ESQUEMA NACIONAL DE SEGURIDAD (ENS)
Principios básicos (I)

Introducción

En el anterior artículo que publicamos, definíamos **qué es el Esquema Nacional de Seguridad y cuáles eran los fundamentos jurídicos en los que se basaba**. Recordemos que el **Esquema Nacional de Seguridad establece una forma de trabajar (procedimientos, estructura organizativa, normas, etc.) para evitar problemas que afecten a la seguridad de la información que "pasa por las manos" de las Administraciones Públicas.**

Volvamos a nuestro sufrido trabajador al que le han encomendado implantar el ENS. Ya le hemos explicado y tiene claro (o al menos eso dice):

- Qué es el ENS.
- Por qué existe el ENS.
- Cuál es la legislación en la que se basa.

A continuación, probablemente, nos pedirá que le resumamos en pocas palabras **qué deberíamos tener en cuenta y qué nos van a exigir que hagamos**. De forma muy simplificada

- **Que deberíamos tener en cuenta->Principios básicos**
- **Qué nos van a exigir que hagamos->Requisitos mínimos**

En este artículo y en otro posterior expondremos dichos principios básicos a tener en cuenta al diseñar el Sistema de Gestión de Seguridad de Información (SGSI) de seguridad en nuestra empresa para implantar el ENS.

Principios básicos

Recordemos que el punto de partida del ENS es el **Real Decreto 311/2022.** En el mismo se regula su funcionamiento y se definen las responsabilidades administrativas. Otro de los aspectos que se definen en el **artículo 5** son los **principios básicos de seguridad** a en cuenta. Estos principios son los siguientes:

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

e8D Soluciones
www.e8dsoluciones.es
C.T.M. Crtra. Villaverde – Vallecas, km. 3,5 Oficina 801A
28053 Madrid
Tlf: 913552930

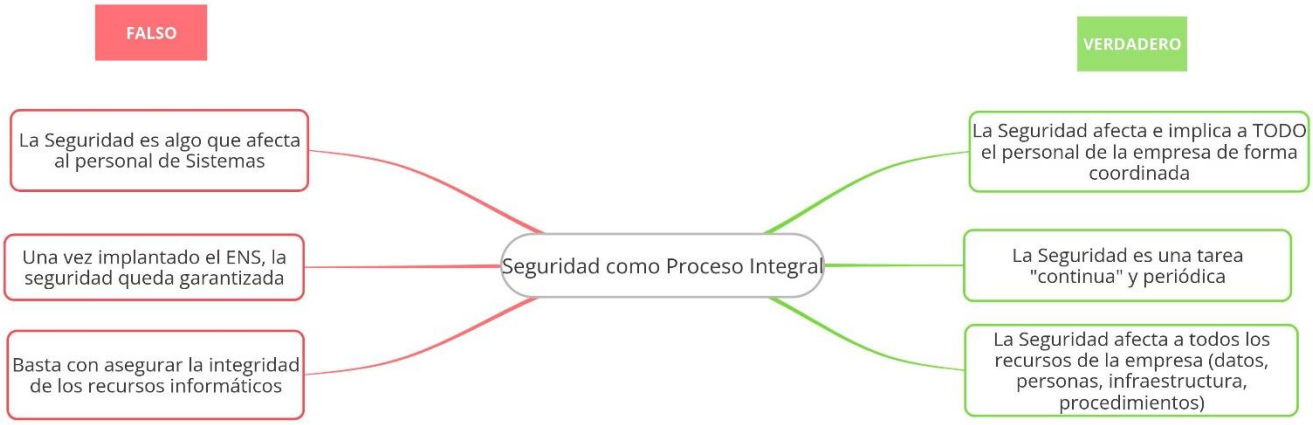
- Reevaluación periódica.
- Diferenciación de responsabilidades.

Vamos a detallar qué debemos y qué no debemos tener en cuenta en cada caso:

1. **Seguridad como proceso integral**

En primer lugar, debemos tener en mente que esto de la Seguridad no es algo que afecte "a los de Sistemas". Tampoco es algo que "se arregle instalando un antivirus y actualizando los PCs". Una empresa se compone de personas (desde el Director a los estudiantes que están haciendo prácticas), equipos, procesos, datos (informatizados o en papel, etc.) De la misma forma, la Seguridad debe abarcar todos esos aspectos.

Y, lo sentimos, esto no es algo que "se arregle" con unos meses de trabajo tras los cuales nos podamos olvidar del tema: **es algo vivo, que debe gestionarse de forma continua**.



2. **Gestión de la seguridad basada en los riesgos.**

En nuestra vida diaria, nos pueden pasar muchas cosas. Por ejemplo:

- Nos puede caer un meteorito
- Conduciendo un coche, podemos tener un accidente de tráfico

Ambas cosas son posibles, pero el riesgo de que nos caiga un meteorito encima es muy bajo y, la verdad, podemos hacer muy poco para evitarlo y eliminar sus consecuencias. Por el contrario, existe un cierto riesgo de sufrir un accidente de tráfico, pero **podemos minimizar este riesgo y sus consecuencias** (conduciendo de forma responsable y poniéndonos el cinturón de seguridad)

De igual forma, cuando abordamos la Seguridad, debemos **analizar y evaluar los riesgos a los que estamos sometidos para orientar la planificación.** Nos centraremos, en primer lugar, en actuar sobre los riesgos críticos, dejando para el final aquellos que muy

raramente podrían afectarnos (y por cierto este análisis debe realizarse periódicamente).

3. **Prevención, detección, respuesta y reparación.**

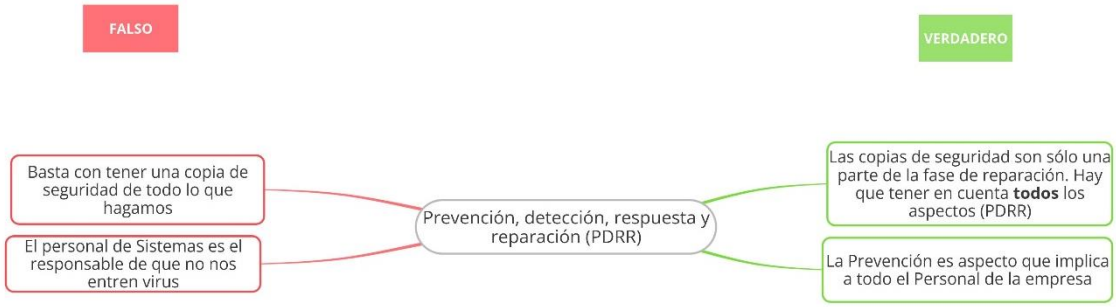
Tenemos que establecer una operativa de trabajo y medios que permitan:

- **Prevenir** las amenazas: por ejemplo, establecemos la obligación de actualizar automáticamente las aplicaciones de nuestros PCs. De esta forma nos adelantamos a posibles brechas de seguridad.

- **Detectar las amenazas:** formando a los usuarios para que sepan cómo actuar a la hora de gestionar los mensajes de correo, distinguiendo aquellos válidos de los que son amenazas (malware, phishing, etc.)

- **Responder a dichas amenazas**: redactando un procedimiento en el que se especifique cómo actuar cuando se detecte/produzca dicha amenaza.

- **Reparar el daño**: utilizando las copias de seguridad para restaurar los archivos/equipos dañados



4. **Existencia de líneas de defensa**

Ya hemos visto que la seguridad es algo que debe abordarse desde muchos puntos de vista:

- **Formando y concienciando al personal:** este es, sin duda, el patito feo de la prevención. Por el contrario, debería ser uno de los primeros pilares sobre el que edificar la Seguridad en la empresa.

- **Contando con medios técnicos que permitan detectar y eliminar amenazas**

- **Redactando e implantando procedimientos de trabajo** para que el personal sepa cómo actuar ante las amenaza.

- **Estableciendo responsabilidades precisas**: un técnico de sistemas tiene una serie de tareas que hacer que nos son las mismas que las que debe realizar el Presidente de la empresa o un administrativo

- **Prevenir** las amenazas: por ejemplo, establecemos la obligación de actualizar automáticamente las aplicaciones de nuestros PCs. De esta forma nos adelantamos a posibles brechas de seguridad.

Pues bien, en consonancia con todo lo anterior, la Seguridad debe garantizarse en capas de cebolla", estableciendo:

- **Múltiples líneas de defensa**: no basta con tener una sola línea de defensa "muy fuerte" (por ejemplo, un antivirus infalible).

- **De diferente tipología:** debemos tener líneas de defensa

    - Tecnológicas: antivirus, firewall
    - Físicas: acceso a sala de servidores restringido mediante clave
    - Organizativas: únicamente el personal de Sistemas conocerá las claves de acceso a la sala de servidores
    - Formativas: sesiones periódicas de formación a **todo** el personal

Resumen

En este primer artículo y en otro posterior expondremos los Principios Básicos de Seguridad que debemos tener en mente a la hora implantar un Sistema de gestión de Seguridad acorde a los requisitos del Esquema Nacional de Seguridad. Como idea

principal, es importante tener en mente que la Seguridad es un entorno **integral que afecta e implica a toda la empresa (personal, procedimientos, infraestructuras, datos…)**

En un artículos posteriores **expondremos el resto de Principios** y empezaremos a detallar, **de forma concreta qué nos exige el Esquema Nacional de Seguridad para implantar y certificar nuestro Sistema de Gestión de Seguridad**.