Nº 91 junio 2024

El Cifrado de las Comunicaciones y los Datos en el Esquema Nacional de Seguridad

El Esquema Nacional de Seguridad (ENS) es un conjunto de principios y requisitos diseñado para garantizar la seguridad de la información gestionada por las administraciones públicas españolas y sus entidades colaboradoras. Aunque cada vez más entidades privadas están adoptando el ENS al tener que relacionarse con las administraciones públicas. El ENS fue establecido en el RD 3/2010 con el objetivo de crear confianza en el uso de medios electrónicos. Un componente esencial de este esquema es el cifrado de las comunicaciones y los datos, cuya finalidad es proteger la confidencialidad e integridad de la información.

Cifrado de las Comunicaciones

Para asegurar la confidencialidad de las comunicaciones, el ENS establece el uso de protocolos de cifrado robustos. Entre ellos, destacan HTTPS y SSL/TLS, que garantizan que los datos intercambiados entre los sistemas estén protegidos contra interceptaciones no autorizadas. Estas tecnologías son esenciales para prevenir que la información sensible sea accesible a personas no autorizadas durante su transmisión.

Además, el uso de redes privadas virtuales (VPN) es recomendado para proteger las comunicaciones en redes inseguras. Las VPN cifran y autentifican los datos transmitidos, asegurando así su integridad y confidencialidad. Otra medida importante es el uso de protocolos de cifrado para el correo electrónico, como S/MIME (Secure/Multipurpose Internet Mail Extensions) o PGP (Pretty Good Privacy). Estos protocolos aseguran que los correos electrónicos sean confidenciales y no hayan sido alterados durante su transmisión.

Cifrado de los Datos

El ENS también hace hincapié en el cifrado de los datos en reposo. La información almacenada debe ser cifrada para protegerla contra accesos no autorizados, lo cual incluye bases de datos, sistemas de archivos y copias de seguridad. Es crucial utilizar algoritmos y claves adecuados para garantizar la seguridad a largo plazo. Entre los algoritmos recomendados se encuentra el Advanced Encryption Standard (AES) con longitudes de clave de 128 bits o más, dependiendo del nivel de sensibilidad de los datos.

La gestión de claves criptográficas es otro aspecto fundamental. La seguridad del cifrado depende en gran medida de una gestión adecuada de las claves, que incluye su generación, almacenamiento, distribución y destrucción segura. El uso de módulos de seguridad de hardware (HSM) es recomendado para la protección de las claves criptográficas.

Requisitos del ENS en Relación al Cifrado

El ENS establece distintos niveles de seguridad (básico, medio y alto) y define requisitos específicos para cada uno en relación al cifrado de datos y comunicaciones:

- **Nivel Básico:** Requiere implementar mecanismos de cifrado en comunicaciones sensibles y cifrar la información confidencial almacenada.
- **Nivel Medio:** Obliga al uso de cifrado en todas las comunicaciones de información sensible y en bases de datos y ficheros que contengan datos de carácter personal o información confidencial.
- **Nivel Alto:** Exige cifrado avanzado en todas las comunicaciones y datos críticos, utilizando algoritmos de cifrado robustos y gestionando las claves mediante HSM.

Para ampliar el conocimiento del propio ENS se puede recurrir al propio RD 3/2010, o a las opciones más amigables como el ENS Navegable, así como las numerosas guías CCN-STIC de las series 800 y 400 que el Centro Criptologíco Nacional ha desarrollado para ayudar a cumplir con los requisitos del ENS.

Juanma Herrera.