NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST Cybersecurity Framework 2.0:
Guía de inicio rápido para crear y utilizar perfiles organizativos

U.S. Department of Commerce
Gina M. Raimondo, Secretary
National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

Publicación especial del NIST
NIST SP 1301 spa
https://doi.org/10.6028/NIST.SP.1301.spa
Febrero de 2024

NIST CSF 2.0: CREACIÓN Y USO DE PERFILES ORGANIZATIVOS

UNA GUÍA DE INICIO RÁPIDO

INTRODUCCIÓN

Impulse el Progreso con el paso del tiempo con Perfiles Organizativos

Un ***Perfil Organizativo*** describe la postura de seguridad cibernética actual y/u objetivo de una organización en términos de resultados de seguridad cibernética del Marco de Seguridad Cibernética (CSF, por sus siglas en inglés) principal. Los perfiles organizativos se utilizan para comprender, adaptar, evaluar y priorizar los resultados de la seguridad cibernética en función de los objetivos de la misión de una organización, las expectativas de las partes interesadas, el panorama de amenazas y los requisitos. La organización puede así actuar estratégicamente para lograr esos resultados. Estos perfiles también pueden utilizarse para evaluar el progreso hacia los resultados previstos y para comunicar la información pertinente a las partes interesadas.

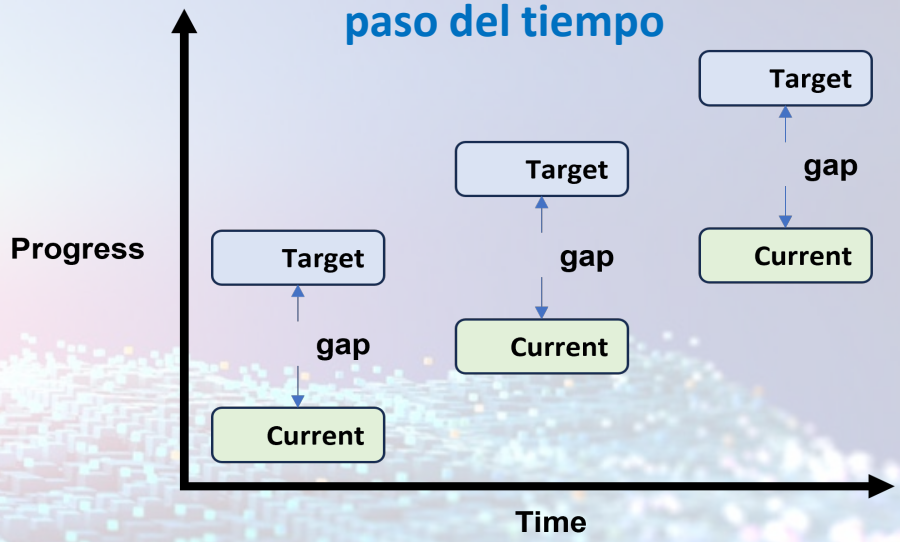
Los Perfiles organizativos pueden clasificarse de la siguiente manera:

- Un ***Perfil Actual*** que especifica los resultados del CSF que una organización está obteniendo actualmente y caracteriza cómo o en qué medida se está obteniendo cada resultado.
- Un ***Perfil Objetivo*** que especifica los resultados del CSF deseados que una organización ha seleccionado y priorizado para alcanzar sus objetivos de gestión de riesgos de seguridad cibernética. Un Perfil Objetivo considera cambios anticipados a la postura de seguridad cibernética de la organización, tales como nuevos requerimientos, adopción de nuevas tecnologías y tendencias en inteligencia de amenazas.

Creación y uso de perfiles organizativos con el proceso de cinco pasos del CSF

El CSF 2.0 describe un proceso de cinco pasos para crear y utilizar perfiles organizativos. Más específicamente, el proceso compara un Perfil Objetivo al que se aspira con un Perfil Actual evaluado. A continuación, se realiza un análisis de las deficiencias y se desarrolla e implementa un plan de acción. Este proceso conduce naturalmente al perfeccionamiento del Perfil Objetivo que se utilizará durante la siguiente evaluación.

Impulse el progreso con el paso del tiempo



Creación y uso de perfiles organizacionales

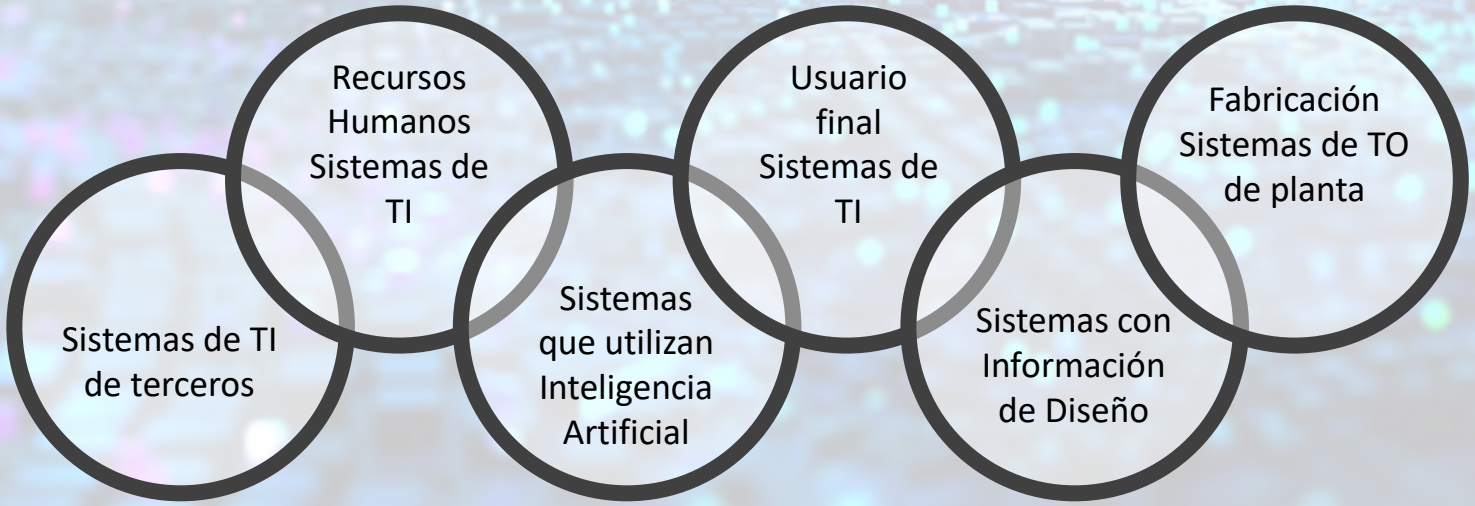
NIST CSF 2.0: CREACIÓN Y USO DE PERFILES ORGANIZATIVOS

UNA GUÍA DE INICIO RÁPIDO

ALCANCE DEL PERFIL ORGANIZATIVO

El alcance define los hechos y suposiciones de alto nivel en los que se basarán los Perfiles. Puede tener tantos Perfiles organizativos como desee, cada uno con un alcance diferente. Algunas de las preguntas a las que debe responder al definir el alcance de su perfil son:

- ¿Cuál es la razón para crear el perfil organizativo?
- ¿Cubrirá el perfil a toda la organización? Si no, ¿cuáles de las divisiones de la organización, activos de datos, activos tecnológicos, productos y servicios, y/o colaboradores y proveedores serán incluidos?
- ¿El perfil abordará todos los tipos de amenazas, vulnerabilidades, ataques y defensas en materia de seguridad cibernética? En caso negativo, ¿qué tipos se incluirán?
- ¿Qué individuos o equipos serán responsables de desarrollar, revisar y hacer operativo el Perfil?
- ¿Quién será responsable de establecer las expectativas de las acciones para lograr los resultados previstos?



Datos sobre perfiles organizativos

Formas de pensar en los perfiles

Es posible que una organización determinada desee utilizar varios Perfiles.

Cada Perfil puede tener un alcance distinto basado en factores como:

- categoría tecnológica (TI, TO)
- tipos de datos (PII, PHI, PCI)
- usuarios (empleados, terceros)

El alcance de un Perfil determina la *aplicabilidad* de un resultado del CSF dado.

Puede ser útil combinar dos o más Perfiles cuando los ámbitos se solapan.

NIST CSF 2.0: CREACIÓN Y USO DE PERFILES ORGANIZATIVOS

UNA GUÍA DE INICIO RÁPIDO

RECOPILACIÓN DE LA INFORMACIÓN NECESARIA

Algunos ejemplos de información pueden ser las políticas organizativas, las prioridades y recursos de gestión de riesgos, los requisitos y estándares de seguridad cibernética... Las fuentes de información necesarias dependerán del caso de uso, los elementos que capturarán los Perfiles y el nivel de detalle deseado. Las fuentes de información más comunes son

1. Perfiles comunitarios

Un ***perfil comunitario*** es una línea base de resultados de CSF creada y publicada para abordar intereses y objetivos compartidos entre varias organizaciones. Un perfil comunitario suele estar destinado a un sector o subsector, tecnología, tipo de amenaza u otro caso de uso concreto.

Una organización puede utilizar un Perfil Comunitario como base para su propio Perfil Objetivo copiando el Perfil Comunitario en un Perfil Organizativo. Un Perfil Comunitario puede adaptarse de las siguientes maneras:

- Ajustando las prioridades de determinados resultados del CSF
- Añadiendo subcategorías específicas de la organización, referencias informativas u orientaciones para la implementación.

Consulte *Una Guía para la creación de perfiles comunitarios del CSF 2.0* para obtener más información sobre la creación y el uso de perfiles comunitarios.

2. Plantilla de perfil organizativo del NIST

El NIST proporciona una **plantilla de perfil organizativo del CSF** en forma de hoja de cálculo de Microsoft Excel. Puede descargarla y completarla para crear los perfiles actual y objetivo de su organización. La plantilla facilita la comparación de los perfiles actual y objetivo para identificar y analizar las brechas. Puede encontrar la plantilla en el Sitio web del CSF 2.0.

Priorización

La característica distintiva de un perfil

La noción central de un perfil objetivo es determinar diferentes prioridades para los resultados aplicables del CSF. Las prioridades le ayudan a determinar las partes de su programa de seguridad cibernética que deben recibir más o menos recursos. Las prioridades de seguridad cibernética son impulsadas por objetivos estratégicos, leyes, regulaciones y respuestas a riesgos. Para obtener más información, consulte SP 800-37 sobre las tareas de gestión de riesgos en toda la organización en el *Paso Preparar*. IR 8286B ofrece información sobre cómo el CSF principal apoya las decisiones de respuesta al riesgo.

NIST CSF 2.0: CREACIÓN Y USO DE PERFILES ORGANIZATIVOS

UNA GUÍA DE INICIO RÁPIDO

CREACIÓN DEL PERFIL ORGANIZATIVO - PARTE 1

Determine qué tipos de información de apoyo debe incluir cada Perfil para los resultados del CSF seleccionados... Los pasos para crear un perfil organizativo son los siguientes:

3a: Descargue la última plantilla de hoja de cálculo del perfil organizativo del CSF y personalícela como desee.

3b: Incluya los resultados de seguridad cibernética que se aplican a su caso de uso y documente las razones según sea necesario.

3c: Documente las **Prácticas** actuales de seguridad cibernética en las columnas del Perfil actual. Las anotaciones más detalladas pueden proporcionar una mejor perspectiva para los pasos posteriores.

3d: Documente los **Objetivos** de seguridad cibernética y los planes para alcanzarlos en las columnas del Perfil Objetivo. Las entradas pueden basarse en referencias informativas del CSF, nuevos requisitos de seguridad cibernética, nuevas tecnologías y tendencias en inteligencia de ciberamenazas.

3e: Anote la importancia de cada Objetivo utilizando el campo **Prioridad**.

Resultados del CSF		Perfil actual			Perfil Objetivo	
Identificador	**Descripción**	**Prácticas**	**Estado**	**Valoración**	**Prioridad**	**Objetivos**
Los identificadores y descripciones del CSF principal - Funciones, Categorías, Subcategorías. También puede añadir sus propios resultados para hacer frente a los riesgos y requisitos específicos de su organización.		Políticas, procesos, procedimientos y otras actividades relacionadas con un resultado. Puede incluir elementos que contengan pruebas del logro de un resultado.	El estado o condición actual de un resultado, por ejemplo, si se está logrando y en qué grado.	Una valoración o evaluación de las prácticas actuales utilizando escalas como: • alto/medio/bajo • 1-5 • 0-100 %, • rojo/amarillo/verde	La importancia relativa de un resultado utilizando escalas como: • Bajo/Medio/Alto • 1/2/3/4/5 • clasificaciones (1, 2, 3...)	Tales como: • Políticas, procesos y procedimientos • Papeles y Responsabilidades Seleccionados de: • Referencias informativas - estándares, orientaciones y mejores prácticas

NIST CSF 2.0: CREACIÓN Y USO DE PERFILES ORGANIZATIVOS

UNA GUÍA DE INICIO RÁPIDO

CREACIÓN DEL PERFIL ORGANIZATIVO - PARTE 2

La siguiente tabla muestra un ejemplo teórico de una sola fila de un perfil organizativo.
Su finalidad es meramente ilustrativa. A continuación se proporcionan algunos consejos extraídos del ejemplo:

- Añada y elimine columnas de la plantilla de perfil organizativo según sus necesidades. El CSF alienta a los usuarios a registrar cualquier información que les resulte significativa y a utilizar el formato que prefieran.
- Las columnas no tienen por qué ser las mismas para el Perfil Actual y el Perfil Objetivo.
- Incluya referencias informativas para comprender las diferencias entre Prácticas y Objetivos. Este ejemplo muestra los SP 800-53 controles entre corchetes.

Resultados del CSF		Perfil actual			Perfil Objetivo	
Identificador	**Descripción**	**Prácticas**	**Estado**	**Valoración**	**Prioridad**	**Objetivos**
PR.PS-01	Se establecen y aplican prácticas de gestión de la configuración	Política: Política de gestión de la configuración versión 1.4, última actualización 14/10/22. Define la política de control de cambios en la configuración [**CM-1**]. Procedimientos: Los propietarios de los sistemas y los responsables tecnológicos aplican informalmente las prácticas de gestión de la configuración. Los procesos para el control de cambios no se siguen de forma coherente. El CIO especifica las líneas base de configuración **[CM-2]** para las plataformas de TI y aplicaciones más utilizadas dentro de la organización, pero el uso de la línea de base no es monitoreado o aplicado de manera coherente en toda la organización.	La gestión de la configuración está parcialmente implementada en la organización. Algunos sistemas no siguen las líneas de base disponibles y otros sistemas no tienen líneas de base, por lo que pueden tener configuraciones deficientes que los hacen más susceptibles al mal uso y al compromiso. Los cambios no autorizados pueden pasar desapercibidos. Algunos cambios no se prueban ni se les hace un seguimiento.	3 *de 5*	Alto	Política: La política de gestión de la configuración exige que se especifiquen, utilicen, apliquen y mantengan líneas de base de configuración para todas las tecnologías básicas utilizadas por la organización. La política exige que se sigan procesos de control de cambios para todas las tecnologías de la organización [**CM-1**]. Procedimientos: Cada división de la organización tiene un plan de gestión de la configuración [**CM-9**], así como el mantenimiento, implementación y aplicación de líneas de base de configuración [**CM-2**] y ajustes [**CM-6**] para sus sistemas. Las líneas de base se aplican a todos los sistemas antes de la liberación de la producción. Todos los sistemas se monitorean continuamente para detectar cambios de configuración inesperados, y se generan tickets automáticamente cuando se producen desviaciones de las líneas de base. Las partes designadas revisan las solicitudes de cambio y los correspondientes análisis de impacto **[CM-4]** y aprueban o deniegan cada uno de ellos **[CM-3]**.

NIST CSF 2.0: CREACIÓN Y USO DE PERFILES ORGANIZATIVOS

UNA GUÍA DE INICIO RÁPIDO

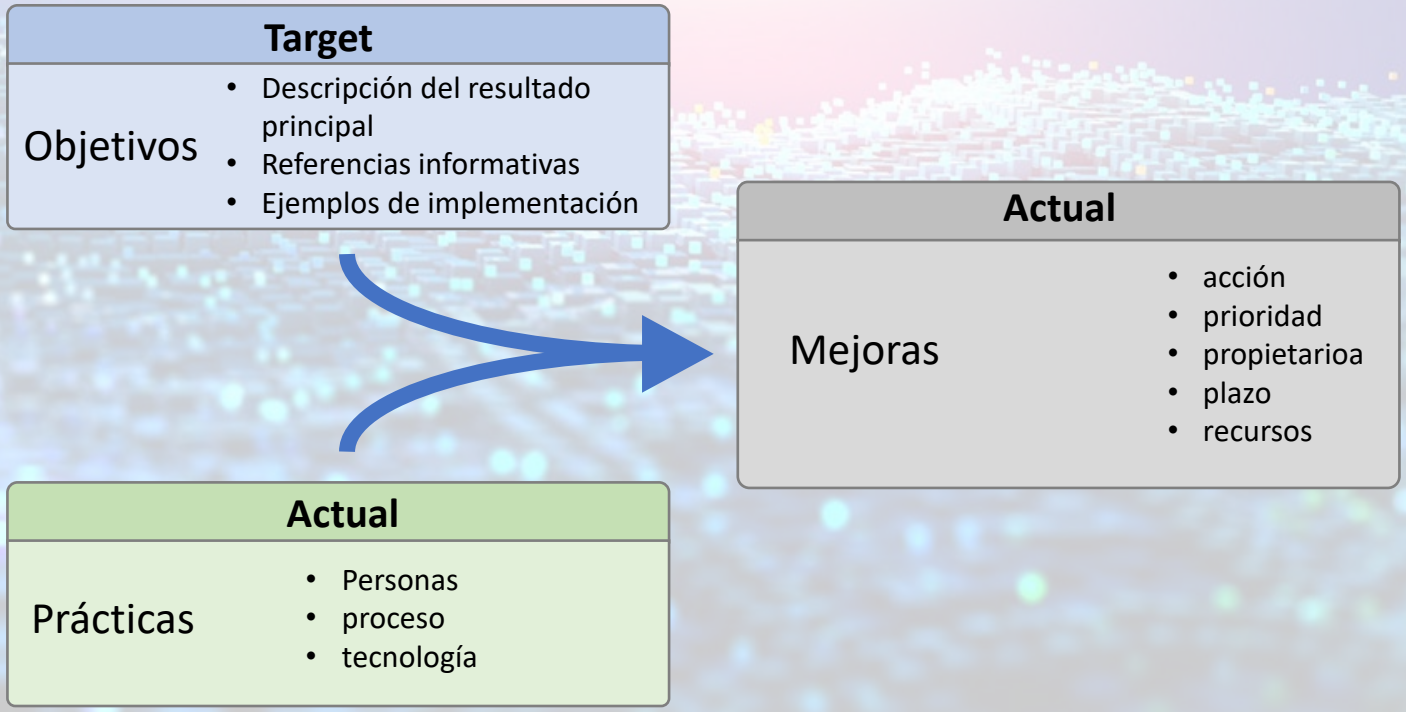
ANÁLISIS DE BRECHAS Y CREACIÓN DE UN PLAN DE ACCIÓN - PARTE 1

La identificación y el análisis de las diferencias entre los perfiles actual y objetivo permiten a una organización encontrar brechas y desarrollar un plan de acción priorizado para abordar esas brechas. El uso de Perfiles de esta manera ayuda a su organización a tomar decisiones mejor informadas sobre cómo mejorar la gestión de riesgos de seguridad cibernética de una manera prioritaria y rentable.

Paso 4a

Cómo analizar las brechas

Compare y contraste sus **prácticas** actuales, respecto a personas, procesos y tecnología, con las mejores prácticas descritas en las descripciones de resultados de los CSF, Referencias Informativas y Ejemplos de Implementación. Con esos **objetivos** en mente, haga observaciones sobre las diferencias y documente esos elementos como posibles mejoras.



Paso 4b

Cómo crear planes de acción

El plan de acción es una lista de **mejoras** pendientes para su programa de seguridad cibernética. Además del análisis de brechas del Perfil Organizativo, el plan de acción debe considerar los impulsores de la misión, los beneficios, los riesgos y los recursos necesarios (p. ej., personal, financiación). Los planes de acción deben tener todos los elementos esenciales del gráfico (izquierda).

NIST CSF 2.0: CREACIÓN Y USO DE PERFILES ORGANIZATIVOS

UNA GUÍA DE INICIO RÁPIDO

ANÁLISIS DE BRECHAS Y CREACIÓN DE UN PLAN DE ACCIÓN - PARTE 2

La identificación y el análisis de las diferencias entre los perfiles actual y objetivo permiten a una organización encontrar brechas y desarrollar un plan de acción priorizado para abordar esas brechas. El CSF proporciona enlaces a herramientas, controles y recursos de implementación que le ayudarán a analizar las brechas [**Paso 4a**] y a crear planes de acción [**Paso 4b**]. Un enfoque recomendado para la elaboración de planes de acción es utilizar Herramienta de Referencia de CSF 2.0 del NIST para seguir las referencias de las Subcategorías pertinentes de su Perfil Objetivo a los controles NIST SP 800-53 asociados.

Qué buenas prácticas se deben utilizar

Referencias informativas: relaciones entre la práctica principal y varias mejores prácticas, que incluyen estándares, directrices, regulaciones y otros recursos. Las referencias ayudan a informar sobre cómo una organización puede lograr los resultados del CSF. También ayudan a conectar los resultados deseados con otros documentos comunes de seguridad cibernética, como ISO/IEC 27001 y SP 800-53 que proporciona un catálogo de controles de seguridad y privacidad.

Cómo implementar las mejores prácticas

Ejemplos de implementación: Descripciones teóricas de las formas en que pueden cumplirse los resultados de los CSF. Los ejemplos no son una lista exhaustiva de todas las acciones que podría emprender una organización, ni tampoco una línea de base de las acciones requeridas; son ideas útiles para que las organizaciones piensen en pasos concretos. La Herramienta de referencia de CSF 2.0 del NIST permite que los usuarios exploren el CSF 2.0 principal completo y lo descarguen en formatos Excel y JSON.

Ejemplo de implementación

Un extracto de la Herramienta de Referencia de CSF 2.0 del NIST

Subcategory

PR.PS-01: Se aplican prácticas de gestión de la configuración (anteriormente PR.IP-01, PR.IP-03, PR.PT-02, PR.PT-03)

Ejemplos de implementación

Ej. 1: Establecer, probar, desplegar y mantener líneas de base sólidas que apliquen las políticas de seguridad cibernética de la organización y proporcionen únicamente las capacidades esenciales (es decir, el principio de mínima funcionalidad).

Ej. 2: Revisión de todos los ajustes de configuración por defecto que puedan afectar potencialmente a la seguridad cibernética al instalar o actualizar software.

NIST CSF 2.0: CREACIÓN Y USO DE PERFILES ORGANIZATIVOS

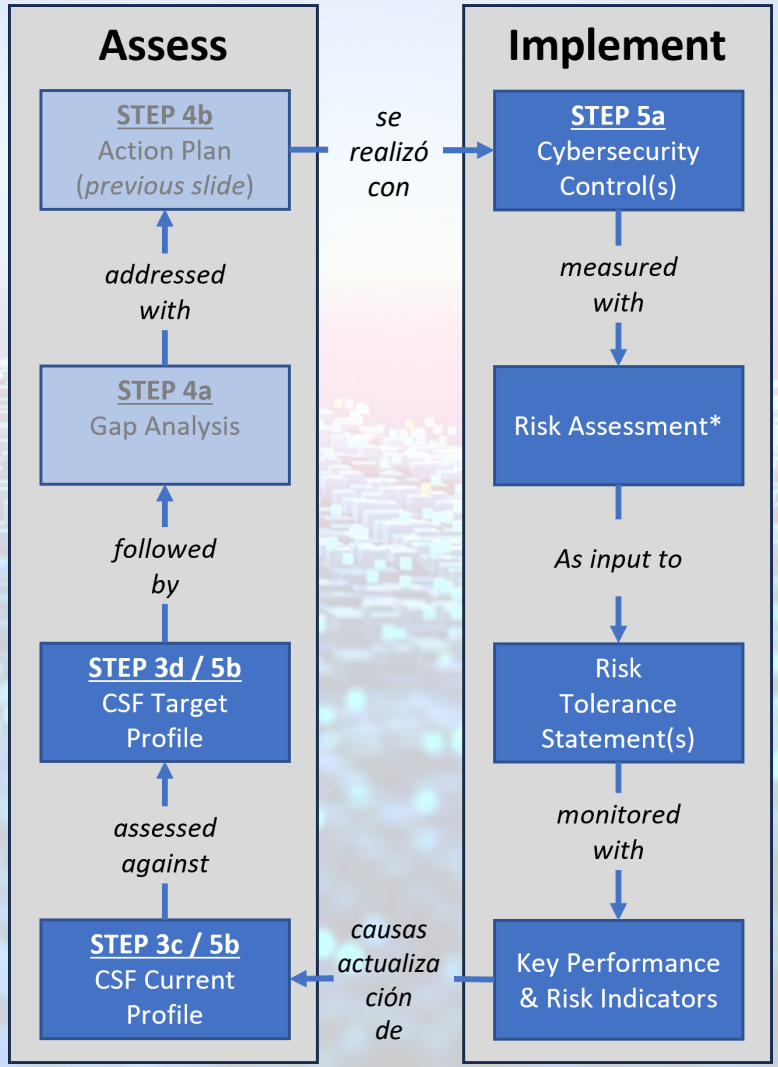
UNA GUÍA DE INICIO RÁPIDO

IMPLEMENTAR EL PLAN DE ACCIÓN Y ACTUALIZAR EL PERFIL

Paso 5a

Implementación de planes de acción

El Plan de Acción se realiza a través de cualquier combinación de controles de gestión, programáticos y técnicos. A medida que se implementan dichos controles, el Perfil Organizativo puede utilizarse para realizar un seguimiento del estado de implementación. Posteriormente, los controles y los riesgos asociados pueden monitorearse a través de Indicadores Clave de Desempeño (KPI) e Indicadores Clave de Riesgo (KRI). Los riesgos cibernéticos que superan la Tolerancia al Riesgo se observan mediante Evaluaciones de Riesgo. Los riesgos que superan la Tolerancia al Riesgo pueden conducir a actualizaciones del Plan de Acción, del Perfil Organizativo y/o de las declaraciones de Tolerancia al Riesgo. El análisis de brechas también puede conducir a la creación de POA&M para las brechas que requerirán un plazo de remediación más largo. Encontrará más información sobre KPI, KRI, Tolerancia al riesgo y POA&M en IR 8286B y SP 800-37.



Paso 5b

Actualización de su perfil

La **implementación** de las actividades que siguen a su Plan de Acción forman parte de un programa continuo de gestión de riesgos cibernéticos (los bucles de retroalimentación y las líneas de comunicación son más matizadas de lo que se muestra). Las Evaluaciones de Riesgo, como se describe en SP 800-30 pueden utilizar las declaraciones de Tolerancia al Riesgo cuando se identifican los riesgos, así como determinar la probabilidad y el impacto de esos riesgos. La probabilidad y el impacto cambiantes son una medida de la eficacia del Plan de Acción y de los controles discretos. El seguimiento de los riesgos también se realiza mediante KPI y KRI. Los cambios en los riesgos, las probabilidades y/o los impactos pueden conducir a actualizaciones del Perfil Organizativo.

* La Evaluación de Riesgos puede ocurrir en cualquier momento y puede informar cualquier paso

NIST CSF 2.0: CREACIÓN Y USO DE PERFILES ORGANIZATIVOS

UNA GUÍA DE INICIO RÁPIDO

PASOS SIGUIENTES

Lo que aprendimos. Este QSG explicó los siguientes términos:

Perfil organizativo - resultados principales del CSF relevantes para una organización específica.

Perfil Comunitario - resultados principales del CSF que se aplican a diversas organizaciones

Perfil Actual - los resultados de seguridad cibernética que una organización está logrando actualmente

Perfil Objetivo - los resultados deseados que una organización quiere alcanzar

Análisis de Brechas - determinación de las diferencias entre los Perfiles Actual y Objetivo

Referencias informativas - mejores prácticas que implementan varios resultados principales del CSF

Ejemplos de implementación - formas teóricas en que las organizaciones pueden alcanzar las subcategorías del CSF

Plan de acción - abordar las carencias y avanzar hacia el perfil objetivo

Lo que sigue. A continuación encontrará una lista de cosas que puede hacer para poner en práctica esta Guía de inicio rápido:

- Familiarizarse con la plantilla del perfil organizativo del CSF del NIST.
- Vea si hay un perfil comunitario relevante para usted en el sitio de perfiles comunitarios del NIST.
- Determine cuántos perfiles organizativos de CSF necesita [**Paso 1**].
- Haga un inventario de sus requisitos de seguridad cibernética
- Priorice los resultados de CSF en sus perfiles organizativos [**Paso 2**].
- Evalúe su perfil actual [**Paso 3**]
- Más información sobre Referencias informativas
- Mejore su programa de seguridad cibernética con el paso del tiempo [**Pasos 4 y 5**]

Más información

Lea

IR 8286B NIST IR 8286B, *Priorización del riesgo de seguridad cibernética para la gestión del riesgo empresarial*

SP 800-37 NIST SP 800-37 Revisión 2, *Marco de Gestión de Riesgos para Sistemas de Información y Organizaciones*

SP 800-53 NIST SP 800-53 Revisión 5, *Controles de Seguridad y Privacidad para Sistemas de Información y Organizaciones*

SP 800-30 NIST SP 800-30 Revision 1, *Guía para la realización de evaluaciones de riesgos*

Recursos

Plantilla de perfil organizativo Herramienta de referencia de CSF 2.0 del NIST

Referencias informativas Ejemplos de implementación

Guía para crear perfiles comunitarios de CSF 2.0

Guía de inicio rápido para utilizar los niveles del CSF