Tema 2

Introducción al cumplimiento normativo

Bloque 1 Introducción y contexto actual

1. Tendencias y factores externos.
2. Marco normativo nacional e internacional

Contenido

1.1 Tendencias y factores externos

Factores globales que influyen en la gestión de la seguridad de la información y justifica la importancia del rol del CISO en las organizaciones modernas:

- Alta probabilidad de ciberataques y robo o uso fraudulento de datos.
- Transformación Digital, Cloud Computing, IoT o Big Data.
- Tendencia Fast, Cheap & Easy.
- Definición de marcos regulatorios.
- El CISO (Chief Information Security Officer) es trascendental
- La entidad define las atribuciones y el perfil del CISO

El foro económico mundial identifica los ciberataques y robo o uso fraudulento como los más preocupantes tanto en el entorno público como privado debido a su elevada probabilidad e impacto. La dependencia de las redes y de los sistemas de información para el bienestar, estabilidad y crecimiento de las Naciones es un hecho además de la interdependencia de tecnologías e infraestructuras.

Se producen cambios drásticos en la forma de entender cómo la tecnología facilita el negocio, algunos ejemplos son la Transformación Digital, soluciones basadas en Cloud Computing, dispositivos IoT (internet of things) o el Big Data.

La tendencia Fast, Cheap and Easy (rápido, barato y fácil) en la gestión de Sistemas de Información para reducir el tiempo y coste de provisión de nuevas soluciones apoyadas en metodologías ágiles supone un reto en la elaboración de los Análisis de Riesgos y en el control del desarrollo, además de la necesidad de tener en cuenta la Seguridad de la Información durante todo el ciclo de vida de cualquier producto o servicio.

Tanto entidades como empresas se preparan para este cambio, la administración se esfuerza en definir marcos regulatorios tales como La Estrategia de Ciberseguridad, el Reglamento General de Protección de Datos Personales, el Real Decreto-Ley de Seguridad de las Redes y los Sistemas de información, el Esquema Nacional de Seguridad o la normativa sobre protección de infraestructuras críticas y la normativa de seguridad privada. Todas con el objetivo de establecer criterios o medidas de seguridad a aplicar.

Es por todo lo mencionado anteriormente, que el CISO (Chief Information Security Officer) cobra un papel trascendental en las organizaciones del siglo XXI, la seguridad por defecto, desde el diseño y la gestión de los riesgos de seguridad es un elemento clave para garantizar la supervivencia de las organizaciones y la sociedad. El CISO debe ser capaz de cohesionar la estrategia en materia de Seguridad de la información de las organizaciones.

Sin embargo, dependiendo de la entidad estas funciones del CISO pueden ser asignadas a otros roles de la estructura organizativa tales como el CRO (Chief Risk Officer), COO

(Chief Operating Officer), CIO(Chief Information Officer), DPO (Data Protection Officer), CTSO (Chief Technology Security Officer) o CSO (Chief Security Officer). La entidad es quien debe definir el modelo organizativo en base al principio de segregación de funciones. Además, dependiendo de la madurez de las entidades y su sensibilidad el CISO puede encontrarse en diferentes áreas como la alta dirección (formando parte de los comités de dirección), la Dirección de IT, en la dirección de riesgos o en Seguridad Corporativa.

El CISO es una figura clave en las organizaciones, por ello se debe definir sus atribuciones y perfil, de la misma forma que se hizo con el CIO, CFO o Auditoría Interna.

El libro blanco del CISO recoge las diferentes funciones y roles del CISO del siglo XXI, como facilitador del negocio para alcanzar sus objetivos y aumentar su resiliencia.

1.2 Marco normativo nacional e internacional

- Orienta al CISO en las leyes y normativas.
- Depende del modelo organizativo de la empresa.
- Marco legislativo y regulatorio en constante evolución.

El objetivo principal del marco normativo nacional e internacional tiene como finalidad orientar al CISO en las leyes y normativas que debe tener en consideración para ejercer su actividad. Por ello es importante destacar que la normativa aplicable a su función dependerá del modelo organizativo de la empresa, naturaleza y su sector de actividad.

A continuación identificaremos las áreas de actividad sujetas a regulación o normativa, pero siempre debemos tener en mente que el marco legislativo y regulatorio se encuentra en constante evolución, por lo que debemos mantenernos actualizados en cada momento de la regulación de la aplicación.

A este efecto, el Código de Derecho de la Ciberseguridad que publica el BOE:

BOE.es - Ámbitos de la Seguridad Nacional: Ciberseguridad junto con el de Protección de Datos de Carácter Personal, son dos buenas fuentes para identificar y acceder a las versiones actualizadas de la legislación identificada.

Esquema Nacional de Seguridad (ENS)

- Determina la política de seguridad de la información
- Principios básicos y requisitos mínimos para una protección adecuada.
- Referencia legislativa del responsable de la información.
- Esta obligación afecta a todo el Sector Público, a los sistemas de información clasificada y a las entidades del sector privado que les presten soluciones y servicios para el ejercicio de competencias y potestades administrativas.
- Marco de referencia para establecer una política de seguridad

La LEY 11/2007, DE 22 DE JUNIO, DE ACCESO ELECTRÓNICO DE LOS CIUDADANOS A LOS SERVICIOS PÚBLICOS ESTABLECIÓ EL ESQUEMA NACIONAL DE SEGURIDAD (ENS), aprobada mediante Real Decreto 3/2010, de 8 de enero, determina la política de seguridad en la utilización de medios electrónicos en su ámbito de aplicación y se constituye por principios básicos y requisitos mínimos que permiten una protección adecuada de la información.

En 2022 se publicó la nueva versión del Esquema Nacional de Seguridad a través del REAL DECRETO 311/2022, DE 3 DE MAYO.

El ENS tiene por objeto determinar la política de seguridad de la ingormación. Establece los principios básicos y requisitos mínimos que permitan una protección adecuada de la información.

En el ENS encontramos la primera referencia legislativa del responsable de seguridad de la información, la cual dice: "El responsable de la información determinará los requisitos de los servicios prestados; y el responsable de seguridad determinará las decisiones para satisfacer los requisitos de seguridad de la información y los servicios".

Para consideración del CISO el ENS es de aplicación en la Administración General del Estado, Administraciones de las Comunidades Autónomas y Administraciones Locales y en las entidades de derecho público vinculadas a ellas. Las relaciones con las administraciones también se encuentran sujetas al ENS.

Aunque no es de obligada aplicación en empresas privadas, es un marco de referencia para el establecimiento de una adecuada política de seguridad y es de especial interés para aquellas que trabajen próximas a la Administración o quieran acreditarse para el manejo de información clasificada.

Código Penal y Ley de Enjuiciamiento Criminal

El CODIGO PENAL. LEY ORGÁNICA 10/1995, DE 23 DE NOVIEMBRE, del Código Penal está en constante evolución, siendo su última actualización importante en abril de 2023.

El Código Penal es de atención por dos motivos diferentes:

A partir de 2015, la persona jurídica puede ser responsable penalmente de los delitos que expresamente señala el Código Penal que pueden dar lugar a su responsabilidad. Por ello es habitual que las organizaciones desarrollen sistemas de Compliance para prevenir la infracción de normas de carácter penal y evitar eventuales sanciones que generen responsabilidad a la empresa. La participación del CISO es fundamental en estos sistemas de Compliance.

Propiamente por la codificación de los "delitos informáticos", es decir, tanto aquellos en los que la infraestructura IT o la información son el objeto o bien jurídico protegido, como los delitos en los que la tecnología es el medio para su comisión (el llamado "Ciberdelito").

Así mismo, la Ley de Enjuiciamiento Criminal es de atención por contener en el Título VIII, Capítulo 4 y siguientes, información relevante para la obtención de evidencias y el despliegue de controles.

Directiva NIS (Network and Information Systems)

DIRECTIVA 2016/1148 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 6 de julio de 2016 garantiza un elevado nivel común de seguridad de las redes y sistemas de información en la Unión Europea y su REAL DECRETO-LEY 12/2018, DE 7 DE SEPTIEMBRE, DE SEGURIDAD DE LAS REDES Y SISTEMAS DE INFORMACIÓN.

La directiva NIS establece condiciones de seguridad para empresas y organismos que proporcionan servicios esenciales, enmarcadas en los sectores estratégicos tales como la administración, espacio, industria nuclear, industria química, investigación, agua, energía, salud, tecnologías de la información, transporte, alimentación y sistema financiero y tributario.

Regula la seguridad de redes y sistemas de información usados para la provisión de servicios esenciales y servicios digitales (comercio electrónico, motores de búsqueda y grandes servicios de computación en la nube).

El Real-Decreto Ley será ratificado a Ley para que pueda desarrollarse su reglamente en el que se incidirá en las medidas necesarias para la debida protección de los sistemas de información y comunicación de los servicios esenciales y digitales.

Es importante destacar que el RD 12/2018 decía en su artículo 16.3:

"Los operadores de servicios esenciales designarán y comunicarán a la autoridad competente, en el plazo que reglamentariamente se establezca, la persona, unidad u órgano colegiado responsable de la seguridad de la información, como punto de contacto y de coordinación técnica con aquella. Sus funciones específicas serán las previstas reglamentariamente."

La Directiva NIS2 (Network and Information Systems Directive 2) es una actualización de la anterior NIS (2016/1148), que regulaba la seguridad de las redes y sistemas de información en la Unión Europea.

En la NIS original, los Estados miembros eran quienes designaban a los operadores de servicios esenciales y les comunicaban su inclusión dentro del ámbito de aplicación.

Con NIS2, ese enfoque cambia:

Ya no se comunica sólo a los operadores de servicios esenciales, sino a todas las organizaciones que estén dentro del alcance de la normativa (es decir, empresas de sectores considerados críticos o importantes según la Directiva).

Estas organizaciones deben notificarse e inscribirse por iniciativa propia ante la autoridad competente. Si no lo hacen, pueden ser sancionadas.

Por tanto, la NIS2 amplía el número de entidades obligadas a cumplir con medidas de ciberseguridad y gestión de incidentes, reforzando la responsabilidad directa de las empresas.

Los países de la unión europea están en proceso de aplicación de la normativa NIS2 en sus respectivos marcos normativos. En España a día de hoy (octubre 2025) todavía no se ha realizado una trasposición completa de la norma. Existe el anteproyecto de ley: https://www.interior.gob.es/opencms/pdf/servicios-al-ciudadano/participacion-ciudadana/Participacion-publica-en-proyectos-normativos/Audiencia-e-informacion-publica/01_2025_Anteproyecto_ley_coordinacion_gobernanza_ciberseguridad.pdf