STORMSHIELD

CUMPLIMIENTO EN MATERIA DE CIBERSEGURIDAD PARA ORGANIZACIONES SANITARIAS

En el campo de la salud, donde es vital la disponibilidad del servicio, un ciberataque puede ser, literalmente, una cuestión de vida o muerte. Además, los proveedores de asistencia sanitaria están legalmente obligados a proteger los datos de los pacientes. Esto es así en un momento en que los sistemas sanitarios dependen cada vez más de los datos móviles, que deben permanecer protegidos frente a intrusiones.

> 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 sanitarias 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.

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 sanitarias 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.

Lista de recomendaciones de la ENISA

La Agencia Europea de Seguridad de las Redes y de la Información (ENISA) ha publicado una lista de recomendaciones en el ámbito de la ciberseguridad para los mercados públicos hospitalarios, ya sean de servicios, productos o infraestructuras. Un documento para los responsables de informática de los centros hospitalarios.

Los productos Stormshield están calificados y certificados al más alto nivel europeo, una garantía de confianza y solidez. Permiten a los Operadores de Servicios Esenciales (OSE) implantar soluciones de seguridad que mejoran el nivel de protección de los Sistemas de Información Esenciales (SIE). Por ejemplo, Stormshield Network Security garantiza la segmentación de redes, la seguridad del acceso a distancia, la autenticación de usuarios y la gestión de vulnerabilidades. Al implantar una solución calificada y certificada al más alto nivel europeo, se beneficia de un producto cuya solidez ha quedado demostrada durante el proceso de certificación.

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

> CUMPLIMIENTO OPCIONAL

Las organizaciones sanitarias 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.

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

Código de la salud pública - Artículo sobre alojadores de datos de salud

El Artículo L1111-8 del Código de la salud pública define las condiciones de actividad de los alojadores de datos personales de salud. De este modo, el alojador y su servicio de archivo deben garantizar la seguridad eficiente de los datos de salud que les sean confiados.

Las soluciones Stormshield le acompañan en el cumplimiento normativo de su empresa gracias a un conjunto completo de funcionalidades, como la seguridad de sus datos con garantía de cumplimiento, incluso en caso de almacenamiento de datos confidenciales en la nube, e independientemente de su localización, con la solución Stormshield Data Security.

Instrucción interministerial nº 901/SGDSN

La Instrucción interministerial n.° 901, relativa a la protección de los sistemas de información sensibles, se aplica especialmente a las entidades públicas o privadas sujetas a la normativa sobre la protección del potencial científico y técnico de la nación (PPST) que ponen en práctica los sistemas de información sensible.
Los datos tratados en estos sistemas de información sensibles, como por ejemplo las patentes, que deben estar consignados en zonas con regímenes restrictivos, deberán ostentar también la indicación de «Difusión restringida».

Para impedir comprometer la información sensible y proteger la imagen de la entidad, la solución Stormshield Data Security ofrece un cifrado de datos de extremo a extremo. Su implantación criptográfica certificada EAL3+, cualificada por la ANSSI y la OTAN, está adaptada a la protección de datos de tipo «Difusión restringida».

Orden francesa n.°2020-1407 de 18 de noviembre de 2020 sobre las misiones de las agencias regionales de salud

El artículo 1 de esta orden establece la obligación de comunicar los incidentes informáticos a las autoridades competentes del Estado y a la Agencia Nacional de Salud Pública francesa en el caso de todas las estructuras sanitarias y médico-sociales.

Los registros de eventos proporcionados por las soluciones Stormshield, tales como los eventos de seguridad, forman parte de la información esencial que debe transmitirse a las autoridades competentes en caso de incidente. La evolución de la solución Stormshield Endpoint Security aborda este problema, en particular cuando el ataque es sofisticado y trata de eludir los medios de protección. Además de bloquear proactivamente los comportamientos de ataque más sofisticados, Stormshield Endpoint Security Evolution brinda los elementos de contextualización necesarios para investigar en profundidad los incidentes de seguridad.

> REGLAMENTOS ESPECÍFICOS DE CADA PAÍS

FRANCIA

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.

En «Seguridad digital para las entidades territoriales: lo esencial de la normativa», encontrará una guía complementaria a nuestro libro electrónico. Un documento sintético, práctico y sencillo para los cargos públicos y los gestores territoriales responsables de garantizar su aplicación y cumplimiento.

> 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 sanitarios 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 el nivel mínimo en términos abstractos. Además, en 2016 se aprobó el BSI-Kritisverordnung para especificar qué sistemas críticos están cubiertos por las disposiciones de la Ley de seguridad de TI. Esta ordenanza también abarca al sector de la salud.

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)

Si se trata de datos sobre salud, deben adoptarse medidas apropiadas y específicas para proteger a los interesados de conformidad con el Artículo 22 (2) de la ley BDSG.
Este artículo especifica las medidas técnicas y organizativas que deben tomarse en el tratamiento de datos sanitarios.

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

ALEMANIA

Ley de e-Salud y tomo quinto del Código social

La Ley de e-Salud se refiere a la comunicación electrónica y sus aplicaciones en el sector sanitario. Contiene una hoja de ruta concreta para el establecimiento de una infraestructura telemática segura y la introducción de aplicaciones médicas. La Ley de e-Salud es una norma que modifica el tomo quinto del Código social.

Los productos de Stormshield ayudan a las organizaciones a cumplir con esta directiva 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 contribuye al cumplimiento de los requisitos de protección de datos.

> REGLAMENTOS ESPECÍFICOS DE CADA PAÍS

ITALIA

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. 178 del año 2015 (e-Expediente sanitario - Fascicolo Sanitario Elettronico - FSE)

El e-Expediente sanitario es un registro de información sociosanitaria y de salud relativo al historial clínico de los pacientes, cuyo principal objetivo es facilitar la asistencia del paciente, potenciando las sinergias en las actividades de asistencia y cuidados sanitarios. El cumplimiento de la ley (también en términos de seguridad) se basa en el RGPD y la disposición Garante del FSE.

Los productos de Stormshield ayudan a las organizaciones sanitarias 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

ESPAÑA

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

Si un hospital es considerado una entidad de derecho público (vinculada a o dependiente de la Administración General del Estado, Comunidades Autónomas o entidades locales), se aplicará en su totalidad el siguiente régimen en aquellas actividades que no se lleven a cabo en virtud del derecho privado.

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 sanitario

> 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.

Créditos de la foto: ShutterStock©, aressy.com