Proceso de certificación de conformidad con el **Esquema Nacional de Seguridad**

Según Real Decreto 311/2022 de 8 de enero

1. ALCANCE

Este documento describe el Proceso de Certificación que ha desarrollado Bureau Veritas, para realizar auditoría de evaluación de conformidad de acuerdo con el R.D. 311/2022 de 8 de octubre Esquema Nacional de Seguridad (en adelante ENS). Atendiendo así al requerimiento que realiza el ENS, en su art. 31 auditoría de la seguridad.

Este procedimiento es aplicable a cualquier entidad que solicite a Bureau Veritas la contratación de nuestro servicio de auditoría, y en concreto la auditoria de evaluación de conformidad con ENS.

Bureau Veritas como Entidad de Certificación de tercera parte, nunca puede subcontratar a personal externo el proceso de toma de decisión de certificación.

2. ESQUEMA NORMATIVO

Este documento ha sido elaborado teniendo en cuenta los criterios establecidos en:

Marco de control:

- ISO/IEC 17065. Evaluación de la conformidad. Requisitos para organismos que certifican productos y servicios.
- Real Decreto 311/2022, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- ENS: Guías CCN – STIC (Principalmente serie 800 y 101)

Documentación relacionada con el proceso de acreditación y certificación de conformidad del ENS

- Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.
- Resolución de 13 de octubre de 2016, de la secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Conformidad con el Esquema Nacional de Seguridad.
- CCN-CERT IC-01/19 - ENS: Criterios adicionales de Auditoría y Certificación.
- D - Producto. Lista de documentos para la Acreditación de Entidades de Certificación de Producto.
- PAC-ENAC - Procedimiento de Acreditación.
- CEA-ENAC - 01 Criterios para la utilización de la marca ENAC o referencia a la condición de acreditado.
- RDE - 24 Criterios y procesos de acreditación específico para la certificación de la Conformidad con el Esquema Nacional de Seguridad (ENS).
- NT - 17 Independencia, imparcialidad e integridad de las entidades.
- NT - 37 Conversión de certificados no acreditados en certificados bajo acreditación ENAC.
- NT - 60 Entidades de Certificación de Producto: Acreditación para Alcances Flexibles.
- NT - 72 Notificación de cambios.
- NT - 80 Evaluación de actividades en el extranjero (antes NO-05).
- NO - 11 No Conformidades y Toma de Decisión.
- G-ENAC - 22 Consultoría e independencia de los organismos de evaluación de la conformidad.
- G-ENAC - 23 Guía de auditorías en remoto.
- G-ENAC - 24 Guía para el aseguramiento de la integridad de datos.
- Instrucción Técnica de Seguridad (ITS) de conformidad con el Esquema Nacional de Seguridad (Documento BOE-A-2016-10109).
- Instrucción Técnica de Seguridad (ITS) de Informe del Estado de la Seguridad. (Documento BOE-A-2016-10108).
- Instrucción Técnica de Seguridad (ITS) de Auditoría de la Seguridad. (Documento BOE-A-2018-4S73).

Los documentos citados no son limitativos pudiendo incluir algún documento adicional de aplicación y que podrán ser consultados por diferentes medios: como en los diferentes medios de consulta: www.boe.es, www.ccn-cert.cni.es

3. PROPUESTA DE CERTIFICACIÓN

A petición de la organización que solicite la certificación de Conformidad del ENS confirmará a BUREAU VERITAS los sistemas de información a certificar y la categorización de los mismos (Básica, Media, Alta).

Como parte del proceso de certificación, Bureau Veritas, con el objeto de garantizar la imparcialidad e independencia de sus procesos, ha segregado las tareas comerciales de las tareas del cálculo de jornadas de auditoría, como buenas prácticas y cumplimiento de los requisitos de acreditación. Aplicando la segregación de tareas de las responsabilidades de las partes intervinientes en las actividades de elaboración de oferta de certificación.

3.1 Solicitud de oferta

Cuando el cliente muestra su interés en realizar una petición de oferta de auditoría de conformidad con el ENS, deberá ponerse en contacto con Bureau Veritas y se le asignará un comercial, quien se hace responsable de todas su peticiones, a nivel comercial.

El comercial asignado, le enviará un formulario, SF01, deberá rellenar el documento con toda la información que se solicita. Esta información es necesaria para poder elaborar el cálculo del tiempo de auditoría necesario para abordar la evaluación de conformidad con el ENS.

Una vez cumplimento el documento deberá enviarlo al comercial que es responsable de su cuenta para que podamos revisar la información aportada.

3.2 Revisión de la información

Una vez recibido el documento, el área correspondiente, centro técnico de ofertas (CTO), revisará que toda la información solicitada está correctamente cumplimentada.

Cabe mencionar que en caso de errores o datos incompletos, CTO, notifica al Responsable Técnico del Esquema RTS tal circunstancia, y éste se pondrá en contacto con la empresa para solicitar las aclaraciones necesarias, hasta la completitud de la información requerida.

3.3 Cálculo de las jornadas

CTO, tras la revisión del formulario SF01, procede a realizar los cálculos para determinar el tiempo exacto para la realización de la auditoría.

Cabe mencionar que este proceso es imparcial, se aplican las tablas de referencia conforme al documento Tabla Cálculo Jornadas Auditorías ENS.

Para el cálculo de las jornadas se tiene en cuenta una serie de factores como son: complejidad de los sistemas de información, Magnitud del Alcance, número de emplazamientos incluidos, número de personas incluidas, entre otros factores, Categoría del Sistema de Información, a mayor categoría más controles se deberán evaluar.

Los tiempos incluyen:

- Revisión documental previa para la preparación de la auditoría.
- Realización de la auditoría.
- Elaboración del Informe de auditoría.

3.4 Revisión del cálculo de jornadas

Tras la elaboración de los cálculos de la oferta, será necesaria la revisión de las jornadas de auditoría, antes del envío al área comercial que deberá ser siempre aprobado por el RTS o Dirección Técnica.

3.5 Envío de la documentación al comercial y Revisión de oferta

Tras la revisión de los cálculos de las jornadas, se devolverá la información junto a la distribución del tiempo de jornadas de auditoría del ENS al área Comercial para que proceda a la elaboración de la oferta, que posteriormente lo enviará al cliente.

Una vez recibida la aceptación de la oferta aceptada por el cliente, el área de Client Services lo subirá a la plataforma para que se proceda a la revisión de la oferta y posterior planificación de la auditoría de Certificación de Conformidad con el ENS.

La aceptación de la oferta, supone la aceptación de las condiciones del contrato, entre Bureau Veritas y el cliente.

3.6 Análisis de riesgos del proceso de Revisión de oferta

La realización de una oferta entraña una serie de riesgos relacionados con el proceso de auditoría de certificación, que podría afectar a la eficacia del sistema de gestión de Bureau Veritas y al cumplimiento de los requisitos de acreditación, impactando negativamente en la continuidad de una de las líneas de negocio de la entidad de certificación. Igualmente el análisis de riesgo puede identificar las oportunidades de mejora en el proceso de auditoría, como pilar fundamental de la mejora continua.

Actividades identificadas en el proceso:

- Recogida datos clientes.
- Cálculo de jornadas de auditoría.
- Revisión de las jornadas.
- Imparcialidad/Confidencialidad/ Independencia (ICI).
- Registros y control.
- Elaboración de la oferta.
- Revisión de la oferta/Solicitud.

4. LOS AUDITORES DE BUREAU VERITAS CERTIFICATION

Los auditores de Bureau Veritas Certification disponen de acuerdos firmados con la Entidad de Certificación con la finalidad de reforzar los siguientes aspectos:

- La confidencialidad e imparcialidad de los intervinientes.
- La uniformidad del enfoque de la auditoria y de las normas.

Todos los auditores de Bureau Veritas, están cualificados conforme a los requisitos de la del Esquema Nacional de Seguridad, ENS. Disponen de una gran experiencia tanto en el campo de actividad de los servicios en los que se encuadra la auditoría como en la práctica de auditoría de sistemas de gestión de seguridad de sistemas de la información.

Se les designa para formar parte del equipo auditor en función de los tres criterios siguientes:

- La competencia en el campo de actividad de la organización.
- La cercanía al emplazamiento de la empresa.
- La disponibilidad de las fechas indicadas como deseables por la organización.

5. PROCESO DE AUDITORÍA

5.1 Preparación auditoría

Tras la aceptación de la oferta, se planificará la realización de la auditoría.

El área de planificación se comunicará con el cliente para acordar las fechas exactas.

Se asignará a un lead auditor, quien es responsable de la ejecución de la auditoría. El equipo podrá estar compuesto por un lead auditor o bien por varios auditores y un lead auditor.

En el momento de la comunicación del auditor, se solicita al cliente y al auditor que se comprueba la imparcialidad, que en caso de verse afectada, se modifica el equipo auditor.

En el día acordado por ambas partes, se realiza la revisión de la documentación de la preparación de la auditoría.

Esta revisión tiene el siguiente objeto: obtener información para dimensionar las actividades de auditoría, programar reuniones, verificar posibles deficiencias del Sistema de Seguridad.

Documentación requerida como estudio previo a la realización de la auditoría: Política de seguridad, funciones y responsabilidades de seguridad, identificación de los responsables de las áreas implicadas en el alcance, organigrama de la empresa, categorización del sistema, informes de análisis de riesgos, requisitos legales aplicables, informes de auditorías previas, informe de seguimiento de deficiencias detectadas, listado de proveedores externos cuyos servicios estén incluidos en el alcance, sistema de métrica conforme guías CCN-STIC 815, 824. Se envía al cliente un listado completo con todos los requisitos documentales en la programación de la preparación de auditoría.

Elaboración del Plan de Auditoría: el Lead Auditor, deberá redactar el plan de auditoría teniendo en cuenta la información proporcionada por el auditado, los requisitos de cumplimiento de la norma de referencia y los criterios definidos por Bureau Veritas. El plan de auditoría será acorde con las actividades, procesos del auditado, debe reflejar el alcance de la auditoría, los tiempos, las reuniones con los representantes de las áreas a verificar, criterio de la auditoría, ubicaciones, horario, fechas y auditores, método. El plan de auditoría podrá adaptarse en la reunión inicial, a las modificaciones de última hora que pudiera surgir, siempre manteniendo el tiempo total de auditoría.

5.2 Realización de la auditoría

Reunión de apertura. El Lead Auditor, inicia la auditoría con la reunión de inicio, donde confirma una serie de cuestiones relacionadas con la realización de la auditoría: presentación equipo auditor, confidencialidad, seguridad e imparcialidad del equipo, explicación del proceso, objetivo, criterios, métodos, notificación de los hallazgos y alcance de la auditoría, verificación del plan de auditoría, motivos de suspensión de la auditoría, cumplimiento de las medidas de seguridad relacionadas con Prevención de Riesgos Laborales,

Auditoría: El equipo auditor, deberá verificar la conformidad de cada uno de los requisitos definidos en el Real Decreto 311/2022 ENS, alineado con el Alcance y la Categoría del Sistema de Información, Guía CCN STIC 802 y 808.

El equipo auditor debe recopilar las evidencias necesarias, suficientes y significativas, para sustentar su decisión tanto si es conforme, como si es no conforme, con el requisito de la norma auditado. Estas evidencias se recopilan mediante entrevistas, observaciones, revisión de documentos, registros u otros.

Hallazgos: Clasificación: Conforme; Oportunidad de Mejora; Observación; No conformidad menor; No conformidad Mayor. Durante la auditoría el equipo auditor irá informando de los hallazgos detectados, para que sean entendidos por el auditado.

Reunión final: Tras la reunión del equipo auditor, se notificará al auditado un resumen de todos los hallazgos de la auditoría, indicará el proceso de discrepancia, revisará que se ha cumplido el tiempo de auditoría, confidencialidad, método y plazo para el tratamiento de las no conformidades, actividades de Bureau Veritas posteriores.

5.3 Redacción informe auditoría

El informe de auditoría es el documento donde queda plasmado todos los hallazgos detectados durante la auditoría, por ello debe ser preciso, completo, claro en lo referente a: Objetivo de la auditoría, criterio, alcance, identificación de la organización auditada, ubicación, fecha, equipo auditor, hallazgos, resumen ejecutivo, plan de auditoría, conclusión de la auditoría.
Tras la recepción del informe de auditoría, el cliente tendrá el plazo de 1 mes para la enviar a Bureau Veritas el Plan de Acciones Correctivas en adelante PAC, en el caso de que el dictamen haya sido favorable con no conformidades. Deberá enviar evidencias para verificar su implantación. En el caso que el dictamen haya sido desfavorable se deberá realizar una auditoría extraordinaria en el plazo de 6 meses desde la auditoria de certificación.
El plazo para la toma de decisión para un dictamen favorable, habiéndose realizado una auditoria extraordinaria, no puede superar los 6 meses desde el último día de la auditoría de certificación, por lo que se recomienda realizar dicha auditoría extraordinaria en los primeros 4 meses.

5.4 Evaluación y decisión sobre la certificación

Para poder conceder la certificación, las acciones correctivas deben ser adecuadas para resolver las no conformidades detectadas y deben encontrarse adecuadamente implantadas.

No se concederá un certificado de conformidad con el ENS en los casos siguientes:

- Existe una no conformidad mayor para la que no se haya evidenciado el cierre.
- Existan no conformidades menores y el Plan de Acciones presentado no es suficiente para poder resolver las desviaciones.
- Cuando no se presente Plan de Acciones, siendo este necesario, o se presente fuera de plazo.

En algunos casos, Bureau Veritas podrá acordar la concesión o denegación de la certificación, y podrá llevar a cabo la realización de una auditoría extraordinaria, antes de la concesión, para comprobar la implantación de las acciones correctivas.

La decisión de certificación corresponde exclusivamente a BUREAU VERITAS y en ningún caso será externalizada.

5.5 Emisión del Certificado de Conformidad del ENS

Una vez emitida la decisión de certificación, Bureau Veritas, emitirá al cliente el certificado Conformidad de ENS.

Los certificados de Conformidad de ENS se emiten con una vigencia de 2 años siempre y cuando no se den las circunstancias que requieran la realización de una auditoría extraordinaria según lo indicado en el Artículo 31 del RD 311/2022.

Dicha Certificación de Conformidad, así como su distintivo de cumplimiento se expresarán en documentos electrónicos, en formato no editable y poseerán el aspecto que se muestra en los Anexos III y IV respectivamente Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad (aprobada en la Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas).

El certificado no exime en ningún caso de las garantías y responsabilidades que corresponden a la organización conforme a la legislación vigente.

El certificado acredita la conformidad de los sistemas de información con su correspondiente categorización, el cumplimiento del RD 311/2022 que se reflejan en el propio certificado. No se debe hacer uso del certificado, ni de ningún otro documento derivado del proceso de certificación, con objetivos distintos de aquellos para los que se generaron ni con fines engañosos o no autorizados.

5.6 Renovación del Certificado

Antes de finalizar el periodo de 2 años de validez se realiza una auditoría de renovación. La auditoría de renovación seguirá el mismo proceso de auditoría que la certificación inicial.

Al menos con 3 meses de antelación de finalizar el período de validez del certificado, se efectuará la auditoría de recertificación con el fin de comprobar que las condiciones iniciales de certificación se mantienen.

Si del resultado de la auditoría de recertificación el resultado es positivo, se emitiría un nuevo certificado con una vigencia de 2 años.

5.7 Información disponible al público

En conformidad con la norma ISO 17065 y el CCN-Cert, Bureau Veritas Certification mantiene al día una lista de organizaciones certificadas que está accesible al público o bajo solicitud. Asimismo, en la página web existe un buscador que indica las empresas y la situación de sus certificados.

6. SUSPENSIÓN, RESTAURACIÓN, RETIRADA O CANCELACIÓN DE LA CERTIFICACIÓN

Bureau Veritas Certification se reserva el derecho de suspender, retirar o cancelar los certificados emitidos, en cualquier momento del ciclo de certificación si se dan alguna de las tres condiciones siguientes:

- Si la organización no trasmite en el plazo anunciado las respuestas adecuadas a las no.- conformidades.
- Si la organización hace un uso inadecuado de las marcas de certificación, distintivos del ENS o del logo de Bureau Veritas Certification.
- Si la organización no respeta los acuerdos técnicos y comerciales firmados con Bureau Veritas Certification.

Si la certificación se termina (por solicitud del cliente) se suspende o se retira el certificado. Bureau Veritas Certification tomará las acciones informando sobre la situación de un certificado, como retirado o suspendido en su página web, a sí como a CCN-Cert.

En el caso de retiradas o suspensiones para el caso de los operadores del sector privado que presten servicios o provean soluciones a las entidades públicas, a los que resulte exigible el cumplimiento del ENS, deberán:

- Identificar todos sus principales clientes, e informarles por escrito de la suspensión o la retirada, dentro de los tres días hábiles posteriores a la suspensión o la retirada.
- Mantener registros de esta comunicación a sus clientes.
- Cesar cualquier uso las Certificaciones o los Distintivos de Conformidad acerca del cumplimiento de los requisitos de certificación de Conformidad ENS.

7. EXTENSIÓN Y REDUCCIÓN DE ALCANCE DE LA CERTIFICACIÓN

La certificación puede ser ampliada en cualquier momento, con el fin de poder:

- Incorporar nuevos emplazamientos al alcance de la certificación.
- Incluir actividades nuevas en la empresa.
- Modificar la categoría del nivel de la organización certificada.

La ampliación se realiza, generalmente, en el marco de una auditoría de renovación con el fin de minimizar el impacto económico suplementario que podría originarse.

Si las circunstancias lo requieren, Bureau Veritas Certification puede realizar una auditoría específica extraordinaria con el fin de validar la ampliación de la certificación.

Si esta ampliación estaba prevista, no hay que modificar el contrato de certificación, puesto que ya la incluye, pero si no fuera así se debe realizar una modificación o adenda del contrato que permita dimensionar correctamente el tiempo de auditoría sobre los emplazamientos a auditar.

Una reducción de alcance (emplazamientos, actividades o categorías) se puede realizar comunicándolo antes de la realización de la auditoría renovación a Bureau Veritas Certification.

8. MODIFICACIÓN DEL SISTEMA DE GESTIÓN

Si la organización realiza modificaciones importantes en su sistema de gestión, debe informar, de forma inmediata, a Bureau Veritas Certification. Estos cambios serán evaluados de forma que se asegure su compatibilidad con las normas y los referenciales aplicables. En determinadas ocasiones, se podrá realizar una visita de seguimiento especial.

Las modificaciones menores del sistema de gestión se comunicarán al equipo auditor durante las auditorías de renovación con el fin de que las puedan revisar.

9. RECLAMACIONES DE LOS CLIENTES

Las reclamaciones de los clientes o de terceras partes comunicadas a Buereau Veritas son tratadas bajo la responsabilidad de la Dirección Técnica, que investiga y realiza un análisis de las causas. Una vez estudiada se le proporciona al reclamante una respuesta y se registra el tipo de tratamiento dado a la reclamación. Bureau Veritas Certification, realiza un análisis de las reclamaciones con el fin de definir si se deben implantar acciones correctivas o preventivas. El comité de certificación es informado del análisis de las reclamaciones.

10. APELACIONES O RECURSOS

Las organizaciones pueden apelar las decisiones de Bureau Veritas Certification en los siguientes casos:

- Rechazo a aceptar la solicitud de certificación.
- No emisión de un certificado.
- Suspensión, retirada o cancelación de un certificado.

Las apelaciones son tratadas en primer nivel por la Dirección Técnica, y en una segunda etapa por la Dirección General con la información del comité de certificación quien finalmente decide sobre el recurso.

11. CAMBIO DE LAS REGLAS DE ACREDITACIÓN O DE LA REGLAMENTACIÓN APLICABLE

En caso de cambios en los requisitos de acreditación o en las reglamentaciones aplicables al Esquema Nacional de Seguridad, que afecten a los contratos existentes, Bureau Veritas Certification informará a sus clientes de las condiciones para realizar la transición requerida por esos cambios.

El mantenimiento de los certificados vigentes estará condicionado al cumplimiento de los requisitos de la transición que podrá ser objeto de una modificación o adenda al contrato de certificación en vigor.

Para más información:

C/ Valportillo Primera 22-24, 28108 Alcobendas (Madrid)
Teléfono: 91 270 22 00
certification.spain@bureauveritas.com
www.bureauveritas.es

Shaping a World of Trust