DP_ENS_02
DOCUMENTO PÚBLICO DEL PROCESO DE CERTIFICACIÓN DEL ESQUEMA NACIONAL DE SEGURIDAD

PROCESO COMERCIAL.

El proceso se inicia con la solicitud por parte del cliente que se realizará en el formato establecido para tal fin.
Los datos son revisados a fin de garantizar que toda la información pertinente queda reflejada en la referida solicitud.
Una vez verificados los datos de la solicitud y que estos son completos se procede a la elaboración de la oferta

PLANIFICACIÓN

Una vez aceptada la oferta el departamento técnico acuerda con el cliente las fechas de auditoría. Una vez fijadas fechas, el departamento técnico procede a designar al equipo auditor que podrá ser recusado por el cliente.
La auditoría se podrá realizar, en remoto, mixta, -en ambos casos, previo análisis de riesgos y que se pueda confirmar la viabilidad de la auditoría en remoto-, o in situ.

REVISIÓN DOCUMENTAL

Previo a la realización de la auditoria en las instalaciones de cliente, el auditor jefe solicitara la documentación conforme se indica en la guía CCN-STIC 802

PLAN DE AUDITORIA

Conforme al estudio documental, el auditor jefe remite a la organización, con plazo suficiente, el plan de auditoría.

REALIZACIÓN AUDITORIA

El equipo auditor, dirigido por el auditor jefe verificará todas las disposiciones aplicables del ENS mediante revisión de registros, entrevistas con el personal y por observación directa.
Los hallazgos de la auditoría se clasifican en no conformidades mayores, no conformidades menores y observaciones.
El auditor jefe es el responsable de elaborar el informe que recoja las evidencias obtenidas durante la auditoria y el dictamen de la evaluación que puede ser:

- Favorable (no se han detectado “No Conformidad Mayor” o “No Conformidad Menor)
- Favorable con no conformidades (se han detectado “No Conformidades Menores” y/o “No Conformidades Mayores”)
- Desfavorable (Existe un número significativo de No Conformidades Mayores cuya solución no pueda evidenciarse a través de un Plan de Acciones Correctivas)

Contra las no conformidades identificadas en la Auditoría la organización cliente podrá interponer apelaciones si así lo considera.

ACCIONES CORRECTIVAS

Para dictámenes de favorable con no conformidades, La organización cliente dispone de 30 días desde la firma electrónica del informe para presentar un plan de acciones correctivas sobre la totalidad de las no conformidades -mayores o menores-

En el caso de dictámenes desfavorables, la organización cliente deberá someterse a una auditoría extraordinaria en un plazo no superior a seis meses desde la emisión del informe.
Asimismo, con independencia del dictamen, se realizarán auditorías extraordinarias siempre que se produzcan modificaciones sustanciales en los sistemas de información, incrementos de categoría o ampliaciones del alcance de certificación, conforme a lo indicado en la Guía CCN-STIC 802 y en los Criterios Generales de Auditoría IC-01/19.

REVISIÓN

La revisión es realizada por el revisor técnico cualificado y que no haya participado en el proceso de auditoría.
La revisión es completa desde la solicitud de oferta hasta la evaluación del PAC, si fuera el caso.
Las organizaciones certificadas o en proceso de certificación tienen el derecho de apelar a las decisiones de certificación

EMISIÓN

Cuando la decisión es favorable se emite un certificado cuya validez es de dos años y se emitirá en castellano o a petición de la organización cliente, en castellano en castellano y, a petición de la organización cliente, en otra lengua cooficial.

La vigencia se mantiene por dos (2) años o hasta que se produzcan modificaciones sustanciales en el sistema de información auditado que hagan necesario verificar de nuevo la eficacia de las medidas de seguridad implantadas, conforme al art. 38 del RD 311/2022 y la Guía CCN-STIC 802.

COMUNICACIÓN AL CCN

ACCM comunicará al Centro Criptológico Nacional dentro de los 15 días desde la emisión del certificado por medio de AMPARO, así como cualquier cambio asociado al mismo como modificación, suspensión o retirada.

ACTIVIDADES DE VIGILANCIA

Con periodicidad máxima de seis meses y tomando como fecha de referencia la emisión del certificado, ACCM vigilará el cumplimiento de marca conforme a lo referenciado en la guía CCN-STIC-809.
Ante un uso incorrecto, se procederá a informar a la organización como de un proveedor de esta para su subsanación en un plano no superior a un mes y en caso, de no subsanación, se comunicará directamente al CCN.

SUSPENSIÓN Y RETIRADA.

Un certificado podrá ser suspendido, cuando se incumplen las cláusulas establecidas en las Reglas para el Uso del Distintivo de Conformidad, por desviaciones en auditoria completa no inicial o a solicitud de cliente.
El periodo de suspensión es específico de cada caso y no podrá ser superior a seis meses. Cuando las condiciones que dieron a lugar una suspensión del certificado sean subsanadas se podrá solicitar la restauración de una certificación suspendida, caso contrario la certificación será retirada.

CAMBIOS EN EL SISTEMA O ALCANCE

Cuando se produzcan cambios sustanciales en el sistema de información, modificaciones en el alcance certificado o una recategorización del sistema (por incremento o disminución de categoría), la organización deberá comunicarlo al Organismo de Certificación. En función de la magnitud de los cambios, se determinará la necesidad de realizar una auditoría extraordinaria parcial o completa, limitada a los aspectos afectados. Estas auditorías no alteran la fecha de cómputo del ciclo de certificación ordinaria de dos años salvo que abarquen la totalidad de los requerimientos del ENS (IC-01/19, epígrafe 2.7 y 2.16).