Que es el enisa

- El enisa es la Agencia de la Unión Europea para la Ciberseguridad que se encarga de poner las nuevas normas relacionadas con la ciberseguridad en todos los paises europeos.

Propositos del marco europeo

- Se trata de una apuesta estratégica de la Unión Europea por la ciberseguridad como pilar fundamental para asegurar la resiliencia en la sociedad del siglo XXI.
- Los dos propositos fundamentales:
    - Establecer objetivos, tareas y aspectos organizativos de ENISA.
    - Dar soporte al marco para la creacción de esquemas europeos de certificación de la ciberseguridad.

Que es un SGSI

- Es el Sistema de Gestión de Seguridad de la Información con el objetivo de gestionar la seguridad de la información de las organizaciones

ISO 27001+

- Es parte de la norma ISO 27000.
- La norma ISO 27001 engloba los requisitos del SGSI
- Es certificable.
- Estructura de la norma:
    - Introducción.
    - Alcance.
    - Referencias normativas.
    - Términos y definiciones.
    - Contexto de la Organización.
    - Liderazgo.
    - Planificación.

Las 3 dimensiones que compone el SGSI:

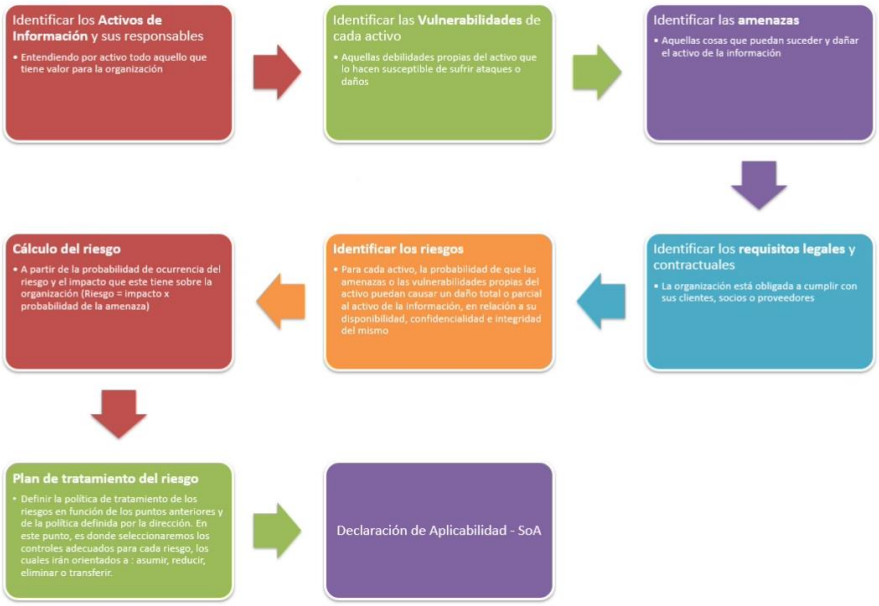
- Confidencialidad (Sólo las personas autorizadas pueden acceder a esta).
- Integridad (No ha sido manipulada de manera no autorizada).
- Disponibilidad (La información puede ser accedida por las personas autorizadas cuando lo necesitan).

Objetivo del SGSI

- El sistema SGSI es una guía que permite a las empresas evaluar los riesgos y definir las aplicaciones de control necesarias para poder eliminarlos o minimizar sus consecuencias negativas.
- Es certificable pero no obligatoria.

Partes de como hacer un Analisis de riesgo

Pasos del Analisis de riesgo



- Los más importantes son los dos últimos.

Plan de tratamiento del riesgo

- El Plan de Gestión de Riesgos o Plan de Tratamiento de Riesgos es un documento que define claramente cómo se va a actuar en el control de los riesgos.

- Este plan establece claramente los recursos necesarios, las responsabilidades y las prioridades establecidas derivadas de la evaluación de riesgos.
- Cuatro acciones del plan:
    - Mitigar el riesgo.
    - Asumir el riesgo.
    - Transferir el riesgo a un tercero.
    - Eliminar el riesgo

SoA (Statement of Applicability) - Declaración de aplicabilidad

- Es un documento formado por la relación completa de los controles de seguridad de la información evaluables. En ella la organización indica si cada uno de ellos es de aplicación o no, detallando los motivos y su estado de implantación.
- Características:
    - El documento SoA puede registrarse en el formato que considere más conveniente la organización, lo realmente importante es su contenido, que generalmente incluirá:
        - Los controles del estándar.
        - Si aplican o no y sus justificaciones.
        - Su estado de implementación.
        - Documentación relacionada (procedimientos, evidencias, etc,...)
        - Todos aquellos datos adicionales que puedan ser considerados necesarios registrar.
- Importancia del SoA:
    - Permite la trazabilidad entre los controles de la norma y lo que realmente se hace en la organización.
    - Permite justificar la inclusión o exclusión de cada control.
    - Las organizaciones que desarrollan e implantan un Sistema de Gestión de Seguridad de la Información (SGSI), y que quieran obtener la certificación para la norma ISO 27001, deberán contar obligatoriamente con el documento SoA.
    - Al documentar cada control aplicable e indicar si se ha implementado o no, se convierte en la guía principal para auditores tanto internos como externos. El auditor accederá a la declaración de Aplicabilidad, y en base a ella desarrollará la auditoría y verificará el cumplimiento de lo documentado.
- Cuando se actualiza:
    - La SoA es un documento vivo, que debe ser actualizado cuando se cumpla uno de los siguientes motivos pero ha de ser actualizado en cualquier momento en que haya cualquier movimiento de datos:
        - Nueva información.
        - La adquisición o sustitución de activos.
        - Cambios organizativos u operacionales.
        - Cambios en el contexto o las necesidades o requisitos de las partes interesadas.

ISO 27001

- Esta norma esta compuesta por un total de 114 controles de seguridad divididos entre 14 secciones.
- Fases de implementación de la norma:
    - Auditoria inicial – GAP
    - Determinación del alcance.
    - Elaboración Política, Objetivos SGSI.
    - Planificación SGSI.
    - Documentación SGSI.
    - Implementación SGSI.
    - Comunicación y sensibilización.
    - Auditoria interna ISO:27001.
    - Revisión por la dirección.
    - Proceso de certificación.
- Ventajas de la norma:
    - Identificar los Activos de Información y sus responsables.
    - Identificar las Vulnerabilidades de cada activo.
    - Identificar las amenazas.
    - Identificar los requisitos legales y contractuales.
    - Identificar los riesgos.
    - Cálculo del riesgo.
    - Plan de tratamiento del riesgo.
    - Declaración de Aplicabilidad – SoA

Acceso electronico

- Mejorar la eficencia de la Administración electrónica.
- El funcionamiento electrónico interno de la administración se realice electrónicamente.
- Incrementar la transparencia de la actuación administrativa y la participación de las personas en la Administración Electrónica.
- Se busca disponer de servicios digitales fácilmente utilizables.

ENS

- El ENS o Esquema Nacional de Seguridad es una normativa que tiene como objetivo establecer los principios que regulan y asguran la información empleada en medios electrónicos en o relacionados con las Administraciones Públicas (estatales, autonómicas y locales).
- Se crea con la necesidad de establecer aspectos y metodologías comunes relativas a la seguridad en la implantación y utilización de los medios electrónicos por las Administraciones Públicas.
- Empresas que deben cumplir con el ENS:
    - Públicos:
        - Dentro de este grupo se encuentran todas las entidades públicas, ya sean nacionales o de comunidades autónomas que tengan a su disposición cualquier tipo de dato sensible de clientes o ciudadanos. Se encuentran en este grupo también las universidades, hospitales o entidades sin ánimo de lucro.
    - Privados:

        - Este grupo está compuesto por cualquier organización de naturaleza privada que preste servicios o cualquier tipo de solución a los organismos públicos que estén contenidos en el anterior grupo. Es decir, cualquier empresa que tenga algún tipo de relación con la administración pública.
- El ámbito de aplicación del Esquema Nacional de Seguridad es el de las Administraciones Públicas, los ciudadanos en sus relaciones con las mismas y el de las relaciones entre ellas
- Categorías del Esquema Nacional de seguridad (ENS):
    - ENS nivel Bajo
        - Este nivel se utiliza cuando las consecuencias de un incidente de seguridad solamente afectan a alguna de las dimensiones de seguridad dentro de la empresa, pero no a todas. Es decir, este nivel supone un perjuicio a las funciones de la organización, a sus activos o a las personas afectadas.
    - ENS nivel Medio
        - Este nivel se utiliza cuando las consecuencias de un incidente de seguridad afectan a alguna de las dimensiones de seguridad dentro de la empresa. Es decir, este nivel supone en perjuicio grave a las funciones de la organización, a sus activos o a los personas afectadas.
    - ENS nivel Alto
        - Este nivel se utiliza cuando las consecuencias de un incidente de seguridad afectan a muchas de las dimensiones de seguridad dentro de la emrpesa. Es decir, este nivel supone un perjuicio muy grave a las funciones de la organización, a sus activos o a las personas afectadas.
- Ambito de aplicación del ENS
    - Como regla general, podemos afirmar que el ENS es de aplicación a:
        - Sedes electrónicas.
        - Registros electrónicos.
        - Sistemas de información accesibles electrónicamente por los ciudadanos.
        - Sistemas de información para el ejercicio de derechos.
        - Sistemas de información para el cumplimiento de deberes.
        - Sistemas de información para recabar información y estado del procedimiento administrativo.
    - No es de aplicación en el caso que el sistema:
        - No esté relacionado con el ejercicio de derechos por medios electrónicos.
        - No esté relacionado con un cumplimiento de deberes por medios electrónicos.
        - No esté relacionado con el acceso por medios electrónicos de los ciudadanos a la información y al procedimiento administrativo.
- Los niveles de categorias entre ENS y LOPD son diferentes entre ellos ya que en LOPD los niveles de seguridad se determinan por la pertenencia del dato a un nivel concreto, para el ENS la categoría del sistema se sustenta en el impacto que un incidente de seguridad podría tener.
- Dimensiones del ENS:
    - El acceso.
    - La confidencialidad.
    - La integridad.
    - La trazabilidad.

    - La autenticidad.
    - La disponibildad.
    - La conservación.
- Caracteristicas y estructuras del ENS:
    - Esta formado por 10 capítulos, 4 disposiciones adicionales, 1 disposición transitoria, 1 disposición derogatoria, 3 disposiciones finales y 5 anexos.
    - Elementos principales:
        - Los principios básicos.
        - Los requisitos mínimos.
        - Medidas de seguridad.
        - Las comunicaciones electrónicas.
        - La auditoría de la seguridad.
        - La respuesta ante incidentes de seguridad.
        - La categorización de los sistemas.
        - La certificación de la seguridad.
        - La conformidad.
- Que es un principio basico
    - Un principio basico es un tipo de guia que usa las empresas para poder garantizar que una organización pueda cumplir sus objetivos, desarrollar sus funciones y ejercer sus competencias utilizando sistemas de información.
- Requisito mínmo:
    - Gestión de personal.
    - Profesionalidad.
    - Mínimo privilegio.
    - Incidentes de seguridad.
    - Continuidad de la activadad.
- Fases para implementar un ENS:
    - Política de Seguridad.
    - Categorización de sistemas.
    - Análisis de riesgos.
    - Declaración de aplicabilidad.
    - Plan de adecuación.
    - Implementación de seguridad.
    - Auditorías.
    - Certificación de conformidad.
    - Vigilancia y mejora continua.
- Plan de adecuación del ENS:
    - Implantar, operar y monitorizar el sistema.
    - Auditar cada dos años.
    - Mejorar la seguridad.
    - Preparar y aprobar la política de seguridad.
    - Definir roles y asignar personas.
    - Valorar/Categorizar el sistema: Información/servicios.
    - Realizar análisis de riesgos.

    - Preparar y aprobar la declaración de aplicabilidad.
- Auditoria de seguridad
    - El objetivo de la auditoria de seguridad es determinar los posibles deficiencias existentes y deberán ponerse en marcha las correspondientes acciones correctoras por el Responsible de Seguridad.
    - Si tiene un nivel Bajo, el ENS no pedira una auditoria sino una auto-evaluación
- Que es el plan de adecuación ?
    - Es el punto de partida para abordar el proceso de implantación del ENS.
- Que es el plan de aplicabilidad ?
    - La Declaración de Aplicabilidad, en el ámbito del ENS, es el documento en el que se formaliza la relación de medidas de seguridad que resultan de aplicación al sistema de información de que se trate, conforme a su categoría.
- Miembros del plan de comité de seguridad.
    - Responsible de la información.
    - Responsible de la Seguridad.
    - Responsible de Sistemas.
    - Responsible del Sistema.
- Funciones del plan de comite de seguridad.
    - Promover la mejora continua del sistema de gestión de la segurida de la información.
    - Aprobar la normativa de seguridad de la información.
    - Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.

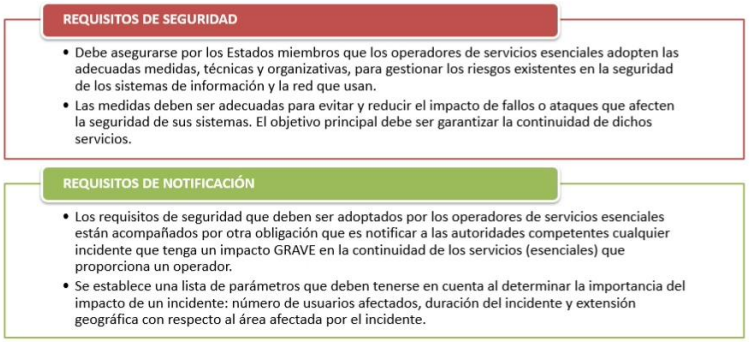
Directiva NIS I

- Es una ley que a la vez es la primera legislación horizontal adoptada a nivel de la UE, para la protección de redes y sistemas de información en toda la Unión.
- Establece requisitos mínimos comunes en materia de desarrollo de capacidades y planificación, intercambio de información, cooperación y requisitos comunes de seguridad para los operadores de servicios esenciales y los proveedores de servicios digitales.
- A quien afecta ?
    - A los operadores de servicios esenciales y a los proveedores de servicios digitales.
- Diferencias entre ellos?

Directiva NIS I - Contexto

¿A quien afecta? La Directiva NIS afecta a dos categorías de empresas:
Operadores de servicios esenciales:
Su definición incluye una entidad pública o privada que se activa en sectores específicos, como el sector de la energía, el transporte, la banca y la salud, y que al mismo tiempo cumple algunos criterios esenciales que lo califican como una entidad de ese tipo.

Estados miembros pueden ampliar las obligaciones de seguridad y notificación previstas para los operadores de servicios esenciales a entidades pertenecientes a otros sectores y subsectores distintos de los enumerados en el anexo de la Directiva NIS.

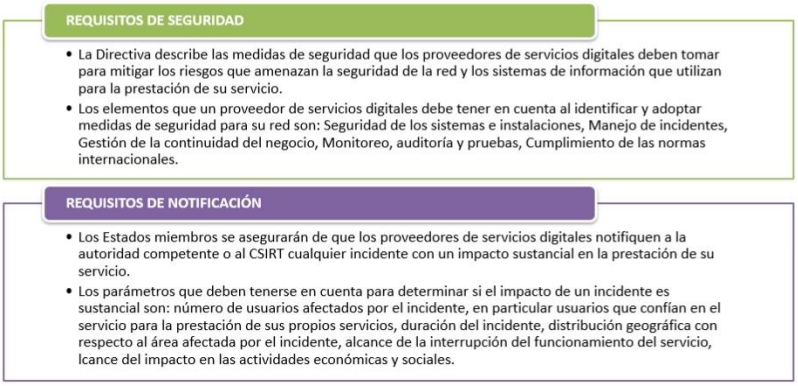


-

Directiva NIS - Contexto

Proveedores de Servicios Digitales:
Estos incluyen cualquier persona jurídica que ofrezca un servicio digital y más específicamente un mercado en línea, un motor de búsqueda en línea o un servicio de computación en la nube.

Su regulación se justifica debido al hecho de que muchas empresas dependen de estos proveedores para la prestación de sus propios servicios. Y por ello, una parada del servicio digital podría tener importantes efectos para las actividades económicas y sociales esenciales en la UE.



-

- Elementos de la directiva NIS:
  - Responsible de Seguridad.
  - Políticas de seguridad.
  - Medidas de seguridad.
  - Obligaciones de seguridad a terceros.
  - Certificado de cumplimiento.
  - Informe de auditoria.

- Elemento de la directiva NIS II fuera de la directiva NIS:
    - Uso de la inteligencia artificial.
- Objetivos de la LPIC.
    - Catalogar el conjunto de infraestructuras que prestan servicios esenciales a nuestra sociedad.
    - Diseñar un planeamiento que contenga medidas de prevención y protección eficaces contra las posibles amenazas hacia tales infraestructuras, tanto en el plano de la seguridad física como en el de la seguridad de las tecnologias de la información y las comunicaciones.
- Diferencias entre infraestructuras criticas y estrategicas:

Legislación sobre la protección de infraestructuras críticas - LPIC

¿Cómo define la Ley PIC las infraestructuras críticas, los servicios esenciales y las infraestructuras estratégicas?

La Ley PIC define como:

- **Infraestructuras críticas** aquellas cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales.

Estos a su vez, se definen como los servicios necesarios para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las Instituciones del Estado y las Administraciones Públicas.

- **Infraestructuras estratégicas** las instalaciones, redes, sistemas y equipos físicos y de tecnología de la información sobre las que descansa el funcionamiento de los servicios esenciales.

- Mejoras de la directiva NIS II:

Directiva NIS II

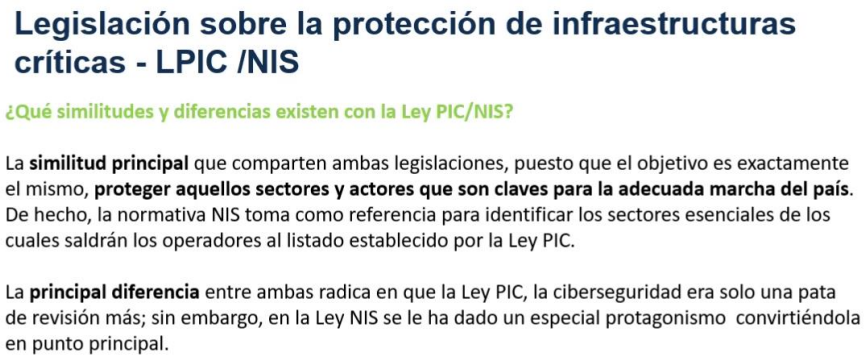
Directiva NIS II vs NIS I

A pesar del reglamento sancionador existente, no podemos decir que la adecuación a NIS I haya sido homogénea en los Estado Miembros, creándose distintos grados de aplicación a la misma y facilitando, en última instancia, la fragmentación del mercado único. Esta circunstancia, unido al incremento de la ciberdelincuencia a nivel mundial debido a distintos factores, hacen de NIS II una directiva muy esperada.

NIS II define las siguientes mejoras respecto a NIS I resumidas en los siguientes puntos:

- Los requerimientos de seguridad se incrementan con un listado de medidas concretas y enfocadas a objetivo, entre las que destacan: respuesta a incidentes, gestión de crisis, gestión de vulnerabilidades, auditorías de ciberseguridad y el uso efectivo del cifrado.
- Se potencia la ciberseguridad en la cadena de suministros de la información crítica y las comunicaciones.
- Responsabilidad de la Dirección en el cumplimiento de las medidas de la gestión de riesgos de ciberseguridad.
- Requisitos y obligaciones en la notificación de incidentes con disposiciones más precisas sobre el proceso, el contenido y los tiempos de respuesta.

- Infraestructura critica:
    - Aquella cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su pertubación o destrucción tendría un grave impacto sobre los servicios esenciales.
- Principal diferencia entre la ley PIC/NIS:



Legislación sobre la protección de infraestructuras críticas - LPIC /NIS

¿Qué similitudes y diferencias existen con la Ley PIC/NIS?

La **similitud principal** que comparten ambas legislaciones, puesto que el objetivo es exactamente el mismo, **proteger aquellos sectores y actores que son claves para la adecuada marcha del país**. De hecho, la normativa NIS toma como referencia para identificar los sectores esenciales de los cuales saldrán los operadores al listado establecido por la Ley PIC.

La **principal diferencia** entre ambas radica en que la Ley PIC, la ciberseguridad era solo una pata de revisión más; sin embargo, en la Ley NIS se le ha dado un especial protagonismo convirtiéndola en punto principal.

    -