certiprof®

LEAD CYBERSECURITY

PROFESSIONAL CERTIFICATION

LCSPC™ Versión 062024

LEAD CYBERSECURITY PROFESSIONAL CERTIFICATION LCSPC™

LCSPC™ Versión 062024

¿Quién es Certiprof®?

Certiprof® es una entidad certificadora fundada en los Estados Unidos en 2015, ubicada actualmente en Sunrise, Florida.

Nuestra filosofía se basa en la creación de conocimiento en comunidad y para ello su red colaborativa está conformada por:

- **Nuestros Lifelong Learners (LLL)** se identifican como Aprendices Continuos, lo que demuestra su compromiso inquebrantable con el aprendizaje permanente, que es de vital importancia en el mundo digital en constante cambio y expansión de hoy. Independientemente de si ganan o no el examen.
- Las universidades, centros de formación, y facilitadores en todo el mundo forman parte de nuestra red de aliados **ATPs (Authorized TrIAning Partners.)**
- **Los autores (co-creadores)** son expertos de la industria o practicantes que, con su conocimiento, desarrollan contenidos para la creación de nuevas certificaciones que respondan a las necesidades de la industria.
- **Personal Interno:** Nuestro equipo distribuido con operaciones en India, Brasil, Colombia y Estados Unidos está a cargo de superar obstáculos, encontrar soluciones y entregar resultados excepcionales.

Nuestras Afiliaciones

Memberships

itcc
IT CERTIFICATION COUNCIL

Agile Alliance®

ANSI MEMBER

Digital badges issued by

Credly
by Pearson

IT Certification Council - ITCC

Certiprof® es un miembro activo de ITCC.

Una de las ventajas de hacer parte del ITCC es como líderes del sector colaboran entre sí en un formato abierto para explorar maneras nuevas o diferentes formas de hacer negocios que inspiran y fomentan la innovación, estableciendo y compartiendo buenas prácticas que nos permiten extender ese conocimiento a nuestra comunidad.

Certiprof ha contribuido a la elaboración de documentos blancos en el Career Path Ways Taskforce, un grupo de trabajo que se implementó internamente para ofrecer a los estudiantes la oportunidad de saber qué camino tomar después de una certificación.

Algunos de los miembros del ITCC

- **IBM**
- **CISCO**
- **ADOBE**
- **AWS**
- **SAP**
- **GOOGLE**
- **ISACA**

itcc
IT CERTIFICATION COUNCIL

Agile Alliance

Certiprof® es un miembro corporativo de Agile Alliance.

Al unirnos al programa corporativo Agile Alliance, continuamos empoderando a las personas ayudándolas a alcanzar su potencial a través de la educación. Cada día, brindamos más herramientas y recursos que permiten a nuestros socios formar profesionales que buscan mejorar su desarrollo profesional y sus habilidades.

https://www.agilealliance.org/organizations/certiprof/

Credly

Esta alianza permite que las personas y empresas certificadas con Certiprof® cuenten con una distinción a nivel mundial a través de un distintivo digital.

Credly es el emisor de insignias más importante del mundo y empresas líderes en tecnología como IBM, Microsoft, PMI,Nokia, la Universidad de Stanford, entre otras, emiten sus insignias con Credly.

Empresas que emiten insignias de validación de conocimiento con Credly:

- **IBM**
- **Microsoft**
- **PMI**
- **Universidad de Stanford**
- **Certiprof**

Insignias Digitales

Insignias Digitales:
¿Qué Son?

- Según el estudio del IT Certification Council (ITCC), años atrás, la gente sabía muy poco sobre las insignias digitales. Hoy, grandes empresas e instituciones educativas de todo el mundo expiden insignias.
- Las insignias digitales contienen metadatos detallados sobre quién las ha obtenido, las competencias requeridas y la organización que las ha expedido. Algunas insignias incluso están vinculadas a las actividades necesarias para obtenerlas.
- Para las empresas e instituciones educativas, las insignias y la información que proporcionan son tan importantes que muchas decisiones, como las de contratación o admisión, se basan en los datos que aportan.

¿Por qué son importantes?

- **Facilidad de Compartir y Verificar Logros:**

  - Las insignias digitales permiten a los profesionales mostrar y verificar sus logros de manera instantánea y global. Según un informe de Credly, **los perfiles de LinkedIn con insignias digitales reciben un 40% más de atención por parte de reclutadores y empleadores.**

- **Visibilidad en Plataformas Digitales:**

  En una encuesta realizada por Pearson y Credly, el **85%** de los usuarios que obtuvieron insignias digitales **las compartieron en LinkedIn,** y el **75%** reportó que esto mejoró su **credibilidad profesional en sus redes.** Además, el **76%** de los empleadores encuestados afirmó que las insignias digitales les ayudan a identificar rápidamente habilidades específicas.

¿Por qué son importantes?

- **Impacto en la Contratación:**

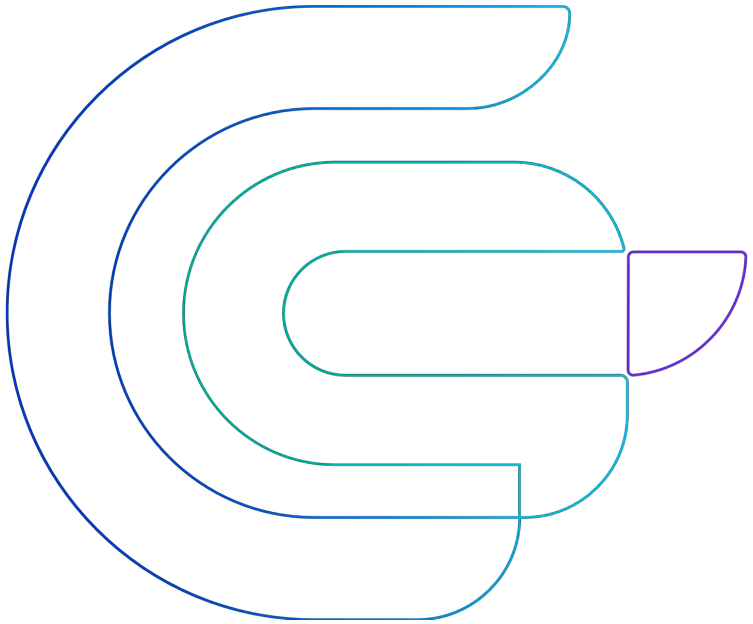
  Un estudio de la **Asociación Internacional de Gestión de Proyectos (PMI)** encontró que los candidatos que muestran insignias digitales de gestión de proyectos tienen **un 60%** más de probabilidades de ser contratados en comparación con aquellos que solo mencionan sus habilidades sin verificación digital.

¿Por qué son importantes?

- **Empoderamiento de la Marca Personal:**

La visibilidad y verificación instantánea proporcionada por las insignias digitales permiten a los profesionales no solo demostrar sus habilidades, sino también construir una marca personal fuerte. Según un estudio de LinkedIn, los profesionales que utilizan insignias digitales tienen un 24% más de probabilidades de avanzar en sus carreras.

La certificación y las insignias digitales no son solo una validación del conocimiento, sino también una herramienta poderosa para la mejora continua y la empleabilidad. En un mundo donde el aprendizaje permanente se ha convertido en la norma, estas credenciales son clave para el desarrollo profesional y la competitividad en el mercado laboral global.



- No todas las insignias son iguales, y en **Certiprof,** estamos comprometidos con ofrecerte más que un simple reconocimiento digital. Al obtener una insignia emitida por certiprof, estarás recibiendo una validación de tu conocimiento respaldada por una de las entidades líderes en certificación profesional a nivel mundial.

- **Da el siguiente paso y obtén la insignia que te abrirá puertas y te posicionará como un experto en tu campo.**

¿Por qué es importante obtener su certificado?

- **Prueba de experiencia:** Su certificado es un reconocimiento formal de las habilidades y conocimientos que ha adquirido. Sirve como prueba verificable de sus cualificaciones y demuestra su compromiso con la excelencia en su campo.

- **Credibilidad y reconocimiento:** En el competitivo mercado laboral actual, las empresas y los compañeros valoran las credenciales que le distinguen de los demás. Un certificado de una institución reconocida, como Certiprof, proporciona credibilidad instantánea e impulsa su reputación profesional.

- **Avance profesional:** Tener tu certificado puede abrirte las puertas a nuevas oportunidades. Ya se trate de un ascenso, un aumento de sueldo o un nuevo puesto de trabajo, las certificaciones son un factor diferenciador clave que los empleadores tienen en cuenta a la hora de evaluar a los candidatos.

¿Por qué es importante obtener su certificado?

- **Oportunidades de establecer contactos:** Poseer un certificado le conecta con una red de profesionales certificados. Muchas organizaciones cuentan con grupos de antiguos alumnos o de trabajo en red en los que puede compartir experiencias, intercambiar ideas y ampliar su círculo profesional.

- **Logro personal:** Obtener una certificación es un logro importante, y su certificado es un recordatorio tangible del trabajo duro, la dedicación y el progreso que ha realizado. Es algo de lo que puede sentirse orgulloso y mostrar a los demás.

Insignia

https://www.credly.com/org/certiprof/badge/lead-cybersecurity-professional-certification-lcspc.1

Aprendizaje Permanente

- Certiprof ha creado una insignia especial para reconocer a los aprendices constantes.
- Para el 2024, se han emitido más de 1,000,000 de estas insignias en más de 11 idiomas.

Propósito y Filosofía

- Esta insignia está destinada a personas que creen firmemente en que la educación puede cambiar vidas y transformar el mundo.
- La filosofía detrás de la insignia es promover el compromiso con el aprendizaje continuo a lo largo de la vida.

Acceso y Obtención de la Insignia

- La insignia de Lifelong Learning se entrega sin costo a aquellos que se identifican con este enfoque de aprendizaje.
- Cualquier persona que se considere un aprendiz constante puede reclamar su insignia visitando:

https://certiprof.com/pages/certiprof-lifelong-learning

Referencias del Entrenamiento

El presente material ha sido elaborado con base en los siguientes marcos de referencia internacionales que actualmente son referencia mundial en la temática abordada por este entrenamiento:

- **Cybersecurity – Guidelines for Internet Security ISO 27032:2023 by International Organization for Standardization.**
- **Workforce Framework for Cybersecurity 1.0 (NICE Framework) (NIST SP 800-18) (2020).**
- **Cybersecurity Framework (CSF) v 2.0 (2024) by National Institute of Standars and Technology (NIST).**

COMPARTE Y VERIFICA TUS LOGROS DE APRENDIZAJE FÁCILMENTE

#LCSPC #certiprof

certiprof®

Estructura del Contenido

Cybersecurity – Guidelines for Internet Security ISO 27032:2023

Fundamentos del Ciberespacio y la Ciberseguridad.

Relaciones entre la seguridad en internet, Seguridad en la Web, Seguridad de Red y la Ciberseguridad.
Visión general de la seguridad en Internet. Partes Interesadas (Roles).

- Coordinación y Estandarización.
- Autoridades de Gobierno.
- Leyes y agencias de regulación.
- Proveedores de Servicio de Internet

Evaluación y tratamiento de los riesgos para la seguridad en Internet

Amenazas.
Vulnerabilidades.
Vectores de Ataque.

Estructura del Contenido

Directrices de seguridad para Internet

Generalidades (Estrategias).
Controles de Seguridad en Internet

- Políticas de Seguridad en Internet.
- Control de Acceso.
- Educación Concientización y Entrenamiento.
- Gestión de Incidentes de Seguridad.
- Gestión de Activos.
- Gestión de Proveedores
- Continuidad del negocio en Internet.
- Protección de la privacidad.
- Gestión de vulnerabilidades.
- Gestión de Redes
- Control de Cambios.
- Protección antimalware.
- Identificación de Legislación y requisitos de cumplimiento aplicables.
- Uso de criptografía.
- Seguridad de las aplicaciones orientadas a Internet.
- Gestión de dispositivos de usuario final.
- Control de Acceso.
    - Gestión de Incidentes.
    - Gestión de proveedores

Referencias cruzadas entre ISO 27032 e ISO 27002

Estructura del Contenido

NICE Framework v 1.0 (SP 800-18) (2020)

NICE Background

Atributos del NICE Framework.
Propósito y Aplicabilidad.
Audiencia.
Estructura.

Bloques del NICE Framework

Tareas.
Conocimientos.
Habilidades.

Uso del NICE Framework

Uso de (TKS) Tareas, Conocimientos y Habilidades existentes.
Creación de (TKS) Tareas, Conocimientos y Habilidades nuevas.
Competencias.
Roles de Trabajo.
Equipos.

Estructura del Contenido

Cybersecurity Framework (CSF) v 2.0 (2024)

Generalidades CSF

Introducción al Nucleo del CSF

CSF Perfiles
CSF Niveles

Riesgos de Ciberseguridad, Mejora de Comunicación e Integración

Mejoras en la comunicación de la Gestión de Riesgos
Mejoras en la integración con otros programas de Gestión de Riesgos

Núcleo del CSF
Niveles del CSF
Perfiles del CSF

Glosario

Objetivos del Entrenamiento

Adquirir o complementar los conocimientos y habilidades requeridos por los profesionales para diseñar, establecer y/o mejorar la estrategia de ciberseguridad de una organización.

Identificar el vocabulario y terminología propia del ciberespacio y la ciberseguridad de tal forma que el profesional aprenda el lenguaje común utilizado por los diferentes equipos de ciberseguridad y ciberdefensa.

Conocer los diferentes marcos de referencia vigentes asociados con la gestión de seguridad y ciberseguridad considerados como buenas prácticas para la gestión de riesgos, seguridad en el ciberespacio.

Fundamentos del Ciberespacio y la Ciberseguridad ISO 27032

LCSPC™ Versión 062024

Relación Dominios Seguridad

Relaciones entre la seguridad en internet, Seguridad en la Web, Seguridad de Red y la Ciberseguridad.

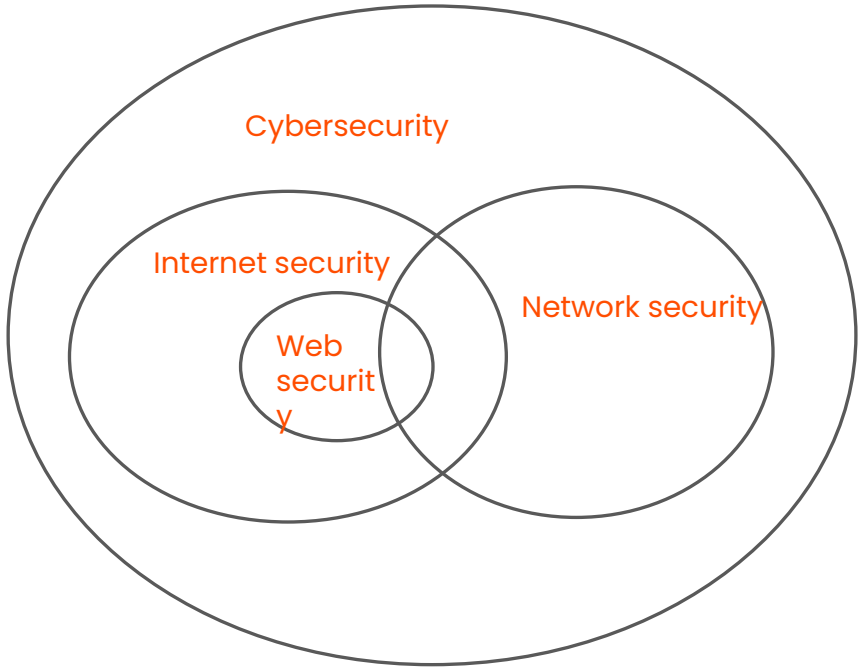
Internet es una red global conecta miles de millones de servidores, ordenadores y otros dispositivos de hardware. El intercambio de información en Internet también utiliza la red de telefonía móvil que, por tanto, forma parte de Internet.

Cada dispositivo está conectado con cualquier otro a través de su conexión a Internet. Internet crea un entorno propicio para compartir.

El objetivo de estos esfuerzos es reducir los riesgos de seguridad relacionados con Internet para las organizaciones, los clientes y otras partes interesadas.

La seguridad en Internet se ocupa de proteger los servicios relacionados con Internet y los sistemas y redes TIC relacionados como una extensión de la seguridad de la red.

La seguridad en Internet también garantiza la disponibilidad y fiabilidad de los servicios de Internet.



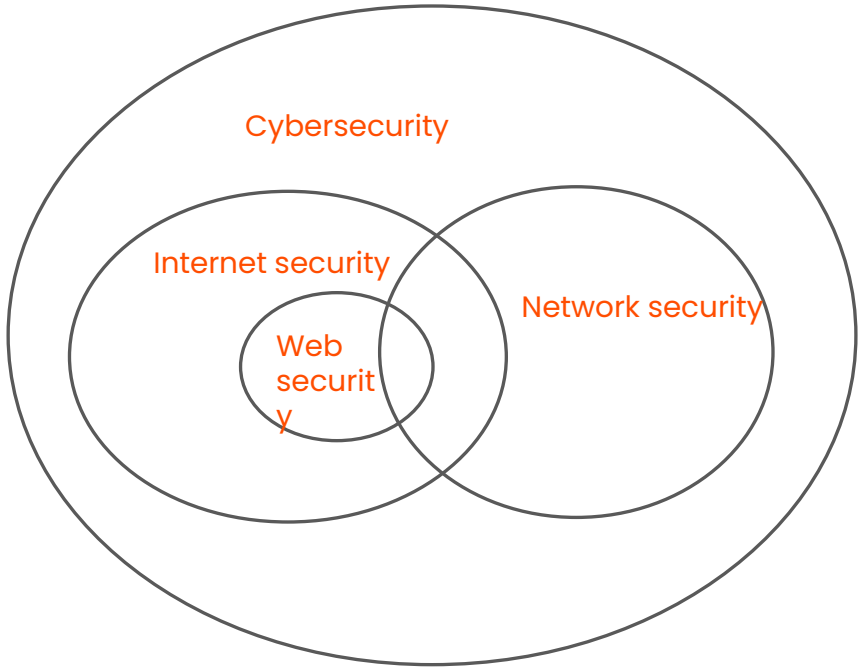
Relación Dominios Seguridad

En Internet se ofrecen diversos servicios, como los de transferencia de archivos, correo o cualquier otro que pueda compartirse públicamente con los usuarios finales. En este contexto, la seguridad en Internet se ocupa de la prestación segura de estos servicios a través de la red pública.

La web es una de las formas de compartir información en Internet otras son el correo electrónico, el protocolo de transferencia de archivos (FTP) y los servicios de mensajería instantánea.

La web está compuesta por miles de millones de documentos digitales conectados que pueden visualizarse mediante un navegador web.

La seguridad web se ocupa de la seguridad de la información en el contexto de la World Wide Web (WWW) y de los servicios web a los que se accede a través de la red pública.



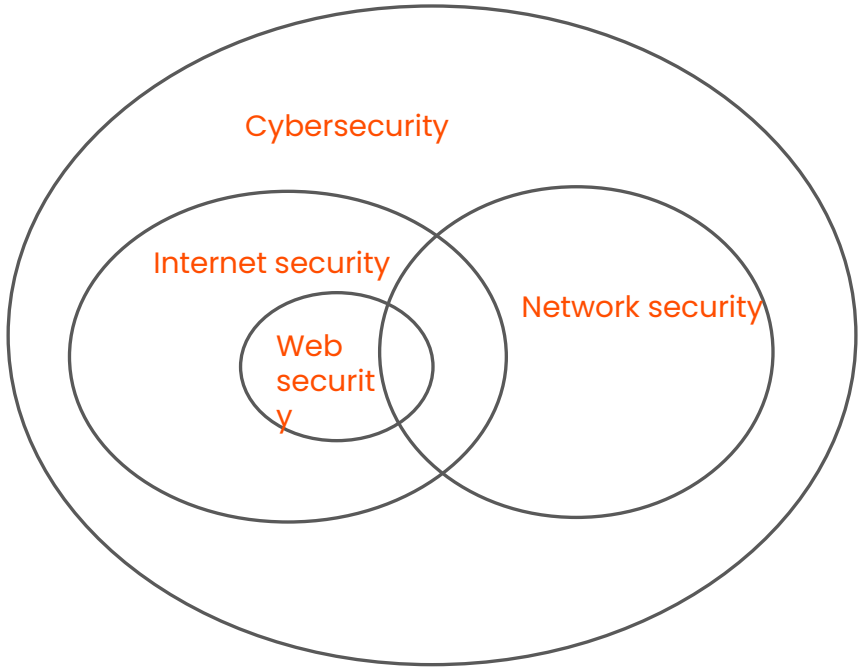
Relación Dominios Seguridad

La seguridad web también se ocupa de la seguridad de esta conexión HTTP utilizada para el intercambio de información.

Una red puede incluir componentes como routers, hubs, cableado, controladores de telecomunicaciones, centros de distribución de claves y dispositivos de control técnico.

La seguridad de las redes abarca en general todos los tipos de redes que existen en una organización, desde la red de área local, la red de área amplia, la red de área personal y las redes inalámbricas.

La seguridad de las redes se ocupa del diseño, la implantación, el funcionamiento y la mejora de las redes, así como de la identificación y el tratamiento de los riesgos de seguridad relacionados con las redes dentro de las organizaciones, entre organizaciones y entre organizaciones y usuarios.

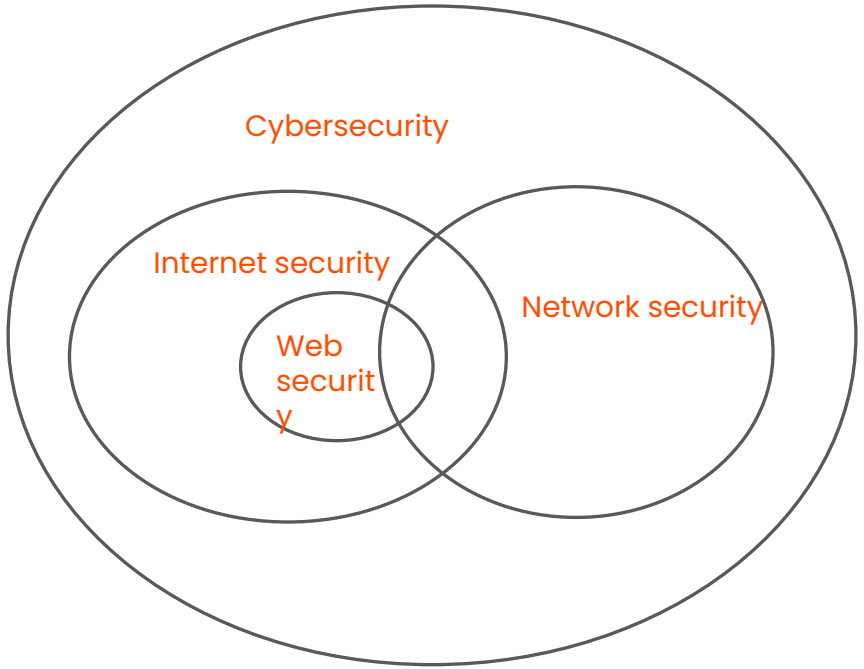


Relación Dominios Seguridad

La ciberseguridad se refiere a la gestión de los riesgos de seguridad de la información cuando ésta se encuentra en forma digital en ordenadores, almacenamiento y redes. Muchos de los controles, métodos y técnicas de seguridad de la información pueden aplicarse a la gestión de los ciber riesgos.

La ciberseguridad también se ocupa de proteger los sistemas conectados a Internet, incluidos el hardware, el software, los programas y los datos, frente a posibles ataques. Muchos de estos ataques se caracterizan por ser ataques dirigidos y combinados con un alto grado de sofisticación y persistencia.

Las amenazas pueden estar basadas en Internet y/o deberse a la conectividad con otras redes y sistemas dentro de la organización o de la red del cliente y del proveedor de servicios, con los que la organización se comunica durante el curso normal de sus actividades.



Ciberespacio

Que entendemos por Ciberespacio …

El ciberespacio es un entorno complejo que resulta de la interacción de personas, software y servicios en Internet, respaldado por tecnologías de Información y comunicación. (dispositivos conectados y redes distribuidas físicamente en todo el mundo).

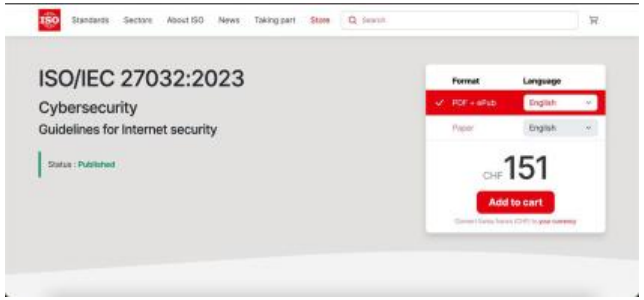
Ciberseguridad

Que entendemos por Ciberseguridad …

La ciberseguridad se refiere a la gestión de los riesgos de seguridad de la información cuando ésta se encuentra en forma digital en ordenadores, almacenamiento y redes.

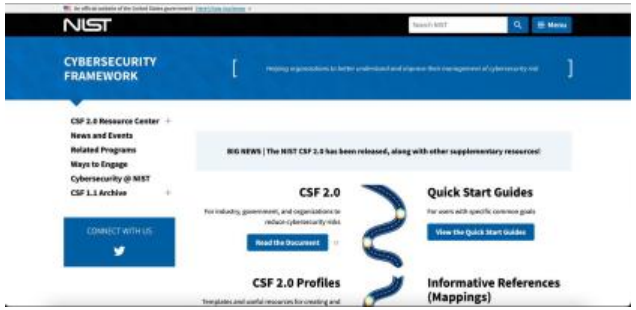
La ciberseguridad también se ocupa de proteger los sistemas conectados a Internet, incluidos el hardware, el software, los programas y los datos, frente a posibles ataques.

ISO 27032: 2023



https://www.iso.org/standard/76070.html

CSF NIST v 2.0



Seguridad en Internet

Visión general de la seguridad en internet.

La Información Personal Identificable (IPI) de los usuarios de Internet es captada por muchos sitios y servicios ofrecidos en la Red.

Entre ellos hay proveedores de servicios de aplicaciones que siguen de cerca las actividades de los usuarios y utilizan técnicas de **inteligencia artificial (IA)** para ofrecerles recomendaciones sobre compras, atención sanitaria, gestión del tiempo y un sinfín de comentarios con la intención de facilitarles la vida y las tareas. Muchos de estos sitios recopilan estos datos sin el permiso de los usuarios y los facilitan a terceros con fines lucrativos, también sin el conocimiento de los usuarios.

Las partes interesadas han ido estableciendo su presencia en Internet a través de sitios web, realizando comercio electrónico a escala mundial, prestando servicios digitales en Internet, utilizando servicios públicos en la nube para prestar servicios y utilizando aplicaciones y servicios empresariales basados en la web.

Seguridad en Internet

Muchos usos de Internet implican el intercambio de información y la prestación de servicios que no afectan a las personas ni a la **Información Personal Identificable** (IPI) . La IIP varía según la jurisdicción.

La seguridad de dicha información y servicios puede ser crítica para las partes interesadas. Además, la gama de hardware conectado a Internet ya sea como dispositivos individuales o como redes privadas, está aumentando rápidamente en la llamada Internet de las cosas.

La autonomía y la aplicación de la inteligencia artificial en la Internet de las cosas crean retos para la seguridad en Internet

Aunque Internet puede facilitar importantes resultados empresariales, siempre hay muchos riesgos de seguridad que hay que gestionar.

https://www.youtube.com/watch?v=HVHKYXJq7qo

Seguridad en Internet

Es importante recordar que Internet no se diseñó originalmente pensando en la seguridad.

Las organizaciones dependen en gran medida del uso de Internet para llevar a cabo sus actividades.

Debido al bajo nivel de confianza asociado a Internet, las operaciones empresariales pueden enfrentarse a importantes consecuencias adversas derivadas de la pérdida de **confidencialidad, integridad y disponibilidad** de la información y los servicios, si no se controlan adecuadamente.

Aunque algunos individuos son cuidadosos en la gestión de su identidad en línea, la mayoría de la gente sube detalles de sus perfiles personales para compartirlos con otros.

Seguridad en Internet

Los perfiles de muchos sitios, en particular las redes sociales y las salas de chat, pueden ser descargados y almacenados por terceros.

Esto puede dar lugar a la creación de un expediente digital de datos personales que puede utilizarse indebidamente, revelarse a otras partes o utilizarse para la recopilación secundaria de datos.

Aunque la exactitud e integridad de estos datos son cuestionables, crean vínculos con personas y organizaciones que a menudo no pueden borrarse por completo.

Estos avances en los ámbitos de la comunicación, el ocio, el transporte, las compras, las finanzas, los seguros y la asistencia sanitaria crean nuevos riesgos para las partes interesadas en Internet.

Así pues, la pérdida de privacidad en Internet puede conllevar riesgos.

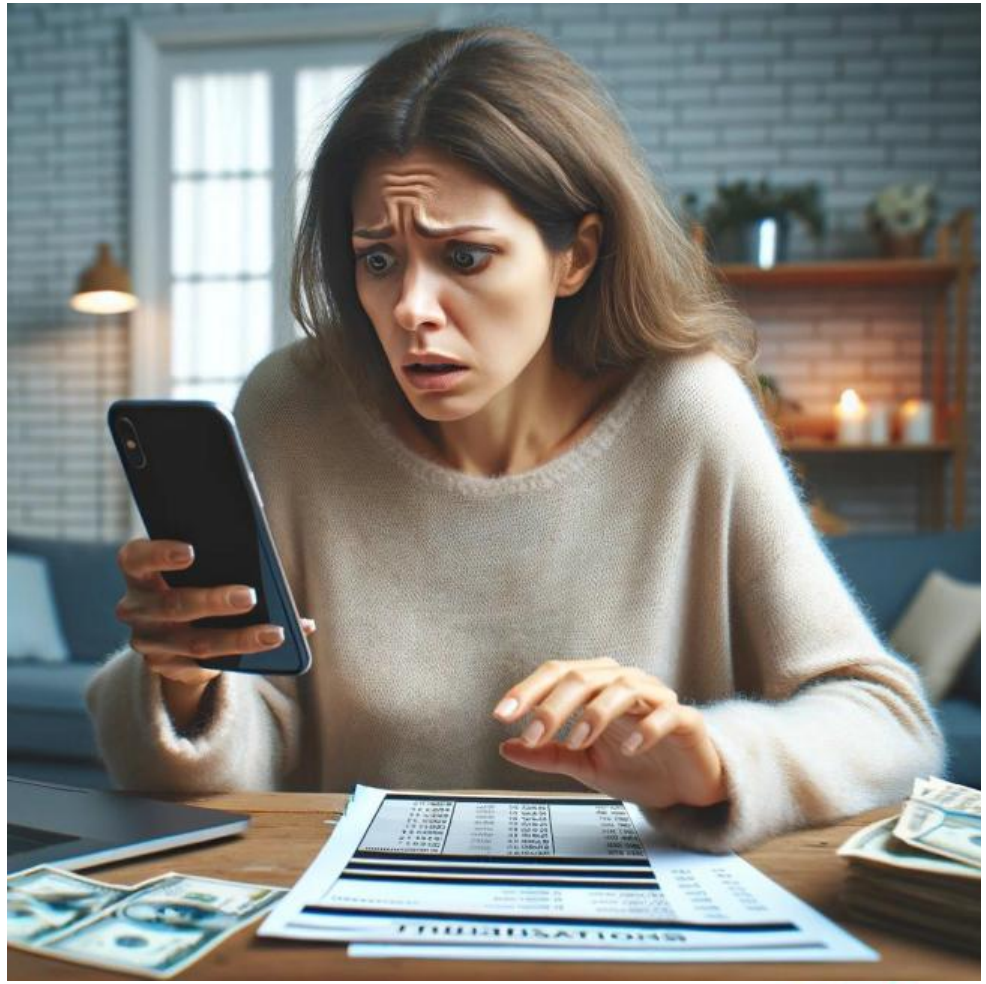
https://www.youtube.com/watch?v=izdDPlEmhJc

Seguridad en Internet

La convergencia de las tecnologías de la información y la comunicación, la facilidad para entrar en Internet desde ordenadores de sobremesa y portátiles hasta dispositivos móviles y de IoT, y el estrechamiento del espacio personal entre los individuos, están llamando la atención de los agentes maliciosos y las organizaciones delictivas.

Estas entidades están utilizando mecanismos como el **phishing**, el **spam** y el **spyware,** además de desarrollar técnicas de ataque como los ataques de **día cero,** el **vishing**, los sitios **web** maliciosos y otras técnicas de engaño para explotar cualquier punto débil que puedan descubrir en Internet.

En los últimos años, los ataques a la seguridad en Internet han evolucionado desde el pirateo por fama personal a la delincuencia organizada o ciberdelincuencia. Una plétora de herramientas y procesos antes observados en incidentes aislados de ciberseguridad se utilizan ahora juntos en ataques combinados múltiples, a menudo con objetivos maliciosos de gran alcance.



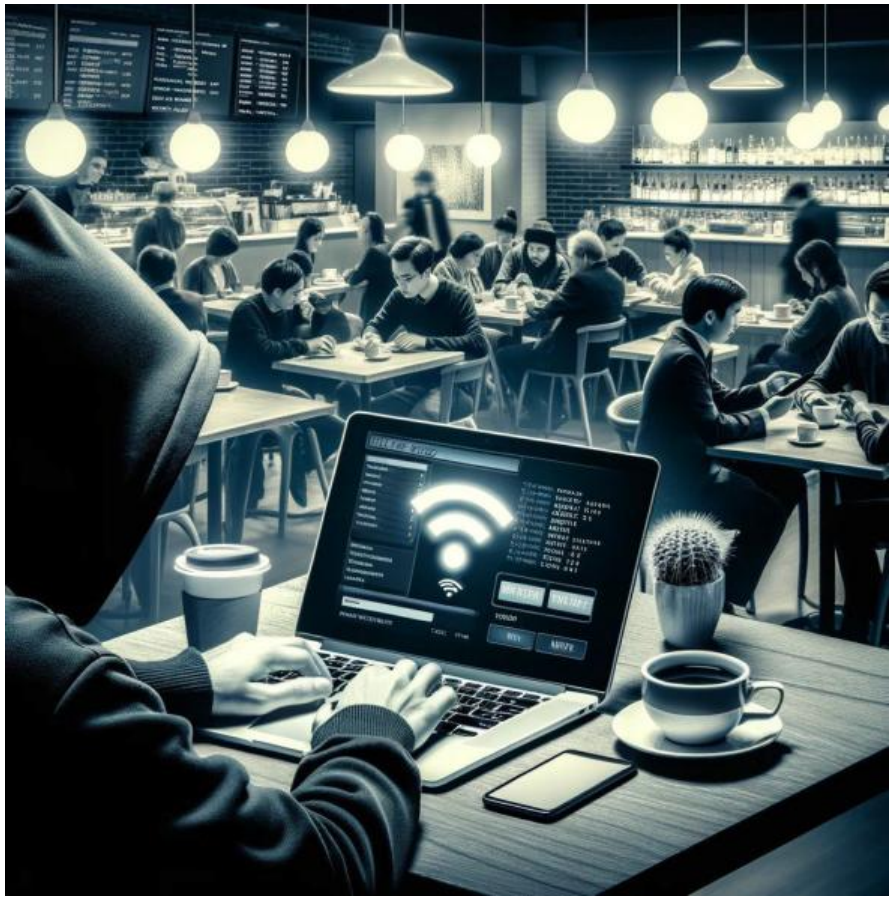
Seguridad en Internet

Muchas de estas herramientas también están disponibles en repositorios públicos de software y otros recursos de acceso público.

Los objetivos de un ataque van desde los ataques personales, la usurpación de identidad, los fraudes o robos financieros, hasta el **hacktivismo** y la manipulación de la información en Internet.

Muchos de los datos personales y de clientes robados también se ponen a disposición en la **red oscura**, que puede ser de acceso público.
Las organizaciones, y las PYME en particular, deben comprender las consecuencias reales de "manipular" información en Internet. Estos riesgos de seguridad son los ciber riesgos para los usuarios que acceden a Internet.

Como **Internet es una red pública mundial,** las transacciones pueden originarse en cualquier parte del mundo, al igual que los ataques.



Seguridad en Internet

Las múltiples modalidades de transacciones comerciales que se llevan a cabo en Internet se están convirtiendo en el objetivo de los sindicatos de la ciberdelincuencia. Los riesgos que se plantean son intrínsecamente complejos: de **empresa a empresa, de empresa a consumidor** y de **consumidor a consumidor.**

Otra complejidad se deriva del hecho de que todas las partes interesadas, incluso cuando no son malintencionadas, tienen una visión diferente de sus necesidades, requisitos y amenazas, por lo que tienen una lista diferente de riesgos y controles para contrarrestarlos. Esto significa que no existe una solución única.

Criterios como lo que constituye una transacción o un acuerdo dependen de los entornos jurídicos y normativos específicos de las distintas jurisdicciones.
Estos criterios también dependen de la interpretación de la ley y de cómo cada parte de la relación gestiona su responsabilidad.

Seguridad en Internet

A menudo, la cuestión del uso de los datos recopilados durante la transacción o la relación no se aborda adecuadamente.

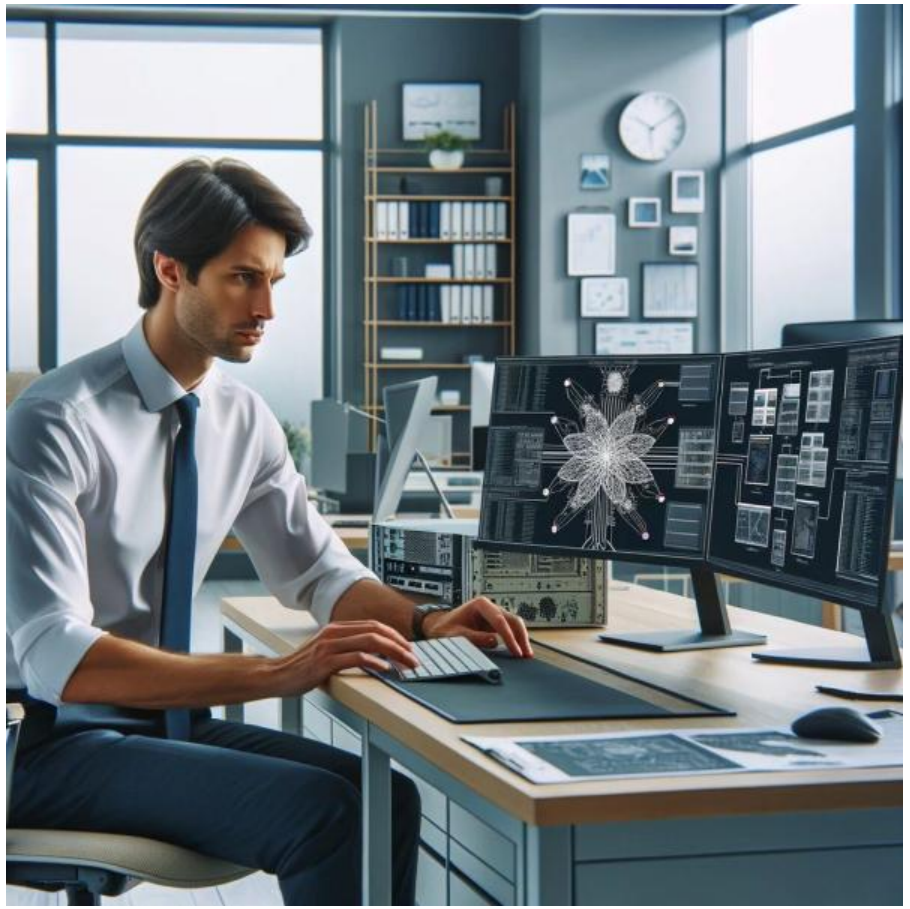
Esto puede acabar provocando problemas de seguridad, como la fuga de información.

Los retos jurídicos y técnicos que plantean estas cuestiones de Internet son de gran alcance y de naturaleza global.

Estos retos sólo pueden abordarse mediante la **colaboración entre la comunidad técnica** de la **seguridad de la información,** la comunidad jurídica y las distintas regiones para adoptar una **estrategia** coherente.

Esta estrategia debe tener en cuenta el papel de cada parte interesada y las iniciativas existentes, en un marco de cooperación internacional.

Seguridad en Internet



La información viaja por Internet de forma instantánea, lo que significa que los ataques también pueden producirse al instante.

Como estas velocidades no son fácilmente aprehensibles por la mente humana, el ataque siempre se descubre mucho tiempo después de haberse producido, y los daños ya son potencialmente enormes.

En la mayoría de los casos, la identidad de los atacantes está oculta. Por ello, se propone con frecuencia el uso de la inteligencia artificial (IA) para contrarrestar los ataques.

Partes Interesadas Ciberespacio

Partes Interesadas

Las partes interesadas de la seguridad en Internet incluyen a quienes:

- Utilizan servicios a través de Internet.
- Utilizan Internet para prestar servicios.
- Proporcionan la infraestructura y las capacidades de comunicación de Internet.
- Coordinan globalmente el funcionamiento de Internet.
- Proporcionan y aplican leyes y reglamentos.

Las partes interesadas en la seguridad de Internet pueden clasificarse en **Usuarios, Coordinadores y Organizaciones de estandarización, Autoridades gubernamentales, Organismos encargados de hacer cumplir la ley y Proveedores de servicios de Internet.**

Usuarios

Estandarización

Gobierno

Legal

Proveedores

Partes Interesadas Ciberespacio

Usuarios

Usuarios es un término que hace referencia a individuos, usuarios finales, así como a organizaciones privadas y públicas que utilizan Internet.
Entre las organizaciones privadas se incluyen las pequeñas y medianas empresas (PYME), así como las grandes empresas.

La Administración y otros organismos públicos se denominan colectivamente organizaciones públicas.

Un individuo o una organización se convierte en usuario cuando accede a Internet o a cualquier servicio disponible a través de Internet.
Los usuarios pueden hacer uso de los servicios de Internet, ver o recopilar información.

También pueden proporcionar cierta información específica que está dentro del espacio de una aplicación, o abierta a miembros o grupos limitados dentro del espacio de la aplicación, o al público en general.

Partes Interesadas Ciberespacio

Los roles de usuario pueden incluir, entre otros, los siguientes...

- **Usuario general** de aplicaciones de Internet, o usuario general, como jugador de juegos en línea, usuario de mensajería instantánea o internauta;
- **Comprador/vendedor,** que participa en la colocación de bienes y servicios en sitios de subastas y mercados en línea para compradores interesados, y viceversa.
- **Blogger** y otros contribuidores de contenidos (por ejemplo, un autor de un artículo en una wiki), en los que se publica información en texto y multimedia (por ejemplo, videoclips) para consumo del público en general o de una audiencia limitada;
- **Miembro de una organización** (por ejemplo, empleado de una empresa, u otra forma de asociación con una empresa);
- **Otros roles,** por los que a un usuario se le puede asignar un rol involuntariamente o sin su consentimiento.

Partes Interesadas Ciberespacio

EJEMPLO 1:
Cuando un usuario visita un sitio que requiere autorización y, de forma intencionada o no, consigue acceder a él, puede ser calificado de intruso.

EJEMPLO 2:
Un individuo, actuando como comprador o vendedor, puede participar sin saberlo en transacciones delictivas de venta de bienes robados o en actividades de blanqueo de dinero.

Las organizaciones suelen utilizar Internet para dar a conocer la empresa e información relacionada, así como para comercializar productos y servicios relacionados.

Las organizaciones también utilizan Internet como parte de su red para la entrega y recepción de mensajes electrónicos (por ejemplo, correos electrónicos) y otros documentos (por ejemplo, transferencia de archivos)

Partes Interesadas Ciberespacio

Las organizaciones suelen utilizar Internet para dar a conocer la empresa e información relacionada, así como para comercializar productos y servicios relacionados.

Las organizaciones también utilizan Internet como parte de su red para la entrega y recepción de mensajes electrónicos (por ejemplo, correos electrónicos) y otros documentos (por ejemplo, transferencia de archivos).

En línea con los mismos principios de ser un buen ciudadano corporativo, estas organizaciones deberían extender sus responsabilidades corporativas a Internet asegurándose proactivamente de que sus prácticas y acciones en el uso de Internet no introducen más riesgos de seguridad en la comunidad de usuarios de Internet.

Partes Interesadas Ciberespacio

Algunas medidas proactivas son:

- Gestión de la seguridad de la información mediante la implantación y el funcionamiento de un sistema eficaz de gestión de la seguridad de la información (SGSI) para los requisitos de los sistemas de gestión de la seguridad de la información).

- Aplicación de controles basados en la norma ISO/IEC 27002 y otras normas pertinentes, sin aplicar un SGSI.

- Supervisión de la seguridad y respuesta a incidentes;

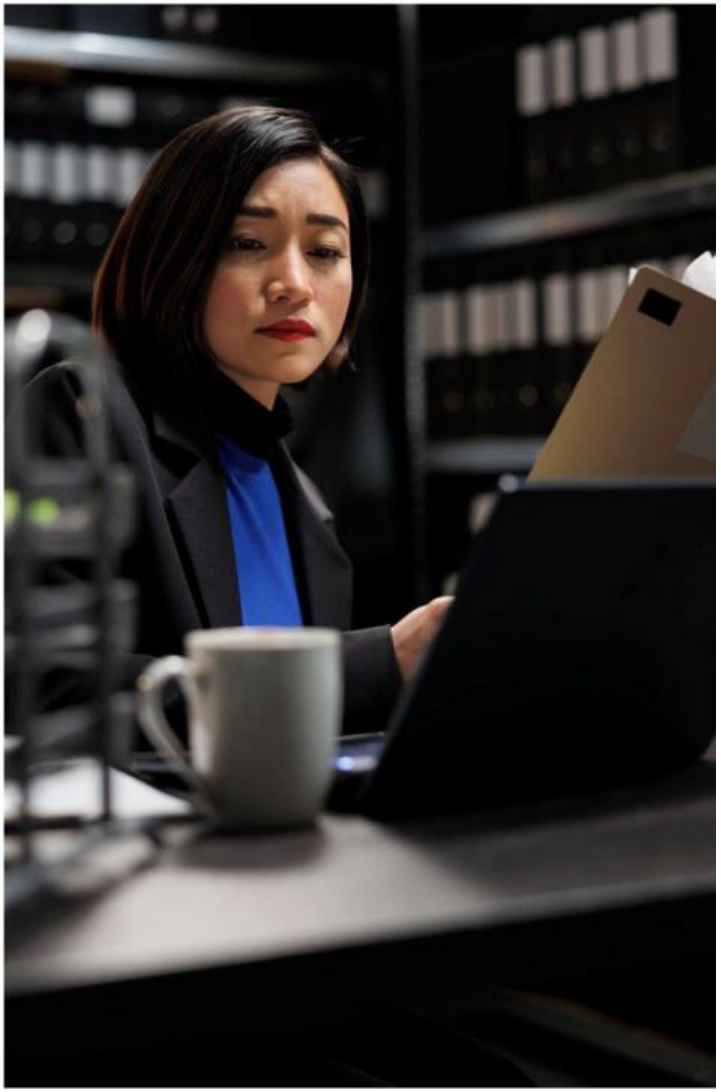
Partes Interesadas Ciberespacio

- Incorporación de la seguridad como parte del ciclo de vida de desarrollo de software (SDLC), en el que el nivel de seguridad incorporado a los sistemas debe determinarse en función de la criticidad de los datos de la organización;

- Formación periódica de los usuarios de la organización en materia de seguridad, mediante actualizaciones continuas de la tecnología y los procesos y el seguimiento de los últimos avances tecnológicos; y

- Comprender y utilizar los canales adecuados para comunicarse con los vendedores y proveedores de servicios sobre los problemas de seguridad descubiertos durante el uso.

Partes Interesadas Ciberespacio



Coordinadores y Organizaciones de estandarización

Las organizaciones de coordinación y normalización (ICANN, IETF, W3C, etc.) elaboran normas técnicas sobre el uso de Internet y los servicios que prestan los proveedores de servicios.

Asesoran a las organizaciones sobre sus funciones y responsabilidades en Internet.

https://www.icann.org/es

https://www.ietf.org/

https://www.w3.org/

Partes Interesadas Ciberespacio

Autoridades de Gobierno

Los gobiernos poseen información sobre seguridad nacional, cuestiones estratégicas, militares y de inteligencia, entre otros muchos elementos relacionados con el gobierno y el Estado, pero también un vasto conjunto de información sobre individuos, organizaciones y la sociedad en su conjunto.

Los gobiernos deben proteger la infraestructura y la información de su propio país del acceso y la explotación no autorizados.

Existe una tendencia creciente y en expansión de ofrecer servicios de administración electrónica utilizando Internet.

Este es un nuevo canal, entre otros, para lanzar ataques y acceder a la información antes mencionada que, de tener éxito, puede resultar en un grave impacto para una región, su gobierno y la sociedad.

Partes Interesadas Ciberespacio

Las autoridades gubernamentales desempeñan un papel de coordinación entre las fuerzas de seguridad y son el principal coordinador para difundir la información y orquestar los recursos necesarios, tanto a nivel nacional como corporativo, en momentos de crisis derivados de un ciberataque masivo.

Esto incluye también a autoridades como **CERT** y organizaciones similares a las que se encomiendan tales responsabilidades dependiendo de la región específica en contexto.

Los gobiernos ordenan programas de educación en ciberseguridad para universidades y escuelas secundarias, y garantizan que se organice una asociación público-privada adecuada con la estructura legal necesaria, que organice los organismos encargados de hacer cumplir la ley y defina sus misiones.

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

https://www.cisa.gov/

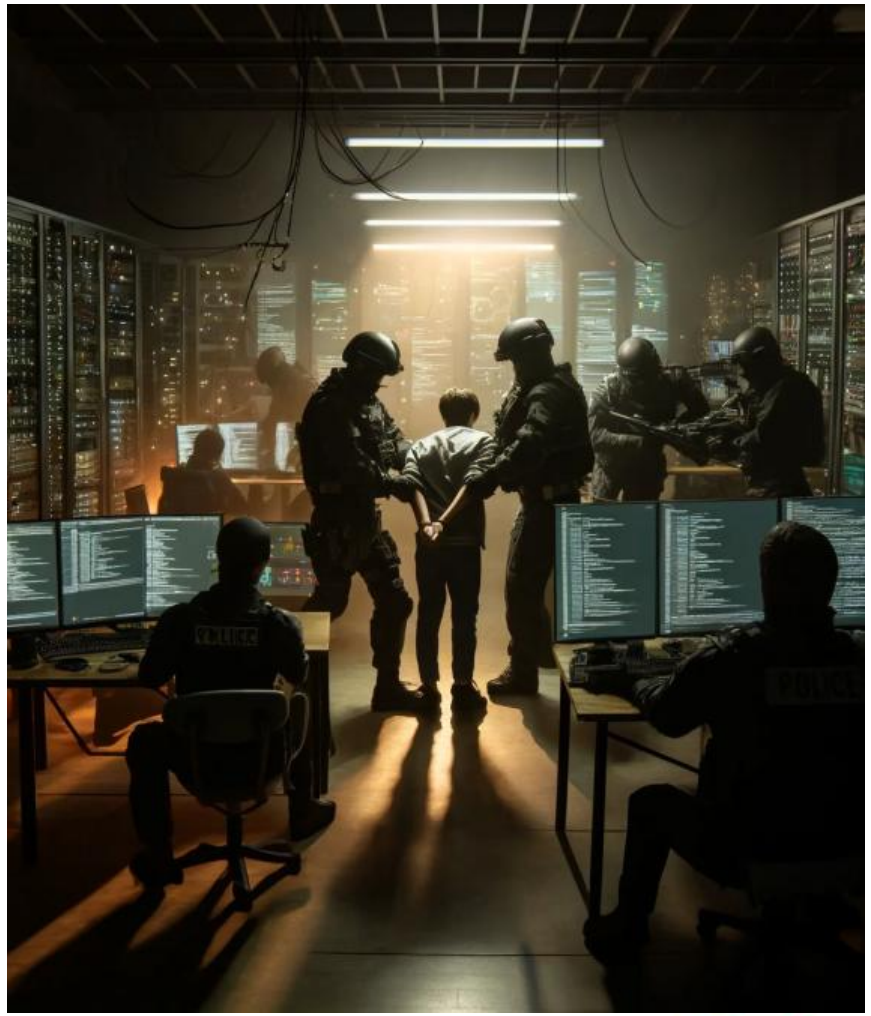
enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

https://www.enisa.europa.eu/about-enisa/about/es

Partes Interesadas Ciberespacio

Organismos encargados de hacer cumplir la ley

Los organismos encargados de la aplicación de la ley hacen cumplir la normativa y exigen responsabilidades a todas las partes interesadas en cuanto al cumplimiento de la normativa pertinente dentro de su jurisdicción nacional.



https://www.fbi.gov/

https://www.interpol.int/es/

https://www.oas.org/en/

Partes Interesadas Ciberespacio

Proveedores de Servicios de Internet

Las organizaciones proveedoras de servicios pueden incluir dos categorías

- Proveedores de acceso a Internet para empleados y socios;
- Proveedores de servicios a consumidores de Internet.

Estos servicios se prestan bien a una comunidad cerrada (por ejemplo, usuarios registrados), bien al público en general, mediante la entrega de aplicaciones, incluidos los proveedores de servicios en la nube, a través de Internet.

Un consumidor también puede ser un proveedor de servicios, si a su vez presta un servicio a través de Internet o permite a otro consumidor acceder a Internet.

Los proveedores de servicios también pueden entenderse como transportistas o mayoristas, frente a los distribuidores y minoristas de servicios de acceso.
Esta distinción es importante desde el punto de vista de la seguridad y, especialmente, de la aplicación de la ley.

Partes Interesadas Ciberespacio

Proveedores de Servicios de Internet

En caso de que un distribuidor o minorista sea incapaz de proporcionar una seguridad adecuada o un acceso legal, los servicios de apoyo suelen volver al transportista o mayorista.

Los proveedores de servicios de Internet (ISP) pueden prestar apoyo supervisando el "tráfico" y proporcionando rutas alternativas o hosts para el control del tráfico. También pueden buscar transferencias "peligrosas" a través de Internet.

Con las autorizaciones legales necesarias y las de los usuarios, pueden filtrar lo que es peligroso, como ocurre con las soluciones que proporcionan "cajas de arena" para verificar los archivos transferidos en busca de malware.

Los ISP pueden avisar a sus clientes cuando descubran patrones de amenazas.

Evaluación y tratamiento de los riesgos para la seguridad en Internet ISO 27032

LCSPC™ Versión 062024

Gestión de Riesgos en Internet

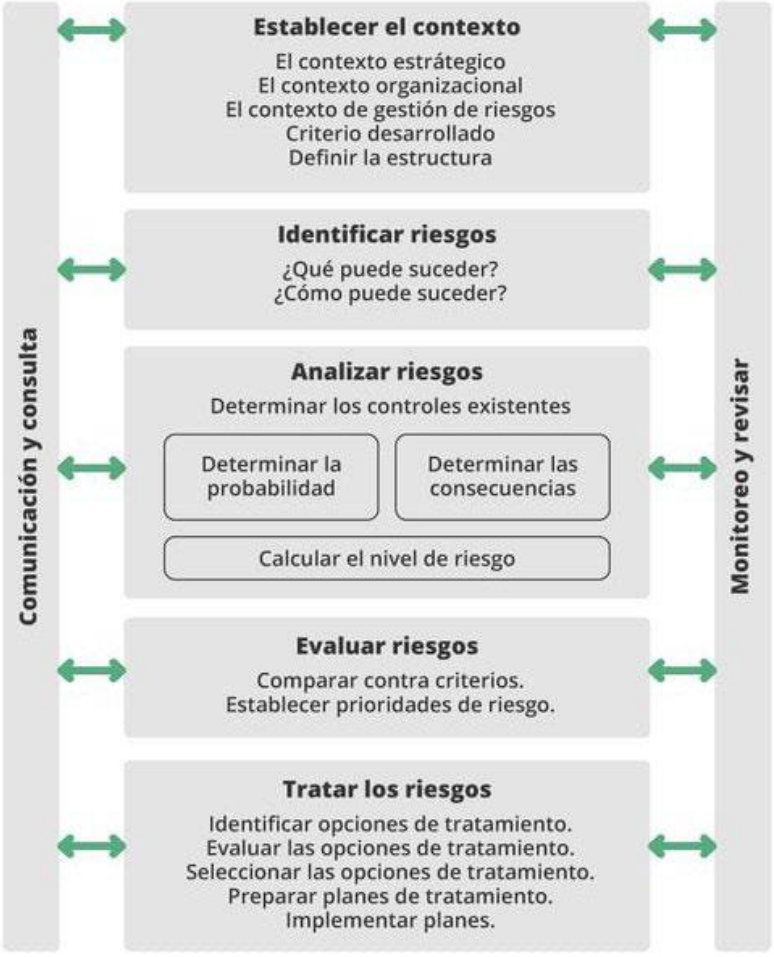
Evaluación y tratamiento de los riesgos para la seguridad en Internet

ISO 31000 proporciona principios y directrices genéricas sobre la gestión de riesgos, mientras que ISO/IEC 27005 proporciona directrices y procesos para la gestión de riesgos de seguridad de la información en una organización, apoyando los requisitos de un SGSI según ISO/IEC 27001.

Las directrices y procesos que proporcionan estos documentos se recomiendan para abordar la gestión de riesgos en el contexto de Internet.

Es responsabilidad de las partes interesadas definir su enfoque para la gestión de riesgos. Se pueden utilizar varias metodologías existentes bajo el marco descrito en ISO/IEC 27005 para llevar a cabo una evaluación de riesgos y gestionar los riesgos asociados con el uso de Internet por parte de la organización, teniendo en cuenta las amenazas y vulnerabilidades relevantes y los problemas de seguridad de Internet.

En las organizaciones que disponen de recursos limitados, los controles deben tener en cuenta la racionalidad entre las necesidades organizativas de seguridad y los recursos para evitar errores en la selección de los controles.



Gestión de Riesgos en Internet

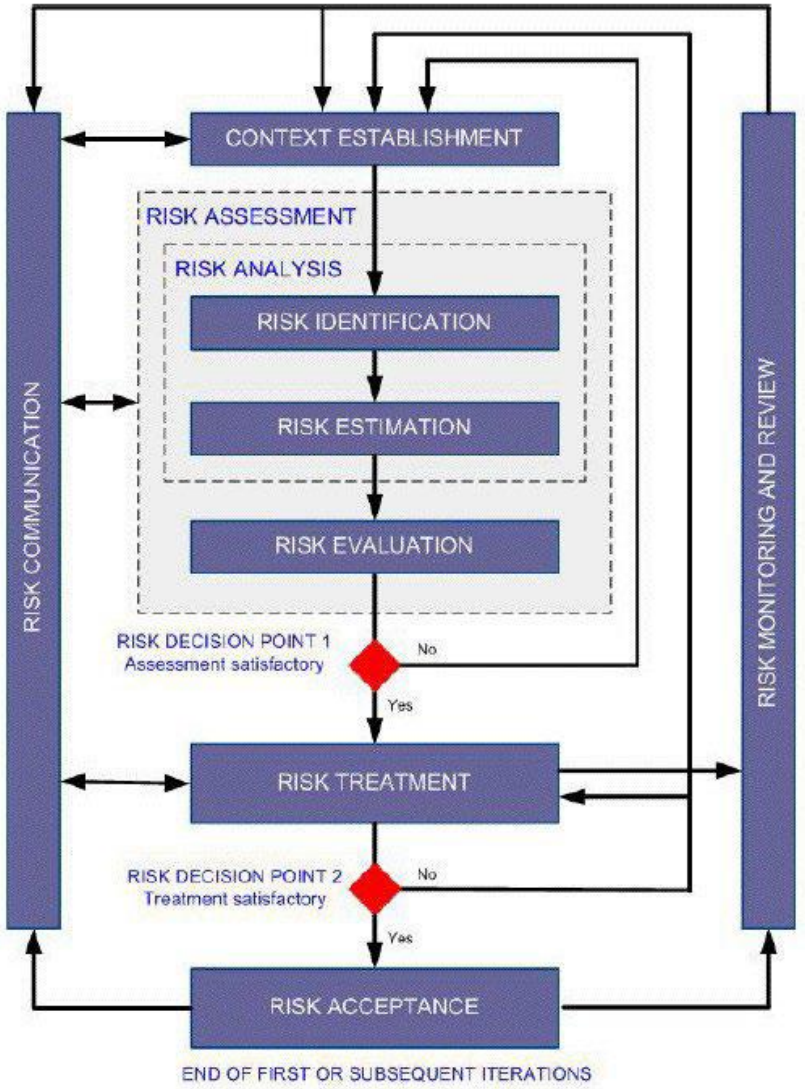
Amenazas

Un agente de amenaza es un individuo o grupo de individuos que desempeñan algún papel en la ejecución o apoyo de un ataque.

Comprender a fondo sus motivos (religiosos, políticos, económicos, etc.), capacidades (conocimientos, financiación, tamaño, etc.) e intenciones (diversión, crimen, espionaje, etc.) es fundamental en la evaluación de vulnerabilidades y riesgos, así como en el desarrollo y despliegue de controles.

Los programas maliciosos pueden poner en peligro los controles de seguridad (por ejemplo, la captura y divulgación de contraseñas), la divulgación involuntaria de información, los cambios involuntarios en la información, la destrucción de información y/o el uso no autorizado de los recursos del sistema.

Los programas maliciosos suelen propagarse a través de virus, gusanos y troyanos, con consecuencias de gran alcance.



Gestión de Riesgos en Internet

Un virus es un programa ejecutable y replicable que inserta su propio código en programas legítimos con el objetivo de dañar el ordenador anfitrión (es decir, borrar archivos y programas, corromper el almacenamiento y los sistemas operativos).

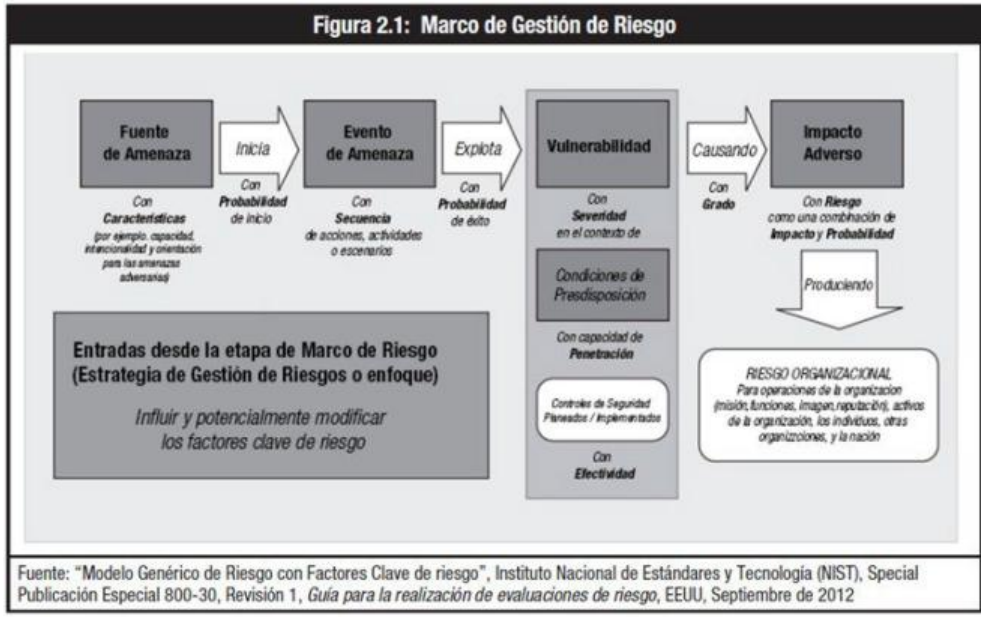


Figura 2.1: Marco de Gestión de Riesgo

Fuente: "Modelo Genérico de Riesgo con Factores Clave de riesgo", Instituto Nacional de Estándares y Tecnología (NIST), Special Publicación Especial 800-30, Revisión 1, *Guía para la realización de evaluaciones de riesgo*, EEUU, Septiembre de 2012

En su estado más simple, un gusano es un programa informático destinado a autorreplicarse y propagarse a otros ordenadores a través de mensajes salientes a todas las direcciones de la lista de contactos de un usuario para agotar los recursos de un sistema. Además, de igual que un virus, un gusano puede propagar código que puede dañar a su anfitrión. Dicho código se denomina carga útil (por ejemplo, la capacidad de cifrar archivos en el ransomware y la instalación de puertas traseras del sistema que permiten el acceso remoto).

Un troyano es un programa malicioso disfrazado de software legítimo o incrustado en él que tiene objetivos similares a los de los virus y gusanos, pero que, a diferencia de éstos, no se replica ni propaga por sí mismo.

Gestión de Riesgos en Internet

Las amenazas a la seguridad en Internet para la **Información Personal Identificable (IPI)** de los usuarios de Internet giran principalmente en torno a los problemas de identidad, planteados por la filtración o el robo de información personal. Si la identidad en línea de una persona es robada o enmascarada, la persona puede verse privada de acceso a servicios y aplicaciones clave.

En escenarios más graves, las consecuencias pueden ir desde incidentes financieros hasta incidentes a nivel nacional.

El acceso no autorizado a la información financiera de una persona también abre la posibilidad de robo de su dinero y fraude.

EJEMPLO 1: La información crediticia puede venderse en el mercado negro o darknet, lo que puede facilitar el robo de identidad en línea.

Gestión de Riesgos en Internet

EJEMPLO 2: Otros ejemplos de amenazas que a su vez equivalen a amenazas para la vida incluyen el ciberacoso, el acoso en línea y los delitos de explotación, incluida la explotación infantil y la trata de seres humanos.

Otra amenaza es la posibilidad de que el endpoint, incluidos los dispositivos personales y Bring Your Own Device (BYOD), se convierta en un zombi o un bot. Los dispositivos informáticos pueden verse comprometidos y pasar a formar parte de una red de bots mayor.
La presencia en línea y el negocio en línea de una organización son a menudo el objetivo de malhechores cuya intención es algo más que una simple travesura.

A mayor escala, la infraestructura que sustenta Internet también puede ser objeto de ataques. Aunque esto no afecta al funcionamiento de Internet de forma permanente, sí afecta a la fiabilidad y disponibilidad de la infraestructura, lo que contribuye a la seguridad de Internet.

Gestión de Riesgos en Internet

A nivel nacional o internacional, Internet es un ámbito en el que prosperan los comportamientos ilegales en una jurisdicción determinada.

Debido a la naturaleza de Internet, y concretamente a los retos que plantea la definición de límites y fronteras, resulta difícil regular y controlar la forma en que puede utilizarse.

Los delincuentes pueden comprar legítimamente las aplicaciones, los servicios y los recursos que facilitan su causa, o pueden recurrir a medios ilegales de asegurar estos recursos para evitar ser detectados y rastreados.

Esto puede incluir la adquisición de recursos informáticos masivos a través de botnets.

Otra amenaza se refiere a la modificación deliberada de la información disponible públicamente o sujeta a derechos de propiedad, o la creación de información falsa y bulos que, si se confía en ellos, pueden generar graves daños.

Gestión de Riesgos en Internet

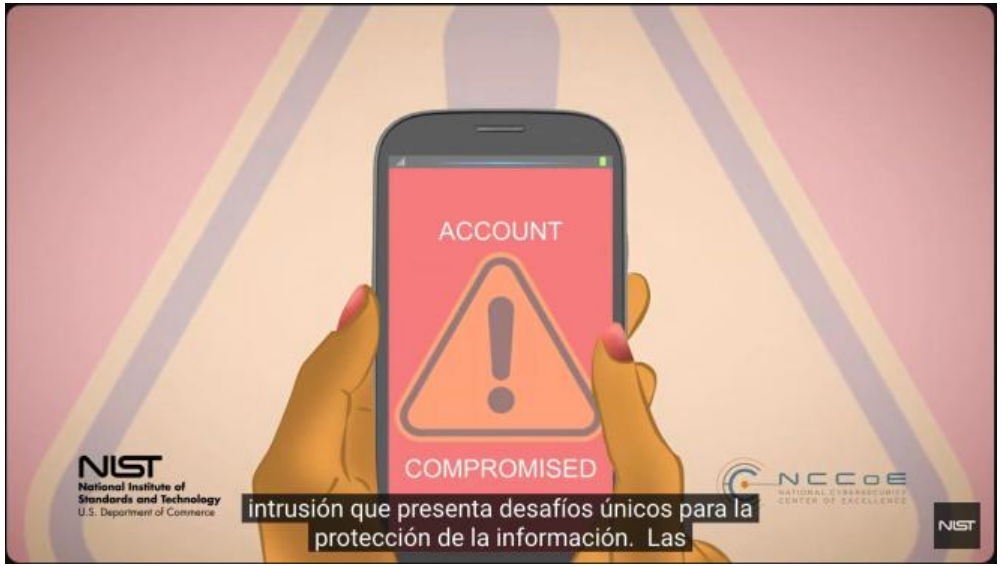
Vulnerabilidades

Las vulnerabilidades son puntos débiles de un activo o control que pueden ser explotados por una amenaza.

Los fabricantes, desarrolladores de software y otros creadores de tecnología producen actualizaciones y parches de seguridad para corregir estas debilidades una vez que se han encontrado y solucionado.

A medida que los sistemas reciben parches, se añaden actualizaciones o nuevos elementos. A medida que los sistemas quedan obsoletos o no reciben soporte del fabricante o no se parchean a la última versión, pueden introducirse nuevas vulnerabilidades.

Las partes interesadas deben tener un profundo conocimiento y comprensión del activo o control en cuestión, así como de las amenazas, agentes de amenaza y riesgos implicados, con el fin de realizar una evaluación exhaustiva.



https://www.youtube.com/watch?v=BLBcz2Qet2E

Gestión de Riesgos en Internet

Las partes interesadas deben ser conscientes de las vulnerabilidades de día cero para las que no hay parche disponible.

Las aplicaciones web a las que se accede a través de Internet son susceptibles de sufrir una serie de vulnerabilidades introducidas por un diseño deficiente, un código mal escrito y unas bibliotecas y ejecutables de producción mal construidos.

Ejemplos de estas vulnerabilidades son el bypass de autenticación, los ataques de inyección en bases de datos y los ataques de scripting entre sitios.

En estos ataques, las peticiones pueden manipularse para abusar del servidor web riesgos implicados, con el fin de realizar una evaluación exhaustiva.

Gestión de Riesgos en Internet

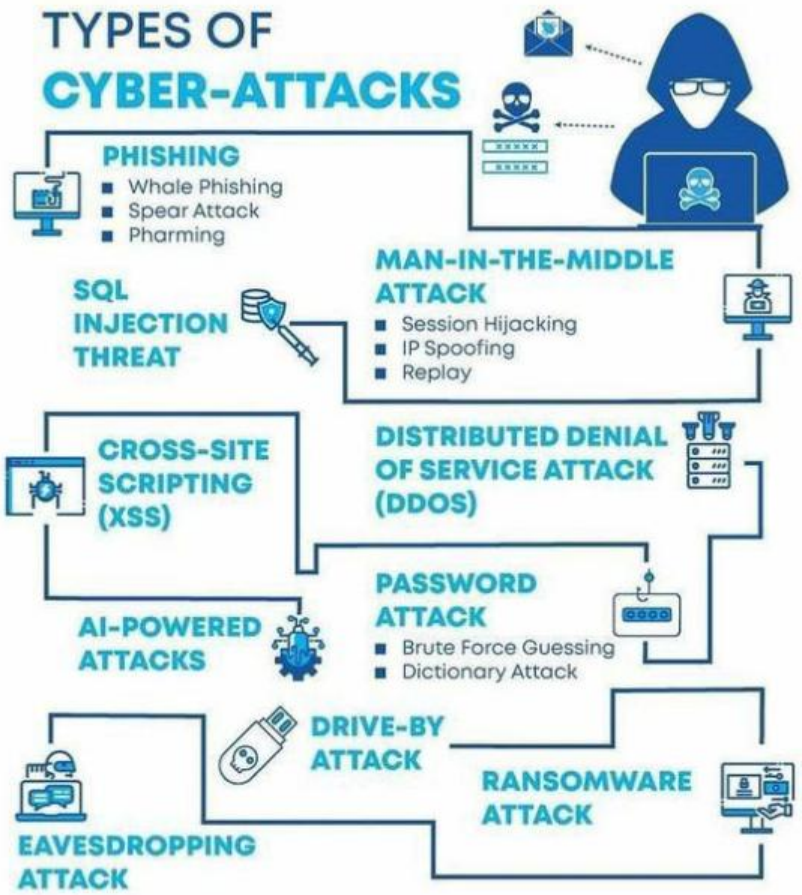
Vectores de Ataque

Un vector de ataque es un camino o medio por el cual un atacante puede obtener acceso a un ordenador o servidor de red con el fin de entregar un resultado malicioso. Los escáneres de puertos son una de las herramientas más antiguas y todavía muy eficaces utilizadas por los atacantes.

Escanean todos los puertos disponibles en el sistema orientado a Internet para confirmar qué puertos están abiertos. Normalmente, este es uno de los primeros pasos que ejecuta un posible atacante en el sistema objetivo orientado a Internet.

Aunque el ataque inicial siempre tiene como objetivo un sistema de cara al público (por ejemplo, un router, un servidor, un cortafuegos, un sitio web, etc.), los atacantes también pueden tratar de explotar los activos que residen dentro de la red privada y que están conectados a estos sistemas de cara al público.

Escuchar los canales de comunicación es un vector de ataque simple y fácil. También es uno de los más antiguos. Copiar y analizar el tráfico puede ser extremadamente valioso para detectar puntos de entrada e iniciar otros vectores de amenaza.



Gestión de Riesgos en Internet

Un atacante también puede utilizar el secuestro de comunicaciones (mediante tailgating o piggy-backing) y camuflarse tras la identidad o las credenciales, y a expensas del usuario legítimo sin que éste lo sepa.

Muchos de los ataques en Internet se llevan a cabo mediante software malicioso, como programas espía, gusanos y virus. A menudo, la información se obtiene mediante técnicas de phishing.

Un ataque puede producirse como un vector de ataque singular o llevarse a cabo como un ataque combinado o un ataque dirigido.

Estos ataques pueden propagarse, por ejemplo, a través de sitios web sospechosos, descargas no verificadas, correos electrónicos de spam, explotación remota, explotación de día cero y medios extraíbles infectados.

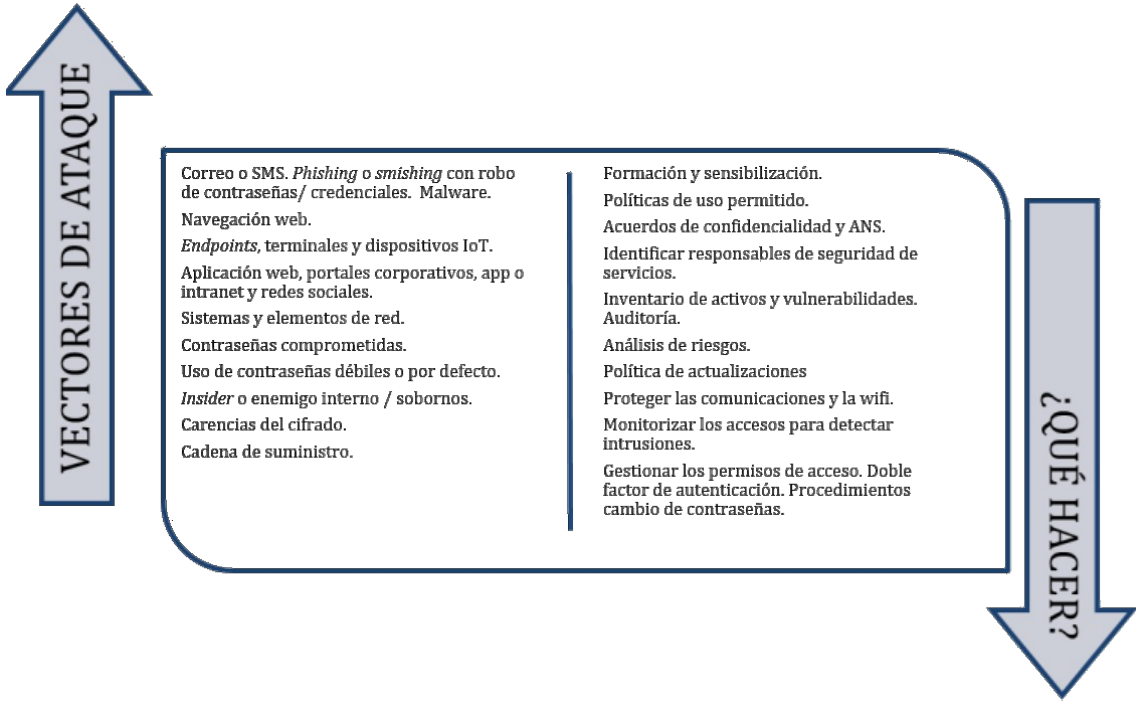
Gestión de Riesgos en Internet

Otros mecanismos cada vez más utilizados y sofisticados para llevar a cabo ataques son los basados en sitios web de redes sociales y el uso de archivos dañados en sitios web legítimos.

Los sitios web legítimos también pueden ser pirateados y algunos de sus archivos corrompidos y utilizados como medio para perpetrar ataques. Las personas tienden a confiar implícitamente en los sitios web que visitan habitualmente.

Los atacantes pueden aplicar la técnica de la charca para comprometer a un grupo específico de usuarios finales infectando los sitios web visitados con frecuencia.

Además de los ataques lanzados por atacantes humanos, los ordenadores infectados con malware también lanzan diversos ataques a los ordenadores conectados circundantes.



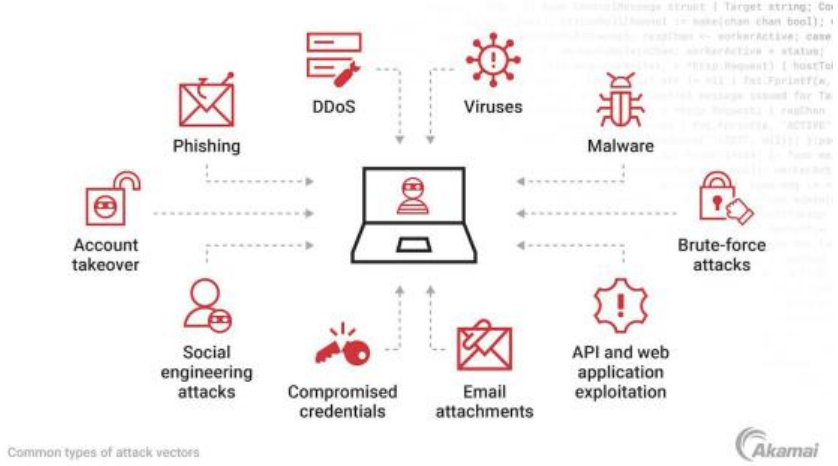
Gestión de Riesgos en Internet

Con la proliferación de las aplicaciones peer-to-peer, utilizadas habitualmente para compartir archivos como música digital, vídeo, fotos, etc., los atacantes son cada vez más sofisticados a la hora de camuflarse y disfrazar su código malicioso utilizando los archivos intercambiados como troyano para sus ataques.

Otra técnica es la suplantación de IP, en la que el atacante manipula la dirección IP asociada a sus mensajes en un intento de disfrazarla de fuente conocida y de confianza, obteniendo así acceso no autorizado a los sistemas

El atacante no utiliza siempre el mismo vector de ataque. Utiliza múltiples vectores y los cambia con frecuencia. Algunos ataques se ocultan hasta tal punto que no se detectan hasta que ya es demasiado tarde para el usuario.

Los defensores deben tener esto en cuenta y buscar defensa contra múltiples vectores y no sólo contra los que ya se han utilizado contra ellos. Los dispositivos IoT, teléfonos inteligentes, etc. pueden estar conectados a Internet.



Common types of attack vectors

Gestión de Riesgos en Internet

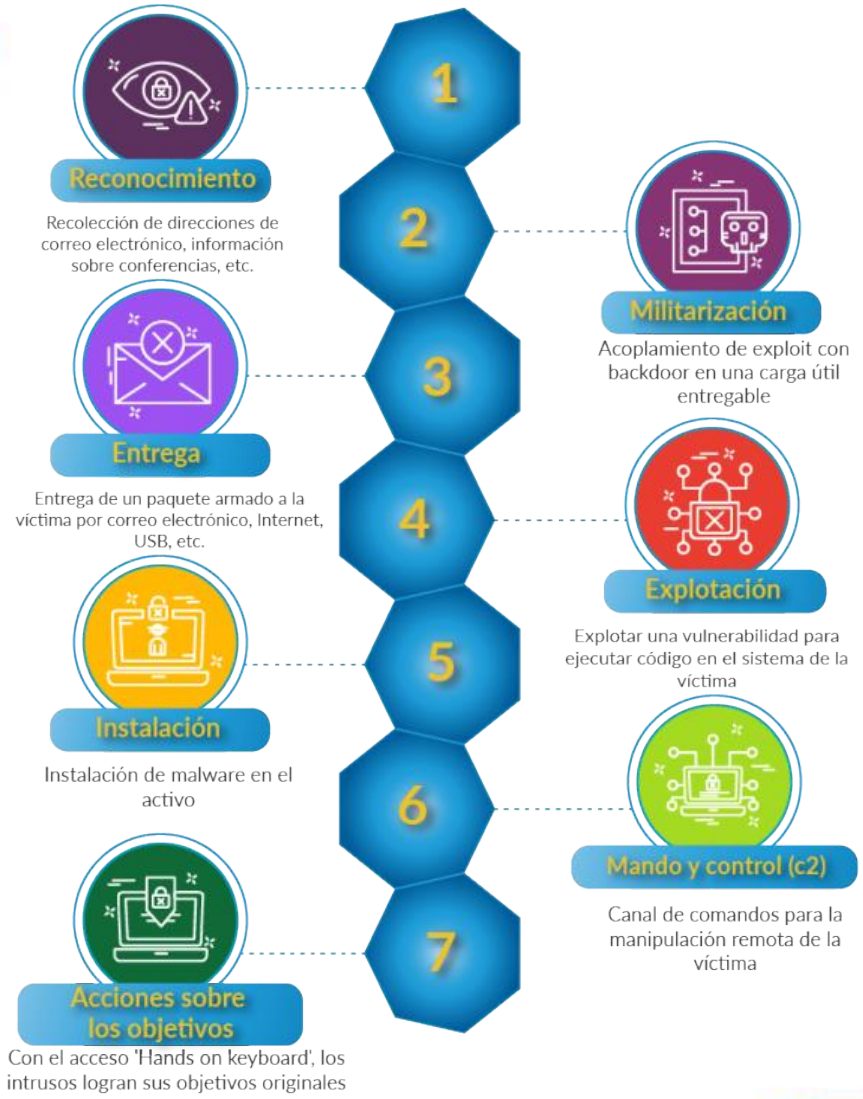
Estos dispositivos pueden actuar como un vector de ataque adicional al igual que cualquier otro dispositivo conectado a Internet, si no se controlan adecuadamente cuando están conectados a la red de la organización.

Una **amenaza persistente avanzada (APT)** es un método de ataque con el objetivo de robar información durante un largo periodo de tiempo por el que los atacantes obtienen acceso continuo a la red de una organización, se establecen sin ser detectados, se mueven lateralmente, buscan, aprenden y permanecen en la red.

Otro método de ataque antiguo es la fuerza bruta.

Este método utiliza el método de ensayo y error para adivinar las credenciales de inicio de sesión, las claves de cifrado, la búsqueda de páginas web ocultas, etc.

Los atacantes trabajan a través de todas las combinaciones posibles con la esperanza de adivinar correctamente para obtener acceso a la red y a la información de una organización.



ENISA Evaluatión Tool

National Cybersecurity Strategies Evaluation Tool

ENISA creó esta herramienta para ayudar a los Estados miembros a evaluar sus prioridades y objetivos estratégicos relacionados con las Estrategias Nacionales de Ciberseguridad.

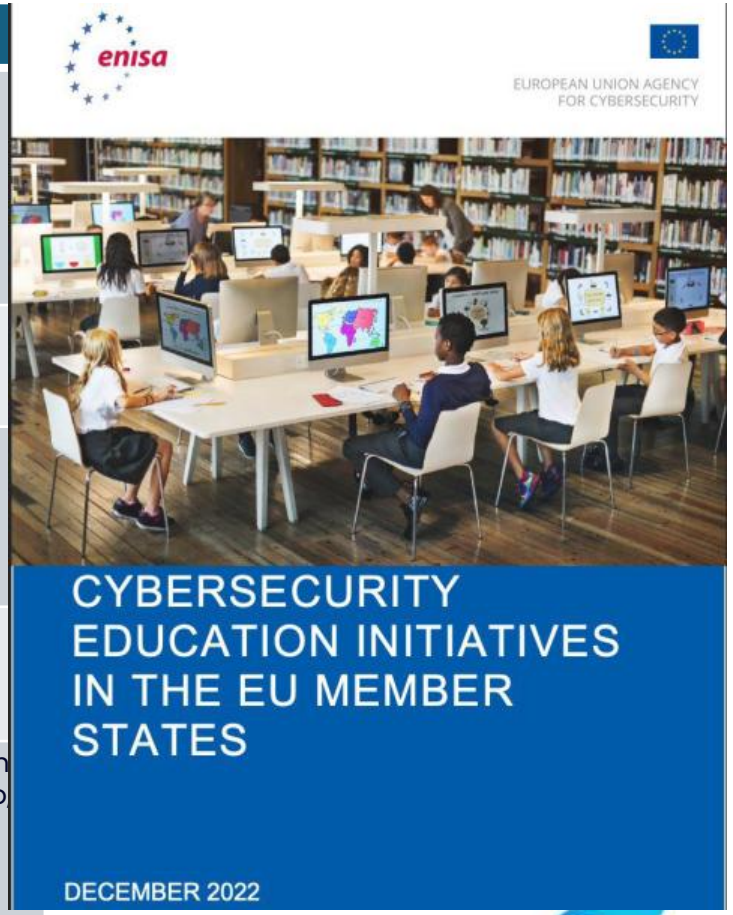
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national- cyber-security-strategies-evaluation-tool

El Mapa Interactivo ENISA NCSS enumera todos los documentos de Estrategias Nacionales de Ciberseguridad en la UE junto con sus objetivos estratégicos y buenos ejemplos de aplicación. El objetivo de ENISA es crear un info-hub con información proporcionada por los Estados miembros sobre sus esfuerzos para mejorar la ciberseguridad nacional.

ENISA Iniciativa de Educación

Iniciativas en educación de Ciberseguridad por los países miembros

	Principio Clave	Ejemplo de un Estado Miembro
1	**Enfoque colaborativo:** basar las iniciativas en una estrecha colaboración con las partes interesadas (ministerios, escuelas y profesores, industrias y otros expertos...).	Además de las iniciativas presentadas anteriormente en relación con las comunidades de expertos: en **Eslovenia**, la URSIV tiene previsto colaborar con determinados centros de enseñanza secundaria y facultades para impartir talleres de ciberseguridad a nivel local, y conectar el mundo académico, la industria y las instituciones de I+D para atraer a más jóvenes a las carreras de ciberseguridad.
2	**Enfoque pedagógico:** implicar activamente a los alumnos en las actividades	En **Francia**, la ANSSI ha creado un kit destinado a los niños para que puedan desarrollar un ciber juego
3	**Principio de Pareto:** buscar multiplicadores para intentar obtener los máximos resultados explotando la menor cantidad de recursos.	En **Grecia**, la NCSA está formando asociaciones estratégicas con estimadas partes interesadas, con el fin de llegar a un público más amplio y beneficiarse de sus probados conocimientos técnicos.
4	Preparar **planes anuales** para adelantarse a las próximas iniciativas	En **Malta**, MITA se centra en la preparación y ejecución de planes anuales que aborden los retos y tendencias en el ámbito de la ciberseguridad, manteniendo al mismo tiempo un plan lo suficientemente flexible como para hacer frente a nuevos problemas.
5	**Educar a los hijos a través de los padres:** crear una reacción en cadena que empiece por los padres y llegue a todos los niveles educativos.	La Fundación eSkills Malta lleva a cabo iniciativas para padres sobre cómo hacer un uso prudente de las redes sociales y las consecuencias de un mal uso (por ejemplo ir al lugar de trabajo de los padres e impartir sesiones sobre seguridad en línea), con el fin de que los padres tengan el mejor comportamiento y se conviertan así en buenos ejemplos para sus hijos.



Directrices de seguridad en Internet ISO 27032

LCSPC™ Versión 062024

Directrices Seguridad Internet

Directrices de Seguridad en Internet

Las partes interesadas pueden evaluar los riesgos teniendo en cuenta las amenazas que se aplican a sus activos. Este análisis puede ayudar en la selección de controles para contrarrestar los riesgos y reducirlos a un nivel aceptable.

Los controles se implementan para reducir la probabilidad o las consecuencias de dichos riesgos, y para cumplir los requisitos de seguridad de las partes interesadas (ya sea directa o indirectamente, proporcionando instrucciones a otras partes).

Las vulnerabilidades pueden persistir tras la aplicación de los controles. Dichas vulnerabilidades pueden ser explotadas por agentes de amenaza. Las partes interesadas intentan minimizar el riesgo, dadas otras limitaciones.

Las partes interesadas deben estar seguras de que los controles son adecuados para contrarrestar las amenazas a los activos antes de permitir la exposición de los activos a las amenazas especificadas.

Si las partes interesadas no poseen la capacidad de evaluar todos los aspectos de los controles, pueden solicitar la evaluación de los controles a organizaciones externas.

Una forma eficaz de hacer frente a los riesgos de seguridad en Internet implica una combinación de múltiples estrategias, teniendo en cuenta a las distintas partes interesadas.

Directrices Seguridad Internet

Estas estrategias incluyen ...

- Enfoques específicos del sector, con la colaboración de todas las partes interesadas para identificar y abordar los problemas y riesgos de Internet.

- Amplia educación de consumidores y empleados, proporcionando un recurso de confianza sobre cómo identificar y abordar riesgos específicos de Internet dentro de la organización, así como en la comunidad de usuarios de Internet;

- Soluciones tecnológicas innovadoras para ayudar a proteger a los consumidores de los ataques conocidos basados en Internet, para mantenerse al día y estar preparados contra las nuevas explotaciones;

- Legislación y normativa actualizadas para que prevalezca la justicia en todas las jurisdicciones.

Controles de seguridad para Internet

La mayoría de las organizaciones utilizan Internet para diversos fines, desde la navegación web, los blogs, las redes sociales y el acceso a servicios públicos en la nube, hasta el intercambio de información y la realización de negocios de comercio electrónico. Esto implica compartir información comercial clasificada, incluida información personal, mientras se ejecutan transacciones en línea. Internet, al ser una red pública, es propensa a ciertas amenazas únicas. Si no se abordan, estas amenazas dan lugar a ataques que pueden ser difíciles de gestionar.

Las organizaciones deben desarrollar políticas, procedimientos y capacidad de respuesta para:

a) Definir las normas de uso aceptable de Internet por parte del personal;
b) Definir qué servicios pueden exponerse a través de Internet;
c) Identificar las amenazas, vulnerabilidades, vectores de ataque y sus riesgos asociados;
d) Definir las funciones y responsabilidades de los distintos usuarios de Internet;
e) Sensibilizar a los usuarios sobre las prácticas seguras de uso de Internet;
f) Especificar los departamentos responsables de gestionar los problemas de seguridad de Internet;
g) Establecer un mecanismo de respuesta a los incidentes de ciberseguridad;
h) Realizar simulacros de seguridad para poner a prueba el mecanismo de respuesta ante ataques procedentes de Internet.

Controles Seguridad ISO 27032

Política de seguridad en Internet

Una organización debe preparar y publicar una política relativa al uso de Internet por parte del personal y otras partes relevantes en consonancia con los objetivos de seguridad.

Determina qué servicios de Internet se utilizan, quién está autorizado a utilizarlos y cuáles son los objetivos de seguridad. Esta política dirige todas las demás directrices para la conexión y el uso seguros de Internet. Las políticas de seguridad en Internet deben ser definidas, aprobadas por la dirección, publicadas, comunicadas y reconocidas por el personal pertinente, los contratistas y las partes externas.

Las políticas de seguridad de Internet deben estipular el personal autorizado a acceder a Internet, los contenidos que pueden ver, las conductas prohibidas en Internet, entre otros. Deben asignarse responsabilidades para todas las actividades relacionadas con Internet, y para el diseño, aprobación, implementación, operación y monitoreo de todos los controles específicos aplicables a la seguridad en Internet.

La norma ISO/IEC 27002 ofrece más orientaciones sobre las políticas de seguridad en Internet.

Controles Seguridad ISO 27032

Política de Control de Acceso

El control de acceso incluye los derechos de acceso no sólo de los usuarios, sino también de otras entidades como dispositivos, aplicaciones o procesos automatizados. Por lo tanto, cada conexión debe ser autenticada, y cada actividad debidamente autorizada, en función de los roles y permisos establecidos según las reglas de negocio y de seguridad, y a cada entidad se le deben asignar los permisos menos privilegiados. Esto mejora la trazabilidad del acceso a la información y a los activos, y reduce el anonimato para aumentar la seguridad.

Las reglas para controlar el acceso físico y lógico a la información y a los activos, a otros activos asociados con Internet y a las instalaciones de procesamiento de la información deben establecerse e implementarse basándose en el valor del negocio y de la información. Las normas relativas al acceso a la información y los activos esenciales, otros activos asociados con la información y las instalaciones de procesamiento de la información deben estar en consonancia con una política de control de acceso establecida y una política de clasificación de la información.

Las normas ISO/IEC 27002 e ISO/IEC 29146 ofrecen más orientaciones sobre la gestión de accesos.

Controles Seguridad ISO 27032

Educación, concientización y entrenamiento

El personal de la organización (incluida la alta dirección, los administradores de sistemas, el personal informático y los usuarios con privilegios, etc.) debe recibir información actualizada periódicamente sobre las principales amenazas (por ejemplo, phishing y vishing) y las medidas que deben tomarse para prevenirlas y responder en caso de acción indebida. Cada día aparecen en Internet numerosas amenazas nuevas que evolucionan continuamente y se vuelven más sigilosas y sofisticadas. Al implantar un control para contrarrestar un ataque, es posible que los usuarios no sean conscientes de que son víctimas de un ataque nuevo o más sofisticado.

Las organizaciones deben proporcionar periódicamente material de concienciación y formación para el personal utilizando diversos formatos, como comunicaciones por correo electrónico, formación en línea y mensajería a través de intranets, para informar al personal de las amenazas en línea, así como de sus obligaciones de uso aceptable y de notificación de incidentes. Esto proporciona un nivel de comprensión y capta su atención para protegerse a sí mismos y a la organización.

La norma ISO/IEC 27002 ofrece más orientaciones sobre educación, concienciación y formación.

Controles Seguridad ISO 27032

Gestión de incidentes de seguridad

Los incidentes de seguridad en Internet pueden ir desde una amplia variedad de ciberataques a los recursos organizativos orientados a Internet, así como a los servidores, bases de datos y aplicaciones que están detrás de los recursos orientados a Internet. Los incidentes de seguridad pueden desencadenarse desde cualquier punto de Internet. A veces, el host que lleva a cabo el ataque puede ser un host comprometido. Algunos incidentes pueden ser de naturaleza sofisticada e implicar habilidades especiales para responder adecuadamente.

Los incidentes a menudo cruzan fronteras nacionales, geográficas y organizativas, y la velocidad del flujo de información y los cambios del incidente en desarrollo a menudo dan un tiempo limitado para que las personas y organizaciones que responden actúen. Debe establecerse un equipo de gestión de incidentes (IMT) con un equipo de respuesta a incidentes (IRT) de apoyo para proporcionar a la organización la capacidad de evaluar, responder y aprender de tales incidentes.

La norma ISO/IEC 27002 y la serie ISO/IEC 27035 ofrecen más orientaciones sobre la gestión de incidentes.

Controles Seguridad ISO 27032

Gestión de activos

Deben identificarse los componentes de las TIC que contienen información y aplicaciones críticas. Tradicionalmente, se ha esperado que las organizaciones sepan dónde se encuentran físicamente sus activos para protegerlos adecuadamente.

Las organizaciones no sólo deben mantener un inventario actualizado de los activos TIC bajo su control, sino que también deben mantener un registro de activos de información sobre dónde se procesa, almacena y transfiere su información, tanto si se encuentra en su red interna como si utiliza soluciones de alojamiento basadas en la nube/Internet.

De esta manera, la organización puede gestionar los riesgos de su información dondequiera que resida y tomar decisiones basadas en el riesgo sobre si es apropiado que esa información se almacene fuera del entorno de control de la organización. Del mismo modo, en el caso de los componentes de red, se espera que las organizaciones sepan dónde se encuentran los activos sensibles con respecto a los puntos de entrada de posibles atacantes.

La norma ISO/IEC 27002 ofrece más orientaciones sobre la gestión de activos.

Controles Seguridad ISO 27032

Gestión de proveedores

Deben identificarse y aplicarse procesos y procedimientos para gestionar los riesgos de seguridad de Internet asociados al uso de proveedores. Todos los requisitos de seguridad de la información pertinentes deben establecerse y acordarse con cada proveedor en función del tipo de proveedor y de los riesgos asociados. La gestión de riesgos en relación con los proveedores de TIC y la información que almacenan, explotan o a la que pueden tener acceso, es clave para preparar contratos que garanticen la consecución continua de los objetivos de seguridad de la información de la organización.

Los acuerdos con los proveedores relevantes para Internet (como los ISP y los proveedores de servicios en la nube a través de Internet) deben establecerse y documentarse para garantizar que existe un entendimiento claro entre la organización y los proveedores respecto a las obligaciones de ambas partes de cumplir los requisitos relevantes de seguridad de la información.

Las organizaciones deben tener asociaciones abiertas con los ISP, los proveedores de servicios de telecomunicaciones, los proveedores de servicios en la nube y los socios para informar/avisar de las detecciones de amenazas entrantes...

Controles Seguridad ISO 27032

Para satisfacer los requisitos de seguridad de Internet identificados, se puede considerar la inclusión en los acuerdos de los siguientes aspectos:

a) Requisitos legales y reglamentarios, incluidos los requisitos de protección de la información por parte del PSI, como la protección frente a ataques DDoS y de otro tipo;
b) Obligación de cada parte contractual de aplicar un conjunto acordado de controles que incluyan el control
c) de acceso, la supervisión de la red y del sistema, la elaboración de informes y la auditoría; así como las obligaciones del proveedor de cumplir los requisitos de seguridad de la organización;
d) Requisitos y procedimientos de gestión de incidentes (especialmente notificación y colaboración durante la reparación de incidentes);
e) Seguimiento, revisión y gestión de cambios de los servicios de los proveedores para garantizar que se
f) cumplen los términos y condiciones de seguridad de la información de los acuerdos, y que permiten el seguimiento de los niveles de rendimiento del servicio para verificar el cumplimiento de los acuerdos, controlar los cambios realizados por los proveedores y supervisar los cambios en los servicios de los proveedores.

ISO/IEC 27002, la serie ISO/IEC 27036, ISO/IEC TR 23187 e ISO/IEC 27017 proporcionan más orientación relacionada con los proveedores.

Controles Seguridad ISO 27032

Continuidad de negocio en internet.

Algunas actividades empresariales como el comercio basado en Internet y otras actividades de comercio electrónico dependen de la infraestructura de Internet dentro de la organización. Las interrupciones de los servicios de Internet pueden deberse a ataques DoS y DDoS por parte de agentes malintencionados, a un mal funcionamiento del dispositivo perimetral o a cualquier interrupción del ISP. Los ataques DoS y DDoS también pueden ser llevados a cabo por actores malintencionados en el extremo ISP que pueden resultar en la interrupción completa de la red troncal de Internet. Las instalaciones de procesamiento de la información deben implementarse con la redundancia suficiente para cumplir los requisitos de disponibilidad.

Cualquier interrupción en la infraestructura de Internet constituye un riesgo para la continuidad de la organización y debe ser abordada por ésta. Las organizaciones deben planificar la adquisición de servicios de Internet de diferentes ISP para las medidas básicas de continuidad.

Las normas ISO/IEC 27002, ISO 22301 e ISO/IEC 27031 ofrecen más orientaciones relacionadas con la continuidad de las TIC.

Controles Seguridad ISO 27032

Protección de privacidad en internet.

La mayoría de los proveedores de servicios controlan o procesan la IIP. Cuando esta información se utiliza para fines distintos de los intereses del titular de los datos, surgen problemas de privacidad. Un proveedor de servicios de alojamiento procesa la IPI en su red y centro de datos como parte de sus servicios empresariales.

Estos servicios, que incluyen sitios web y otras aplicaciones en línea, son a menudo reempaquetados y revendidos por los suscriptores de alojamiento a otros consumidores, como pequeñas empresas y usuarios finales, y son accesibles a través de Internet.

Si los suscriptores de alojamiento instalan un servidor inseguro o alojan contenidos maliciosos en sus sitios o aplicaciones, la seguridad de los consumidores, incluida la IIP almacenada por dichas aplicaciones en línea, se verá afectada negativamente.

Las normas ISO/IEC 27002, ISO/IEC 27701, ISO/IEC 29100 e ISO/IEC 27018 proporcionan más orientaciones relacionadas con la privacidad.

Controles Seguridad ISO 27032

Gestión de vulnerabilidades

Debe evaluarse la exposición de la organización a dichas vulnerabilidades y deben tomarse las medidas adecuadas para abordar el riesgo asociado. Las configuraciones, incluyendo las configuraciones de seguridad de hardware, software, servicios y redes deben ser establecidas, documentadas, implementadas y monitoreadas y revisadas.

Otras medidas para mitigar las vulnerabilidades son:
a) Cambiar las prácticas operativas;
b) Reconfigurar los sistemas técnicos;
c) Evitar el riesgo gestionando el acceso a Internet;
d) Formar al personal y a los usuarios;
e) Aplicar medidas de defensa en profundidad, es decir, cuando falla un control, existe otro método independiente para seguir defendiéndose;
f) Pruebas de seguridad del sistema, SDLC seguro y pruebas de parches y actualizaciones antes de su despliegue.

Las normas ISO/IEC 27002, ISO/IEC 30111 e ISO/IEC 29147 proporcionan más orientaciones relacionadas con la gestión de vulnerabilidades.

Controles Seguridad ISO 27032

Gestión de redes

La reducción de la exposición de los activos conectados a Internet reduce los riesgos relacionados con el acceso no autorizado, la manipulación o los daños. Deben establecerse controles para garantizar la seguridad de la información conectada a Internet y la protección de los servicios conectados frente a accesos no autorizados.

Deben establecerse controles para salvaguardar la confidencialidad e integridad de los datos que pasan por Internet y para proteger los sistemas y aplicaciones conectados. Los sistemas que pueden conectarse a Internet deben estar restringidos y, cuando se permita, deben estar autenticados.

El registro y la supervisión de los dispositivos y sistemas de red asociados a la infraestructura de Internet de la organización deben aplicarse para registrar y detectar acciones que puedan afectar a la seguridad de Internet o que sean relevantes para la misma. La organización debe considerar la gestión de la seguridad de los sistemas conectados a Internet mediante la segregación de estos de otras redes organizativas como redes privadas y DMZ. El perímetro de esta red segregada debe estar bien definido y debe controlarse mediante una pasarela (por ejemplo, cortafuegos, enrutador de filtrado).

Controles Seguridad ISO 27032

Para la implementación de la seguridad de la red debe tenerse en cuenta lo siguiente:

- Asegúrese de que existe una interfaz supervisada y fiable entre la red de la organización e Internet, que también garantice el control de acceso de todas las entidades, y no sólo de las personas autorizadas. La información y las aplicaciones también deben controlarse antes de conceder acceso tanto a la infraestructura interna como desde ella.
- Estructurar la red interna para aislar los activos altamente críticos de los de uso general, creando una especie de silos o clúster con un control de acceso adecuado. Garantizar subredes con enrutadores de filtrado y subredes incrustadas para evitar tener un camino directo a los activos críticos.
- Supervisar y analizar el tráfico interno para detectar y bloquear actividades ilícitas.
- Garantizar el acceso y uso de Internet y sus servicios (incluida la comunicación con el personal que trabaja fuera de las instalaciones físicas).
- Garantizar que la red interna esté suficientemente segregada con protecciones de frontera interna para aislar los componentes críticos o cruciales de los puntos de entrada y transferencia interna de fácil acceso.

La norma ISO/IEC 27002 y la serie ISO/IEC 27033 ofrecen más orientaciones sobre la seguridad de las redes.

Gestión de antimalware

El software antimalware escanea datos y programas para identificar patrones sospechosos asociados a malware. Para permitir la detección de nuevos códigos maliciosos, es muy importante asegurarse de que el software de análisis se mantiene siempre al día, a ser posible mediante actualizaciones diarias.

Dado el potencial de los nuevos programas maliciosos para atacar vulnerabilidades de día cero, existe software que puede identificar variantes conocidas. Esto incluye tecnología que puede identificar patrones de ataque potenciales. Aunque no es infalible, este software proporciona un mayor nivel de protección que si no se utiliza. Varios sistemas operativos populares tienen algunas funciones integradas para proteger contra el malware común, pero aun así deben complementarse con tecnología anti-malware para entornos de alto riesgo.

La aplicación de medidas antimalware debe ampliarse a la protección del tráfico y el intercambio no deseados en Internet (en ambas direcciones), ya que los usuarios suelen recibir y enviar programas maliciosos sin saberlo. Deben aplicarse medidas de prevención, detección, corrección y recuperación para proteger contra los programas maliciosos, combinadas con una concienciación adecuada de los usuarios.

Controles Seguridad ISO 27032

Gestión de control de cambios

Deben establecerse políticas y procesos de gestión de cambios para garantizar que a las organizaciones les resulte más fácil implantar cambios en la infraestructura de TI, gestionar los cambios en los sistemas y aplicaciones de TI con el fin de evitar interrupciones no programadas, corrupción o pérdida de datos. Las organizaciones deben incluir los cambios relacionados con la seguridad de los sistemas alojados en Internet en su proceso de gestión de cambios. Estos procesos ayudan a la organización a solicitar, priorizar, autorizar, aprobar, programar y aplicar cualquier cambio.

Las políticas de gestión de cambios incluyen declaraciones sobre responsabilidades y deberes de los gestores de sistemas, importación de software y archivos, control de acceso, entre otros.

Todos los cambios (modificaciones, traslados, supresiones o adiciones) de los componentes o la estructura de la red deben gestionarse para mantener actualizados la arquitectura y los planos de la infraestructura.

La norma ISO/IEC 27002 ofrece más orientaciones sobre la gestión de cambios.

Controles Seguridad ISO 27032

Identificación de la legislación aplicable y de los requisitos de cumplimiento

La Internet se utiliza cada vez más como plataforma para desplegar numerosos servicios de transacciones en línea. Puede haber leyes y reglamentos de seguridad de datos, ciberseguridad y privacidad sobre la protección de la confidencialidad, integridad y disponibilidad de los detalles de las transacciones.

Las transacciones bancarias, los canales de pago, las transacciones basadas en aplicaciones móviles y otras actividades de comercio electrónico suelen estar reguladas debido a la implicación del dinero en forma digital. Deben identificarse, documentarse y mantenerse actualizados todos los requisitos legales, estatutarios, reglamentarios y contractuales pertinentes en materia de seguridad de la información y ciberseguridad, así como el enfoque de la organización para cumplir estos requisitos. Se espera que los registros mantenidos en sistemas en línea a los que se accede a través de Internet estén protegidos frente a pérdidas, destrucción, falsificación, acceso no autorizado y divulgación no autorizada, de acuerdo con los requisitos legales, estatutarios, reglamentarios, contractuales y empresariales.

La norma ISO/IEC 27002 ofrece más orientación sobre la legislación y los requisitos de conformidad.

Controles Seguridad ISO 27032

Uso de Criptografía

La criptografía es una de las formas de garantizar la protección de la información transmitida e impedir el análisis del tráfico. Una red privada virtual (VPN) es una solución sencilla. La criptografía tiene algunas limitaciones asociadas a la gestión de las claves de cifrado y descifrado, y a la gestión de los dispositivos criptográficos, que deben considerarse confidenciales y críticas.

La criptografía debe utilizarse para proteger la confidencialidad, autenticidad y/o integridad de la información transmitida por Internet. La implementación de VPN y HTTPS (hypertext transfer protocol secure) utiliza criptografía para conexiones seguras. Los algoritmos criptográficos, la longitud de las claves y las prácticas de uso deben seleccionarse de acuerdo con las mejores prácticas. Una gestión de claves adecuada requiere procesos seguros para generar, almacenar, archivar, recuperar, distribuir, retirar y destruir claves criptográficas. Todas las claves criptográficas deben estar protegidas contra modificaciones y pérdidas. Además, las claves secretas y privadas necesitan protección contra el uso no autorizado, así como contra su divulgación.

La norma ISO/IEC 27002 ofrece más orientaciones sobre el uso de la criptografía.

Controles Seguridad ISO 27032

Seguridad de las aplicaciones en Internet

Pueden adoptarse nuevas tecnologías para los sistemas que forman parte de la infraestructura de Internet. La nueva tecnología debe ser analizada para detectar riesgos de seguridad y el diseño debe ser revisado frente a patrones de ataque conocidos. La seguridad debe integrarse en el diseño del sistema. Los sistemas también deben revisarse periódicamente para garantizar que se mantienen actualizados en cuanto a la lucha contra las nuevas amenazas potenciales y para seguir siendo aplicables a los avances en las tecnologías y soluciones que se aplican.

Las organizaciones deben adoptar principios de ingeniería segura, incluyendo la implementación de un ciclo de vida de desarrollo seguro para identificar y mitigar los riesgos en los productos y soluciones que se están desarrollando. Esto debería tener en cuenta la modelización de amenazas, las técnicas de autenticación de usuarios, los componentes de la cadena de suministro, el control de sesiones seguras y la validación de datos, la desinfección y una revisión del diseño orientada a la seguridad para ayudar a identificar las vulnerabilidades de seguridad en los sistemas orientados a Internet. El código de las aplicaciones orientadas a Internet se diseña mejor desde el punto de vista de la seguridad partiendo de la base de que siempre está sujeto a ataques, ya sea por error o por actos malintencionados.

Controles Seguridad ISO 27032

En el caso de las aplicaciones en las que las transacciones se procesan a través de Internet, debe tenerse en cuenta lo siguiente:

- Los requisitos relativos al nivel de protección necesario para mantener la confidencialidad y la integridad de los detalles de las transacciones;
- Transmitir los detalles de las transacciones por Internet con los controles de seguridad adecuados (por ejemplo, ruta de transmisión cifrada, certificación digital);
- Almacenamiento de los datos de las transacciones fuera de cualquier entorno de acceso público y garantía de que el medio de almacenamiento no es directamente accesible desde Internet;
- Requisitos de resistencia frente a ataques, que pueden incluir requisitos para proteger los servidores de aplicaciones implicados o garantizar la disponibilidad de las interconexiones de red necesarias para prestar el servicio;
- Cuando sea necesario un alto grado de confianza en la seguridad de los productos de software, los productos deben ser validados de forma independiente según el esquema de Criterios Comunes, tal y como se describe en la serie ISO/IEC 15408.

Controles Seguridad ISO 27032

Las pruebas de seguridad deben ser parte integrante de las pruebas de sistemas o componentes antes de su exposición a Internet.

La organización puede utilizar herramientas automatizadas, como herramientas de análisis de código y escáneres de vulnerabilidades, y debe verificar la corrección de los defectos relacionados con la seguridad antes de poner los sistemas en funcionamiento en Internet.

Las pruebas de seguridad deben incluir pruebas de:

a) funciones de seguridad, por ejemplo, autenticación de usuarios, restricción de acceso, uso seguro de API y uso de criptografía;
b) Configuraciones seguras, incluidas las de los sistemas operativos, cortafuegos y otros componentes de seguridad.

La serie ISO/IEC 15408 ofrece orientaciones sobre la seguridad de las aplicaciones.

Las series ISO/IEC 27002 e ISO/IEC 27034 proporcionan orientaciones relacionadas con la seguridad de las aplicaciones.

Controles Seguridad ISO 27032

Gestión de dispositivos de usuario final

Debe protegerse la información almacenada, procesada o accesible a través de dispositivos de punto final (por ejemplo, dispositivos IoT, dispositivos USB, BYOD). Debe controlarse adecuadamente el transporte y uso de dispositivos endpoint en zonas seguras.

Debe desarrollarse e implementarse una estrategia de seguridad para la gestión de dispositivos endpoint. Esta estrategia debe incluir la gestión de cortafuegos de dispositivos, herramientas de filtrado específicas para el correo electrónico, seguridad y filtrado de Internet, herramientas de gestión y seguridad de dispositivos móviles, cifrado y herramientas de detección de intrusiones.

La seguridad de los puntos finales se ha vuelto aún más importante, ya que los puntos finales se están moviendo fuera del perímetro de la organización y los usuarios pueden utilizar Internet para acceder a la nube y a los recursos dentro de la red de la organización.

El compromiso en el punto final debe responderse con una acción inmediata para bloquear al atacante y limitar daños mayores.

Controles Seguridad ISO 27032

Las organizaciones deben desplegar capacidades técnicas en los puntos finales para detectar cualquier tráfico malicioso de fuentes desconocidas y actores maliciosos, y responder. Estas tecnologías también se conocen como tecnologías de detección y respuesta de puntos finales (EDR). Las organizaciones deben disponer de un mecanismo que garantice que todas las políticas de seguridad de la organización aplicables a los sistemas y dispositivos de los usuarios finales estén activadas en todo momento.

Estas tecnologías deben garantizar que el usuario final no pueda desactivar o eludir las funciones de seguridad instaladas en su puesto final. La pérdida o el compromiso del endpoint puede suponer un riesgo importante para los datos que residen en él, incluidos los dispositivos móviles. Las organizaciones deben desplegar técnicas para garantizar que pueden rastrear estos dispositivos y, en caso de pérdida o compromiso del dispositivo, deben ser capaces de borrar remotamente el contenido de los dispositivos incluso antes de que los datos sean robados por los malos actores.

La serie ISO/IEC 27034 proporciona orientaciones relacionadas con la seguridad de las aplicaciones

Controles Seguridad ISO 27032

Monitoreo

Los registros que registran actividades, excepciones, fallos y otros eventos relevantes deben ser producidos, protegidos, guardados y analizados.

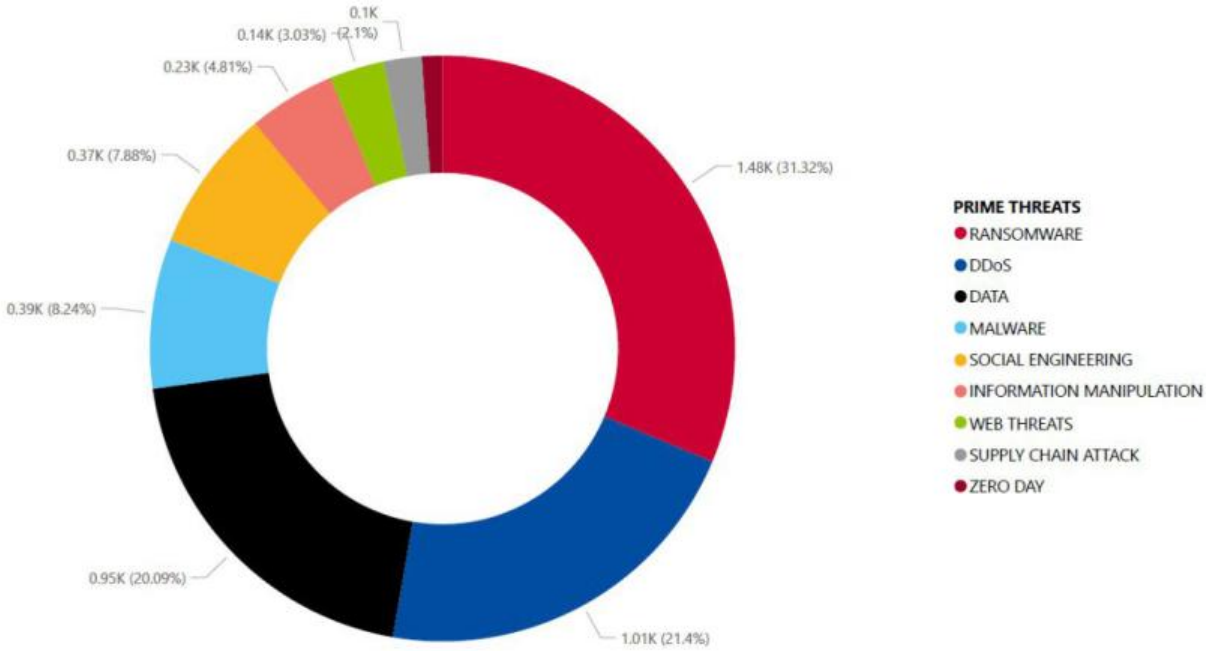
Los registros deben protegerse y guardarse en un lugar seguro para su análisis y auditoría. Algunas normativas exigen almacenar los registros durante un periodo de tiempo determinado.
Las redes, sistemas y aplicaciones orientados a Internet deben supervisarse para detectar comportamientos anómalos y deben tomarse las medidas adecuadas para evaluar posibles incidentes de seguridad de la información.

La norma ISO/IEC 27002 proporciona más orientación sobre la gestión de monitoreo.

Panorama de Ciber amenazas

Panorama de Ciber amenazas ENISA 2023

Informe anual sobre el estado del panorama de las amenazas a la ciberseguridad. Identifica las principales amenazas, las principales tendencias observadas con respecto a las amenazas, los actores de las amenazas y las técnicas de ataque, así como el análisis del impacto y la motivación. También describe las medidas de mitigación pertinentes.



El **ransomware** y los ataques **DDoS** fueron las formas de ataque más denunciadas durante el periodo de referencia y representaron casi la mitad de los sucesos observados, seguidos de las amenazas relacionadas con los datos.

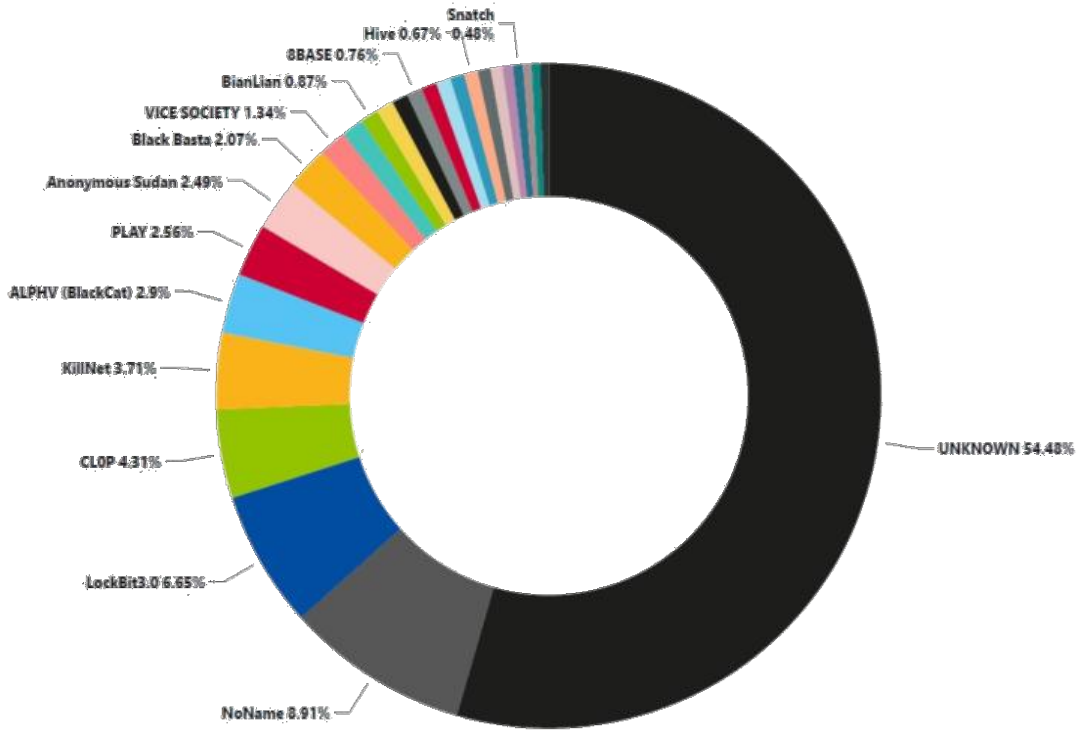
https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

Panorama de Ciber amenazas

Panorama de Ciber amenazas ENISA 2023

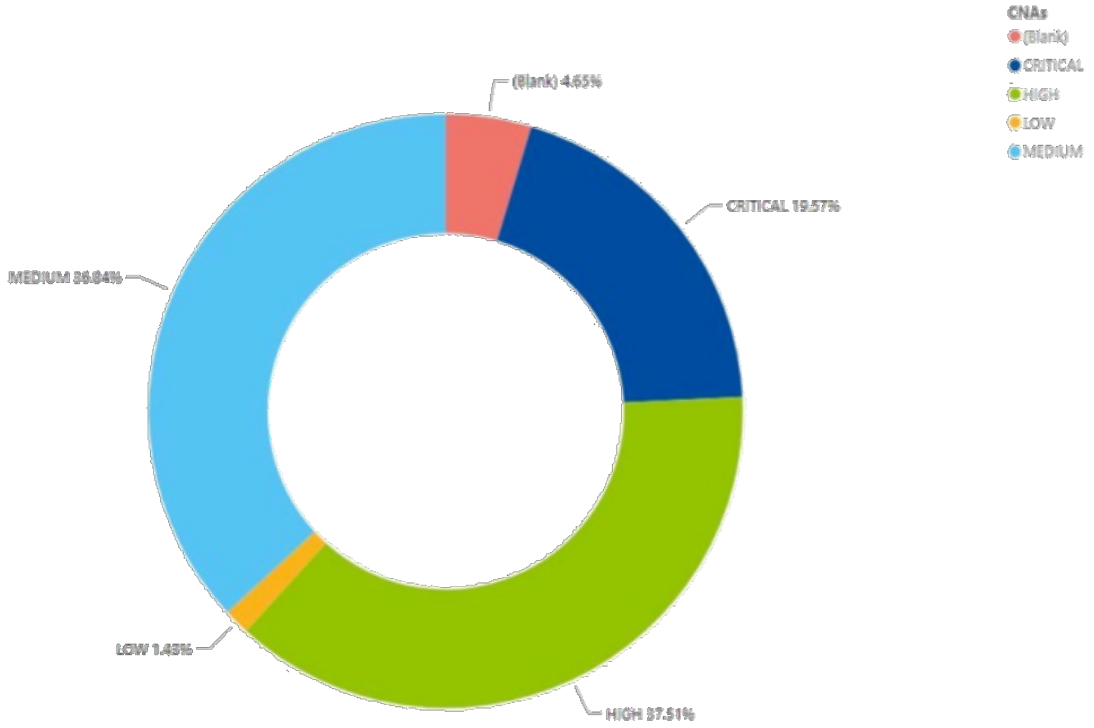
TENDENCIAS DE LOS ACTORES DE AMENAZAS

Figure 11: 25 most attributed threat actors during the reporting period



ANÁLISIS DEL PANORAMA DE VULNERABILIDADES 2022- 2023 CVE

Figure 14: Percentage of CVEs by Severity (Percentage of the total)



Anexo A-Referencias Cruzadas 27032 y 27002

LCSPC™ Versión 062024

Controles 27032 vs 27002

Mapping entre controles para la seguridad en Internet

ISO / IEC 27032 v 2023	ISO / IEC 27002 v 2022
9.2.2 – Políticas de Internet seguro	**5.1 –** Políticas de Seguridad de la Información. **5.4** – Gestión de Responsabilidades
9.2.3 – Control de Acceso	**5.15** – Control de acceso **5.16** – Gestión de identidad **5.18** – Derechos de acceso **8.2** – Derechos de acceso privilegiado **8.18** – Uso de privilegio a programas utilitarios
9.2.4 – Educación, concientización y entrenamiento	**6.3** - Sensibilización, educación y formación en seguridad de la información

Controles 27032 vs 27002

Mapping entre controles para la seguridad en Internet

ISO / IEC 27032 v 2023	ISO / IEC 27002 v 2022
9.2.5 - Gestión de incidentes de seguridad	**5.7** – Inteligencia de Amenazas 24. – Planificación y preparación de la gestión de incidentes de seguridad de la información 25. – Evaluación y decisión sobre incidentes de seguridad de la información 26. – Respuesta a incidentes de seguridad de la información. 27. – Aprender de los incidentes de seguridad de la información. 28. – Recolección de Evidencias **6.8** – Notificación de incidentes de seguridad de la información.
9.2.6 – Gestión de Activos	**9. -** Seguridad de la información en las relaciones con los proveedores. **10. -** Uso aceptable de la información y otros activos asociados **11. -** Devolución de activos. **12. -** Clasificación de Información
9.2.7 – Gestión de Proveedores	19. - Seguridad de la información en las relaciones con los proveedores 20. - Tratamiento de la seguridad de la información en los acuerdos con proveedores. 21. - Gestión de la seguridad de la información en la cadena de suministro de TIC. 22. - Supervisión, revisión y gestión de cambios de los servicios de proveedores.

Controles 27032 vs 27002

Mapping entre controles para la seguridad en Internet

ISO / IEC 27032 v 2023	ISO / IEC 27002 v 2022
9.2.8 - Continuidad del negocio en Internet	**5.29 -** Seguridad de la información durante las interrupciones. **5.30** - Preparación de las TIC para la continuidad del negocio. **8.13** - Copia de seguridad de la información **8.14** - Redundancia de las instalaciones de procesamiento de la información
9.2.9 - Protección de la privacidad en Internet	**5.34** - Privacidad y protección de la IIP **8.11** - Enmascaramiento de datos
9.2.10 – Gestión de vulnerabilidades	**8.8** - Gestión de vulnerabilidades técnicas **8.9** - Gestión de la configuración **8.19** - Instalación de software en sistemas operativos.
9.2.11 – Gestión de Redes	**8.16 -** Monitoreo de Actividades **8.20 -** Seguridad de redes **8.21 -** Seguridad de los servicios de red **5.12 -** Segregación de redes
9.2.12 – Protección contra malware	**8.7** – Protección contra malware
9.2.13 - Continuidad del negocio en Internet	**8.32 –** Gestión de cambios.

Controles 27032 vs 27002

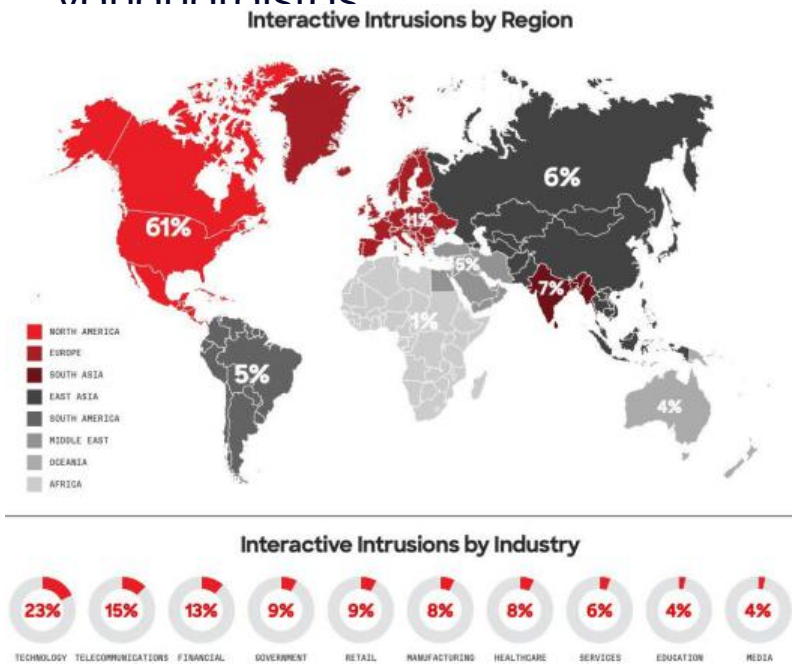
Mapping entre controles para la seguridad en Internet

ISO / IEC 27032 v 2023	ISO / IEC 27002 v 2022
9.2.14 - Identificación de la legislación aplicable y de los requisitos de cumplimiento	**5.28** – Recolección de pruebas **5.31** - Requisitos legales, reglamentarios y contractuales **5.33** - Protección de aplicaciones de registros
9.2.15 – Uso de criptografía	**8.24** – Uso de criptografía
9.2.16 - Seguridad de las aplicaciones para Internet.	**23. -** Filtrado web **24. -** Uso de criptografía **25. -** Ciclo de vida del desarrollo seguro **26. -** Requisitos de seguridad de las aplicaciones **27. -** Arquitectura de sistemas seguros y principios de ingeniería **28. -** Codificación segura **29. -** Pruebas de seguridad en el desarrollo y la aceptación
9.2.17 - Gestión de dispositivos de punto final	**8.1 -** Dispositivos de usuario **8.9 -** Gestión de la configuración
9.2.18 - Monitoreo	**8.15 -** Registro **8.16 -** Monitorización de actividades

Reporte Global de Amenazas

Reporte Global de Amenazas 2024 Crowdstrike

La velocidad y la ferocidad de los ciberataques continúan acelerándose a medida que los adversarios reducen el tiempo entre la entrada inicial, el movimiento lateral y la brecha. Al mismo tiempo, el auge de la IA generativa tiene el potencial de reducir la barrera de entrada para los adversarios poco cualificados, facilitando el lanzamiento de ataques más [illegible] vanguardistas.



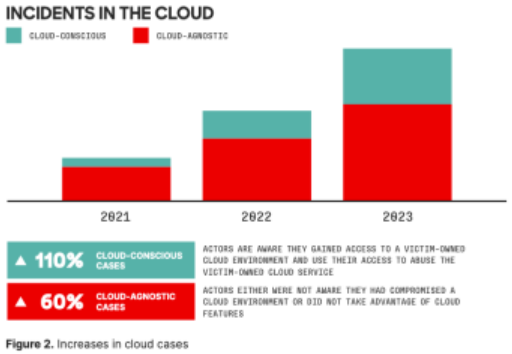
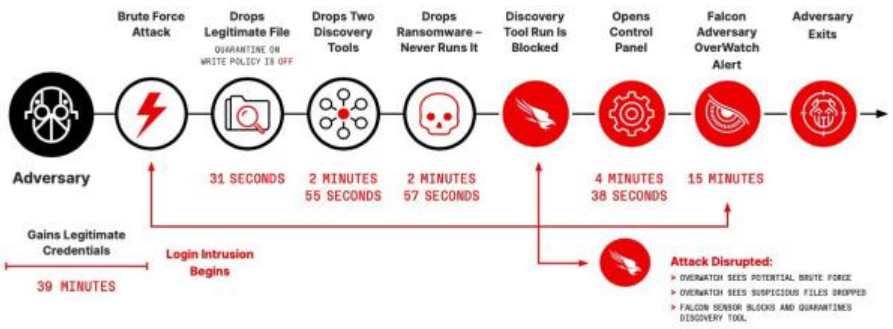
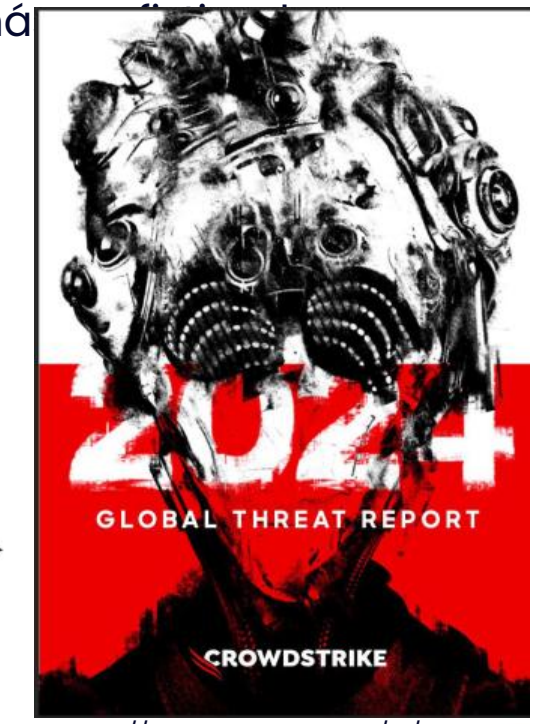


Figure 2. Increases in cloud cases





https://go.crowdstrike.com/rs/281-OBQ-266/images/GlobalThreatReport2024.pdf

Reporte Global de Amenazas

Crowdstrike Recomendaciones

01 Convierta la protección de la identidad en algo imprescindible

Las credenciales robadas otorgan a los adversarios acceso y control rápidos, una puerta de entrada instantánea a una brecha.

Para contrarrestar estas amenazas, es esencial implementar la autenticación multifactor resistente al phishing y extenderla a los sistemas y protocolos heredados, educar a los equipos en ingeniería social e implementar tecnología que pueda detectar y correlacionar amenazas a través de entornos de identidad, endpoint y nube.

02 Dar prioridad a las aplicaciones nativas en la nube

Las empresas necesitan una visibilidad total de la nube, incluidas las aplicaciones y las API, para eliminar los errores de configuración, las vulnerabilidades y otras amenazas a la seguridad.

Las CNAPP son fundamentales: Las herramientas de seguridad en la nube no deben existir de forma aislada, y las CNAPP proporcionan una plataforma unificada que simplifica la supervisión, detección y actuación ante posibles amenazas y vulnerabilidades de seguridad en la nube.

03 Obtenga visibilidad en las áreas más críticas del riesgo empresarial

Para identificar este tipo de ataque, es necesario comprender la relación entre la identidad, la nube, el endpoint y la telemetría de protección de datos, que pueden estar en sistemas separados. Al consolidarse en una plataforma de seguridad unificada con capacidades de IA, las organizaciones tienen visibilidad completa en un solo lugar y pueden controlar fácilmente sus operaciones.

Con una plataforma de seguridad consolidada, las organizaciones pueden descubrir, identificar y detener las brechas rápido.

Crowdstrike Recomendaciones

04 Impulse la eficiencia: Los adversarios son cada vez más rápidos, ¿y usted?

Los adversarios tardan una media de 62 minutos -y los más rápidos sólo 2 minutos-en desplazarse lateralmente desde un host inicialmente comprometido a otro dentro del entorno. ¿Puede ¿Puede seguirles el ritmo? Admitámoslo: las soluciones SIEM heredadas han fallado al SOC. Necesita una herramienta que sea más rápida, fácil de implantar y más rentable que las soluciones SIEM heredadas. Si no dispone de un equipo SOC interno, considere la detección y respuesta gestionadas (MDR) 24/7.

05 Crear una cultura de ciberseguridad

El usuario final sigue siendo un eslabón crucial en la cadena para detener las brechas. Deben iniciarse programas de concienciación de los usuarios para combatir la amenaza continua del phishing y las técnicas de ingeniería social relacionadas. Para los equipos de seguridad, la práctica hace al maestro.

Fomente un entorno en el que se realicen rutinariamente ejercicios de simulación y equipos rojos y azules para identificar lagunas y eliminar puntos débiles en sus prácticas y respuestas de ciberseguridad.

NICE Framework 1.0 – NIST SP 800-18 v 2020

LCSPC™ Versión 062024

NICE NIST SP 800-18

Workforce Framework for Cybersecurity 1.0 (NICE) NIST SP 800-18 v 2020

El marco NICE ayuda a las organizaciones a superar la barrera de describir su fuerza de trabajo a múltiples partes interesadas presentando un enfoque de bloques de construcción. Mediante el uso de bloques de construcción conceptuales, el Marco NICE presenta un lenguaje común para que las organizaciones lo utilicen internamente y con otros.

Este enfoque permite a las organizaciones adaptar y aplicar el Marco NICE a su contexto operativo único. Además, al crear un lenguaje común, el Marco NICE reduce la barrera de entrada para las organizaciones que desean entrar e interoperar con otras organizaciones.

La tecnología sigue evolucionando a un ritmo cada vez más rápido. Concretamente, la tecnología que facilita la capacidad de acceder a la información y procesarla con rapidez y eficacia está cambiando drásticamente.

El trabajo necesario para diseñar, construir, asegurar e implantar estos datos, redes y sistemas aumenta en complejidad. Además, describir este trabajo y a quienes pueden realizarlo sigue siendo un reto. Para agravar este problema, las organizaciones utilizan métodos diversos y de creación propia para intentar resolver el reto.

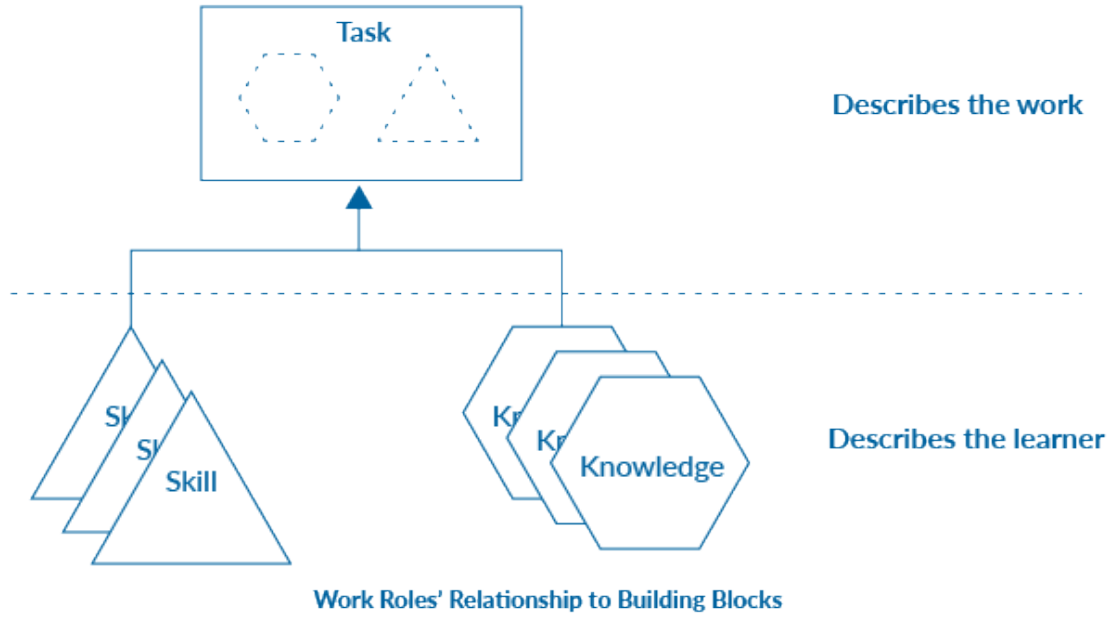
NICE NIST SP 800-18

Los principales componentes del Marco NICE son las declaraciones de Tareas, Conocimientos y Habilidades (TKS) (explicadas en la Sección 2) que se muestran junto a los conceptos que describen.

La figura muestra que se describen dos tipos principales de conceptos: **"el trabajo" y "el alumno".**

En particular, quienes realizan (o realizarán) un trabajo (por ejemplo, estudiantes, empleados actuales o solicitantes de empleo) están continuamente aprendiendo y alcanzando objetivos y pueden encontrarse en cualquier parte del ciclo de vida del aprendizaje.

El Marco NICE intenta describir tanto "el trabajo" como "el alumno" en términos genéricos que puedan aplicarse a todas las organizaciones.



NICE NIST SP 800-18

El **"trabajo"** es lo que una organización necesita para alcanzar los objetivos de gestión de riesgos de ciberseguridad.

Cada organización ejecuta tareas comunes, así como algunas tareas únicas en su contexto.

Por ejemplo, cada organización tiene algún tipo de tareas de gestión, mientras que sólo algunas organizaciones tienen tareas para "desplegar sistemas de energía a granel de forma segura."

El Marco NICE proporciona a las organizaciones una forma de describir su trabajo a través de enunciados de Tareas que agrupan enunciados de Conocimientos y Habilidades de apoyo.

NICE NIST SP 800-18

El "alumno" es la persona que posee conocimientos y habilidades.

El término alumno se aplica a todas las personas incluidas en el ámbito de este documento.

Un alumno puede ser un estudiante, una persona en busca de empleo, un empleado u otras personas dentro de la población activa.

En un contexto organizativo, los alumnos ejecutan tareas. En un contexto educativo, los alumnos adquieren nuevos conocimientos y habilidades.

Todos los individuos son considerados aprendices debido a la educación o formación que recibieron antes de entrar en la fuerza de trabajo, la formación continua, el autoaprendizaje o un plan de progresión profesional.

NICE NIST SP 800-18

Credit: NICE Program Office

https://www.nist.gov/news-events/news/2024/03/unveiling-nice-framework-components-v100-explore-latest-updates-today

NICE NIST SP 800-18

El Marco NICE proporciona a las organizaciones una forma de describir a los alumnos asociando declaraciones de **Conocimientos y Habilidades** a un individuo o grupo. Utilizando sus conocimientos y habilidades, los alumnos pueden completar tareas para alcanzar los objetivos de la organización.
Aunque no todas las organizaciones utilizarán todos los conceptos relativos a los alumnos, el marco NICE proporciona a las organizaciones un conjunto flexible de elementos básicos que pueden utilizar en función de sus necesidades específicas.

Al describir tanto el trabajo como al alumno, el marco NICE proporciona a las organizaciones un lenguaje común para describir su trabajo y su personal de ciberseguridad. Algunas partes del marco NICE describen un contexto de trabajo organizativo (tareas), otras partes describen un contexto de aprendizaje (conocimientos y habilidades) y, por último, el enfoque de bloques de construcción del marco NICE permite a las organizaciones vincular los dos contextos.

Además, el Marco NICE proporciona un mecanismo para comunicar entre organizaciones a nivel de pares, sectorial, estatal, nacional o internacional utilizando los mismos bloques de construcción. Esta comunicación puede impulsar soluciones innovadoras a retos comunes, reducir las barreras de entrada para nuevas organizaciones y personas, y facilitar la movilidad de la mano de obra.

Atributos del Marco NICE

El Marco NICE es un recurso de referencia para aquellos que buscan describir el trabajo de ciberseguridad que realiza su organización, las personas que llevarán a cabo el trabajo, y el aprendizaje continuo que será necesario para hacer ese trabajo con eficacia. La naturaleza del trabajo y, en consecuencia, la mano de obra puede describirse utilizando los bloques de construcción del **TKS** que se presentan en las siguientes secciones.

Estos bloques de construcción incorporan los siguientes atributos:

- **Agilidad:**

Las personas, los procesos y la tecnología maduran y deben adaptarse al cambio. Por lo tanto, el Marco NICE permite a las organizaciones seguir el ritmo de un ecosistema en constante evolución.

NICE NIST SP 800-18

- **Flexibilidad:**

Aunque todas las organizaciones se enfrentan a retos similares, no existe una solución única para esos retos comunes. Por lo tanto, el Marco NICE permite a las organizaciones tener en cuenta el contexto operativo único de la organización.

- **Interoperabilidad:**

Aunque cada solución a los retos comunes es única, esas soluciones deben acordar un uso coherente de los términos. Por lo tanto, el Marco NICE permite a las organizaciones intercambiar información sobre la fuerza de trabajo utilizando un lenguaje común.

- **Modularidad:**

Aunque el riesgo de ciberseguridad sigue siendo la base de este documento, existen otros riesgos que las organizaciones deben gestionar dentro de la empresa. Por lo tanto, el Marco NICE permite a las organizaciones comunicarse sobre otros tipos de fuerzas de trabajo dentro de una empresa y entre organizaciones o sectores (por ejemplo, privacidad, gestión de riesgos, ingeniería/desarrollo de software).

NICE NIST SP 800-18

Finalidad y aplicabilidad del Marco NICE

Las organizaciones gestionan muchas funciones empresariales diferentes (como operaciones, finanzas, asuntos jurídicos y recursos humanos) como parte de su empresa global. Cada una de estas funciones empresariales tiene riesgos asociados.

A medida que la tecnología se ha convertido en un factor habilitador en la gestión de una empresa, los riesgos asociados con la ciberseguridad también se han vuelto más prominentes.

El Marco NICE ayuda a las organizaciones a gestionar los riesgos de ciberseguridad proporcionando una forma de discutir el trabajo y los aprendices asociados a la ciberseguridad.
Estos riesgos de ciberseguridad son una entrada importante en las decisiones de riesgo de la empresa como se describe en el Informe **NIST Interagency 8286, Integración de la Ciberseguridad y la Gestión del Riesgo Empresarial** (ERM).

Este documento sirve como guía potencial para otras funciones empresariales que estén considerando la creación de marcos de fuerza de trabajo.
Las organizaciones pueden aumentar su eficiencia utilizando los mismos bloques de construcción en varias funciones empresariales.

NICE NIST SP 800-18

Audiencia del Marco NICE

El tema de la gestión de una fuerza de trabajo para la ciberseguridad implica muchos tipos diferentes de puestos, así como muchos tipos diferentes de organizaciones.

La audiencia de este documento incluye agencias del sector público, organizaciones privadas y sin ánimo de lucro,
proveedores de educación y formación, desarrolladores de currículos, proveedores de credenciales, profesionales de recursos humanos, directores de contratación, directores de línea, planificadores de mano de obra, reclutadores y todos los alumnos.

Elementos NICE Framework NIST SP 800-18

LCSPC™ Versión 062024

Elementos del NICE

Elementos del NICE

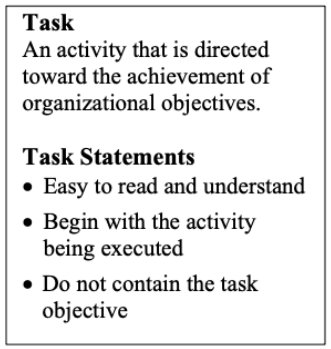
Elementos del Marco NICE

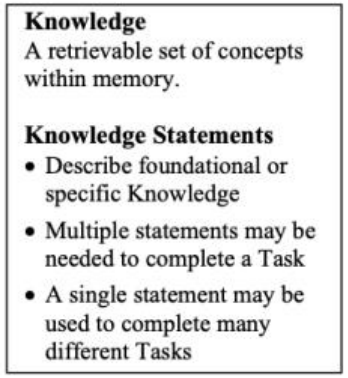
El marco de la fuerza de trabajo para la ciberseguridad (marco NICE) se basa en un conjunto de bloques de construcción discretos que describen el trabajo a realizar (en forma de tareas) y lo que se requiere para llevar a cabo ese trabajo (a través de conocimientos y habilidades).

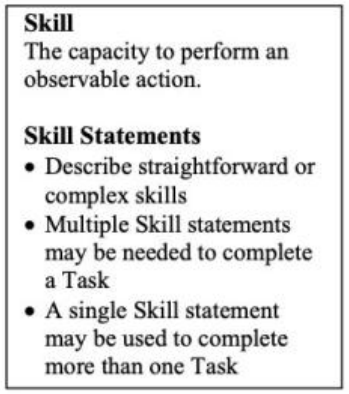
Estos módulos son estructuras organizativas que facilitan el uso y la aplicación del marco NICE.

Proporcionan un mecanismo mediante el cual tanto las organizaciones como los individuos pueden comprender el alcance y el contenido del Marco NICE.

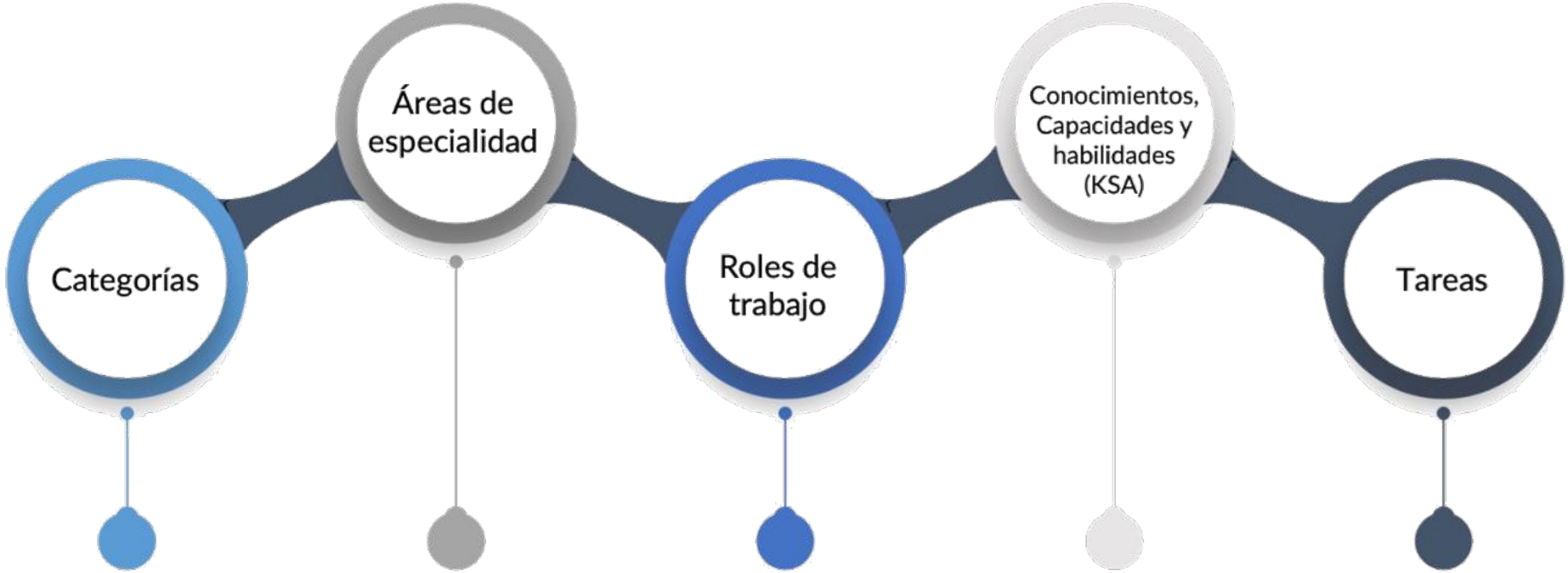
Estos módulos se conciben como directrices que pueden utilizarse para mejorar la comprensión y no como estructuras rígidas.







Elementos del NICE



Las categorías proporcionan la estructura organizativa general del marco NICE.

Las categorías contienen agrupaciones de trabajo de ciberseguridad, que se denominan Áreas de especialidad. Y son 33 en la versión 2.0.

Las áreas de especialidad contienen agrupaciones más detalladas de trabajo de ciberseguridad que se componen de conocimientos específicos. Y son 52 en la versión 2.0.

El conocimiento, las capacidades y las habilidades (KSA) son los atributos necesarios para desempeñar funciones de trabajo.

Una tarea es un trabajo específico que, combinado con otras Tareas identificadas, compone el trabajo en un área de especialidad específica o rol de trabajo.

Elementos del NICE

Task
An activity that is directed toward the achievement of organizational objectives.

Task Statements
- Easy to read and understand
- Begin with the activity being executed
- Do not contain the task objective

Tareas
Una tarea puede definirse como una actividad dirigida a la consecución de los objetivos de la organización, incluidos los objetivos empresariales, tecnológicos o de misión.

Una Declaración de Tarea
O Las tareas deben ser sencillas.
O Comenzar con la actividad que se está ejecutando.
O No contener el objetivo de la tarea.

Enunciados de tareas

Las declaraciones de tareas describen el trabajo, mientras que las declaraciones de conocimientos y destrezas describen al alumno.

Las declaraciones de tareas deben centrarse en el lenguaje organizativo y los patrones de comunicación que aportan valor a la organización.

Estas declaraciones están diseñadas para describir el trabajo que debe realizarse y deben estar en consonancia con el contexto de la organización.

Una declaración de Tarea debe ser sencilla
Ejemplo: Diligenciamiento bitácora de monitoreo

Una declaración de Tarea comienza con la actividad que se está ejecutando.
Ejemplo: Solucionar problemas de hardware y software del sistema.

Elementos del NICE

Task
An activity that is directed toward the achievement of organizational objectives.

Task Statements
- Easy to read and understand
- Begin with the activity being executed
- Do not contain the task objective

Tareas
Una tarea puede definirse como una actividad dirigida a la consecución de los objetivos de la organización, incluidos los objetivos empresariales, tecnológicos o de misión.

Una Declaración de Tarea
O Las tareas deben ser sencillas.
O Comenzar con la actividad que se está ejecutando.
O No contener el objetivo de la tarea.

Una declaración de Tarea no contiene el objetivo dentro de la declaración, ya que el objetivo puede variar en función de los impulsores de la misión y las necesidades de la organización. *Ejemplo: Realizar ejercicios de formación interactivos.*

En el ejemplo anterior, el propósito de estos ejercicios puede ser crear un entorno de aprendizaje eficaz, pero ese objetivo no está incluido en la propia declaración de Tarea.

Elementos del NICE

Knowledge
A retrievable set of concepts within memory.

Knowledge Statements
- Describe foundational or specific Knowledge
- Multiple statements may be needed to complete a Task
- A single statement may be used to complete many different Tasks

Conocimientos
Conjunto recuperable de conceptos en la memoria.

Enunciados de conocimiento
O Describen conocimientos fundamentales o específicos
O Pueden necesitarse varios enunciados para completar una tarea.
O Un único enunciado puede utilizarse para realizar varias tareas diferentes.

Enunciados de conocimiento

Los enunciados de Conocimiento se relacionan con los enunciados de Tarea en el sentido de que sólo con la comprensión descrita por el enunciado de Conocimiento podrá el alumno completar la Tarea.
El conocimiento se define como un conjunto recuperable de conceptos en la memoria.
Los enunciados de Conocimiento pueden describir conceptos fundamentales o específicos.
Es posible que se necesiten varios enunciados de Conocimiento para completar una Tarea determinada.
Del mismo modo, un enunciado de Conocimiento puede utilizarse para completar muchas Tareas diferentes.

Una declaración de conocimiento debe ser fundacional.
Ejemplo: Conocimiento de las amenazas y vulnerabilidades del ciberespacio.

Elementos del NICE

Knowledge
A retrievable set of concepts within memory.

Knowledge Statements
- Describe foundational or specific Knowledge
- Multiple statements may be needed to complete a Task
- A single statement may be used to complete many different Tasks

Conocimientos
Conjunto recuperable de conceptos en la memoria.

Enunciados de conocimiento
O Describen conocimientos fundamentales o específicos
O Pueden necesitarse varios enunciados para completar una tarea.
O Un único enunciado puede utilizarse para realizar varias tareas diferentes.

Una declaración de conocimiento debe ser específica
Ejemplo: Conocimiento de las fuentes de difusión de información sobre vulnerabilidades (por ejemplo, alertas de proveedores, avisos gubernamentales, erratas en la literatura de productos y boletines sectoriales).

Las organizaciones que elaboran Declaraciones de conocimientos deben tener en cuenta los distintos niveles de conocimiento y experiencia de los alumnos.

Un ejemplo de estos distintos niveles se describe en la Taxonomía de Bloom (revisada), que utiliza un lenguaje que facilita la observación y la evaluación del alumno.

Elementos del NICE

Skill
The capacity to perform an observable action.

Skill Statements
- Describe straightforward or complex skills
- Multiple Skill statements may be needed to complete a Task
- A single Skill statement may be used to complete more than one Task

Habilidad
Capacidad de realizar una acción observable.

Enunciados de Habilidad
- Describen habilidades sencillas o complejas
- Pueden ser necesarias varias Declaraciones de Habilidad para completar una Tarea
- Una única Declaración de Habilidad puede utilizarse para realizar más de una Tarea.

Enunciados de Habilidades

Los enunciados de habilidades se relacionan con los enunciados de Tarea en el sentido de que un alumno está demostrando destrezas en la realización de tareas.
Un alumno que no sea capaz de demostrar la habilidad descrita no podrá completar la Tarea que depende de dicha habilidad.
Una habilidad se define como la capacidad de realizar una acción observable. Los enunciados de Habilidad pueden describir destrezas sencillas o complejas.
Pueden ser necesarias varias Declaraciones de Habilidad para completar una Tarea determinada. Del mismo modo, el ejercicio de una habilidad puede utilizarse para completar más de una tarea.

Una declaración de habilidad debe ser sencilla
Ejemplo: Reconocer las alertas de un sistema de detección de intrusos.

Elementos del NICE

Skill
The capacity to perform an observable action.

Skill Statements
- Describe straightforward or complex skills
- Multiple Skill statements may be needed to complete a Task
- A single Skill statement may be used to complete more than one Task

Habilidad
Capacidad de realizar una acción observable.

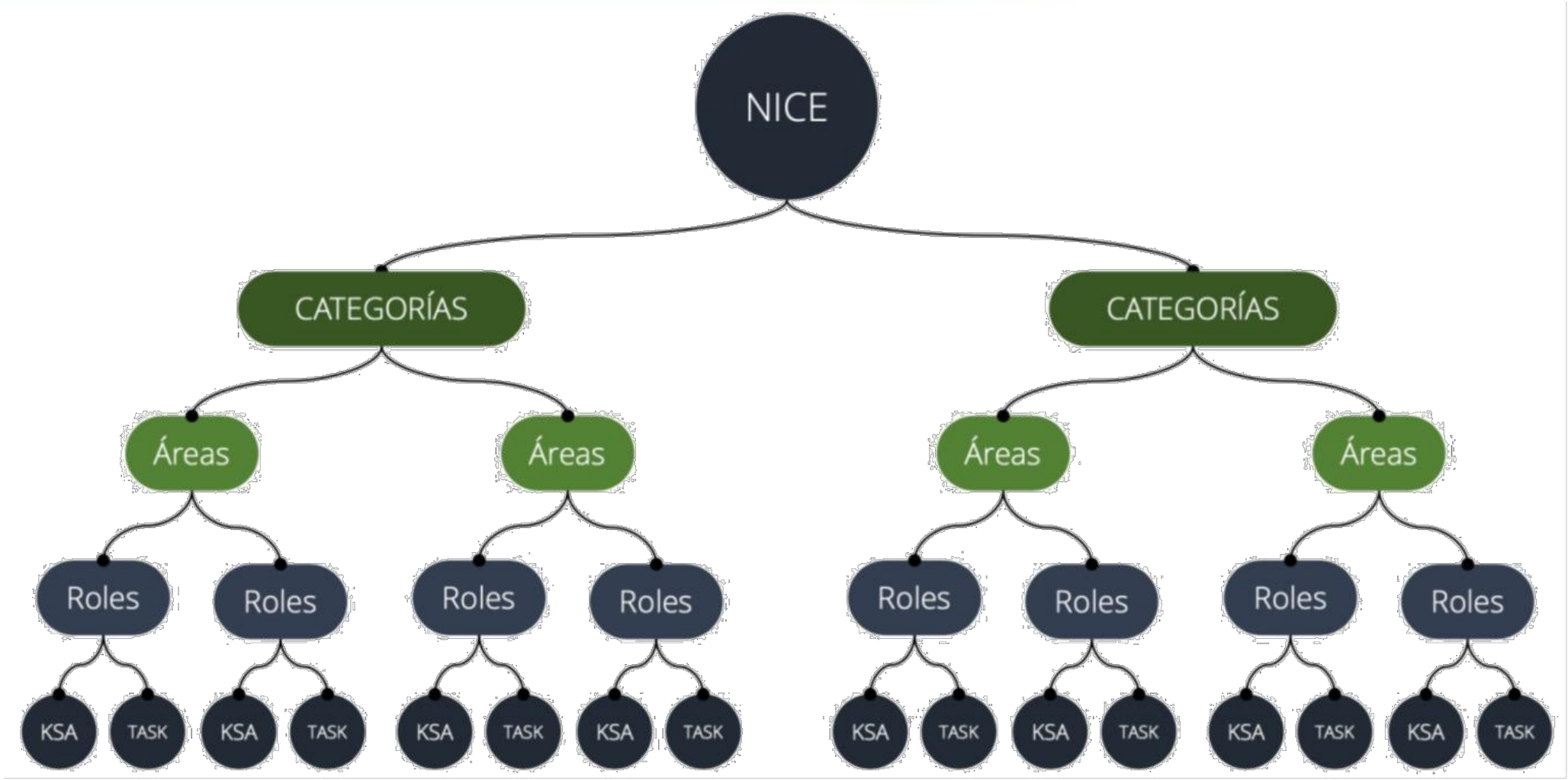
Enunciados de Habilidad
O Describen habilidades sencillas o complejas
O Pueden ser necesarias varias Declaraciones de Habilidad para completar una Tarea
O Una única Declaración de Habilidad puede utilizarse para realizar más de una Tarea.

Una declaración de habilidad puede ser complejo
Ejemplo: Destreza para generar una hipótesis sobre la forma en que un agente de amenazas burló el Sistema de Detección de Intrusiones.

Las habilidades describen lo que el alumno puede hacer, mientras que las tareas describen el trabajo a realizar.

Por lo tanto, es importante separar el lenguaje utilizado entre las Habilidades y las Tareas y utilizar términos que faciliten la observación y la evaluación del alumno.

Elementos del NICE



Usando el NICE Framework NIST SP 800-18

LCSPC™ Versión 062024

Usando el NICE Framework

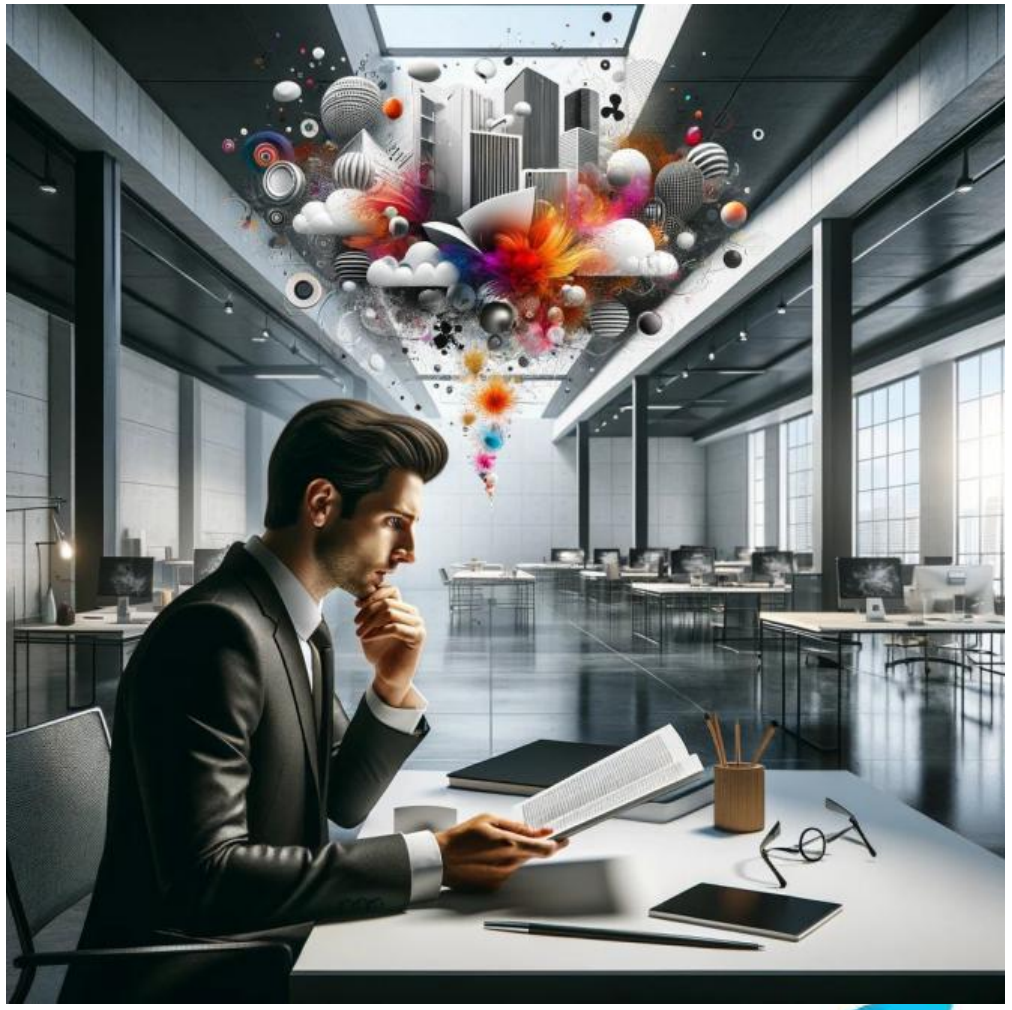
Usando el NICE Framework

En particular, aunque el Marco de la fuerza de trabajo para la ciberseguridad (Marco NICE) tiene por objeto proporcionar un conjunto común de bloques de construcción de los que muchos puedan partir, algunas organizaciones encontrarán la necesidad de adaptar el modelo para alinearse más estrechamente con su contexto único.

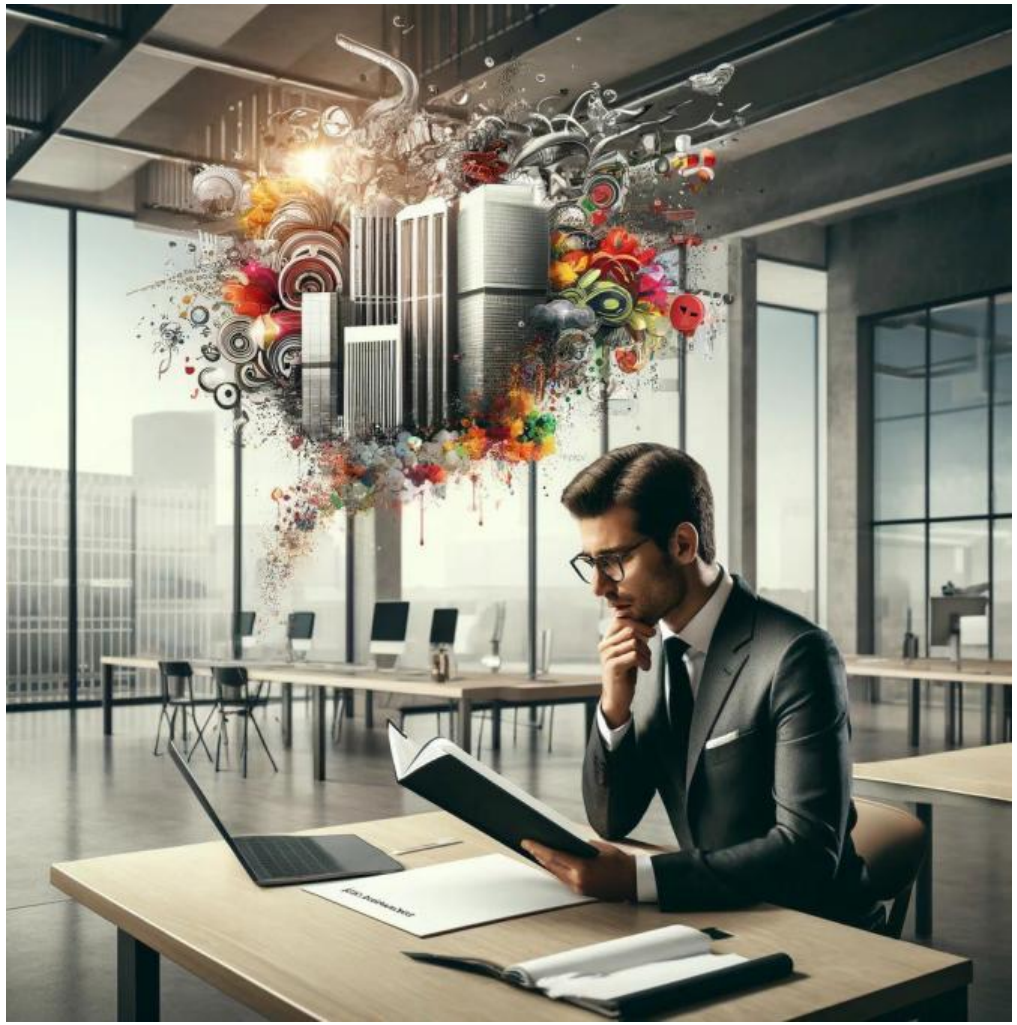
Por ejemplo, un fabricante puede tener tareas específicas del sector o de la organización que no se describen en el Marco NICE.

Otros pueden encontrar que las Tareas son aplicables, pero necesitan ajustar o desarrollar declaraciones específicas de K&S para aumentar la probabilidad de que las Tareas puedan ser completadas según lo definido por su contexto único.

Como tales, estos elementos constitutivos no pretenden ser rígidos, sino proporcionar un lenguaje común para que las organizaciones o los sectores lo utilicen de forma beneficiosa para un contexto determinado.



Usando el NICE Framework



Por último, los ejemplos de utilización de los elementos constitutivos del Marco NICE que se ofrecen a continuación son de naturaleza teórica o conceptual; una organización puede utilizar los elementos constitutivos de cualquier forma para satisfacer mejor las necesidades locales.

Estos ejemplos pretenden ilustrar posibles enfoques prácticos del Marco NICE que han demostrado ayudar a alcanzar objetivos organizativos comunes.

Proporcionan orientación a las organizaciones o sectores que buscan un punto de partida y no una forma única de utilizar el Marco NICE.

Usando el NICE Framework

Utilización de las declaraciones de tareas, conocimientos y habilidades (TKS) existentes

Los usuarios del Marco NICE hacen referencia a uno o más enunciados de Tareas, Conocimientos y Habilidades (enunciados TKS), como se describe en la Sección 2, para describir tanto el trabajo como a los alumnos.

Los enunciados de tarea se utilizan para describir el trabajo.

Las Enunciados de Tarea tienen asociados Enunciados de Conocimientos y Habilidades.
Aunque un enunciado de Tarea puede tener un conjunto recomendado de enunciados K&S asociados, los usuarios pueden incluir otros enunciados K&S existentes para adaptar las Tareas a su contexto único.

Las afirmaciones de C&S se utilizan para describir a los alumnos.

Las afirmaciones de K&S pueden utilizarse de muchas maneras para gestionar la fuerza de trabajo de ciberseguridad.

Pueden usarse en parte, en su totalidad, o no usarse en absoluto, dependiendo del contexto único de la organización implementadora.

Los ejemplos teóricos de uso que se muestran a continuación demuestran las áreas en las que podrían implementarse las declaraciones TKS:

- Programa de seguimiento de las habilidades de los empleados para determinar las cualificaciones para ascensos.
- Conocimientos necesarios para completar un curso.
- Lista de tareas semanales para completar en una organización.

Usando el NICE Framework

Creación de nuevas declaraciones TKS

Se advierte a los usuarios que no modifiquen el texto de las declaraciones TKS existentes del Marco NICE.

Las declaraciones están pensadas para apoyar la interoperabilidad, por lo que cambiar su contenido puede dar lugar a una desalineación posterior cuando se utilicen fuentes externas.

Si se necesita una redacción diferente en una declaración TKS para apoyar el contexto único de un usuario, se puede crear una nueva declaración.

Los usuarios también pueden crear declaraciones de Tareas, Conocimientos o Habilidades completamente nuevas para ayudar a adaptar el uso del Marco NICE al uso local dentro de su contexto único.

Estos enunciados adicionales ayudarán a mantener debates internos claros y coherentes sobre los alumnos y sus actividades laborales.

Usando el NICE Framework

Competency
A mechanism for organizations to assess learners.

Competencies are
- Defined via an employer-driven approach
- Learner-focused
- Observable and measurable

Competencia
Un mecanismo para que las organizaciones evalúen a los alumnos.
Las competencias son
- Definidas por el empleador
- Centradas en el alumno
- Observables y Medibles

Competencias

Las competencias ofrecen a las organizaciones un mecanismo para evaluar a los alumnos. Las competencias se definen a través de un enfoque impulsado por el empleador que proporciona una visión del contexto único de una
organización.

Además, las competencias permiten a los proveedores de educación y formación responder a las necesidades del empleador o del sector mediante el desarrollo de experiencias de aprendizaje que ayuden a los alumnos a desarrollar y demostrar las competencias.

Las competencias constan de un nombre, una descripción de la competencia, un método de evaluación y un grupo de enunciados TKS asociados.

Usando el NICE Framework

Competency
A mechanism for organizations to assess learners.

Competencies are
- Defined via an employer-driven approach
- Learner-focused
- Observable and measurable

Competencia
Un mecanismo para que las organizaciones evalúen a los alumnos.

Las competencias son
- **O** Definidas por el empleador
- **O** Centradas en el alumno
- **O** Observables y Medibles

Las competencias ofrecen flexibilidad al permitir a las organizaciones agrupar varias afirmaciones del TKS en una categoría que define una necesidad general.

Mientras que una Tarea individual y sus declaraciones de Conocimientos y Habilidades asociadas pueden no cambiar, la Competencia definida de forma más amplia puede introducir nuevas Tareas o incluso Conocimientos y Habilidades individuales - o eliminar los existentes en respuesta a las necesidades cambiantes en un ecosistema de ciberseguridad cambiante.

Usando el NICE Framework

Competencias

Existen varias formas de utilizar las competencias. Por ejemplo, como se muestra en la Figura, una organización podría utilizar las Competencias como parte del proceso de contratación destinado a cumplir objetivos organizativos específicos.

En este caso, las competencias podrían definirse como un grupo de declaraciones de tareas relacionadas. La organización podría utilizar estas Competencias para evaluar si un candidato puede realizar esas Tareas.

Esta evaluación podría adoptar la forma de una entrevista, una prueba previa a la contratación o una observación del aprendizaje basado en el trabajo.

Los ejemplos anteriores son teóricos.

Pueden utilizarse en parte, en su totalidad o no utilizarse en absoluto, en función del contexto específico de la organización que los aplique.

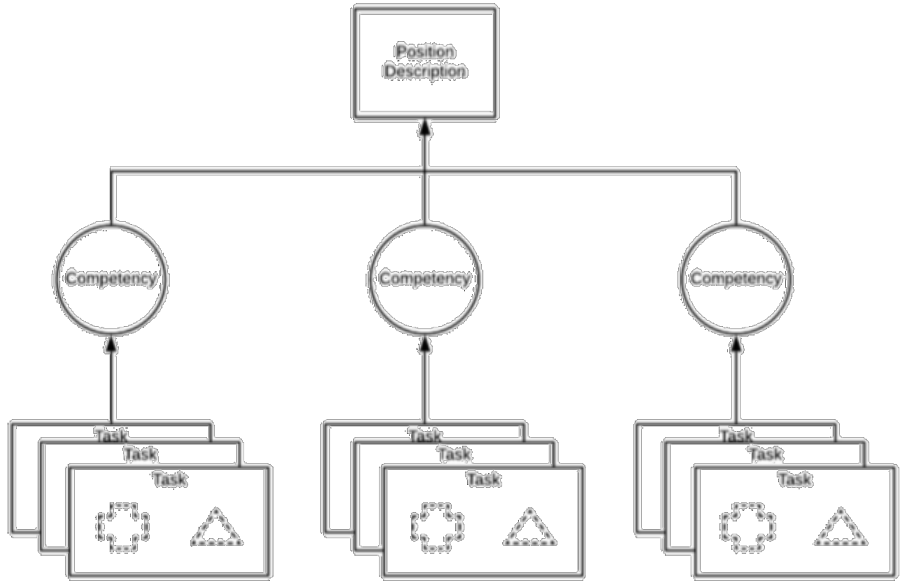


Figure 2. Using Competencies to Assess Learners through a Position Description

Usando el NICE Framework

Otras organizaciones podrían utilizar las Competencias para determinar si un alumno ha alcanzado un conjunto definido de Habilidades y Conocimientos.

Como se muestra en la figura, estas organizaciones podrían optar por utilizar las competencias como grupos de enunciados de conocimientos y habilidades.

A continuación, estas organizaciones podrían evaluar a los alumnos en relación con estos enunciados de conocimientos y habilidades.

Las evaluaciones podrían adoptar la forma de exámenes, demostraciones de laboratorio o evaluaciones orales.

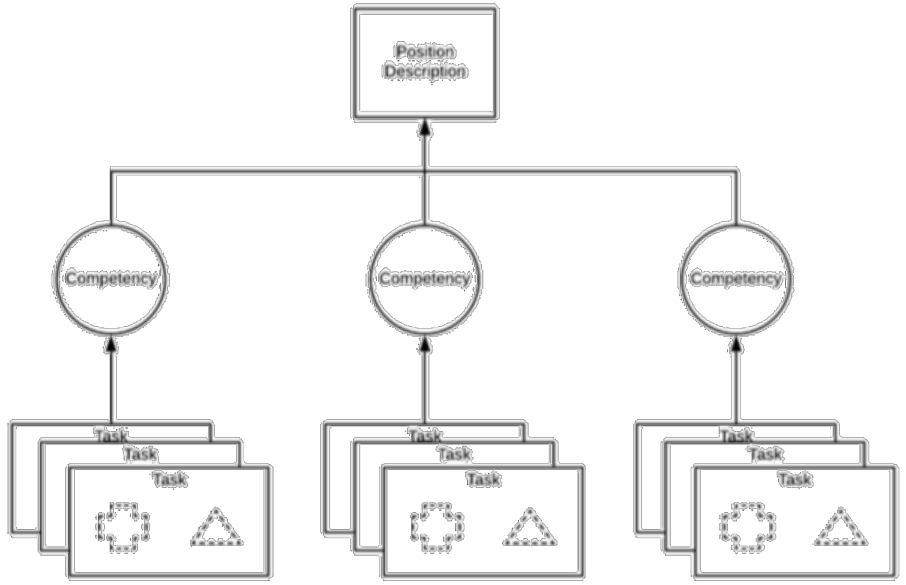


Figure 2. Using Competencies to Assess Learners through a Position Description

Usando el NICE Framework

Utilizar las competencias existentes

Las Competencias del Marco NICE son una forma de que las organizaciones se alineen con el Marco NICE a un alto nivel sin profundizar en los detalles de las declaraciones TKS.

Las competencias son una forma de describir la evaluación de un alumno. Al permitir grupos de declaraciones TKS definidos por la organización, las competencias permiten a las organizaciones comunicar de forma sucinta y organizar eficazmente su trabajo de ciberseguridad con el fin de proporcionar una visión racionalizada de la fuerza de trabajo.

Otros usos potenciales de las Competencias incluyen:

- Describir tipos de tareas dentro de un puesto determinado
- Realizar un seguimiento de las capacidades de la plantilla
- Describir los requisitos del equipo Demostrar las capacidades del alumno

Usando el NICE Framework

Aunque una competencia tiene un conjunto recomendado de afirmaciones TKS asociadas, los usuarios pueden añadir o eliminar afirmaciones existentes para adaptar las competencias a su contexto particular.

Sin embargo, se advierte a los usuarios que no modifiquen el título o la descripción de una competencia del Marco NICE

Las competencias están pensadas para favorecer la interoperabilidad, por lo que modificar su contenido puede dar lugar a una desalineación posterior cuando se utilicen fuentes externas.

Si se necesita una redacción diferente en una competencia para apoyar el contexto único de un usuario, se puede crear una nueva competencia tal y como se describe a continuación...

Usando el NICE Framework

Creando nuevas competencias

Algunas organizaciones pueden necesitar describir una Competencia para el contexto específico de su trabajo de ciberseguridad.

El Marco NICE, desarrollado con el principio de agilidad, permite a las organizaciones describir una Competencia para satisfacer un ecosistema de ciberseguridad cambiante.

Esto podría hacerse modificando una competencia existente para satisfacer las necesidades locales o creando una competencia completamente nueva.
A continuación, se ofrecen dos ejemplos teóricos para explicar los posibles procesos de utilización de las Competencias.

Los dos ejemplos se centran en el Análisis de Datos para mostrar que la misma Competencia puede utilizarse a través de diferentes enfoques. Además, estos ejemplos se basan en las Figuras anteriores para que el lector pueda comprender su posible aplicación.
Estos ejemplos utilizan una estructura de tabla para comunicar la Competencia.

Este enfoque tabular es uno de los muchos que podría utilizar una organización que desee implantar Competencias.

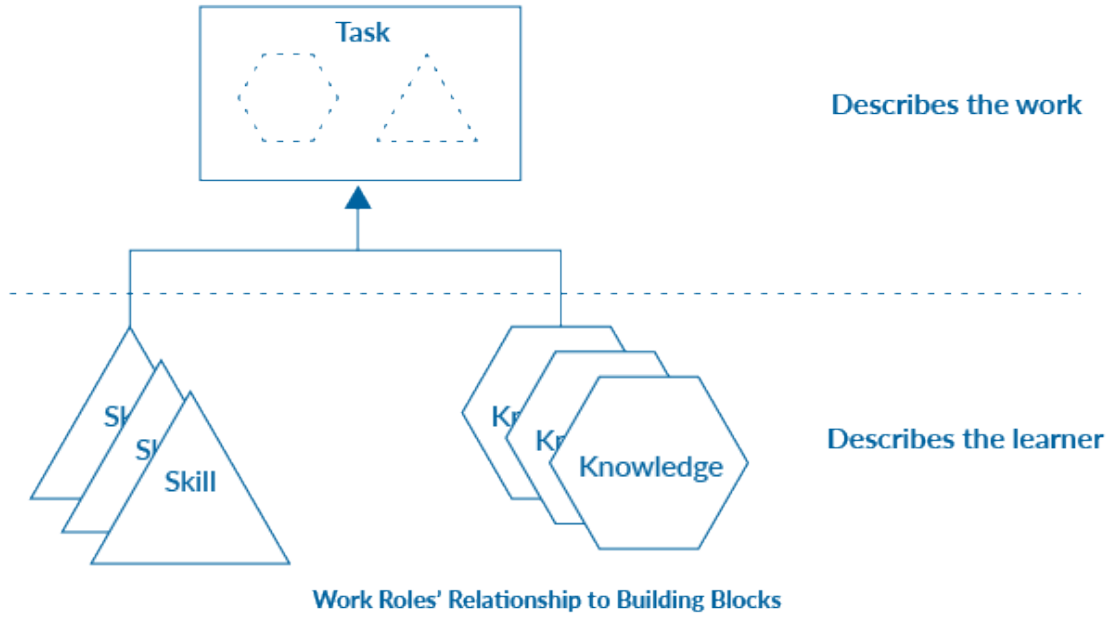
Usando el NICE Framework

Roles de Trabajo

Los roles de trabajo son un caso de uso común del marco NICE.

Las funciones de trabajo son una forma de describir un conjunto de tareas de las que alguien es responsable.
Mientras que los anteriores marcos de recursos humanos también asociaban funciones de trabajo con especificaciones de conocimientos, destrezas y habilidades, el marco NICE fomenta un enfoque más ágil a través de las tareas.

Los Roles de Trabajo se componen de Tareas que constituyen el trabajo a realizar; las Tareas incluyen declaraciones de Conocimientos y Habilidades asociadas que representan el potencial de los alumnos para realizar esas Tareas.
Este enfoque transitivo, ilustrado en la figura, favorece la flexibilidad y simplifica la comunicación.



Work Roles' Relationship to Building Blocks

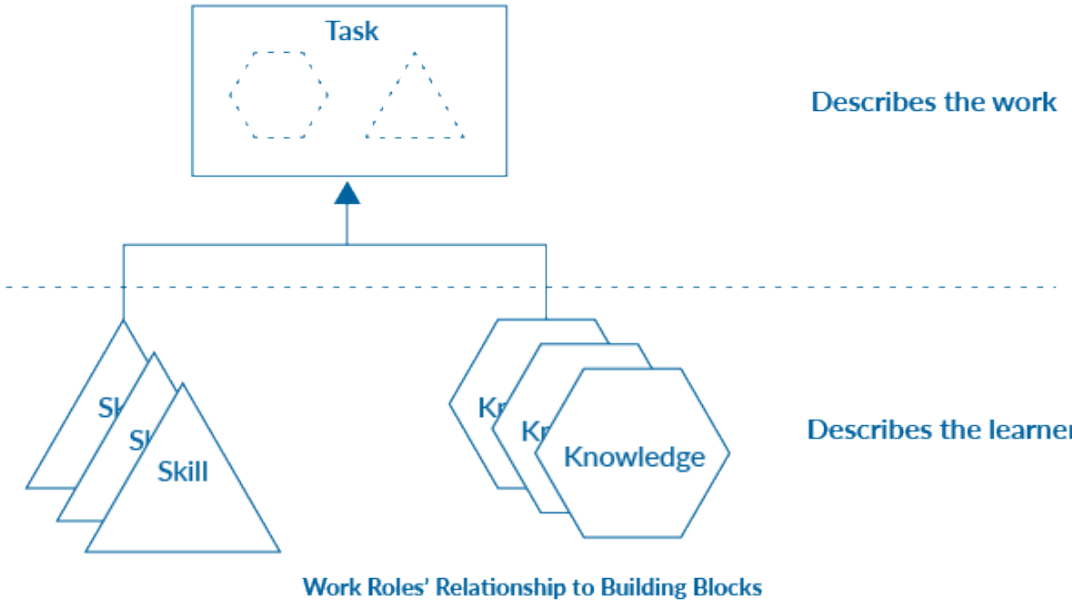
Usando el NICE Framework

Los nombres de los roles de trabajo no son sinónimos de los títulos de los puestos. Algunos Roles de Trabajo pueden coincidir con un título de trabajo dependiendo del uso que haga la organización de los títulos de trabajo.

Además, los roles de trabajo no son sinónimos de ocupaciones.
Un único rol de trabajo (por ejemplo, desarrollador de software) puede aplicarse a personas con varios títulos de trabajo (por ejemplo, ingeniero de software, programador, desarrollador de aplicaciones). A la inversa, podrían combinarse varios roles para crear un puesto de trabajo concreto.

Este enfoque aditivo favorece un mayor modularidad e ilustra el hecho de que todos los alumnos de la población activa desempeñan numerosas tareas en diversas funciones, independientemente de sus títulos laborales.

Del mismo modo, el Marco NICE no define niveles de competencia (por ejemplo, Básico, Intermedio, Avanzado). Tales atributos, y los relativos a la competencia con la que un alumno realiza las tareas, se dejan para otros modelos o recursos.



Work Roles' Relationship to Building Blocks

Usando el NICE Framework

Utilizar roles de trabajo existentes

Cada Rol de Trabajo está destinado a apoyar la consecución de objetivos a través de Tareas. Aunque un Rol de Trabajo puede tener un conjunto predeterminado de Tareas asociadas, los usuarios pueden incluir otras Tareas existentes para adaptar los Roles de Trabajo a su contexto único.

Del mismo modo, un usuario puede desear basarse en los roles de trabajo enumerados o añadir otros para apoyar objetivos adicionales. El conjunto actual de componentes del Marco NICE está disponible en el Centro de Recursos del Marco NICE.

Se advierte a los usuarios que no modifiquen internamente el nombre y la descripción de un rol de trabajo existente. Los roles de trabajo están pensados para apoyar la interoperabilidad, por lo que cambiar su contenido puede dar lugar a una desalineación posterior.

Si se necesita una redacción diferente, se puede crear un nuevo rol de trabajo como se describe a continuación.

Usando el NICE Framework

Creando un nuevo rol de trabajo

Los usuarios también pueden crear nuevos roles de trabajo para ayudar a adaptar el uso del Marco NICE a su contexto único.

Estos roles de trabajo adicionales ayudarán a mantener debates internos claros y coherentes sobre el trabajo de ciberseguridad.

Usando el NICE Framework

Equipos

Muchas organizaciones utilizan equipos para abordar colectivamente retos complejos reuniendo a personas con conocimientos y experiencia complementarios.

Al utilizar diferentes recursos y perspectivas, los equipos permiten a las organizaciones gestionar los riesgos de forma holística.

Los equipos aprovechan la especialización de los conocimientos y procesos de cada miembro para distribuir eficazmente el trabajo.

Los equipos pueden definirse utilizando funciones de trabajo o competencias.

Construyendo equipos con roles de trabajo

Un enfoque de la creación de equipos centrado en los roles de trabajo permite a las organizaciones definir qué tipos de roles de trabajo son necesarios para alcanzar los objetivos definidos.

Dado que los roles de trabajo se componen a su vez de competencias, este enfoque de la creación de equipos parte del trabajo que debe realizarse.

Este enfoque puede considerarse "descendente".

Usando el NICE Framework

Categorías de Roles de Trabajo

Analizar
Realiza una revisión y evaluación altamente especializada de la información de seguridad cibernética entrante para determinar su utilidad para la inteligencia.

Recolectar y Operar
Proporciona operaciones especializadas de denegación y engaño, y recopila información de ciberseguridad que puede usarse para desarrollar inteligencia.

Investigar
Investiga eventos de ciberseguridad o delitos relacionados con los sistemas, redes y pruebas digitales de tecnología de la información (T.I).

Operar y Mantener
Proporciona el soporte, la administración y el mantenimiento necesarios para garantizar el rendimiento y la seguridad del sistema de tecnología de la información (T.I) eficaz y eficiente.

Supervisar y Gobernar
Proporciona liderazgo, gestión, dirección o desarrollo y promoción para que la organización pueda realizar efectivamente el trabajo de ciberseguridad.

Proteger y Defender
Identifica, analiza y mitiga las amenazas a los sistemas y/o redes de tecnología interna de la información (T.I).

Provisión Segura
Conceptualiza, diseña, procura y/o construye sistemas seguros de tecnología de la información (T.I), con la responsabilidad de los aspectos del desarrollo del sistema y/o la red.

Usando el NICE Framework

Table 3 - Example of a Secure Software Development Team Using the NICE Framework 2017 Work Roles

Lifecycle Phase	Work Role
Design	SP-ARC-002 | Security Architect
Build	SP-DEV-001 | Software Developer
Deploy	OM-NET-001 | Network Operations Specialist
Operate	OM-STS-001 | Technical Support Specialist
Maintain	OM-DTA-001 | Database Administrator
Decommission	OV-LGA-001 | Cyber Legal Advisor

La Tabla 3 muestra una forma de crear un equipo de desarrollo de software seguro.
Los roles de trabajo están referenciados utilizando la versión 2017 de los IDs de roles de trabajo del Marco NICE. Los equipos construidos de esta manera comienzan con la identificación del trabajo que debe llevarse a cabo.
En este ejemplo, el equipo de desarrollo de software seguro se organiza por fase del ciclo de vida.
La primera fila ilustra que el equipo tendría en cuenta los objetivos de la fase de Diseño, incluida la planificación, y por tanto necesitaría un Arquitecto de Seguridad.

La Tabla 3 es un ejemplo informativo y no cubre todos los Roles de Trabajo que pueden estar presentes o ser necesarios para un Equipo dado. Para más información, véase el Marco de Desarrollo Seguro de Software del NIST.

Usando el NICE Framework

Table 4 - Example Creating A Cybersecurity Team Using NICE Framework 2017 Work Roles and New Work Roles

Cybersecurity Framework Function	Work Role
Identify	NewWorkRole1 | Risk Manager
Protect	SP-RSK-002 | Security Control Assessor
Detect	PR-CDA-001 | Cyber Defense Analyst
Respond	PR-CIR-001|Cyber Defense Incident Responder
Recover	NewWorkRole2 | Communications Specialist

La Tabla 4 describe un ejemplo de equipo de ciberseguridad. Al igual que el equipo de desarrollo de software seguro, el equipo de ejemplo se construye con un enfoque centrado en el trabajo. Utilizando el Núcleo del Marco para Mejorar la Ciberseguridad de las Infraestructuras Críticas (Marco de Ciberseguridad), se seleccionan los objetivos de ciberseguridad, se identifican las Tareas para alcanzar esos objetivos, y se seleccionan los Roles de Trabajo para definir los roles necesarios para apoyar esos objetivos.

La Tabla 4 es un ejemplo informativo y no cubre todos los Roles de Trabajo que pueden estar presentes o ser necesarios para un Equipo dado. Se añaden dos nuevos Roles de Trabajo para mostrar un enfoque mixto de uso de Roles de Trabajo existentes (Sección 3.4.1) y creación de nuevos Roles de Trabajo (Sección 3.4.2). Al crear nuevas Funciones de Trabajo, el ejemplo demuestra un enfoque flexible y ágil para la adaptación del Marco NICE.

Usando el NICE Framework

Crear equipos con competencias

Los equipos también pueden construirse utilizando Competencias. Este enfoque de la creación de equipos reconoce que las Tareas individuales pueden ser desconocidas, pero se conocen los tipos de Competencias necesarias para resolver el reto. Este enfoque puede considerarse "ascendente". Por lo tanto, los equipos construidos de esta manera pueden ayudar a identificar a los alumnos que pueden participar en el trabajo del equipo en el futuro. Estos alumnos pueden o no estar asociados a un Rol de Trabajo y simplemente poseer las Competencias necesarias para ayudar a cumplir los objetivos de la organización.

Por ejemplo, un equipo defensivo de ciberseguridad que utiliza sus habilidades para imitar las técnicas de ataque de los adversarios (es decir, un "Equipo Rojo") puede estar compuesto por las siguientes Competencias teóricas:

- Planificación del compromiso
- Reglas de actuación
- Pen Testing
- Recogida de datos
- Explotación de vulnerabilidades

Mediante la creación de equipos u otras agrupaciones TKS, cada organización puede adaptar el Marco NICE de la forma que mejor ayude a aplicar y comunicar sobre los alumnos para permitir la consecución de los objetivos de la misión.

Conclusiones NICE NIST SP 800-18

Conclusión

A través de la aplicación del enfoque de bloques de construcción descrito por el Marco NICE, los usuarios pueden beneficiarse de un método coherente para organizar y comunicar el trabajo a realizar a través de declaraciones de Tareas y los Conocimientos y Habilidades de los alumnos individuales que apoyan ese trabajo.

El Marco NICE ayuda a guiar los esfuerzos de los empleadores para describir el trabajo de ciberseguridad, a los proveedores de educación y formación para preparar a los trabajadores de ciberseguridad, y a los alumnos para demostrar sus capacidades para realizar el trabajo de ciberseguridad.
La capacidad de describir tareas, conocimientos y habilidades es importante para garantizar una comprensión global del trabajo y de la mano de obra.

El Marco NICE proporciona un recurso de referencia extensible que puede ser aplicado y utilizado por diversas organizaciones o sectores para describir el trabajo a realizar en muchas áreas.

Los beneficios para estas organizaciones apoyan la misión de NICE de dinamizar, promover y coordinar una comunidad sólida que trabaje conjuntamente para avanzar en un ecosistema integrado de educación, formación y desarrollo de la mano de obra en ciberseguridad.

NICE Framework – Áreas de Competencia NIST IR 8355

NICE NIST IR 8355

Áreas de Competencia

Esta publicación de NICE describe las Áreas de Competencia incluidas en el Marco de la Fuerza Laboral para la Ciberseguridad (Marco NICE), Publicación Especial 800-181 del NIST, Revisión 1. El Marco NICE es una referencia fundamental para describir y compartir información sobre el trabajo en ciberseguridad.

En su núcleo se encuentran las declaraciones de Tareas, Conocimientos y Habilidades (TKS) que proporcionan una base para los alumnos, incluidos estudiantes, solicitantes de empleo y empleados. Estos enunciados se utilizan para definir las Áreas de Competencia -grupos de enunciados de Conocimientos y Habilidades relacionados que se correlacionan con la capacidad de una persona para realizar Tareas en un dominio particular- y los Roles de Trabajo, que se componen de enunciados de Tareas que constituyen el trabajo del que alguien es responsable.

Este documento ofrece más detalles sobre lo que son las Áreas de Competencia del Marco NICE, incluyendo su evolución y desarrollo, aclara las diferencias entre las Áreas de Competencia y los Roles de Trabajo, y proporciona ejemplos de uso de las Áreas de Competencia desde las perspectivas de varias partes interesadas. Por último, la publicación identifica dónde se publica por separado la lista de Áreas de Competencia del Marco NICE y se mantiene separada de esta publicación para que pueda actualizarse con mayor frecuencia como recurso de referencia flexible y actual.

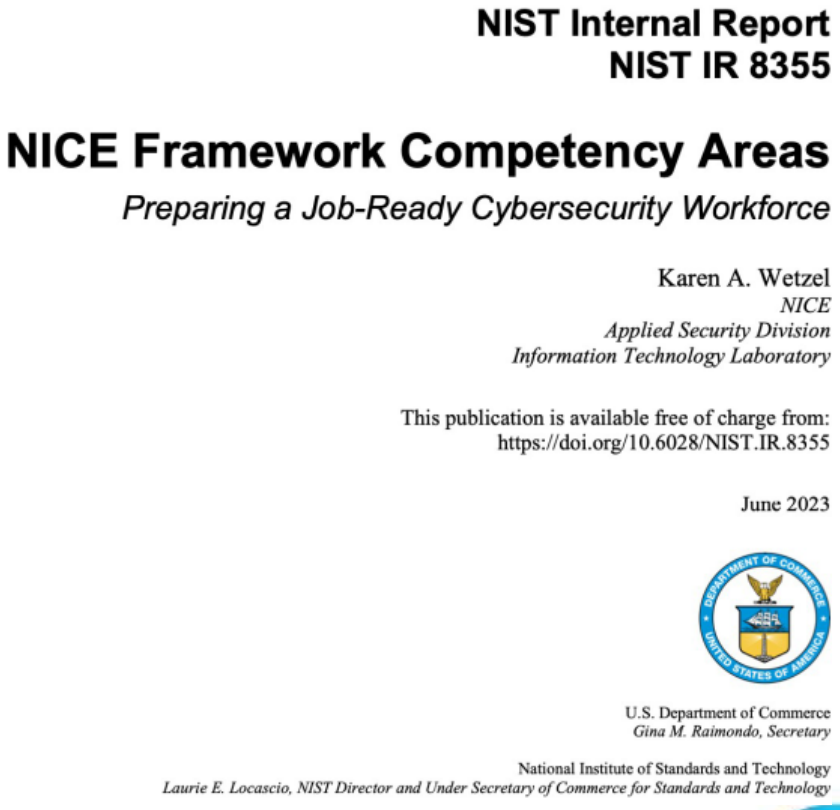
NICE NIST IR 8355

Audiencia

El Marco NICE sirve de puente entre los empleadores y los proveedores de educación, formación y certificación, así como de herramienta para ayudar a los alumnos a determinar sus necesidades y demostrar sus capacidades.

Un enfoque estandarizado de las áreas de competencia proporciona información accesible sobre lo que los individuos necesitan saber y ser capaces de hacer, permite el desarrollo de un aprendizaje más eficaz y establece procesos regulares para describir y validar de forma coherente las capacidades de un alumno.

Por lo tanto, las partes interesadas y los destinatarios de este trabajo son los empleadores, los profesionales del desarrollo de la mano de obra y de los recursos humanos, los proveedores de educación, formación y certificación, y los alumnos.



NIST Internal Report
NIST IR 8355

NICE Framework Competency Areas

Preparing a Job-Ready Cybersecurity Workforce

Karen A. Wetzel
NICE
Applied Security Division
Information Technology Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8355

June 2023

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

NICE Áreas de Competencia

El NICE publicó el Marco de la fuerza de trabajo para la ciberseguridad (Marco NICE), Publicación especial 800-181 del NIST, Revisión 1, en noviembre de 2020.

El Marco NICE revisado estableció un conjunto de bloques de construcción -enunciados de Tareas, Conocimientos y Habilidades- que describen el trabajo de ciberseguridad y lo que alguien debe saber o ser capaz de hacer para completar ese trabajo. También identifica formas comunes de aplicar estos componentes básicos, sobre todo a través de las funciones laborales y, como novedad en la revisión 1 del marco NICE, las áreas de competencia.

Las Áreas de Competencia del Marco NICE agrupan declaraciones relacionadas de Tareas, Conocimientos y Habilidades (TKS) para formar una descripción de alto nivel de las capacidades típicamente necesarias en un dominio particular de ciberseguridad.

Al definir claramente lo que una persona necesita saber y hacer para desempeñarse bien en un área definida de trabajo de ciberseguridad, las áreas de competencia proporcionan un medio para comunicar las necesidades de los empleadores, las capacidades de los alumnos (que, a los efectos del Marco NICE, incluye a estudiantes, solicitantes de empleo y empleados) y el valor de la educación, la formación y las certificaciones.

NICE Áreas de Competencia

Learners: Individuals who perform cybersecurity work, including students, job seekers, and employees.

Alumnos: Personas que realizan trabajos de ciberseguridad, incluidos estudiantes, solicitantes de empleo y empleados.

Las áreas de competencia se definen mediante un enfoque impulsado por el empleador que permite a los proveedores de educación y formación responder a las necesidades del empleador o del sector creando experiencias que ayuden a los alumnos a desarrollar y demostrar capacidades pertinentes y necesarias.

Se correlacionan con el rendimiento en el trabajo y pueden mejorarse a través de la educación, la formación (incluido el aprendizaje en el puesto de trabajo) u otras experiencias de aprendizaje.

NICE Áreas de Competencia

Propósito

Proporciona información básica sobre las Áreas de Competencia del Marco NICE y por qué se introdujeron en NICE; describe cómo se definen y redactan las Áreas de Competencia y comparte con los lectores las formas en que pueden utilizarse las Áreas de Competencia del NICE.

Ámbito de aplicación

Las Áreas de Competencia descritas forman parte del Marco de la Fuerza Laboral para la Ciberseguridad (NICE), que proporciona un léxico para describir el trabajo y roles de ciberseguridad.

El Marco NICE considera que la "fuerza de trabajo de ciberseguridad" incluye no sólo a aquellos cuyo objetivo principal es la ciberseguridad, sino también a aquellos que necesitan conocimientos y habilidades específicos relacionados con la ciberseguridad para gestionar adecuadamente los riesgos relacionados con la ciberseguridad para la empresa.

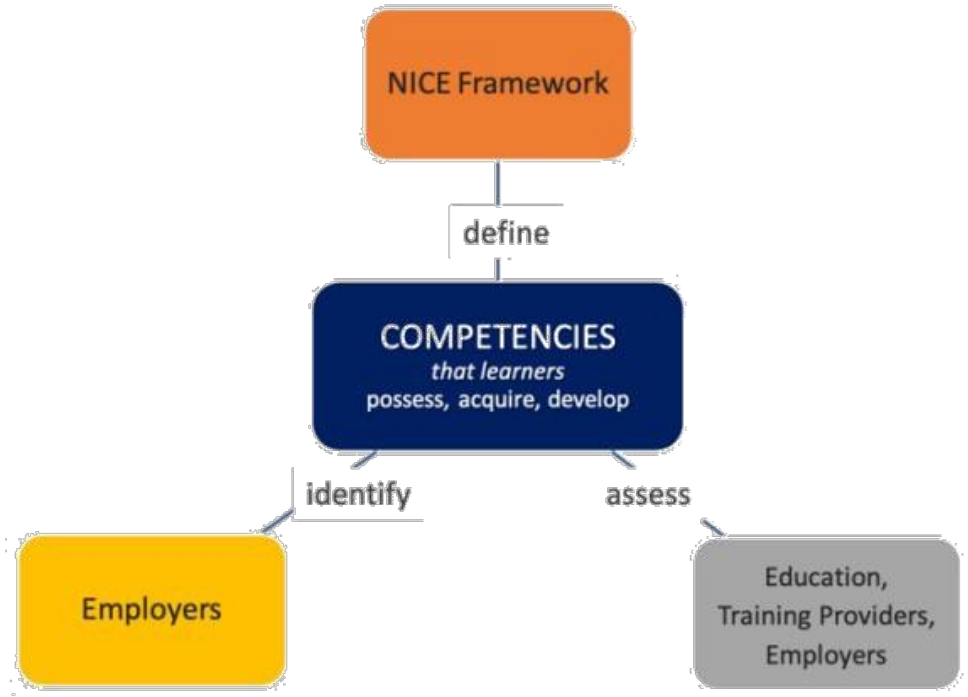


Figure 1: NICE Competencies Stakeholders

NICE Áreas de Competencia

Las áreas de competencia y el Marco NICE

La introducción de las Áreas de Competencia en el Marco NICE responde a la creciente necesidad de identificar y asegurar mejor el talento mediante la contratación basada en habilidades y competencias.

La contratación basada únicamente en los títulos aumenta la probabilidad de excluir a candidatos cualificados, sobre todo para puestos relacionados con las tecnologías emergentes.

Un cambio hacia la contratación y promoción basadas en las competencias garantiza que las personas más capaces de desempeñar las funciones y responsabilidades requeridas para un puesto específico sean las seleccionadas para dicho puesto.

Con la inclusión de las Áreas de Competencia, el Marco NICE proporciona un medio para ayudar a los usuarios del Marco NICE a cambiar a prácticas de contratación basadas en competencias.

NICE Áreas de Competencia

Las Áreas de Competencia utilizan un enfoque impulsado por el empleador para agrupar declaraciones relacionadas de Conocimientos y Habilidades que se correlacionan con la capacidad de una persona para realizar Tareas en un dominio particular.

Con el tiempo, NICE puede trabajar con la comunidad de ciberseguridad para introducir nuevas Áreas de Competencia o actualizar o retirar las Áreas de Competencia existentes en respuesta a la evolución de las necesidades.

Las Áreas de Competencia del Marco NICE son complementarias a los Roles de Trabajo y proporcionan un medio para evaluar las capacidades del alumno en las áreas definidas.

(Véase la Sección 2.3, Áreas de Competencia y Roles de Trabajo, para más información sobre cómo las Áreas de Competencia difieren y funcionan conjuntamente con los Roles de Trabajo).

2.3. Competency Areas and Work Roles

NICE Framework Competency Areas and Work Roles are complementary and may be used together or separately. However, there are differences. While Work Roles focus on the work to be done (Task statements), Competency Areas focus on what a learner must know or be able to do (Knowledge and Skill statements) to complete that work (see Fig. 2. TKS Statements, Competency Areas, and Work Roles).

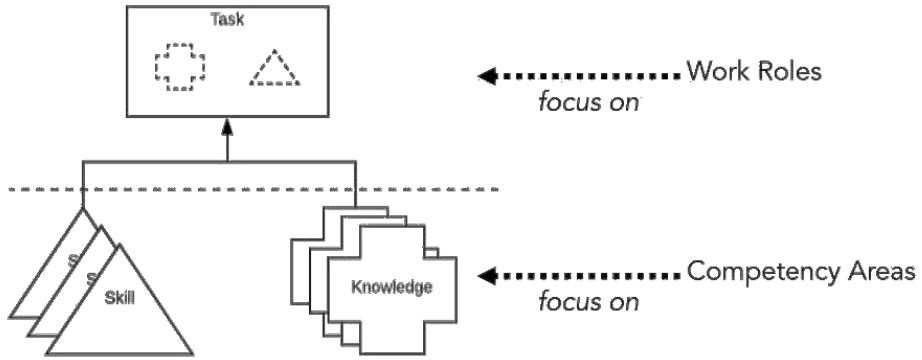


Fig. 2. TKS Statements, Competency Areas, and Work Roles

NICE Áreas de Competencia

Definición de las áreas de competencia

Las áreas de competencia ofrecen una perspectiva de alto nivel de áreas definidas de trabajo de ciberseguridad y apoyan un enfoque inclusivo basado en la evaluación para determinar las capacidades.

Un enfoque basado en la evaluación permite ampliar los grupos de solicitantes e identificar a los candidatos con mayor éxito, especialmente en áreas como las tecnologías emergentes y en rápida evolución.

También pueden utilizarse para identificar trayectorias profesionales, determinar las demandas actuales y futuras de mano de obra, y a la hora de desarrollar la educación, la formación u otras experiencias de aprendizaje para satisfacer necesidades definidas.

Competency Area: A cluster of related Knowledge and Skill statements that correlates with one's capability to perform Tasks in a particular domain. Competency Areas can help learners discover areas of interest, inform career planning and development, identify gaps for knowledge and skills development, and provide a means of assessing or demonstrating a learner's capabilities in the domain.

Competency Areas consist of a name, description of the area, and group of associated TKS statements.

Área de competencia: Conjunto de enunciados de Conocimientos y Habilidades relacionados que se correlacionan con la capacidad de una persona para realizar Tareas en un dominio concreto. Las Áreas de Competencia pueden ayudar a los alumnos a descubrir áreas de interés, informar sobre la planificación y el desarrollo de la carrera, identificar lagunas en el desarrollo de conocimientos y habilidades, y proporcionar un medio para evaluar o demostrar las capacidades de un alumno

Las áreas de competencia constan de un nombre, una descripción del área y un grupo de enunciados TKS asociados.

NICE Áreas de Competencia

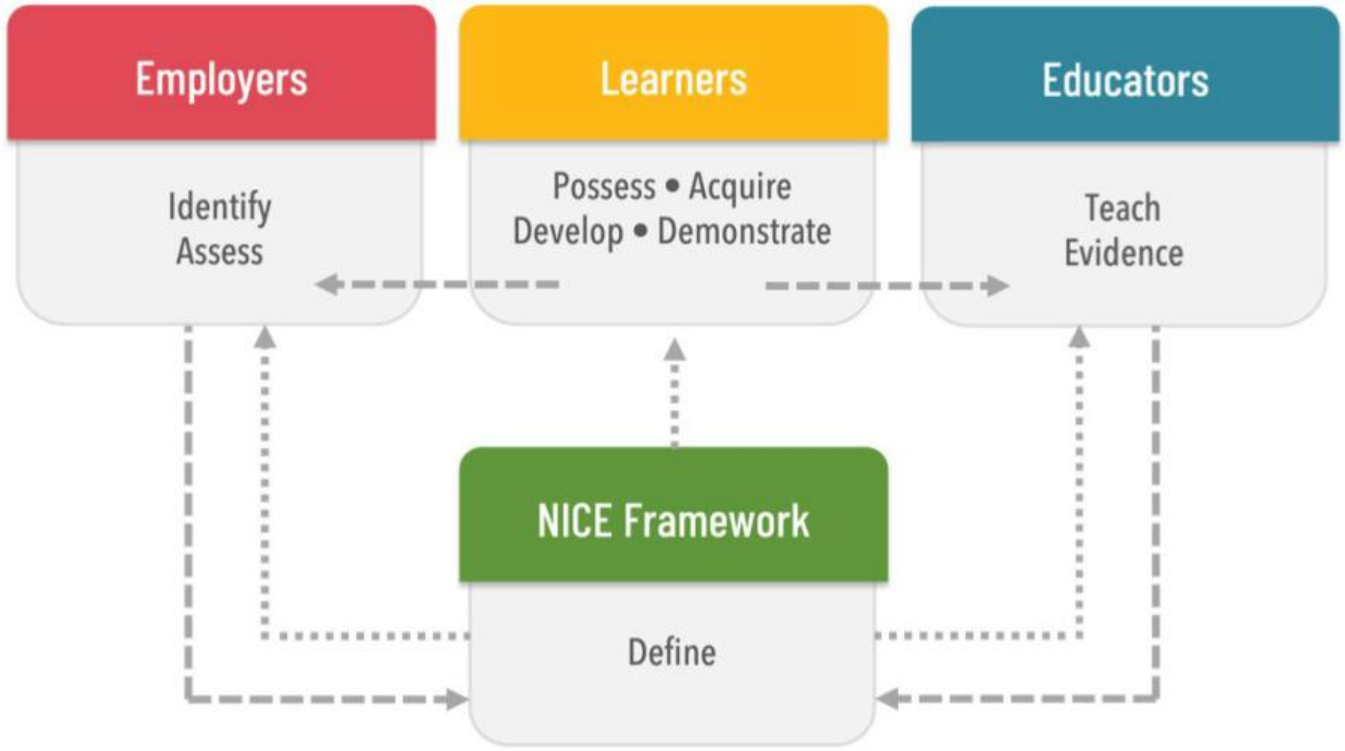


Fig. 1. NICE Framework Competency Area Stakeholders

En consecuencia, en lugar de especificar únicamente el trabajo que debe realizarse (Tareas) o lo que se necesita para realizar el trabajo (Conocimientos y Habilidades), se trata de determinar la capacidad general de un alumno para esa área de trabajo de ciberseguridad.

Las Áreas de Competencia ofrecen una oportunidad para aumentar la alineación y la coordinación entre empleadores, alumnos y proveedores de educación, formación y certificación

(véase la Fig. 1. Partes interesadas del Área de Competencia del Marco NICE).

NICE Áreas de Competencia

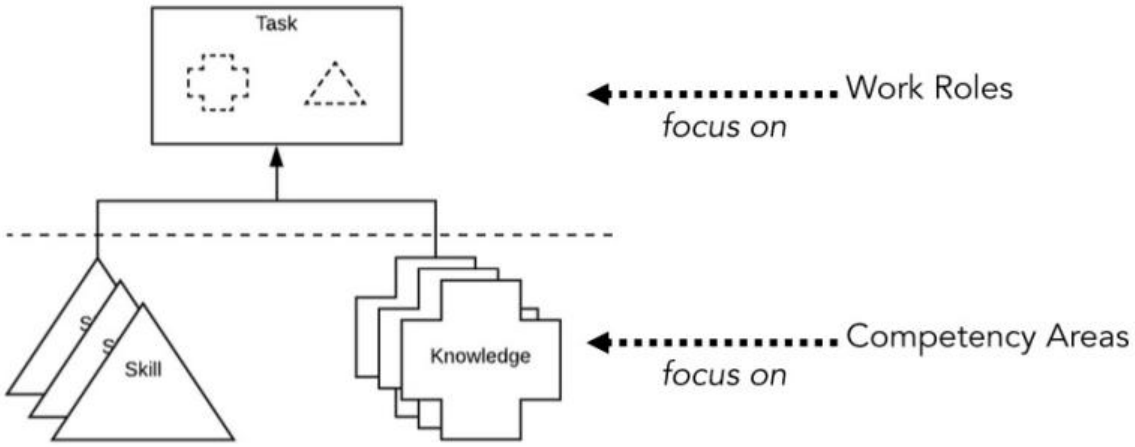


Fig. 2. TKS Statements, Competency Areas, and Work Roles

Áreas de competencia y funciones

Las áreas de competencia y las funciones del Marco NICE son complementarias y pueden utilizarse juntas o por separado.

Sin embargo, existen diferencias. Mientras que las funciones de trabajo se centran en el trabajo que hay que realizar (enunciados de tareas), las áreas de competencia se centran en lo que el alumno debe saber o ser capaz de hacer (enunciados de conocimientos y habilidades) para completar ese trabajo.

(véase la Fig. 2. Enunciados TKS, áreas de competencia y funciones de trabajo).

NICE Áreas de Competencia

Las Áreas de Competencia ayudan a cubrir las necesidades de capacidades de los empleadores de forma más amplia, mientras que las Funciones Laborales se utilizan para definir puestos y responsabilidades específicos.

Por último, la evaluación suele basarse en el área de competencia en su conjunto, mientras que la evaluación de las funciones laborales suele realizarse a nivel de tarea.

Las funciones laborales representan un área de trabajo definida y comúnmente aceptada en muchos tipos de organizaciones y sectores.

Las Áreas de Competencia, sin embargo, pueden representar áreas emergentes que aún no están ampliamente incorporadas en los Roles de Trabajo definidos, capacidades que se derivan de múltiples Roles de Trabajo y áreas fundamentales de experiencia en ciberseguridad.

Table 1. NICE Framework Competency Areas vs. Work Roles

Competency Areas	Work Roles
Learner focused	Work focused
Help address employer needs	Help define positions and responsibilities
Assessment is typically based on a Competency Area as a whole	Assessment typically occurs at the Task level

Tabla 1. Áreas de competencia del Marco NICE frente a funciones laborales

Áreas de Competencia	Roles de Trabajo
Centrado en el alumno	Centrado en el trabajo
Ayudar a satisfacer las necesidades de los empleadores	Ayuda a definir cargos y responsabilidades
La evaluación suele basarse en un área de competencia en su conjunto	La evaluación suele realizarse a nivel de tarea

NICE Áreas de Competencia

Desarrollo del Área de Competencia

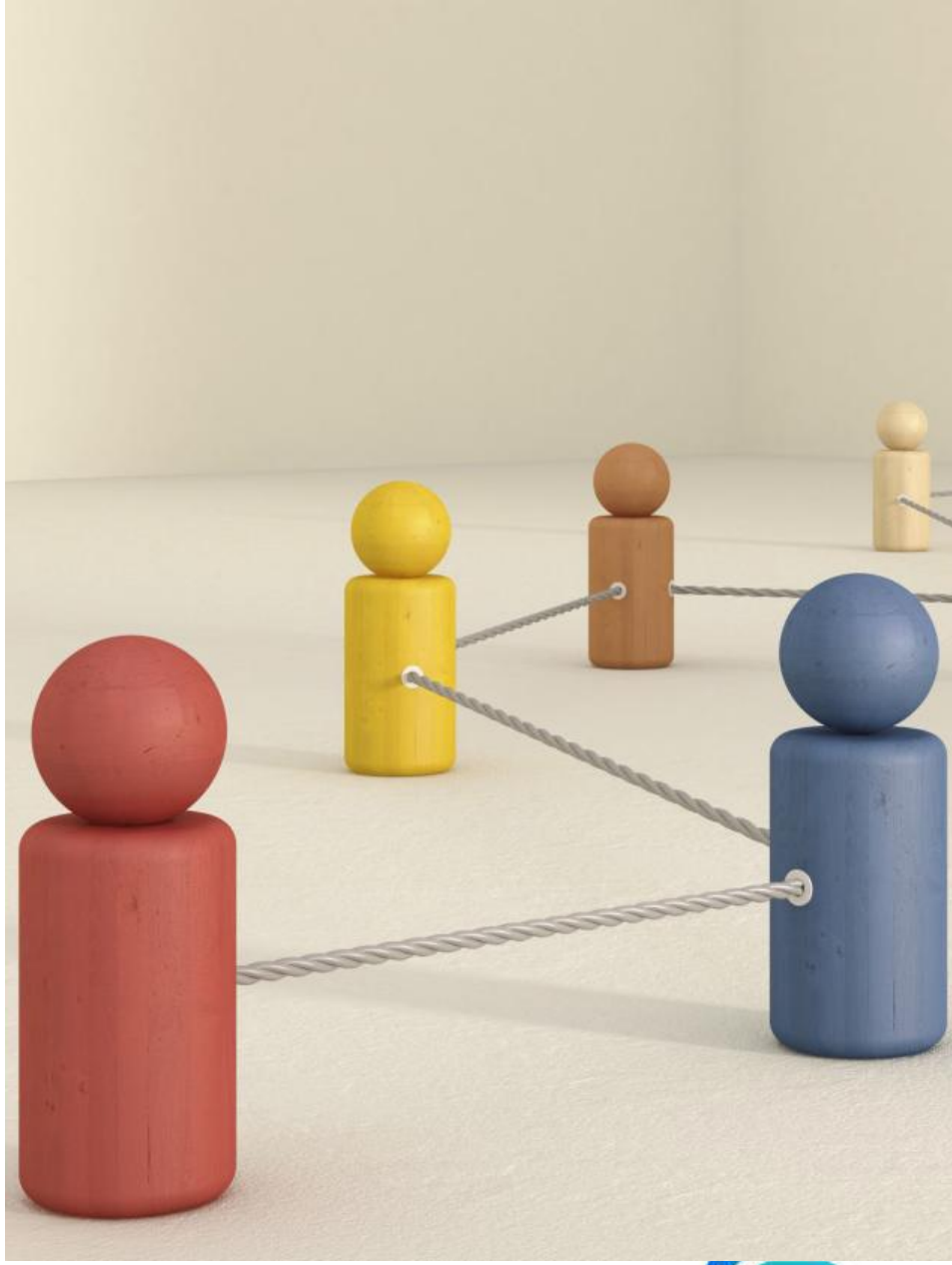
Las siguientes directrices se utilizan para el desarrollo de Áreas de Competencia individuales como parte del Marco NICE.

Áreas de competencia:

- Pueden utilizarse independientemente de las Funciones Laborales.
- Pueden añadirse o superponerse a una o más Funciones Laborales.
- Pueden abarcar varias funciones laborales (es decir, incorporar declaraciones de conocimientos y habilidades de varias funciones laborales).
- Pueden representar ámbitos emergentes que aún no tienen funciones de trabajo establecidas.

Además, las áreas de competencia:

- No duplican funciones de trabajo existentes



NICE Áreas de Competencia

Las Áreas de Competencia están formadas por los siguientes componentes:

1. Título del área de competencia: El nombre del Área de Competencia; el título señala claramente a todas las partes interesadas el área que se va a describir.

2. Descripción del área de competencia: La descripción debe:

a. **Comenzar con "Esta área de competencia describe las capacidades del alumno relacionadas con....".** Utilizar el mismo lenguaje estándar para introducir cada descripción sirve como indicador para los lectores de que se trata de una descripción de Área de Competencia, al tiempo que centra la competencia en el alumno al principio.

b. **Defina el Área de Competencia de forma sencilla y clara.** Las Áreas de Competencia deben definirse utilizando un lenguaje sencillo. Cualquier persona que lea la descripción debe ser capaz de comprender rápida y fácilmente el alcance y el significado del Área de Competencia.

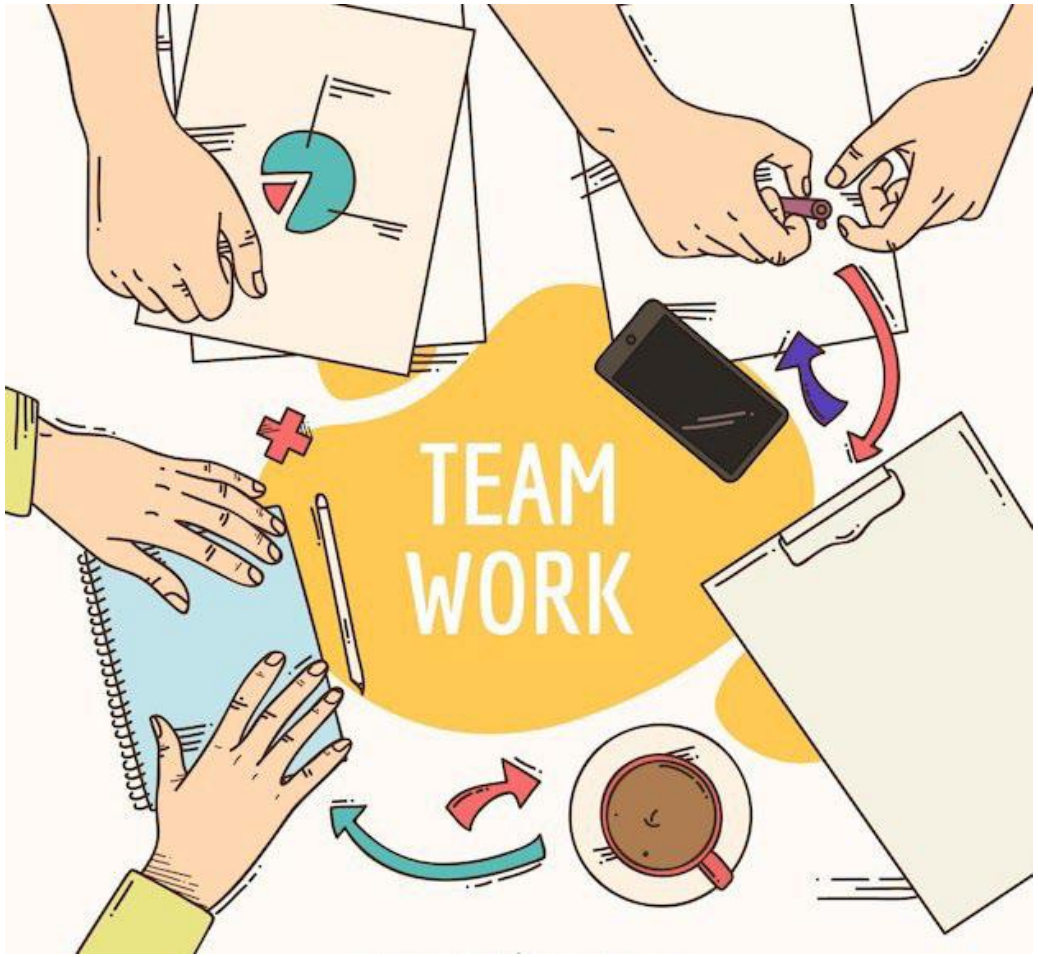
c. **Reflejar el contenido de las declaraciones TKS.** La descripción puede reflejar el lenguaje de los enunciados de Tareas, Habilidades o Conocimientos asociados al Área de Competencia, aunque no debe duplicar totalmente ese lenguaje.

NICE Áreas de Competencia

d. **Equilibrar la especificidad con una amplia aplicación.** Uno de los objetivos de un área de competencia del Marco NICE es proporcionar flexibilidad de aplicación; la descripción debe ser lo suficientemente detallada como para definir claramente su alcance y significado, pero no tan limitada como para restringir su uso por parte de múltiples interesados o poner fecha de caducidad a la competencia (por ejemplo, haciendo referencia a un programa informático o lenguaje de codificación concreto).

e. **Omita los calificativos innecesarios.** Los calificativos (por ejemplo, "conocimiento profundo", "habilidad considerable" o "comprensión básica") y otros indicadores de nivel de competencia no deben incluirse en la descripción de la competencia. Al omitirlos, las áreas de competencia pueden utilizarse para múltiples niveles de competencia.

NICE Áreas de Competencia



3. Declaraciones TKS asociadas: Cada área de competencia estará asociada a un grupo definido de enunciados de tareas, conocimientos y habilidades del Marco NICE que ofrecen una visión más detallada del área de competencia. Tenga en cuenta que los enunciados individuales pueden estar asociados a más de un área de competencia.

NICE Ejemplos de USO

Ejemplos de Uso

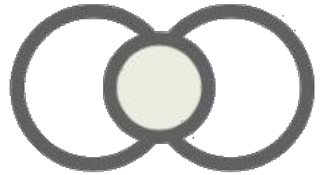
El marco NICE permite una rápida adaptación al cambio, al tiempo que tiene en cuenta los contextos operativos únicos de las organizaciones.

Al mismo tiempo, al establecer un lenguaje y un enfoque comunes, es posible un intercambio coherente de información sobre el personal de ciberseguridad en una organización, entre varias organizaciones y en todo el sector.

Las áreas de competencia amplían los atributos de agilidad, flexibilidad, interoperabilidad y modularidad del marco NICE, lo que se refleja en las múltiples formas en que podrían ser aplicadas por sus diversas partes interesadas. No hay una talla única para todos; pueden utilizarse de diversas maneras, entre ellas:

NICE Ejemplos de USO

Superpuesto al rol o roles de trabajo:
Pueden ser necesarias capacidades adicionales para desempeñar eficazmente una o más Funciones Laborales. Un puesto responsable de más de una función laboral puede necesitar el área de competencia para todas esas funciones.
Ejemplo: Ciberseguridad en la nube.



Puntos en común:
Un Área de Competencia puede definir las capacidades únicas de ciberseguridad que necesitan los profesionales de la ciberseguridad y otro personal de la organización para
mitigar los riesgos. En estos casos, sirve como base común para la comunicación y la coordinación. *Ejemplo: Ciberseguridad de la Tecnología Operativa (OT).*

Aprendizaje:
Para los estudiantes, los solicitantes de empleo o los empleados, las Áreas de Competencia pueden servir como punto de partida para el aprendizaje o como vía para desarrollar una experiencia de mayor nivel en un área.
Ejemplo: Programación segura.

NICE Ejemplos de USO

Perspectiva del empleado

Desde el punto de vista del empleador, las áreas de competencia del Marco NICE pueden utilizarse para apoyar la contratación, el desarrollo y la evaluación de la mano de obra de múltiples maneras, entre ellas:

NICE Ejemplos de USO

Describir un puesto de trabajo determinado:

Las Áreas de Competencia se pueden utilizar para describir ampliamente y realizar un seguimiento de las capacidades de la fuerza de trabajo de ciberseguridad de una organización, o un empleador podría considerar una agrupación de Tareas, Conocimientos y Habilidades y definir un Área de Competencia personalizada para sus necesidades únicas.

Especificar los requisitos del equipo:

A veces, es necesario formar un equipo antes de definir las tareas individuales que realizará el equipo. En estos casos, conocer las Áreas de Competencia más amplias que necesita el equipo para resolver el reto puede ayudar a identificar a los miembros del equipo, que a su vez determinarán el trabajo específico a realizar.

Evaluar las capacidades individuales de los alumnos:

Los alumnos pueden ser evaluados en relación con las áreas de competencia en varias o múltiples etapas, como parte de una entrevista, una evaluación del aprendizaje basado en el trabajo, un proceso de promoción o el desarrollo de la carrera profesional.

NICE Ejemplos de USO

Perspectiva del proveedor de educación, formación o credenciales.

Desde la perspectiva de un proveedor de educación, formación o credenciales, las áreas de competencia del Marco NICE pueden utilizarse de forma similar para apoyar múltiples procesos, entre los que se incluyen:

NICE Ejemplos de USO

Desarrollar programas:

Los proveedores pueden utilizar un conjunto de Áreas de Competencia para desarrollar un programa de aprendizaje -agrupando áreas relacionadas- o para diferenciar niveles de competencia dentro de un Área de Competencia individual.

Desarrollar cursos:

Los instructores pueden seleccionar enunciados específicos de Conocimientos y Habilidades en un Área de Competencia para hacer hincapié en esos enunciados en el proceso de aprendizaje.

Evaluar a los estudiantes:

Los proveedores pueden evaluar si un alumno ha alcanzado un grado definido de capacidad en un área de competencia antes de concederle una credencial.

NICE Ejemplos de USO

Perspectiva del alumno

Por último, desde la perspectiva del alumno, las Áreas de Competencia del Marco NICE pueden utilizarse en varias etapas y de diversas maneras, entre ellas para:

NICE Ejemplos de USO

Evaluar las propias capacidades:

Por ejemplo, para determinar la capacidad global de una persona en un Área de Competencia definida.

Identificar las áreas que pueden necesitar desarrollo:

Esto puede hacerse a través de la evaluación o utilizando el Área de Competencia para autoidentificar las áreas que requieren un mayor aprendizaje.

Aprender sobre un área de especialización definida:

Las Áreas de Competencia pueden ofrecer una vista de pájaro para cualquier persona interesada en la ciberseguridad para ayudarles a entender la experiencia necesaria que puede estar fuera de los Roles de Trabajo definidos, así como para conectar a un alumno con los detalles a través de las declaraciones TKS asociadas.

Navegar y elegir trayectorias profesionales:

Comprender las capacidades propias en las Áreas de Competencia definidas puede ayudar a los alumnos a identificar y progresar hacia Funciones Laborales y puestos de trabajo relacionados.

Comprender las necesidades de mano de obra de una organización: Para los alumnos que buscan un nuevo empleo, los que ya tienen un empleo, pero desean cambiar, o los que están planificando su carrera profesional, las áreas de competencia pueden dar una idea de las necesidades específicas de personal de ciberseguridad de una organización.

NICE Áreas de Competencia

Lista de Áreas de Competencia del Marco NICE

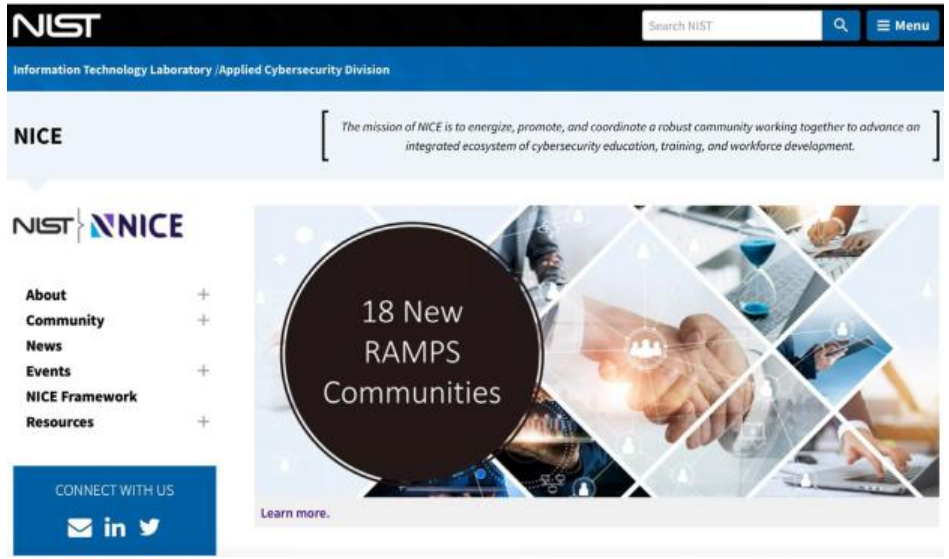
Los recursos del Marco NICE, incluida la última lista de Áreas de Competencia, están disponibles en el Centro de Recursos del Marco NICE.

El NIST mantiene la lista de Áreas de Competencia separada de este documento y de la publicación del Marco NICE para permitir su revisión y actualización periódicas.

El Centro de Recursos del Marco NICE también incluye información sobre cómo participar y mantenerse informado sobre las actualizaciones y el desarrollo del Marco NICE y los recursos de apoyo.

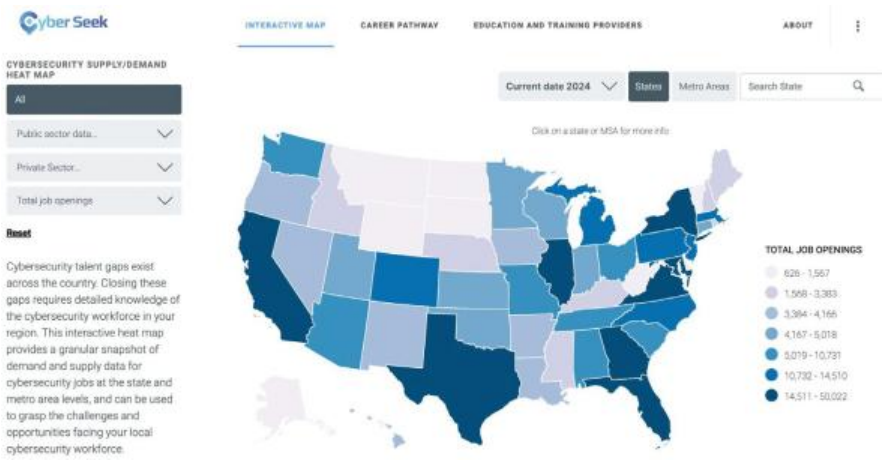
NICE Áreas de Competencia

NICE Framework Resource Center.



https://www.nist.gov/itl/applied-cybersecurity/nice

NICE Framework Resource Center.



https://www.cyberseek.org/heatmap.html

Existen brechas de talento en ciberseguridad en todo el país. Cerrar estas brechas requiere un conocimiento detallado de la mano de obra en ciberseguridad de su región. Este mapa interactivo ofrece una instantánea granular de los datos de oferta y demanda de empleos en ciberseguridad a nivel estatal y de área metropolitana, y puede utilizarse para comprender los retos y oportunidades a los que se enfrenta la mano de obra local en ciberseguridad.

NICE Framework – Casos de Estudio

LCSPC™ Versión 062024

NICE Casos de Estudio

Caso de estudio, Espionaje!

Aproximadamente entre abril de 2016 y noviembre de 2017, un antiguo empleado de la Agencia Central de Inteligencia (CIA), Joshua Adam Shulte, filtró a WikiLeaks información clasificada sobre herramientas de ciberguerra y vigilancia electrónica desarrolladas por la CIA. Los documentos clasificados etiquetados como "Bóveda 7" y "Bóveda 8" fueron considerados como una de las mayores filtraciones de datos orquestadas en la historia de la CIA. También se atribuyó como la mayor divulgación no autorizada de cuentas de información clasificada en la historia de Estados Unidos.

De 2012 a 2016, Shulte trabajó como ingeniero informático desarrollador de software en el Center for Cyber Inntelligence (CCI) de la CIA. Schulte ayudó a crear las herramientas de hackeo como codificador en la Rama de Apoyo a las Operaciones en la sede de la agencia en Langley, Virginia, y tenía privilegios de administrador en uno de los servidores que contenían los programas utilizados para construir herramientas cibernéticas. Se detectó que Schulte abusaba de los privilegios de administrador.

CASE STUDY

Espionage

Joshua Adam Schulte

- U.S. Citizen
- Former CIA employee, Computer Engineer and Software Developer
- Age 35 at time of conviction

CDSE
Center for Development of Security Excellence

WHAT HAPPENED

From approximately April of 2016 to November of 2017, a former Central Intelligence Agency (CIA) employee, Joshua Adam Shulte, leaked classified information to WikiLeaks that entailed cyber warfare and electronic surveillance tools developed by the CIA. The classified documents labeled "Vault 7" and "Vault 8" were considered one of the largest orchestrated data breaches in the history of the CIA. It was also attributed as the largest unauthorized disclosure of classified information accounts in U.S. history.

From 2012 to 2016, Shulte was employed as a computer engineer software developer at the CIA's Center for Cyber Inntelligence (CCI). Schulte helped create the hacking tools as a coder at the Operations Support Branch at the agency's headquarters in Langley, Virginia and had administrator privileges to one of the servers that contained the programs used to build cyber tools. It was detected that Schulte abused administrator privileges. As a result, leadership removed his privileges and transferred Schulte to another division. Schulte was also previously given a warning about granting privileges to himself that were previously revoked. Before his privileges were removed, Schulte secretly transmitted stolen CIA files to his custom desktop computer at his residence. Schulte then transferred those files to WikiLeaks and deleted any internal hard drives to cover his tracks. During the FBI's investigation, child pornography, disturbing images from the dark web, and Russian websites were found on Schulte's computer in encrypted files.

Schulte was arrested on August 24, 2017, and in September of 2023, he was found guilty of espionage, computer hacking, contempt of court, making false statements to the FBI and child pornography. On February 1, 2024, Schulte was sentenced to serve 40 years in prison.

INDICATORS

Access Attributes: Schulte used placement and access, while having adminstrator privileges to CIA files, to transmit classified information that revealed cyber warfare and electronic surveillance tools developed by the CIA.

Technical Activity (Security Violations): Schulte abused administrator privileges when he knowingly and willingly transmitted classified information that could be used to cause injury to the United States. This was after receiving a warning regarding self-granting privileges that were previously revoked.

Criminal Conduct:
The FBI investigation used digital forensics to discover that Schulte downloaded child pornography from the dark web and visited Russian websites.

https://www.cdse.edu/Portals/124/Documents/casestudies/case-study-schulte.pdf

NICE Casos de Estudio

Caso de estudio, Sabotaje!

Deepanshu Kher fue empleado por una empresa de consultoría de tecnología de la información desde 2017 hasta mayo de 2018. En 2017, la empresa de consultoría fue contratada por la empresa Carlsbad para ayudar con su migración a un entorno de Microsoft Office 365 (MSO365). En respuesta, la empresa de consultoría envió a su empleado, Kher, a la sede de la empresa en Carlsbad para ayudar con la migración.

La empresa no estaba satisfecha con el trabajo de Kher y transmitió su descontento a la consultora poco después de la llegada de Kher. En enero de 2018, la consultora retiró a Kher de la sede de la empresa. Unos meses más tarde, el 4 de mayo de 2018, la empresa despidió a Kher, y un mes después, en junio de 2018, Kher regresó a Delhi (India).

Deepanshu Kher

- Indian National
- Age 32 at the time of the attack
- Launched Cyber-attack from his home in Delhi, India

CDSE
Center for Development

CASE STUDY

Cyber Intrusion/Sabotage

WHAT HAPPENED

Deepanshu Kher was employed by an information technology consulting firm from 2017 through May 2018. In 2017, the consulting firm was hired by the Carlsbad Company to assist with its migration to a Microsoft Office 365 (MSO365) environment. In response, the consulting firm sent its employee, Kher, to the company's Carlsbad headquarters to assist with the migration.

The company was dissatisfied with Kher's work and relayed their dissatisfaction to the consulting firm soon after Kher's arrival. In January 2018, the consulting firm pulled Kher from the company's headquarters. A few months later, on May 4, 2018, the firm fired Kher, and a month after that, in June 2018, Kher returned to Delhi, India.

On August 8, 2018, two months after his return to India, Kher hacked into the Carlsbad Company's server and deleted over 1,200 of its 1,500 MSO365 user accounts. The attack affected the bulk of the company's employees and completely shut down the company for two days.

Unfortunately, even after those two days, the problems remained. Employees were not receiving meeting invites or cancellations, employees' contacts lists could not be completely rebuilt, and affected employees could no longer access folders to which they previously had access. The Carlsbad Company repeatedly handled multitudes of IT problems for three months.

Kher was arrested when he flew from India to the United States on January 11, 2021, unaware of the outstanding warrant for his arrest.

Deepanshu Kher pled guilty to Intentional Damage to a Protected Computer and was sentenced to two years in prison.

INDICATORS

- Access Attributes – Kher had privileged access to the Carlsbad Company servers
- Professional Lifecycle and Performance – Kher was removed from the MSO365 project due to unsatisfactory performance and was later fired
- Foreign Considerations – Kher was an Indian national and therefore

https://www.cdse.edu/Portals/124/Documents/casestudies/case-study-deepanshu-kasaba-kher.pdf

NICE Casos de Estudio

Caso de estudio, Sabotaje!

El 8 de agosto de 2018, dos meses después de su regreso a la India, Kher hackeó el servidor de la empresa de Carlsbad y eliminó más de 1.200 de sus 1.500 cuentas de usuario de MSO365. El ataque afectó al grueso de los empleados de la empresa y la paralizó por completo durante dos días.

Por desgracia, incluso después de esos dos días, los problemas persistían. Los empleados no recibían invitaciones a reuniones ni cancelaciones, las listas de contactos de los empleados no se podían reconstruir completamente y los empleados afectados ya no podían acceder a carpetas a las que antes tenían acceso. La empresa de Carlsbad gestionó repetidamente multitud de problemas informáticos durante tres meses.

Deepanshu Kher

- Indian National
- Age 32 at the time of the attack
- Launched Cyber-attack from his home in Delhi, India

CDSE
Center for Development

CASE STUDY

Cyber Intrusion/Sabotage

WHAT HAPPENED

Deepanshu Kher was employed by an information technology consulting firm from 2017 through May 2018. In 2017, the consulting firm was hired by the Carlsbad Company to assist with its migration to a Microsoft Office 365 (MSO365) environment. In response, the consulting firm sent its employee, Kher, to the company's Carlsbad headquarters to assist with the migration.

The company was dissatisfied with Kher's work and relayed their dissatisfaction to the consulting firm soon after Kher's arrival. In January 2018, the consulting firm pulled Kher from the company's headquarters. A few months later, on May 4, 2018, the firm fired Kher, and a month after that, in June 2018, Kher returned to Delhi, India.

On August 8, 2018, two months after his return to India, Kher hacked into the Carlsbad Company's server and deleted over 1,200 of its 1,500 MSO365 user accounts. The attack affected the bulk of the company's employees and completely shut down the company for two days.

Unfortunately, even after those two days, the problems remained. Employees were not receiving meeting invites or cancellations, employees' contacts lists could not be completely rebuilt, and affected employees could no longer access folders to which they previously had access. The Carlsbad Company repeatedly handled multitudes of IT problems for three months.

Kher was arrested when he flew from India to the United States on January 11, 2021, unaware of the outstanding warrant for his arrest.

Deepanshu Kher pled guilty to Intentional Damage to a Protected Computer and was sentenced to two years in prison.

INDICATORS

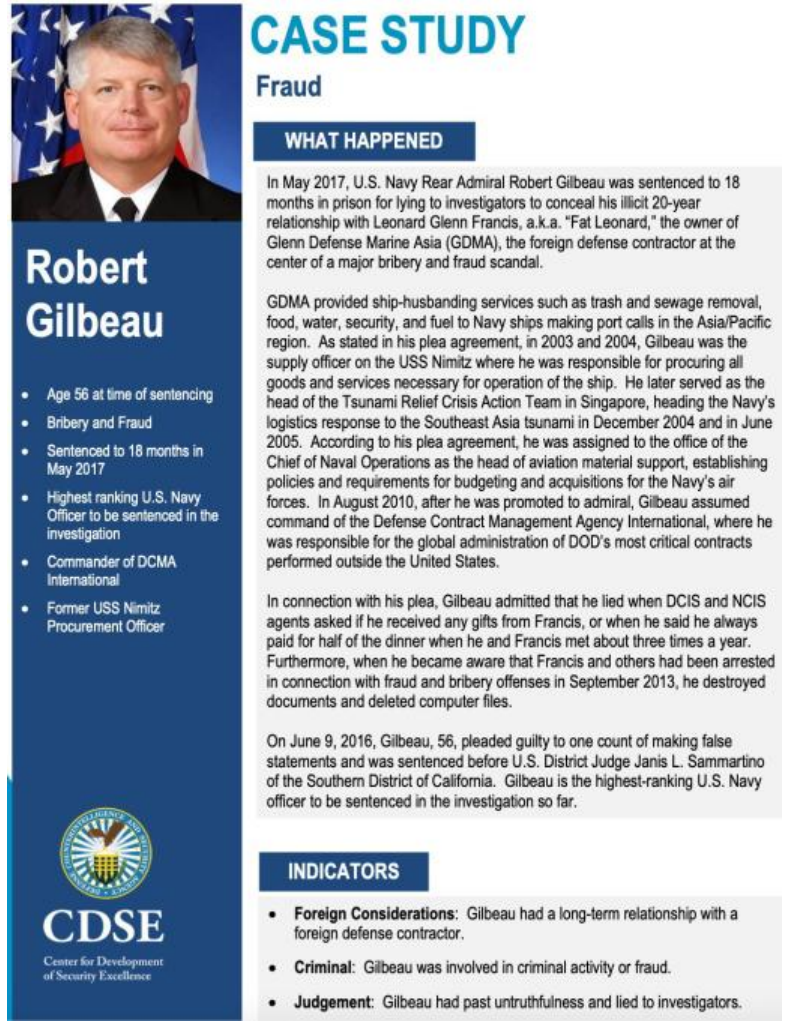
- Access Attributes – Kher had privileged access to the Carlsbad Company servers
- Professional Lifecycle and Performance – Kher was removed from the MSO365 project due to unsatisfactory performance and was later fired
- Foreign Considerations – Kher was an Indian national and therefore

https://www.cdse.edu/Portals/124/Documents/casestudies/case-study-deepanshu-kasaba-kher.pdf

NICE Casos de Estudio

Caso de estudio, Fraude!

En mayo de 2017, el contralmirante de la Marina estadounidense Robert Gilbeau fue condenado a 18 meses de prisión por mentir a los investigadores para ocultar su relación ilícita de 20 años con Leonard Glenn Francis, alias "Fat Leonard", el propietario de Glenn Defense Marine Asia (GDMA), el contratista de defensa extranjero en el centro de un gran escándalo de soborno y fraude.
GDMA prestaba servicios de esponsorización de buques, como recogida de basura y aguas residuales, comida, agua, seguridad y combustible, a buques de la Armada que hacían escala en la región de Asia y el Pacífico. Según consta en su acuerdo de culpabilidad, en 2003 y 2004, Gilbeau fue oficial de suministros en el USS Nimitz, donde era responsable de la adquisición de todos los bienes y servicios necesarios para el funcionamiento del buque. Posteriormente, fue jefe del Equipo de Acción de Crisis para el Socorro en caso de Tsunami en Singapur, dirigiendo la respuesta logística de la Armada al tsunami del sudeste asiático en diciembre de 2004 y en junio de 2005.
Según su acuerdo de culpabilidad, fue destinado a la oficina del Jefe de Operaciones Navales como jefe de apoyo de material de aviación, estableciendo políticas y requisitos para la elaboración de presupuestos y adquisiciones para las fuerzas aéreas de la Armada. En agosto de 2010, tras ser ascendido a almirante, Gilbeau asumió el mando de la Agencia Internacional de Gestión de Contratos de Defensa, donde era responsable de la administración global de los contratos más importantes del Departamento de Defensa realizados fuera de Estados Unidos.



CASE STUDY

Fraud

Robert Gilbeau

- Age 56 at time of sentencing
- Bribery and Fraud
- Sentenced to 18 months in May 2017
- Highest ranking U.S. Navy Officer to be sentenced in the investigation
- Commander of DCMA International
- Former USS Nimitz Procurement Officer

CDSE
Center for Development of Security Excellence

WHAT HAPPENED

In May 2017, U.S. Navy Rear Admiral Robert Gilbeau was sentenced to 18 months in prison for lying to investigators to conceal his illicit 20-year relationship with Leonard Glenn Francis, a.k.a. "Fat Leonard," the owner of Glenn Defense Marine Asia (GDMA), the foreign defense contractor at the center of a major bribery and fraud scandal.

GDMA provided ship-husbanding services such as trash and sewage removal, food, water, security, and fuel to Navy ships making port calls in the Asia/Pacific region. As stated in his plea agreement, in 2003 and 2004, Gilbeau was the supply officer on the USS Nimitz where he was responsible for procuring all goods and services necessary for operation of the ship. He later served as the head of the Tsunami Relief Crisis Action Team in Singapore, heading the Navy's logistics response to the Southeast Asia tsunami in December 2004 and in June 2005. According to his plea agreement, he was assigned to the office of the Chief of Naval Operations as the head of aviation material support, establishing policies and requirements for budgeting and acquisitions for the Navy's air forces. In August 2010, after he was promoted to admiral, Gilbeau assumed command of the Defense Contract Management Agency International, where he was responsible for the global administration of DOD's most critical contracts performed outside the United States.

In connection with his plea, Gilbeau admitted that he lied when DCIS and NCIS agents asked if he received any gifts from Francis, or when he said he always paid for half of the dinner when he and Francis met about three times a year. Furthermore, when he became aware that Francis and others had been arrested in connection with fraud and bribery offenses in September 2013, he destroyed documents and deleted computer files.

On June 9, 2016, Gilbeau, 56, pleaded guilty to one count of making false statements and was sentenced before U.S. District Judge Janis L. Sammartino of the Southern District of California. Gilbeau is the highest-ranking U.S. Navy officer to be sentenced in the investigation so far.

INDICATORS

- **Foreign Considerations**: Gilbeau had a long-term relationship with a foreign defense contractor.
- **Criminal**: Gilbeau was involved in criminal activity or fraud.
- **Judgement**: Gilbeau had past untruthfulness and lied to investigators.

https://www.cdse.edu/Portals/124/Documents/casestudies/robert-gilbeau.pdf

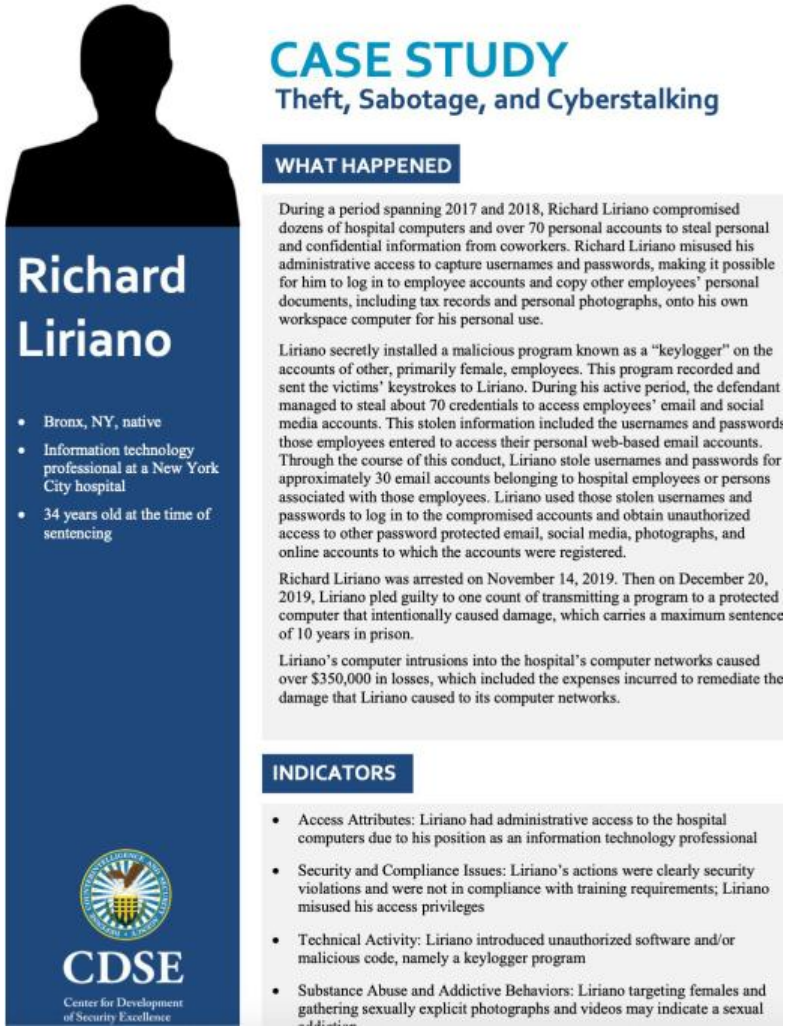
NICE Casos de Estudio

Caso de estudio, Hacking!

Durante un período que abarcó 2017 y 2018, Richard Liriano comprometió docenas de ordenadores del hospital y más de 70 cuentas personales para robar información personal y confidencial de compañeros de trabajo. Richard Liriano hizo un uso indebido de su acceso administrativo para capturar nombres de usuario y contraseñas, lo que le permitió iniciar sesión en cuentas de empleados y copiar documentos personales de otros empleados, incluidos registros fiscales y fotografías personales, en su propio ordenador del espacio de trabajo para su uso personal.

Liriano instaló en secreto un programa malicioso conocido como "keylogger" en las cuentas de otros empleados, principalmente mujeres. Este programa grababa y enviaba a Liriano las pulsaciones de teclado de las víctimas. Durante su periodo activo, el acusado consiguió robar unas 70 credenciales de acceso a las cuentas de correo electrónico y redes sociales de los empleados. Esta información robada incluía los nombres de usuario y las contraseñas que esos empleados introducían para acceder a sus cuentas personales de correo electrónico basadas en la web.

En el transcurso de esta conducta, Liriano robó nombres de usuario y contraseñas para aproximadamente 30 cuentas de correo electrónico pertenecientes a empleados del hospital o a personas asociadas con esos empleados. Liriano utilizó esos nombres de usuario y contraseñas robados para iniciar sesión en las cuentas comprometidas y obtener acceso no autorizado a otros correos electrónicos protegidos por contraseña, redes sociales, fotografías y cuentas en línea a las que estaban registradas las cuentas.



CASE STUDY

Theft, Sabotage, and Cyberstalking

Richard Liriano

- Bronx, NY, native
- Information technology professional at a New York City hospital
- 34 years old at the time of sentencing

CDSE

Center for Development of Security Excellence

WHAT HAPPENED

During a period spanning 2017 and 2018, Richard Liriano compromised dozens of hospital computers and over 70 personal accounts to steal personal and confidential information from coworkers. Richard Liriano misused his administrative access to capture usernames and passwords, making it possible for him to log in to employee accounts and copy other employees' personal documents, including tax records and personal photographs, onto his own workspace computer for his personal use.

Liriano secretly installed a malicious program known as a "keylogger" on the accounts of other, primarily female, employees. This program recorded and sent the victims' keystrokes to Liriano. During his active period, the defendant managed to steal about 70 credentials to access employees' email and social media accounts. This stolen information included the usernames and passwords those employees entered to access their personal web-based email accounts. Through the course of this conduct, Liriano stole usernames and passwords for approximately 30 email accounts belonging to hospital employees or persons associated with those employees. Liriano used those stolen usernames and passwords to log in to the compromised accounts and obtain unauthorized access to other password protected email, social media, photographs, and online accounts to which the accounts were registered.

Richard Liriano was arrested on November 14, 2019. Then on December 20, 2019, Liriano pled guilty to one count of transmitting a program to a protected computer that intentionally caused damage, which carries a maximum sentence of 10 years in prison.

Liriano's computer intrusions into the hospital's computer networks caused over $350,000 in losses, which included the expenses incurred to remediate the damage that Liriano caused to its computer networks.

INDICATORS

- Access Attributes: Liriano had administrative access to the hospital computers due to his position as an information technology professional
- Security and Compliance Issues: Liriano's actions were clearly security violations and were not in compliance with training requirements; Liriano misused his access privileges
- Technical Activity: Liriano introduced unauthorized software and/or malicious code, namely a keylogger program
- Substance Abuse and Addictive Behaviors: Liriano targeting females and gathering sexually explicit photographs and videos may indicate a sexual

https://www.cdse.edu/Portals/124/Documents/casestudies/case-study-liriano.pdf

Cybersecurity Framework NIST v 2.0

LCSPC™ Versión 062024

CSF NIST v 2.0

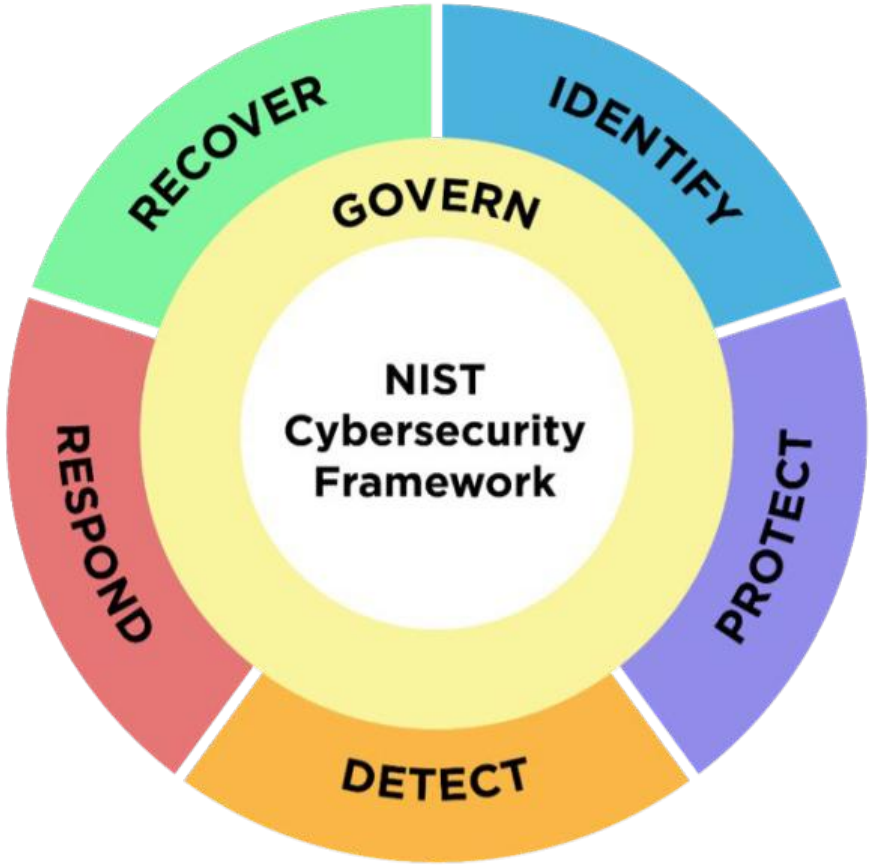
CSF NIST 2.0
Nueva versión

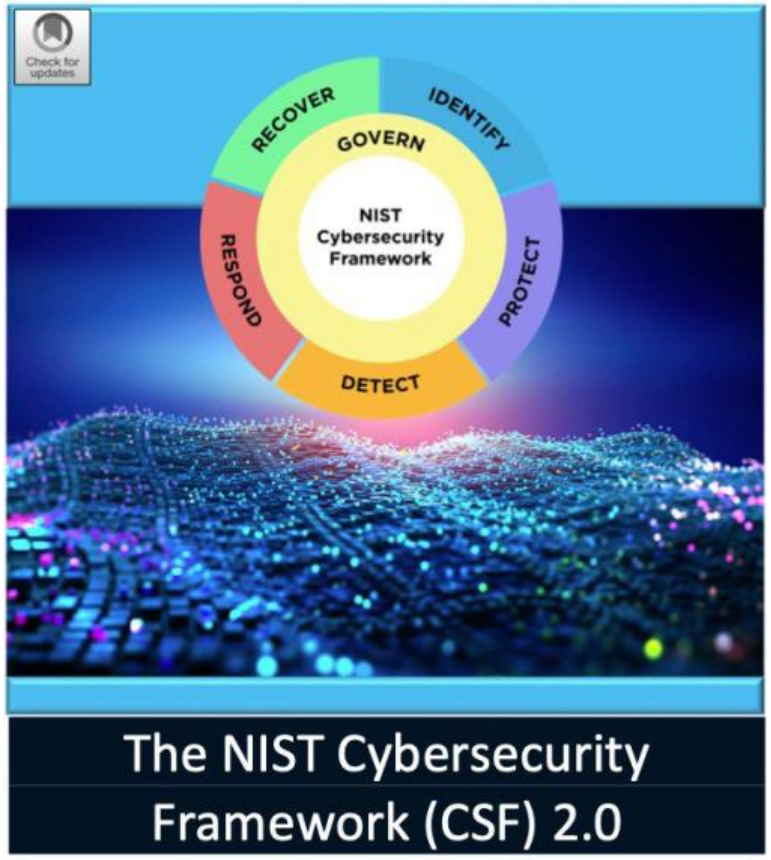
The NIST Cybersecurity Framework (CSF) 2.0

National Institute of Standards and Technology
This publication is available free of charge from: https://doi.org/10.6028/NIST.CSWP.29
February 26, 2024

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

CSF NIST v 2.0





National Institute of Standards and Technology
This publication is available free of charge from: https://doi.org/10.6028/NIST.CSWP.29
February 26, 2024

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

CSF NIST v 2.0

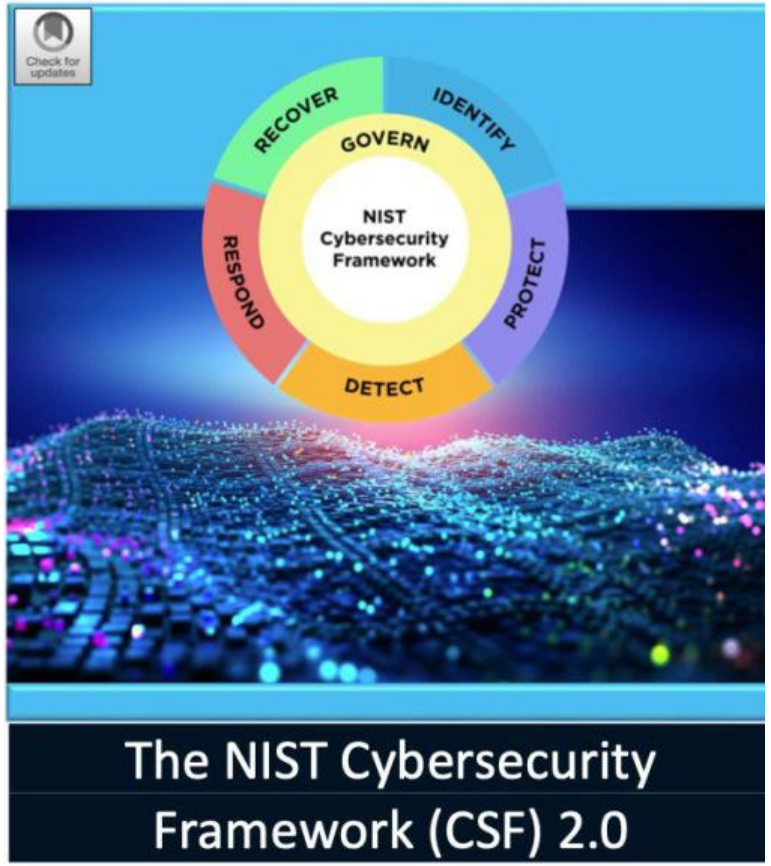
El Marco de Ciberseguridad (CSF) 2.0 del NIST

Proporciona orientación a la industria, las agencias gubernamentales y otras organizaciones para gestionar los riesgos de ciberseguridad.
Ofrece una taxonomía de resultados de ciberseguridad de alto nivel que pueden ser utilizados por cualquier organización - independientemente de su tamaño, sector o madurez - para comprender, evaluar, priorizar y comunicar mejor sus esfuerzos de ciberseguridad.

El CSF no prescribe cómo deben lograrse los resultados.

Más bien, enlaza con recursos en línea que proporcionan orientación adicional sobre prácticas y controles que podrían utilizarse para lograr esos resultados.

Este documento describe el CSF 2.0, sus componentes y algunas de las muchas formas en que puede utilizarse.



National Institute of Standards and Technology
This publication is available free of charge from: https://doi.org/10.6028/NIST.CSWP.29
February 26, 2024
NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

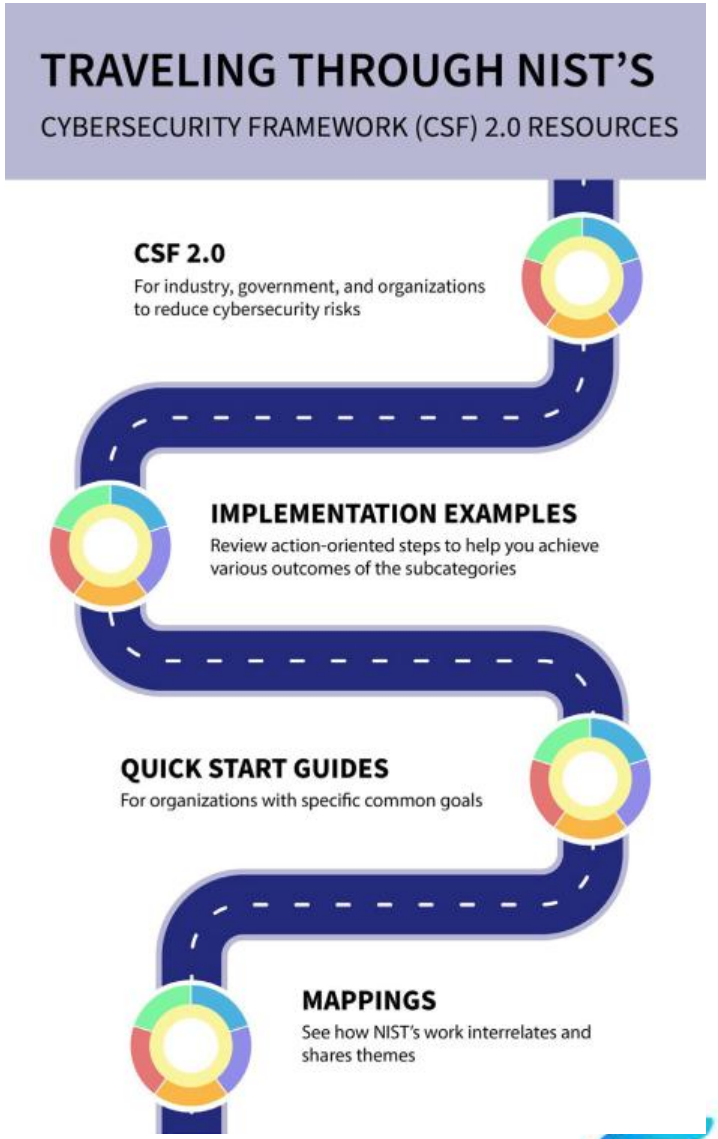
CSF NIST v 2.0

Audiencia

Las personas responsables de desarrollar y dirigir estrategias de ciberseguridad son el público principal del CSF.
El CSF también puede ser utilizado por otras personas involucradas en la gestión de riesgos - incluyendo ejecutivos, consejos de administración, profesionales de adquisiciones, profesionales de la tecnología, gestores de riesgos, abogados, especialistas en recursos humanos y auditores de ciberseguridad y gestión de riesgos - para guiar sus decisiones relacionadas con la ciberseguridad.

Además, el CSF puede ser útil para aquellos que hacen e influyen en la política (por ejemplo, asociaciones, organizaciones profesionales, reguladores) que establecen y comunican las prioridades para la gestión de riesgos de ciberseguridad.

El CSF es el resultado de un esfuerzo de colaboración de varios años entre la industria, el mundo académico y el gobierno de Estados Unidos y de todo el mundo.



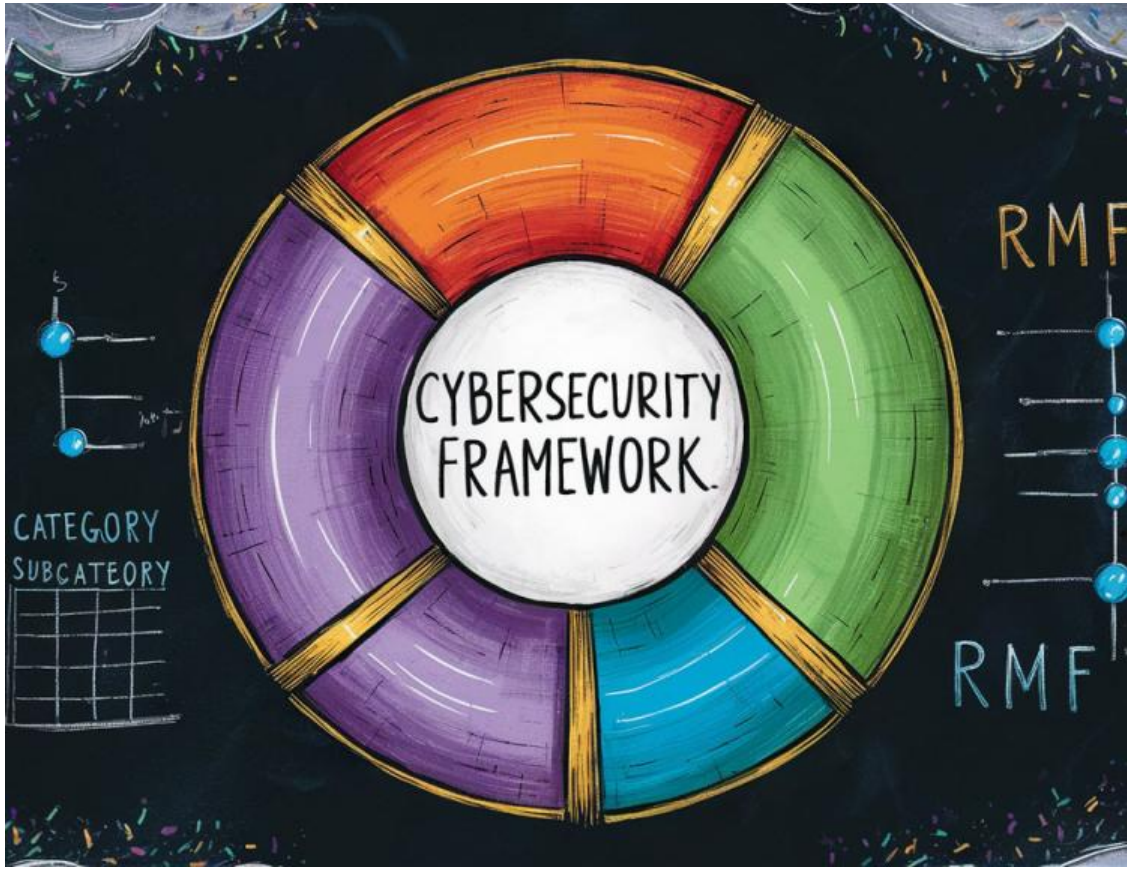
CSF NIST v 2.0

El Marco de Ciberseguridad (CSF) 2.0 está diseñado para ayudar a las organizaciones de todos los tamaños y sectores - incluyendo la industria, el gobierno, el mundo académico y las organizaciones sin ánimo de lucro - a gestionar y reducir sus riesgos de ciberseguridad.
Es útil independientemente del nivel de madurez y sofisticación técnica de los programas de ciberseguridad de una organización.

Sin embargo, el CSF no adopta un enfoque de talla única.

Cada organización tiene riesgos comunes y únicos, así como diferentes apetitos y tolerancias de riesgo, misiones específicas y objetivos para lograr esas misiones. Por necesidad, la forma en que las organizaciones apliquen el MSC variará.

Idealmente, el CSF se utilizará para abordar los riesgos de ciberseguridad junto con otros riesgos de la empresa, incluidos los financieros, de privacidad, de la cadena de suministro, de reputación, tecnológicos o de naturaleza física.



Introducción al CORE de CSF v 2.0

LCSPC™ Versión 062024

NUCLEO CSF v 2.0

Introducción al Núcleo CSF

El Apéndice A es el Núcleo del CSF - un conjunto de resultados de ciberseguridad ordenados por Función, luego Categoría y finalmente Subcategoría, como se muestra en la Fig. 1. Estos resultados no son una lista de acciones a realizar.

Estos resultados no son una lista de acciones a realizar; las acciones específicas tomadas para lograr un resultado variarán según la organización y el caso de uso, al igual que el individuo responsable de esas acciones.

Además, el orden y el tamaño de las funciones, categorías y subcategorías del núcleo no implican la secuencia o la importancia de su consecución.

La estructura del Núcleo está pensada para que tenga mayor resonancia entre los encargados de hacer operativa la gestión de riesgos dentro de una organización.

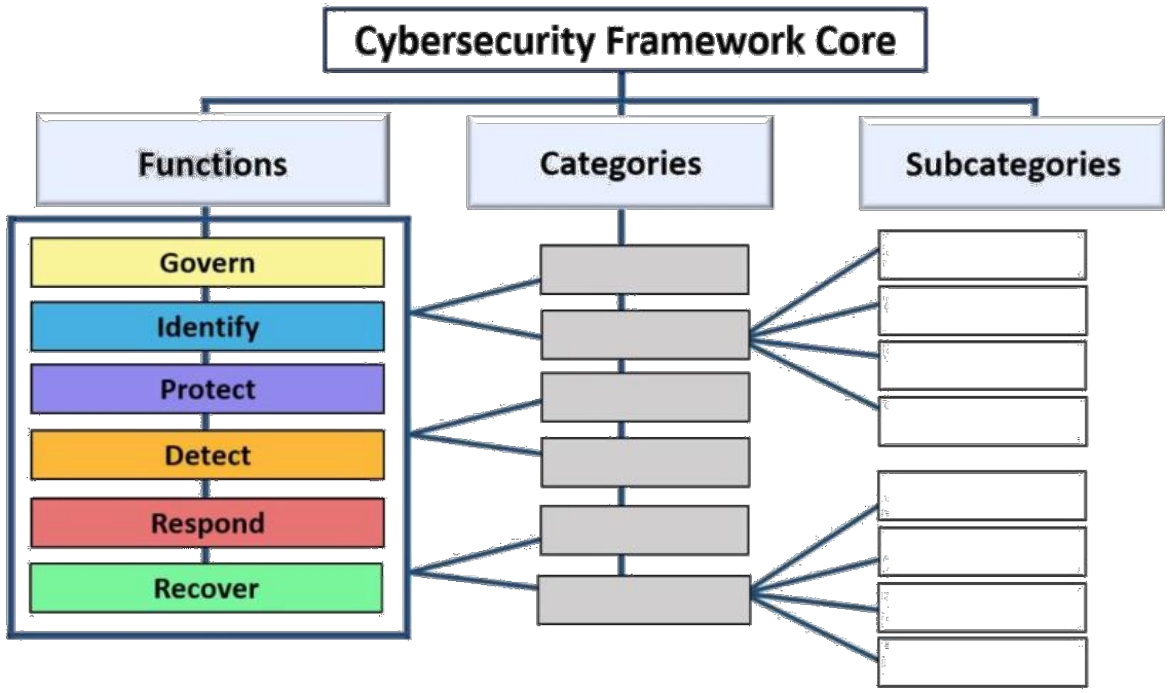


Fig. 1. CSF Core structure

NUCLEO CSF v 2.0

Las Funciones Básicas del CSF **– GOBERNAR, IDENTIFICAR, PROTEGER, DETECTAR, RESPONDER y RECUPERAR –** organizan los resultados de la ciberseguridad en su nivel más alto.

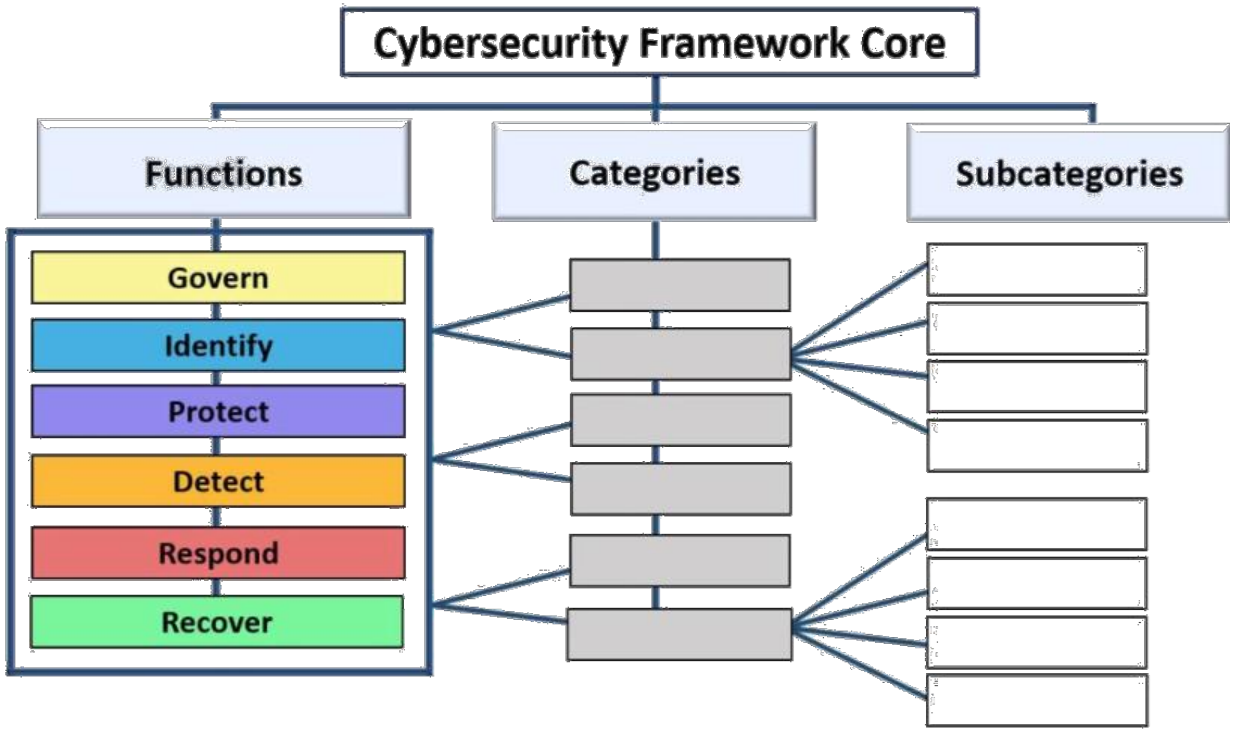


Fig. 1. CSF Core structure

NUCLEO CSF v 2.0

GOBERNAR (GV) - Se establecen, comunican y supervisan la estrategia, las expectativas y la política de gestión de riesgos de ciberseguridad de la organización.

La función **GOBERNAR** proporciona resultados para informar de lo que una organización puede hacer para lograr y priorizar los resultados de las otras cinco funciones en el contexto de su misión y las expectativas de las partes interesadas.

Las actividades de gobernanza son fundamentales para incorporar la ciberseguridad en la estrategia más amplia de gestión de riesgos empresariales (ERM) de una organización.

GOBERNAR aborda la comprensión del contexto organizativo; el establecimiento de la estrategia de ciberseguridad y la gestión del riesgo de la cadena de suministro de ciberseguridad; las funciones, responsabilidades y autoridades; la política; y la supervisión de la estrategia de ciberseguridad.

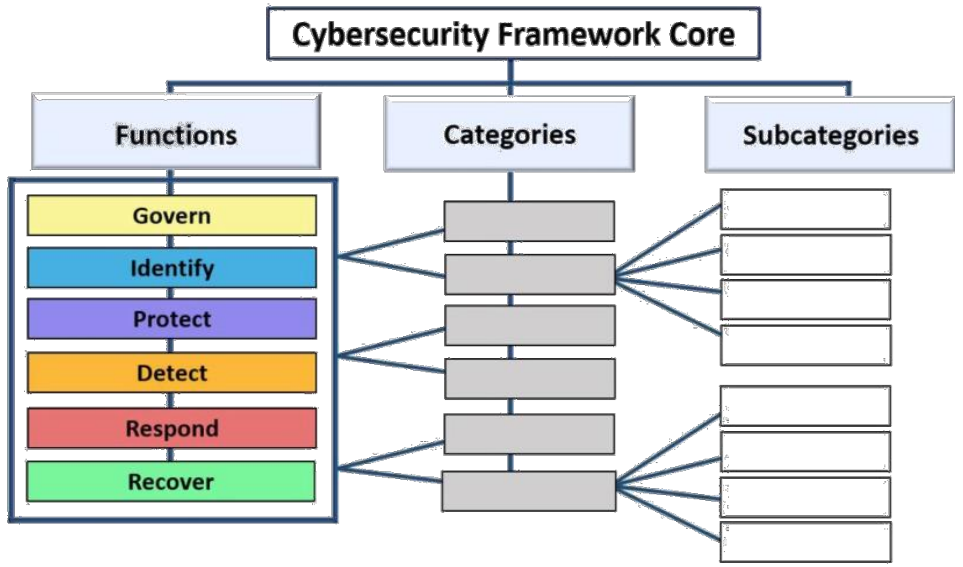


Fig. 1. CSF Core structure

NUCLEO CSF v 2.0

IDENTIFICAR (ID) – Se conocen los riesgos actuales de ciberseguridad de la organización.

La comprensión de los activos de la organización (por ejemplo, datos, hardware, software, sistemas, instalaciones, servicios, personas), proveedores y riesgos de ciberseguridad relacionados permite a una organización priorizar sus esfuerzos en consonancia con su estrategia de gestión de riesgos y las necesidades de la misión identificadas en *GOBERNAR.*

Esta Función también incluye la identificación de oportunidades de mejora para las políticas, planes, procesos, procedimientos y prácticas de la organización que apoyan la gestión de riesgos de ciberseguridad para informar los esfuerzos bajo las seis Funciones.

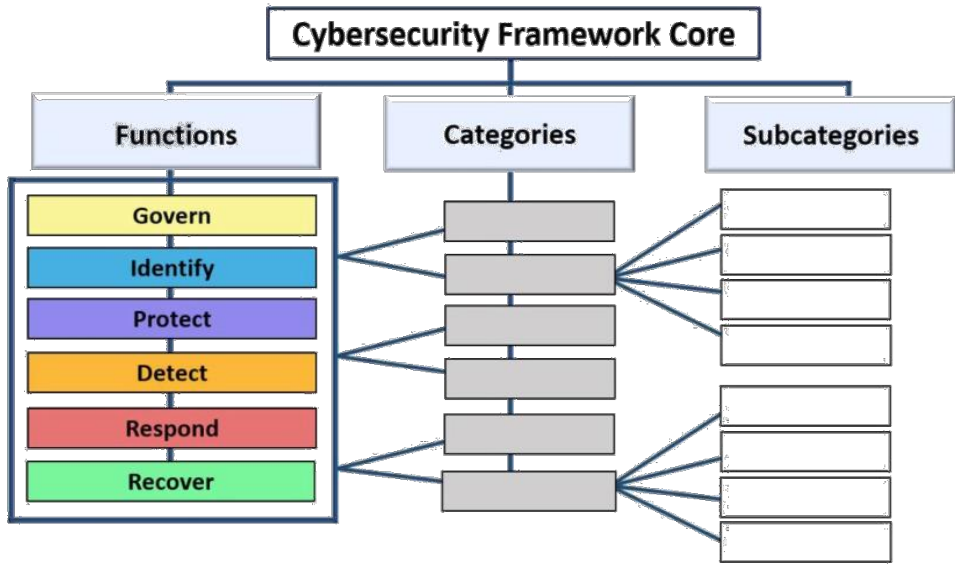


Fig. 1. CSF Core structure

NUCLEO CSF v 2.0

PROTEGER (PR) - Se utilizan salvaguardas para gestionar los riesgos de ciberseguridad de la organización.

Una vez identificados y priorizados los activos y riesgos, PROTEGER apoya la capacidad de asegurar esos activos para prevenir o reducir la probabilidad y el impacto de eventos adversos de ciberseguridad, así como para aumentar la probabilidad y el impacto de aprovechar las oportunidades.

Los resultados cubiertos por esta función incluyen la gestión de identidades, la autenticación y el control de acceso; la concienciación y la formación; la seguridad de los datos; la seguridad de las plataformas (es decir, asegurar el hardware, el software y los servicios de las plataformas físicas y virtuales); y la resistencia de la infraestructura tecnológica.

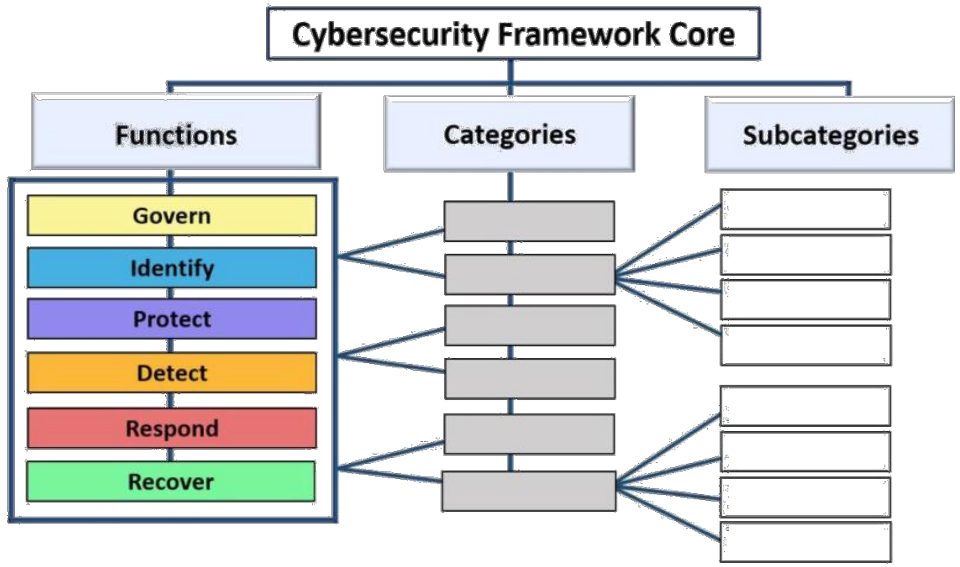


Fig. 1. CSF Core structure

NUCLEO CSF v 2.0

DETECTAR (DE) - Se descubren y analizan posibles ataques e incidentes de ciberseguridad. **DETECTAR** permite el descubrimiento y análisis oportunos de anomalías, indicadores de compromiso y otros eventos potencialmente adversos que pueden indicar que se están produciendo ataques e incidentes de ciberseguridad. Esta función contribuye al éxito de las actividades de respuesta y recuperación en caso de incidente.

RESPONDER (RS) - Se toman medidas en relación con un incidente de ciberseguridad detectado. **RESPONDER** apoya la capacidad de contener los efectos de los incidentes de ciberseguridad. Los resultados de esta función abarcan la gestión, el análisis, la mitigación, la notificación y la comunicación de incidentes.

RECUPERAR (RC) - Se restauran los activos y operaciones afectados por un incidente de ciberseguridad. **RECUPERAR** apoya el restablecimiento oportuno de las operaciones normales para reducir los efectos de los incidentes de ciberseguridad y permitir una comunicación adecuada durante los esfuerzos de recuperación.

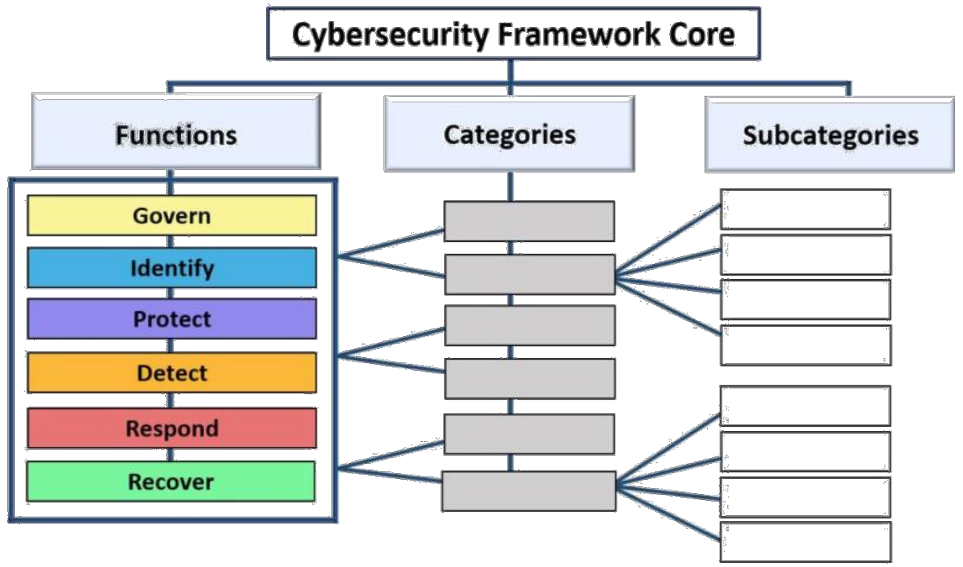


Fig. 1. CSF Core structure

NUCLEO CSF v 2.0

Aunque muchas actividades de gestión de riesgos de ciberseguridad se centran en evitar que se produzcan sucesos negativos, también pueden apoyar el aprovechamiento de oportunidades positivas.

Las acciones para reducir el riesgo de ciberseguridad pueden beneficiar a una organización de otras maneras, como el aumento de los ingresos (por ejemplo, primero ofreciendo el exceso de espacio de las instalaciones a un proveedor de alojamiento comercial para alojar sus propios centros de datos y los de otras organizaciones, y luego trasladando un importante sistema financiero del centro de datos interno de la organización a los proveedores de alojamiento para reducir el riesgo de ciberseguridad).

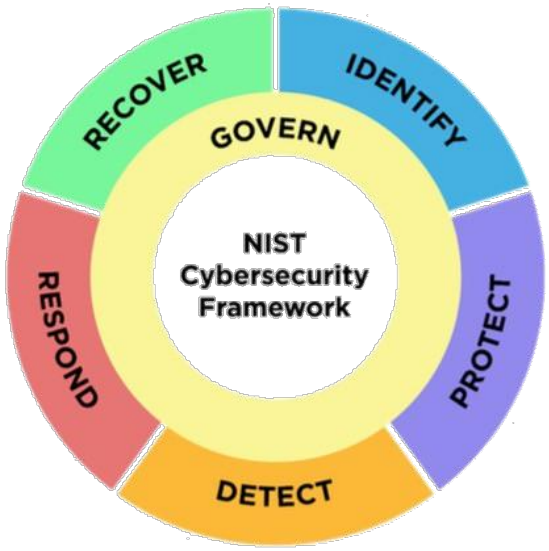


Fig. 2. CSF Functions

La Figura 2 muestra las Funciones del CSF como una rueda porque todas las Funciones se relacionan entre sí.
Por ejemplo, una organización clasificará los activos en IDENTIFICAR y tomará medidas para protegerlos en PROTEGER. Las inversiones en planificación y pruebas en las Funciones GOVERN e IDENTIFY apoyarán la detección oportuna de eventos inesperados en la Función DETECT, así como las acciones de respuesta a incidentes y recuperación de incidentes de ciberseguridad en las Funciones RESPOND y RECOVER. GOVERN está en el centro de la rueda porque informa sobre cómo una organización implementará las otras cinco Funciones.

NUCLEO CSF v 2.0

Las funciones deben abordarse simultáneamente. Las acciones que apoyan la GESTIÓN, IDENTIFICACIÓN, PROTECCIÓN y DETECCIÓN deben realizarse de forma continua, y las acciones que apoyan la RESPUESTA y RECUPERACIÓN deben estar preparadas en todo momento y llevarse a cabo cuando se produzcan incidentes de ciberseguridad. Todas las funciones tienen papeles vitales relacionados con los incidentes de ciberseguridad. Los resultados GOVERN, IDENTIFY y PROTECT ayudan a prevenir y prepararse para los incidentes, mientras que los resultados GOVERN, DETECT, RESPOND y RECOVER ayudan a descubrir y gestionar los incidentes.

Cada Función recibe el nombre de un verbo que resume su contenido. Cada función se divide en categorías, que son los resultados de ciberseguridad relacionados que componen colectivamente la función. Las subcategorías dividen a su vez cada categoría en resultados más específicos de actividades técnicas y de gestión. Las subcategorías no son exhaustivas, pero describen resultados detallados que apoyan cada categoría.

Las Funciones, Categorías y Subcategorías se aplican a todas las TIC utilizadas por una organización, incluida la tecnología de la información (TI), el Internet de las Cosas (IoT) y la tecnología operativa (OT). También se aplican a todos los tipos de entornos tecnológicos, incluidos los sistemas en la nube, móviles y de inteligencia artificial. El Núcleo CSF está orientado al futuro y pretende aplicarse a futuros cambios en tecnologías y entornos.

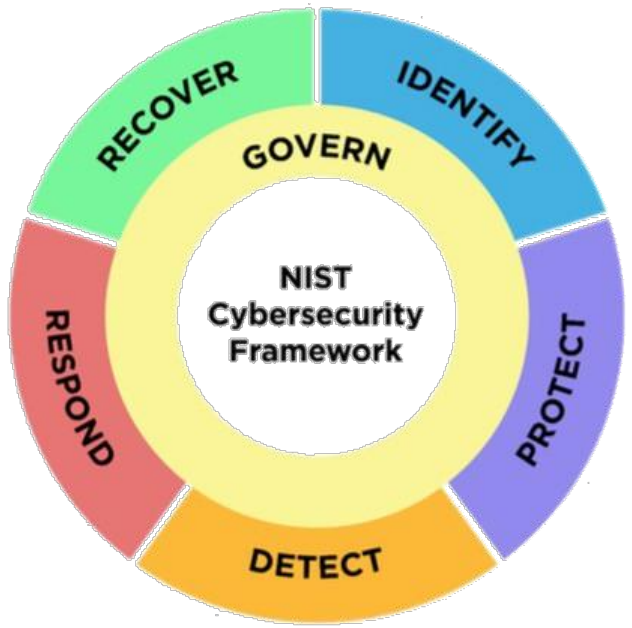


Fig. 2. CSF Functions

Introducción a Perfiles y Niveles de CSF v 2.0

LCSPC™ Versión 062024

Perfiles CSF NIST v 2.0

Perfiles CSF

Un Perfil Organizacional CSF describe la postura de ciberseguridad actual y/u objetivo de una organización en términos de los resultados del Núcleo.

Los Perfiles Organizativos se utilizan para comprender, adaptar, evaluar, priorizar y comunicar los resultados del Núcleo teniendo en cuenta los objetivos de la misión de una organización, las expectativas de las partes interesadas, el panorama de amenazas y los requisitos.

Una organización puede entonces priorizar sus acciones para lograr resultados específicos y comunicar esa información a las partes interesadas.

Fig. 3. Steps for creating and using a CSF Organizational Profile

Perfiles CSF NIST v 2.0

Cada perfil organizativo incluye uno o ambos de los siguientes elementos:

Un Perfil Actual especifica los resultados básicos que una organización está logrando actualmente (o intentando lograr) y caracteriza cómo o en qué medida se está logrando cada resultado.

Un Perfil Objetivo especifica los resultados deseados que una organización ha seleccionado y priorizado para alcanzar sus objetivos de gestión de riesgos de ciberseguridad. Un Perfil Objetivo considera cambios anticipados a la postura de ciberseguridad de la organización, tales como nuevos requerimientos, adopción de nuevas tecnologías, y tendencias de inteligencia de amenazas.

Un **perfil comunitario** es una base de referencia de los resultados de los CSF que se crea y publica para abordar intereses y objetivos compartidos entre varias organizaciones.
Un **perfil comunitario** suele desarrollarse para un sector, 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. Se pueden encontrar ejemplos de perfiles comunitarios en el sitio web del NIST CSF.

Perfiles CSF NIST v 2.0

1. Alcance del Perfil Organizativo. Documentar los hechos y supuestos de alto nivel en los que se basará el perfil para definir su alcance. Una organización puede tener tantos Perfiles Organizacionales como desee, cada uno con un alcance diferente. Por ejemplo, un perfil puede abarcar toda una organización o limitarse a los sistemas financieros de una organización o a contrarrestar amenazas de ransomware y manejar incidentes de ransomware que involucren esos sistemas financieros.

2. Recopilar la información necesaria para preparar el Perfil Organizativo. Ejemplos de información pueden incluir políticas organizacionales, prioridades y recursos de gestión de riesgos, perfiles de riesgo empresarial, registros de análisis de impacto de negocio (BIA), requisitos y estándares de ciberseguridad seguidos por la organización, prácticas y herramientas (por ejemplo, procedimientos y salvaguardas), y roles de trabajo.

Fig. 3. Steps for creating and using a CSF Organizational Profile

Perfiles CSF NIST v 2.0

3. Crear el perfil organizativo. Determine qué tipo de información debe incluir el Perfil para los resultados del MCA seleccionado y documente la información necesaria. Considere las implicaciones de riesgo del Perfil Actual para informar la planificación y priorización del Perfil Objetivo. Asimismo, considere el uso de un Perfil Comunitario como base para el Perfil Objetivo.

4. Analizar las diferencias entre el Perfil Actual y el Perfil Objetivo, y crear un plan de acción. Llevar a cabo un análisis de brechas para identificar y analizar las diferencias entre el Perfil Actual y el Perfil Objetivo, y desarrollar un plan de acción priorizado (por ejemplo, registro de riesgos, informe detallado de riesgos, Plan de Acción e Hitos [POA&M]) para abordar esas brechas.

5. Aplicar el plan de acción y actualizar el perfil de la organización. Siga el plan de acción para abordar las brechas y mover la organización hacia el Perfil Objetivo. Un plan de acción puede tener un plazo global o ser continuo.

Fig. 3. Steps for creating and using a CSF Organizational Profile

Perfiles CSF NIST v 2.0

Dada la importancia de la mejora continua, una organización puede repetir estos pasos tantas veces como sea necesario.

Existen usos adicionales para los Perfiles Organizacionales.

Por ejemplo, un Perfil Actual puede ser utilizado para documentar y comunicar las capacidades de ciberseguridad de la organización y las oportunidades conocidas de mejora con las partes interesadas externas, tales como socios de negocios o clientes potenciales.

También, un Perfil Objetivo puede ayudar a expresar los requisitos y expectativas de gestión de riesgos de ciberseguridad de la organización a proveedores, socios y otras terceras partes como un objetivo a alcanzar por esas partes.

Fig. 3. Steps for creating and using a CSF Organizational Profile

Niveles CSF NIST v 2.0

Niveles CSF

Una organización puede optar por utilizar los niveles para informar sus perfiles actual y objetivo.

Los niveles caracterizan el rigor de las prácticas de gobierno y gestión de los riesgos de ciberseguridad de una organización, y proporcionan un contexto sobre cómo una organización ve los riesgos de ciberseguridad y los procesos establecidos para gestionar esos riesgos.

Los niveles describen una progresión desde respuestas informales y ad hoc hasta enfoques ágiles, informados sobre el riesgo y en continua mejora. La selección de niveles ayuda a establecer el tono general de cómo una organización gestionará sus riesgos de ciberseguridad.

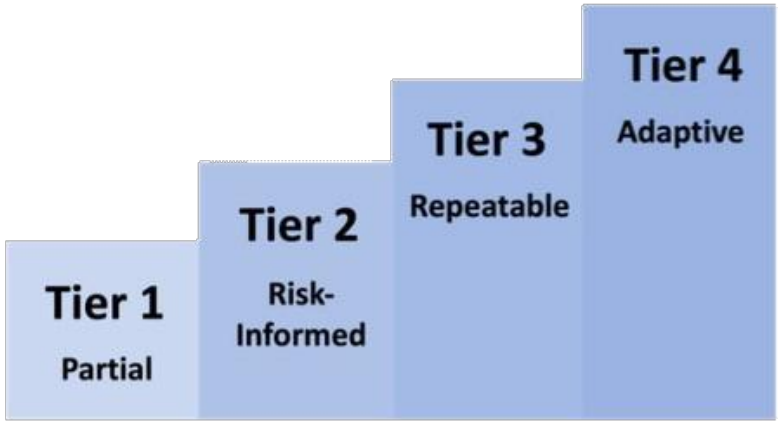


Fig. 4. CSF Tiers for cybersecurity risk governance and management

Los niveles, como se muestra en la Fig. 4 y se ilustra teóricamente en el Apéndice B, reflejan las prácticas de una organización para la gestión de riesgos de ciberseguridad como Parcial (Nivel 1), Informado sobre el Riesgo (Nivel 2), Repetible (Nivel 3) y Adaptable (Nivel 4).

Niveles CSF NIST v 2.0

Los niveles deben complementar la metodología de gestión de riesgos de ciberseguridad de una organización en lugar de sustituirla.

Por ejemplo, una organización puede utilizar los niveles para comunicarse internamente como punto de referencia para un enfoque de toda la organización1 de la gestión de los riesgos de ciberseguridad.

Se fomenta la progresión a niveles superiores cuando los riesgos o mandatos son mayores o cuando un análisis coste-beneficio indica una reducción factible y rentable de los riesgos negativos de ciberseguridad.

El sitio web del NIST CSF proporciona información adicional sobre el uso de perfiles y niveles. Incluye punteros a plantillas de perfiles organizativos alojadas en el NIST y un repositorio de perfiles comunitarios en diversos formatos legibles por máquina y por el ser humano.

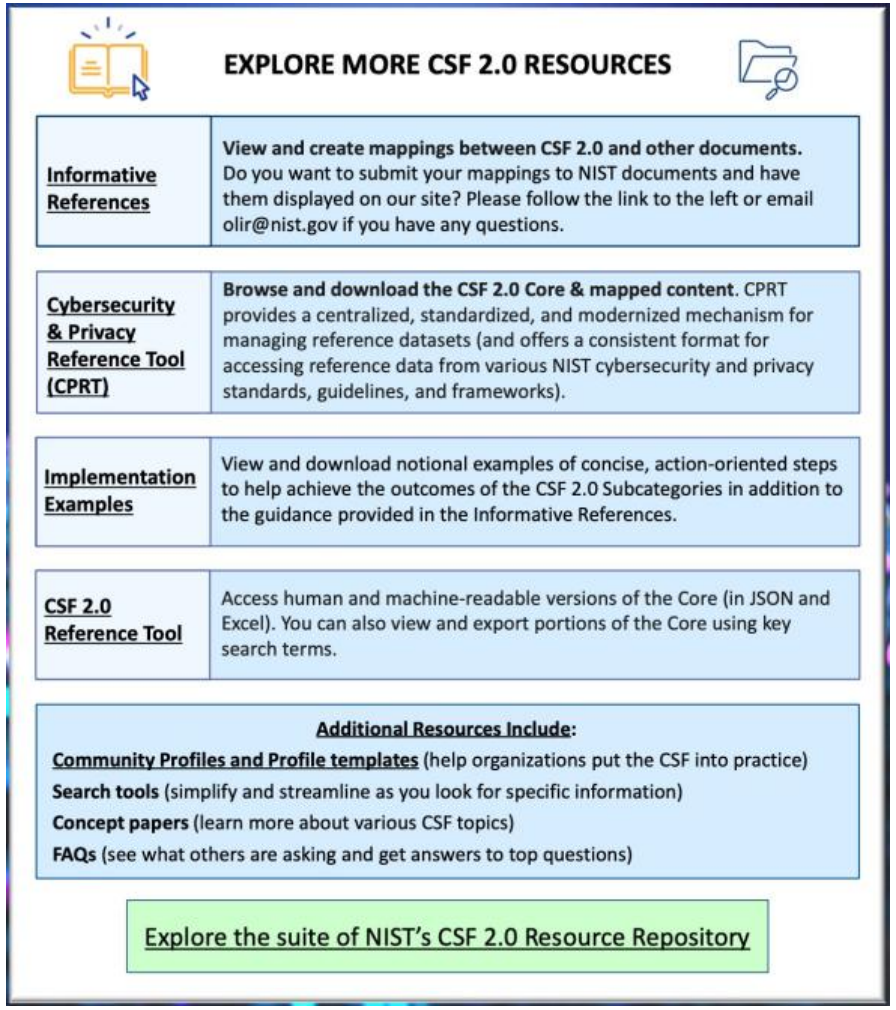
Niveles CSF NIST v 2.0

Recursos en línea que complementan el CSF

El NIST y otras organizaciones han producido un conjunto de recursos en línea que ayudan a las organizaciones a comprender, adoptar y utilizar la CSF.

Dado que están alojados en línea, estos recursos adicionales pueden actualizarse con mayor frecuencia que este documento, que se actualiza con poca frecuencia para brindar estabilidad a sus usuarios, y estar disponibles en formatos legibles, a saber:

- Referencias informativas
- Ejemplos de aplicación
- Guías de inicio rápido.

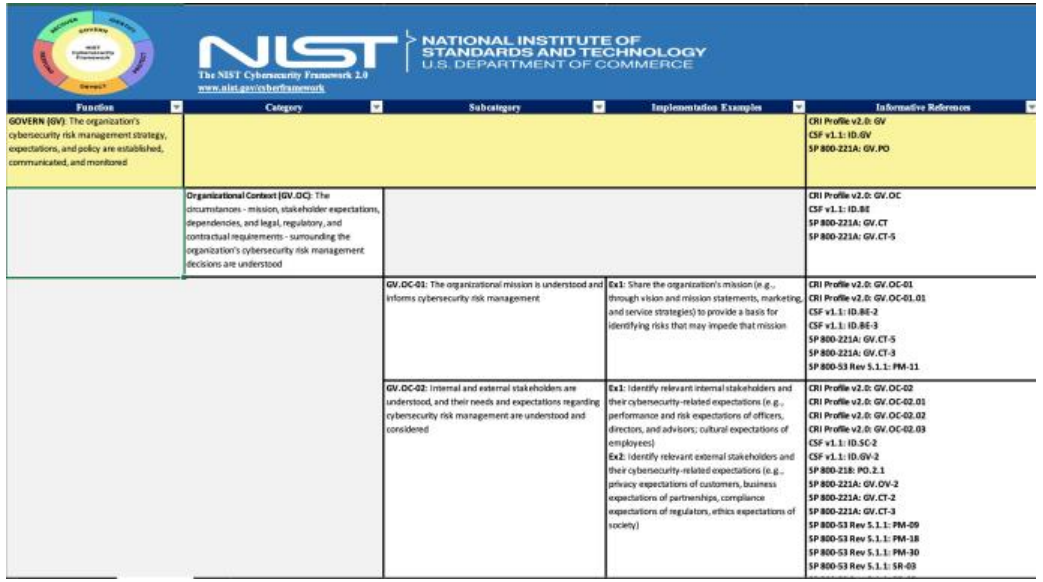


Niveles CSF NIST v 2.0

Las ***referencias informativas*** son mapas que indican las relaciones entre el núcleo básico y diversas normas, directrices, reglamentos y otros contenidos.
Las Referencias Informativas ayudan a informar sobre cómo una organización puede lograr los resultados del Núcleo. Las referencias informativas pueden ser específicas de un sector o de una tecnología. Pueden ser producidas por el NIST o por otra organización. Algunas referencias informativas tienen un alcance más limitado que una subcategoría. Por ejemplo, un control particular de SP 800-53, Controles de Seguridad y Privacidad para Sistemas de Información y Organizaciones, puede ser una de las muchas referencias necesarias para lograr el resultado descrito en una Subcategoría.

Otras Referencias Informativas pueden ser de más alto nivel, como un requisito de una política que aborda parcialmente numerosas Subcategorías.

Al utilizar el CSF, una organización puede identificar las Referencias Informativas más relevantes.


NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE
The NIST Cybersecurity Framework 2.0
www.nist.gov/cyberframework

Function	Category	Subcategory	Implementation Examples	Informative References
GOVERN (GV): The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored				CRI Profile v2.0: GV CSF v1.1: ID.GV SP 800-221A: GV.PO
	Organizational Context (GV.OC): The circumstances - mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements - surrounding the organization's cybersecurity risk management decisions are understood			CRI Profile v2.0: GV.OC CSF v1.1: ID.BE SP 800-221A: GV.CT SP 800-221A: GV.CT-5
		GV.OC-01: The organizational mission is understood and informs cybersecurity risk management	**Ex1**: Share the organization's mission (e.g., through vision and mission statements, marketing, and service strategies) to provide a basis for identifying risks that may impede that mission	CRI Profile v2.0: GV.OC-01 CRI Profile v2.0: GV.OC-01.01 CSF v1.1: ID.BE-2 CSF v1.1: ID.BE-3 SP 800-221A: GV.CT-5 SP 800-221A: GV.CT-3 SP 800-53 Rev 5.1.1: PM-11
		GV.OC-02: Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered	**Ex1**: Identify relevant internal stakeholders and their cybersecurity-related expectations (e.g., performance and risk expectations of officers, directors, and advisors; cultural expectations of employees) **Ex2**: Identify relevant external stakeholders and their cybersecurity-related expectations (e.g., privacy expectations of customers, business expectations of partnerships, compliance expectations of regulators, ethics expectations of society)	CRI Profile v2.0: GV.OC-02 CRI Profile v2.0: GV.OC-02.01 CRI Profile v2.0: GV.OC-02.02 CRI Profile v2.0: GV.OC-02.03 CSF v1.1: ID.SC-2 CSF v1.1: ID.GV-2 SP 800-218: PO.2.1 SP 800-221A: GV.OV-2 SP 800-221A: GV.CT-2 SP 800-221A: GV.CT-3 SP 800-53 Rev 5.1.1: PM-09 SP 800-53 Rev 5.1.1: PM-18 SP 800-53 Rev 5.1.1: PM-30 SP 800-53 Rev 5.1.1: SR-03

https://www.nist.gov/informative-references

Niveles CSF NIST v 2.0

Los ***ejemplos de aplicación*** proporcionan ejemplos teóricos de pasos concisos y orientados a la acción para ayudar a lograr los resultados de las subcategorías. Los verbos utilizados para expresar los Ejemplos incluyen compartir, documentar, desarrollar, realizar, supervisar, analizar, evaluar y ejercer.

Los Ejemplos no son una lista exhaustiva de todas las acciones que podría tomar una organización para lograr un resultado, ni representan una línea de base de las acciones necesarias para hacer frente a los riesgos de ciberseguridad.

NIST CSF 2.0 Implementation Examples
February 26, 2024

Category	Subcategory	Implementation Examples
Organizational Context (GV.OC): The circumstances — mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements — surrounding the organization's cybersecurity risk management decisions are understood		
	GV.OC-01: The organizational mission is understood and informs cybersecurity risk management	**Ex1:** Share the organization's mission (e.g., through vision and mission statements, marketing, and service strategies) to provide a basis for identifying risks that may impede that mission
	GV.OC-02: Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered	**Ex1:** Identify relevant internal stakeholders and their cybersecurity-related expectations (e.g., performance and risk expectations of officers, directors, and advisors; cultural expectations of employees) **Ex2:** Identify relevant external stakeholders and their cybersecurity-related expectations (e.g., privacy expectations of customers, business expectations of partnerships, compliance expectations of regulators, ethics expectations of society)

https://www.nist.gov/system/files/documents/2023/08/07/CSF%202.0%20Core%20with%20Examples%20Discussion%20Draft%5B74%5D.pdf

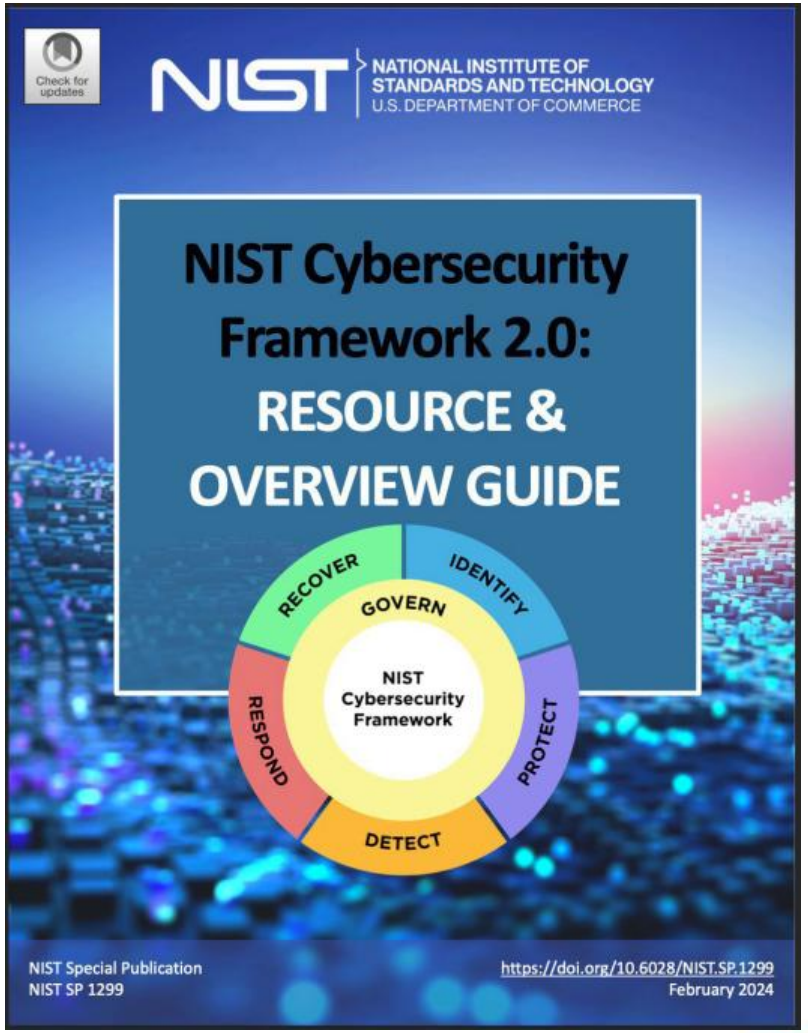
Niveles CSF NIST v 2.0

Las ***Guías de Inicio Rápido*** (QSG) son documentos breves sobre temas específicos relacionados con los CSF y a menudo se adaptan a audiencias específicas.

Las QSG pueden ayudar a una organización a implementar el CSF porque destilan partes específicas del CSF en "primeros pasos" procesables que una organización puede considerar en el camino hacia la mejora de su postura de ciberseguridad y la gestión de los riesgos asociados.

Las guías se revisan en sus propios plazos, y se añaden nuevas guías según sea necesario.

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1299.pdf



Guía de Inicio Rápido CSF v 2.0

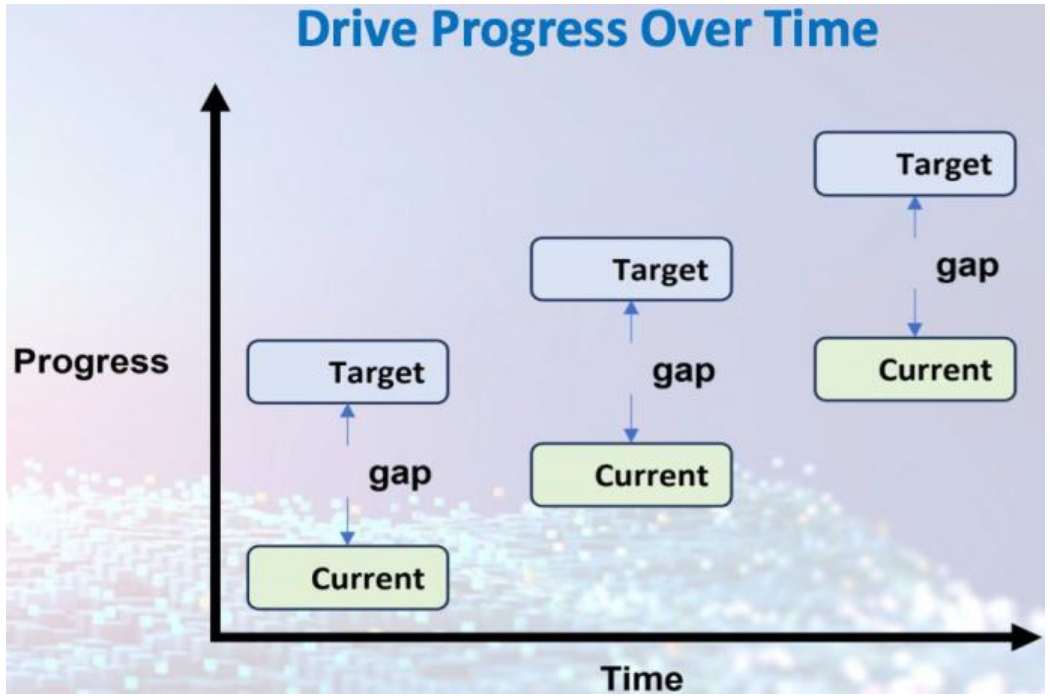
LCSPC™ Versión 062024

Impulsar el progreso a lo largo del tiempo con perfiles organizativos

Un **Perfil Organizativo** describe la postura de ciberseguridad actual y/u objetivo de una organización en términos de resultados de ciberseguridad del Marco de Ciberseguridad (CSF) Básico.

Los perfiles organizativos se utilizan para comprender, adaptar, evaluar y priorizar los resultados de ciberseguridad basándose en los objetivos de la misión de una organización, las expectativas de las partes interesadas, el panorama de amenazas y los requisitos.
La organización puede entonces actuar estratégicamente para lograr esos resultados.

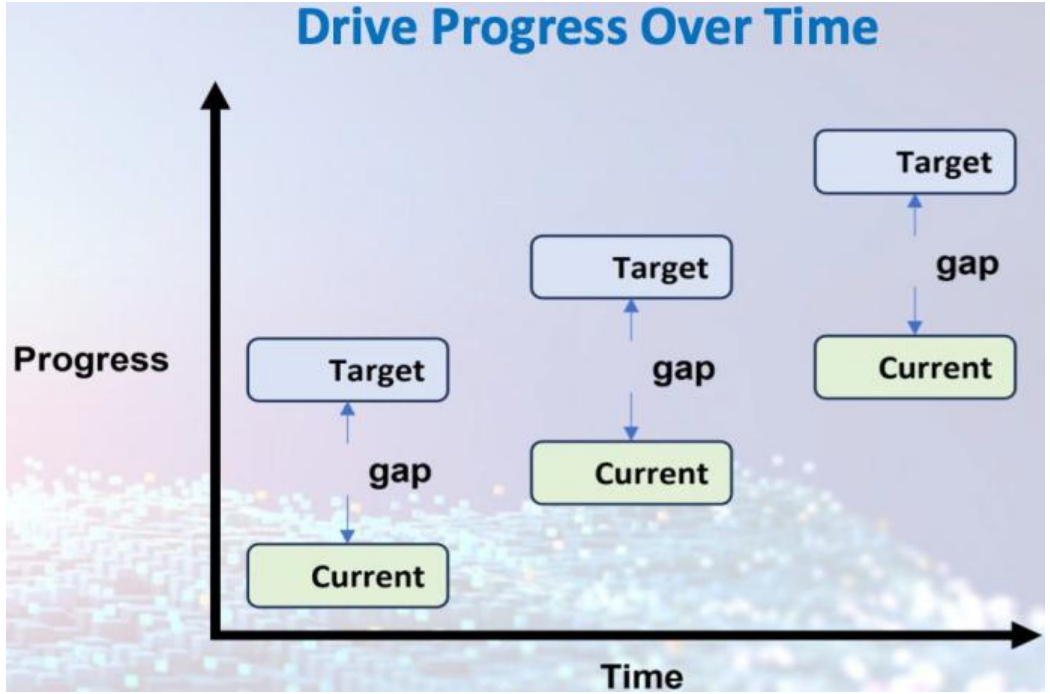
Estos perfiles también pueden utilizarse para evaluar el progreso hacia los resultados previstos y para comunicar la información pertinente a las partes interesadas.



Los Perfiles Organizativos pueden clasificarse como:

- Un ***Perfil Actual*** que especifica los resultados CSF que una organización está logrando actualmente y caracteriza cómo o en qué medida se está logrando cada resultado.

- Un ***Perfil Objetivo*** que especifica los resultados CSF deseados que una organización ha seleccionado y priorizado para alcanzar sus objetivos de gestión de riesgos de ciberseguridad. Un Perfil Objetivo considera cambios anticipados a la postura de ciberseguridad de la organización, tales como nuevos requerimientos, adopción de nuevas tecnologías y tendencias en inteligencia de amenazas.



Guía de Inicio CSF v 2.0

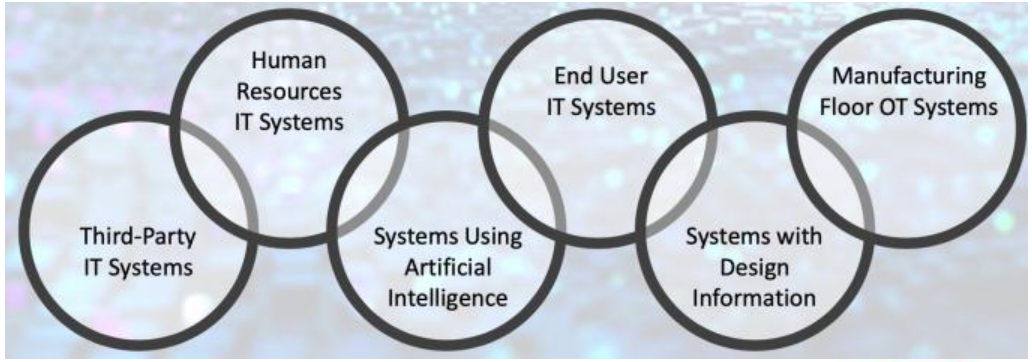
Crear y utilizar perfiles organizativos con el proceso en cinco pasos de CSF

CSF 2.0 describe un proceso de cinco pasos para crear y utilizar perfiles organizativos.

Más concretamente, el proceso compara un Perfil objetivo aspiracional 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 a perfeccionar el perfil objetivo que se utilizará en la siguiente evaluación.



1. ALCANCE DEL PERFIL ORGANIZATIVO

El alcance define los hechos y supuestos de alto nivel en los que se basarán los perfiles.

Puede tener tantos perfiles organizativos como desee, cada uno con un ámbito diferente. Las preguntas que preguntas a las que debe responder al definir el alcance de su perfil:

- ¿Cuál es la razón para crear el perfil organizativo?
- ¿Cubrirá el perfil toda la organización? Si no, ¿cuáles de las divisiones de la organización, activos de datos, activos tecnológicos, productos y servicios, y/o socios y proveedores serán incluidos?
- ¿El perfil abordará todos los tipos de amenazas, vulnerabilidades, ataques y defensas de ciberseguridad? 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 el perfil organizativo

Formas de concebir los perfiles

Una organización determinada puede desear utilizar varios Perfiles.

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

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

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

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

Guía de Inicio CSF v 2.0

2. RECOPILAR LA INFORMACIÓN NECESARIA

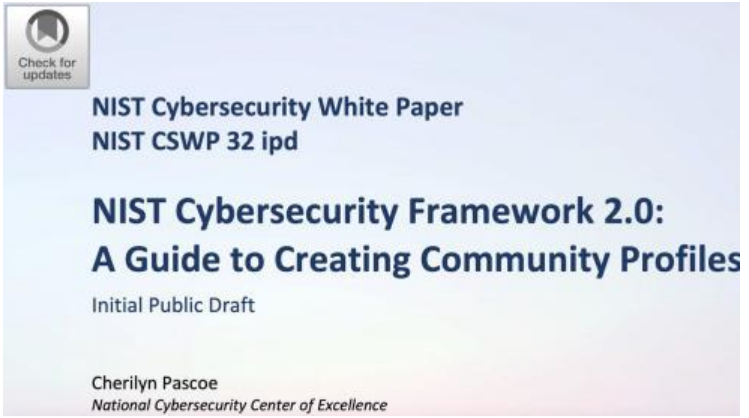
Ejemplos de información pueden incluir políticas organizativas, gestión de riesgos prioridades y recursos, requisitos y normas de ciberseguridad...

Las fuentes de información necesarias dependerán del caso de uso, los elementos que capturarán los perfiles y el nivel de detalle deseado. Las fuentes comunes de información incluyen

1. Perfiles comunitarios

Un **perfil comunitario** es una base de referencia de los resultados de los 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.



https://www.nist.gov/profiles-0

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 ser adaptado mediante:

- Ajustando las prioridades de determinados resultados de los CSF.
- Añadiendo subcategorías específicas de la organización, referencias informativas u orientaciones de aplicación.

Las fuentes de información necesarias dependerán del caso de uso, los elementos que capturarán los perfiles y el nivel de detalle deseado. Las fuentes comunes de información incluyen

2. Plantilla de perfil organizativo del NIST

El NIST proporciona una plantilla de perfil organizativo del CFS en forma de hoja de cálculo de Microsoft Excel.

La plantilla facilita la comparación lado a lado de los Perfiles Actual y Objetivo para identificar y analizar brechas. Puede encontrar la plantilla en el sitio web CSF 2.0

Guía de Inicio CSF v 2.0

Priorización

La característica definitoria de un perfil

La noción central de un *Perfil Objetivo* es determinar diferentes prioridades para los resultados CSF aplicables.

Las prioridades le ayudan a determinar las partes de su programa de ciberseguridad que deben recibir más o menos recursos. Las prioridades de ciberseguridad 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 Core apoya las decisiones de respuesta al riesgo.

https://www.nist.gov/profiles-0

3. CREAR EL PERFIL ORGANIZATIVO – PARTE 1

Determine qué tipos de información de apoyo debe incluir cada Perfil para los resultados del MCA seleccionado...

Los pasos para crear un perfil organizativo son:

3a: Descargue la última hoja de cálculo de plantilla de Perfil Organizacional CSF y personalícela como desee

3b: Incluya los resultados de ciberseguridad que se apliquen a su caso de uso y documente las justificaciones según sea necesario.

3c: Documente las prácticas actuales de ciberseguridad en las columnas del perfil actual. Las entradas más detalladas pueden proporcionar una mejor comprensión para los pasos posteriores.

Guía de Inicio CSF v 2.0

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

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

CSF Outcomes		Current Profile			Target Profile	
Identifier	**Description**	**Practices**	**Status**	**Rating**	**Priority**	**Goals**
The identifiers and descriptions from the CSF Core – Functions, Categories, Subcategories. You can also add your own outcomes to address your organization's unique risks and requirements.		Policies, processes, procedures and other activities related to an outcome. May include artifacts that contain evidence of achieving an outcome.	The current state or condition of an outcome, such as whether it is being achieved and to what degree.	An assessment or evaluation of current practices using scales such as: • high/medium/low • 1-5 • 0-100%, • red/yellow/green	The relative importance of an outcome using scales such as: • Low/Medium/High • 1/2/3/4/5 • rankings (1, 2, 3...)	Such as: • Policies, Processes, and Procedures • Roles and Responsibilities Selected from: • Informative References - standards, guidance, and best practices

3. CREAR EL PERFIL ORGANIZATIVO – PARTE 2

La siguiente tabla muestra un ejemplo teórico de una única fila de un perfil de organización.

Sólo tiene valor ilustrativo. A continuación, se ofrecen algunos consejos extraídos del ejemplo:

- Añada y elimine columnas de la plantilla Perfil de la organización según sus necesidades. El CSF anima a los usuarios a registrar la información que consideren importante y a utilizar el formato que prefieran.
- Las columnas no tienen por qué ser las mismas para el perfil actual y el perfil de destino.
- Este ejemplo muestra los controles de la norma **SP 800-53** entre corchetes.

CSF Outcomes		Current Profile			Target Profile	
Identifier	**Description**	**Practices**	**Status**	**Rating**	**Priority**	**Goals**
PR.PS-01	Configuration management practices are established and applied	Policy: Configuration Management policy version 1.4, last updated 10/14/22. Defines the configuration change control policy [**CM-1**]. Procedures: System owners and technology managers informally implement configuration management practices. Change control processes are not consistently followed. The CIO specifies configuration baselines [**CM-2**] for the IT platforms and applications most widely used within the organization, but baseline use is not monitored or enforced consistently across the organization.	Configuration management is partially implemented within the organization. Some systems do not follow available baselines and other systems do not have baselines, so they may have weak configurations that make them more susceptible to misuse and compromise. Unauthorized changes may go undetected. Some changes are not tested or tracked.	3 *out of 5*	High	Policy: The Configuration Management policy requires configuration baselines to be specified, used, enforced, and maintained for all commodity technologies used by the organization. The policy requires change control processes to be followed for all technologies within the organization [**CM-1**]. Procedures: Each division of the organization has a configuration management plan [**CM-9**], as well as maintains, implements, and enforces configuration baselines [**CM-2**] and settings [**CM-6**] for their systems. Baselines are applied to all systems before production release. All systems are continuously monitored for unexpected configuration changes, and tickets are automatically generated when deviations from baselines occur. Designated parties review change requests and corresponding impact analyses [**CM-4**] and approve or deny each [**CM-3**].

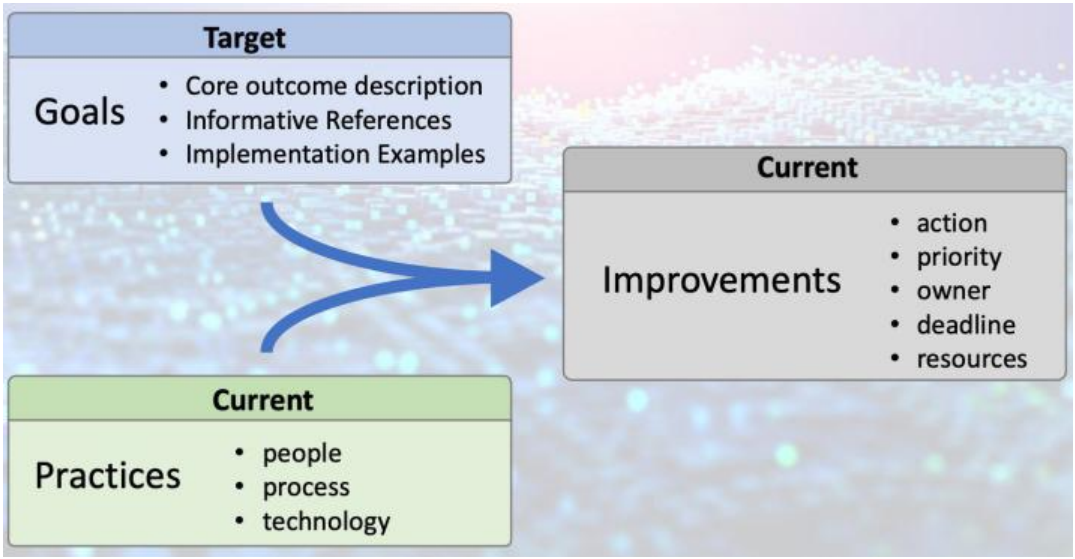
4. GAP ANALISIS Y CREAR UN PLAN DE ACCIÓN – PARTE 1

Identificar y analizar las diferencias entre el perfil actual y el objetivo permite a una organización detectar carencias y desarrollar un plan de acción prioritario priorizado para abordar esas carencias.

Utilizar los Perfiles de esta manera ayuda a su organización a tomar decisiones mejor informadas sobre cómo mejorar la gestión de riesgos de ciberseguridad de una manera prioritaria y rentable.

Paso 4a
Cómo analizar los GAP'S

Compare y contraste sus prácticas actuales, en cuanto 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 ciberseguridad. 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 (por ejemplo, personal, financiación). Los planes de acción deben tener todos los elementos esenciales del gráfico (izquierda).

4. GAP ANALISIS Y CREAR UN PLAN DE ACCIÓN – PARTE 2

La identificación y el análisis de las diferencias entre el perfil actual y el perfil deseado permiten a la organización detectar Gaps y elaborar un plan de acción prioritario para subsanarlas y desarrollar un plan de acción priorizado para abordar esos Gaps.

El CSF ofrece enlaces a herramientas, controles y recursos de aplicación que le ayudarán a analizar las deficiencias **[Paso 4a]** y a crear planes de acción **[Paso 4b].**

Un enfoque recomendado para desarrollar planes de acción es utilizar el NIST CSF 2.0 Reference Tool para seguir las referencias de las Subcategorías pertinentes de su Perfil Objetivo a los controles **NIST SP 800-53** asociados.

Guía de Inicio CSF v 2.0

Qué buenas prácticas utilizar

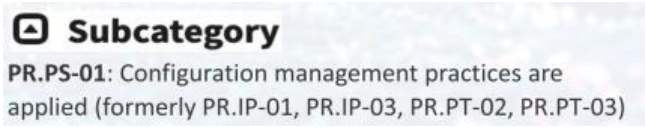
Referencias informativas: relaciones entre el núcleo y diversas mejores prácticas, incluidas normas, directrices, reglamentos y otros recursos. Las referencias ayudan a informar sobre cómo una organización puede lograr los resultados del CSF. También ayudan a conectar los resultados deseados con otros documentos comunes de ciberseguridad, como **ISO/IEC 27001** y **SP 800-53** que proporciona un catálogo de controles de seguridad y privacidad.

Cómo aplicar 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. El NIST CSF 2.0 Reference Tool permite a los usuarios explorar el núcleo completo del CSF 2.0 y descargarlo en formatos Excel y JSON.

Ejemplo de una Implementación

Extracto del NIST CSF 2.0 Reference Tool.



Ejemplos de implementación:

Ej1: Establecer, probar, desplegar y mantener líneas de base reforzadas que apliquen las políticas de ciberseguridad de la organización y proporcionen sólo las capacidades esenciales (es decir, el principio de mínima funcionalidad).

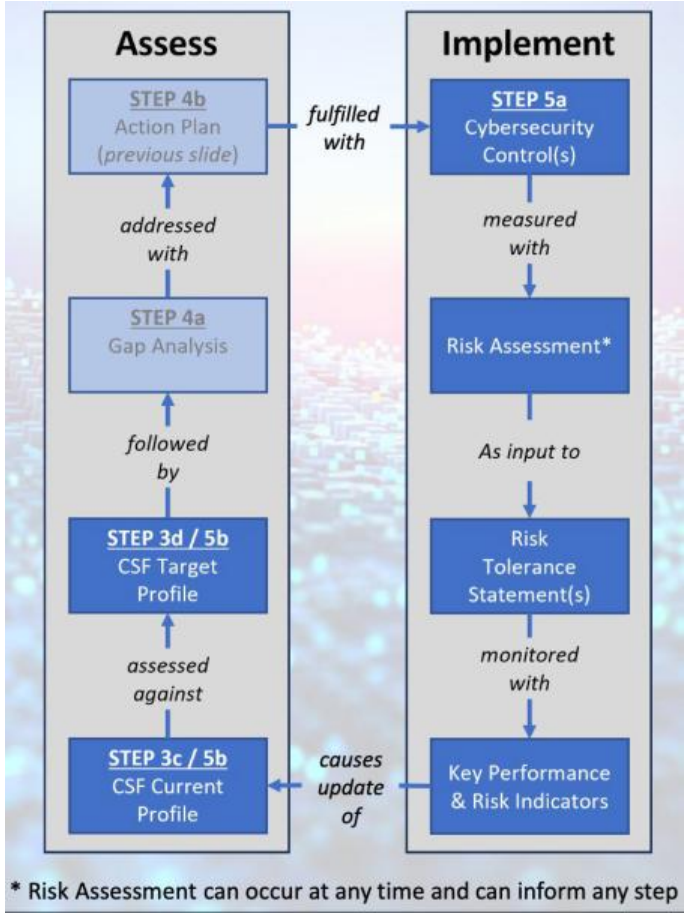
Ej2: Revisar todos los ajustes de configuración por defecto que puedan afectar potencialmente a la ciberseguridad al instalar o actualizar software.

5. APLICAR EL PLAN DE ACCIÓN Y ACTUALIZAR EL PERFIL

Paso 5a

Ejecución de los Planes de Acción

El Plan de Acción se lleva a cabo mediante una 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 supervisarse mediante Indicadores Clave de Rendimiento (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 dar lugar a actualizaciones del Plan de Acción, el Perfil Organizativo y/o las declaraciones de Tolerancia al Riesgo. El análisis de brechas también puede dar lugar a la creación de POA&M para las brechas que requerirán un plazo de remediación más largo. Se puede encontrar más información sobre KPI, KRI, Tolerancia al Riesgo y POA&M en **IR 8286B** y **SP 800-37.**



Guía de Inicio CSF v 2.0

Paso 5b

Actualizar su perfil

Implementar las actividades que siguen a su Plan de Acción son parte de un programa continuo de gestión de riesgos cibernéticos (bucles de retroalimentación y líneas de comunicación más matizadas que las mostradas). Las Evaluaciones de Riesgo, como se describe en SP 800-30 pueden aprovechar 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 dar lugar a actualizaciones del perfil organizativo.

Guía de Inicio CSF v 2.0

Lo que aprendimos. Este QSG explicó los siguientes términos:

Perfil organizativo - resultados básicos del MCA relevantes para una organización específica.
Perfil Comunitario - resultados básicos del CSF que se aplican a múltiples organizaciones.
Perfil Actual - los resultados de ciberseguridad que una organización está logrando actualmente.
Perfil Objetivo - los resultados deseados que una organización quiere lograr.
Gap Análisis - determinar las diferencias entre el perfil actual y el objetivo.
Referencias informativas - mejores prácticas que implementan varios resultados básicos del CSF.
Ejemplos de implementación - formas teóricas en que las organizaciones pueden lograr las subcategorías del CSF
Plan de acción - abordar las brechas y avanzar hacia el perfil objetivo.

Reading

IR 8286B — NIST IR 8286B, *Prioritizing Cybersecurity Risk for Enterprise Risk Management*

SP 800-37 — NIST SP 800-37 Revision 2, *Risk Management Framework for Information Systems & Organizations*

SP 800-53 — NIST SP 800-53 Revision 5, *Security and Privacy Controls for Information Systems & Organizations*

SP 800-30 — NIST SP 800-30 Revision 1, *Guide for Conducting Risk Assessments*

Resources

Organizational Profile Template | NIST CSF 2.0 Reference Tool
Informative References | Implementation Examples
A Guide to Creating CSF 2.0 Community Profiles
Quick-Start Guide for Using the CSF Tiers

Guía de Inicio CSF v 2.0

Lo que sigue. He aquí una lista de cosas que puede hacer para poner en práctica este CSF:

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

Reading

IR 8286B — NIST IR 8286B, *Prioritizing Cybersecurity Risk for Enterprise Risk Management*

SP 800-37 — NIST SP 800-37 Revision 2, *Risk Management Framework for Information Systems & Organizations*

SP 800-53 — NIST SP 800-53 Revision 5, *Security and Privacy Controls for Information Systems & Organizations*

SP 800-30 — NIST SP 800-30 Revision 1, *Guide for Conducting Risk Assessments*

Resources

Organizational Profile Template | NIST CSF 2.0 Reference Tool
Informative References | Implementation Examples
A Guide to Creating CSF 2.0 Community Profiles
Quick-Start Guide for Using the CSF Tiers

Comunicación e Integración Riesgos de CSF

LCSPC™ Versión 062024

Mejorar la comunicación e integración del Ciber riesgo

Mejorar la comunicación e integración de los riesgos de ciberseguridad

El uso del CSF variará en función de la misión y los riesgos únicos de una organización. Con una comprensión de las expectativas de las partes interesadas y el apetito de riesgo y tolerancia (como se indica en GOVERN), una organización puede priorizar las actividades de ciberseguridad para tomar decisiones informadas sobre los gastos y acciones de ciberseguridad.

Una organización puede optar por gestionar el riesgo de una o más maneras -incluyendo mitigar, transferir, evitar o aceptar riesgos negativos y realizar, compartir, mejorar o aceptar riesgos positivos- dependiendo de los impactos y probabilidades potenciales.

Es importante destacar que una organización puede utilizar el CSF tanto internamente para gestionar sus capacidades de ciberseguridad como externamente para supervisar o comunicarse con terceros.

Independientemente de la utilización del CSF, una organización puede beneficiarse del uso del CSF como guía para ayudarla a entender, evaluar, priorizar y comunicar los riesgos de ciberseguridad y las acciones que gestionarán esos riesgos.
Los resultados seleccionados pueden utilizarse para centrarse y aplicar decisiones estratégicas para mejorar las posturas de ciberseguridad y mantener la continuidad de las funciones esenciales de la misión teniendo en cuenta las prioridades y los recursos disponibles.

Mejorar la comunicación de la gestión de riesgos

Mejorar la comunicación de la gestión de riesgos

El CSF proporciona una base para mejorar la comunicación en relación con las expectativas, la planificación y los recursos de ciberseguridad.

El CSF fomenta el flujo bidireccional de información (como se muestra en la mitad superior de la Fig. 5) entre los ejecutivos que se centran en las prioridades de la organización y la dirección estratégica y los gerentes que gestionan los riesgos específicos de ciberseguridad que podrían afectar a la consecución de esas prioridades.
El CSF también apoya un flujo similar (como se muestra en la mitad inferior de la Fig. 5) entre los directivos y los profesionales que implementan y operan las tecnologías.
La parte izquierda de la figura indica la importancia de que los profesionales compartan sus actualizaciones, ideas y preocupaciones con los directivos y ejecutivos.

Fig. 5. Using the CSF to improve risk management communication

Mejorar la comunicación de la gestión de riesgos

La preparación para crear y utilizar perfiles organizativos implica recabar información de los directivos sobre las prioridades, los recursos y la orientación del riesgo de la organización. A continuación, los directivos colaboran con los profesionales para comunicar las necesidades de la empresa y crear perfiles organizativos basados en los riesgos.

Las acciones para cerrar cualquier brecha identificada entre los **Perfiles Actuales** y los **Perfiles Objetivo** serán implementadas por los directivos y los profesionales y proporcionarán aportaciones clave a los planes a nivel de sistema.

A medida que se alcanza el estado objetivo en toda la organización -incluidos los controles y la supervisión aplicados a nivel de sistema-, los resultados actualizados pueden compartirse mediante registros de riesgos e informes de progreso.

Como parte de la evaluación continua, los gestores obtienen información para realizar ajustes que reduzcan aún más los daños potenciales y aumenten los beneficios potenciales.

Fig. 5. Using the CSF to improve risk management communication

Las comunicaciones reflejadas en la mitad superior
de la Fig. 5 pueden incluir consideraciones para ERM
y los programas de nivel inferior y, por lo tanto, informar a los directivos y profesionales

Mejorar la Comunicación e Integración de Riesgos

Mejorar la comunicación de la gestión de riesgos

La función ***GOVERN*** apoya la comunicación de riesgos de la organización con los ejecutivos. Los debates de los ejecutivos tienen que ver con la estrategia, en particular con la forma en que las incertidumbres relacionadas con la ciberseguridad podrían afectar a la consecución de los objetivos de la organización.

Estas discusiones de gobierno apoyan el diálogo y el acuerdo sobre las estrategias de gestión de riesgos (incluido el riesgo de la cadena de suministro de ciberseguridad); funciones, responsabilidades y autoridades; políticas; y supervisión.

A medida que los ejecutivos establecen prioridades y objetivos de ciberseguridad basados en esas necesidades, comunican las expectativas sobre el apetito de riesgo, la responsabilidad y los recursos.

Los ejecutivos también son responsables de integrar la gestión de riesgos de ciberseguridad con los programas de ERM y los programas de gestión de riesgos de nivel inferior.

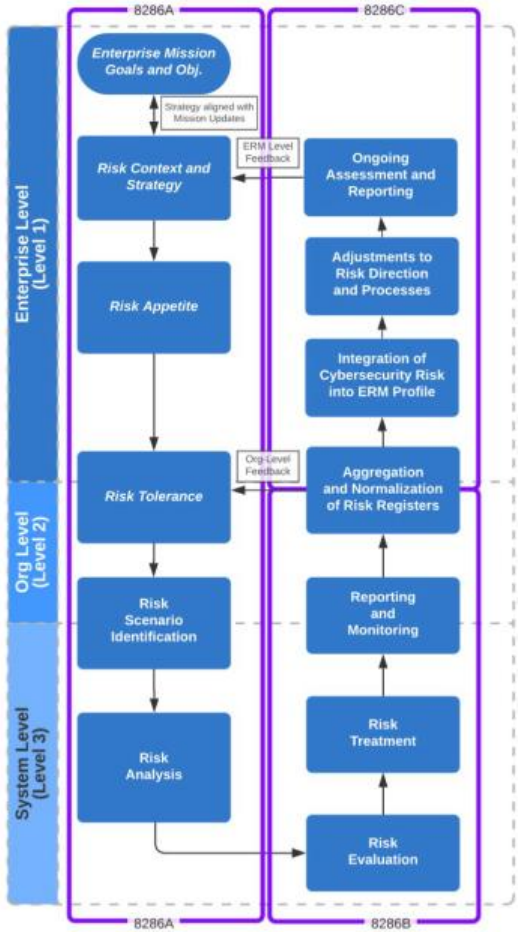


Figure 1: NISTIR 8286 Series Publications Describe Detailed CSRM/ERM Integration

Este informe destaca los aspectos de la Gestión de Riesgos de Ciberseguridad (CSRM) que son inherentes a las empresas, organizaciones y sistemas.

La gestión del riesgo empresarial (ERM) exige comprender los principales riesgos a los que se enfrenta una organización.

Mejorar la Comunicación e Integración de Riesgos

Los objetivos generales de ciberseguridad fijados por los ejecutivos se comunican y se transmiten en cascada a los directivos. En una entidad comercial, pueden aplicarse a una línea de negocio o división operativa. Para las entidades gubernamentales, pueden ser consideraciones a nivel de división o sucursal. Al aplicar el CSF, los directivos se centrarán en cómo alcanzar los objetivos de riesgo a través de servicios comunes, controles y colaboración, tal y como se expresa en el perfil de objetivos y se mejora a través de las acciones que se siguen en el plan de acción (por ejemplo, registro de riesgos, informe detallado de riesgos, POA&M).

Los profesionales se centran en implementar el estado objetivo y medir los cambios en el riesgo operativo para ayudar a planificar, llevar a cabo y supervisar actividades específicas de ciberseguridad.

A medida que se implementan los controles para gestionar el riesgo a un nivel aceptable, los profesionales proporcionan a los gerentes y ejecutivos la información (por ejemplo, indicadores clave de rendimiento, indicadores clave de riesgo) que necesitan para comprender la postura de ciberseguridad de la organización, tomar decisiones informadas y mantener o ajustar la estrategia de riesgo en consecuencia.

Los ejecutivos también pueden combinar estos datos de riesgo de ciberseguridad con información sobre otros tipos de riesgo de toda la organización. Las actualizaciones de las expectativas y prioridades se incluyen en Perfiles Organizativos actualizados a medida que se repite el ciclo.

Mejorar la integración con otros programas de gestión de riesgos

Mejorar la comunicación de la gestión de riesgos

Cada organización se enfrenta a numerosos tipos de riesgo de TIC (por ejemplo, privacidad, cadena de suministro, inteligencia artificial) y puede utilizar marcos y herramientas de gestión específicos para cada riesgo. Algunas organizaciones integran las TIC y todos los demás esfuerzos de gestión de riesgos a un alto nivel mediante el uso de ERM, mientras que otras mantienen los esfuerzos separados para garantizar una atención adecuada a cada uno de ellos.

Las organizaciones pequeñas, por su naturaleza, pueden supervisar el riesgo a nivel de empresa, mientras que las empresas más grandes pueden mantener esfuerzos separados de gestión de riesgos integrados en la ERM.
Las organizaciones pueden emplear un enfoque de ERM para equilibrar una cartera de consideraciones de riesgo, incluida la ciberseguridad, y tomar decisiones informadas.

Los ejecutivos reciben información significativa sobre las actividades de riesgo actuales y planificadas a medida que integran las estrategias de gobierno y riesgo con los resultados de los usos anteriores del CSF.

El CSF ayuda a las organizaciones a traducir su terminología sobre ciberseguridad y gestión de riesgos de ciberseguridad a un lenguaje general de gestión de riesgos que los ejecutivos entiendan.

Mejorar la integración con otros programas de gestión de riesgos

Una organización también puede encontrar el CSF beneficioso para integrar la gestión de riesgos de ciberseguridad con programas individuales de gestión de riesgos de TIC, tales como:

- **Gestión y evaluación de riesgos de ciberseguridad:** El CSF puede integrarse con programas establecidos de gestión y evaluación de riesgos de ciberseguridad, como SP 800- 37, Marco de gestión de riesgos para sistemas de información y organizaciones, y SP 800-30, Guía para realizar evaluaciones de riesgos del Marco de gestión de riesgos (RMF) del NIST. Para una organización que utilice el RMF del NIST y su conjunto de publicaciones, el CSF puede utilizarse para complementar el enfoque del RMF para seleccionar y priorizar los controles del SP 800-53, Controles de seguridad y privacidad para sistemas de información y organizaciones.

- **Riesgos para la privacidad:** Aunque la ciberseguridad y la privacidad son disciplinas independientes, sus objetivos se solapan en determinadas circunstancias, como se ilustra en la Fig. 6. La gestión de los riesgos de ciberseguridad es esencial para hacer frente a los riesgos para la privacidad relacionados con la pérdida de la confidencialidad, integridad y disponibilidad de los datos de las personas...

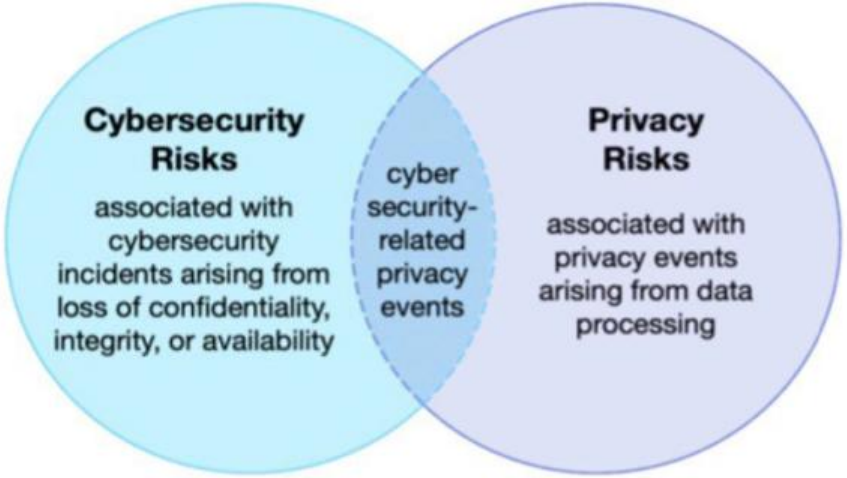


Fig. 6. Cybersecurity and privacy risk relationship

Mejorar la integración con otros programas de gestión de riesgos

- … Por ejemplo, las violaciones de datos pueden conducir al robo de identidad. Sin embargo, los riesgos para la privacidad también pueden surgir por medios no relacionados con incidentes de ciberseguridad. Una organización procesa datos para lograr objetivos de misión o de negocio, lo que a veces puede dar lugar a incidentes de privacidad por los que los individuos pueden experimentar problemas como resultado del procesamiento de datos. Estos problemas pueden expresarse de diversas maneras, pero el NIST los describe como efectos que van desde los de tipo dignidad (por ejemplo, vergüenza o estigma) hasta daños más tangibles (por ejemplo, discriminación, pérdida económica o daño físico). **El Marco de Privacidad y el Marco de Ciberseguridad del NIST** pueden utilizarse conjuntamente para abordar los diferentes aspectos de los riesgos de ciberseguridad y privacidad. Además, la **Metodología de Evaluación de Riesgos para la Privacidad (PRAM) del NIST** cuenta con un catálogo de problemas de ejemplo para su uso en evaluaciones de riesgos para la privacidad.

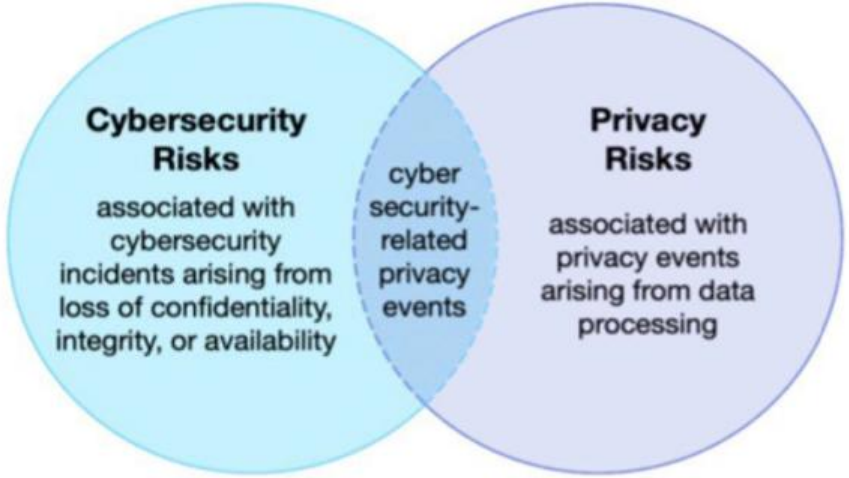


Fig. 6. Cybersecurity and privacy risk relationship

Mejorar la integración con otros programas de gestión de riesgos

- **Riesgos de la cadena de suministro:** Una organización puede utilizar el CSF para fomentar la supervisión de los riesgos de ciberseguridad y las comunicaciones con las partes interesadas a través de las cadenas de suministro. Todos los tipos de tecnología dependen de un ecosistema de cadena de suministro complejo, distribuido globalmente, extenso e interconectado, con rutas geográficamente diversas y múltiples niveles de subcontratación. Este ecosistema está compuesto por entidades de los sectores público y privado (por ejemplo, adquirentes, proveedores, desarrolladores, integradores de sistemas, proveedores de servicios de sistemas externos y otros proveedores de servicios relacionados con la tecnología) que interactúan para investigar, desarrollar, diseñar, fabricar, adquirir, entregar, integrar, operar, mantener, eliminar y utilizar o gestionar de otro modo productos y servicios tecnológicos. Estas interacciones están determinadas e influidas por tecnologías, leyes, políticas, procedimientos y prácticas.

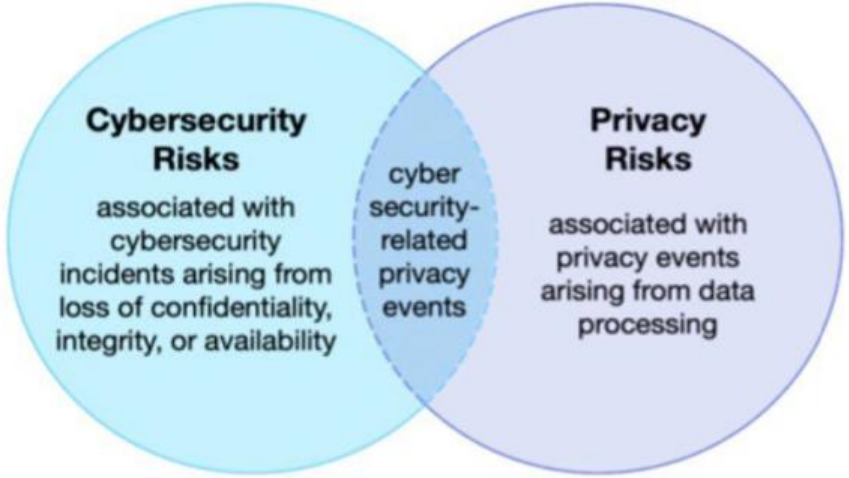


Fig. 6. Cybersecurity and privacy risk relationship

Mejorar la integración con otros programas de gestión de riesgos

- … Dadas las complejas e interconectadas relaciones de este ecosistema, la gestión de riesgos de la cadena de suministro (SCRM) es fundamental para las organizaciones. La SCRM de ciberseguridad (C-SCRM) es un proceso sistemático para gestionar la exposición al riesgo de ciberseguridad a lo largo de las cadenas de suministro y desarrollar estrategias, políticas, procesos y procedimientos de respuesta adecuados. Las Subcategorías dentro de la Categoría CSF C-SCRM [GV.SC] proporcionan una conexión entre los resultados que se centran puramente en la ciberseguridad y los que se centran en la C-SCRM. SP 800-161r1 (Revisión 1), ***Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations,*** proporciona información en profundidad sobre C-SCRM.

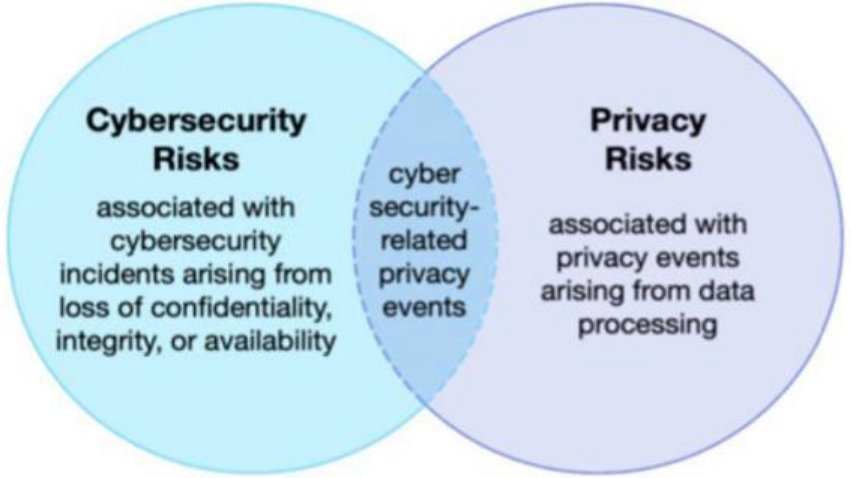


Fig. 6. Cybersecurity and privacy risk relationship

Mejorar la integración con otros programas de gestión de riesgos

- **Riesgos de las tecnologías emergentes:** A medida que aparecen nuevas tecnologías y nuevas aplicaciones de la tecnología, aparecen nuevos riesgos. Un ejemplo contemporáneo es la inteligencia artificial (IA), que presenta riesgos de ciberseguridad y privacidad, así como muchos otros tipos de riesgo. ***El Marco de Gestión de Riesgos de la Inteligencia Artificial del NIST*** (Artificial Intelligence Risk Management Framework, AI RMF) se desarrolló para ayudar a abordar estos riesgos. Tratar los riesgos de la IA junto con otros riesgos empresariales (por ejemplo, financieros, de ciberseguridad, de reputación y de privacidad) producirá un resultado más integrado y eficiencias organizativas. Las consideraciones y enfoques de gestión de riesgos de ciberseguridad y privacidad son aplicables al diseño, desarrollo, despliegue, evaluación y uso de sistemas de IA. El AI RMF Core utiliza Funciones, Categorías y Subcategorías para describir los resultados de la IA y ayudar a gestionar los riesgos relacionados con la IA.

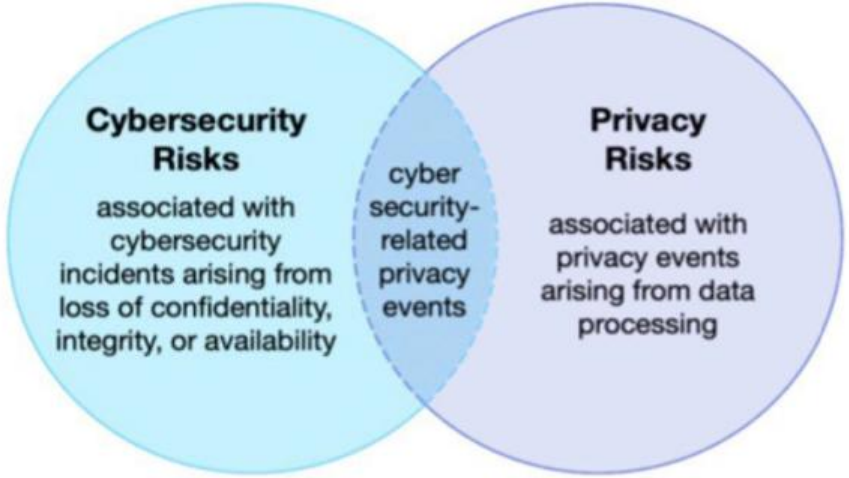


Fig. 6. Cybersecurity and privacy risk relationship

Apéndice A Núcleo del CSF

Apéndice A núcleo el CSF

Mejorar la comunicación de la gestión de riesgos

Este apéndice describe las funciones, categorías y subcategorías del núcleo del CSF.

La Tabla 1 enumera los nombres de las **Funciones y Categorías** del Núcleo CSF 2.0 y sus identificadores alfabéticos únicos.

Cada nombre de función de la tabla está vinculado a su parte del apéndice.

El orden de las **Funciones, Categorías y Subcategorías** del Núcleo no es alfabético, sino que está pensado para que tenga mayor resonancia entre los encargados de hacer operativa la gestión de riesgos dentro de una organización.

La numeración de las **subcategorías** no es secuencial intencionadamente; los huecos en la numeración indican subcategorías del MCA 1.1 que se reubicaron en el MCA 2.0.

Table 1. CSF 2.0 Core Function and Category names and identifiers

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

FUNCIÓN – GOBIERNO

Comprender y evaluar las necesidades específicas de ciberseguridad. Determine los riesgos y necesidades específicos de su organización. Discuta el entorno de riesgo actual y previsto y la cantidad de riesgo que su organización está dispuesta a aceptar. Recabe aportaciones e ideas de toda la organización. Comprenda lo que ha funcionado o no en el pasado y discútalo abiertamente.

Desarrolle una estrategia de riesgos de ciberseguridad a medida. Debe basarse en los objetivos específicos de ciberseguridad de su organización, el entorno de riesgo y las lecciones aprendidas del pasado y de otros. Gestione, actualice y discuta la estrategia a intervalos regulares. Las funciones y responsabilidades deben estar claras.

Establecer políticas definidas de gestión de riesgos. Las políticas deben ser aprobadas por la dirección y deben abarcar a toda la organización, ser repetibles y recurrentes, y estar en consonancia con el entorno actual de amenazas a la ciberseguridad, los riesgos (que cambiarán con el tiempo) y los objetivos de la misión. Integrar las políticas en la cultura de la empresa para ayudar a impulsar e inspirar la capacidad de tomar decisiones informadas. Tener en cuenta las obligaciones legales, reglamentarias y contractuales.

GOBERNAR (GV): Se establecen, comunican y supervisan la estrategia, las expectativas y la política de gestión de riesgos de ciberseguridad de la organización.

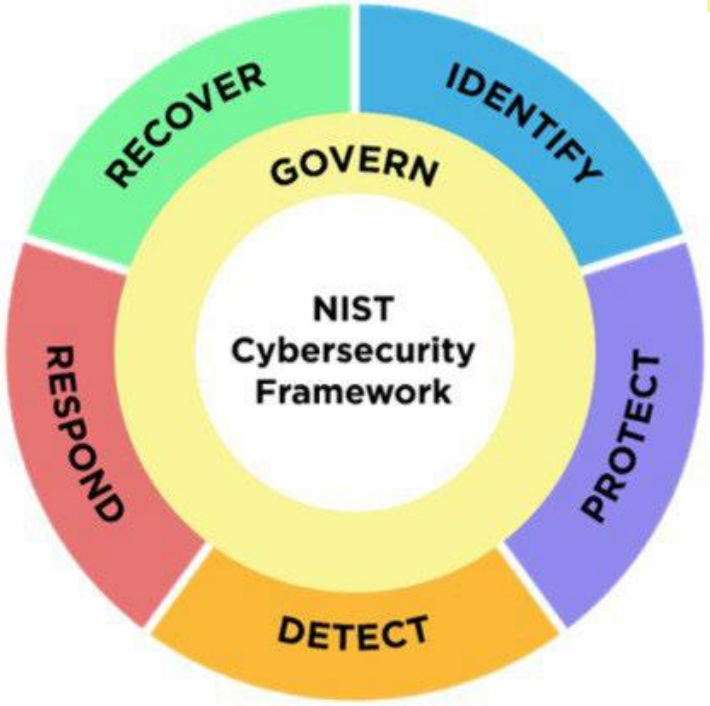


Fig. 2. CSF Functions

FUNCIÓN – GOBIERNO

Desarrollar y comunicar las prácticas de ciberseguridad de la organización. Éstas deben ser claras y comunicarse con regularidad. Deben reflejar la aplicación de la gestión de riesgos a los cambios en la misión o los requisitos empresariales, las amenazas y el panorama técnico general. Documente las prácticas y compártalas con espacio para la retroalimentación y la agilidad para cambiar de rumbo.

Establecer y supervisar la gestión de riesgos de la cadena de suministro de ciberseguridad. Establecer estrategias, políticas, funciones y responsabilidades, incluida la supervisión de proveedores, clientes y socios. Incorporar requisitos a los contratos. Implicar a socios y proveedores en la planificación, respuesta y recuperación.

Implemente una supervisión continua y puntos de control. Analice los riesgos a intervalos regulares y vigílelos continuamente (igual que haría con los riesgos financieros).

GOBERNAR (GV): Se establecen, comunican y supervisan la estrategia, las expectativas y la política de gestión de riesgos de ciberseguridad de la organización.

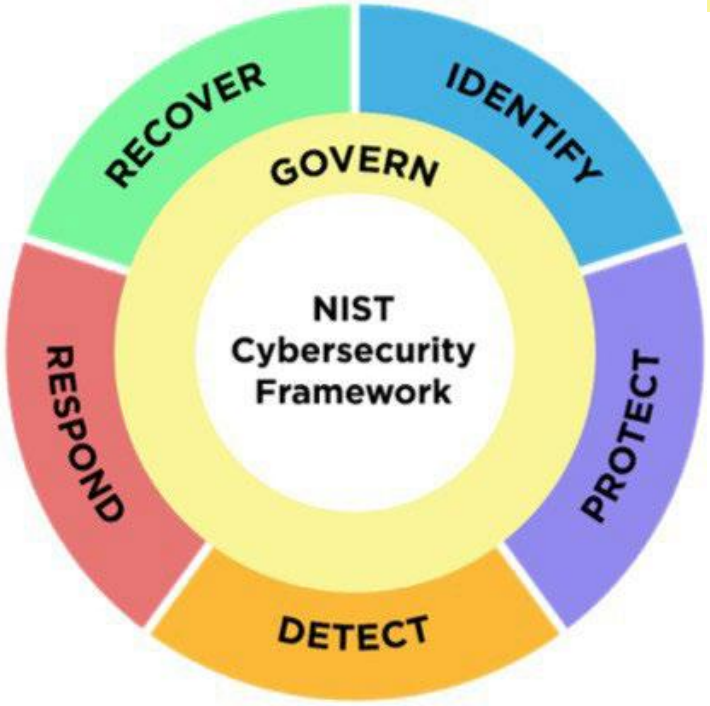


Fig. 2. CSF Functions

Apéndice A núcleo el CSF

GOBERNAR (GV): Se establecen, comunican y supervisan la estrategia, las expectativas y la política de gestión de riesgos de ciberseguridad de la organización.

Contexto organizativo (GV.OC): Se comprenden las circunstancias - misión, expectativas de las partes interesadas, dependencias y requisitos legales, reglamentarios y contractuales - que rodean las decisiones de gestión de riesgos de ciberseguridad de la organización.

- **GV.OC-01:** La misión de la organización es entendida e informa la gestión de riesgos de ciberseguridad.
- **GV.OC-02:** Se comprenden las partes interesadas internas y externas, y se comprenden y consideran sus necesidades y expectativas con respecto a la gestión de riesgos de ciberseguridad.
- **GV.OC-03:** Se comprenden y gestionan los requisitos legales, reglamentarios y contractuales relativos a la ciberseguridad, incluidas las obligaciones en materia de privacidad y libertades civiles.
- **GV.OC-04:** Se comprenden y comunican los objetivos, capacidades y servicios críticos de los que dependen las partes interesadas externas o que esperan de la organización.
- **GV.OC-05:** Se comprenden y comunican los resultados, capacidades y servicios de los que depende la organización.

Apéndice A núcleo el CSF

Estrategia de gestión de riesgos (GV.RM): Las prioridades de la organización, las limitaciones, las declaraciones de tolerancia y apetito de riesgo y los supuestos se establecen, comunican y utilizan para apoyar las decisiones de riesgo operacional.

- **GV.RM-01:** Los objetivos de gestión de riesgos son establecidos y acordados por las partes interesadas de la organización.
- **GV.RM-02:** Se establecen, comunican y mantienen declaraciones sobre el apetito de riesgo y la tolerancia al riesgo.
- **GV.RM-03:** Las actividades y resultados de la gestión de riesgos de ciberseguridad se incluyen en los procesos de gestión de riesgos de la empresa.
- **GV.RM-04:** Se establece y comunica una dirección estratégica que describa las opciones apropiadas de respuesta al riesgo.
- **GV.RM-05:** Se establecen líneas de comunicación en toda la organización para los riesgos de ciberseguridad, incluidos los riesgos de proveedores y otros terceros.
- **GV.RM-06:** Se establece y comunica un método estandarizado para calcular, documentar, categorizar y priorizar los riesgos de ciberseguridad.
- **GV.RM-07:** Se caracterizan las oportunidades estratégicas (es decir, los riesgos positivos) y se incluyen en los debates sobre riesgos de ciberseguridad de la organización.

Apéndice A núcleo el CSF

GOBERNAR (GV): Se establecen, comunican y supervisan la estrategia, las expectativas y la política de gestión de riesgos de ciberseguridad de la organización.

Funciones, responsabilidades y autoridades (GV.RR): Se establecen y comunican las funciones, responsabilidades y autoridades en materia de ciberseguridad para fomentar la rendición de cuentas, la evaluación del desempeño y la mejora continua.

- **GV.RR-01:** La dirección de la organización es responsable de los riesgos de ciberseguridad y fomenta una cultura consciente de los riesgos, ética y de mejora continua.
- **GV.RR-02:** Las funciones, responsabilidades y autoridades relacionadas con la gestión de riesgos de ciberseguridad se establecen, comunican, comprenden y aplican.
- **GV.RR-03:** Se asignan recursos adecuados y proporcionales a la estrategia, funciones, responsabilidades y políticas sobre riesgos de ciberseguridad.
- **GV.RR-04:** La ciberseguridad se incluye en las prácticas de recursos humanos.

Apéndice A núcleo el CSF

Política (GV.PO): La política de ciberseguridad de la organización se establece, comunica y Aplicada.

- **GV.PO-01**: La política de gestión de riesgos de ciberseguridad se establece en base al contexto organizacional, la estrategia de ciberseguridad y las prioridades, y es comunicada y aplicada.
- **GV.PO-02:** La política de gestión de riesgos de ciberseguridad es revisada, actualizada, comunicada y aplicada para reflejar los cambios en los requerimientos, amenazas, tecnología y misión organizacional.

Supervisión (GV.OV): Los resultados de las actividades de gestión de riesgos de ciberseguridad en toda la organización y el rendimiento se utilizan para informar, mejorar y ajustar la estrategia de gestión de riesgos.

- **GV.OV-01**: Los resultados de la estrategia de gestión de riesgos de ciberseguridad se revisan para informar y ajustar la estrategia y la dirección
- **GV.OV-02**: La estrategia de gestión de riesgos de ciberseguridad es revisada y ajustada para asegurar la cobertura de los requerimientos y riesgos organizacionales.
- **GV.OV-03:** El desempeño de la gestión de riesgos de ciberseguridad de la organización es evaluado y revisado para realizar los ajustes necesarios.

Apéndice A núcleo el CSF

Gestión de riesgos de la cadena de suministro de ciberseguridad (GV.SC): Los procesos de gestión de riesgos de la cadena de suministro cibernética son identificados, establecidos, gestionados, monitoreados y mejorados por las partes interesadas de la organización.

- **GV.SC-01:** Las partes interesadas de la organización establecen y acuerdan un programa, estrategia, objetivos, políticas y procesos de gestión de riesgos de la cadena de suministro de ciberseguridad.
- **GV.SC-02:** Se establecen, comunican y coordinan interna y externamente las funciones y responsabilidades en materia de ciberseguridad de proveedores, clientes y socios.
- **GV.SC-03:** La gestión de riesgos de la cadena de suministro de ciberseguridad está integrada en la ciberseguridad y la gestión de riesgos empresariales, la evaluación de riesgos y los procesos de mejora.
- **GV.SC-04:** Los proveedores son conocidos y priorizados por criticidad
- **GV.SC-05:** Los requisitos para hacer frente a los riesgos de ciberseguridad en las cadenas de suministro se establecen, priorizan e integran en los contratos y otros tipos de acuerdos con los proveedores y otros terceros pertinentes.

Apéndice A núcleo el CSF

- **GV.SC-06:** Se lleva a cabo la planificación y la diligencia debida para reducir los riesgos antes de entablar relaciones formales con proveedores u otros terceros.
- **GV.SC-07:** Los riesgos planteados por un proveedor, sus productos y servicios, y otros terceros son comprendidos, registrados, priorizados, evaluados, respondidos y monitoreados durante el curso de la relación.
- **GV.SC-08:** Los proveedores relevantes y otros terceros se incluyen en las actividades de planificación, respuesta y recuperación de incidentes.
- **GV.SC-09:** Las prácticas de seguridad de la cadena de suministro están integradas en los programas de ciberseguridad y de gestión de riesgos empresariales, y su desempeño es monitoreado a lo largo del ciclo de vida de los productos y servicios tecnológicos.
- **GV.SC-10:** Los planes de gestión de riesgos de la cadena de suministro de ciberseguridad incluyen disposiciones para las actividades que ocurren después de la conclusión de un acuerdo de asociación o de servicio.

FUNCIÓN – IDENTIFICAR

Identifique los procesos y activos empresariales críticos. Considere qué actividades de su organización deben seguir siendo viables. Por ejemplo, podría tratarse del mantenimiento de un sitio web para recuperar pagos, la protección segura de la información de clientes/pacientes o la garantía de que la información crítica para su organización sigue siendo accesible y precisa.

Mantenga inventarios de hardware, software, servicios y sistemas. Sepa qué ordenadores y programas utiliza su organización -incluidos los servicios prestados por los proveedores- porque suelen ser los puntos de entrada de los actores maliciosos. Este inventario puede ser tan sencillo como una hoja de cálculo.

Considere la posibilidad de incluir los dispositivos y aplicaciones propios, alquilados y personales de los empleados.

Documente los flujos de información. Considere qué tipo de información recopila y utiliza su organización (y dónde se encuentran los datos y cómo se utilizan), especialmente cuando haya contratos y socios externos implicados.

IDENTIFICAR (ID): Se conocen los riesgos actuales de ciberseguridad de la organización

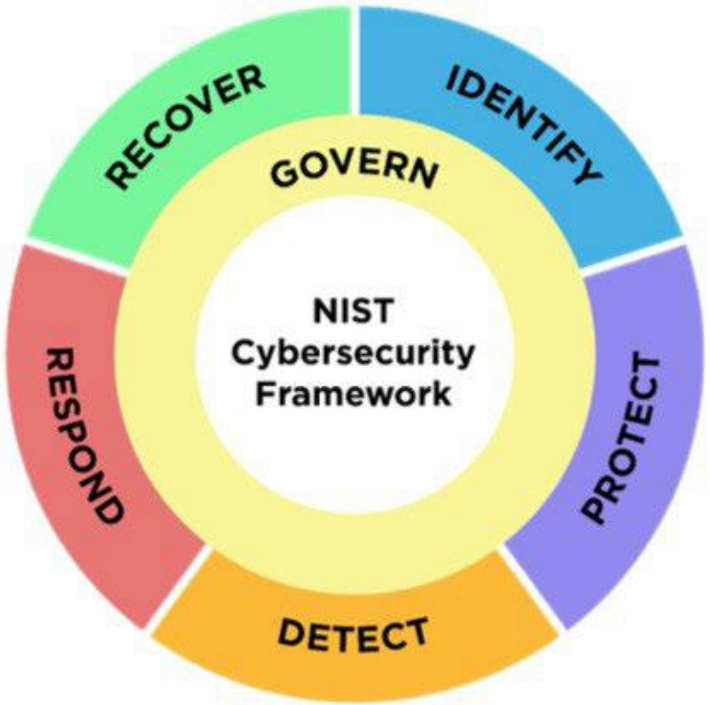


Fig. 2. CSF Functions

FUNCIÓN – IDENTIFICAR

Identifique amenazas, vulnerabilidades y riesgos para los activos. A partir del conocimiento de las amenazas internas y externas, deben identificarse, evaluarse y documentarse los riesgos. Ejemplos de formas de documentarlos son los registros de riesgos, depósitos de información sobre riesgos, incluidos los datos sobre riesgos a lo largo del tiempo. Garantizar que se identifican, priorizan y ejecutan las respuestas a los riesgos, y que se supervisan los resultados.

Las lecciones aprendidas se utilizan para identificar mejoras. Al llevar a cabo las operaciones empresariales cotidianas, es importante identificar formas de perfeccionar o mejorar el rendimiento, incluidas las oportunidades para gestionar y reducir mejor los riesgos de ciberseguridad. Esto requiere un esfuerzo decidido por parte de su organización a todos los niveles. Si se produce un incidente, evalúe lo ocurrido. Prepare un informe posterior que documente el incidente, la respuesta, las medidas de recuperación adoptadas y las lecciones aprendidas.

IDENTIFICAR (ID): Se conocen los riesgos actuales de ciberseguridad de la organización

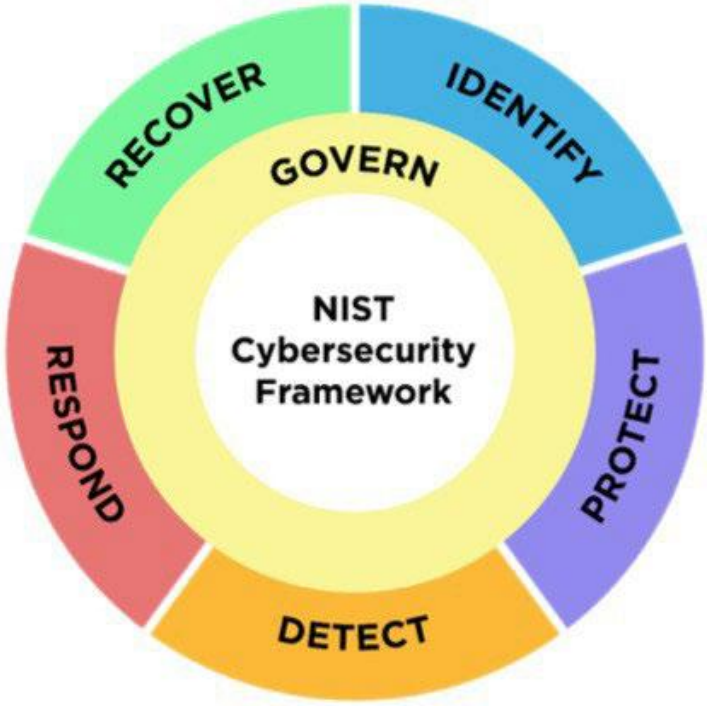


Fig. 2. CSF Functions

FUNCIÓN - IDENTIFICAR

IDENTIFICAR (ID): Se conocen los riesgos actuales de ciberseguridad de la organización

Gestión de activos (ID.AM): Los activos (por ejemplo, datos, hardware, software, sistemas, instalaciones, servicios, personas) que permiten a la organización alcanzar sus objetivos de negocio se identifican y gestionan de acuerdo con su importancia relativa para los objetivos de la organización y la estrategia de riesgos de la organización.

- **ID.AM-01:** Se mantienen inventarios del hardware gestionado por la organización.
- **ID.AM-02:** Se mantienen inventarios de software, servicios y sistemas gestionados por la organización gestionados por la organización.
- **ID.AM-03:** Se mantienen representaciones de la comunicación de red autorizada de la organización y de los flujos de datos de red internos y externos.
- **ID.AM-04:** Se mantienen inventarios de los servicios prestados por los proveedores.
- **ID.AM-05:** Los activos se priorizan en función de su clasificación, criticidad, recursos e impacto en la misión.
- **ID.AM-07:** Se mantienen inventarios de datos y los metadatos correspondientes para los tipos de datos designados
- **ID.AM-08:** Los sistemas, el hardware, el software, los servicios y los datos se gestionan a lo largo de sus ciclos de vida.

FUNCIÓN - IDENTIFICAR

Mejora (ID.IM): Se identifican mejoras en los procesos, procedimientos y actividades procesos, procedimientos y actividades en todas las funciones de la CSF.

- **ID.IM-01:** Las mejoras se identifican a partir de las evaluaciones.
- **ID.IM-02:** Las mejoras se identifican a partir de pruebas y ejercicios de seguridad, incluyendo aquellos realizados en coordinación con proveedores y terceras partes relevantes.
- **ID.IM-03:** Las mejoras se identifican a partir de la ejecución de procesos, procedimientos y actividades operativas
- **ID.IM-04:** Se establecen, comunican, mantienen y mejoran los planes de respuesta a incidentes y otros planes de ciberseguridad que afectan a las operaciones

FUNCIÓN – PROTEGER

Gestione el acceso. Cree cuentas únicas para los empleados y asegúrese de que los usuarios sólo tienen acceso a los recursos necesarios. Autentique a los usuarios antes de concederles acceso a la información, los ordenadores y las aplicaciones. Gestione y controle el acceso físico a las instalaciones/dispositivos.

Formar a los usuarios. Forme periódicamente a los empleados para asegurarse de que conocen las políticas y procedimientos de ciberseguridad y de que tienen los conocimientos y habilidades necesarios para realizar tareas generales y específicas; explíqueles cómo reconocer ataques comunes y cómo informar de actividades sospechosas. Determinadas funciones pueden requerir formación adicional.

Proteja y controle sus dispositivos. Considere el uso de productos de seguridad para puntos finales. Aplique configuraciones uniformes a los dispositivos y controle los cambios en las configuraciones de los dispositivos. Desactive los servicios o funciones que no apoyen las funciones de la misión. Configure los sistemas y servicios para que generen registros. Asegúrese de que los dispositivos se eliminan de forma segura.

PROTEGER (PR): Se utilizan salvaguardias para gestionar los riesgos de ciberseguridad de la organización.

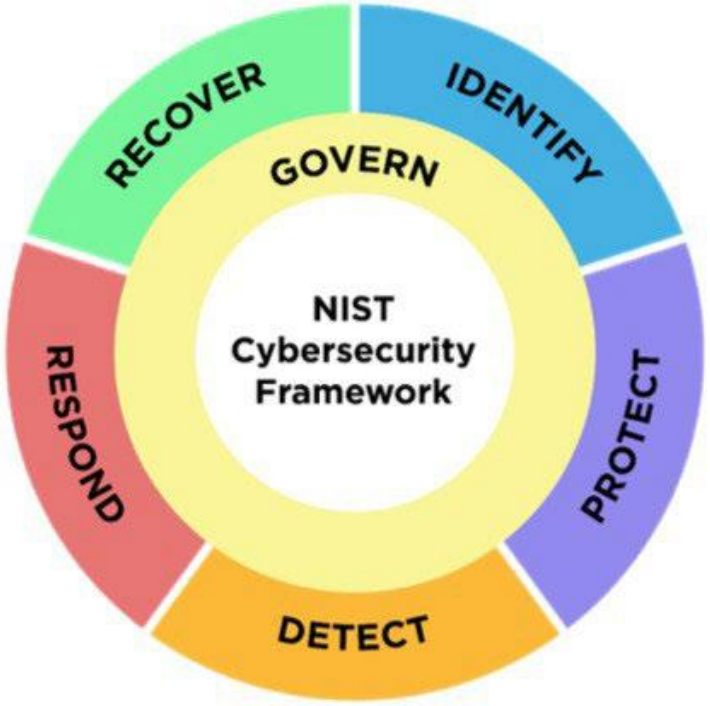


Fig. 2. CSF Functions

FUNCIÓN – PROTEGER

Proteger los datos confidenciales. Asegúrese de que los datos confidenciales almacenados o transmitidos estén protegidos mediante cifrado. Considere la posibilidad de utilizar la comprobación de integridad para que sólo se realicen cambios aprobados en los datos. Elimine y/o destruya los datos de forma segura cuando ya no sean necesarios o requeridos.

Gestionar y mantener el software. Actualice periódicamente los sistemas operativos y las aplicaciones; active las actualizaciones automáticas. Sustituya el software obsoleto por versiones compatibles. Considere el uso de herramientas de software para escanear los dispositivos en busca de vulnerabilidades adicionales y remediarlas.

Realice copias de seguridad periódicas. Realice copias de seguridad de los datos en los plazos acordados o utilice las funciones de copia de seguridad integradas; las soluciones de software y en la nube pueden automatizar este proceso. Mantenga fuera de línea al menos un conjunto de datos de los que se realizan copias de seguridad con frecuencia para protegerlo contra el ransomware. Realice pruebas para garantizar que los datos de las copias de seguridad pueden restaurarse correctamente en los sistemas.

PROTEGER (PR): Se utilizan salvaguardias para gestionar los riesgos de ciberseguridad de la organización.

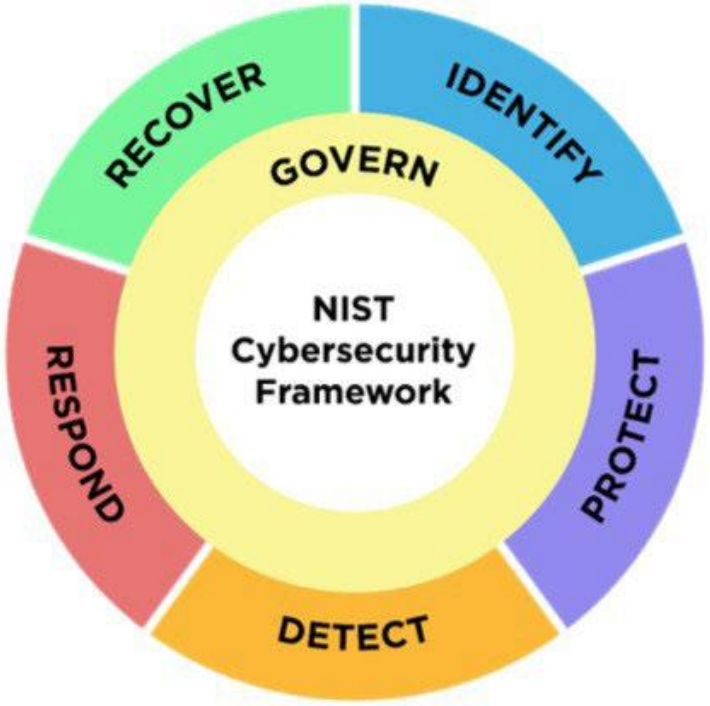


Fig. 2. CSF Functions

FUNCIÓN – PROTEGER

PROTEGER (PR): Se utilizan salvaguardas para gestionar los riesgos de ciberseguridad de la organización

Gestión de identidades, autenticación y control de acceso (PR.AA): El acceso a los activos físicos y lógicos se limita a los usuarios, servicios y hardware autorizados y se gestiona de forma proporcional al riesgo evaluado de acceso no autorizado.

- **PR.AA-01:** La organización gestiona las identidades y credenciales de los usuarios, servicios y hardware autorizados.
- **PR.AA-02:** Las identidades son probadas y vinculadas a credenciales basadas en el contexto de las interacciones.
- **PR.AA-03:** Los usuarios, servicios y hardware son autenticados.
- **PR.AA-04:** Las afirmaciones de identidad se protegen, transmiten y verifican.
- **PR.AA-05:** Los permisos de acceso, los derechos y las autorizaciones se definen en una política, se gestionan, se aplican y se revisan, e incorporan los principios de mínimo privilegio y separación de funciones.
- **PR.AA-06:** El acceso físico a los activos se gestiona, supervisa y aplica de forma proporcional al riesgo.

FUNCIÓN – PROTEGER

Concienciación y formación (PR.AT): Se proporciona al personal de la organización concienciación y formación en ciberseguridad para que puedan realizar sus tareas relacionadas con la ciberseguridad.

- **PR.AT-01:** Se sensibiliza y forma al personal para que posea los conocimientos y habilidades necesarios para realizar tareas generales teniendo en cuenta los riesgos de ciberseguridad.
- **PR.AT-02:** Se sensibiliza y forma a las personas que desempeñan funciones especializadas para que posean los conocimientos y habilidades necesarios para realizar las tareas pertinentes teniendo en cuenta los riesgos de ciberseguridad.

Seguridad de los datos (PR.DS): Los datos se gestionan de acuerdo con la estrategia de riesgos de la organización para proteger la confidencialidad, integridad y disponibilidad de la información.

- **PR.DS-01:** La confidencialidad, integridad y disponibilidad de los datos en reposo están protegidas.
- **PR.DS-02:** se protege la confidencialidad, integridad y disponibilidad de los datos en tránsito
- **PR.DS-10:** se protege la confidencialidad, integridad y disponibilidad de los datos en uso.
- **PR.DS-11:** se crean, protegen, mantienen y comprueban copias de seguridad de los datos.

FUNCIÓN – PROTEGER

Seguridad de la plataforma (PR.PS): El hardware, el software (por ejemplo, firmware, sistemas operativos, aplicaciones) y los servicios de las plataformas físicas y virtuales se gestionan de acuerdo con la estrategia de riesgos de la organización para proteger su confidencialidad, integridad y disponibilidad.

- **PR.PS-01:** Se establecen y aplican prácticas de gestión de la configuración.
- **PR.PS-02:** El software es mantenido, reemplazado y eliminado de manera proporcional al riesgo.
- **PR.PS-03:** El hardware se mantiene, sustituye y elimina en función delriesgo.
- **PR.PS-04:** Los registros se generan y están disponibles para un control continuo.
- **PR.PS-05:** Se previene la instalación y ejecución de software no autorizado.
- **PR.PS-06:** Las prácticas de desarrollo de software seguro están integradas, y su desempeño es monitoreado a lo largo del ciclo de vida de desarrollo del software.

FUNCIÓN – PROTEGER

Resistencia de la infraestructura tecnológica (PR.IR): Las arquitecturas de seguridad se gestionan con la estrategia de riesgos de la organización para proteger la confidencialidad, integridad y disponibilidad de los activos y la resiliencia de la organización.

- **PR.IR-01:** Las redes y los entornos están protegidos contra el acceso lógico y el uso no autorizados.
- **PR.IR-02:** Los activos tecnológicos de la organización están protegidos de amenazas ambientales.
- **PR.IR-03:** Se implementan mecanismos para alcanzar los requerimientos de resiliencia en situaciones normales y adversas.
- **PR.IR-04:** Se mantiene una capacidad de recursos adecuada para asegurar la disponibilidad.

FUNCIÓN – DETECTAR

Supervisar continuamente las redes, sistemas e instalaciones para detectar eventos potencialmente adversos. Desarrollar y probar procesos y procedimientos para detectar indicadores de un incidente de ciberseguridad en la red y en el entorno físico. Recopilar información de registro de múltiples fuentes organizativas para ayudar a detectar actividades no autorizadas.

Determinar y analizar el impacto estimado y el alcance de los eventos adversos. Si se detecta un evento de ciberseguridad, su organización debe trabajar rápida y minuciosamente para comprender el impacto del incidente. Comprender los detalles relativos a cualquier incidente de ciberseguridad ayudará a informar la respuesta.

Proporcione información sobre eventos adversos al personal y las herramientas autorizadas. Cuando se detecten eventos adversos, proporcione información sobre el evento internamente al personal autorizado para garantizar que se toman las medidas adecuadas de respuesta al incidente.

DETECTAR (DE): Se encuentran y analizan posibles ataques y compromisos de ciberseguridad.

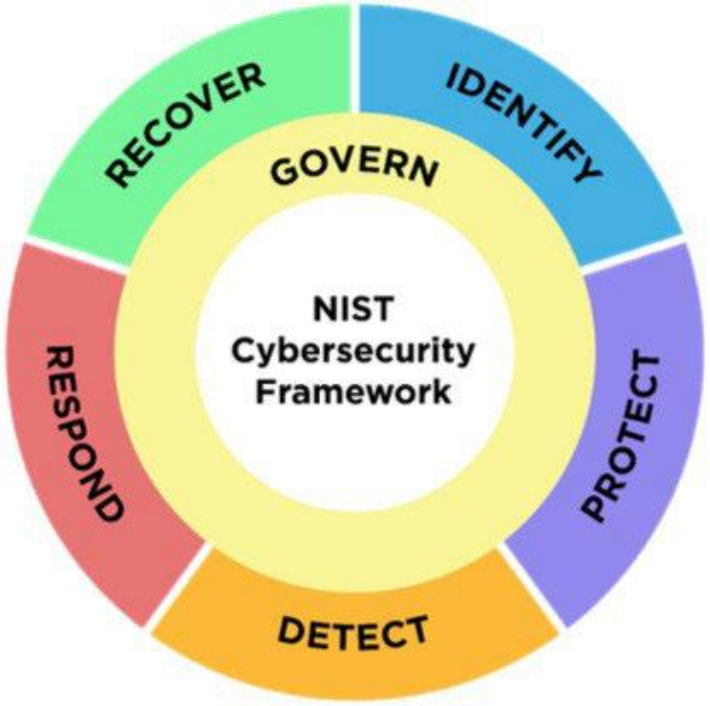


Fig. 2. CSF Functions

FUNCIÓN – DETECTAR

DETECTAR (DE): Se encuentran y analizan posibles ataques y compromisos de ciberseguridad.

Monitorización continua (DE.CM): Los activos se monitorizan para encontrar anomalías, indicadores de compromiso y otros eventos potencialmente adversos.

- **DE.CM-01:** Las redes y los servicios de red son monitorizados para encontrar eventos potencialmente adversos.
- **DE.CM-02:** El entorno físico es monitorizado para encontrar eventos potencialmente adversos.
- **DE.CM-03:** La actividad del personal y el uso de la tecnología son monitorizados para encontrar eventos potencialmente adversos.
- **DE.CM-06:** Las actividades y servicios de proveedores de servicios externos son monitorizados para encontrar eventos potencialmente adversos.
- **DE.CM-09:** El hardware y software informático, los entornos de ejecución y sus datos son monitorizados para encontrar eventos potencialmente adversos.

FUNCIÓN - DETECTAR

Análisis de eventos adversos (DE.AE): Se analizan anomalías, indicadores de compromiso y otros eventos potencialmente adversos para caracterizar los eventos y detectar incidentes de ciberseguridad.

- **DE.AE-02:** Los eventos potencialmente adversos se analizan para comprender mejor las actividades asociadas.
- **DE.AE-03:** La información se relaciona a partir de múltiples fuentes
- **DE.AE-04:** Se comprende el impacto estimado y el alcance de los eventos adversos.
- **DE.AE-06:** La información sobre eventos adversos se proporciona al personal y a las herramientas autorizadas.
- **DE.AE-07:** La inteligencia sobre ciber amenazas y otra información contextual se integran en el análisis.
- **DE.AE-08:** Los incidentes se declaran cuando los eventos adversos cumplen los criterios de incidente definidos

FUNCIÓN – RESPONDER

Ejecutar un plan de respuesta a incidentes una vez declarado un incidente, en coordinación con los terceros pertinentes. Para ejecutar correctamente un plan de respuesta a incidentes, asegúrese de que todo el mundo conoce sus responsabilidades; esto incluye comprender cualquier requisito (por ejemplo, reglamentario, de notificación legal y de intercambio de información).

Clasificar y priorizar los incidentes y escalarlos o elevarlos según sea necesario. Analice lo que ha estado ocurriendo, determine la causa raíz del incidente y priorice los incidentes que requieren atención prioritaria por parte de su organización. Comunique esta priorización a su equipo y asegúrese de que todos entienden a quién debe comunicarse la información relativa a un incidente priorizado cuando se produzca.

RESPONDER (RS): Se toman medidas en relación con un incidente de ciberseguridad detectado.

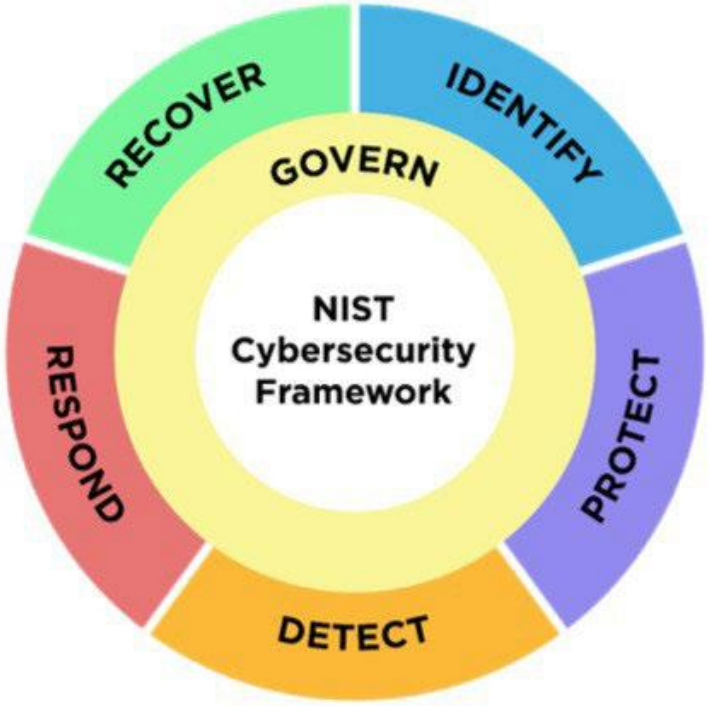


Fig. 2. CSF Functions

FUNCIÓN – RESPONDER

Recopile los datos del incidente y preserve su integridad y procedencia. Recopilar información de forma segura ayudará a su organización a responder a un incidente. Asegúrese de que los datos siguen siendo seguros después del incidente para mantener la reputación de su organización y la confianza de las partes interesadas. Almacenar esta información de forma segura también puede ayudar a actualizar y elaborar futuros planes de respuesta para que sean aún más eficaces.

Notifique cualquier incidente a las partes interesadas internas y externas y comparta con ellas la información sobre el incidente, siguiendo las políticas establecidas por su organización. Comparta la información de forma segura y coherente con los planes de respuesta y los acuerdos de intercambio de información. Notifique los incidentes a socios comerciales y clientes de acuerdo con los requisitos contractuales.

Contener y erradicar los incidentes. La ejecución de un plan de respuesta desarrollado y probado ayudará a su organización a contener los efectos de un incidente y a erradicarlo. Una coordinación y comunicación significativas con las partes interesadas pueden dar lugar a una respuesta más eficaz y a la mitigación del incidente.

RESPONDER (RS): Se toman medidas en relación con un incidente de ciberseguridad detectado.

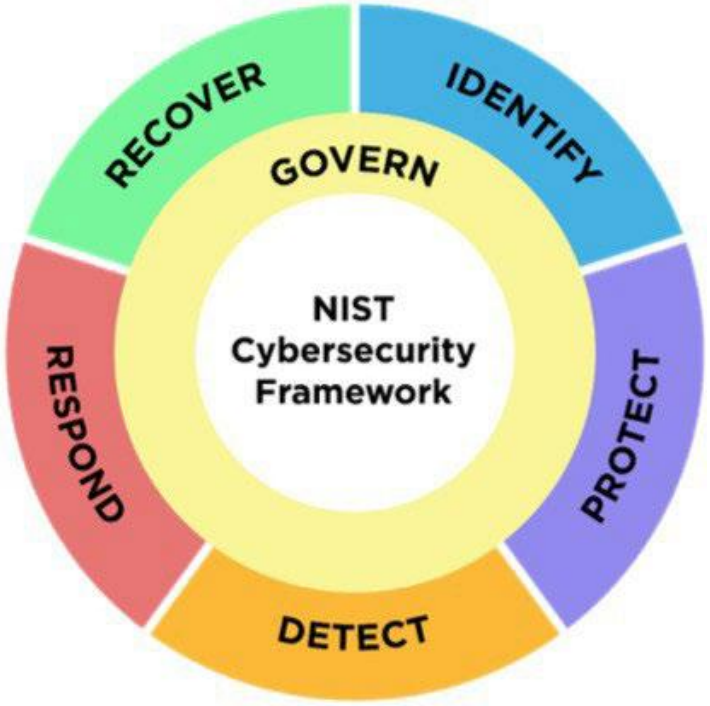


Fig. 2. CSF Functions

FUNCIÓN – RESPONDER

RESPONDER (RS): Se toman medidas en relación con un incidente de ciberseguridad detectado

Gestión de incidentes (RS.MA): Las respuestas a los incidentes de ciberseguridad detectados se gestionan

- **RS.MA-01:** El plan de respuesta a incidentes se ejecuta en coordinación con los terceros pertinentes una vez que se declara un incidente.
- **RS.MA-02:** Los informes de incidentes se clasifican y validan.
- **RS.MA-03:** Los incidentes se clasifican y priorizan.
- **RS.MA-04:** Los incidentes se intensifican o elevan según sea necesario.
- **RS.MA-05:** Se aplican los criterios para iniciar la recuperación de incidentes.

FUNCIÓN – RESPONDER

Análisis de incidentes (RS.AN): Las investigaciones se llevan a cabo para garantizar una respuesta eficaz y apoyar las actividades forenses y de recuperación.

- **RS.AN-03:** El análisis se realiza para establecer lo que ha ocurrido durante un incidente y la causa raíz de este.
- **RS.AN-06:** Se registran las acciones realizadas durante una investigación y se preservan la integridad y la procedencia de los registros.
- **RS.AN-07:** se recopilan los datos y metadatos del incidente y se preservan su integridad y procedencia.
- **RS.AN-08:** Se estima y valida la magnitud de un incidente.

Notificación y comunicación de la respuesta a incidentes (RS.CO): Las actividades de respuesta se coordinan con las partes interesadas internas y externas, según lo exijan las leyes, reglamentos o políticas.

- **RS.CO-02:** Se notifican los incidentes a las partes interesadas internas y externas.
- **RS.CO-03:** La información se comparte con las partes interesadas internas y externas designadas.

Mitigación de incidentes (RS.MI): Se realizan actividades para evitar la expansión de un incidente y mitigar sus efectos

- **RS.MI-01:** Los incidentes se contienen.
- **RS.MI-02:** Los incidentes se erradican.

FUNCIÓN – RECUPERAR

Comprenda las funciones y responsabilidades. Comprenda quién, dentro y fuera de su empresa, tiene responsabilidades de recuperación. Sepa quién tiene acceso y autoridad para tomar decisiones para llevar
a cabo sus esfuerzos de respuesta en nombre de la empresa.

Ejecute su plan de recuperación. Garantice la disponibilidad operativa de los sistemas y servicios afectados, y priorice y ejecute las tareas de recuperación.

Compruebe su trabajo. Es importante garantizar la integridad de las copias de seguridad y otros activos de recuperación antes de utilizarlos para reanudar las operaciones normales de la empresa.

Comuníquese con las partes interesadas internas y externas. Tenga muy en cuenta qué, cómo y cuándo se compartirá la información con las distintas partes interesadas, de modo que todas ellas reciban la Información que necesitan, pero no se comparta información inapropiada. Comunique a su personal las lecciones aprendidas y las revisiones de procesos, procedimientos y tecnologías (siguiendo las políticas ya establecidas por la organización). Es un buen momento para formar, o reciclar, al personal en las mejores prácticas de ciberseguridad.

RECUPERAR (RC): Se restablecen los activos y operaciones afectados por un incidente de ciberseguridad.

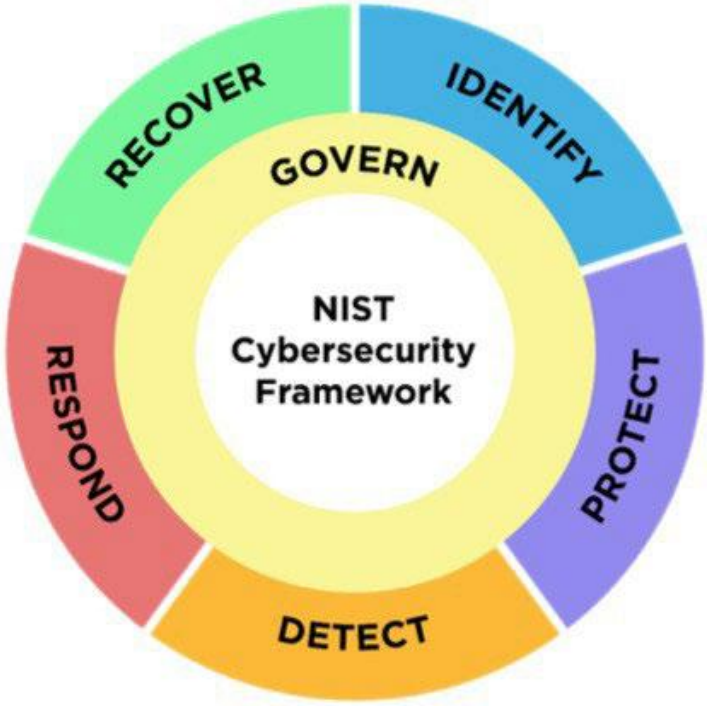


Fig. 2. CSF Functions

FUNCIÓN – RECUPERAR

RECUPERACIÓN (RC): Se restablecen los activos y operaciones afectados por un incidente de ciberseguridad

Ejecución del Plan de Recuperación de Incidentes (RC.RP): Se realizan actividades de restauración para garantizar disponibilidad operativa de los sistemas y servicios afectados por incidentes de ciberseguridad.

- **RC.RP-01:** La parte de recuperación del plan de respuesta a incidentes se ejecuta una vez iniciada desde el proceso de respuesta a incidentes.
- **RC.RP-02:** Las acciones de recuperación son seleccionadas, delimitadas, priorizadas y ejecutadas.
- **RC.RP-03:** Se verifica la integridad de las copias de seguridad y otros activos de restauración antes de utilizarlos para la restauración para la restauración.
- **RC.RP-04:** Se tienen en cuenta las funciones críticas de la misión y la gestión de riesgos de ciberseguridad para establecer normas operativas posteriores a los incidentes.
- **RC.RP-05:** Se verifica la integridad de los activos restaurados, se restablecen los sistemas y servicios y se confirma el estado normal de funcionamiento.
- **RC.RP-06:** Se declara el fin de la recuperación del incidente en base a criterios, y se completa la documentación relacionada con el incidente

FUNCIÓN – RECUPERAR

Comunicación de recuperación de incidentes (RC.CO): Las actividades de restauración se coordinan con las partes internas y externas.

- **RC.CO-03:** Las actividades de recuperación y los avances en el restablecimiento de las capacidades operativas se comunican a las partes interesadas internas y externas designadas.
- **RC.CO-04:** Las actualizaciones públicas sobre la recuperación del incidente son compartidas usando métodos y mensajes aprobados.

Apéndice B Niveles del CSF

NIVELES DEL CSF

Niveles el Cibersecurity Framework

Los niveles caracterizan el rigor de las prácticas de gobernanza de los riesgos de ciberseguridad de una organización (GOVERN) y las prácticas de gestión de los riesgos de ciberseguridad (IDENTIFY, PROTECT, DETECT, RESPOND y RECOVER).

Nivel	Gobierno de los riesgos de ciberseguridad	Gestión de riesgos de ciberseguridad
Nivel 1: Parcial	La aplicación de la estrategia de riesgos de ciberseguridad de la organización se gestiona de manera ad hoc. La priorización es ad hoc y no se basa formalmente en objetivos o en el entorno de amenazas.	Existe una conciencia limitada de los riesgos de ciberseguridad a nivel organizativo. La organización aplica la gestión de riesgos de ciberseguridad de forma irregular, caso por caso. Es posible que la organización no disponga de procesos que permitan compartir información sobre ciberseguridad dentro de la organización. La organización desconoce en general los riesgos de ciberseguridad asociados a sus proveedores y a los productos y servicios que adquiere y utiliza.
Nivel 2: Riesgo informado	Las prácticas de gestión de riesgos son aprobadas por la dirección, pero no pueden establecerse como política de toda la organización. La priorización de las actividades de ciberseguridad y las necesidades de protección se basa directamente en los objetivos de riesgo de la organización, el entorno de amenazas o los requisitos de negocio/misión.	Existe una concienciación de los riesgos de ciberseguridad a nivel organizativo, pero no se ha establecido un enfoque a nivel de toda la organización para gestionar los riesgos de ciberseguridad. La consideración de la ciberseguridad en los objetivos y programas organizativos puede darse en algunos niveles de la organización, pero no en todos. La evaluación del riesgo cibernético de los activos organizativos y externos se produce, pero no suele ser repetible o recurrente. La información sobre ciberseguridad se comparte dentro de la organización de manera informal. La organización es consciente de los riesgos de ciberseguridad asociados a sus proveedores y a los productos y servicios que adquiere y utiliza, pero no actúa de manera coherente o formal en respuesta a dichos riesgos.

NIVELES DEL CSF

Niveles el Cibersecurity Framework

Nivel	Gobierno de los riesgos de ciberseguridad	Gestión de riesgos de ciberseguridad
Nivel 3: Repetible	Las prácticas de gestión de riesgos de la organización se aprueban formalmente y se expresan como política. Las políticas, procesos y procedimientos basados en el riesgo se definen, implementan y revisan según lo previsto. Las prácticas de ciberseguridad de la organización se actualizan periódicamente en función de la aplicación de los procesos de gestión de riesgos a los cambios en los requisitos de negocio/misión, las amenazas y el panorama tecnológico.	Existe un enfoque a nivel de toda la organización para gestionar los riesgos de ciberseguridad. La información sobre ciberseguridad se comparte de forma rutinaria en toda la organización. Existen métodos coherentes para responder eficazmente a los cambios en los riesgos. El personal posee los conocimientos y habilidades necesarios para desempeñar las funciones y responsabilidades que le han sido asignadas. La organización supervisa de forma coherente y precisa los riesgos de ciberseguridad de los activos. Los altos ejecutivos de ciberseguridad y de no ciberseguridad se comunican regularmente en relación con los riesgos de ciberseguridad. La estrategia de riesgos de la organización se basa en los riesgos de ciberseguridad asociados a sus proveedores y a los productos y servicios que adquiere y utiliza. El personal actúa formalmente sobre esos riesgos a través de mecanismos como acuerdos escritos para comunicar los requisitos básicos, estructuras de gobernanza (por ejemplo, consejos de riesgos) y aplicación y supervisión de políticas. Estas acciones se aplican de forma coherente y según lo previsto, y se supervisan y revisan continuamente.

NIVELES DEL CSF

Niveles el Cibersecurity Framework

Nivel	Gobierno de los riesgos de ciberseguridad	Gestión de riesgos de ciberseguridad
Nivel 4: Adaptativo	Existe un enfoque a nivel de toda la organización para gestionar los riesgos de ciberseguridad que utiliza políticas, procesos y procedimientos informados por el riesgo para hacer frente a posibles eventos de ciberseguridad. La relación entre los riesgos de ciberseguridad y los objetivos de la organización se entiende claramente y se tiene en cuenta a la hora de tomar decisiones. Los ejecutivos supervisan los riesgos de ciberseguridad en el mismo contexto que los riesgos financieros y otros riesgos organizativos. El presupuesto de la organización se basa en la comprensión del entorno de riesgo actual y previsto y en la tolerancia al riesgo. Las unidades de negocio implementan la visión ejecutiva y analizan los riesgos a nivel de sistema en el contexto de las tolerancias de riesgo de la organización. La gestión de riesgos de ciberseguridad forma parte de la cultura organizativa. Evoluciona a partir de la conciencia de las actividades previas y de la conciencia continua de las actividades en los sistemas y redes de la organización. La organización puede tener en cuenta de forma rápida y eficaz los cambios en los objetivos de negocio/misión en la forma de enfocar y comunicar el riesgo.	La organización adapta sus prácticas de ciberseguridad basándose en actividades de ciberseguridad anteriores y actuales, incluidas las lecciones aprendidas y los indicadores predictivos. A través de un proceso de mejora continua que incorpora tecnologías y prácticas avanzadas de ciberseguridad, la organización se adapta activamente a un panorama tecnológico cambiante y responde de manera oportuna y eficaz a las amenazas sofisticadas en evolución. La organización utiliza información en tiempo real o casi real para comprender los riesgos de ciberseguridad asociados a sus proveedores y a los productos y servicios que adquiere y utiliza, y actuar en consecuencia. La información sobre ciberseguridad se comparte constantemente en toda la organización y con terceros autorizados.

COMPARTE Y VERIFICA TUS LOGROS DE APRENDIZAJE FÁCILMENTE

#LCSPC #certiprof

certiprof®

¡Síguenos, ponte en contacto!

www.certiprof.com