Esquema Nacional de Seguridad (ENS) (Normativa de ciberseguridad)

Planes de Continuidad de Negocio (estándares internacionales) (ISO 22.301)

ISO 22301 es una norma internacional de gestión de continuidad de negocio. Esta ha sido creada en respuesta a la fuerte demanda internacional que obtuvo la norma británica original, BS 25999-2 y otras normas.

ISO 22301 identifica los fundamentos de un Sistema de Gestión de la Continuidad de negocio, estableciendo el proceso, los principios y la terminología de gestión de continuidad de negocio.

Proporciona una base de entendimiento, desarrollo e implantación de continuidad de negocio dentro de la organización. Se usa para asegurar a las partes interesadas clave que su empresa está totalmente preparada y que puede cumplir con los requisitos internos, regulatorios y del cliente.

La norma proporciona a las organizaciones un marco que asegura que ellos pueden continuar trabajando durante las circunstancias más difíciles e inesperadas, siempre protegiendo a sus empleados, manteniendo su reputación y proporcionando la capacidad de continuar trabajando y comercializando.

La norma ISO 22301 puede ser aplicada a todo tipo y tamaño de

organizaciones que quieran:

- Establecer, implantar, mantener y mejorar un SGCN.
- Demostrar conformidad con la política establecida de la continuidad de negocio de la organización.
- Dar a las partes interesadas confianza en su conformidad y compromiso con las buenas prácticas reconocidas.

Directiva NIS

Las redes y sistemas de información desempeñan un papel crucial en la sociedad. Su fiabilidad y seguridad son esenciales para las actividades económicas y sociales, y en particular para el funcionamiento del mercado interior. Debido al carácter transnacional de las operaciones, una perturbación grave de esas redes y sistemas, ya sea o no deliberada, y con independencia del lugar en que se produzca, puede afectar a diferentes Estados miembros y a la Unión en su conjunto. Este tipo de incidentes pueden interrumpir las actividades económicas, generar considerables pérdidas financieras, menoscabar la confianza del usuario y causar grandes daños a la economía de la Unión.

La Unión Europea ha ido dando pasos para garantizar una mayor seguridad en las redes y sistemas de información. En este sentido, en febrero de 2013 se publicó la Estrategia de Ciberseguridad de la Unión Europea (Cybersecurity Strategy of the of the European Union: an Open, Safe and Secure Cyberspace). Este documento comprende los aspectos del mercado interior, justicia y política exterior relacionados con el ciberespacio. La estrategia de ciberseguridad y la propuesta de Directiva sirven de apoyo a la Agenda Digital para Europa, cuyo objetivo es ayudar a los ciudadanos y empresas europeos a aprovechar al máximo las tecnologías digitales.

Esta Estrategia se complementa con la Directiva aprobada y publicada ayer 19 de julio en el Diario Oficial de la Unión

Europea, llamada "Directiva del Parlamento Europeo y del Consejo relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información de la Unión" (conocida como directiva NIS) y que entrará en vigor el próximo 9 de agosto.

Según se indica en la Directiva, las capacidades existentes no bastan para garantizar un elevado nivel de seguridad de las redes y sistemas de información en la Unión. Los niveles de preparación de los Estados miembros son muy distintos, lo que ha dado lugar a planteamientos fragmentados. Esta situación genera niveles desiguales de protección de los consumidores y las empresas, comprometiendo el nivel general de seguridad de las redes y sistemas de información de la Unión.
La Directiva NIS busca mejorar esta situación, estableciendo 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 los que insta a adoptar las medidas oportunas para gestionar los riesgos en seguridad y notificar los incidentes que tendrían un efecto perturbador significativo a las Autoridades Nacionales Competentes, proponiendo la creación de una red de cooperación entre todos los diferentes Estados Miembros.

Descarga el documento completo en español aquí.

Legislación sobre la protección de infraestructuras críticas

Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas. Esta Ley tiene por objeto establecer las estrategias y las estructuras adecuadas que permitan dirigir y coordinar las actuaciones de los distintos órganos de las Administraciones Públicas en

materia de protección de infraestructuras críticas, previa identificación y designación de las mismas, para mejorar la prevención, preparación y respuesta de nuestro Estado frente a atentados terroristas u otras amenazas que afecten a infraestructuras críticas. Para ello se impulsará, además, la colaboración e implicación de los organismos gestores y propietarios de dichas infraestructuras, a fin de optimizar el grado de protección de éstas contra ataques deliberados de todo tipo, con el fin de contribuir a la protección de la población.