Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Vicepresidencia Primera del Gobierno · Ministerio de Asuntos Económicos y Transformación Digital · Secretaría de Estado de Digitalización e Inteligencia Artificial
Plan de Recuperación, Transformación y Resiliencia
España | digital 2026
incibe_ Instituto Nacional de Ciberseguridad

Flavia Luxemburgo Poy Barrio
presenta el resumen del trabajo

Analysis of Cybersecurity Standard and Framework Components

Melwin Syafrizal, Siti Rahayu Selamat, Nurul Azma Zakaria

Revista Internacional de Redes de Comunicación y Seguridad de la Información (IJCNIS), 12 (3), (2022).

22 de mayo de 2024

SERIE DE RESÚMENES EN ESPAÑOL

Palabras clave: estándares, mejores prácticas, ciberseguridad, dominio, marco, directrices, normas.

Introducción

El artículo aborda la importancia de adoptar estándares y marcos de ciberseguridad para proteger, fundamentalmente, activos digitales críticos, y detalla la diferencia entre ambos conceptos y su incidencia regulatoria internacionalmente. Los autores destacan las dificultades que enfrentan las organizaciones en la implementación de estos estándares, marcos, directrices o guías de buenas prácticas debido a la falta de personal experimentado y la complejidad de elegir el enfoque adecuado que cumpla con las leyes y regulaciones vigentes, al mismo tiempo que se adaptan a las diferentes líneas de negocio de una misma institución o empresa.

1. Metodología

Para abordar las dificultades mencionadas, los autores realizaron una revisión exhaustiva de la literatura sobre los diferentes tipos de estándares y marcos de ciberseguridad. La metodología incluye la identificación y análisis de los elementos presentes en cada estándar y marco, con el objetivo de facilitar a las organizaciones y gobiernos la elección del estándar más adecuado. El estudio se basó en la recopilación de datos de fuentes secundarias y el uso de un enfoque de análisis comparativo para identificar las relaciones y diferencias entre los distintos estándares y los componentes de los marcos de ciberseguridad que se adaptarán a las necesidades de cada organización o empresa para el gobierno.

2. Resultados

El análisis reveló una serie de componentes clave que son comunes a los principales estándares y marcos de ciberseguridad. Entre estos se encuentran las mejores prácticas para la protección de datos, la gestión de riesgos, y la respuesta a incidentes. Además, se identificaron ocho pasos esenciales para la implementación efectiva de un marco de ciberseguridad, que incluyen la evaluación de riesgos, el establecimiento de políticas de seguridad, y la capacitación continua del personal. Estos resultados proporcionan una guía estructurada para que las organizaciones puedan mejorar su postura de ciberseguridad de manera efectiva.

Así, la investigación parte de la definición de estándar como una condición ideal como logro mínimo, a veces también definido como el más alto logro [1]. Las normas también significan especificaciones técnicas. Los hallazgos muestran alrededor de 250 tipos de marcos y estándares de ciberseguridad que se utilizan a nivel mundial en todo el mundo.

La diferenciación entre los estándares y los marcos de ciberseguridad es crucial. Los estándares de desempeño pueden ser una política o ley que deben cumplir ciertos países u organizaciones de un país, como FISMA, HIPAA y GDPR. Se pueden utilizar varios estándares junto con otros estándares para complementar y fortalecer otros requisitos, como los de ISO, BSI y NIST con sus publicaciones especiales de la serie 800. Así mismo, tienen dos elementos sustancialmente diferenciadores respecto de los marcos: un país tiene la autoridad para emitir sus normas, o rechazar reglas o estándares publicados por otros países; y se trata de una norma que especifica lo que se debe hacer para cumplir con la norma; explicando y proporcionando métodos uno por uno para completar el proceso. Mientras, un marco es una guía general que normalmente sólo proporciona una descripción general como base para construir algo o lograr un objetivo grande y útil.

De este modo, se observa que los estándares de ciberseguridad pueden tener un alcance amplio y profun-

do, que van desde algoritmos criptográficos hasta la integridad de características de seguridad en aplicaciones, como navegadores web y Gestión Independiente de Seguridad de la Información, con el objetivo de satisfacer las necesidades del usuario, práctico, de bajo costo, teniendo en cuenta las limitaciones de la tecnología y los recursos para cumplir con el estándar. Por el contrario, el Marco de Ciberseguridad es un conjunto de directrices que las empresas deben seguir para estar mejor equipadas para identificar, detectar y responder a los ciberataques. Se destaca como caso ejemplar el Marco de Seguridad Cibernética del NIST por su aportación a las organizaciones a aumentar sus medidas de ciberseguridad, desarrollado en 2014 por orden ejecutiva del presidente de los Estados Unidos, Barack Obama.

El marco central tiene varias funciones: identificar, proteger, detectar, responder y recuperar. Este modelo más conocido como PDCA (Plan, DO, Check, Act) es considerado abolido por el presente artículo con la formulación de la ISO 9001:2013.

Se demuestra así también que, además de la consolidación del Estándar y marco internacional general de NIST, los marcos (frameworks) con mayor estudio y aplicación internacional son ISO/IEC 27001:2013, COBIT 5, COSO y ETSI TC CYBER. Por otro lado, los estándares de ciberseguridad por su especificidad de la industria, destacan los casos de NIST SP 800 (series), ISO/IEC 27032:2012 y PCI DSS.

Las guías y las buenas prácticas también tienen una gran relevancia en el estudio. Las Best Practices o Mejores Prácticas son un ejemplo de cómo trabajar mejor basándose en situaciones y condiciones existentes, y otras organizaciones lo han implementado con éxito en su organización. Las mejores prácticas de ciberseguridad, a menudo se refieren a políticas, procedimientos, estrategias u otras actividades relacionadas con la seguridad cibernética. En general, el público ha aceptado esta norma o actividad como la mejor solución o la más rentable y, así, se demuestra que la mayoría de los elementos de un marco de ciberseguridad son las mejores prácticas.

Por su parte, las guías, como conjuntos de documentos o instrucciones, ayudan a hacer un plan, dirigir una acción o una guía para construir una idea. Esto las diferencia al mismo tiempo de las directrices, que el estudio sugiere su conceptualización en torno a actividades que permitan a los usuarios realizar más libremente traducciones, aplicaciones o uso sin estar sujetas a las recomendaciones de normas y prácticas dictadas por las diferentes autoridades. Por ejemplo, para ISO, estas directrices suelen constituir las primeras versiones de los documentos antes del nacimiento de un estándar, cuyo periodo de emisión de instrucciones para el estado formal como estándar es de 5 años.

3. Discusión y Conclusiones

La idea clave es que la estrategia de ciberseguridad no se puede implementar de manera efectiva sin el marco de ciberseguridad adecuado, en tanto que consiste y se entiende también en términos de seguridad, estándares, implementaciones y mejores prácticas para la gestión de la seguridad cibernética.

La discusión del artículo subraya la importancia de personalizar los estándares y marcos de ciberseguridad según las necesidades específicas de cada organización. Los autores argumentan que, aunque existen muchas similitudes entre los diferentes marcos, la selección del más adecuado depende del contexto específico y los requisitos legales de la organización. Concluyen que una comprensión profunda de los componentes y la implementación de un enfoque flexible y adaptativo son cruciales para la protección efectiva contra amenazas cibernéticas. En concordancia, los componentes comunes que más comparten tanto los estándares como los marcos de ciberseguridad tienen en cuenta las variables de Control de acceso, Concientización y Capacitación (Personal), Gestión de incidentes (planificación de respuesta a incidentes), Evaluación de riesgos y Gobernanza.

Se plantean así dos últimas consideraciones al respecto de la temática. Por un lado, es importante que el cumplimiento de estándares tenga en cuenta una necesidad de negocio específica, esto es, no implementándose en todas las partes o departamentos de una empresa o institución. Se identifica claramente que estándares de la industria como HIPAA, PCI-DSS e ISA/IEC 62443 son muy específicos, con muchos elementos estándar que no son similares a los elementos de un estándar en general. Por otro lado, se identifican las líneas de investigaciones pendientes, que especialmente son ausentes en temas de tendencia actual, como la seguridad de IoT, marcos de ciberseguridad basados en blockchain, criptografía cuántica segura, la protección hardware - software (directrices o mejores prácticas) o la agilidad criptográfica.

4. Valoración del documento original

El documento aporta una contribución significativa al campo de la ciberseguridad al proporcionar un análisis detallado y comparativo de diversos estándares y marcos, con una conceptualización muy precisa entre sí y al respecto de buenas prácticas y guías, cuya segmentación es valiosa cuando se habla de regulación. La presentación de un mapa relacional y una metodología estructurada facilita a las organizaciones la comprensión y aplicación de estos marcos. La originalidad del trabajo radica en su enfoque holístico y práctico, que no solo identifica las mejores prácticas sino también proporciona una guía clara para su entendimiento, algo que es particularmente valioso para

organizaciones con recursos limitados en términos de experiencia en ciberseguridad. La identificación precisa sobre las líneas de investigación que requieren profundidad a nivel internacional también arroja luz sobre el estado de la cuestión.

Referencias

· [1] C. E. Dictionary. , *"Collins Dictionary online"*, , Collins. (2020).