Proceso de certificación de conformidad con el Esquema Nacional de Seguridad

Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad

Tabla de contenido

Histórico de modificaciones

Revisión No	Fecha	Comentarios
1.0	Diciembre 2025	Primera edición.

Documentos relacionados

Código	Descripción
CCN-CERT IC-01-19	Criterios Generales Auditorias
CCN-STIC-808	Verificación_del_cumplimiento_del_ENS
GP045/ SUP ENAC	Guía del logotipo de ENAC (GP045 Supp/ENAC)

1. Objeto

El objeto del presente documento es describir el Proceso de Certificación que ha desarrollado BSI Group Iberia SAU (BSI España) para realizar las auditorías de evaluación de conformidad de acuerdo con el R.D. 311/2022 de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (en adelante ENS)., atendiendo así al requerimiento que realiza el ENS, en su art. 31 auditoría de la seguridad.

2. Alcance

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

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

Este documento se basa en el documento Guía de Seguridad CCN-STIC CCN-CERT IC-01/19 que define los Criterios Generales de Auditoría y Certificación, y los requisitos para los Organismos de Certificación que auditan y certifican a los Proveedores de Capacitación de acuerdo con los Criterios para Proveedores de Capacitación y los Estándares de Capacitación en el marco del Esquema Nacional de Seguridad (Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad).

Debe leerse junto con la *Guía de Seguridad CCN-STIC ENS. Criterios generales de auditoría y certificación y la Guía de Seguridad de las TIC CCN-STIC 802. Guía de auditoría ENS.*

3. 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 3 de mayo, por el que se regula el ENS 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).

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, p.ej. consulta www.boe.es, www.ccn-cert.cni.es, etc.

4. Propuesta de certificación

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

Como parte del proceso de certificación, BSI España, 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.

4.1 Solicitud de oferta

Cuando un cliente esté interesado en realizar una petición de oferta de auditoría de conformidad con el ENS, deberá ponerse en contacto con BSI España y se le asignará un comercial, quien se encargará de atenderle y presentarle una oferta personalizada.

El comercial designado le enviará el formulario *PF2123 Formulario de Solicitud de Información (ENS Company Profile*) y el cliente deberá completarlo 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 y presentar la propuesta que mejor se ajuste a las necesidades del cliente.

Una vez cumplimentado el documento, el cliente deberá enviarlo al comercial que es responsable de su cuenta para que podamos revisar la información aportada y elaborar la correspondiente oferta.

4.2 Revisión de la información

Una vez recibido el documento, el área comercial correspondiente revisará que toda la información solicitada está correctamente cumplimentada.

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

4.3 Cálculo de jornadas

El equipo comercial correspondiente, tras la revisión del formulario *PF2123*, procede a realizar los cálculos para determinar el tiempo exacto para la realización de la auditoría.

Cabe mencionar que este proceso es imparcial y se aplican las tablas de referencia recomendadas por el CCN:

Fase de estudio documental previo	Mínimo entre 0,5 y 1 jornada
Fase de auditoría remoto/in situ	❑ BÁSICA: mínimo 1,5 jornada. ❑ MEDIA: mínimo 2,5 jornadas. ❑ Alta: mínimo 3,5 jornadas
Fase de redacción de informes	Cualquier categoría: mínimo 1 jornada

Como se puede observar en la tabla anterior, los tiempos incluyen:

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

Asimismo, el CCN recomienda utilizar el **Anexo C de la norma ISO/IEC 27006** para el cálculo de tiempos de auditoría, teniendo en cuenta distintos factores, como son, entre otros, los siguientes:

Complejidad de los sistemas de información, magnitud del alcance, número de emplazamientos incluidos, número de personas incluidas, categoría de los sistemas de información, etc.

4.4 Revisión del cálculo de jornadas y de oferta

Tras la elaboración de los cálculos de la oferta, será necesaria la revisión de las jornadas de auditoría, y confirmación de disponer de personal cualificado e imparcial antes del envío al área comercial que deberá ser siempre aprobado por el departamento de Operaciones.

4.5 Envío de la documentación al comercial y revisión de oferta

Tras la revisión de los cálculos de las jornadas, el área Comercial procederá a la elaboración de la oferta, que posteriormente lo enviará al cliente.

La aceptación de la oferta supone la aceptación de las condiciones contractuales entre BSI España y el cliente y los Anexos de Derechos Y Obligaciones del cliente ENS.

5. Auditores de BSI España

Los auditores de BSI España disponen de acuerdos firmados con la Entidad de Certificación con la finalidad de reforzar los siguientes aspectos:

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

Todos los auditores de BSI España están cualificados conforme a los requisitos del ENS. Disponen de una gran experiencia tanto en el campo de actividad de los servicios en los que se enmarca la auditoría como en la práctica de auditoría de sistemas de gestión de seguridad de sistemas de la información.

Los auditores son designados 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.

6. Proceso de auditoría

6.1 Preparación de auditoría

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

El equipo 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, y en caso de verse afectada, se modificaría 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 y verificar posibles deficiencias del Sistema de Gestión de Seguridad de la Información.

La documentación requerida como estudio previo a la realización de la auditoría es la siguiente:

- Visión general: análisis de contexto, partes interesadas, etc.
- Alcance del SGSI, actividades, etc.
- Procesos clave, equipos, redes, sistemas informáticos y servicios utilizados.
- Ubicaciones dentro del alcance, incluyendo oficinas y CPDs.
- Política de seguridad de la información.
- Departamentos y funciones, roles y responsabilidades, organigrama.
- Categorización de sistemas.
- Declaración de aplicabilidad.
- Procedimiento y resultados de la evaluación del riesgo.
- Plan de tratamiento del riesgo.
- Listado de requisitos legales de aplicación.
- Informes de auditoría interna/externa previas.
- Planes de acción correctiva de hallazgos de auditorías previas.
- Informe INES.
- Listado de proveedores externos críticos tecnológicos cuyos servicios estén incluidos en el alcance, incluyendo servicios en la nube.
- Sistema de métricas conforme guías CCN-STIC 815, 824.

Se enviará al cliente un listado completo con todos los requisitos documentales en la programación de la preparación de auditoría, además de incluirlo en el documento de oferta.

El Lead Auditor de BSI España 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 BSI España.

El plan de auditoría será acorde con las actividades y procesos del auditado, debiendo reflejar el alcance de la auditoría, los tiempos, las reuniones con los representantes de las áreas que se van a verificar, el criterio, modalidad y metodología de la auditoría, ubicaciones, horario, fechas y miembros del equipo auditor, así como otros posibles asistentes que eventualmente pudieran acudir en calidad de observador, supervisor, etc.

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.

6.2 Realización de auditoría

- *Reunión de apertura:*

El Lead Auditor comienza la auditoría con la reunión inicial, 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, etc.

- *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 comunicará al auditado, en la reunión de cierre, 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 así como las actividades de BSI España posteriores.

6.3 Redacción de informe de auditoría

El informe de auditoría es el documento donde quedan reflejados 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 y conclusión de la auditoría.

Tras la recepción del informe de auditoría, el cliente tendrá el plazo de 1 mes para enviar a BSI España el Plan de Acciones Correctivas (en adelante PAC), a través del Portal de BSI Connect, en el caso de que el dictamen haya sido favorable con no conformidades.

Deberá enviar asimismo evidencias para verificar la subsanación de tales hallazgos.

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.

6.4 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 implementadas.

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, BSI España 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 BSI España y en ningún caso será externalizada.

6.5 Emisión del certificado de conformidad ENS

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

Los certificados de Conformidad de ENS se emiten con una vigencia de **2 años máximo** 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, así como el cumplimiento del RD 311/2022, lo cual 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 según indicado en la Guía del logotipo de ENAC (GP045 Supp/ENAC)

El servicio de auditoria se ofrece como no Acreditado. BSI Group Iberia S.A.U. se encuentra en proceso de solicitud de Acreditación del Esquema Nacional de Seguridad con ENAC. Una vez obtenida la Acreditación por parte de ENAC, se remitirá el certificado ENS acreditado de forma automática y sin coste para el cliente.

6.6 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.

6.7 Información disponible al público

En conformidad con la norma ISO 17065 y el CCN-Cert, BSI España mantiene al día una lista de organizaciones certificadas que está accesible al público en la página web de nuestra organización:

https://www.bsigroup.com/en-MY/products-and-services/assessment-and-certification/validation-and-verification/

Asimismo, existe un buscador del CCN que indica las empresas certificadas ENS y la situación de sus certificados.

Empresas certificadas: Gobernanza de la Ciberseguridad Nacional

7. Suspensión, restauración, retirada o cancelación de la certificación

BSI España 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 BSI.
- Si la organización no respeta los acuerdos técnicos y comerciales firmados con BSI España.

Si la certificación se termina (por solicitud del cliente) se suspende o se retira el certificado, BSI España tomará las acciones informando sobre la situación de un certificado, como retirado o suspendido en su página web, así 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.

8. Extensión y reducción del 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, BSI España 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 BSI España.

El tránsito de una Certificación de Conformidad de categoría BÁSICA a otra de categoría MEDIA, o de categoría MEDIA a otra de categoría ALTA, con la exclusiva evaluación de aquellas medidas que no hayan sido evaluadas en la auditoría anterior, podrá ser posible si concurren las siguientes circunstancias:

- El proceso de realización de la nueva auditoría para la categoría superior, incluyendo la evaluación del Plan de Acciones Correctivas, debe realizarse, íntegramente, dentro del período de validez de la Declaración o Certificación de Conformidad vigente.
- El alcance del sistema de información que pretende elevarse de categoría debe ser exactamente el mismo que el que fue evaluado para la categoría inferior, garantizándose que no se hayan producido cambios en el sistema de información concernido, y, en todo

caso, solo podrá realizarse si no han transcurrido más de seis (6) meses desde la evaluación previa.

- Se deberá mantener la fecha de la Declaración o Certificación de Conformidad con la que se expidió el certificado precedente, lo que supone que el período de validez de la nueva Certificación será coincidente con el expresado en la Declaración o Certificación anterior.

9. Modificación del sistema de gestión

Si la organización realiza modificaciones importantes en su sistema de gestión, debe informar, de forma inmediata, a BSI España.

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.

10. Reclamaciones

Las reclamaciones de los clientes o de terceras partes comunicadas a BSI España 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 cliente que ha presentado la reclamación una respuesta y se registra el tipo de tratamiento dado a la reclamación.

BSI España realiza un análisis de las reclamaciones con el fin de definir si se deben implantar acciones correctivas o preventivas.

El comité Tecnico es informado del análisis de las reclamaciones.

11. Apelaciones o recursos

Las organizaciones pueden apelar las decisiones de BSI España en los siguientes casos:

- Hallazgos y No conformidades levantadas en Auditoria.
- No emisión de un certificado.
- Suspensión, retirada o cancelación de un certificado.

Las apelaciones son tratadas por la Dirección Técnica de forma autónoma e independiente a través de un panel de expertos adentro de los 21 días laborales

12. 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, BSI España 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.