

ENS

ESQUEMA NACIONAL
DE SEGURIDAD

GUÍA CCN-STIC-802



AUDITORÍAS INTERNAS DE VERIFICACIÓN EN EL ENS

Adaptación de los Sistemas de Gestión de Seguridad de la Información (SGSI) ante la actualización de los requisitos de auditoría interna de verificación en el marco del ENS.

**MEJORA
CONTINUA****OPTIMIZACIÓN
DE RECURSOS****INDEPENDENCIA
Y RIGOR**

ASUNTO: Adaptación de los Sistemas de Gestión de Seguridad de la Información (SGSI) ante la actualización de los requisitos de auditoría interna de verificación en el marco del ENS.**Estimados clientes y colaboradores:**

Nos ponemos en contacto con ustedes para trasladarles una importante actualización relativa a la gestión del cumplimiento normativo en el marco del Esquema Nacional de Seguridad (ENS).

Recientemente, el Centro Criptológico Nacional (CCN) ha clarificado en su guía técnica **CCN-STIC-802** el marco regulatorio que rige las auditorías internas de verificación, matizando que no es un requisito exigible en el ENS pero que son muy recomendables para garantizar la eficacia, salud y mejora continua de su Sistema de Gestión de Seguridad de la Información (SGSI).

Implicaciones prácticas y nuestra recomendación profesional

Contar con una visión externa y especializada aporta los siguientes beneficios clave:

Garantía de mejora continua:	Permite detectar desviaciones y áreas de mejora antes de que se conviertan en incidencias de seguridad o no conformidades en las auditorías de certificación bienales.
Optimización de recursos:	Facilita el mantenimiento proactivo del SGSI sin poner en riesgo la conformidad regulatoria de la organización.
Independencia y rigor:	Un equipo auditor externo aporta una perspectiva objetiva, imparcial y altamente capacitada para evaluar la verdadera eficacia operativa de los controles de seguridad implantados.

Además, se recuerda que el mantenimiento del SGSI según ENS requiere un esfuerzo constante a las organizaciones:

 Presentación del Informe INES de forma anual	 Realización de formaciones de seguridad de la información de forma periódica
 Concienciación de toda la plantilla de forma periódica	 Control continuo sobre proveedores
 Revisión de cambios que puedan afectar al SGSI	 Revisión y actualización del análisis y gestión de riesgos
 Actualización del BIA y planes de continuidad	 Testeo periódico de los planes de continuidad
 Gestión de mantenimientos de infraestructura	 Registro de actas de seguimiento del Comité de Seguridad
 Revisión de las guías CCN y marco legal aplicable	 Actualización de la Declaración de aplicabilidad

Quedamos a su entera disposición para resolver cualquier duda al respecto, así como para asesorarles en el diseño de un plan de revisiones periódicas adaptado a las necesidades de su organización y a las exigencias de su nivel de categoría en el ENS.