



IMPORTANCIA DE LA ADOPCIÓN DEL NIST CYBERSECURITY FRAMEWORK EN LAS ORGANIZACIONES

ARTÍCULO CIENTÍFICO

RECIBIDO: 15/07/2019 ACEPTADO: 15/09/2019 ÚLTIMA VERSIÓN: 15/02/2020

IMPORTANCE OF THE ADOPTION OF THE NIST CYBERSECURITY FRAMEWORK IN ORGANIZATIONS

¹ Luis Eduardo Baquero Rey

² Miguel Hernández Bejarano

³ Gabriel Antonio Rojas Díaz

Como citar este artículo: Baquero et al., (2020) Importancia de la adopción del nist cybersecurity framework en las organizaciones, revista científica Dynamikos 1 (1). Recuperado de: <https://teinco.edu.co/revistas-2-2/>

ABSTRACT

In the context of the research project entitled "Cyber resilience model for online applications" whose main objective is based on the design and implementation of a resilience or recovery model against security problems that may arise in the online transactions of an organization, and from the computer security research hotbed, by advancing what corresponds to the preliminary investigation and attending to the activities programmed for the proper development of the project, we identified the need for organizations in cybersecurity to have and maintain a common framework related to information security. In this sense, we set out to study the NIST Cybersecurity Framework and determine the importance of its adoption in an organization.

KEYWORDS: Cybersecurity, framework, NIST, organization.

¹ [https://scienti.minciencias.gov.co/cvlac/visualizador/generarCurriculoCv.do?cod_rh=0000550892] Profesor del Departamento de Ingeniería de Sistemas de la Fundación Universitaria Los Libertadores, Colombia – lebaqueror@libertadores.edu.co

² [https://scienti.minciencias.gov.co/cvlac/visualizador/generarCurriculoCv.do?cod_rh=0001158414] Profesor del Departamento de Ingeniería de Sistemas de la Fundación Universitaria Los Libertadores, Colombia – mhernandezb@libertadores.edu.co

³ Gabriel Antonio Rojas Díaz [CV] Estudiante del Departamento de Ingeniería de Sistemas de la Fundación Universitaria Los Libertadores, Colombia – garojasd@libertadores.edu.co

1. INTRODUCCIÓN

El marco para mejorar la ciberseguridad de la infraestructura crítica fue emitido el 12 de febrero de 2014, según lo dispuesto por el presidente de los Estados Unidos en Orden Ejecutiva 13636. Se refiere a un marco voluntario, basado en estándares existentes, directrices y prácticas que proporciona una guía para reducir riesgos dentro de las infraestructuras críticas de las organizaciones; este marco de ciberseguridad (CSF, por sus siglas en inglés) fue desarrollado por el Instituto Nacional de Estándares y Tecnología (NIST). Provee un conjunto detallado de controles de seguridad que se centran en desarrollar perfiles individuales para los operadores. Los controles de seguridad de CSF se distribuyen en cinco dominios: Identificar; Proteger; Detectar; Responder; Recuperar.

La seguridad de la información, por fortuna, es un tema que día a día preocupa más a las organizaciones, esto cubre el aseguramiento de su infraestructura crítica buscando garantizar la continuidad del negocio y desde años atrás vienen haciendo esfuerzos ingentes en ello, cuyo resultado ha sido la suma de esfuerzos y experiencias significativas, muchas de ellas aisladas, sin ningún marco de trabajo común que les pueda ahorrar tiempos y dinero, y que a la vez se puedan sentir mejor protegidos frente al sinnúmero de amenazas cibernéticas existentes tanto internas como externas. Pensando en esta situación, se estudia y se resalta la importancia de su adopción del NIST Cybersecurity Framework en las organizaciones.

2. LAS CIBERAMENAZAS

Los ciberdelincuentes se están volviendo cada vez más sofisticados y son capaces de explotar la vulnerabilidad de día cero y la amenaza persistente avanzada (APT) (Zhao et al., 2020), los ciberdelincuentes y los ciberterroristas tienen un amplio arsenal de armas para utilizar en sus actividades, siendo esto un problema de seguridad siempre han sido el foco principal, sin importar en el sector académico o industrial, agentes difieren considerablemente en términos del nivel de participación requerido por el perpetrador, la sofisticación de la herramienta, los mecanismos de protección y muchos otros factores. Sin embargo, lograr la ciberseguridad requiere que las personas, las empresas y las agencias gubernamentales se aseguren de que están preparados y son capaces de defender sus propios datos y redes de todas y cada una de las formas, dado que incluso las soluciones tecnológicas más avanzadas pueden ser eludidas por un pirata informático que pueda engañar a un empleado para que dé su información de inicio de sesión.

Los métodos más comunes se enumeran y describen brevemente aquí incluyen (Bullock, Haddow, & Coppola, 2018):

- Sitio web malicioso: funciona explotando la forma en que funcionan los navegadores web, de modo que se descarga software dañino en la computadora del usuario.
- Virus: programas que funcionan sin ser vistos ni detectados en una computadora u otro hardware para influir en la forma en que funciona el sistema operativo del dispositivo.
- Caballo de Troya: un programa que, como un virus, existe para influir en la forma en que opera un componente de hardware o un programa de software, pero que se disfraza para aparecer como un programa útil que el usuario afectado instala a sabiendas en su sistema o dispositivo.

- Gusano: un tipo de virus que puede replicarse en un sistema infectado sin ninguna acción humana.
- Spyware: programas que se instalan en un sistema o dispositivo sin el conocimiento del usuario con el fin de recopilar información y transmitirla al origen del ataque.
- Registrador de pulsaciones de teclas (keylogger): programas o dispositivos físicos que registran cada tecla pulsada por el usuario en una sucesión ordenada.
- Malware: un nombre general para cualquier programa que busque comprometer, interrumpir o robar un dispositivo o sistema (también conocido como código malicioso o software malicioso).
- Ataque de denegación de servicio (DOS) / denegación de servicio distribuido (DDOS): impide el acceso o el uso de un sitio web o sistema de gestión de información.
- Bot: una computadora que ha sido tomada de forma remota por un atacante, casi exclusivamente a través de su conexión a Internet, con fines nefastos (generalmente para ataques DDOS).
- Hack: un acceso exitoso a un sistema informático o de información utilizando medios nefastos.
- Phishing: un método que utilizan los piratas informáticos para obtener la información de identificación y contraseña de un objetivo involuntario que generalmente implica el uso de ingeniería social.
- Spoofing: un método que se usa a menudo en esquemas de phishing en el que un pirata informático puede disfrazar su propia dirección de correo electrónico para que parezca una en la que su objetivo podría confiar.
- Envenenamiento de DNS (o suplantación de DNS): una forma de piratería en la que el pirata informático puede desviar el tráfico de un sitio web legítimo al suyo, dándoles así acceso a todos los datos que los usuarios normalmente proporcionarían al propietario legítimo del sitio web.
- Exploit: un error o una vulnerabilidad desconocida en el software o sistema que permite que un hacker acceda.
- Clickjacking: un método de piratería en el que el pirata informático engaña a un objetivo para que haga clic en algo que parece legítimo, pero de hecho lo dirige a otro sitio web o intenta instalar software malicioso en su computadora.
- Cookies: pequeños paquetes de información que un sitio web almacena en la computadora de un usuario para rastrear, almacenar y luego devolver información al sitio web con el fin de comprender la actividad previa (utilizada tanto para sitios web legítimos como para piratas informáticos).
- Inyección de SQL: un método de piratería en el que el pirata informático ingresa código en una interfaz de base de datos, u otro programa basado en datos, para ordenar al programa que les envíe parte o toda la información que el sistema está almacenando.
- Skim: una acción en la que se recopilan datos personales de una tarjeta de crédito durante una transacción en persona sin el conocimiento del propietario.

• Ingeniería social: métodos que utilizan medios psicológicos o no técnicos para engañar a las víctimas para que entreguen voluntaria o involuntariamente su información personal, incluida la información de inicio de sesión y las contraseñas.

• Ransomware, rescate y chantajes cibernéticos: herramientas y acciones en las que un ciberdelincuente altera o corrompe los datos en un sistema objetivo y luego instruye a una persona a cargo del material objetivo para que proporcione un pago de rescate a cambio de la reparación de los datos.

3. COMPROMISO PÚBLICO DESDE LA CASA BLANCA

El ciberespacio toca prácticamente todo y a todos. Proporciona una plataforma para la innovación y la prosperidad y los medios para mejorar el bienestar general en todo el mundo. Pero con el amplio alcance de una infraestructura digital flexible y ligeramente regulada, los grandes riesgos amenazan a las naciones, las empresas privadas y los derechos individuales.

El gobierno tiene la responsabilidad de abordar estas vulnerabilidades estratégicas para garantizar que los Estados Unidos y sus ciudadanos, junto con la comunidad más amplia de naciones, puedan realizar todo el potencial de la revolución de la tecnología de la información; en tal sentido la arquitectura de la infraestructura digital de la nación, basada en gran medida en Internet, no es segura ni resistente. Sin grandes avances en la seguridad de estos sistemas o un cambio significativo en la forma en que se construyen u operan, es dudoso que Estados Unidos pueda protegerse de la creciente amenaza del ciberdelito y las intrusiones y operaciones patrocinadas por el estado.

La infraestructura digital ya ha sufrido intrusiones que han permitido a los delincuentes robar cientos de millones de dólares, y a los estados-nación y otras entidades robar propiedad intelectual e información militar sensible (House, 2020). Otras intrusiones amenazan con dañar partes de nuestra infraestructura crítica. Estos y otros riesgos tienen el potencial de socavar la confianza de la Nación en los sistemas de información que subyacen a nuestros intereses económicos y de seguridad nacional; señalan desde la sede de gobierno federal.

4. EL MARCO DE CIBERSEGURIDAD CSF

El NIST Cybersecurity Framework es un marco de trabajo con enfoque basado en el riesgo que ayuda a quienes enfrentan amenazas de ciberseguridad a observar sistemáticamente qué son (personas, información, instalaciones, etc.), qué los amenaza (y cuáles podrían ser las posibles consecuencias de esas amenazas), qué se puede hacer para abordar esas amenazas y responder a ellas, y qué se puede hacer para garantizar una recuperación rápida.

Hay tres partes principales del marco, que incluyen:

El Marco Básico o Framework Core, descrito como un conjunto de actividades de ciberseguridad y referencias informativas que son comunes en los sectores de infraestructura crítica. Las actividades de ciberseguridad están agrupadas en cinco funciones, cada una de las cuales proporciona una visión de alto nivel de la gestión de los riesgos cibernéticos de una organización. Estos incluyen (Bullock, Haddow, & Coppola, 2018) (NIST, 2020):

Identificar: desarrolle la comprensión organizacional para administrar el riesgo de ciberseguridad de los sistemas, activos, datos y capacidades. Comprender el contexto empresarial, los recursos que respaldan las funciones críticas y los riesgos de ciberseguridad relacionados permite a una organización enfocar y priorizar sus esfuerzos, de acuerdo con su estrategia de gestión de riesgos y sus necesidades comerciales.

• Proteger: desarrolle e implemente las salvaguardas apropiadas para asegurar la entrega de servicios de infraestructura crítica. La función Proteger admite la capacidad de limitar o contener el impacto de un posible evento de ciberseguridad.

• Detectar: desarrolle e implemente las actividades apropiadas para identificar la ocurrencia de un evento de ciberseguridad. La función Detectar permite el descubrimiento oportuno de eventos de ciberseguridad.

• Responder: desarrollar e implementar las actividades adecuadas para tomar medidas con respecto a un evento de ciberseguridad detectado. La función Responder admite la capacidad de contener el impacto de un posible evento de ciberseguridad.

• Recuperar: desarrolle e implemente las actividades apropiadas para mantener los planes de resiliencia y restaurar cualquier capacidad o servicio que se haya visto afectado debido a un evento de ciberseguridad. La función de recuperación admite la recuperación oportuna de las operaciones normales para reducir el impacto de un evento de ciberseguridad.

Tabla 1. Framework NIST

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Fuente: <https://bit.ly/2GiIO8g> 2020

Los perfiles, que ayudan a las organizaciones a alinear sus actividades de ciberseguridad con los requisitos comerciales, las tolerancias de riesgo y los recursos. El análisis de las diferencias entre los perfiles puede identificar brechas que se deben gestionar para lograr los objetivos de gestión de riesgos. Con este fin, se debe desarrollar un plan de acción, que incluye priorizar las actividades en función de las necesidades comerciales de la organización y los procesos de gestión de riesgos. Este enfoque basado en el riesgo permite a las organizaciones estimar los recursos (por ejemplo, personal y fondos) necesarios para lograr los objetivos de ciberseguridad establecidos de una manera rentable y priorizada.

Los niveles del marco de ciberseguridad, que permiten a las partes interesadas de los sectores público y privado evaluar cómo están gestionando su riesgo cibernético y comprender mejor cómo se miden esas acciones hasta lo que se considere efectivo. Hay cuatro niveles, que se describen como "Parciales" en el extremo inferior y "Adaptativo" en el extremo superior. Los niveles incluyen descripciones generales de cuánta atención se presta a la gestión de riesgos, el grado en que estas actividades están vinculadas a las necesidades del negocio y cuánta integración disfruta la ciberseguridad en las operaciones más amplias de la empresa u organización.

Figura 1. Niveles de implementación del CSF



Fuente: <https://marvin-soto.medium.com/nist-ciberseguridad-hol%C3%ADstica-ce4b3911dae7>

Tal como se aprecia, el nivel varía de parcial (nivel 1) al adaptado (nivel 4) y describe el grado de toma de decisiones de riesgo cada vez más rigurosa e integral, el grado en que la ciberseguridad se incluye en decisiones de riesgo más amplias y la organización la comparte y recibe; incluye información de ciberseguridad de fuentes externas.

5. MARCO DE LA NIST EN LAS ORGANIZACIONES

La infraestructura crítica, o CI, es una subcategoría de infraestructura que incluye aquellos activos, sistemas y redes, ya sean físicos o virtuales, que son tan vitales que su falla o destrucción tendría un impacto debilitante en la seguridad, la gobernanza, la salud pública y la seguridad. confianza pública, así mismo las herramientas de evaluación de vulnerabilidades de seguridad cibernética existentes se diseñaron en base a las políticas y estándares definidos por organizaciones como el Departamento de Energía de los EE. UU. y el Instituto Nacional de Estándares y Tecnología (NIST) (Gupta Gouriseti, Gouriseti, & Patangia, 2020).

Para las organizaciones es vital asegurar la información procesada y almacenada por las tecnologías de la información y la comunicación es una tarea cada vez más importante debido al creciente ingenio y la cantidad de ataques detectados en el ciberespacio, a este respecto la seguridad de la información propende por la preservación de la confidencialidad, integridad y disponibilidad de la información, sin embargo están las amenazas causas potenciales de un incidente no deseado, que puede resultar en daño a un sistema u organización otro elemento a considerar son las vulnerabilidades los cuales son una debilidad o defecto de un activo o control que puede ser explotado por una o más amenazas, el evento de seguridad de la información es la ocurrencia identificada del estado de un sistema, servicio o red que indica una posible violación de la seguridad de la información política o falla de los controles, o una situación previamente desconocida que puede ser relevante para la seguridad, incidente de seguridad de la información es uno o una serie de eventos de seguridad y el riesgo la probabilidad de que una vulnerabilidad pueda ser explotada por una amenaza, generando un impacto (Disterer, 2013) (Meszaros & Buchalcevova, 2017).

El modelo de la NIST se desarrollará de tal manera que pueda ser aplicable a la mayoría de las organizaciones. Para ser lo suficientemente flexible y genérico como para ser aplicado a diferentes realidades organizacionales, este modelo tendrá en cuenta los siguientes supuestos (Teodoro, Gonçalves, & Serrão, 2015):

- Diferentes niveles de madurez de CS en toda la organización.
- La relevancia de las subcategorías NIST CSF puede diferir entre organizaciones.
- Agnóstico tecnológico, enfocándose en la funcionalidad y objetivos.
- Estructura interna y organizaciones entre equipos y departamentos.

El modelo pretende ser lo más genérico posible desde la perspectiva de la organización (representado por los tres pilares, RRHH, procesos y tecnología) y tender un puente entre cada realidad propia con NIST CSF, proporcionando como resultado un conjunto de métricas que permitan un análisis de línea base de nivel de cumplimiento de esa norma; como una visión estratégica de alto nivel del ciclo de vida de la gestión del riesgo de ciber seguridad de una organización. Las cinco funciones principales de marco de NIST para una organización son (AWS, 2020):

A. Identificar (ID) Los datos, el personal, los dispositivos, los sistemas y las instalaciones que permiten a la empresa conseguir objetivos empresariales se identifican y gestionan de forma consistente con su importancia relativa para los objetivos empresariales y la estrategia de los riesgos de la empresa.

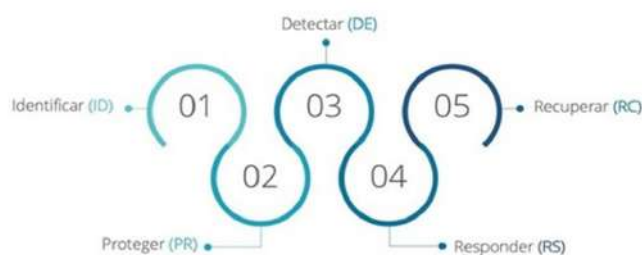
B. Proteger (PR) El acceso a los activos físicos y lógicos y las instalaciones asociadas se limita a los usuarios, los procesos y los dispositivos autorizados, y se gestiona de forma consistente con el riesgo evaluado del acceso no autorizado a actividades y transacciones autorizadas.

C. Detectar (DE) La actividad anómala se detecta de forma oportuna y se comprende el posible impacto de los eventos.

D. Responder (RS) Los procesos y los procedimientos de respuestas se ejecutan y mantienen para garantizar una respuesta oportuna a los eventos de seguridad cibernética detectados.

E. Recuperarse (RC) las actividades de restauración se coordinan con partes internas y externas, como centros coordinadores, proveedores de servicios de Internet, propietarios de sistemas de ataque, víctimas, otros CSIRT y vendedores.

Figura 2. Funciones principales del NIST Cybersecurity Framework



Fuente: NIST

Otras consideraciones es que el marco de ciberseguridad del Instituto Nacional de Estándares y Tecnología (NIST) dada su flexibilidad permite una integración con el Modelo de Alineación Estratégica (SAM), COBIT, la ISO 22316 correspondiente a la Resiliencia Organizacional. La alineación entre las estrategias comerciales y de TI, con sus respectivas infraestructuras administrativas, procesos y habilidades del personal, mantiene una resiliencia mutuamente dependiente (Belalcázar, Belalcázar, Díaz, & Molinari, 2017).

La implementación de seguridad cibernética basado en la CSF incluye unos pasos iterativos, tal como se muestra en la siguiente figura:

Figura 3. Pasos para la implementación de un programa de ciberseguridad basado en el CSF



Fuente: <https://marvin-soto.medium.com/nist-ciberseguridad-hol%C3%ADstica-ce4b3911dae7>

• **Paso 1** – Priorización y definición de alcance: Se deberá identificar las prioridades de alto nivel de la organización y los objetivos de negocios. Con toda la información ya obtenida se puede decidir el alcance del programa.

• **Paso 2** – Orientación: Se deben determinar los sistemas activos, las amenazas, los requisitos regulatorios y las vulnerabilidades relacionados con el entorno de idoneidad definido.

• **Paso 3** – Crear un perfil actual: A través de las funciones del marco básico y el uso de categorías y subcategorías, se pueden obtener los resultados de la ejecución de controles en el entorno.

• **Paso 4** – Ejecutar un análisis de riesgos: Se realizó un análisis de riesgo para determinar la probabilidad y el impacto de incidentes de ciberseguridad en el entorno analizado.

• **Paso 5** – Crear un perfil objetivo: Determina los objetivos de seguridad cibernética que la organización pretende cubrir.

• **Paso 6** – Determinar, analizar y priorizar las brechas detectadas: A través del análisis de la diferencia entre el perfil actual y el perfil objetivo, se puede definir un plan de acción prioritario según costo/beneficio, de manera que se puedan determinar los recursos y se puedan tomar medidas de mejora.

• **Paso 7** – Implementar el plan de acción: Realizamos ajustes controlados y despliegues mejorados de forma gradual y monitoreada.

• **Paso 8** – Revisión del plan de acción.

• **Paso 9** – Gestión del ciclo de vida.

Existen herramientas de software para soportar la implementación del CSF, una de ellas es referida al proyecto Baldrige (NIST Programa Baldrige, s.f.) que permite el diseño de un enfoque integrado para la gestión del desempeño organizacional, integrando las normas del CSF en su marco de excelencia llamado "Marco de excelencia Baldrige".

Finalmente, una buena cantidad de estudios de casos, guías de implementación, herramientas y recursos educativos de gran apoyo se pueden encontrar en la página de recursos de la industria del NIST (NIST RESOURCES, s.f.) facilitando y aportando ayuda a las actividades de desarrollo en este sentido.

6. CONCLUSIONES

Las organizaciones se han vuelto cada vez más dependientes de los sistemas de información para realizar el Core del negocio como siempre. Además, ciber ataques como espionaje industrial, fuga de información confidencial, robo digital, daño a la imagen y reputación de la organización. Para mitigar estos incidentes informáticos, organizaciones como el Instituto Nacional de Estándares y Tecnología (NIST) han hecho un esfuerzo por establecer una guía de protección de ciberseguridad.

Los Estados, las organizaciones, las entidades financieras, los hospitales y otras empresas recopilan, procesan y almacenan grandes cantidades de información confidencial en las computadoras y las transmiten a través de redes a otras computadoras, con el fin de mitigar el riesgo y reducir la brecha en Ciberseguridad las organizaciones implementan el marco NIST.

El Marco de la NIST ofrece una estructura, sencilla y efectiva, que apoyan las cinco funciones de gestión de riesgos: Identificar, Proteger, Detectar, Responder y Recuperar. Con el fin de brindar la seguridad cibernética actual y futura a una organización.



REFERENCIAS



- AWS. (25 de 10 de 2020). AWS. Obtenido de <https://bit.ly/34IW5jR>
- Belalcázar, A., Belalcázar, M., Díaz, J., & Molinari, L. (2017). Towards a Strategic Resilience of Applications through the NIST Cybersecurity Framework and the Strategic Alignment Model (SAM). International Conference on Information Systems and Computer Science (INCISCOS). Quito: IEEE.
- Bullock, J., Haddow, G., & Coppola, D. (2018). 8 - Cybersecurity and Critical Infrastructure Protection. En H. Security. Elsevier Inc.
- Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for Information Security Management. Journal of Information Security.
- Gupta Gourisetti, S., Gourisetti, G., & Patangia, H. (2020). Cybersecurity vulnerability mitigation framework through empirical paradigm. Enhanced prioritized gap analysis., 410-431.
- House, W. (28 de 10 de 2020). National Archives. Obtenido de www.whitehouse.gov/issues/cybersecurity .
- Meszaros, J., & Buchalcevova, A. (2017). Introducing OSSF: A framework for online service cybersecurity risk management. Computers & Security, 300-313.
- NIST. (2020 de 10 de 2020). NIST releases Cybersecurity Framework version 1.0. Obtenido de <https://bit.ly/3oKIG3Y>
Nist Programa Baldrige. (s.f.). Obtenido de <https://www.nist.gov/baldrige/how-baldrige-works>
- NIST RESOURCES. (s.f.). Obtenido de <https://www.nist.gov/cyberframework/resources>
- Teodoro, N., Gonçalves, L., & Serrão, C. (2015). NIST CyberSecurity Framework Compliance: A Generic Model for Dynamic Assessment and Predictive Requirements. Trustcom/BigDataSE/ISPA, 418-425.
- Zhao et al., J. (2020). TIMiner: Automatically extracting and analyzing categorized cyber threat intelligence from social data. Computers & Security.