13	Use of physical diagnostic and test interfaces	2,3,4	EDR, HDR, NDR
	• Active monitoring	3,4	

FR 3 – System integrity (SI) / Integridad del sistema

		Nivel de Seguridad (SL 1-4)	**Tipo de componente** (CR, SAR, HDR, NDR, EDR)
	Requisitos		
3.1	Communication integrity	1,2,3,4	CR
	• Communication authentication	2,3,4	
3.2	Protection from malicious code	1,2,3,4	SAR, EDR, HDR, NDR
	• Report version of code protection	2,3,4	HDR
3.3	Security functionality verification	1,2,3,4	CR
	• Security functionality verification during normal operation	4	
3.4	Software and information integrity	1,2,3,4	CR
	• Authenticity of software and information	2,3,4	
	• Automated notification of integrity violations	3,4	
3.5	Input validation		CR
3.6	Deterministic output	1,2,3,4	CR
3.7	Error handling	1,2,3,4	CR
3.8	Session integrity	2,3,4	CR
3.9	Protection of audit information	2,3,4	CR
	• Audit records on write-once media	4	
3.10	Support for updates	1,2,3,4	EDR, HDR, NDR
	• Update authenticity and integrity	2,3,4	
3.11	Physical tamper resistance and detection	2,3,4	EDR, HDR, NDR
	• Notification of a tampering attempt	3,4	
3.12	Provisioning product supplier roots of trust	2,3,4	EDR, HDR, NDR
3.13	Provisioning asset owner roots of trust	2,3,4	EDR, HDR, NDR
3.14	Integrity of the boot process	1,2,3,4	EDR, HDR, NDR
	• Authenticity of the boot process	2,3,4	

FR 4 – Data confidentiality (DC) / Confidencialidad de los datos

		Nivel de Seguridad (SL 1-4)	**Tipo de componente** (CR, SAR, HDR, NDR, EDR)
	Requisitos		
4.1	Information confidentiality	1,2,3,4	CR
4.2	Information persistence	2,3,4	CR
	• Erase of shared memory resources	3,4	
	• Erase verification	3,4	
4.3	Use of cryptography	1,2,3,4	CR

FR 5 – Restricted data flow (RDF) / Flujo de datos restringido

		Nivel de Seguridad (SL 1-4)	**Tipo de componente** (CR, SAR, HDR, NDR, EDR)
	Requisitos		
5.1	Network segmentation	1,2,3,4	CR
5.2	Zone boundary protection	1,2,3,4	NDR
	• Deny all, permit by exception	2,3,4	
	• Island mode	3,4	
	• Fail close	3,4	
5.3	General purpose, person-to-person communication restrictions	1,2,3,4	NDR

FR 6 – Timely response to events (TRE) / Respuesta oportuna a los eventos

		Nivel de Seguridad (SL 1-4)	**Tipo de componente** (CR, SAR, HDR, NDR, EDR)
	Requisitos		
6.1	Network segmentation	1,2,3,4	CR
	• Programmatic access to audit logs	3,4	
6.2	Continuous monitoring	2,3,4	CR

FR 7 – Resource availability (RA) / Disponibilidad de recursos

		Nivel de Seguridad (SL 1-4)	**Tipo de componente** (CR, SAR, HDR, NDR, EDR)
	Requisitos		
7.1	Denial of service protection	1,2,3,4	CR
	• Manage communication load from component	2,3,4	
7.2	Resource management	1,2,3,4	CR
7.3	Control system backup	1,2,3,4	CR
	Backup integrity verification	2,3,4	
7.4	Control system recovery and reconstitution	1,2,3,4	CR
7.5	Emergency power	--	CR
7.6	Network and security configuration settings	1,2,3,4	CR
	• Machine-readable reporting of current security settings	3,4	
7.7	Least functionality	1,2,3,4	CR
7.8	Control system component inventory	2,3,4	CR

Leyenda
CR: Requisito común a todos los tipos de componentes
SAR: Requisito aplicables a software
EDR: Requisito relativo a Dispositivos Integrados
HDR: Requisito relativo a Dispositivos Host
NDR: Requisito relativo Dispositivo de Red