Nº 88 febrero 2024

AES propone un decálogo de acciones que ayudarán a cumplir con los requisitos que establece el ENS

El Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, establece que el ENS está constituido por los principios básicos y requisitos mínimos necesarios para una protección adecuada de la información tratada y los servicios prestados por las entidades de su ámbito de aplicación, con objeto de asegurar el acceso, la confidencialidad, la integridad, la trazabilidad, la autenticidad, la disponibilidad y la conservación de los datos, la información y los servicios utilizados por medios electrónicos que gestionen en el ejercicio de sus competencias.

El ámbito de aplicación citado real decreto contempla a los sistemas de información de las entidades del sector privado, cuando presten servicios o provean soluciones a entidades del sector público, extendiendo esté ámbito de aplicación a la cadena de suministro de dichas entidades privadas.

La Asociación Española de empresas de Seguridad (AES) en su manifiesto 2020-2022 declaraba su compromiso con la seguridad de la sociedad.

> *"Una de las necesidades más básicas de la sociedad actual es la protección frente a las amenazas, en cualquiera de las formas en las que se produzcan. Sin las medidas de protección adecuadas, los ciudadanos que conforman la sociedad afrontan riesgos."*

AES teniendo en cuenta su compromiso con la seguridad de la sociedad y con el de aportar valor a sus asociados, y teniendo en cuenta que la mayoría de ellos son proveedores de soluciones y servicios a la administración pública o forman parte de la cadena de suministro de dichas soluciones y servicios, y por lo tanto se encuentran dentro del ámbito de aplicación del ENS, continuando con su labor de concienciación en el ámbito de la seguridad de información, propone las siguientes acciones que ayudarán a cumplir con los requisitos que establece el ENS.

1. Disponer de una política de seguridad de la información que defina los objetivos, responsabilidades, roles y funciones relacionados con la seguridad de la información.
2. Identificar y clasificar los activos de información según su nivel de criticidad y sensibilidad, valorando el impacto en cada una de las dimensiones de la seguridad: disponibilidad, autenticidad, integridad, confidencialidad y trazabilidad.
3. Realizar un análisis de riesgos, identificando las amenazas, vulnerabilidades y activos a proteger, y evaluando el impacto potencial de los incidentes de seguridad.
4. Implementar controles de acceso físico y lógico para proteger los activos de información de accesos no autorizados o indebidos.
5. Realizar copias de seguridad periódicas de la información y almacenarlas en lugares seguros y accesibles, para facilitar la restauración de la información en caso de pérdida o daño.
6. Adoptar medidas de prevención, detección, respuesta y recuperación ante los incidentes de seguridad, estableciendo planes de contingencia y continuidad de negocio.
7. Mantener actualizados los sistemas operativos, las aplicaciones y los dispositivos de seguridad, aplicando los parches de seguridad y las actualizaciones necesarias para evitar las vulnerabilidades conocidas.
8. Utilizar mecanismos de cifrado, firma electrónica y certificación digital para garantizar la confidencialidad, integridad y autenticidad de la información, así como el no repudio de las transacciones electrónicas.
9. Sensibilizar y formar al personal sobre la importancia de la seguridad de la información y las buenas prácticas a seguir, fomentando la creación de una cultura de seguridad en toda la organización.
10. Implantar procedimientos de registrar y gestión de los incidentes de seguridad de la información, que permitan resolver e informar de las incidencias de forma rápida y efectiva.

Ricardo Cañizares Sales
Vocal de la Junta Directiva y miembro del área de ciberseguridad de AES