REGLAMENTO PARTICULAR DE CERTIFICACIÓN DE SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

RP-CSG-08

Rev. 02

Reglamento aprobado el 2017-09-07

Índice

1. Objeto

El presente Reglamento particulariza el Reglamento General de Certificación de Sistemas de Gestión y sus Marcas de Conformidad para la certificación de los sistemas de gestión de seguridad de la información que son conformes con la Norma UNE-ISO/IEC 27001 *Tecnologías de la Información. Técnicas de seguridad. Sistema de Gestión de Seguridad de la Información (SGSI). Requisitos*, en su edición vigente.

La certificación se llevará a cabo según las condiciones establecidas en el Reglamento General, con las especificidades o salvedades establecidas en el presente, y en conformidad con la Norma ISO/IEC 27006 *Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems*, en su edición vigente.

La certificación da lugar a la emisión del "Certificado de Seguridad de la Información" a la organización certificada, y ésta obtiene el derecho al uso de la marca AENOR de "Seguridad de la Información" que se describe en la Instrucción de Uso de Marca AENOR.

2. Definiciones

Para la interpretación del presente Reglamento serán de aplicación las definiciones referenciadas y las contenidas en el Reglamento General y en las normas UNE-ISO/IEC 27001 *Tecnologías de la Información. Técnicas de seguridad. Sistema de Gestión de Seguridad de la Información (SGSI). Requisitos* e ISO/IEC 27002 *Information technology – Security techniques – Code of practice for information security management* e ISO/IEC 27006 *Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems,* en sus ediciones vigentes.

3. Concesión, mantenimiento y renovación del certificado

Los procesos de concesión, mantenimiento y renovación del certificado se ajustarán a los descritos en el Reglamento General, con las siguientes consideraciones:

3.1. Auditoría inicial

El auditor verificará el cumplimiento del Sistema de Gestión de Seguridad de la Información conforme a la Norma UNE-ISO/IEC 27001, y en relación con su apartado 9.2, "Auditorías Internas del SGSI", el auditor verificará que, al menos, se han llevado a cabo una auditoría interna completa que incluya la evaluación de los apartados del 4 al 10 de la Norma UNE-ISO/IEC 27001 y la revisión de

los objetivos de control y controles que están definidos en el documento de aplicabilidad de la organización.

3.2. Plazo para la presentación del plan de acciones correctivas

Si en la auditoría inicial o en una auditoría de seguimiento, renovación o extraordinaria existen no conformidades, se establece un plazo de 30 días naturales para que la organización presente a AENOR el plan de acciones correctivas necesarias para corregirlas, así como cuantas evidencias sean necesarias para demostrar la eficacia de las mismas.

4. Compromisos

En relación con el apartado f) del Capítulo 9, "Compromisos", del Reglamento General, la organización debe disponer y poner a disposición de AENOR, un procedimiento para el tratamiento, investigación y registro de las reclamaciones y las acciones de remedio y correctivas que contemple, entre otras, las siguientes acciones:

Notificación a las autoridades apropiadas, si la Ley así lo exige.

- Restaurar la conformidad.
- Prevenir la recurrencia.
- Evaluar y mitigar cualquier incidente de seguridad adverso así como sus impactos asociados.
- Asegurar la interacción satisfactoria con otros componentes del SGSI.
- Asegurar la eficacia de las acciones de remedio y correctivas adoptadas.