

Nota informativa

Proceso de certificación eIDAS con TCAB

Esta **nota informativa** tiene por objetivo explicar las etapas principales del proceso de evaluación y certificación eIDAS por parte de Trust Conformity Assessment Body (en adelante, TCAB).

Proceso de auditoría

La compañía auditada debe tener implementado, en todo caso, un Sistema de Gestión que cumpla con los criterios de evaluación que TCAB considere necesarios, en concordancia con la normativa aplicable: ETSI, Reglamento eIDAS (Reglamento (UE) 910/2014). Este Sistema de Gestión, el servicio y la infraestructura que lo soporta será objeto de auditoría por parte de TCAB.

Antes de iniciar el proceso en sí mismo, los auditores de TCAB tendrán una reunión de pre-auditoría con el cliente para confirmar el alcance, los datos recopilados en el Plan de auditoría, establecer una secuencia de la auditoría y analizar los puntos necesarios. Después de este paso, la auditoría comenzará siguiendo el Plan de Auditoría como guía de trabajo.

En concreto, el proceso de auditoría se lleva a cabo en dos etapas:

- **Revisión documental:** Se comprobará la conformidad del sistema (documentación, registros...), mediante el cumplimiento de los puntos de las normas y/o leyes de referencia. Se verificará la resolución de posibles no conformidades de auditorías anteriores.
- **Inspección presencial:** Se llevarán a cabo pruebas de cumplimiento de los controles implantados. Se examinarán por muestreo las evidencias objetivas para comprobar la correcta operación de procesos técnicos y organizacionales relacionados con el alcance de la auditoría. Se verificará la resolución de posibles no conformidades de la revisión documental.

Una vez finalizada la auditoría, el equipo de auditoría redactará un informe de resultados denominado **Informe de Evaluación de la Conformidad (Conformity Assessment Report – CAR, en inglés)** para ser presentado a la autoridad supervisora de la entidad¹ y un **informe breve de auditoría** apto para ser publicado, identificando de forma clara y definida las desviaciones detectadas.

Los hallazgos en la auditoría pueden ser de los siguientes tipos:

- **No Conformidad Mayor:** Incumplimiento sistemático y crítico contra un Apartado de la/s Norma/s de referencia o un procedimiento establecido, de tal manera que no se puede garantizar la seguridad o la continuidad de los servicios, procesos o

¹ Es obligatorio enviar el CAR al organismo supervisor dentro de los 3 días posteriores a su recepción.

actividades. Su aparición supone la no certificación inicial o la pérdida de la existente. Requiere acciones correctivas inmediatas.

- **No Conformidad Menor:** Incumplimiento puntual (no sistemático) y no crítico contra un Apartado de la/s Norma/s de referencia o un procedimiento establecido, de tal manera que aun siendo un fallo del Sistema, se puede garantizar la seguridad o continuidad de los servicios, procesos o actividades. Su aparición en una auditoría supone un toque de atención, pero nunca la no certificación inicial o la pérdida de la existente. Un número importante de ellos puede suponer un indicio de precariedad del sistema y constituir en su conjunto un incumplimiento muy grave. Requiere acciones correctivas y evidencia de su implementación antes de que se pueda tomar ninguna decisión positiva respecto a la certificación.
- **Observación:** Situaciones poco recomendables con potenciales riesgo de desviación en un futuro que conviene que el auditor ponga de manifiesto. No requieren acciones correctivas, si bien es recomendable su vigilancia por parte de la entidad.
- **Mejora:** Oportunidad detectada por el auditor para incrementar la eficacia y/o seguridad del servicio, sistema, procesos o actividades.

Además, habrá una reunión final en la que el equipo de auditoría expondrá los hallazgos encontrados al cliente, para que pueda comentarlos y revisarlos. En aquellos casos donde hay presencia de no conformidades significativas, se programará una nueva fecha para la siguiente auditoría para verificar la corrección y eliminación de esas no conformidades.

El cliente debe conservar registros de todos los informes de auditoría de los que TCAB haga entrega durante, al menos, seis años o hasta que estos queden obsoletos.

Proceso de certificación

Tras una decisión de certificación positiva, TCAB proporcionará la documentación referida a la certificación, incluido el certificado acreditativo del resultado positivo de la auditoría. TCAB realizará las tareas de vigilancia del certificado emitido de forma semestral.

Las actividades de vigilancia buscarán confirmar la conformidad del servicio evaluado en los contextos del esquema, el uso de la marca de conformidad y la imagen asociada a TCAB, así como cualquier uso de la marca o imagen de la entidad de acreditación de las actividades de TCAB (garantizando que no se hace uso de la misma).

Asimismo, se realizará una auditoría de revisión anualmente para comprobar el cumplimiento satisfactorio de requisitos de la misma forma en que se certificó.

Por último, TCAB mantendrá información sobre los productos certificados que contendrá los siguientes datos:

- Identificación del producto y del cliente.
- Normativa con la cual se ha certificado la conformidad.
- Validez de la certificación.

Cuando TCAB suministra la información a un Esquema ya definido, el directorio del Esquema puede satisfacer este requisito.

En caso contrario se encontrará accesible esta información en un directorio habilitado para ello en la página web de TCAB.

Transferencia de una certificación

Los clientes que lo deseen pueden transferir su certificación desde otro Organismo de Evaluación de la Conformidad a TCAB.

El cliente deberá transferir la documentación relativa a la certificación para que TCAB pueda realizar una revisión documental. Si dicha información no resultase suficiente para que TCAB conceda la certificación tras una revisión exhaustiva por el personal de TCAB, se realizará una evaluación en las instalaciones del cliente antes de recomendar la aprobación.

Una vez que TCAB haya emitido la decisión de certificación, y siempre y cuando esta haya sido positivo, se llevarán a cabo acciones y visitas de vigilancia para mantener la certificación.

Si no se encontrase ningún problema en la revisión documental o en las visitas, TCAB emitirá el certificado. La fecha de caducidad del certificado dependerá del certificado que se sustituya. Si el certificado actual:

- No tiene fecha de caducidad: el certificado de TCAB será válido por un periodo de tres años, salvo que el esquema de certificación tenga un ciclo de validez inferior.
- Tiene fecha de caducidad: la validez del certificado de TCAB será la del certificado existente o el periodo de validez del esquema con el que se haya realizado la auditoría, la que sea menor.

Confidencialidad

TCAB garantiza la más absoluta confidencialidad de cualquier información relativa a su empresa que se trate con motivo del proceso de auditoría (incluyendo en contenido de los Informes de Evaluación de la Conformidad).

Solo se compartirá este tipo de información en caso de que el cliente otorgue una autorización expresa a TCAB.

Más información

Si desea conocer más sobre TCAB o los servicios que ofrece, por favor visite nuestra página web: www.tcab.eu.

Documentos relacionados

- IT.PC.02-05 Nota informativa II – Suspensión o retirada
- IT.PC.02-06 Nota informativa III – Apelaciones y quejas

Control de versiones

Versión	Fecha	Cambios
1.0	30/04/2018	Primera emisión
2.0	25/06/2019	Clarificación de ciertos conceptos. Harmonización con la versión en inglés.