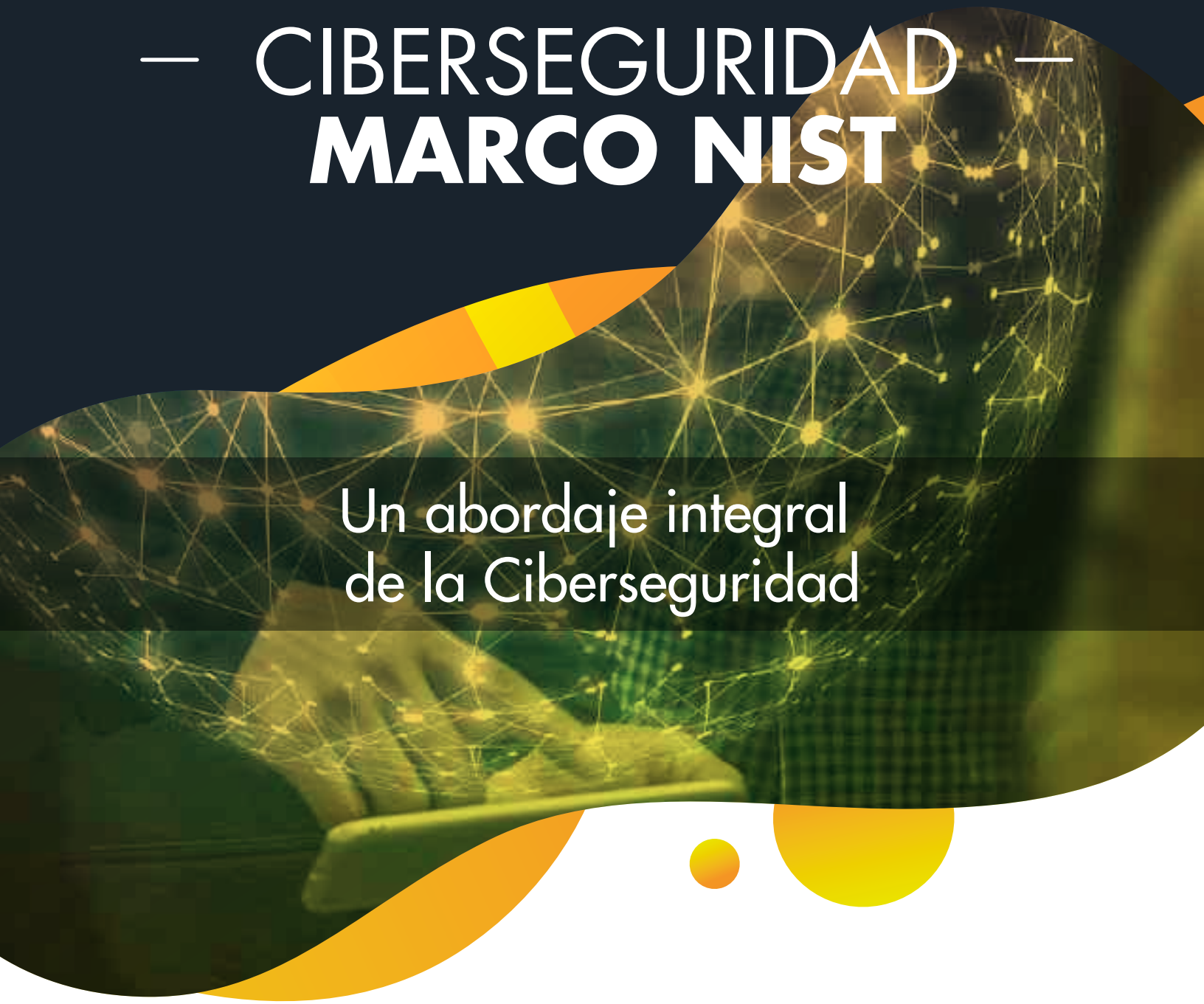
2019

White paper series
Edición 5

CIBERSEGURIDAD
MARCO NIST



Un abordaje integral de la Ciberseguridad

OEA Más derechos para más gente

aws

— CIBERSEGURIDAD —
MARCO NIST

Un abordaje integral
de la Ciberseguridad

CRÉDITOS

Luis Almagro

Secretario General
Organización de los Estados Americanos (OEA)

Equipo Técnico de la OEA

Farah Diva Urrutia
Alison August Treppel
Belisario Contreras
Santiago Paz
Fabiana Santellán
Kerry-Ann Barrett
Nathalia Foditsch
Diego Subero
David Moreno
Mariana Cardona
Jaime Fuentes
Miguel Ángel Cañada

Equipo Técnico de AWS

Abby Daniell
Michael South
Andres Maz
Melanie Kaplan
Min Hyun

CONTENIDO

1. Introducción

Dado un aumento sostenido de la cantidad de incidentes de ciberseguridad en los EEUU, el presidente Barack Obama, el 12 de febrero de 2013, emite la orden ejecutiva 13636 [1] en donde se encarga al Instituto de Nacional de Estándares y Tecnologías (NIST, por sus siglas en inglés) el desarrollo del Marco de ciberseguridad para la protección de infraestructuras críticas, lo que hoy se conoce como el Cybersecurity Framework (CSF). EEUU identifica 16 sectores de infraestructuras críticas, estos son: químico; instalaciones comerciales; comunicaciones; fabricación crítica; presas/represas; base industrial de defensa; servicios de emergencia; energía; servicios financieros; comida y agricultura; instalaciones gubernamentales; salud y salud pública; tecnología de información; reactores nucleares, materiales y residuos; sistemas de transporte; sistemas de agua y aguas residuales. [18]

El Marco fue concebido bajo las premisas de identificar las normas y directrices de seguridad aplicables en todos los sectores de infraestructura crítica, proporcionando un enfoque flexible y repetible, que permite la priorización de actividades y apunta a obtener un buen rendimiento de las infraestructuras, manteniéndose rentable para el negocio.

Es sin dudas una herramienta para la gestión de riesgos de ciberseguridad, que habilita la innovación tecnológica y se ajusta a cualquier tipo de organización (sin importar rubro o tamaño).

El Marco tomó como estrategia basarse en estándares de la industria ya aceptados por el ecosistema de ciberseguridad (NIST SP 800-53 Rev.4 [2], ISO/IEC 27001:2013 [3], COBIT 5 [4], CIS CSC [5], entre otros). Se presentan como una estrategia de abordaje simple de la gobernanza de la ciberseguridad, permitiendo trasladar fácilmente conceptos técnicos a los objetivos y necesidades del negocio. Su desarrollo fue bajo una metodología participativa, donde todas las partes interesadas (gobierno, industria, academia) pudieron participar y brindar mejoras.

La principal innovación del CSF está dada por dejar de lado estándares rígidos, que era la norma en ese momento; pero no fue el primero en desarrollar una iniciativa para la protección de las infraestructuras críticas. La OTAN ya había desarrollado una serie de manuales orientados hacia la protección de infraestructuras críticas para la defensa nacional, como es el caso del "Manual del Marco de Trabajo de Ciberseguridad Nacional" (National Cyber Security Framework Manual) [14]. Esto no quiere decir que el CSF de NIST excluya estos documentos, al contrario, los complementa y mejora.

El gran diferencial que ha presentado el CSF respecto a sus antecesores es su simplicidad y flexibilidad; simplicidad para poder transmitir una estrategia técnica en términos que el negocio comprenda y flexibilidad para adecuarse a cualquier organización. Esta diferencia es lo que ha hecho que, a la fecha, la industria y comunidad técnica de todo el mundo haya visto con muy buenos ojos este marco. Empresas, academia y gobiernos han adoptado de manera voluntaria el CSF como parte de su estrategia de ciberseguridad. Incluso organizaciones líderes en la generación de normas y estándares han incorporado el CSF, como por ejemplo ISACA e ISO. En particular, ISO generó la ISO/IEC TR 27103:2018 [6] que proporciona orientación sobre cómo aprovechar los estándares existentes en un marco de ciberseguridad, en otras palabras, cómo utilizar el CSF.

2. NIST Cybersecurity Framework (CSF)

2.1. Historia del CSF

El proceso de desarrollo del Marco se inició en EEUU con la Orden Ejecutiva número 13636, que se publicó el 12 de febrero de 2013. La Orden Ejecutiva introdujo esfuerzos para compartir información sobre amenazas de ciberseguridad y para construir un conjunto de enfoques actuales y exitosos, un marco para reducir los riesgos para infraestructura crítica. A través de esta Orden Ejecutiva, NIST se encargó del desarrollo del "Cybersecurity Framework".

Algunos de los requerimientos para su desarrollo fueron: Identificar las normas y directrices de seguridad aplicables en todos los sectores de infraestructura crítica; Proporcionar un enfoque prioritario, flexible, repetible, basado en el rendimiento y rentabilidad; Ayudar a identificar, evaluar y gestionar el riesgo cibernético; Incluir orientación para medir el desempeño de la implementación del Marco de Ciberseguridad; e Identificar áreas de mejora que deben abordarse a través de la colaboración futura con sectores particulares y organizaciones que desarrollan estándares.

Creación del Marco

El Marco fue, y sigue siendo, desarrollado y promovido a través del compromiso continuo y con el aporte de las partes interesadas del gobierno, la industria y la academia. Para desarrollar el Marco, en el transcurso de un año, el NIST utilizó una Solicitud De Información (RFI) y una Solicitud De Comentarios (RFC), así como una amplia difusión y talleres en todo EEUU para: **(i)** identificar las normas de ciberseguridad existentes, directrices, marcos y mejores prácticas que eran aplicables para aumentar la seguridad de los sectores de infraestructura crítica y otras entidades interesadas; **(ii)** especifique brechas de alta prioridad para las cuales se necesitaron estándares nuevos o revisados; y **(iii)** desarrollar planes de acción en colaboración mediante los cuales se puedan abordar estas brechas.

Para la actualización del CSF a la versión 1.1 cuya publicación se efectuó en abril de 2018, NIST continuó con su estrategia de elaboración participativa dando lugar a expertos e industria, así como a gobiernos y empresas no estadounidenses, a modo de ejemplo participó el gobierno de Israel y la empresa Huawei Technologies. [17]

2.2. Estructura del CSF

El Cybersecurity Framework (CSF) consta de tres componentes principales:

- Framework Core
- Niveles de implementación (Tiers)
- Perfiles

Framework Core

El Core es un conjunto de actividades y resultados de ciberseguridad deseados, organizados en Categorías y alineados con Referencias Informativas a estándares aceptados por la industria. Está diseñado para ser intuitivo y actuar como una capa de traducción para permitir la comunicación entre equipos multidisciplinarios mediante el uso de lenguaje simplista y no técnico.

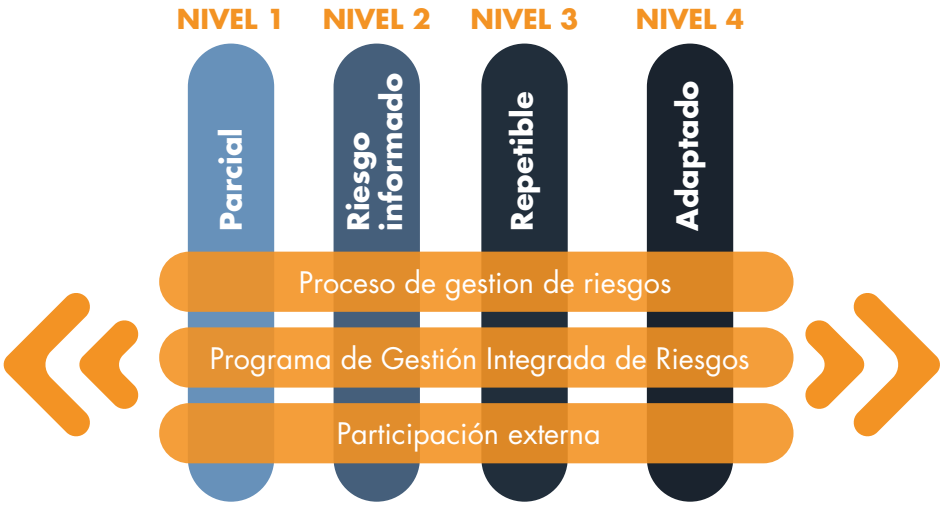
El Core consta de tres partes: Funciones, Categorías y Subcategorías. Incluye cinco **funciones** de alto nivel: Identificar, Proteger, Detectar, Responder y Recuperar.

El siguiente nivel hacia abajo son las 23 **categorías**, que se dividen en las cinco funciones. Fueron diseñadas para cubrir la amplitud de los objetivos de ciberseguridad para una organización, sin ser demasiado detalladas, cubriendo temas relacionados a los aspectos técnicos, las personas y los procesos, con un enfoque en los resultados.

Las **subcategorías** son el nivel más profundo de abstracción en el Core. Hay 108 Subcategorías, que son declaraciones basadas en resultados que proporcionan consideraciones para crear o mejorar un programa de ciberseguridad. Debido a que el Marco está orientado a los resultados y no establece cómo una organización debe lograr esos resultados, permite implementaciones basadas en el riesgo que se adaptan a las necesidades de las distintas organizaciones.

Niveles de implementación del CSF

Los niveles describen el grado en que las prácticas de gestión de riesgos de ciberseguridad de una organización exhiben las características definidos en el Marco. Los niveles van desde Parcial (Nivel 1) a Adaptativo (Nivel 4) y describen un grado cada vez mayor de rigor, y qué tan bien integradas están las decisiones de riesgo de ciberseguridad en decisiones de riesgo más amplias, y el grado en que la organización comparte y recibe información de ciberseguridad de fuentes externas.



Si bien NIST remarca que los niveles no necesariamente representan niveles de madurez, en la práctica se asemejan. Lo sustancial es que las organizaciones determinen el nivel deseado (no todos los controles deben implementarse en el nivel más alto), asegurándose de que el nivel seleccionado cumple al menos con los objetivos de la organización, reduce el riesgo de ciberseguridad a niveles aceptables, tienen un costo admisible y que son factibles de implementar.

Perfiles

Los perfiles son la alineación única de una organización de sus requisitos y objetivos organizacionales, la tolerancia al riesgo y los recursos con respecto a los resultados deseados del Framework Core. Los perfiles se pueden utilizar para identificar oportunidades para mejorar la postura de ciberseguridad comparando un perfil "actual" con un perfil "objetivo".

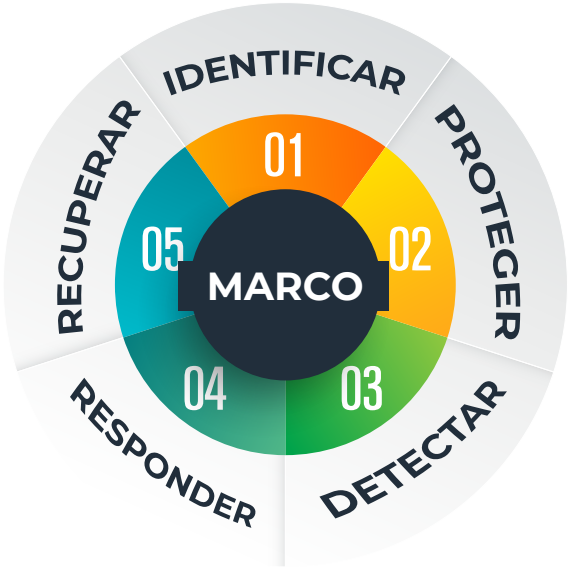
La identificación del perfil actual les permite a las organizaciones realizar una revisión objetiva (sin implicar esto una auditoría formal u otras evaluaciones técnicas) de su programa de ciberseguridad en relación con el CSF y conocer certeramente cuál es su situación actual de seguridad.

Teniendo en cuenta la evaluación del riesgo organizacional, los requisitos de cumplimiento y los objetivos organizacionales, se puede crear un perfil objetivo, que, en comparación con el perfil actual, informará la estrategia de liderazgo y las prioridades para la contratación, capacitación, cambios de políticas, cambios de procedimientos y adquisición de tecnología.

2.3. Funciones del CSF

Las cinco funciones incluidas en el Framework Core son:

1. Identificar
2. Proteger
3. Detectar
4. Responder
5. Recuperar



Las Funciones son el nivel más alto de abstracción incluido en el Marco. Actúan como la columna vertebral del Framework Core en el que se organizan todos los demás elementos.

Estas cinco funciones fueron seleccionadas porque representan los cinco pilares principales para un programa de ciberseguridad exitoso y holístico. Ayudan a las organizaciones a expresar fácilmente su gestión del riesgo de ciberseguridad a un alto nivel y posibilitan decisiones de gestión de riesgos.

Identificar

Ayuda a desarrollar un entendimiento organizacional para administrar el riesgo de ciberseguridad de los sistemas, las personas, los activos, los datos y las capacidades. La comprensión del contexto empresarial, los recursos que respaldan las funciones críticas y los riesgos relacionados con la ciberseguridad permiten que una organización se centre y priorice sus esfuerzos, de acuerdo con su estrategia de administración de riesgos y sus necesidades comerciales.

Proteger

Describe las medidas de seguridad adecuadas para garantizar la entrega de servicios de las infraestructuras críticas. Esta función contempla la capacidad de limitar o contener el impacto de un potencial evento de ciberseguridad.

Detectar

Define las actividades necesarias para identificar la ocurrencia de un evento de ciberseguridad., permitiendo el descubrimiento oportuno de los mismos.

Responder

Incluye actividades necesarias para tomar medidas con respecto a un incidente de ciberseguridad detectado, desarrollando la capacidad de contener el impacto de un potencial incidente.

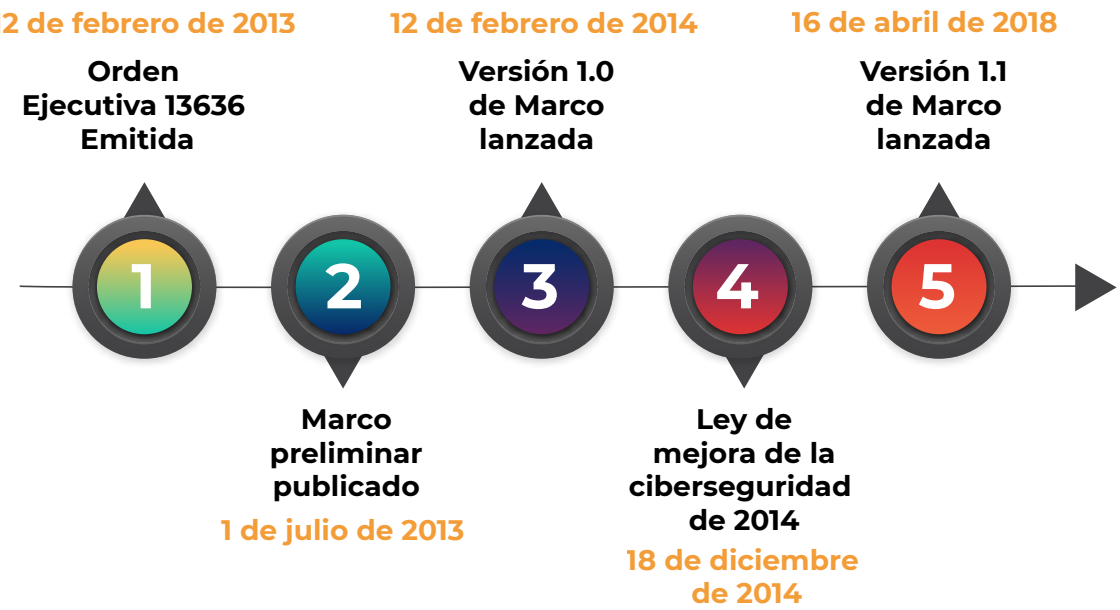
Recuperar

Identifica las actividades necesarias para mantener los planes de resiliencia y para restaurar cualquier capacidad o servicio que se haya deteriorado debido a un incidente de ciberseguridad. Esta función es compatible con la recuperación oportuna de las operaciones normales para reducir el impacto de un incidente de ciberseguridad.

2.4. Versiones y mecanismos de evolución

El CSF ha sido desarrollado y promovido a través del compromiso continuo y con el aporte de las partes interesadas en el gobierno, la industria y la academia. Eso incluye un proceso público abierto de revisión y comentarios, talleres y otros medios de participación.

A continuación, se presenta un gráfico con la evolución del Cybersecurity Framework:



3. ¿Cómo usar el CSF?

El CSF se presenta como una herramienta que permite gestionar los riesgos de ciberseguridad de manera flexible y adaptable a la realidad de cualquier organización, sin importar su tamaño o rubro.

Es importante destacar que el Marco no plantea nuevos controles ni procesos, sino que agrupa los controles planteados por los principales estándares de la industria, internacionalmente reconocidos como son el NIST SP 800-53, ISO 27001, COBIT 5, entre otros). Por tanto, no va a sustituir los procesos y controles que tenga ya implementados la organización, sino que la misma continuará utilizando lo que ya ha implementado y eventualmente complementará los mismos, de manera de presentar una estrategia con un enfoque ejecutivo, orientado a resultados.

3.1. Estrategia para adoptar el CSF

A continuación, se presentan tres estrategias posibles, planteadas en el Marco [11], para la utilización del CSF, no siendo las únicas.

Revisión básica de prácticas de ciberseguridad

Una organización puede utilizar el Marco como una parte clave de su proceso sistemático de gestión del riesgo de ciberseguridad; éste no está diseñado para reemplazar los procesos existentes, sino para determinar las brechas en su enfoque actual de riesgo de ciberseguridad y desarrollar una hoja de ruta para la mejora; permitiendo la optimización de costos y resultados.

Creación o mejora de un programa de ciberseguridad

El Marco está diseñado para complementar las operaciones de negocio y de ciberseguridad existentes; pudiendo tomarlo como base para la creación de nuevo programa de ciberseguridad o como herramienta para la mejora de un programa existente.

Los siguientes 7 pasos pueden guiar la creación de un nuevo programa de ciberseguridad o mejorar uno existente. Estos pasos deben repetirse según sea necesario para mejorar y evaluar continuamente la ciberseguridad:

Paso 1: Priorizar y determinar el alcance. Se deben identificar los objetivos de negocios y las prioridades de alto nivel de la organización. Con esta información se puede determinar el alcance del programa de ciberseguridad: qué línea de negocio o procesos serán abordados.

Paso 2: Orientación. Se identifican los sistemas y activos vinculados al alcance, los requisitos legales o regulatorios, así como el enfoque de riesgo general. activos.

Paso 3: Crear un perfil actual. Se realiza una evaluación del programa de ciberseguridad para crear un perfil actual, esta indicará qué resultados de categoría y subcategoría del Framework Core se están logrando actualmente. Es esencial que esta evaluación incluya Personas (cantidad de personal, roles de trabajo, habilidades y capacitación para profesionales de seguridad y conocimiento general del usuario), Procesos (estrategia, políticas, procedimientos, manual vs. automatización, canales de comunicación con las partes interesadas, etc.), y Tecnología (capacidades, configuraciones, vulnerabilidades, parches, operaciones y contratos de soporte, etc.).

Paso 4: Realizar una evaluación de riesgos. Se analiza el entorno operativo para discernir la probabilidad de un evento de ciberseguridad y el impacto que el evento podría tener en la organización. Es importante que las organizaciones identifiquen los riesgos emergentes teniendo en cuenta la identificación de vulnerabilidades de los activos y la información de amenazas de ciberseguridad de fuentes internas y externas para obtener una mejor comprensión de la probabilidad y el impacto de los eventos de ciberseguridad. Si bien este paso se enfoca en la identificación de riesgos de ciberseguridad, es importante que este proceso esté alineado a la evaluación de riesgos organizacional, así como a la evaluación de riesgos de negocio para que exista una retroalimentación en las evaluaciones.

Paso 5: Crear un perfil objetivo. Se debe centrar en la evaluación de las Categorías y subcategoría del Marco que describen los resultados deseados de ciberseguridad de la organización, teniendo siempre presente la misión y objetivos del negocio, así como requisitos vinculados a cumplimiento legal o normativo. Las organizaciones también pueden desarrollar sus propias Categorías adicionales basados en los requisitos de negocio, así como requisitos de las partes interesadas externas, como son las entidades del sector, los clientes y los socios empresariales; sin olvidar que los requisitos no son únicamente de corte técnico o tecnológico, sino también asociados al personal y capacitación, políticas, procedimientos y demás necesidades administrativas.

Paso 6: Determinar, analizar y priorizar las brechas. Se compara el Perfil Actual y el Perfil Objetivo para determinar las brechas. A continuación, crea un plan de acción priorizado para abordar las brechas (que reflejan los impulsores, los costos y los beneficios, y los riesgos de la misión) para lograr los resultados en el Perfil Objetivo. Luego, la organización determina los recursos necesarios para abordar las brechas, que incluyen los fondos y la fuerza laboral.

Paso 7: Implementar el plan de acción. Se determinan qué acciones tomar para abordar las brechas, si las hay, identificadas en el paso anterior y luego ajusta sus prácticas actuales de ciberseguridad para lograr el Perfil Objetivo. Es importante que las acciones contemplen todas las aristas de la gobernanza de la ciberseguridad: Personal (contrataciones, capacitación, formación, etc.); Tecnología (soluciones actuales, soluciones comerciales disponibles, nuevos desarrollos, innovación, etc.) y Procesos (políticas, procesos y procedimientos adecuados a la necesidad y realidad de la organización).

Comunicación de los requisitos de ciberseguridad a las partes interesadas

El Marco puede proporcionar un medio para expresar los requisitos de ciberseguridad a los socios de negocio, clientes y proveedores; en particular a los proveedores de servicios o productos vinculados a la infraestructura crítica de la organización.

3.2. Principales desafíos

El CSF tiene el gran desafío de adecuarse a diferentes sectores, industrias e incluso países. Este no utiliza ningún estándar específico para satisfacer los controles de ciberseguridad, sino que se abstrae de ellos aplicando un enfoque conceptual y sugiriendo una lista de múltiples posibles estándares para satisfacer los requerimientos del control. De esta manera permite ser utilizado en diferentes ámbitos como Infraestructuras Críticas, Gobierno o sector privado.

Claramente dependerá enormemente del punto de partida de cada organización a la hora de implementar el CSF para identificar cuáles son los principales desafíos que deberán abordar las mismas. En términos generales, existen algunos desafíos que suelen presentarse en buena parte de las organizaciones, los mismos están asociados al compromiso de la alta dirección para la adopción de una estrategia de ciberseguridad, la cultura del riesgo organizacional [16] y la falta de profesionales calificados para poder liderar estos procesos [15].

Según el informe de OEA "Ciberseguridad: ¿Estamos preparados en América Latina y el Caribe?" [12] publicado en 2016, los aspectos vinculados a la política y estrategia de ciberseguridad de los países es uno de los puntos a reforzar en toda la región de Latinoamérica y el Caribe; entendemos que la adopción de este tipo de marcos puede aportar positivamente en la elaboración de las estrategias de ciberseguridad de los gobiernos (en particular, en la protección de sus infraestructuras críticas) y en fortalecer los procesos de colaboración regional.

4. Casos de estudio

El CSF es en la actualidad un marco reconocido por la comunidad técnica que contempla las mejores prácticas en lo que refiere a ciberseguridad. Este marco ha sido adoptado por diversos países como parte de su estrategia en ciberseguridad y algunos de ellos incluso lo han incluido en su legislación nacional. Dentro del conjunto de países que han adoptado el CSF podemos encontrar: Bermudas, Estados Unidos, Israel, Italia, Japón, Reino Unido, Suiza y Uruguay. [13]

A continuación, presentamos el estudio de dos de estos casos con adopciones de enfoque diferentes.

4.1. **Reino Unido -** Un enfoque abierto

Reino Unido cuenta con un Marco Políticas de Seguridad (HMG Security Policy Framework - SPF) [7] que es de cumplimiento obligatorio para todos los departamentos de gobierno. Para colaborar en la implementación del mencionado Marco, se han desarrollado una serie de guías que abordan los distintos aspectos de la seguridad, dentro de la que se encuentra el Estándar Mínimo de Ciberseguridad (MCSS - Minimum Cyber Security Standard) [8].

El Estándar Mínimo de Ciberseguridad es un desarrollo conjunto entre el gobierno del Reino Unido y el Centro Nacional de Seguridad Cibernética (NCSC); el mismo fue publicado en junio de 2018 y es la aproximación más cercana a la CSF en la normativa británica.

Dicho estándar define las medidas de seguridad mínimas que los departamentos del Reino Unido deben implementar con respecto a la protección de su información, tecnología y servicios digitales para cumplir con sus obligaciones de SPF y Estrategia Nacional de Seguridad Cibernética.

Este estándar toma las cinco funciones del CSF (Identificar, Proteger, Detectar, Responder y Recuperar) y, si bien algunas de las funciones y categorías, y la redacción de cada una de ellas se han modificado, en general son muy fieles al CSF original.

Las funciones planteadas por el MCSS son:

1. **Identificar:** Los departamentos deben implementar procesos apropiados de gobernanza de la ciberseguridad.
2. Los departamentos identificarán y catalogarán la información sensible que tengan.
3. Los departamentos deben identificar y catalogar los servicios operacionales clave que proporcionan.
4. La necesidad de que los usuarios accedan a información sensible o servicios operacionales clave debe ser entendida y administrada continuamente.

5. **Proteger:** El acceso a información sensible y servicios operativos clave sólo se proporcionará a usuarios o sistemas identificados, autenticados y autorizados.

6. Los sistemas que manejan información sensible o servicios operacionales clave deben estar protegidos contra la explotación de vulnerabilidades conocidas.

7. Las cuentas altamente privilegiadas no deben ser vulnerables a ataques cibernéticos comunes.

8. **Detectar:** Los departamentos deben tomar medidas para detectar ataques cibernéticos comunes.

9. **Responder:** Los departamentos deben tener una respuesta definida, planificada y probada a los incidentes de ciberseguridad que afecten la información confidencial o los servicios operativos clave.

10. **Recuperar:** Los departamentos deben tener procesos bien definidos y probados para garantizar la continuidad de los servicios operativos clave en caso de falla o compromiso.

Al igual que el CSF, el MCSS deja deliberadamente abierta la implementación de los lineamientos, ya que se entiende que tratar de definir un enfoque de ciberseguridad único en diferentes industrias, plataformas y situaciones es casi imposible. En su lugar, se alienta a las empresas a interpretar la estándar de forma independiente y adaptar sus propios procesos de seguridad para garantizar su cumplimiento.

4.2. Uruguay - Un enfoque guiado

El Marco de Ciberseguridad de Uruguay (MCU) [9], tiene como principal objetivo generar confianza en el uso de la tecnología, unificar todos los recursos existentes en materia de ciberseguridad, y sustentar la evolución del gobierno digital de Uruguay. Asimismo, busca promover una visión integral y multi-sectorial de la ciberseguridad, apostando a la mejora continua de la seguridad de la información y a contribuir a la definición de planes de acción.

Su implementación se basó en Core del CSF v1.0 (ISO/IEC 27001:2013, ISO 27799:2016 [10], COBIT 5 y NIST 800-53 rev.4), además contó con el trabajo de especialistas en seguridad de la información, consultoras internacionales y la academia. Una vez elaborado el primer borrador del MCU este fue puesto a consideración de la Universidad de la Republica, donde se lo analizó y dio sus recomendaciones. Luego fue puesto a consideración de consultaros privadas del país y se recogieron también sus comentarios. Finalmente, en agosto de 2016 se publicó su versión 1.0

Hoy ya ha sido utilizado para el diagnóstico y evaluación de todos los Ministerios del Gobierno Central, Gobiernos Departamentales, Instituciones de Salud e instituciones financieras.

Adecuación del CSF al MCU

Si bien el MCU toma todo el núcleo del NIST CSF v1.0, implementa solo un conjunto de subcategorías, dejando para etapas posteriores la implementación de las subcategorías faltantes.

Dicho Marco presenta una serie de requisitos que incluyen buenas prácticas sobre gobernanza de la seguridad, gestión de riesgos, control de acceso, seguridad de las operaciones, gestión de incidentes y continuidad del negocio asociados a las distintas subcategorías del NIST CSF; además, incluye perfil de organización y un modelo de madurez con el que las organizaciones podrán definir las líneas de acción para mejorar su ciberseguridad. Dichos requisitos tienen adecuaciones para organismos de la Administración Central de Uruguay y para instituciones de salud; actualmente, se trabaja en la adecuación para instituciones financieras.

Requisitos propios

El MCU propone un conjunto de 65 requisitos generados a partir de los controles ISO/IEC 27001 y la normativa uruguaya vinculada a ciberseguridad.

Perfil de organización
Las organizaciones se separan en tres perfiles: básico, estándar y avanzado. La asignación del perfil está dada por la percepción del riesgo tecnológico. Es bueno aclarar que solo el perfil avanzado incluye la totalidad de las subcategorías adoptadas por el MCU.

Priorización de subcategorías
En el entendido de que las organizaciones no son todas iguales, y que dependiendo de su perfil podrían tener que priorizar la implementación de algunas subcategorías antes que otras; el MCU prioriza el abordaje de las subcategorías del CSF con el propósito de facilitar el abordaje y la elaboración de los planes de acción.

Modelo de madurez
Este modelo permite a las organizaciones evaluar su posición actual y establecer conforme a su priorización la meta de madurez en cada subcategoría presentada. En términos generales, los niveles establecen:

- **Nivel 0:** Acciones vinculadas ciberseguridad casi o totalmente inexistentes.

- **Nivel 1:** Existen algunas iniciativas sobre ciberseguridad. Enfoques ad-hoc. Alta dependencia del personal. Actitud reactiva ante incidentes de seguridad.

- **Nivel 2:** Existen ciertos lineamientos para la ejecución de las tareas. Existe dependencia del personal. Se ha avanzado en el desarrollo de los procesos y documentación de las tareas.

- **Nivel 3:** Se caracteriza por la formalización y documentación de políticas y procedimientos. Gobernanza de la ciberseguridad. Métricas de seguimiento.

- **Nivel 4:** El Responsable de Seguridad de la Información (RSI) tiene un rol clave en el control y mejora del SGSI. Se realiza control interno. Se trabaja en la mejora continua. La ciberseguridad está alineada con los objetivos y estrategias de la organización.

Cualquier organización pública o privada podrá usar el documento como herramienta de autoconocimiento y mejora de sus niveles de seguridad. A la fecha no es de adopción obligatoria, aunque se prevé a corto plazo su obligatoriedad para algunos sectores críticos.

5. Conclusiones

Las amenazas de ciberseguridad continúan creciendo y afectan a todas las organizaciones sin importar su rubro o tamaño.

Si bien el CSF fue concebido inicialmente como una herramienta para evaluar la ciberseguridad en las Infraestructuras Criticas de EEUU, su enfoque, agnóstico del punto de vista de los estándares y requerimientos tecnológicos, han mostrado que se adapta perfectamente a diferentes sectores y países, y resulta de fácil adopción en los procesos de auditoria.

El CSF puede utilizarse para generar un nuevo programa de ciberseguridad o como herramienta para analizar la brecha de programas de ciberseguridad existentes y mejorarlos. Está estructurado de tal forma que permite un abordaje integral de la gobernanza de la ciberseguridad, alineándolo fácilmente a las necesidades del negocio.

Las subcategorías del CSF han sido mapeadas a los controles de los principales estándares de la industria, permitiendo una consolidación de los mismos, y brindando un abordaje flexible y claro.

Finalmente, el CSF tiene que ser visto como una herramienta de gestión de riesgos de ciberseguridad que permite evaluar la efectividad de los controles y la rentabilidad de los mismos.

Los programas de ciberseguridad más exitosos son aquellos que no se basan simplemente en la aplicación de controles técnicos, sino que definen una estrategia, un marco, para abordar cada una de las funciones esenciales de ciberseguridad: identificar el contexto, proteger los sistemas y activos, detectar los desvíos, responder antes incidentes y recuperar las operaciones del negocio. En resumen, la ciberseguridad es un problema del negocio que solo se puede resolver con una visión holística de Personas, Procesos y Tecnología.

6. Referencias

[1] Casa Blanca (2013), *Orden ejecutiva 13636:* https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

[2] NIST (2013), *NIST 800-53 Rev.4:* https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-53r4.pdf

[3] ISO (2013), *ISO/IEC 27001:* https://www.iso.org/standard/54534.html

[4] ISACA (2012), *COBIT 5:* http://www.isaca.org/COBIT/Pages/COBIT-5-spanish.aspx

[5] CIS (2018), *Critical Security Controls (CSC):* https://www.cisecurity.org/controls/

[6] ISO (2018), *ISO/IEC TR 27103:* https://www.iso.org/standard/72437.html

[7] Gobierno de Reino Unido (2013), *Marco de Políticas de Seguridad de Reino Unido:* https://www.gov.uk/government/collections/government-security

[8] Gobierno de Reino Unido (2018), *Marco de ciberseguridad de Reino Unido:* https://www.gov.uk/government/publications/the-minimum-cyber-security-standard

[9] AGESIC (2018), *Marco de Ciberseguridad de Uruguay:* https://www.agesic.gub.uy/innovaportal/v/5823/1/agesic/marco-de-ciberseguridad-v40.html

[10] ISO (2016), *ISO 27799:* https://www.iso.org/standard/62777.html

[11] NIST (2018), *CSF v1.1 (en español):* https://www.nist.gov/sites/default/files/documents/2018/12/10/frameworkesmellrev_20181102mn_clean.pdf

[12] OEA (2016), *Ciberseguridad: ¿Estamos preparados en América Latina y el Caribe?:* https://publications.iadb.org/es/publicacion/17071/ciberseguridad-estamos-preparados-en-america-latina-y-el-caribe

[13] NIST, *Adaptaciones internacionales del CSF:* https://www.nist.gov/cyberframework/international-resources

[14] OTAN (2012), *National Cyber Security Framework Manual:* https://ccdcoe.org/uploads/2018/10/NCSFM_0.pdf

[15] ISC2 (2017), 2017 *Global Information Security Workforce Study - Benchmarking Workforce Capacity and Response to Cyber Risk (LATAM):* https://iamcybersafe.org/wp-content/uploads/2017/06/LATAM-GISWS-Report.pdf

[16] Deloitte (2016), *La Evolución de la Gestión de Ciber-Riesgos y Seguridad de la Información:* https://www2.deloitte.com/pe/es/pages/risk/articles/la-evolucion-de-la-gestion-de-ciber-riesgos-y-seguridad.html

[17] NIST (2018), RFC - *Cybersecurity Framework Draft Version 1.1:* https://www.nist.gov/cyberframework/rfc-cybersecurity-framework-draft-version-11

[18] Homeland Security, *Sectores de infraestructura crítica:* https://www.dhs.gov/cisa/critical-infrastructure-sectors

7. Fuentes

NIST, *Sitio web oficial del CSF*:
https://www.nist.gov/cyberframework/

NIST, *Historia y creación del CSF:*
https://www.nist.gov/cyberframework/online-learning/history-and-creation-framework

NIST, *Estructura del CSF:*
https://www.nist.gov/cyberframework/online-learning/components-framework

NIST, *Funciones del CSF:*
https://www.nist.gov/cyberframework/online-learning/five-functions

NIST, *Evolución del CSF:*
https://www.nist.gov/cyberframework/evolution

AWS, *NIST Cybersecurity Framework – Aligning to the NIST CSF in the AWS Cloud*:
https://d1.awsstatic.com/whitepapers/compliance/NIST_Cybersecurity_Framework_CSF.246c0a886c7d16d2b370c20a04f99511d212613a.pdf

— CIBERSEGURIDAD —
MARCO NIST

Un abordaje integral
de la Ciberseguridad

2019

White paper series
Edición 5

OEA | Más derechos para más gente

aws

— CIBERSEGURIDAD —
MARCO NIST

Un abordaje integral de la Ciberseguridad