AES
FUNDACIÓN

Concienciando a la industria en ciberseguridad

Índice

En la Industria de la Seguridad en España y como asociación decana, AES siempre ha desarrollado un papel vital. Representamos a nuestro país tanto en los Comités Nacionales y Europeos donde se crean las normas como en las dos principales asociaciones europeas como son Eurosafe y Euralarm. Todo ello es posible gracias a la dedicación y conocimiento de nuestros expertos pertenecientes a las diferentes Áreas de Trabajo que disponemos. La información es poder y por supuesto vital para la competitividad de nuestras empresas asociadas. El compromiso social es parte de nuestro ADN y para ello creamos continuamente guías, recomendaciones y publicaciones desde donde transmitimos nuestro conocimiento. En nombre de toda la Junta Directiva de AES esperamos que disfrutes de este trabajo que con tanto cariño hemos realizado.

Iñigo Ugalde Blanco –Presidente de AES.

Después de muchos meses de trabajo y dedicación, el pasado 27 de junio quedo registrada AES FUNDACIÓN en el Registro Nacional de Fundaciones. Uno de los objetivos establecidos para la Fundación es la difusión de los documentos elaborados por las áreas de trabajo de AES.

Es por ello que todas las publicaciones de nuestras áreas de trabajo (ya tenemos incorporadas la guía de seguridad en el turismo y alojamiento turístico y tres guías de PCI), así como la Newsletter y el Boletín, han empezado a aparecer con el color naranja distintivo de la Fundación, y en el caso de Newsletter y Boletín, con una nueva numeración de segunda época.

Todo ello forma parte del desarrollo #UniversoAES y #HaciendoIndustria. Espero que esta nueva publicación que os traemos hoy sirva de ayuda y siga contribuyendo con nuestra propuesta de valor **“dinamizando la seguridad ciudadana”**

Antonio Escamilla Recio –Presidente de AES FUNDACIÓN.

El *área de trabajo de ciberseguridad* de la Asociación Española de empresas de Seguridad (AES) lleva años trabajando para concienciar a sus asociados sobre la necesidad de mejorar la ciberseguridad tanto de sus sistemas de información y comunicaciones (utilizados en su propia gestión empresarial o para la prestación de servicios a clientes), , así como de los sistemas que diseñan, fabrican, implantan y mantienen.

Este compromiso con la ciberseguridad forma parte de la responsabilidad de AES para con la seguridad de la sociedad, como declara la asociación en su manifiesto 2020-2022.

> *"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."*

El fruto del trabajo del área de ciberseguridad de AES se ha plasmado en varios documentos que pueden descargarse desde la página web de la asociación, https://www.aesseguridad.es/, el último de ellos publicado a finales del 2023 y titulado "Guía de adecuación al Esquema Nacional de Seguridad". Este documento puso de manifiesto la necesidad de ampliar la difusión de los trabajos del área de ciberseguridad con el objeto de divulgar y concienciar, no solo a los asociados de AES, sino también a nuestros clientes y proveedores sobre la importancia y la necesidad de contemplar la ciberseguridad en cualquier actividad, tanto empresarial como personal.

Por ello, para ampliar la difusión de las actividades de divulgación y concienciación, durante este año 2024, hemos realizado cuatro Webinar y publicado en los boletines y en las newsletter de la asociación una serie de artículos con foco en el cumplimiento del Esquema Nacional de Seguridad (ENS). Todos estos contenidos se han recopilado en la presente publicación.

Además, el área de trabajo de ciberseguridad no solo ha estado trabajando en la divulgación y concienciación del ENS, también ha creado, dentro del propio área de trabajo, un *grupo de trabajo de Inteligencia Artificial y Protección de Datos*, que se ha centrado en el análisis y la respuesta a los retos que supone para la industria de la seguridad la publicación, por parte de la Agencia Española de Protección de Datos, de la "Guía sobre tratamientos de control de presencia mediante sistemas biométricos"

Durante el próximo año seguiremos ampliando las actividades de divulgación y concienciación en ciberseguridad, aumentando su difusión utilizando todos los canales y formatos que puedan estar a nuestro alcance. Además, trabajaremos en el desarrollo de guías sectoriales especificas que complementen las guías que han elaborado otras áreas de trabajo de AES, y que ayuden al cumplimiento de la regulación actual y a la adecuación a lo establecido por las directivas NIS2 y CER.

Decálogo de medidas de seguridad contempladas por 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.

Decálogo de medidas de seguridad contempladas por 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

¿Qué es PILAR?

La aplicación CHINCHÓN para análisis de riesgos podría considerarse como la precursora de PILAR.

PILAR es un conjunto de herramientas EAR (Entorno de Análisis de Riesgos) cuya función es el análisis y la gestión de riesgos de un sistema de información siguiendo la metodología Magerit (Metodología de Análisis y Gestión de Riesgos de los sistemas de información) y está desarrollada y financiada principalmente por el CCN. Sufre actualizaciones periódicas y existen diversas variantes (Versión Íntegra, Pilar Basic, µPilar –Versión Reducida, RMat –Personalizada). Permite la gestión de riesgos en cinco dimensiones: confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad (accountability).

PILAR está dirigía a todas aquellas organizaciones/organismos que cuentan con infraestructuras de TIC y que tienen la necesidad de gestionar de forma eficiente sus activos, realizando Análisis de Impacto y Continuidad de las Operaciones, tanto de manera cuantitativa como cualitativa.

Es de uso libre para todas las AAPP y de pago para la empresa privada, aunque su coste es bastante reducido para las capacidades que tiene y en comparación con otras herramientas similares del mercado. A partir de 1.500 euros licencia/año. Es autoinstalable, traducida a 8 idiomas, dispone de un módulo específico para el **cumplimiento del ENS**, verificación del RGPD y se integra con otras herramientas del CCN –CERT como INÉS –AR.

Los requisitos son contar con un ordenador personal cuyo SO sea MAC, Linux o Windows y máquina virtual java 2 (lenguaje de programación java), opcionalmente se puede usar un repositorio de tipo base de datos con acceso a SQL.

Los objetivos perseguidos por la herramienta Pilar son realizar el análisis de riesgos según la metodología Magerit e ISO/IEC 27005 para el diseño del plan de mejora de la seguridad. Una vez conocidos los riesgos, se pueden determinar una serie de salvaguardas y estimar el riesgo residual. El tratamiento del riesgo es un proceso continuo y recurrente en el que el sistema de protección se va mejorando regularmente para afrontar nuevos riesgos y aumentar la confianza que el sistema merece para los responsables y los usuarios.

Los resultados que se obtienen con el uso de la herramienta son:

- Impacto potencial y residual.
- Riesgo potencial y residual.
- Mapa de riesgos.
- Plan de mejora de la seguridad.
- Monitorización continua del Estado de Riesgo.

Sus ventajas principales se centran en conocer los Riesgos a fin de poder tratarlos, conocer el grado de cumplimiento de diferentes perfiles de seguridad: ISO 27002, protección de datos de carácter personal (RGPD), ENS, etc., e implementar la metodología Magerit e ISO/IEC 27005.

En definitiva, PILAR interesa a todos aquellos que trabajan con información mecanizada y los sistemas informáticos que la tratan. Si dicha información o los servicios que se prestan gracias a ella son valiosos, PILAR les permitirá saber cuanto de este valor está en juego y les ayudará a protegerla.

Jorge Noguerales Bautista

El ENS: un marco de referencia para la seguridad de la información

El ENS (Esquema Nacional de Seguridad) actualmente en vigor fue aprobado por el Real Decreto 311/2022 y es una evolución del anterior Esquema Nacional de Seguridad que fue promulgado en su día por el Real Decreto 3/2010, durante los 12 años que transcurrieron desde la aprobación del primer ENS hasta la promulgación del actual, se han producido grandes cambios en el entorno, tanto en el externo como en el interno, en el que desarrollan sus actividades las Administraciones Públicas y las empresas que les prestan servicios de muy diferente índole. Entre esos cambios en el entorno podemos citar la nueva legislación nacional y europea que ha entrado en vigor durante estos y años, la transformación digital de la sociedad y en un número mayor de las ciberamenazas a las que están expuestos nuestros sistemas de información y comunicaciones, que se ha puesto de manifiesto con un notable incremento de los ciberataques, tanto en volumen y frecuencia como en sofisticación.

¿Qué es el ENS?

El ENS es un marco común para la seguridad de la información, un conjunto de normas y principios que establecen los requisitos mínimos de seguridad que deben cumplir los sistemas de información y comunicaciones de las Administraciones Públicas y de las entidades privadas que les prestan servicios.

El ENS tiene como objetivo final garantizar el acceso, la conservación, la confidencialidad, la integridad, la trazabilidad, la autenticidad y la disponibilidad de la información, de las entidades bajo su ámbito de aplicación, así como el adecuado funcionamiento de los servicios prestados por dichas entidades.

Para ello el ENS establece unos principios básicos y unos requisitos mínimos, que son imprescindibles para alcanzar su objetivo final. Los principios básicos son:

- ☑ Seguridad como proceso integral.
- ☑ Gestión de la seguridad basada en los riesgos.
- ☑ Prevención, detección, respuesta y conservación.
- ☑ Existencia de líneas de defensa.
- ☑ Vigilancia continua.
- ☑ Reevaluación periódica.
- ☑ Diferenciación de responsabilidades.

¿Por qué es importante el ENS para las empresas?

El ENS además de ser una obligación legal para las empresas que prestan servicios a las Administraciones Públicas, tal como establece el artículo 3 del Real Decreto 311/2022 supone además una oportunidad de crecimiento y de diferenciación en el mercado, ya que es una herramienta que les ayuda a mejorar su seguridad de la información y a adaptarse a las exigencias de la transformación digital del mercado.

Hay que recordar, la obligación que tienen las Administraciones Públicas de incluir en los pliegos de prescripciones administrativas o técnicas de las licitaciones que publiquen y en sus correspondientes contratos, todos aquellos requisitos necesarios para asegurar la conformidad con el ENS de los sistemas de información en los que se sustenten los servicios objeto de la licitación.

La mejor forma que tienen de cumplir los requisitos establecidos al respecto, las empresas privadas que quieran acudir a las licitaciones públicas es contar con las correspondientes Declaraciones o Certificaciones de Conformidad con el ENS, que garanticen la conformidad con el ENS de los sistemas de información y comunicaciones que van a utilizar para la prestación de los servicios incluidos en la licitación, teniendo en cuenta que está obligación también se extiende a su cadena en la medida que sea necesario y de acuerdo con los resultados del correspondiente análisis de riesgos. Todo ello sin olvidar que cada vez más en muchas licitaciones públicas es un requisito excluyente contar con una Declaración o una Certificación de Conformidad con el ENS de acorde con la categoría de seguridad de los sistemas que se establece en el pliego de condiciones.

¿Qué ventajas aporta el ENS a las empresas?

Disponer de una Certificación de Conformidad con el ENS aporta a las empresas una serie de ventajas competitivas y beneficios, la primera es que le permite acceder a licitaciones del sector público a las que no podría acceder si no dispone de ella. Ya solo con está ventaja competitiva, poder acceder a licitaciones del sector público, se justifica el esfuerzo de obtener un Certificación de Conformidad, pero es que además se consigue:

- ☑ Una mejora de la competitividad: no solo permite a la empresa a acceder a más oportunidades de negocio en el sector público, sino también en el sector privado, tanto como un elemento de la cadena de suministro de la administración pública, como al demostrar su compromiso con la seguridad de la información.
- ☑ Una mejora de la reputación: disponer de un Certificación de Conformidad con el ENS, muestra al mercado y a todas las partes interesadas el compromiso de la empresa con la seguridad de la Información.
- ☑ Una mejora de la cultura de seguridad: al implantar el ENS en una empresa se consigue una mayor concienciación y sensibilización sobre la importancia de la seguridad de la información entre sus trabajadores, creando un entorno de trabajo más seguro y protegido.
- ☑ Una mejora de la seguridad de los sistemas de información y comunicaciones de la empresa: al implantar el ENS en una empresa se establecen un conjunto de medidas de seguridad técnicas y organizativas que cubren todos los aspectos clave de la seguridad, logrando una mejor protección de los sistemas, de la información y de los datos de la empresa, reduciendo el riesgo de sufrir ciberataques y fraudes.

En resumen, disponer de un Certificado de Conformidad con el ENS permite a una empresa ser mucho más competitiva y prestar servicios mucho más resistentes y resilientes a los ciberataques.

Ricardo Cañizares Sales

Jorge Noguerales Bautista

Configuraciones seguras

Regulaciones como la CRA, la nueva NIS2 o el hecho de prestar servicios a las administraciones públicas están promoviendo la cultura de la ciberseguridad dentro de las organizaciones. La adopción de estándares como ISO27001, ISA/IEC62443 o el ENS están obligando a las organizaciones a desarrollar y adoptar una política de seguridad dentro de la organización.

Las políticas proporcionan el marco general de seguridad, establecen las directrices y responsabilidades, mientras que los procedimientos operativos se encargan de la ejecución práctica de esas políticas. Uno de los procedimientos básicos que hay que desarrollar es el de securización de los sistemas dentro de la organización.

Definimos la securización como la implementación de medidas de seguridad que protejan al sistema de potenciales ataques y vulnerabilidades. Al securizar los sistemas las organizaciones están reduciendo el riesgo de accesos no autorizados, filtraciones de datos u otros incidentes de seguridad.

Existen una serie de estrategias generales para la securización de los sistemas entre las que se pueden citar: gestión de parches, configuración segura, control de accesos, supervisión y registro, encriptación y repuesta a los incidentes. Nos centraremos en este artículo en la configuración segura de los dispositivos.

Existen diferentes componentes que tenemos que tener en cuenta para configurar de manera segura un dispositivo.

Inventario de activos

Lo que no se conoce no se puede proteger. Mantener actualizado el inventario de los dispositivos que están en el sistema y disponer no solo del número de los dispositivos sino también su configuración, versiones de hardware, firmware o software, posición física y conexiones lógicas con otros dispositivos. El inventario es un elemento vivo que hay que ir actualizando de manera periódica con nuevos dispositivos o con los cambios que se hayan producido en los elementos ya existentes.

Gestión de los servicios y los puertos

Deshabilitar los servicios y los puertos que no sean necesarios. Habilitar únicamente los servicios que se vayan a usar y utilizar siempre las versiones seguras de los servicios. La idea es reducir la superficie de ataque y limitar potenciales puntos de entrada de los atacantes. Se reduce el riesgo de accesos no autorizados.

Contraseñas

Cambiar las contraseñas por defecto y requerir el uso de contraseñas fuertes con un número suficiente y variado de caracteres o, dependiendo del dispositivo, requerir el cambio regular de las contraseñas o mejor aún el uso de autenticación multifactor. Se reduce el riesgo de accesos no autorizados.

Gestión de las cuentas de usuario

Crear varias cuentas en función de los requisitos de cada rol y asegurarse de implementar contraseñas distintas. Seguir siempre el principio de mínimo privilegio y permitir a los usuarios solo los permisos necesarios para realizar su función y ninguno más. De esta manera reducimos el riesgo de accesos no autorizados, limitamos el impacto de las amenazas internas y mantenemos la confidencialidad.

Gestión de firmware/software

Mantenerse informado de los últimos parches de seguridad de los fabricantes disponibles para los dispositivos y mantener todos los dispositivos actualizados a la última versión disponible. Aunque no todas las organizaciones son iguales y debe existir un procedimiento de parcheo donde se recojan cuáles son los pasos para aplicar el parcheo en los diferentes dispositivos, los riesgos del parcheo, necesidad de un banco de pruebas, responsables, ...

Como hemos visto la configuración segura juega un papel importante en fortalecer la postura de seguridad de los sistemas, mitigando riesgos y mejorando la resiliencia frente a las ciber amenazas. Al implementar de manera eficiente las prácticas de configuración segura las organizaciones pueden crear entornos seguros que protegen datos sensibles, mantienen la continuidad de la operación y cumplen con los requerimientos regulatorios.

Juan Manuel Herrera

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 electronicos. 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.

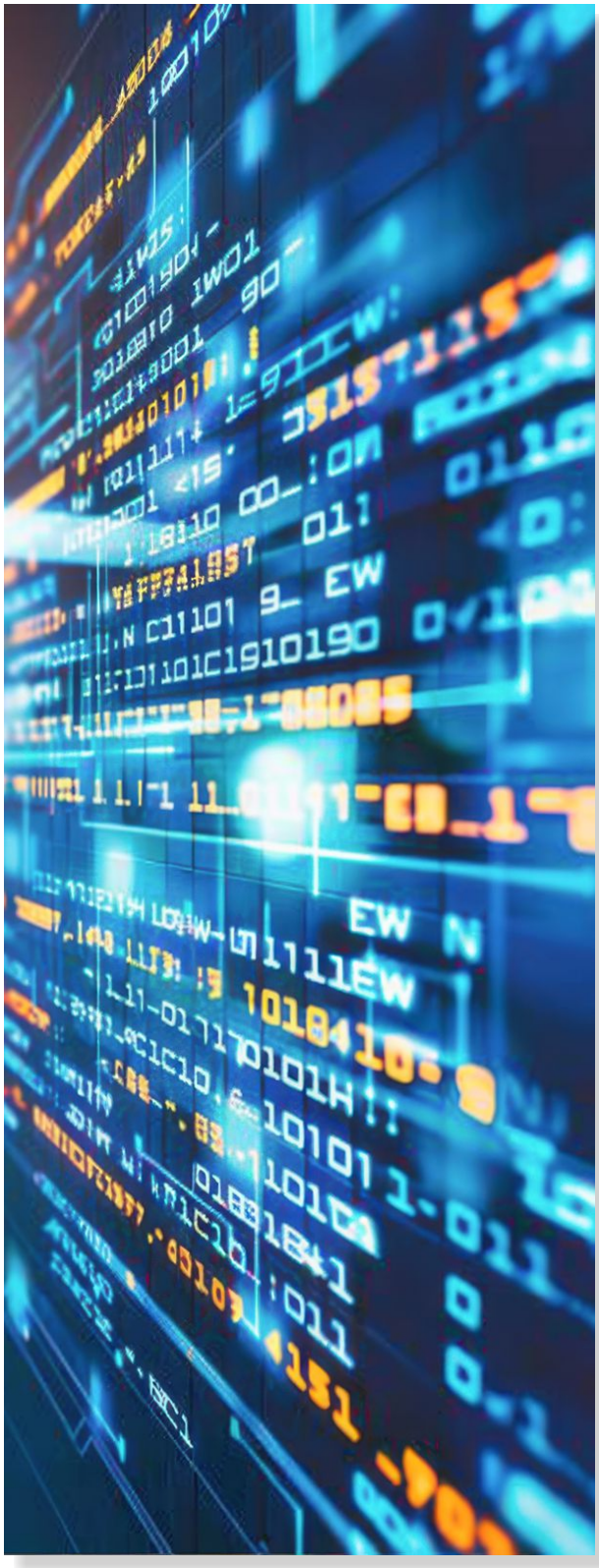
Requisitos del ENS en Relación al Cifrado

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 guias CCN-STIC de las series 800 y 400 que el Centro Criptologíco Nacional ha desarrollado para ayudar a cumplir con los requisitos del ENS.

Juan Manuel Herrera



IA: videovigilancia y normativa

La IA ha venido para revolucionar el campo de la seguridad, y muy especialmente la videovigilancia. Ofrece mejoras significativas en la capacidad de detectar y predecir situaciones y comportamientos. Pero entraña otros retos y peligros, como el uso indebido y el riesgo en ciberseguridad.

¿Qué es la IA?

La inteligencia artificial (IA) es una tecnología que permite a las máquinas simular la inteligencia humana y resolver problemas. Puede realizar tareas que normalmente requerirían intervención humana.

La IA se basa en algoritmos, reglas matemáticas que guían el proceso de aprendizaje de la máquina, y en datos, la información que la máquina utiliza para entrenar y mejorar sus algoritmos.

En el campo de la informática, la IA abarca el aprendizaje automático y el aprendizaje profundo, que desarrollan algoritmos basados en procesos de toma de decisiones similares al cerebro humano, con aplicaciones en todos los campos tecnológicos, siendo uno de ellos la videovigilancia.

¿Cómo puede ayudar la IA a gestionar la videovigilancia en las empresas?

La inteligencia artificial está revolucionando el campo de la seguridad, ya que brinda nuevas herramientas y capacidades para la protección, vigilancia y prevención. Esta tecnología está siendo aplicada en diversas áreas, como la predicción de amenazas, el reconocimiento facial o la monitorización en tiempo real, para mejorar la seguridad de manera exponencial en diferentes entornos.

Especialmente la IA se utiliza en la vigilancia y prevención de delitos. Por ejemplo, en sistemas de videovigilancia, los algoritmos de aprendizaje automático pueden identificar comportamientos sospechosos, como personas merodeando en áreas restringidas o acciones violentas, o también situaciones anómalas en gestión del tráfico o en un proceso fabril automatizado. Esto permite autoridades y usuarios tomar medidas rápidas y prevenir posibles consecuencias.

A nivel tecnológico, los sensores de vídeo más avanzados incorporan IA para permitir a los usuarios comprender mejor su entorno, analizar lo que está ocurriendo en cada momento y responder de manera proactiva. Y, en última instancia, asistir para predecir situaciones imprevistas o futuras.

Las compañías que utilizan el poder de la IA en sus procesos dan un salto cualitativo enorme en el conocimiento, la prevención de delitos y riesgos, y en general en la efectividad de su negocio.

¿Qué implicaciones tiene la IA aplicada a la videovigilancia?

La IA presenta uno de los mayores retos para la seguridad de los sistemas, dada la velocidad con la que evoluciona esta tecnología y los múltiples usos que surgen cada día, que no siempre son debidamente supervisados y autorizados por los agentes reguladores.

El mayor beneficio de la IA en la videovigilancia es la detección rápida y precisa y la reducción de falsos positivos

De manera simplificada, el reto de la IA en videovigilancia es doble: el que se deriva de sus usos o aplicaciones, como la gestión de masas o el reconocimiento facial, que tienen enormes ventajas, pero deben ser ratificados a nivel normativo en cuanto a límites para los derechos de los usuarios y la ciudadanía en general, y las brechas de seguridad que continuamente se generan en los sistemas donde se aplica la IA.

¿Cuál es el marco normativo regulador?

Aunque existen distintas normativas aplicables, nos centraremos en la más novedosa y de inminente aplicación, el Reglamento de Inteligencia Artificial (RIA) de la Unión Europea que se acaba de publicar en el Diario Oficial de la Unión Europea el 12 de julio y entrará en vigor el 1 de agosto de 2024, y que es la primera ley integral sobre IA del mundo.

Este marco regulador propone que los sistemas de IA que puedan utilizarse en distintas aplicaciones se analicen y clasifiquen según el riesgo que supongan para los usuarios. Los distintos niveles de peligro implicarán una mayor o menor regulación. Se establecen cuatro niveles: riesgo inaceptable, riesgo alto, riesgo limitado y riesgo mínimo.

La prioridad del Parlamento es garantizar que los sistemas de IA utilizados en la UE sean seguros, transparentes, trazables, no discriminatorios y respetuosos con el medio ambiente. Los sistemas de IA deben ser supervisados por personas, en lugar de por la automatización, para evitar resultados perjudiciales.

El Parlamento también quiere establecer una definición uniforme y tecnológicamente neutra de la IA que pueda aplicarse a futuros sistemas de IA.

¿Qué deben tener en cuenta las empresas en cuanto a la utilización de tecnología con IA?

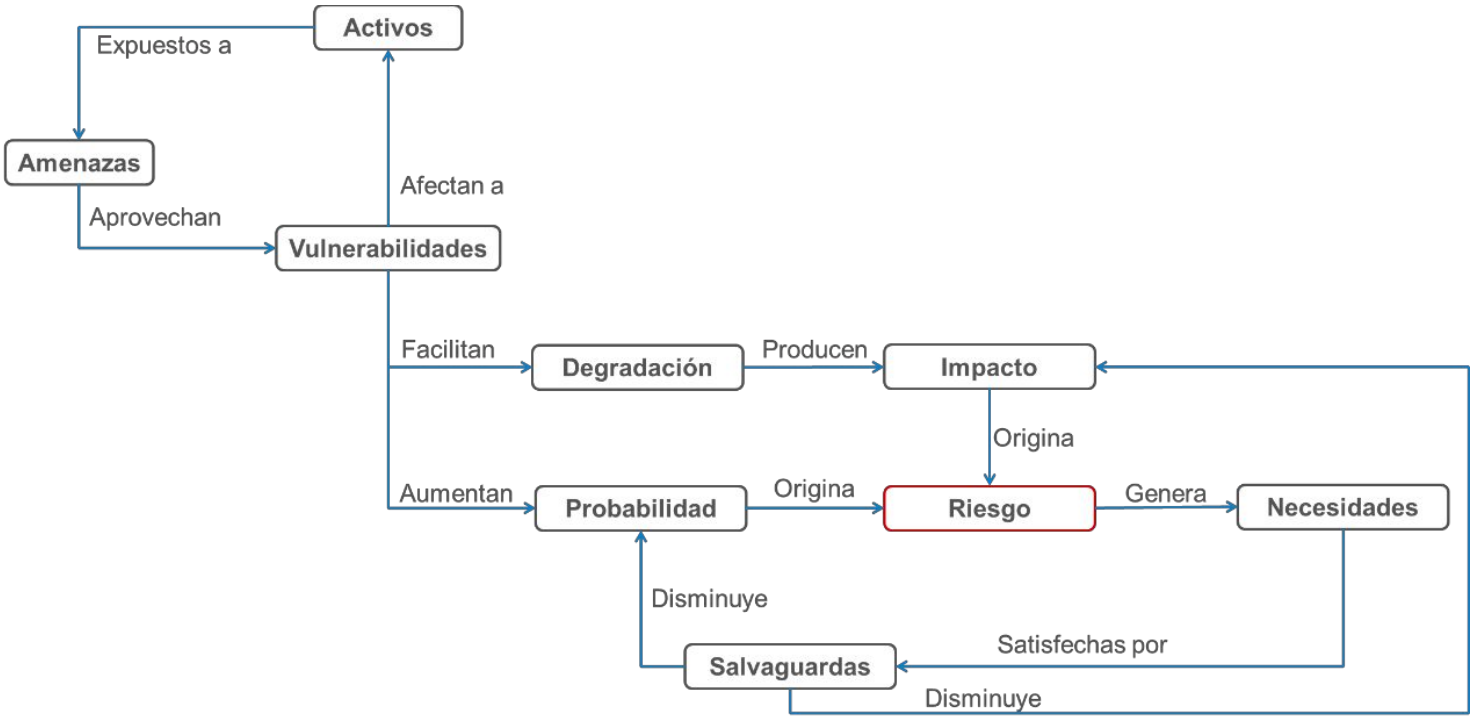
Las compañías instaladoras de soluciones de videovigilancia asistidas por IA tendrán una ventaja competitiva al ofrecer a sus clientes la detección más rápida y precisa y la capacidad predictiva en sus procesos de protección y seguridad, si bien deberán observar la nueva regulación europea implementada en los países, según el nivel de riesgo que la IA suponga para la actividad concreta.

Laura Alcázar Moratilla

Realizar un análisis de riesgos es algo imprescindible a la hora de diseñar un Plan de Seguridad. Conocer los riesgos y sus consecuencias permite a las organizaciones optimizar las inversiones en Seguridad e implantar un conjunto de medidas de seguridad que les ayuden a alcanzar sus objetivos de negocio, para lo que es necesario garantizar la continuidad de sus operaciones y proteger sus procesos y sus activos, tanto tangibles como intangibles, lo que es imprescindible para la generación de valor por parte de cualquier organización.

Los activos y procesos de cualquier organización están expuestos a amenazas, además de tener vulnerabilidades que influyen tanto en la probabilidad de la materialización de la amenaza, como en la degradación del activo y por lo tanto en la magnitud del impacto. El valor del riesgo al que está expuesto un activo o proceso productivo es función de la probabilidad de materialización de la amenaza y del impacto de esta.

Cuando implantamos una medida de seguridad, una salvaguarda, esta actúa reduciendo la probabilidad de materialización de la amenaza y/o minimizando la magnitud el impacto.



Este marco conceptual se aplica a la mayoría de las metodologías de análisis de riesgos habitualmente utilizadas, como pueden ser Mosler, Cuantitativo Mixto y Magerit.

Al realizar el análisis de riesgos, y elaborar un Plan de Seguridad habremos dado respuesta a las cuatro preguntas clave:

- **¿Qué debemos proteger?**
- **¿Dónde lo debemos proteger?**
- **¿Cómo lo debemos proteger?**
- **¿Cuándo lo debemos proteger?**

De estas cuatro respuestas, con total seguridad, va a surgir la necesidad de instalar Sistemas Electrónicos de Seguridad. Estamos hablando de sistemas de detección de intrusión, de sistemas de control de acceso, de sistemas de video vigilancia, etc.

Implantar un Sistema Electrónico de Seguridad en una instalación implica que estamos incorporando elementos y activos que no se encontraban en la instalación en el momento de realizar el AA.RR. en el que se basa el Plan de Seguridad, por lo tanto, se requiere volver a analizar los riesgos teniendo en cuenta estos nuevos activos.

Estos nuevos activos que hemos incorporado a la instalación hoy día no son dispositivos aislados, son equipos que están conectados, que utilizan redes de comunicaciones, tanto de la propia instalación, como de los proveedores de comunicaciones, como de los fabricantes y proveedores de servicios de seguridad.

La casuística y tipología de la conectividad de los dispositivos de Seguridad Electrónica puede ser muy variada, y debe analizarse de forma individualizada para cada instalación. Nos podemos encontrar con redes internas específicas para seguridad, redes internas compartidas por otros servicios, o redes mixtas. También se encuentran implantaciones de sistemas en la nube, implantaciones completas en local, implantaciones individuales por instalación, implantaciones que controlan múltiples instalaciones, modelos mixtos, etc.

Estamos hablando de que cuando implantamos Sistemas Electrónicos de Seguridad instalando elementos que necesitan que analicemos su nivel de ciberseguridad, estos componentes están sujetos a ciberamenazas, pueden ser objeto de un ataque, o si son comprometidos pueden utilizarse como un medio para para realizar un ciberataque a otros sistemas u otras organizaciones.

Para conocer el riesgo derivado de la materialización de una ciberamenaza sobre un Sistema Electrónico de Seguridad concreto es necesario analizar en profundidad su diseño e implementación, y conocer las características de todos los elementos implicados.

El objeto de este artículo no es analizar un caso concreto de forma detallada, sino poner de manifiesto la necesidad de realizar un análisis de riesgos que contemple la exposición a las ciberamenazas que supone la instalación de Sistemas Electrónicos de Seguridad. Los escenarios de riesgos a los que tenemos que hacer frente son múltiples. A continuación, se exponen algunos de estos que hay que tener en cuenta.

Sistema de Control de Acceso

Sistema de Control de Acceso, tanto para personal propio como para visitantes, que utiliza tarjetas identificativas, que utiliza la red interna corporativa y los datos del personal propio están sincronizados con la base de datos corporativa de RRHH.

En este caso hay que aplicar los mismos criterios de ciberseguridad que se apliquen en la organización al resto de sistemas de gestión de esta, si se compromete el Sistema de Control de Accesos, el atacante podría llegar a tener acceso a la base de datos corporativa de RRHH y a otros sistemas de la organización, sin olvidar la posible fuga de datos de carácter personal.

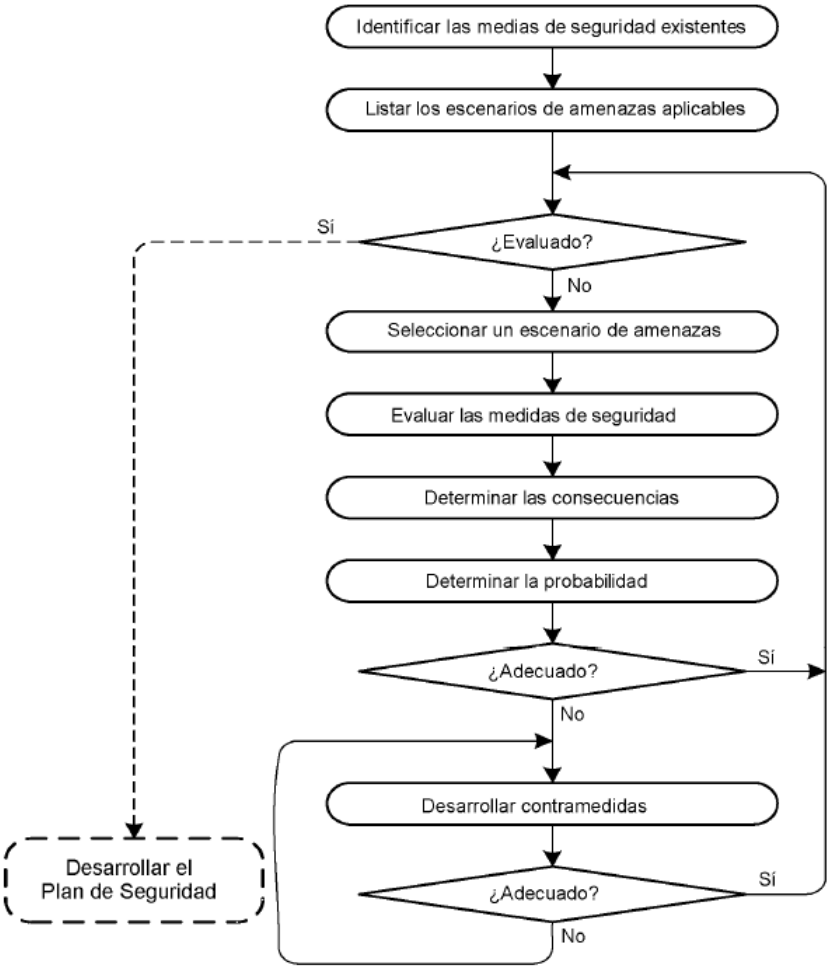
Sistema de videovigilancia

Sistema de videovigilancia, instalado sobre una red interna específica para seguridad, sin conexión a la red de gestión de la instalación, con las cámaras conectadas a una nube publica, la gestión de la videovigilancia se realiza sobre la nube publica y las cámaras incorporan capacidad de análisis.

En este caso, el riesgo para los restantes sistemas informáticos de la instalación no es relevante. Nos encontramos ante dos posibles escenarios de riesgos, el primero con un impacto interno sobre la seguridad de la propia instalación, que un atacante comprometa el sistema de videovigilancia y lo deje inoperativo con un ataque de denegación de servicios o tome el control del sistema y manipule la información que nos está proporcionando.

El segundo escenario es que el atacante tome el control de sistema de videovigilancia y utilice las capacidades de proceso de las cámaras para realizar un ataque a un tercero, ya que estas cámaras cuentan con capacidad de análisis y por lo tanto de proceso.

A la hora de analizar los riesgos derivados de las ciberamenazas a las que están expuestos los Sistemas Electrónicos de Seguridad, es fundamental analizar el mayor número de escenarios posibles, para ello debemos ser sistemáticos y utilizar una metodología de análisis de escenarios.



Como estamos viendo la ciberseguridad de los Sistemas Electrónicos de Seguridad no es algo trivial, es necesario prestarle la atención adecuada y realizar un análisis de los riesgos derivados de las ciberamenazas a los que están expuestos y adoptar las medidas de seguridad necesarias. Sin olvidar los requisitos de la regulación presente y futura, no podemos dejar de tener en cuenta lo que supone el Esquema Nacional de Seguridad y las Directivas NIS2 y CER a la hora de diseñar, implantar y operar los Sistemas Electrónicos de Seguridad.

Como resumen, tenemos que hacer foco en la seguridad por diseño y en la formación y concienciación del personal.

Ricardo Cañizares Sales

NIS 2 y CER, esas grandes desconocidas

No cabe ninguna duda de que el ciber crimen es actualmente una de las mayores amenazas para nuestra sociedad. Se considera ya a la altura del tráfico de armas y del narcotráfico, pero quizás, por su enorme difusión es la amenaza que sentimos más próxima como personas y en cada organización.

Seguramente por ello, las autoridades no descansan promulgando leyes y regulaciones para elevar el nivel de protección de los ciudadanos y de las empresas y entidades que prestan servicios en nuestra sociedad. Eso ha generado una cascada de nuevas normas, actualización de las ya existentes y nuevos marcos regulatorios que pretenden implantar requisitos de diverso nivel de exigencia para que la protección contra la amenaza cibernética no sea de carácter opcional sino de obligado cumplimiento.

En esa línea de actuación la Unión Europea, a través de su Parlamento y Comisión Europea, está desplegando toda una estrategia de Ciber Resiliencia que se va concretando en diferentes directivas y reglamentos. Dos de esas directivas son la directiva NIS 2 y la directiva CER. Se trata de directivas enfocadas en aumentar el nivel de protección de las entidades críticas y otras entidades de importancia en nuestra sociedad. Ciertamente el marco regulatorio europeo disponía ya de elementos aplicables en estos ámbitos, la primera versión de NIS de 2016, y la directiva de protección de entidades críticas de 2008. No obstante, a la vista del escaso y desigual cumplimiento en los estados de la Unión, la Comisión Europea ha decidido avanzar con nuevos elementos regulatorios de obligado cumplimiento, más exigentes, incorporando sanciones, y que afectan a una mayor parte de los operadores económicos de nuestra sociedad.

NIS 2 y CER fueron aprobadas entre finales de 2022 e inicios de 2023. Así pues, el plazo para su trasposición a los diferentes marcos legales de cada estado miembro está prácticamente cumplido. No obstante, en España aún no se ha producido la pertinente trasposición, que tendrá por fuerza que producirse sin mayor dilación. La ausencia de trasposición o una aprobación urgente que trasponga la directiva tal cual se encuentra redactada traería como resultado una norma incompleta, sin establecer un órgano de gobernanza con capacidad de control y sin determinar un régimen sancionador, no respetando así el contenido de la directiva aprobada por el órgano legislativo europeo.

Esta demora en la trasposición de las normas es quizás la responsable de cierta inconsciencia y confusión entre los responsables de las empresas y profesionales en cuanto a los requisitos y obligaciones que estas nuevas normas introducen.

Cabría empezar por enfatizar que el cumplimiento de los requisitos que establecen estas directivas es, además de conveniente en lo que concierne a la conformidad con las leyes una vez transpuestas las directivas al marco jurídico español, una muy buena práctica para elevar las medidas de protección de las entidades afectadas y mantenerse alerta frente a esa amenaza creciente de ciber ataques.

La directiva NIS 2 se ocupa de las medidas de protección frente a las amenazas cibernéticas y la directiva CER se centra en un amplio concepto de protección integral que, complementado con la directiva NIS 2 conduce a garantizar la continuidad de las operaciones de las entidades denominadas críticas. Conviene observar que mientras la directiva CER continúa dirigida hacia esas entidades críticas, la directiva NIS 2 es más ambiciosa y amplia su ámbito de aplicación más allá de esas entidades (ahora definidas como esenciales) incidiendo en esta nueva versión en un mayor número de empresas y organismos denominados "importantes" Eso, para hacernos una idea, extiende el ámbito de impacto de esta directiva respecto a la anterior situación, donde contábamos con unos pocos cientos de operadores críticos, hasta un escenario de varias decenas de miles de empresas y entidades que se verán afectadas por la nueva regulación. Y lo relevante es que serán esas mismas entidades quienes tendrán que auto evaluarse para determinar si el cumplimiento de la norma es aplicable a su caso en particular.

Por lo tanto, convendría, aun cuando la trasposición no está efectuada, que todas las entidades comenzasen a conocer los criterios de calificación que establece la directiva para saber si finalmente se verán afectadas de forma directa.

En el caso de los sistemas de seguridad física, existe cierta tendencia a pensar que se sitúan fuera de la aplicación de los requisitos y obligaciones que aplican a los sistemas informáticos. A ello contribuye que la norma se refiere siempre a sistemas de información y datos sensibles o críticos, pero no hace mención expresa a los sistemas de seguridad física. Se trata de una ilusión que hay que evitar. No hay duda de que los actuales sistemas de seguridad física, toda vez que se trata de sistemas basados en redes de información que gestionan imágenes personales, datos personales, credenciales, etc., forman parte de las infraestructuras de tecnologías de la información (TI) y por lo tanto se ven igualmente afectados por las mismas regulaciones de aplicación que esos sistemas de información.

Si observamos a las entidades financieras, se encuentran actualmente en un proceso de adecuación a su propia directiva, Digital Operational Resilience Act (DORA), en este caso de carácter reglamentario, esto es, de aplicación directa, sin necesidad de trasposición, en definitiva, una ley europea. Esta ley, que busca igualmente elevar la protección frente a las ciber amenazas en el ámbito financiero sería el equivalente NIS 2 para ese tipo de entidades. De manera análoga, y a la espera de la trasposición al Ordenamiento Jurídico español, las principales entidades críticas (en esta NIS 2 esenciales) que son ya conscientes de su afectación directa, han efectuado o están efectuando auditorias para analizar el estado de sus sistemas y las medidas necesarias para el cumplimiento de la norma. Para ayudar en esta labor, el Centro Criptológico Nacional (CCN) ha elaborado diferentes perfiles de cumplimiento específico para las categorías establecidas en NIS 2. Estos perfiles, se apoyan en perfiles ya establecidos por el CCN para el Esquema Nacional de Seguridad (ENS).

En el cumplimiento de estas obligaciones, estas entidades deberán poner el máximo celo en la protección de la cadena de suministro, como exige la propia norma. Eso significa que muy pronto la exigencia de cumplimiento y de medidas específicas de protección se extenderá hacia sus proveedores, en un efecto dominó que ya hemos visto en acción en relación con los requerimientos del ENS y que claramente es un objetivo de los legisladores para provocar la difusión de la conciencia de protección y contar con la colaboración de cada una de las entidades en la supervisión del cumplimiento de los requisitos.

Así pues, si alguien podía pensar que mientras que no exista un regulador establecido por la trasposición de la directiva y consecuentemente un organismo que arbitre el régimen sancionador, el cumplimiento no será necesario, puede encontrarse en un error puesto que es muy posible que sus clientes le reclamen la documentación que acredite sus medidas de protección en base a su propia evaluación de la cadena de suministro.

En definitiva, las directivas NIS 2 y CER, junto con otras ya en vigor y algunas más que se incorporarán, constituirán nuestra realidad en materia de ciberseguridad y protección de entidades críticas. Puede que en este momento no estemos muy familiarizados con ellas, pero es seguro que en el ámbito de los sistemas y servicios de seguridad física formarán una parte sustancial de las normativas aplicables. Cuanto antes nos adentremos en los detalles de estas normas antes estaremos en situación de cumplir con ellas, y lo más importante, estaremos en el camino de garantizar la explotación de los sistemas y servicios de seguridad con la debida protección frente a las grandes amenazas cibernéticas.

Alberto Alonso

Alberto Trigo

Control de acceso basado en el mínimo privilegio (Principle of Least Privilege, PoLP)

Entender el principio de mínimo privilegio es fundamental, ya que los administradores deben encontrar un equilibrio entre la facilidad y la seguridad, protegiendo el acceso sin causar fricciones a los usuarios. Si el acceso es demasiado restrictivo, los empleados no podrán hacer su trabajo. Si es demasiado laxo, se abre la puerta a los ataques.

¿Qué es el mínimo privilegio?

El mínimo privilegio es la práctica de restringir la creación de cuentas y los niveles de permiso a sólo los recursos que un usuario requiere para realizar una actividad autorizada.

Los términos acceso mínimo de usuario y cuentas de usuario con menos privilegios se aplican a los seres humanos que utilizan un ordenador o un servicio de red. Pero la gestión del acceso con mínimos privilegios también se aplica a las máquinas, incluyendo aplicaciones, procesos, sistemas y dispositivos conectados.

El principio del modelo de mínimo privilegio (también llamado principio de mínimo privilegio o principio de mínima autoridad) está ampliamente considerado como una de las mejores prácticas en seguridad de la información. Y es un paso fundamental para proteger el acceso privilegiado a los datos y activos críticos.

¿Por qué es importante?

El principio del mínimo privilegio ofrece muchas ventajas, ya que consigue un equilibrio entre la facilidad de uso y la aplicación de las protecciones de seguridad. Una política de este tipo salvaguarda los datos y sistemas críticos condensando la superficie de ataque, limitando el alcance de los ataques, mejorando el rendimiento operativo, simplificando la auditoría y el cumplimiento, y reduciendo el impacto de los errores humanos.

El principio del mínimo privilegio ayuda a las organizaciones a cumplir con la tríada de la CIA: confidencialidad, integridad y disponibilidad, centrándose en el segundo concepto del trío.

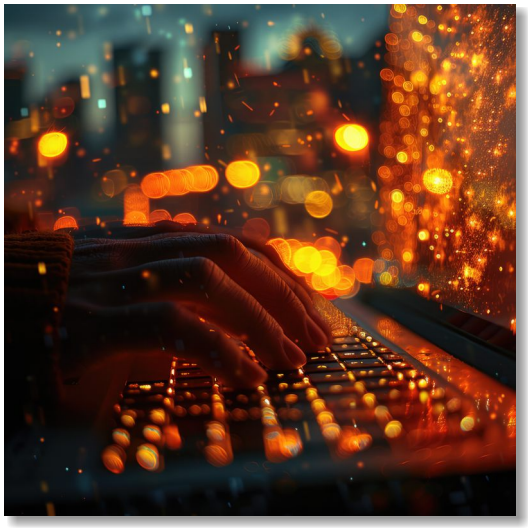
Los usuarios con demasiados privilegios ya sean humanos o máquinas, aumentan la posibilidad de que se produzcan incidentes dentro de una organización y el alcance de los daños a los sistemas críticos en caso de que se produzca una infracción. Sin las protecciones adecuadas, los vectores de amenazas privilegiadas más comunes, incluidos los cibercriminales/actores maliciosos/adversarios digitales, el malware y las personas con información privilegiada, pueden hacer un mal uso, explotar o dañar activamente los sistemas altamente sensibles. Incluso los usuarios bien intencionados pueden causar daños. Cerca del 50% de las violaciones de datos por parte de personas con información privilegiada no son intencionadas (2022 - Huawei Whitepaper "Amenazas de seguridad en entornos de Nube")

¿Cuáles son las ventajas del mínimo privilegio?

Minimiza la superficie de ataque

Limitar los privilegios condensa la superficie de ataque general de tu organización, disminuyendo las vías que un actor malicioso, o no, podría utilizar para explotar credenciales privilegiadas para acceder a datos y credenciales sensibles o llevar a cabo un ataque. Una amplia superficie de ataque (muchas vías de entrada) es difícil de defender. Al limitar los privilegios de superusuario y de administrador, se facilita la prevención, detección y defensa de actividades peligrosas.

Reduce la propagación del malware



Cuando a los usuarios se les concede demasiado acceso, el malware puede aprovechar los privilegios elevados para moverse lateralmente por la red, lanzando potencialmente un ataque contra otros ordenadores conectados en red. Puedes limitar la propagación del malware conteniéndolo en la pequeña sección en la que entra por primera vez en tu red. Además, la gestión de puntos finales con privilegios mínimos frena la capacidad de los usuarios de instalar aplicaciones no autorizadas, reduciendo aún más las posibilidades de propagación.

Mejora el rendimiento operativo

El principio de mínimos privilegios, cuando se aplica correctamente, mejora la productividad del personal, refuerza la estabilidad del sistema y mejora la tolerancia a los fallos. Reduce el tiempo de inactividad del sistema que, de otro modo, podría producirse como resultado de una infracción, la propagación de malware o problemas de incompatibilidad entre aplicaciones.

Facilita la preparación para las auditorías

Además de cumplir con un requisito común de cumplimiento, PoLP ayuda a las organizaciones a prepararse para pasar una auditoría estableciendo y manteniendo las políticas internas de la empresa y proporcionando una pista de auditoría de la actividad privilegiada en la red.

Protege contra el elemento humano

Ya sea por error, malicia o negligencia, los usuarios pueden causar un gran daño a una organización cuando no se les controla. PoLP limita el poder de las personas internas que deciden hacer daño. El sabotaje de los empleados incluye la colocación de códigos maliciosos, el cambio de contraseñas administrativas y el mal manejo de los datos. Pero incluso los usuarios bien intencionados pueden escribir mal un comando o borrar accidentalmente información crucial. El modelo de control de acceso de mínimo privilegio reduce el daño potencial al limitar el alcance de la acción.

Desafíos para la Seguridad del Control de Acceso

El exceso de usuarios puede provocar problemas, como una mayor superficie de ataque, un rendimiento operativo deficiente y dificultades de cumplimiento. ¿Por qué las organizaciones no logran implementar y mantener el acceso con menos privilegios?

El concepto de la gestión de acceso con mínimos privilegios es sencillo, su aplicación puede ser difícil. Hay factores que van desde las expectativas de los empleados hasta la complejidad de los entornos informáticos que pueden obstaculizar el PoLP en la práctica.

Retos:

Frustración de los empleados

Cuando los intentos de restringir el acceso causan fricción, la frustración entre los usuarios y los administradores aumentará. Esto es especialmente cierto en los entornos DevOps (desarrollo de aplicaciones en menos tiempo y la rápida publicación de funciones de software nuevas o revisadas o productos para los clientes), en los que la atención se centra en la velocidad y la automatización. Los administradores de las organizaciones pueden elegir el camino de la menor resistencia en lugar de enfrentarse a una oleada de dolores de cabeza administrativos. Mientras que los de organizaciones más pequeñas, donde los miembros del equipo son conocidos y de confianza, pueden creer que son inmunes a las amenazas. En estos casos hay que pensar en la seguridad desde la viabilidad del proyecto, desde el diseño y por defecto.

Proliferación de la nube

La escala y lo efímero de la computación nativa en la nube también puede causar problemas con el exceso de aprovisionamiento, el uso compartido de cuentas y la falta de segmentación. Muchos usuarios esperan que los servicios en la nube apliquen la seguridad integrada. Y aunque las herramientas basadas en la nube son una mejora respecto a las soluciones manuales para asegurar las cuentas privilegiadas, la implementación de PoLP requiere en última instancia una estrategia, no simplemente un producto.

Falta de granularidad

Los sistemas operativos no aplican el principio de mínimo privilegio por defecto. La mayoría de los sistemas no tienen la granularidad necesaria de privilegios y permisos para aplicar este principio con precisión.

Credenciales por defecto

Los sistemas operativos vienen con condiciones de software por defecto que enfatizan las características, las funciones y la facilidad de uso, a expensas de la seguridad (libro blanco del Instituto SANS). Más allá de las condiciones por defecto del sistema operativo, las credenciales integradas en las herramientas y aplicaciones de CI/CD, así como los errores de configuración, pueden proporcionar un acceso excesivamente privilegiado a las cuentas de la máquina.

Los pequeños desafíos pueden convertirse en grandes problemas. Una mala higiene de las contraseñas, el acceso de terceros/proveedores y las credenciales por defecto fáciles de adivinar, por ejemplo, pueden dejar las cuentas privilegiadas sin ver y sin gestionar. Por lo tanto, no basta con establecer políticas de mínimos privilegios como parte de tu estrategia de gestión de accesos. Las cuentas también deben ser descubiertas y gestionadas cuidadosamente.

CONCLUSIÓN–MEJORES PRÁCTICAS

A medida que las organizaciones trabajan para fortalecer sus defensas, implementar el principio de privilegio mínimo debería ser una máxima prioridad. Al restringir el acceso de los usuarios únicamente a los recursos y datos necesarios para realizar un trabajo, los riesgos se reducen significativamente.

Adoptar un enfoque de "Confianza cero"y verificar cada solicitud como si viniera de una red que no es de confianza es la dirección adecuada. El principio de privilegio mínimo es una mejor práctica fundamental que todos los programas de ciberseguridad deberían adoptar para generar resiliencia y reducir las vulnerabilidades. Hacer cumplir estrictamente los controles de acceso y auditarlos continuamente es lo más responsable y prudente.

Jorge Noguerales Bautista

Política de Seguridad (estrategia de seguridad del ENS) enfocado a PYMES

Hay nuevos requisitos del mercado de gran importancia en la actualidad como los requisitos necesarios para poder adatarse a las nuevas regulaciones y requerimientos del mercado de la Seguridad Privada y su relación con la Seguridad Publica definidos en el : **Esquema de Seguridad Nacional - ENS que AES quiere enfocar en esta NEWSLETTER específicamente para PYMES ,** en los que AES puede ser de gran ayuda a este tipo de empresas, de manera que puedan adaptarse a las normativas que se están elaborando desde el CCN, y poder competir en este segmento tan importante y evolutivo del mercado de la seguridad, con el cumplimiento necesario para concursos Públicos , que serán en un futuro inmediato aplicables también para gran parte de la Seguridad Privada.

A continuación resumimos las **recomendaciones de AES para las PYMES de la industria**, que faciliten el **cumplimiento del nivel básico del ENS** como primer paso hacia la **"autodeclaración del ENS"**

Este sería un paso necesario para aquellas PYMES que trabajen de manera esporádica para la Seguridad Publica –Concursos Públicos de Centros de enseñanza –Centros de Salud etc.- como parte de los requisitos obligatorios para la cadena de suministro de los clientes finales que conecten a Sistemas de Seguridad & Centrales Receptoras de Alarma en España, con atención de las fuerzas y cuerpos de Seguridad del estado.

Además, será el primer paso para futuras regulaciones previstas dentro de la normativa NIS, con una aplicación más amplia que incluye al sector privado, y que claramente tiende a un mercado de Seguridad Global con una normativa más exigente, a la que las PYMES deben de adaptarse para poder competir en igualdad de condiciones.

Adicionalmente, es importantísimo considerar que esta certificación sería un gran paso adelante para el cumplimiento de los **requerimientos y guías que está publicando el CCN** en diversos documentos ya publicados que mencionamos a continuación para el cumplimiento de la **Directiva NIS**.

Esta directiva NIS, en un futuro inmediato afectara no solamente a la Seguridad Publica sino también a gran parte de la Seguridad Privada, tendiendo a la globalización de la normativa como comentaba , en las que **el cumplimiento del ENS en muchos casos garantizaría el cumplimiento del NIS** y en cualquier caso sería de gran ayuda para completar su cumplimento en casos específicos que sean necesarios, en los que la **CCN recomienda los pasos a seguir para complementarlos en sus Guías y simuladores que recomendamos a continuación para su cumplimiento:**

Obligatoriedad de cumplimiento del ENS para trabajar con Seguridad Publica –Nivel Básico:

Permite una posible autodeclaración que habilita a la PYMES para el cumplimiento del primer nivel –previa a la certificación necesaria en casos más avanzados- que serán tratados en el futuro.

Para elaborar la declaración de aplicabilidad se recomienda utilizar:

BP/14 Declaración de aplicabilidad –Buenas Prácticas CCN-CERT

https://www.ccn-cert.cni.es/es/informes/informes-de-buenas-practicas-bp/3830-ccn-cert-bp-14-declaracion-de-aplicacibilidad-ens/file;

Simulador de declaración de aplicabilidad CCN-CERT

https://www.ccn-cert.cni.es/informes/informes-ccn-certpublicos/6945-ccn-cert-bp-14-declaracion-de-aplicabilidad-ensanexos/file.html;

En AES hemos configurado una **Guía de ayuda para las PYMES**, y queremos ayudar no solamente a nuestras PYMES asociadas , sino **también animar a aquellas PYMES que no están asociadas a considerar su incorporación a nuestra asociación**, en la que facilitaremos la adaptación a una serie de normas –que están avanzando y evolucionando muy rápidamente –de acuerdo con la Normativa ya publicada por en CCN , que describimos a continuación.

GUÍA DE ADECUACIÓN AL ESQUEMA NACIONAL DE SEGURIDAD- AES:

https://aesseguridad.es/documentacion/GuiaAdecuacionENS_v3_web.pdf;

El objeto de esta guía es ayudar a las empresas asociadas a AES a analizar las medidas de seguridad de las que disponen sus sistemas de información y determinar si cumplen los requisitos que establece el ENS para disponer de una Declaración de Conformidad de categoría Básica

Desde AES os animamos a que las PYMES de nuestra asociación den este primer paso, que sin duda va a ser necesario para el cumplimiento de la normativa ya vigente a nivel nacional, y que todo parece indicar que será de amplia aplicación en el Seguridad Privada a través de la normativa NIS en un futuro cercano, tendiendo a la Globalización de la seguridad

Desde mi punto de vista, estos requisitos de Certificación están avanzando más rápidamente en los últimos años, y **requiere un esfuerzo de adaptación. especialmente para las PYMES** que no tienen los recursos de las grandes empresas, si quieren sobrevivir en este mercado, cada vez más acostumbrado a “Filtrar los candidatos“ a los concursos tanto de Seguridad Publica como Seguridad Privada.

Desde AES queremos animar a todas las PYMES a considerar este esfuerzo de adaptación a las normas de manera decidida, estamos a vuestra disposición para tomar este importante paso adelante.

Pedro de Ibarrondo.

Elaborado por el Área de
Trabajo de ciberseguridad de:

AES
ASOCIACIÓN ESPAÑOLA
EMPRESAS DE SEGURIDAD

C/Alcalá, 99 2ºA - 28009 Madrid
Telf. 915 765 225

www.aesfundacion.es
patronato@aesfundacion.es

@FundacionAES AES Fundación