STORMSHIELD

CUMPLIMIENTO EN MATERIA DE CIBERSEGURIDAD PARA ORGANIZACIONES DE ENERGÍA

En el sector de la energía, donde la distribución es absolutamente vital, un ciberataque puede generar un efecto dominó en la economía, puesto que todo el planeta -desde los mercados de valores y los hospitales hasta las fábricas y las centrales nucleares- dependen de la energía. Un ciberataque puede tener un enorme efecto financiero en la organización afectada y en sus clientes. Aun así, la mayoría de los efectos generalizados se derivan de situaciones en las que todas las partes están conectadas a una única red. Un claro ejemplo de ello es el ataque Industroyer, que paralizó la red eléctrica de Ucrania en 2016. Un ciberataque también puede tener importantes efectos medioambientales, ya que todas las instalaciones energéticas (como las centrales de carbón, plataformas de perforación y exploración petrolíferas, plataformas marinas, etc.) conllevan un importante riesgo de daño medioambiental. Estos riesgos se multiplican en gran medida en el caso de la energía nuclear.

> 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 del sector de la energía 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.

Directiva de seguridad de las redes y de la información (NIS)

La Directiva NIS, la primera legislación a nivel comunitario sobre ciberseguridad, está concebida para aumentar el nivel general de seguridad cibernética en la UE, y debe ser incorporada a la legislación de cada uno de los Estados miembro. En virtud de la NIS, cada país debe designar Operadores de Servicios Esenciales (OES) en sectores como la energía, el transporte, el agua, la banca, la sanidad y la infraestructura digital. A continuación, los OES designados deberán cumplir con esta Directiva.

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 de rebote.

> **REGLAMENTOS EUROPEOS: CUMPLIMIENTO OBLIGATORIO**

Norma de seguridad de los datos en el sector de las tarjetas de pago (PCI-DSS)

La PCI-DSS es un conjunto de normas de seguridad de la información para las organizaciones que manejan tarjetas de crédito de marca emitidas por las principales empresas de tarjetas de crédito. Los vendedores, instituciones financieras u otras entidades que almacenen, traten o transmitan datos de titulares de tarjetas deben cumplir con estas normas, que incluyen disposiciones para la seguridad de la red, cifrado de datos, gestión de vulnerabilidades y un sólido control de acceso.

Los productos de Stormshield permiten a las organizaciones cumplir con muchos de los principales requisitos de la norma PCI-DSS. Por ejemplo, Stormshield Network Security (SNS) es capaz de aislar áreas de la red y cifrar el tráfico saliente, gestionar las vulnerabilidades y autenticar a los usuarios. Stormshield Data Security puede cifrar los datos de titulares de tarjetas para garantizar su integridad y confidencialidad. Stormshield Endpoint Security (SES), junto con un antivirus, refuerza la protección de las estaciones de trabajo frente a amenazas avanzadas. SES también puede mejorar la protección de los sistemas operativos heredados, detectar y gestionar incidentes, así como proteger frente a ataques de rebote.

Directiva sobre la reutilización de la información del sector público (PSI)

La Directiva PSI establece un marco legislativo común que fomenta que los Estados miembro de la UE faciliten la mayor cantidad de información del sector público posible para su reutilización. La PSI incluye toda la información que los organismos públicos producen, recopilan o adquieren. La Directiva PSI, transpuesta a la legislación de cada país, es la base de la Política de datos abiertos de la UE. Todas las organizaciones que gestionan información pública o generan datos a partir de proyectos de investigación financiados con fondos públicos deben brindar acceso público a estos datos, con sujeción a determinadas limitaciones.

Los productos de Stormshield pueden contribuir a que las organizaciones cumplan con la directiva PSI. En concreto, Stormshield Network Security (SNS) permite la microsegmentación de la red, de modo que se pueda aislar el área de almacenamiento de datos públicos. Y, con su intuitiva gestión de la política de seguridad, SNS facilita la identificación de las áreas de red, la gestión del acceso por parte del usuario o del grupo, y la determinación de restricciones temporales.

> **REGLAMENTOS EUROPEOS: CUMPLIMIENTO OBLIGATORIO**

IEC 62443

La norma ISA-99/IEC 62443, creada por la Sociedad internacional de la automatización, es la norma mundial para sistemas de control industrial (ICS) y está concebida con el objetivo de abordar el creciente volumen de amenazas cibernéticas. La norma permite a las organizaciones mejorar la seguridad digital y la seguridad de sus procesos y sistemas de control, como DCS, PLC, SCADA, etc. La norma se deriva de la serie ISO/IEC 27000 y ha sido totalmente adaptada para centrarse en los entornos de sistemas de control industriales.

Mejorar la ciberseguridad es una tarea a múltiples niveles y abarca gestión, políticas de seguridad y procedimientos organizativos. En este contexto, las soluciones altamente fiables de Stormshield, que cuentan con la certificación EU Restricted, pueden ayudar a las organizaciones a protegerse de las amenazas cibernéticas.

Por ejemplo, Stormshield Network Security (SNS) es capaz de aislar áreas de la red, controlar comandos PLC y garantizar un acceso seguro de mantenimiento remoto. Además, 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.

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 energéticas 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

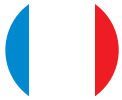
REINO UNIDO

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.

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 energía.

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.

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) y Ley BSI (BSI-Gesetz)

Según la Ley de seguridad de TI, los operadores de energía deben respetar un nivel mínimo de seguridad de TI e informar sobre perturbaciones importantes en este ámbito al BSI. Con respecto al nivel mínimo, el Artículo 8a de la Ley BSI fue promulgado por la Ley de seguridad de TI, que describe los requisitos para los operadores de las redes de suministro de energía o centrales de energía. Además, en 2016 se aprobó el BSI-Kritisverordnung para especificar qué sistemas críticos están sujetos a las disposiciones de la Ley de seguridad de TI. El Artículo 2 del BSI-Kritisverordnung dispone que el suministro de electricidad, gas, combustible y combustible para calefacción y calefacción urbana deben considerarse servicios críticos.

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 del sector energético (Ley EnWG)

El Artículo 11 (1a) de la EnWG especifica los requisitos para una red de suministro de energía segura en lo referente a los requisitos de TI. El Artículo 11 (1b), apartado 1, de la EnWG obliga, por tanto, a los operadores de los sistemas de energía que han sido designados como infraestructura crítica a proporcionar una protección adecuada frente a las amenazas a las telecomunicaciones y los sistemas de procesamiento electrónico de datos utilizados para el control de la red.

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.

> REGLAMENTOS ESPECÍFICOS DE CADA PAÍS

ALEMANIA

Ley de la energía atómica (AtG)

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.

Catálogos de seguridad de la Agencia de red federal

La Agencia de red federal tiene la misión, previa consulta a la Oficina federal para la seguridad de la información (BSI), de redactar y publicar las normas mínimas de seguridad de TI en el sector energético. Estas normas mínimas de seguridad de TI se han publicado para el sector energético en los denominados «Catálogos de seguridad de TI».

> 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 la certificación 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.

> REGLAMENTOS ESPECÍFICOS DE CADA PAÍS

ESPAÑA

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.

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

Este plan se aplica a cualquier empresa de servicios de energía y agua, así como a cualquier empresa privada que preste servicios a estas empresas.

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. 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 Centro Criptológico Nacional español (CCN). 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.

> HAY UNA SOLUCIÓN STORMSHIELD PARA CADA PROBLEMA.

Productos y soluciones Stormshield para las organizaciones del sector energético

> 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.