Descripción del procedimiento de certificación de Sistemas de Gestión ENS

La certificación de un sistema ENS basado en la norma ISO 17065, consta de la fase de oferta y contratación, la preparación de la auditoría, realización de la Etapa 1 auditoría con evaluación de la documentación de gestión, realización de la auditoría de Etapa 2, emisión de certificado y seguimiento/recertificación.

Los auditores son seleccionados por el Responsable del Organismo de Certificación de DEKRA Certification SLde acuerdo con sus requisitos y procedimientos de cualificación.

Procedimiento de certificación

El proceso de certificación de una entidad comienza cuando el cliente proporciona una solicitud oficial para comenzar el proceso de certificación firmada por el representante autorizado del cliente. Al aceptar la solicitud, DEKRA, actuando como Organismo de Evaluación de la Conformidad (CAB), proporciona al cliente potencial un acuerdo de Servicios de Certificación, que incluye las tarifas de certificación, y una estimación del cronograma del proyecto.

Tras la aceptación del acuerdo, el CAB requiere que el cliente haga todos los arreglos necesarios para la realización de la auditoría. Incluye disposiciones para el examen de la documentación y el acceso a todas las áreas, incluidas las de los subcontratistas, los registros (incluidos los informes de auditoría interna y los informes de exámenes independientes de la seguridad de la información) y el personal con fines de auditoría, auditoría de reevaluación y resolución de quejas.

El CAB requiere que el solicitante proporcione al menos la siguiente información, antes de la auditoría in situ:

- Información general sobre el cliente y las actividades que cubre y el alcance de la auditoría.
- información sobre ubicaciones, tamaños y funciones, y sus sitios subcontratistas, que proporcionan o contribuyen a proporcionar al cliente.
- una copia de la documentación sobre las políticas, la declaración de aplicabilidad (SoA) y los procedimientos que rigen la prestación y el funcionamiento del cliente y, cuando sea necesario, la documentación asociada, como los planos de infraestructura de red de TI con todos los sistemas, manuales e instrucciones pertinentes para el funcionamiento del cliente.

El objetivo de la auditoría es confirmar y certificar que el cliente proporciona cumple con los criterios de evaluación aplicables.

El equipo de auditoría revisará antes de la auditoría qué registros son considerados confidenciales o sensibles por el cliente, de modo que el equipo de auditoría no pudo examinarlos durante la auditoría. El equipo de auditoría juzgará si los registros que pueden examinarse son suficientes para una auditoría eficaz. Si el equipo de auditoría llega a la conclusión de que no se justifica una auditoría eficaz, el CAB informará al cliente de que la auditoría sólo podría llevarse a cabo cuando el cliente haya aceptado los acuerdos de acceso adecuados a la información confidencial o sensible.

La auditoría puede realizarse en línea a discreción del auditor principal. Si se considera necesario, la auditoría podría incluir visitas a los sitios del cliente. El CAB acordará con el cliente cuándo y dónde se lleva a cabo el proceso de auditoría. El equipo de auditoría llevará a cabo su auditoría del cliente y de sus clientes en al menos dos etapas.

Auditoría de la etapa 1

En preparación para la auditoría, el equipo de auditoría deberá obtener y revisar la documentación

sobre el cliente y los servicios auditados del cliente. El equipo de auditoría deberá informar al cliente de cualquier otro tipo de información y registros que puedan ser necesarios adicionalmente para la verificación durante la auditoría de la ETAPA 1. En esta etapa de la auditoría, el CAB también deberá obtener documentación sobre el diseño del (los) cliente(s).

Los objetivos de la auditoría de la ETAPA 1 son proporcionar un enfoque para la planificación de la auditoría de la ETAPA 2 mediante la comprensión de la estructura y el alcance de los servicios auditados del cliente. La auditoría de la ETAPA 1 incluirá, entre otros, la revisión de documentos. Otros elementos que pueden incluirse en la auditoría de la ETAPA 1 son la verificación de los registros relacionados con la persona jurídica, los acuerdos para cubrir la responsabilidad, las relaciones contractuales entre el cliente y los contratistas potenciales que operan o prestan servicios de subcomponentes, auditorías o certificaciones internas / externas, revisión de la gestión e investigaciones adicionales con respecto a la auditoría preliminar de los cumplimientos o incumplimientos parciales autodeclarados.

El equipo de auditoría acordará, con el cliente, cuándo y dónde se llevará a cabo la auditoría de la ETAPA 1. Los informes de la ETAPA 1 serán presentados por el líder del equipo de auditoría al CAB. En todos los casos, la revisión de la documentación se completará antes del comienzo de la auditoría de la ETAPA 2.

Los resultados de la auditoría de la ETAPA 1 se documentarán en un informe escrito que incluya cualquier recomendación sobre la planificación para llevar a cabo la auditoría de la ETAPA 2. Los hallazgos de la auditoría de la ETAPA 1, relacionados con las desviaciones de la documentación o incluida la identificación de cualquier área de preocupación que pueda clasificarse como no conformidad durante la auditoría de la ETAPA 2, se comunicarán al cliente.

Al determinar el intervalo entre las auditorías de la ETAPA 1 y la ETAPA 2, se tendrán en cuenta las necesidades del cliente para resolver las áreas de preocupación identificadas durante la auditoría de la ETAPA 1. Es posible que el CAB también necesite revisar sus disposiciones para la ETAPA 2.

El CAB informará al cliente de la planificación de la auditoría de la ETAPA 2 de la evaluación y de los otros tipos de información y registros que pueden ser necesarios para la verificación detallada durante la auditoría de la ETAPA 2.

Auditoría de la etapa 2

Esta etapa puede llevarse a cabo en línea a discreción del auditor principal. Si se considera necesario, la auditoría podría incluir visitas a los sitios del cliente. Sobre la base de las observaciones documentadas durante la auditoría de la ETAPA 1, el equipo de auditoría elaborará un plan de auditoría para la realización de la auditoría de la ETAPA 2.

Los objetivos de la auditoría etapa 2 son:

- confirmar que el cliente se adhiere a sus propias políticas, SoA, alcance, objetivos y procedimientos; y
- Para confirmar que los clientes implementados cumplen con los requisitos de los criterios de auditoría aplicables y cumplen con las políticas, objetivos y procedimientos del cliente aplicable.

Para ello, la auditoría se centrará en recoger evidencias sobre los clientes del cliente con respecto a:

- implementación de los requisitos del cliente;
- procesos y procedimientos organizacionales relacionados con el cliente;

- procesos y procedimientos técnicos relacionados con el cliente;
- implementó medidas de seguridad de la información para los clientes, incluida la protección de la red de TI;
- productos y servicios relacionados con el alcance de la auditoría del cliente;
- y la seguridad física de los sitios de los clientes pertinentes.

Los resultados de la auditoría de la ETAPA 2 se documentarán en un informe escrito que incluya las conclusiones obtenidas después de la auditoría in situ. Los resultados de la auditoría de la ETAPA 2, resultantes de la ejecución del plan de auditoría, se comunicarán al cliente. El cliente definirá un plan de acción correctiva para las no conformidades identificadas durante esta etapa. Las no conformidades identificadas pueden requerir una revisión adicional in situ por parte del equipo de auditoría.

Cuando el Líder del Equipo de Auditoría considera que todos los hallazgos/no conformidades identificados durante la ETAPA 2 son resueltos por el cliente, la ETAPA 2 se considera terminada.

CAR

El equipo de auditoría, con la supervisión del Jefe del Equipo de Auditoría, completará el Informe de Evaluación de la Conformidad (CAR), que determina el cumplimiento del cliente solicitante de acuerdo con la normativa ENS aplicable.

El dictamen final de la CAR será uno de los tres siguientes:

- "APTO": cuando no se evidencie ninguna "No Conformidad Mayor" o "No Conformidad Menor".
- "PASA CON NO CONFORMIDAD": Cuando se evidencian "No Conformidades Mayores" y/o "No Conformidades Menores". En este caso, la entidad propietaria responsable del sistema de información auditado presentará, en el plazo máximo de un mes, un Plan de Acción Correctiva (PAC) sobre dichas desviaciones a la entidad de certificación para su evaluación.
- "FAIL": Cuando existe un número significativo de No Conformidades Mayores cuya solución no puede ser evidenciada a través de un Plan de Acción Correctiva y requiere verificación in situ de su correcta implementación a través de una auditoría extraordinaria.

Aprobación Provisional de conformidad (PCA)

Excepcionalmente, se puede emitir una Aprobación Provisional de Conformidad (PCA) debido a un proceso de certificación en el que se cumplen simultáneamente los siguientes requisitos:

- Tramitación de la emisión del primer Certificado de Conformidad.
- El Plan de Acción Correctiva, por razones apropiadas y razonables, requiere un período de implementación de más de 3 meses.
- No se puede aplicar cuando se han detectado no conformidades importantes. Solo es aplicable a sistemas de información con categorías básicas o medias.

FRECUENCIA DE LAS AUDITORÍAS

Habrá un período no superior a dos años para una auditoría de (re)evaluación completa, a menos que la legislación aplicable o el esquema comercial que aplique el presente documento exijan lo

contrario.

REVISIÓN DE LOS RESULTADOS DE LA EVALUACIÓN

El Responsable del CAB reúne toda la información requerida, incluido el Informe de Evaluación de la Conformidad (CAR), que sirve como evidencia de la conformidad del cliente con el esquema de certificación y realiza una revisión preliminar de los resultados de la auditoría. El propósito de la revisión preliminar es garantizar que toda la información esté disponible y completa. A continuación, el Responsable del CAB elabora un Informe de Certificado que se presenta al Comité de Certificación para su revisión oficial.

El Comité de Certificación lleva a cabo una revisión oficial de los resultados de la auditoría inmediatamente antes y junto con su decisión, que será la emisión del Certificado del cliente o la denegación del Certificado del cliente.

Gestión de no conformidades

Se debe realizar un análisis de las causas de cada no conformidad y se deben implementar las acciones correctivas correspondientes. La organización tiene el deber, dependiendo de la gravedad de la no conformidad, de informar al equipo de auditoría dentro del periodo establecido, ya sea con respecto a las acciones correctivas que se han establecido y las fechas para su implementación o que el se han implementado acciones correctivas. Si no se respeta este plazo, la auditoría se considera no exitosa, es decir, no superada. No se puede emitir ningún certificado o se retira un certificado existente.