Conozca las leyes y marcos normativos más importantes en ciberseguridad

Boletín N°:

Nov 26, 2024 MUNDO

En una era de crecientes amenazas digitales, cumplir con las normativas y leyes de ciberseguridad es un escudo vital para proteger los activos, la reputación y a fin de cuentas, la propia supervivencia de la empresa.

Como las ciberamenazas no muestran signos de desacelerarse, tanto las pequeñas como las grandes organizaciones reconocen cada vez más que la ciberseguridad ya no es opcional.

Los gobiernos y las agencias reguladoras destacan su importancia, especialmente cuando se trata de organizaciones que operan en sectores críticos para la infraestructura nacional de un país. Esto da como resultado un conjunto cada vez mayor de requisitos de cumplimiento.

Para empezar, se distinguen dos tipos de cumplimiento: obligatorio y voluntario, cada uno conlleva su propio conjunto de requisitos. El cumplimiento obligatorio abarca las normativas aplicadas por organismos estatales o adyacentes y dirigidas a empresas que operan en sectores de infraestructuras críticas, como la sanidad, el transporte y la energía.

Por otro lado, el cumplimiento voluntario significa que las empresas solicitan certificaciones y normas específicas que las identifican como expertas en un campo concreto o califican algunos de sus productos como conformes a una norma. Por ejemplo, una empresa que busque credibilidad medioambiental puede solicitar la certificación ISO 14001, que demuestra su compromiso con las prácticas respetuosas con el medio ambiente.

“La normativa específica en materia de ciberseguridad que debe cumplir una organización depende del tipo de sector en el que opere la empresa y de la importancia que tenga la seguridad de sus datos internos para la privacidad, la seguridad de los datos o los actos sobre infraestructuras críticas”, comenta Fabiana Ramírez Cuenca, investigadora de Seguridad Informática de ESET Latinoamérica.

ESET comparte un repaso de las leyes y marcos normativos más importantes en materia de ciberseguridad:

- Reglamento General de Protección de Datos (RGPD): El GDPR es una de las normativas sobre privacidad y seguridad de datos más estrictas a nivel

mundial. Se centra en los derechos de privacidad y protección de datos de las personas en la Unión Europea, dándoles el control sobre sus datos y ordenando el almacenamiento seguro y la notificación de infracciones para las empresas que gestionan los datos.

- Ley de Portabilidad y Responsabilidad de los Seguros Sanitarios (HIPAA): Esta ley regula el tratamiento de la información de los pacientes en hospitales y otros centros sanitarios. Representa un conjunto de normas diseñadas para proteger los datos sanitarios confidenciales de los pacientes frente a usos indebidos, exigiendo a las entidades administrativas que promulguen diversas salvaguardias para proteger dichos datos, tanto física como electrónicamente.
- Marcos del Instituto Nacional de Normas y Tecnología (NIST): Agencia gubernamental estadounidense dependiente del Departamento de Comercio, elabora normas y directrices para diversos sectores, entre ellos el de la ciberseguridad. Al imponer un determinado conjunto de políticas que sirven de base a la seguridad de las organizaciones, permite a las empresas e industrias gestionar mejor su ciberseguridad. Por ejemplo, el Marco de Ciberseguridad 2.0 del NIST contiene orientaciones exhaustivas para organizaciones de todos los tamaños y postura de seguridad actual sobre cómo pueden gestionar y reducir sus riesgos de ciberseguridad.
- Norma de seguridad de datos del sector de las tarjetas de pago (PCI DSS): PCI DSS, diseñada para controlar el manejo de datos de tarjetas de crédito. Su objetivo es reducir los riesgos de fraude en los pagos reforzando la seguridad en torno a los datos de los titulares de tarjetas. Se aplica a todas las entidades que manejan datos de tarjetas, ya sea una tienda, un banco o un proveedor de servicios.
- Directiva sobre seguridad de las redes y de la información (NIS2): Esta directiva refuerza la ciberresiliencia de las entidades críticas de la Unión Europea al imponer requisitos de seguridad y prácticas de gestión de riesgos más estrictos a las entidades que operan en sectores como la energía, el transporte, la sanidad, los servicios digitales y los servicios de seguridad gestionados. NIS2 también introduce nuevas normas de notificación de incidentes y multas por incumplimiento.

Ante un incumplimiento algunas normativas establecen sanciones cuantiosas. Por ejemplo, las infracciones del GDPR pueden dar lugar a multas de hasta 10 millones de euros, o el 2% de la facturación anual global, para cualquier empresa que no notifique una infracción a una autoridad supervisora o a los interesados. Las autoridades supervisoras también pueden imponer multas adicionales por medidas de seguridad inadecuadas, con los consiguientes costes adicionales.

Source

Source: Revista EyN

Link:
https://www.revistaeyn.com/tecnologia-cultura-digital/conozca-las-leyes-y-marcos-normativos-mas-importantes-en-ciberseguridad-CC22758039