Intedya
International Dynamic Advisors

ENS - Esquema Nacional de Seguridad

Los ciudadanos se sienten cada vez más cómodos con el **uso de las nuevas tecnologías** y las van incorporando a su forma de vida: compramos ropa, comida o entradas de cine desde el móvil, usamos la banca electrónica, etc., con oficinas que no cierran y están disponibles en cualquier punto del planeta con conexión a Internet. Solo era cuestión de tiempo que las personas, en su rol de ciudadanos con obligaciones y derechos, demandarán a las administraciones públicas este tipo de relación/servicio.

De aqui nace en España el **Esquema Nacional de Seguridad ENS** que crea las **condiciones** necesarias para que se puedan usar medios electrónicos en la **comunicación** de la administración pública con los ciudadanos y a la inversa, todo ello **con las garantías necesarias**. Se trata de garantizar a los ciudadanos que su información se custodiará y utilizará adecuadamente, creando un sistema de gestión de la seguridad de su información seguro y confiable.

El **Esquema Nacional de Seguridad ENS** se desarrolla sobre las recomendaciones de la UE y los estándares internacionales en materia de seguridad de la información, especialmente la Norma ISO 27001, resultando el **marco obligatorio para las administraciones públicas españolas**, para la protección de la información y su gestión a través de los medios electrónicos **y para todos aquellos proveedores de servicios TIC de la administración publica.**

Principales **REQUISITOS**

- EVALUACIÓN, GESTIÓN y TRATAMIENTO del **RIESGO**, como elemento clave;
- Medidas de Seguridad ORGANIZATIVAS, **OPERACIONALES** y de **PROTECCIÓN**
- Establecimiento de **MECANISMOS DE CONTROL** de acceso físico, lógico, control de red y criptográficos;
- **Asegurar** la **seguridad de la información** en el **SERVICIO A TERCEROS** y en el **INTERCAMBIO** de la información;
- Disponer de **CONTRATOS DE CONFIDENCIALIDAD** con los empleados;
- Formalización de **ACUERDOS CON PROVEEDORES** que incluyan requisitos de seguridad;
- Adquisición de **COMPONENTES CERTIFICADOS**;
- Cumplimiento con la **LEGISLACIÓN APLICABLE** en materia de protección de datos personales;
- **USO DE SOFTWARE** con licencias;
- **GESTIÓN DE INCIDENCIAS** relativas a la seguridad de la información;
- La importancia de la gestión desde el punto de vista seguridad de la información debe comunicarse dentro de la organización, la **TOMA DE CONCIENCIA Y EL COMPROMISO** de todas las personas es imprescindible para que el sistema funcione **;**
- Proporcionar la **FORMACIÓN** necesaria para **garantizar la competencia de las personas** que realizan tareas relacionadas con la seguridad de la información;
- **PRESERVACIÓN DE LA CONTINUIDAD** de los recursos de información, realización de pruebas;
- Protección frente a la **DENEGACIÓN DE SERVICIO.**

Ejemplos de **ACCIONES PRÁCTICAS A IMPLEMENTAR**

- Realización del análisis de riesgos de seguridad de la información.
- Formalización de contratos de confidencialidad con los empleados y proveedores.
- Formalización de acuerdos prestación de servicio.
- Uso de credenciales de acceso a las instalaciones para visitantes.
- Mecanismos que obstaculicen el acceso a las áreas seguras: dispositivos biométricos, etc.
- Uso de dispositivos de alimentación interrumpida.
- Uso de controladores de temperatura CPD.
- Uso de licencias legales.
- Realización de planes de continuidad
- Planes de prueba: caída de suministro eléctrico, fallos en los servidores, fallo comunicaciones, incendio edificio, etc.
- Política de gestión de contraseñas.
- Limitar la utilización de usuarios genéricos y los permisos de administración.
- Restringir los puertos USB a puestos determinados.
- Implantar y configurar un antivirus para todos los equipos de la organización, incluyendo los dispositivos móviles
- Instalación de Firewalls, VPN.
- Controlar y prohibir el acceso remoto hacia la propia organización.
- Limitar la navegación a páginas de ciertos contenidos y Sistemas de Detección de Intrusos.
- Realización de copias de seguridad.
- Segmentación de redes y conexiones seguras.
- Proteger las claves de acceso a sistemas, datos y servicios, almacenándolas de forma cifrada.
- Uso certificado digitales para el intercambio de información.

Intedya
International Dynamic Advisors

*Las acciones indicadas son sólo ejemplos, estás deberán ser adaptadas a la realidad y necesidades de cada organización

Solicitar **Información**

Autoevaluación **On Line**

Descargar **Presentación**

Ver video de **Presentación**

Ventajas para **LA ORGANIZACIÓN**

Las **organizaciones públicas y privadas** que implantan un **Sistema de Gestión de Seguridad de la Información** conforme a las directrices del **Esquema Nacional de Seguridad ENS** consiguen generar confianza en que los sistemas de información prestaran sus servicios y custodiaran la información sin interrupciones o modificaciones fuera de control, y sin que la información pudiera llegar a personas no autorizadas, a través de la implantación de medidas de seguridad **organizativas**, **operacionales** y de **protección** para garantizar la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos, que permita a los ciudadanos y a las Administraciones públicas, el ejercicio de sus derechos y el cumplimiento de sus deberes a través de estos medios.

Los diferentes niveles de configuración de un Sistema de Gestión de Seguridad de la Información conforme a los requisitos del ENS (bajo - medio - alto) permiten a las organizaciones adaptar las medidas de forma proporcional al nivel de seguridad requerido por su configuración. De forma adicional tener certificado el ENS es un requisito para lo proveedores de servicios de TI y similares para prestar servicios y proyectos a entidades públicas en España.

Ventajas para **LOS CLIENTES**

La implantación de Sistemas de Seguridad de la Información conforme a las directrices del Esquema Nacional de Seguridad ENS permiten a los ciudadanos y a las administraciones publicas gestionar información con garantía de seguridad suficiente.

Ventajas para **EL MERCADO**

Las entidades de derecho privado vinculadas o dependientes de las Administraciones Públicas adoptan la condición de sujeto obligado por el ENS a todos los efectos, por lo que la implantación de un Sistema de Gestión de Seguridad de la Información conforme con las directrices que establece el ENS les permite optar a ser proveedores de productos de seguridad de la información y/o de servicios TI para la Administración.

Sectores **DE APLICACIÓN**

- La Administración General del Estado
- Las Administraciones de las Comunidades Autónomas
- Las entidades que integran la Administración Local
- Todas las entidades de derecho público vinculadas o dependientes de la Administración
- Las organizaciones privadas que sean proveedores de productos de seguridad de la información o de servicios TI para la Administración

Solicitar **Información**

Autoevaluación **On Line**

Descargar **Presentación**

Ver video de **Presentación**