RESOURCE CENTER

¿Qué es el Marco de Ciberseguridad del NIST? La guía definitiva

Get the full interactive view at
https://bitwarden.com/es-la/resources/nist-cybersecurity-framework/

bitwarden

Historia del NIST

El Instituto Nacional de Normas y Tecnología (NIST) ofrece orientación y mejores prácticas para que las organizaciones las sigan, con el fin de ayudar a las empresas, organizaciones sin ánimo de lucro y otras instituciones del sector privado a mejorar la gestión de los riesgos de ciberseguridad. El NIST forma parte del Departamento de Comercio de Estados Unidos y es uno de los laboratorios de ciencias (físicas) más antiguos del país.

Ya en 2013, el Presidente emitió la Orden Ejecutiva 13636 que establecía:

> **"Es política de los Estados Unidos mejorar la seguridad y la resistencia de las infraestructuras críticas de la Nación y mantener un entorno cibernético que fomente la eficiencia, la innovación y la prosperidad económica, promoviendo al mismo tiempo la seguridad, la confidencialidad empresarial, la privacidad y las libertades civiles."**

Esta Orden Ejecutiva establecía ciertos requisitos que el NIST aplicaba a su marco de ciberseguridad, entre ellos:

- Identificar las normas y directrices de seguridad aplicables en todos los sectores de las infraestructuras críticas.
- Proporcionar un enfoque priorizado, flexible, repetible, basado en el rendimiento y rentable.
- Ayudar a los propietarios y operadores de infraestructuras críticas a identificar, evaluar y gestionar los riesgos cibernéticos.
- Permitir la innovación técnica y tener en cuenta las diferencias organizativas.
- Proporcionar una orientación tecnológicamente neutra que permita a los sectores de infraestructuras críticas beneficiarse de un mercado competitivo de productos y servicios.
- Incluir orientaciones para medir los resultados de la aplicación del Marco de Ciberseguridad.
- Identificar las áreas de mejora que deberían abordarse mediante la futura colaboración con determinados sectores y organizaciones de elaboración de normas.

¿Por qué es tan importante?

En pocas palabras, las crecientes amenazas a la ciberseguridad afectan a diario a las empresas y otras organizaciones. Sin una única fuente de verdad, sería casi imposible que las empresas desarrollaran un marco exhaustivo y eficaz que les ayudara a aplicar medidas efectivas para mitigar los riesgos de seguridad. Por eso el Marco de Ciberseguridad del NIST se ha vuelto tan crucial para las empresas; fomenta soluciones eficientes, innovadoras y resistentes para mantener la seguridad.

Índice

¿Qué es el Marco de Ciberseguridad del NIST?

En esencia, el Marco de Ciberseguridad del NIST ayuda a organizaciones de todo tipo a comprender, gestionar y reducir mejor los riesgos de ciberseguridad. El resultado final de seguir estas orientaciones es una mejor protección de las redes y los datos. El Marco de Ciberseguridad del NIST se desglosa de tal manera que cualquier empresa u organización podría aplicarlo para comprender mejor dónde centrar el tiempo y los recursos para mejorar la protección de la ciberseguridad. Se trata de capacitar a las empresas para que sean más eficaces a la hora de proteger sus datos, los de sus clientes, sus redes y sus empleados.

Aunque el Marco de Ciberseguridad del NIST fue desarrollado por una organización de Estados Unidos, se creó con la idea de una adopción global. Con ese fin, se ha traducido a muchos idiomas y ha sido adoptada por gobiernos, empresas y organizaciones de todo el mundo.

Desde el Marco de Ciberseguridad 1.1 del NIST, muchas organizaciones y gobiernos han adoptado con éxito el marco, entre ellos:

- Saudi Aramco
- Gobierno de Bermudas
- Dirección Cibernética Nacional de Israel
- Cimpress-FAIR
- Multi-Estado - Centro de Análisis e Intercambio de Información
- Centro Médico de la Universidad de Kansas
- Universidad de Pittsburgh
- ISACA
- Foro intersectorial japonés
- Universidad de Chicago
- Autoridad del Bajo Colorado
- Cibersoluciones ópticas

La última versión del Marco de Ciberseguridad (CSF) del NIST está dirigida a públicos, sectores industriales y organizaciones de todo tipo y tamaño, desde pequeñas escuelas y organizaciones sin ánimo de lucro hasta grandes empresas. El marco se diseñó para que cualquier organización, independientemente de su nivel de sofisticación en materia de ciberseguridad, pueda beneficiarse de la información que presenta.

Según la Directora del NIST y Subsecretaria de Comercio para Normas y Tecnología, Laurie E. Locascio:

> "El CSF ha sido una herramienta vital para muchas organizaciones, ayudándolas a anticiparse y hacer frente a las amenazas a la ciberseguridad... El CSF 2.0, que se basa en las versiones anteriores, no es sólo un documento. Se trata de un conjunto de recursos que pueden personalizarse y utilizarse individualmente o combinados a lo largo del tiempo, a medida que cambian las necesidades de ciberseguridad de una organización y evolucionan sus capacidades."

Explorar la historia del Marco de Ciberseguridad del NIST

La última evolución del Marco de Ciberseguridad del NIST también va más allá de centrarse en las infraestructuras críticas y abarca a todas las organizaciones (de todos los tamaños) dentro de cualquier sector.

Cuando se creó el Marco de Ciberseguridad del NIST, el objetivo consistía en un compromiso continuo con las partes interesadas de la administración, la industria y el mundo académico. Para crear este marco, el NIST recurrió a actividades de divulgación y talleres en todo el país, así como a una solicitud de información (RFI) y una solicitud de comentarios (RFC). Su objetivo inicial era triple:

- Identificar las normas, directrices, marcos y mejores prácticas existentes en materia de ciberseguridad.
- Especifique las lagunas de alta prioridad.
- Desarrollar planes de acción para subsanar esas deficiencias.

El periodo de recogida de comentarios finalizó el 8 de abril de 2013, y el NIST recibió más de 270 respuestas a la solicitud de información. A partir de esas respuestas, el NIST elaboró el programa de su primer taller sobre el Marco de Ciberseguridad, que se celebró en Washington DC con el objetivo de captar el interés, aumentar la concienciación y proporcionar información sobre el proceso de desarrollo colaborativo. Los temas del taller incluyeron la Orden Ejecutiva, los objetivos para el desarrollo y la reafirmación del proceso que se utilizaría para desarrollar el marco.

El segundo taller tuvo lugar entre el 29 y el 31 de mayo de 2013 y se celebró en la Universidad Carnegie Mellon con un orden del día basado en el análisis de la RFI inicial. Los objetivos eran definir y aclarar mejor la información que habían recibido y fomentar el debate sobre varios temas relacionados con la seguridad. Una vez concluido este taller, el NIST analizó la información recopilada y elaboró resúmenes que se compartieron con las industrias y se utilizaron para crear el borrador inicial del Marco de Ciberseguridad.

El primer borrador del Marco de Ciberseguridad del NIST se publicó el 2 de julio de 2013.

Tras la publicación, el NIST organizó varios talleres para debatir y perfeccionar la versión inicial. El 12 de febrero de 2014 se publicó la versión 1.0 del Marco de Ciberseguridad del NIST.

Funciones básicas del Marco de Ciberseguridad del NIST

El Marco de Ciberseguridad del NIST consta de varias funciones básicas, que ofrecen una visión general de las mejores prácticas. Estas funciones no deben considerarse pasos procedimentales, sino que se utilizan para abordar la naturaleza dinámica de los riesgos de

ciberseguridad.

Gobernar

Esta función proporciona resultados que ayudan a informar sobre lo que una organización puede hacer para priorizar las funciones restantes en el contexto de su misión y las expectativas de las partes interesadas.

Identifique

La función de identificación hace referencia a la necesidad de desarrollar una comprensión organizativa de los riesgos de ciberseguridad para los sistemas, activos, datos y capacidades. Este elemento se centra en la empresa, para que pueda priorizar sus esfuerzos de forma coherente con su estrategia de gestión de riesgos.

Proteja

Esta función respalda la capacidad de una organización para proteger sus activos y prevenir o reducir la probabilidad de que se produzca un incidente de ciberseguridad, así como las repercusiones del mismo.

Detectar

Esta función permite descubrir y analizar a tiempo anomalías, indicadores de compromiso y otros sucesos adversos que indican que se ha producido o se va a producir un suceso de ciberseguridad.

Responder

Esta función ayuda a contener los efectos de un incidente de ciberseguridad, abarcando la gestión de incidentes, el análisis, la mitigación, la elaboración de informes y la comunicación.

Recuperar

Esta función se centra en el restablecimiento oportuno de las operaciones normales de la empresa, con el fin de reducir los efectos de un incidente de ciberseguridad, así como permitir la comunicación necesaria (y adecuada) durante la recuperación.

El objetivo final de estas funciones es ofrecer una visión estratégica de alto nivel de cómo una organización se prepara, reacciona y se recupera de los eventos de ciberseguridad.

Implantación del Marco de Ciberseguridad del NIST

Con una sólida comprensión de lo que hace el Marco de Ciberseguridad del NIST y de cómo ha evolucionado, probablemente se esté preguntando cuál es la mejor manera de aplicarlo.

El NIST recomienda un planteamiento de 7 pasos para la implantación, que tiene el siguiente aspecto:

1. **Prioridad y alcance** - Priorice los objetivos de su organización y los activos que deben protegerse.
2. **Orientar** - Familiarícese usted y su equipo con los procesos, sistemas y componentes incluidos en el ámbito de aplicación, así como con la normativa clave que deben cumplir.
3. **Cree un perfil actual** - Indique qué resultados de control del marco ya se están logrando en su organización y, a continuación, elabore una lista de lo que aún debe integrarse.
4. **Realice una evaluación de riesgos**: analice su entorno operativo para determinar la probabilidad de que se produzcan incidentes de ciberseguridad, así como el impacto que podrían tener.
5. **Cree un perfil objetivo** - Céntrese en la evaluación de las Categorías y Subcategorías del Marco de Ciberseguridad para ayudarle a describir los resultados de ciberseguridad deseados.

6. **Determine, analice y priorice las carencias** - Determine cualquier carencia de ciberseguridad que exista en su organización. A partir de este análisis, podrá crear un plan con prioridades para abordar esas necesidades.

7. **Ponga en marcha su plan de acción**: actúe y aplique el plan que ha creado para resolver todos los problemas descubiertos en los pasos anteriores.

Hay que tener en cuenta que el marco no es inflexible. De hecho, el marco ofrece la flexibilidad suficiente para que pueda integrarse con sus procesos de seguridad existentes. Debería ver cómo funciona en los siete pasos enumerados anteriormente.

Ventajas de adoptar el Marco de Ciberseguridad del NIST

Por la forma en que el NIST expone los siete pasos para implantar el marco, las organizaciones obtienen una amplia visión general de los riesgos a los que son susceptibles, cómo planificar en función de esos riesgos, cómo mejorar la comunicación en toda la organización y reforzar el cumplimiento. La educación relativa a los puntos débiles de una organización, y cómo mitigarlos, es uno de los beneficios cruciales del Marco del NIST.

> Según la Comisión Federal de Comercio, el Marco del NIST "ayuda a las empresas de todos los tamaños a comprender, gestionar y reducir mejor sus riesgos de ciberseguridad y a proteger sus redes y datos".

El NIST entiende que cada organización es diferente, e incluso ofrece 3 consejos para mantener seguras las contraseñas (que deberían considerarse universales).

Retos y consideraciones para la adopción del marco

El Marco de Ciberseguridad del NIST puede ser complejo. Es importante comprender bien las funciones básicas antes de pasar a los siete pasos anteriores. Para garantizar un éxito duradero, es fundamental fomentar una cultura de ciberseguridad dentro de su organización; de lo contrario, se encontrará con resistencia a lo que podría ser un cambio drástico en procesos y sistemas.

Otros retos son:

- Limitación de recursos: es posible que actualmente no disponga de personal capaz de aplicar estos cambios.
- Lo más probable es que tenga que dedicar tiempo a personalizar el Marco de Ciberseguridad para que se adapte mejor a su organización.
- Las amenazas evolucionan constantemente, lo que significa que sus prácticas de seguridad tendrán que mantenerse al día.
- Deberá integrar el Marco de Ciberseguridad en los procesos existentes.
- Puede resultar difícil fomentar el compromiso de las partes interesadas, lo que está directamente relacionado con el fomento de una cultura de ciberseguridad capaz de satisfacer estas demandas.

Perfiles y niveles del Marco de Ciberseguridad del NIST

Existen cuatro niveles de aplicación del NIST, que son:

- **Nivel 1 Parcial** - Empresas con procedimientos de seguridad a la carta o nulos.
- **Nivel 2** - Empresas conscientes **de** las amenazas a las que se enfrentan y que aplican algunas políticas, pero carecen de una estrategia coordinada.
- **Nivel 3 Repetible** - Empresas con buenas prácticas de gestión de riesgos y ciberseguridad que han recibido la aprobación de los ejecutivos. Estas empresas suelen medirse con sus competidores, e incluso trabajan con otras organizaciones para asegurarse de que sus prácticas están alineadas.
- **Nivel 4 Adaptable** - Empresas de sectores muy regulados (como la banca y la sanidad) que contribuyen de forma rutinaria a una amplia concienciación sobre los riesgos.

Según el NIST, el Perfil del Marco de Ciberseguridad "es la alineación de las Funciones, Categorías y Subcategorías con los requisitos empresariales, la tolerancia al riesgo y los recursos de la organización." Estos perfiles ayudan a las organizaciones a establecer una hoja de ruta para reducir los riesgos de ciberseguridad.

El NIST ofrece una plantilla de perfil organizativo del marco de ciberseguridad personalizable, así como una lista de perfiles comunitarios que pueden utilizarse.

Actualización y evolución con el Marco del NIST

Tenga en cuenta que el Marco de Ciberseguridad del NIST está diseñado para ser un documento vivo que depende de actualizaciones periódicas que reflejen el panorama siempre cambiante de la ciberseguridad y las amenazas emergentes. Por ello, es crucial que las organizaciones se mantengan al día de las últimas amenazas, de modo que el Marco de Ciberseguridad pueda evolucionar para satisfacer las necesidades actuales y mejorar continuamente.

Para asegurarse de que su organización es capaz de evolucionar con el Marco de Ciberseguridad del NIST, podría considerar cómo construir la mejor pila de tecnología de ciberseguridad para su negocio, como una forma de asegurarse de que es capaz de aprovechar la mejor tecnología capaz de evolucionar con el Marco de Ciberseguridad.

Aprovechar Bitwarden para reforzar la ciberseguridad

Huelga decir que la seguridad se ha convertido en uno de los aspectos más importantes para las organizaciones. Sin unas prácticas sólidas de gestión de riesgos de ciberseguridad, las empresas podrían ser víctimas de cualquier número de amenazas en la naturaleza. Con la ayuda del Marco de Ciberseguridad del NIST, junto con una cuidadosa planificación/comunicación, la seguridad de su organización podría mejorar enormemente. Aborde el Marco de Ciberseguridad del NIST a fondo, siga los 7 pasos y esté siempre preparado para actualizar y evolucionar, de modo que su organización esté mejor protegida frente a los riesgos de ciberseguridad.

¿Listo para empezar hoy mismo? Considere la posibilidad de adoptar una solución de gestión de contraseñas para que su organización empiece con buen pie. Consulte los planes de Bitwarden Business, contacte con ventas y compare los precios de los planes.