# NIS2 - Directiva Europea de Ciberseguridad en Entidades Críticas

El uso de redes y sistemas de información se ha convertido en un aspecto crucial para el desarrollo de las actividades sociales y económicas gracias a la velocidad de la transformación digital y la creciente interconexión de la sociedad. Al mismo tiempo, esta evolución supone una expansión de las **ciber amenazas**, con la aparición de nuevos desafíos que requieren respuestas adaptadas, coordinadas e innovadoras. El número, la magnitud, la sofisticación, la frecuencia y los efectos de los **ciber incidentes** representan una grave amenaza para el funcionamiento de las redes y sistemas de información, que pueden llegar a perturbar las actividades económicas, mermar la confianza de los usuarios y ocasionar grandes daños a la economía, la sociedad y la seguridad nacional, y requieren de un esfuerzo permanente para combatirlos.

En este marco aparece la **NIS2** o **Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo**, relativa a las medidas destinadas a garantizar un elevado **nivel común de ciberseguridad** en toda la Unión con el objetivo de determinar los requisitos de ciberseguridad que deben implementar las organizaciones de la Unión Europea que se consideran como infraestructuras críticas.

**En esta ficha podrá descargar una práctica presentación en PDF de la Directiva NIS2**

Solicitar **Información**

Autoevaluación **On Line**

Descargar **Presentación**

Ver video de **Presentación**

## Principales **REQUISITOS**

- **Evaluación y Gestión de Riesgos:** Las organizaciones deben realizar evaluaciones periódicas de los riesgos de sus redes y sistemas de información
- **Respuesta e Informes sobre Incidentes:** Se imponen estrictos requisitos de notificación de incidentes.
- **Continuidad de las Actividades:** Las entidades deben desarrollar y mantener planes de continuidad de la actividad y de recuperación en caso de catástrofe
- **Seguridad de la Cadena de Suministro:** Las organizaciones son responsables de gestionar los riesgos de ciberseguridad en toda su cadena de suministro.
- **Gobernanza y Responsabilidad:** La dirección debe participar activamente en la supervisión de la ciberseguridad
- **Medidas Técnicas y Organizativas Específicas**

## Ejemplos de **ACCIONES PRÁCTICAS A IMPLEMENTAR**

- Políticas de análisis de riesgos y seguridad de los sistemas de información.
- Gestión de incidentes.
- Continuidad de la actividad y gestión de crisis.
- Seguridad de la cadena de suministro.
- Seguridad de la adquisición, el desarrollo y el mantenimiento de redes y sistemas de información, incluidos la gestión y la divulgación de vulnerabilidades.
- Políticas y procedimientos para evaluar la eficacia de las medidas de gestión de riesgos de ciberseguridad.
- Prácticas básicas de higiene cibernética y formación en ciberseguridad.
- Políticas y procedimientos relativos al uso de la criptografía y, en su caso, del cifrado.
- Seguridad de los recursos humanos, políticas de control de acceso y gestión de activos.
- Uso de la autenticación multifactorial o de la autenticación continua.
- Sistemas seguros de comunicaciones de voz, vídeo y texto y sistemas seguros de comunicaciones de emergencia.

## Ventajas para **LA ORGANIZACIÓN**

La implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) bajo los requisitos de la Directiva NIS2 ofrece a las organizaciones una serie de ventajas significativas, que van más allá del simple cumplimiento normativo. Estas ventajas se traducen en una mayor resiliencia, confianza y competitividad en el entorno digital actual a través de una mayor resiliencia ante ciberataques, protección de la reputación y la confianza, continuidad del negocio, mejora de la eficiencia y la productividad, fortalecimiento de la cadena de suministro, cumplimiento normativo y cooperación y colaboración con las partes interesadas.

## Ventajas para **LOS CLIENTES**

Los clientes de una organización que implanta y mantiene un sistema de gestión de seguridad de la información bajo los requisitos de la Directiva NIS2 saben que la información gestionada por su proveedor para la prestación del servicio o para la generación del producto que reciben dispone de todos los controles necesarios para garantizar su protección y preservación y para asegurar la continuidad de las operaciones.

## Ventajas para **EL MERCADO**

Empresas comprometidas con la seguridad de la información, que garantizan una adecuada gestión de la información con la que trabajan.

## Sectores **DE APLICACIÓN**

Se aplicará a las entidades públicas o privadas que tengan su residencia fiscal en España y que estén dentro de los sectores de **alta criticidad y otros sectores críticos**, cuando sean medianas o grandes empresas (**50 o más trabajadores y un volumen de negocios anual superior a 10 millones de euros**)

**Sectores de ALTA CRITICIDAD:**

ENERGIA: **Electricidad, Sistemas urbanos de calefacción y refrigeración, Crudo, Gas, Hidrogeno**

TRANSPORTE: **Aéreo, Ferrocarril, Marítimo y Fluvial, Carretera**

BANCA: **Entidades de crédito**

INFRAESTRUCTURA DE MERCADOS FINANCIEROS

SECTOR SANITARIO: **Asistencia sanitaria, Laboratorios, Investigación y desarrollo de medicamentos, Fabricación de productos farmacéuticos, Fabricación de productos sanitarios esenciales en situaciones de emergencia se salud pública**

Solicitar **Información**

Autoevaluación **On Line**

Descargar **Presentación**

Ver video de **Presentación**

AGUA POTABLE: **Suministro y distribución**

AGUAS RESIDUALES: **Recogida, eliminación, tratamiento,…**

INFRAESTRUCTURA DIGITAL: **Puntos de intercambio de internet, Servicios DNS, Registro de nombres de dominio, Servicios en la nube, Servicios de centro de datos, Redes de distribución de contenidos, Servicios de confianza, Redes públicas de comunicaciones y Servicios de comunicaciones**

GESTIÓN DE SERVICIOS TIC: **Servicios de seguridad y Servicios gestionados**

ENTIDADES DE LA ADMINISTRACIÓN PÚBLICA: **Exclusión: Poder judicial, Parlamentos y Bancos centrales**

ESPACIO: **Operadores de apoyo a la prestación de servicios espaciales (ej. satélites de comunicación)**

INDUSTRIA NUCLEAR: **Centrales nucleares y entidades relacionadas con la utilización, producción, almacenamiento y transporte de mercancías y materiales nucleares o radiológicos**

**OTROS SECTORES CRÍTICOS:**

SERVICIOS POSTALES Y DE MENSAJERÍA

GESTIÓN DE RESIDUOS

FABRICACIÓN, PRODUCCIÓN Y DISTRIBUCIÓN DE SUSTACIAS Y MEZCLAS QUÍMICAS

PRODUCCIÓN, TRANSFORMACIÓN Y DISTRIBUCIÓN DE ALIMENTOS

FABRICACIÓN: **Productos sanitarios y para diagnóstico in vitro, Productos informáticos, electrónicos y ópticos, Material eléctrico, Maquinaria y equipos, Vehículos de motor, remolques y semirremolques y Otro material de transporte**

PROVEEDORES DE SERVICIOS DIGITALES: **Mercados en línea, Motores de búsqueda en línea y Plataformas de redes sociales**

INVESTIGACIÓN

SEGURIDAD PRIVADA: **Empresas de seguridad privada y Despachos de detectives**