CUMPLIMIENTO EN MATERIA DE CIBERSEGURIDAD PARA ORGANIZACIONES DE DEFENSA

Los organismos militares, los ministerios de defensa y las fuerzas armadas necesitan una protección especialmente potente de sus sistemas de información. En los tiempos que corren, la guerra cibernética desempeña un papel crucial en la seguridad nacional y el mejor ataque es una defensa inquebrantable. Seguridad, fiabilidad y disponibilidad son, por tanto, aspectos vitales cuando hay tanto en juego.

> REGLAMENTOS EUROPEOS: CUMPLIMIENTO OBLIGATORIO

> CUMPLIMIENTO OPCIONAL

> REGLAMENTOS ESPECÍFICOS DE CADA PAÍS

> HAY UNA SOLUCIÓN STORMSHIELD PARA CADA PROBLEMA

> EL CUMPLIMIENTO NO BASTA

> REGLAMENTOS EUROPEOS: CUMPLIMIENTO OBLIGATORIO

Las organizaciones de defensa están obligadas a cumplir los siguientes reglamentos comunitarios sobre ciberseguridad:

Reglamento General de Protección de Datos (RGPD)

El RGPD es un reglamento de la UE destinado a armonizar las leyes de protección de datos en toda Europa, a proteger y empoderar a todos los ciudadanos comunitarios en lo relativo a la privacidad de sus datos, así como a reconcebir el enfoque de las organizaciones con respecto a la protección de datos. Esto genera nuevas restricciones y requisitos para los gerentes de TI y TO, así como para los directores de Información y de Seguridad de la información.

Entre estos requisitos resulta clave la «protección de datos por defecto», que establece la protección de los datos personales como una propiedad predeterminada en los sistemas y servicios. Los productos de Stormshield ayudan a las organizaciones a cumplir estos requisitos incrementando la ciberresistencia de sus infraestructuras. Además, Stormshield Data Security ofrece funciones de cifrado de datos, que el RGPD menciona como una medida técnica apropiada para garantizar el nivel de seguridad adecuado al riesgo.

NATO Restricted

Esta clasificación de seguridad se aplica a la información sensible cuya divulgación no autorizada, alteración o indisponibilidad sería perjudicial para los intereses de la OTAN. Si la información clasificada como «NATO Restricted» se transmite fuera de un área segura físicamente restringida, esta clasificación exige que la información sea cifrada mediante productos certificados.

Stormshield Network Security y Stormshield Data Security han obtenido la certificación NATO Restricted. Como tales, pueden implementarse en entornos sensibles para cifrar información clasificada como NATO Restricted y garantizar la transmisión segura de información clasificada.

Cybersecurity Act

El Reglamento Cybersecurity Act sobre la Ciberseguridad de la UE constituye una respuesta a la creciente amenaza de los ciberataques mediante el fortalecimiento de las prerrogativas de la Agencia de la Unión Europea para la Ciberseguridad (ENISA) y el establecimiento de un marco europeo de certificación de la ciberseguridad. El marco europeo de certificación de la ciberseguridad tiene por objeto mejorar la seguridad de los productos conectados, los dispositivos del Internet de las cosas y la infraestructura crítica mediante certificados. Una certificación de productos, procesos y servicios que será válida en todos los Estados miembros. Los tres niveles definidos («básico», «sustancial» o «elevado») permitirán a los usuarios determinar el nivel de garantía de seguridad y garantizarán que los elementos de seguridad se hayan verificado de forma independiente.

Los productos de Stormshield ya han alcanzado el nivel de «cualificación estándar» otorgado por la Agencia Nacional Francesa para la Seguridad de los Sistemas de Información (ANSSI). Dado que el nivel «elevado» del marco europeo corresponde al nivel de «cualificación básica» de la ANSSI, que es inferior al nivel de «cualificación estándar», los productos Stormshield ya cumplen las expectativas de ciberseguridad de la ENISA.

¿Quiere profundizar aún más en la materia? ¡Allá vamos!

> CUMPLIMIENTO OPCIONAL

Las organizaciones de defensa pueden plantearse adherirse a las siguientes normas para mejorar su nivel de seguridad cibernética, aunque su cumplimiento no es obligatorio en virtud de la legislación vigente.

Criterios comunes / Niveles de garantía de evaluación (EAL3+, EAL4+, etc.)

Los Criterios comunes para la evaluación de la seguridad de las tecnologías de la información son una norma internacional (ISO/IEC 15408) para la certificación de la seguridad informática. Proporciona garantías acerca de que el proceso de especificación, implantación y evaluación de un producto de seguridad informática se ha realizado de manera rigurosa, estándar y replicable a un nivel acorde con el entorno de destino para su uso. En virtud de esta norma, el Nivel de garantía de evaluación del producto (EAL3+, EAL4+, etc.) indica el grado de exhaustividad con el que este ha sido testado (por ejemplo, un cortafuegos). Esta certificación está reconocida por unos treinta países de todo el mundo, en Europa, Norteamérica, Asia y Oriente Medio.

Los productos Stormshield no solo están certificados por las normas de Criterios comunes, sino que han obtenido el nivel de «Clasificación de norma» -muy superior- de la Agencia Nacional de Ciberseguridad francesa (la ANSSI). Para lograr este elevado grado de fiabilidad, el producto debe:

- Obtener una certificación de alto nivel con un objetivo de seguridad definido y validado por la ANSSI;
- Superar análisis adicionales realizados por la ANSSI, incluida una auditoría del código fuente del producto.

Téngase en cuenta que la «Clasificación de norma» es un prerrequisito para que un producto reciba las etiquetas NATO Restricted o EU Restricted necesarias para manejar información clasificada.

ISO/IEC 27000, Tecnologías de la información - Técnicas de seguridad - Sistemas de gestión de la seguridad de la información

La serie ISO/IEC 27000 es una familia de normas de seguridad de la información que brinda un marco reconocido a escala mundial en materia de buenas prácticas de gestión de la seguridad de la información. Deliberadamente amplia en su alcance, la serie es aplicable a organizaciones de cualquier tamaño y sector.

El sistema de gestión de seguridad de la información (ISMS) ofrece un enfoque sistemático para mantener la seguridad de la infraestructura sensible. Dada la naturaleza dinámica del riesgo y la seguridad de la información, el concepto de ISMS incorpora feedback y mejoras constantes para responder a los cambios en las amenazas, vulnerabilidades e impactos de los incidentes.

Los productos de Stormshield están diseñados para mantener la seguridad de la infraestructura sensible. Un formato de registro estándar permite a las organizaciones centralizar toda la información, con vistas a identificar las tendencias y las posibles vulnerabilidades de seguridad. Una IGU tremendamente intuitiva permite a los usuarios implementar mejoras con facilidad.

> REGLAMENTOS ESPECÍFICOS DE CADA PAÍS

REINO UNIDO

Ley de Protección de datos de 2018

Similar al RGPD, la Ley de protección de datos es específica para el Reino Unido. Dispone, para cualquier dato personal, la obligación de contar con «un nivel adecuado de protección» en función de los riesgos si se produce una infracción de seguridad. Esto incluye un nivel de seguridad para evitar el tratamiento no autorizado o ilegítimo, la pérdida accidental, la destrucción o los daños en los datos. El sector de la defensa está exento en cierto modo de esta ley, en la medida en que los datos personales se utilizan con vistas a la protección y prevención de los ciudadanos.

Los productos de Stormshield ayudan a las organizaciones a cumplir estos requisitos incrementando la ciberresistencia de sus infraestructuras. Además, Stormshield Data Security ofrece funciones de cifrado de datos, que el RGPD menciona como una medida técnica apropiada para garantizar el nivel de seguridad adecuado al riesgo.

> REGLAMENTOS ESPECÍFICOS DE CADA PAÍS

FRANCIA

Ley de Programación Militar (LPM)

La Ley de Programación Militar (LPM) establece las orientaciones relativas a la política de defensa de Francia. Frente a la multiplicación de los ciberataques a manos de piratas informáticos, terroristas o incluso de Estados, asegurar la resistencia cibernética de los sistemas de información de los Operadores de Importancia Vital (OIV) supone un eje claramente definido en la LPM. Esta integra, por tanto, un componente de ciberseguridad y enumera a los OIV repartidos en doce sectores de actividad, entre los que se encuentra el sector de la defensa.

Dado que todos están cualificados por la ANSSI, esta confianza en los productos de Stormshield permite a los OIV desplegar estas soluciones de seguridad con el objetivo de aumentar el nivel de protección de los sistemas de información críticos. A modo de ejemplo, Stormshield Network Security garantiza la segmentación de las redes, la seguridad de los accesos remotos, la autenticación de los usuarios y la gestión de vulnerabilidades. Desplegado como complemento a un antivirus, Stormshield Endpoint Security (SES) brinda una protección en profundidad de los puestos de trabajo frente a ataques sofisticados. SES también puede mejorar la seguridad de los sistemas operativos obsoletos, detectar y gestionar los incidentes y garantizar la protección frente a los ataques de rebote.

Manual general de seguridad (RGS)

El Manual general de seguridad (Référentiel Général de Sécurité, RGS) se impone a los sistemas de información implantados por las autoridades administrativas en sus relaciones entre ellas y con los usuarios. Así pues, tienen la obligación de garantizar la seguridad de sus intercambios electrónicos. Este Manual propone una metodología, así como normas y buenas prácticas destinadas a las Administraciones.

La protección de los datos adquiere aquí una dimensión esencial. La solución Stormshield Data Security ofrece funcionalidades de cifrado de datos en respuesta a las exigencias de cualificación de los productos de seguridad y de los proveedores de servicios de confianza. Las demás gamas de productos Stormshield también contribuyen a que las Administraciones cumplan estas exigencias al tiempo que potencian la resistencia de su infraestructura.

Guías de buenas prácticas de la ANSSI

La Agencia Nacional de la Seguridad de los Sistemas de Información (ANSSI) es un auténtico organismo motriz en materia de ciberseguridad en Francia y elabora periódicamente guías de buenas prácticas. En este sentido, no se trata de reglamentos propiamente dichos, sino más bien de ayudas para la toma de decisiones en la selección de sus proveedores, sus soluciones de ciberseguridad e incluso en la puesta en marcha de estas últimas. De la criptografía a los puestos de trabajo, pasando por las redes, estamos ante una bibliografía abundante y apasionante.

> REGLAMENTOS ESPECÍFICOS DE CADA PAÍS

ALEMANIA

Normas de la Oficina federal para la Seguridad de la Información (BSI)

Las Normas BSI son un componente elemental de la metodología TI-Grundschutz. Las Normas BSI en vigor son:

- 200-1 (Requisitos generales para un sistema de gestión de seguridad de información)
- 200-2 (Base para el desarrollo de una gestión sólida de la seguridad de la información)
- 200-3 (Todos los pasos relativos a los riesgos en la implantación de protección básica de TI)

Ley de seguridad de TI (IT-Sicherheitsgesetz) & Ley BSI (BSI-Gesetz)

Los artículos 8a - 8d BSIG también son sumamente importantes para la seguridad de la infraestructura crítica de tecnología de la información y los proveedores de servicios digitales.

Los productos de Stormshield, certificados y fiables, permiten desplegar soluciones de seguridad que aumentan el nivel de protección de los sistemas de TI. Por ejemplo, Stormshield Network Security puede aislar áreas de la red, permitir un acceso remoto seguro, autenticar usuarios y gestionar vulnerabilidades. Stormshield Endpoint Security (SES), junto con un antivirus (en su caso), brinda una exhaustiva protección a estaciones de trabajo frente a amenazas sofisticadas. SES también puede mejorar la protección de los sistemas operativos heredados, detectar y gestionar incidentes, así como proteger frente a ataques de rebote. Stormshield Data Security ayuda a prevenir las fugas de datos mediante el cifrado de la información sensible.

Ley federal de protección de datos (BDSG)

El Artículo 22 (2) de la Ley BDSG aborda requisitos especiales de seguridad de datos que deben cumplirse cuando se tratan categorías especiales de datos personales. El Artículo 64 (3) de la Ley BDSG enumera las finalidades que deben garantizarse a través de medidas adecuadas para abordar la evaluación de riesgos de datos.

Entre estos requisitos resulta clave la «protección de datos por defecto», que establece la protección de los datos personales como una propiedad predeterminada en los sistemas y servicios. Los productos de Stormshield ayudan a las organizaciones a cumplir estos requisitos incrementando la ciberresistencia de sus infraestructuras. Además, Stormshield Data Security ofrece funciones de cifrado de datos que representan una medida técnica apropiada para garantizar el nivel de seguridad adecuado al riesgo.

> REGLAMENTOS ESPECÍFICOS DE CADA PAÍS

ITALIA

Calificaciones de seguridad (DPCM 22 luglio 2011)

Las Calificaciones de seguridad (denominadas AP y NOSI) permiten a las organizaciones formalizar un contrato con las Administraciones públicas para poder participar en los concursos de cara a la adjudicación de contratos clasificados como «reservados» o con una calificación más estricta, más concretamente en el caso de los concursos que impliquen el tratamiento de información calificada como Secreto/Alto secreto/Confidencial/Altamente confidencial. Dicha calificación implica, para las organizaciones, la implantación medidas específicas, desde lógicas hasta físicas y técnicas.

Ley 124/2007 (sistema de información para la seguridad de la República Italiana y nuevo protocolo de secretos), modificada por la Ley 133/2012

El DIS (Dipartimento delle Informazioni per la Sicurezza), la AISE (Agenzia Informazioni e Sicurezza Esterna) y la AISI (Agenzia Informazioni e Sicurezza Interna) pueden comunicarse con todas las administraciones de defensa y aquellos sujetos que prestan, en virtud de un régimen de autorización, concesión o convenio, servicios de utilidad pública y solicitar su colaboración para el cumplimiento de sus funciones institucionales. Con este fin, podrán formalizar concretamente acuerdos con los sujetos antedichos (véase el Art. 13 de la ley para obtener más información).

D.P.C.M. 6 de noviembre de 2015 (protocolo de firma electrónica para documentos secretos/confidenciales)

El protocolo es vinculante para todos los sujetos, públicos y privados, en posesión de las cualificaciones de seguridad necesarias para la gestión de información clasificada. Además, el protocolo especifica cómo generar, estampar y verificar firmas digitales, así como la validación temporal de documentos electrónicos clasificados.

> REGLAMENTOS ESPECÍFICOS DE CADA PAÍS

ITALIA

Directiva de 1 de agosto de 2015 (Marco Nacional para la ejecución de la ciberseguridad)

La Directiva pone en marcha objetivos establecidos en el Marco nacional para la ciberseguridad, potenciando así la coordinación entre los organismos de la Administración pública y la colaboración con todos los operadores no públicos que controlan infraestructuras telemáticas y de TI consideradas como funciones críticas a nivel nacional. La Directiva asigna a la Agenzia per l'Italia Digitale (AgID) la tarea de desarrollar normas para las administraciones.

Decreto Ley 18 maggio 2018, n. 65 [Implantación de la Directiva (UE) 2016/1148 - NIS]

La Ley establece medidas para la seguridad a nivel nacional, incluida la implantación de CSIRT, (también conocido como CIRT), funciones del s.c. «operadores críticos del mercado» y proveedores digitales sobre procedimientos de vulneración de la seguridad, la cooperación internacional en cuestiones de seguridad y la adopción de una estrategia nacional de ciberseguridad.

Los productos de Stormshield, certificados y fiables, permiten a los OES desplegar soluciones de seguridad que aumentan el nivel de protección de los sistemas de información esenciales (EIS). Por ejemplo, Stormshield Network Security puede aislar áreas de la red, permitir un acceso remoto seguro, autenticar usuarios y gestionar vulnerabilidades. Stormshield Endpoint Security (SES), junto con un antivirus (en su caso), brinda una exhaustiva protección a estaciones de trabajo frente a amenazas sofisticadas. SES también puede mejorar la protección de los sistemas operativos heredados, detectar y gestionar incidentes, así como proteger frente a ataques sofisticados.

D.P.C.M. 17 febbraio 2017 (Orientación sobre seguridad nacional de TI y ciberseguridad - Decreto Gentiloni)

La Directiva establece la organización institucional a cargo de la seguridad nacional de TI y ciberseguridad, determina las obligaciones y responsabilidades de cada entidad (CISR, CISR Tecnico, papel y directrices de DIS, Nucleo per la Sicurezza Cibernetica y sus obligaciones). La Directiva también establece medidas para «operadores críticos de mercado», así como para los proveedores de comunicación.

> REGLAMENTOS ESPECÍFICOS DE CADA PAÍS

ITALIA

D.P.C.M. 27 gennaio 2014 (Marco estratégico nacional para el espacio cibernético - QSN)

El Marco estratégico nacional para el espacio cibernético busca garantizar la eficiencia e interoperabilidad de los activos destinados a la defensa común, y respaldar la plena integración del dominio cibernético en el proceso de planificación de defensa de la OTAN y en la doctrina militar, con vistas a garantizar el despliegue de una capacidad robusta contra los ciberataques.

Stormshield Network Security ha recibido las certificaciones NATO Restricted y EU Restricted. Como tales, estos productos pueden implantarse en entornos sensibles para llevar a cabo una transmisión segura de la información clasificada. Esto contribuye a garantizar la interoperabilidad internacional con instituciones de la UE y la OTAN.

Plan trienal 2019-2021 para PA por la AgID

El Plan establece medidas regulatorias para las Administraciones públicas, incluida la implantación de la plataforma Infosec, un piloto para la transmisión automática de IoC cualificados, directrices nacionales para PA sobre ciberseguridad, obligación de implantar las pautas de la AgID sobre medidas de seguridad.

Medidas de seguridad mínimas de la AgID (que desarrollan el DPCM de 1 de agosto de 2015)

Esta Directiva pretende implementar las medidas de la AgID que contribuyen a hacer frente a las amenazas para la ciberseguridad y proporcionar las medidas de seguridad necesarias para el sector de la defensa, en términos de controles tanto técnicos como organizativos.

Los productos de Stormshield ayudan a las organizaciones a cumplir estos requisitos incrementando la ciberresistencia de sus infraestructuras. Entre estos diversos requisitos, Stormshield Network Vulnerabilty Manager, integrado al nivel de red en los productos de Stormshield Network Security, ayuda a gestionar la vulnerabilidad. Además Stormshield Endpoint Security incrementa el nivel de seguridad del antivirus tradicional mediante el bloqueo de amenazas avanzadas. Por último, Stormshield Data Security -producto que ha recibido la certificación EU Restricted- permite cumplir los requisitos de protección de datos.

> REGLAMENTOS ESPECÍFICOS DE CADA PAÍS

ESPAÑA

Código de la ley de ciberseguridad

Este Código pone a disposición de los abogados una herramienta donde poder encontrar las normas actualizadas que afectan directamente a la ciberseguridad, lo que facilita el estudio y análisis necesarios de un aspecto que se ha convertido en imprescindible para lograr un nivel adecuado de protección para las empresas, las instituciones y los ciudadanos en un estado social y democrático de derecho.

Los productos de Stormshield ayudan a las organizaciones a cumplir con este régimen incrementando la ciberresistencia de sus infraestructuras. Stormshield Network Security garantiza la protección perimetral con funcionalidades de Gestión unificada de amenazas. Además, Stormshield Endpoint Security incrementa el nivel de seguridad del antivirus tradicional mediante el bloqueo de amenazas avanzadas. Por último, Stormshield Data Security ofrece funciones de cifrado de datos que representan una medida técnica apropiada para garantizar el nivel de seguridad adecuado al riesgo.

Ley PIC (Protección de infraestructuras públicas)

La Ley de protección de infraestructuras críticas (Ley 8/2011 PIC) se complementa con el Real Decreto 704/2011. Los dos objetivos principales de esta norma son: catalogar el conjunto de infraestructuras que prestan servicios esenciales a nuestra sociedad y diseñar un plan que contenga medidas de prevención y protección efectiva frente a las posibles amenazas para dichas infraestructuras, en términos tanto de seguridad física como de seguridad de las tecnologías de la información y las comunicaciones.

Los productos de Stormshield, certificados y fiables, permiten a las infraestructuras críticas desplegar soluciones de seguridad que aumentan el nivel de protección de los sistemas de información esenciales. Por ejemplo, Stormshield Network Security puede aislar áreas de la red, permitir un acceso remoto seguro, autenticar usuarios y gestionar vulnerabilidades. Stormshield Endpoint Security (SES), junto con un antivirus (en su caso), brinda una exhaustiva protección a estaciones de trabajo frente a amenazas sofisticadas. SES también puede mejorar la protección de los sistemas operativos heredados, detectar y gestionar incidentes, así como proteger frente a ataques de rebote.

> REGLAMENTOS ESPECÍFICOS DE CADA PAÍS

ESPAÑA

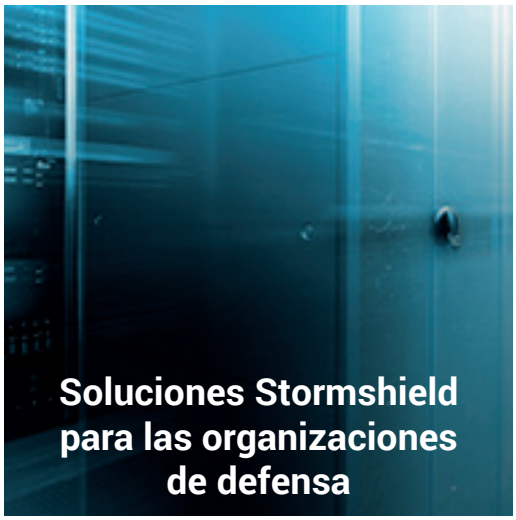
Esquema Nacional de Seguridad, Real Decreto 3/2010, de 8 de enero

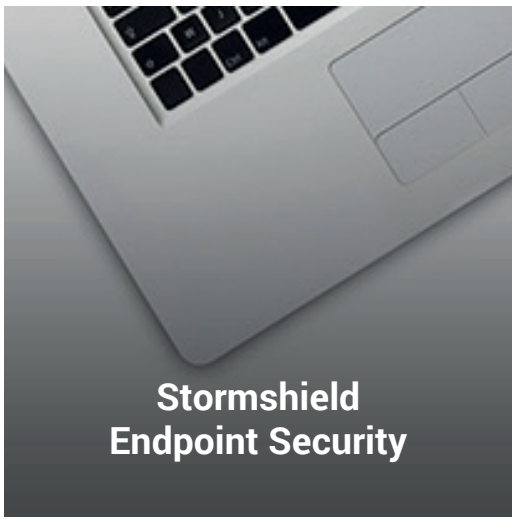
Este plan se aplica del mismo modo que en cualquier otra organización gubernamental. Los sistemas que gestionan la información clasificada deben, además, cumplir el requisito de los productos calificados por el Centro Criptológico Nacional español (CCN).

Los productos de Stormshield ayudan a las organizaciones a cumplir este plan mejorando la ciberresiliencia de su infraestructura. Stormshield Network Security proporciona una protección de última generación con capacidades de gestión de amenazas unifi cadas. Nuestra gama SNS es la única gama europea cuyos componentes se consideran «productos cualificados» y la única gama de cortafuegos con «productos aprobados» por el CCN. Por lo tanto, cumple el requisito de producto cualificado. Además, Stormshield Endpoint Security mejora la seguridad de los antivirus tradicionales bloqueando las amenazas sofisticadas. Por último, Stormshield Data Security proporciona capacidades de encriptación de datos, una medida técnica adecuada para garantizar el nivel de seguridad adecuado en función del riesgo.

> HAY UNA SOLUCIÓN STORMSHIELD PARA CADA PROBLEMA.

Productos y soluciones Stormshield para las organizaciones de defensa





> EL CUMPLIMIENTO NO BASTA

El amplio número de reglamentos y normas se ha tornado toda una preocupación para el conjunto de las organizaciones. Aunque esta guía proporciona una perspectiva acerca de qué reglamentos son de aplicación a cada sector, no basta con el cumplimiento. Es crucial recordar que todas y cada una de las organizaciones han de identificar y gestionar sus riesgos para garantizar su propia seguridad.