Forcepoint

Resumen de la solución

Las soluciones de Forcepoint cumplen los estándares NIST 2.0

Reto

- **Cambio de riesgos y regulaciones:** las organizaciones tienen problemas para gestionar los crecientes riesgos cibernéticos y los cambios en los requisitos normativos.
- **Políticas de seguridad incoherentes:** la fragmentación de los controles de seguridad en los canales de acceso crea brechas de cumplimiento.
- **Visibilidad y control limitados:** la falta de gestión y de alertas centralizadas dificulta la detección de riesgos de seguridad y de violaciones de políticas.

Solución

- **Seguridad Zero Trust:** supervisión continua que protege los datos en todos los dispositivos finales, la red, la nube, la web y el correo electrónico.
- **Clasificación basada en IA:** el motor inteligente de clasificación de datos de aprendizaje continuo mejora la precisión para que las políticas se apliquen de forma eficiente.
- **Implementación flexible:** opciones en la nube, en las instalaciones e híbridas que se adaptan a las necesidades empresariales.

Resultado

- **Simplificación del cumplimiento:** la protección centralizada y adaptable reduce los riesgos de pérdida de datos antes de que se produzcan infracciones de cumplimiento.
- **Menos carga operativa:** la gestión unificada y la implementación automatizada minimizan el esfuerzo manual necesario.
- **Ayuda a la empresa a crecer:** colaboración segura que ayuda a la innovación empresarial.

El Marco de Ciberseguridad del Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés) es una referencia clave para muchas organizaciones que quieren reforzar su seguridad en muchas áreas diferentes para proteger sus activos y datos críticos y, al mismo tiempo, mejorar la gestión y respuesta a los riesgos y las amenazas.

Tras la introducción del NIST 2.0 CSF (Cybersecurity Framework) en febrero de 2024, la nueva directriz ayuda a las organizaciones a mejorar su estrategia de ciberseguridad con un enfoque más sencillo.

Forcepoint reconoce el importante papel que desempeña NIST como guía para que las organizaciones adopten mejores prácticas de seguridad. Nos comprometemos a apoyar estos esfuerzos con soluciones que ayudan a identificar, clasificar y proteger los datos confidenciales mientras detectan y responden a posibles incidentes de exfiltración. Mediante la implementación de los principios del NIST, Forcepoint permite a las organizaciones cumplir con los estándares de cumplimiento, mejorar la protección de datos y defenderse contra los riesgos en el actual entorno cada vez más digital.

¿Qué es el NIST?

El Instituto Nacional de Estándares y Tecnología (National Institute of Standards and Technology) es una agencia que pertenece al Departamento de Comercio de los Estados Unidos y que orienta sobre cumplimiento, privacidad y seguridad. Dentro del ámbito de la ciberseguridad, el Marco de Ciberseguridad del NIST (NIST CSF) proporciona información sobre funciones esenciales para que las organizaciones elaboraren estrategias y creen un programa de ciberseguridad eficiente. El marco define las funciones Identificar, Proteger, Detectar, Responder y Recuperar, además de la función global Gobernar, que permite a la empresa determinar qué decisiones encajan mejor en su estrategia. Al tratarse de un marco voluntario, NIST CSF está diseñado para servir de guía de alto nivel, mientras que otras normas como NIST SP 800-53, 800-221, 800-171, entre otras, proporcionan directrices específicas.

Proteger los datos contra amenazas emergentes

El Marco de Ciberseguridad del NIST permite a las organizaciones tener una estrategia de ciberseguridad flexible. El CSF describe a alto nivel los resultados deseados de los diferentes controles de seguridad y, al mismo tiempo, proporciona las herramientas y los recursos necesarios para crear un esquema más detallado de procesos, personas y tecnología.

Debido a una adopción cada vez más generalizada de tecnologías nuevas, como la IA generativa, muchas organizaciones se enfrentan al desafío de proteger sus datos confidenciales cuando las usan. El uso indebido de estas herramientas, de forma intencionada o no, puede acarrear graves consecuencias para las organizaciones. Es posible que estas herramientas filtren información confidencial o sensible, o que el entrenamiento de un modelo de IA se vea comprometido por contenido malicioso. Forcepoint se dedica a ayudar a que las organizaciones obtengan visibilidad de sus datos, los protejan y prevengan su uso indebido.

El CSF continúa proporcionando orientaciones y mejores prácticas para que las organizaciones construyan, implementen y mantengan sus programas de ciberseguridad. Con la nueva tecnología, las organizaciones tendrán que pensar en cómo pueden utilizar estas herramientas para poder comunicar, medir y supervisar los riesgos.

Protección con Zero Trust

Zero Trust es la práctica y el reconocimiento de que cada solicitud puede ser una amenaza potencial. Las aplicaciones, los sistemas y las personas no son fiables, salvo que puedan autenticarse, tanto si están dentro como fuera de la red.

El marco del NIST 2.0 ha adoptado los principios de la arquitectura Zero Trust, en la que las funciones esenciales se centran en la gestión de identidades y accesos y en la gestión de accesos de usuarios con privilegios. Estas directrices y arquitectura ayudan a las organizaciones a mitigar sus riesgos mientras protegen sus datos.

Forcepoint ofrece soluciones de seguridad centradas en los datos y fundamentadas en el modelo Zero Trust. Esto permite a las organizaciones mitigar su riesgo evitando la exfiltración de datos confidenciales, lo que les permite asegurar el cumplimiento con independencia de dónde se encuentren sus empleados o sus datos.

Adaptarse a los cambiantes riesgos de seguridad y requisitos de cumplimiento

El Marco de Ciberseguridad (CSF) 2.0 del NIST proporciona a las organizaciones un enfoque flexible y de alto nivel para la gestión de los riesgos de ciberseguridad. Aunque, implementar eficazmente sus funciones básicas y priorizar los controles sigue siendo un desafío. Las organizaciones deben determinar qué medidas de seguridad encajan mejor con las necesidades de su empresa y se pueden adaptar a largo plazo.

El carácter voluntario del NIST CSF puede hacer que algunas organizaciones elijan adoptar un enfoque de cumplir tareas, en lugar de crear una estrategia de seguridad dinámica y resistente. Para maximizar su eficacia, las empresas deben evaluar continuamente los riesgos, perfeccionar las políticas de seguridad y alinear los recursos para responder a amenazas que cambian constantemente.

Principales retos de cumplimiento a los que se enfrentan las organizaciones:

- → **Anticiparse a amenazas y regulaciones cambiantes:** debido a unos riesgos cibernéticos cada vez más sofisticados y a requisitos normativos cambiantes, las empresas tienen dificultades para mantenerse actualizadas.
- → **Implementación incoherente de políticas:** muchas organizaciones carecen de una estrategia de seguridad unificada para los dispositivos finales, las aplicaciones SaaS, el tráfico web y el correo electrónico, lo que genera brechas de seguridad y riesgos de cumplimiento.
- → **Brechas en visibilidad y control:** identificar brechas de seguridad, violaciones de políticas y amenazas internas es mucho más difícil sin una gestión centralizada de la seguridad de los datos y sin una implementación en tiempo real.

Para adherirse con éxito al NIST 2.0 y aumentar la resiliencia de la seguridad, las organizaciones tienen que adoptar un enfoque proactivo basado en el riesgo que garantice la implementación unificada de políticas, la detección de amenazas en tiempo real y la supervisión continua de todos los entornos digitales.

Un enfoque unificado y adaptable para la seguridad de los datos

Las organizaciones que adoptan el NIST CSF 2.0 necesitan un enfoque estructurado para la gestión de riesgos, la implementación de políticas y la protección de datos que se alinee con las funciones esenciales del marco. Forcepoint proporciona soluciones diseñadas para que las organizaciones cumplan estos requisitos y, además, mejoran las operaciones de seguridad, reducen la complejidad del cumplimiento y abordan los riesgos de seguridad antes de que se conviertan en violaciones del cumplimiento.

Marco de seguridad de Zero Trust

La arquitectura de seguridad de datos de Forcepoint se basa en los principios de Zero Trust, lo que garantiza que el uso de datos se supervise y verifique constantemente, que se apliquen políticas de privilegio mínimo y que los riesgos potenciales, tanto externos como internos, se mitiguen en tiempo real. Este enfoque se alinea con las recomendaciones del NIST para la gestión proactiva de riesgos y el control de acceso.

Gestión unificada de políticas y cumplimiento

- → **Políticas de seguridad unificadas:** un marco de políticas único aplica controles de seguridad coherentes en los dispositivos finales, las aplicaciones SaaS, la web y el correo electrónico, lo que responde a la necesidad de NIST de una gestión integrada de la seguridad.
- → **Controles automáticos de cumplimiento:** las políticas predefinidas y personalizables para la protección de datos, el control de acceso y la respuesta a incidentes siguen las recomendaciones del NIST CSF 2.0.
- → **Data Classification con IA:** identifica y clasifica con precisión los datos confidenciales en reposo, en tránsito y en uso, lo que minimiza los riesgos de incumplimiento.

Detección e implementación basadas en el comportamiento

- → **Risk-Adaptive Protection:** utiliza análisis de comportamiento para ajustar automáticamente la implementación de políticas en función de los niveles de riesgo en tiempo real.
- → **Análisis forense e investigación de incidentes:** proporciona registros y análisis detallados de eventos de seguridad y violaciones de políticas, lo que ayuda a las organizaciones a mejorar sus procesos de respuesta a incidentes.

Flexibilidad y escalabilidad de las implementaciones

- → **Opciones en la nube, en las instalaciones e híbridas:** las organizaciones pueden implementar las soluciones de Forcepoint en función de sus necesidades de infraestructura de seguridad para mantener la coherencia de sus políticas.
- → **Gestión escalable de la seguridad:** las necesidades de seguridad y cumplimiento evolucionan, y Forcepoint permite a las organizaciones ampliar su protección sin interrumpir las operaciones.

Las soluciones de Forcepoint están diseñadas para ayudar a las organizaciones a poner en práctica las directrices del NIST 2.0, implementar políticas de seguridad a escala y mejorar su estrategia general de ciberseguridad.

Simplificar el cumplimiento para permitir la innovación y el crecimiento

El NIST CSF 2.0 proporciona un enfoque estructurado y basado en riesgos para la ciberseguridad, ayuda a las organizaciones a proteger mejor los datos y simplifica el cumplimiento. La supervisión continua y los controles adaptativos reducen el riesgo de fugas y pérdidas de datos al identificar proactivamente las vulnerabilidades antes de que se violen las normas.

Al integrar la seguridad de datos moderna con las operaciones comerciales, las organizaciones pueden habilitar una colaboración segura, ayudar a la transformación digital e impulsar la innovación sin poner en peligro el cumplimiento. Un enfoque estructurado y basado en el riesgo aumenta la seguridad, optimiza las operaciones y permite que las empresas se centren en su crecimiento.

Protección de datos

El enfoque de Forcepoint Data Security Everywhere protege la información confidencial en todos los principales canales de acceso, unificando la implementación de la seguridad y simplificando la gestión.

SOLUCIONES DE SEGURIDAD DE DATOS DE FORCEPOINT
Forcepoint Data Loss Prevention (en las instalaciones/híbrida/en la nube): dispositivo final, red, descubrimiento, correo electrónico, aplicaciones SaaS y web
Forcepoint DSPM (Data Security Posture Management (en las instalaciones/nube)
Forcepoint Risk-Adaptive Protection (en las instalaciones/nube)

Protección de red

Las soluciones de seguridad de Forcepoint ofrecen una protección integral en redes, aplicaciones en la nube, correo electrónico y la web para evitar la pérdida de datos, controlar el acceso y garantizar el cumplimiento.

SOLUCIONES DE RED DE FORCEPOINT
Forcepoint (CASB y ZTNA)
Forcepoint Web Security (en las instalaciones/híbrida/nube)
Forcepoint Email Security (en las instalaciones/nube)
Forcepoint NGFW y Secure SD-WAN
Forcepoint RBI (Remote Browser Isolation) con CDR (Content Disarm and Reconstruction)

Soluciones de Forcepoint asignadas al NIST CSF 2.0

FUNCIÓN Y SUBCATEGORÍA	DESCRIPCIÓN	PRODUCTOS DE FORCEPOINT	VALOR
IDENTIFICACIÓN			
ID.AM-02	Se mantienen inventarios de software, servicios y sistemas gestionados por la organización	Soluciones de red de Forcepoint	Las soluciones de Forcepoint proporcionan registros e informes que pueden ayudar a las organizaciones a comprender el tráfico web, las aplicaciones en la nube y el uso de datos. Los controles de políticas también permiten a las organizaciones determinar qué sitios web y aplicaciones en la nube son adecuados para su uso, e identifican o bloquean categorías y aplicaciones en la nube que son inapropiadas o inseguras.
ID.AM-03	Se mantienen representaciones de las comunicaciones de red autorizadas de la organización y de los flujos de datos internos y externos de la red	Soluciones de red de Forcepoint	Las soluciones de Forcepoint pueden supervisar el uso de redes, la web, nubes y aplicaciones privadas para redes y dispositivos administrados y no administrados. Las soluciones de Forcepoint pueden utilizar controles de políticas para identificar o bloquear el acceso a estos destinos en función del riesgo, el cumplimiento o, incluso, la pérdida de productividad.
ID.AM-04	Se mantienen inventarios de los servicios prestados por los proveedores	Soluciones de red de Forcepoint	Forcepoint CASB, Web Security y NGFW también pueden detectar, gestionar y bloquear el tráfico, así como el acceso a sitios externos y a aplicaciones SaaS tanto gestionadas como no gestionadas. Además, Forcepoint NGFW puede supervisar el estado de los servicios.
ID.AM-05	Los activos se priorizan en función de su clasificación, su importancia crítica, sus recursos y su impacto en la misión	Soluciones de seguridad de datos de Forcepoint	Forcepoint ayuda a clasificar, identificar y priorizar los datos para su protección mediante Forcepoint DSPM, Forcepoint Classification, Data Detection and Response (DDR), Enterprise DLP y Risk-Adaptive Protection (RAP). Las soluciones de red de Forcepoint también pueden aplicar reglas de calidad de servicio (QoS) y supervisión del estado.
ID.AM-07	Se mantienen inventarios de datos y metadatos correspondientes para los tipos de datos designados	Soluciones de seguridad de datos de Forcepoint	Forcepoint ayuda a las organizaciones descubrir, inventariar y etiquetar datos de dentro de su entorno, y les da la capacidad de mantener un registro de datos de los datos y de las partes responsables.
ID.AM-08	Los sistemas, el hardware, el software, los servicios y los datos se gestionan durante todo su ciclo de vida	Seguridad de datos de Forcepoint	Forcepoint DSPM + DDR supervisa constantemente los datos durante todo su ciclo de vida, para clasificarlos y reclasificarlos a medida que cambian, rastrear su procedencia e incluso marcar los datos ROT al final de su ciclo de vida.

Soluciones de Forcepoint asignadas al NIST CSF 2.0

FUNCIÓN Y SUBCATEGORÍA	DESCRIPCIÓN	PRODUCTOS DE FORCEPOINT	VALOR
IDENTIFICACIÓN			
ID.RA-01	Las vulnerabilidades de los activos se identifican, validan y registran	Soluciones de red de Forcepoint	Las soluciones de Forcepoint pueden identificar riesgos en sitios web en tiempo real y gestionar puntuaciones de riesgo con aplicaciones en la nube. Forcepoint utiliza indicaciones en pantalla o mensajes en la consola para dar información sobre por qué estos recursos en la nube son peligrosos. Además, las capacidades de inspección de Forcepoint NGFW/IPS evalúan vulnerabilidades fuera de los canales web estándar.
ID.RA-02	La inteligencia sobre amenazas cibernéticas se obtiene de foros y fuentes de intercambio de información	Soluciones de red de Forcepoint	Las soluciones de Forcepoint utilizan fuentes de amenazas con diversas procedencias, así como nuestros propios equipos dedicados, que investigan y analizan las amenazas cibernéticas. Esta información se introduce en nuestro ACE (Advanced Classification Engine) y en nuestra red de inteligencia ThreatSeeker, que utilizamos para ayudar a identificar y bloquear amenazas cibernéticas con nuestras soluciones. Con esta información, las organizaciones también pueden crear categorías personalizadas para las soluciones de Forcepoint Web Security.
ID.RA-03	Se identifican y registran las amenazas internas y externas a la organización	Soluciones de seguridad de datos de Forcepoint Soluciones de red de Forcepoint	Se anotan y registran todas las amenazas detectadas o bloqueadas por las soluciones de Forcepoint. Las organizaciones pueden utilizar esta información para identificar el origen, el destino y otros detalles asociados al evento.
ID.RA-04	Se identifican y registran los posibles efectos y probabilidades de que las amenazas exploten vulnerabilidades	Soluciones de red de Forcepoint	Se anotan y registran todas las amenazas cibernéticas que Forcepoint identifique y bloquee. Además, Forcepoint actualiza a diario sus motores de detección de amenazas. Otras soluciones de Forcepoint, como Remote Browser Isolation, Content Disarm and Reconstruction y Advanced Malware Detection, sirven para identificar y detener las amenazas Zero Day.
ID.RA-05	Las amenazas, vulnerabilidades, probabilidades y efectos se utilizan para entender el riesgo inherente e informar sobre la priorización de la respuesta al riesgo	Soluciones de red de Forcepoint	Hay disponibles registros para que las organizaciones puedan saber el origen y el tipo de las amenazas cibernéticas detectadas o bloqueadas por Forcepoint. Además, las amenazas se clasifican por nivel de gravedad según el tipo de amenaza.
ID.RA-06	Las respuestas al riesgo se eligen, priorizan, planifican, rastrean y comunican	Soluciones de red de Forcepoint	Forcepoint ayuda en este proceso proporcionando un seguimiento e información, como el origen, el destino, el tipo de amenaza, etc., basados en la amenaza detectada o bloqueada.
ID.RA-07	Los cambios y las excepciones se gestionan, se evalúan en función del riesgo, se registran y se rastrean		Todo cambio de configuración realizado dentro de las soluciones de Forcepoint se registra para que las organizaciones puedan revisar y volver a implementar políticas en función de su evaluación. Además, Forcepoint es compatible un marco de flujo de trabajo y una API bidireccional para su integración con soluciones de gestión de incidencias de terceros.
ID.RA-09	La autenticidad e integridad del hardware y del software se evalúan antes de su adquisición y uso		Forcepoint proporciona hashes para todos los archivos descargables de software publicado.
ID.RA-10	Los proveedores críticos son evaluados antes de su adquisición	Soluciones de seguridad de datos de Forcepoint Soluciones de red de Forcepoint	Forcepoint pone a disposición toda la información relacionada con sus productos, por ejemplo, cómo administrarlos y todos los detalles relacionados con el contrato.

Soluciones de Forcepoint asignadas al NIST CSF 2.0

FUNCIÓN Y SUBCATEGORÍA	DESCRIPCIÓN	PRODUCTOS DE FORCEPOINT	VALOR
IDENTIFICACIÓN			
CÓDIGO IM-02	Las mejoras se determinan en base a pruebas y ejercicios de seguridad que, incluso, se realizan junto con proveedores y terceros pertinentes		Las soluciones de Forcepoint proporcionan detalles sobre amenazas cibernéticas o eventos de seguridad de datos. Los informes que se generan con esta información pueden ayudar a las organizaciones a determinar qué áreas necesitan mejorar.
CÓDIGO IM-03	Las mejoras se identifican a partir de la ejecución de procesos, procedimientos y actividades operativos		Las soluciones de Forcepoint proporcionan detalles sobre amenazas cibernéticas o eventos de seguridad de datos. Los informes que se generan con esta información pueden ayudar a las organizaciones a determinar qué áreas necesitan mejorar.

FUNCIÓN Y SUBCATEGORÍA	DESCRIPCIÓN	PRODUCTOS DE FORCEPOINT	VALOR
PROTEGER			
PR.AA-01	Se gestionan las identidades y credenciales de dispositivos y usuarios autorizados	Soluciones de seguridad de datos de Forcepoint	Con Enterprise DLP y DLP for Email, Forcepoint ayuda de forma indirecta a limitar las interacciones con los datos confidenciales que salen del entorno. Además, Forcepoint CASB puede ofrecer acceso condicional a aplicaciones SaaS que utilizan la autenticación SSO SAML.
PR.AA-02	Las identidades se verifican y se vinculan a las credenciales en función del contexto de las interacciones	Soluciones de seguridad de datos de Forcepoint Soluciones de red de Forcepoint	Las soluciones de Forcepoint proporcionan registros detallados de la actividad, que pueden ayudar a las organizaciones a identificar a los usuarios o sistemas que están realizando acciones. Con Risk-Adaptive Protection, las credenciales están vinculadas al contexto de los usuarios, los sistemas y las acciones de datos locales.
PR.AA-03	Se autentican los usuarios, los servicios y el hardware	Soluciones de seguridad de datos de Forcepoint Soluciones de red de Forcepoint	Las soluciones de Forcepoint utilizan métodos Zero Trust para autenticar usuarios. Además, utilizan conexiones a Active Directory, Single Sign-On y servicios de autenticación multifactor.
PR.AA-04	Las credenciales de identidad se protegen, transmiten y verifican	Soluciones de seguridad de datos de Forcepoint Soluciones de red de Forcepoint	Las soluciones de Forcepoint que utilizan cualquier SSO SAML 2.0 o autenticación a través de sistemas federados siguen los estándares del sector.
PR.AA-05	Los permisos, derechos y autorizaciones de acceso se definen en una política, se gestionan, se implementan, se revisan e incorporan los principios de privilegio mínimo y separación de funciones	Soluciones de seguridad de datos de Forcepoint Soluciones de red de Forcepoint	Las organizaciones pueden utilizar Forcepoint para restringir el acceso a recursos web, aplicaciones privadas, datos y redes. Además, las soluciones de Forcepoint ofrecen controles de acceso basados en roles, que pueden prohibir el acceso a áreas de las soluciones. El rol de los usuarios determina si tienen acceso para crear o modificar controles de políticas, ejecutar informes y gestionar la configuración de la infraestructura o de la plataforma.

Soluciones de Forcepoint asignadas al NIST CSF 2.0

FUNCIÓN Y SUBCATEGORÍA	DESCRIPCIÓN	PRODUCTOS DE FORCEPOINT	VALOR
PROTEGER			
PR.AT-01	Se proporciona sensibilización y formación al personal para que posea los conocimientos y las habilidades necesarios para realizar tareas generales teniendo en cuenta los riesgos de ciberseguridad	Soluciones de seguridad de datos de Forcepoint Soluciones de red de Forcepoint	Las soluciones de Forcepoint pueden proporcionar mensajes personalizados para las formaciones. Esta manera de formar a los usuarios puede hacer que las organizaciones sean más conscientes de las posibles amenazas de ciberseguridad.
PR.AT-02	Las personas con roles especializados reciben sensibilización y formación para que posean los conocimientos y las habilidades necesarios para realizar tareas relevantes teniendo en cuenta los riesgos de ciberseguridad	Soluciones de seguridad de datos de Forcepoint Soluciones de red de Forcepoint	Forcepoint exige a nuestros socios y alienta a los usuarios de nuestras soluciones a que realicen la formación sobre los productos. Forcepoint también proporciona numerosos artículos de conocimiento, vídeos prácticos y documentación que proporcionan habilidades y conocimientos a los usuarios de nuestras soluciones.
PR.DS-01	Se protegen la confidencialidad, integridad y disponibilidad de los datos en reposo	Soluciones de seguridad de datos de Forcepoint	Forcepoint puede descubrir y clasificar datos en reposo con Forcepoint DSPM. Las soluciones pueden proporcionar esta funcionalidad en recursos en las instalaciones y en la nube, a través de una implementación híbrida.
PR.DS-02	Se protegen la confidencialidad, integridad y disponibilidad de los datos en tránsito	Soluciones de seguridad de datos de Forcepoint	Forcepoint DLP puede proteger los datos confidenciales que se envían a través de recursos web, como sitios web, aplicaciones personalizadas y en la nube, correos electrónicos y canales de dispositivos finales. Las soluciones pueden proporcionar esta funcionalidad en recursos en las instalaciones y en la nube, a través de una implementación híbrida.
PR.DS-10	Se protegen la confidencialidad, integridad y disponibilidad de los datos en uso	Soluciones de seguridad de datos de Forcepoint	Forcepoint DLP protege los datos confidenciales al evitar la exfiltración no autorizada de datos que se cortan/copian/pegan, el acceso de aplicaciones a archivos, la impresión, el uso de medios extraíbles y el correo electrónico. Los controles de implementación de DLP están activos independientemente de dónde se encuentre el equipo del usuario. Los controles están activos tanto in situ como de forma remota. Las soluciones pueden proporcionar esta funcionalidad en recursos en las instalaciones y en la nube, a través de una implementación híbrida.
PR.PS-01	Se establecen y aplican prácticas de gestión de configuración	Soluciones de seguridad de datos de Forcepoint Soluciones de red de Forcepoint	Las soluciones de Forcepoint tienen controles predefinidos que permiten a las organizaciones aplicar las mejores prácticas con respecto a los controles de red y las necesidades de seguridad de datos. Estas políticas predefinidas ayudan a las organizaciones implementar rápidamente controles de seguridad para el entorno.
PR.PS-04	Se generan registros y se ponen a disposición para la supervisión continua	Soluciones de seguridad de datos de Forcepoint Soluciones de red de Forcepoint	Las organizaciones pueden utilizar las soluciones de Forcepoint para supervisar la actividad de los usuarios en diferentes canales para asegurarse de que cumplen las políticas de la empresa. Lo pueden hacer tanto en tanto canales de red como en canales para la exfiltración de datos. Forcepoint DLP conserva los registros de datos forenses para futuras auditorías.
PR.PS-05	Se evita la instalación y ejecución de software no autorizado	Soluciones de red de Forcepoint	Forcepoint puede evitar la descarga de cargas útiles potencialmente maliciosas, previniendo de forma proactiva su ejecución en el equipo del usuario.

Soluciones de Forcepoint asignadas al NIST CSF 2.0

FUNCIÓN Y SUBCATEGORÍA	DESCRIPCIÓN	PRODUCTOS DE FORCEPOINT	VALOR
PROTEGER			
PR.IR-01	Las redes y los entornos están protegidos contra el acceso lógico y el uso no autorizados	Soluciones de red de Forcepoint	Las soluciones de red de Forcepoint pueden impedir que los usuarios accedan a categorías específicas de aplicaciones web y en la nube, y pueden detectar y prevenir el tráfico entrante y saliente a las redes, además del tráfico este-oeste a través de SD-WAN/NGFW.
PR.IR-02	Los activos tecnológicos de la organización se protegen contra amenazas ambientales	Soluciones de seguridad de datos de Forcepoint Soluciones de red de Forcepoint	Las soluciones de Forcepoint se pueden implementar en configuraciones de alta disponibilidad para cumplir con los planes de recuperación ante desastres.
PR.IR-03	Se implementan mecanismos para cumplir los requisitos de resiliencia en situaciones normales y adversas	Soluciones de seguridad de datos de Forcepoint Soluciones de red de Forcepoint	Las soluciones en la nube de Forcepoint cuentan con mecanismos para garantizar la disponibilidad. Para las implementaciones en las instalaciones, Forcepoint recomienda el uso de implementaciones híbridas y de alta disponibilidad.

FUNCIÓN Y SUBCATEGORÍA	DESCRIPCIÓN	PRODUCTOS DE FORCEPOINT	VALOR
DETECTAR			
DE.CM-01	Las redes y los servicios de red se supervisan para detectar eventos potencialmente adversos	Soluciones de seguridad de datos de Forcepoint Soluciones de red de Forcepoint	Forcepoint analiza el tráfico web y de red para detectar posibles pérdidas de datos y tráfico de red general malicioso, y supervisa las amenazas internas con Risk-Adaptive Protection y Forcepoint Insider Threat.
DE.CM-03	Se supervisan las actividades del personal y el uso de la tecnología para detectar posibles eventos adversos	Soluciones de seguridad de datos de Forcepoint Soluciones de red de Forcepoint	Las soluciones de Forcepoint pueden supervisar la actividad de los usuarios y calcular su riesgo en tiempo real, para analizar eventos de red y datos. Además, Risk-Adaptive Protection de Forcepoint puede supervisar la actividad de los usuarios y calcular su riesgo en tiempo real con más de 130 indicadores de comportamiento.
DE.CM-06	Se supervisan las actividades y los servicios de los proveedores de servicios externos para detectar posibles eventos adversos	Soluciones de red de Forcepoint	Las soluciones de Forcepoint pueden supervisar la actividad de los usuarios y las aplicaciones, y calcular su riesgo en tiempo real, para analizar eventos de red y datos. Además, controles de Forcepoint, como ZTNA, pueden ayudar a supervisar las conexiones externas a las aplicaciones internas para identificar y bloquear eventos potencialmente adversos.
DE.CM-09	El hardware y el software informáticos, los entornos de ejecución y sus datos se supervisan para detectar posibles eventos adversos	Soluciones de seguridad de datos de Forcepoint Soluciones de red de Forcepoint	Las soluciones de Forcepoint pueden supervisar la actividad de los usuarios y las aplicaciones, y calcular su riesgo en tiempo real, para analizar eventos de red y datos. Las soluciones de Forcepoint supervisan o bloquean la exfiltración de datos y el tráfico de red para determinar si los eventos son adversos basándose en controles de políticas establecidos.

Soluciones de Forcepoint asignadas al NIST CSF 2.0

FUNCIÓN Y SUBCATEGORÍA	DESCRIPCIÓN	PRODUCTOS DE FORCEPOINT	VALOR
DETECTAR			
DE.AE-02	Los eventos potencialmente adversos se analizan para comprender mejor las actividades relacionadas	Soluciones de seguridad de datos de Forcepoint Soluciones de red de Forcepoint	Forcepoint puede proporcionar a los equipos de SOC datos de incidentes y datos detallados del registro y de análisis forenses, para que puedan determinar si un evento es adverso.
DE.AE-03	La información está correlacionada desde múltiples fuentes	Soluciones de seguridad de datos de Forcepoint Soluciones de red de Forcepoint	Las soluciones de Forcepoint pueden proporcionar informes centralizados para consolidar incidentes y, así, ayudar a las organizaciones a que respondan de forma adecuada. Además, la red ThreatSeeker correlaciona datos de todas las implementaciones de Forcepoint para facilitar la identificación de amenazas.
DE.AE-04	Se conoce el impacto estimado y el alcance de los eventos adversos	Soluciones de seguridad de datos de Forcepoint Soluciones de red de Forcepoint	Las soluciones de Forcepoint pueden proporcionar detalles completos sobre incidentes junto con clasificaciones de gravedad y riesgo, para que las organizaciones comprendan su impacto.
DE.AE-06	El personal autorizado y las herramientas reciben información sobre los eventos adversos	Soluciones de seguridad de datos de Forcepoint Soluciones de red de Forcepoint	Las soluciones de Forcepoint proporcionan información detallada sobre eventos, cuya visualización se controla con RBAC. Cuando Forcepoint detecta un incidente, puede generar alertas para enviarlas a los equipos adecuados a través del panel, correos electrónicos e integraciones con herramientas de terceros (por ejemplo, SIEM o sistemas de incidencias)
DE.AE-07	La inteligencia sobre amenazas cibernéticas y la información contextual se incorporan al análisis	Soluciones de seguridad de datos de Forcepoint Soluciones de red de Forcepoint	Las políticas de Forcepoint utilizan análisis contextuales e integraciones con otras fuentes (por ejemplo, SIEM o fuentes de inteligencia de terceros) para identificar eventos de riesgo o identificar y bloquear acciones de exfiltración de datos.
DE.AE-08	Los eventos adversos se declaran incidentes cuando cumplen los criterios de incidente establecidos	Soluciones de seguridad de datos de Forcepoint Soluciones de red de Forcepoint	Forcepoint proporciona detalles de incidentes basados en la violación de controles de políticas establecidas, para ayudar a las organizaciones en el proceso de declaración.

Soluciones de Forcepoint asignadas al NIST CSF 2.0

FUNCIÓN Y SUBCATEGORÍA	DESCRIPCIÓN	PRODUCTOS DE FORCEPOINT	VALOR
RESPONDER			
RS.MA-01	Cuando se declara un incidente, el plan de respuesta a incidentes se ejecuta en coordinación con los terceros relevantes	Soluciones de seguridad de datos de Forcepoint Soluciones de red de Forcepoint	Las políticas de Forcepoint incluyen acciones proactivas y reactivas que se alinean con los planes de respuesta a incidentes de la organización. La API bidireccional también ayuda en los flujos de trabajo de respuesta a incidentes con soluciones de terceros.
RS.MA-02	Los informes de incidentes se clasifican y validan	Soluciones de seguridad de datos de Forcepoint Soluciones de red de Forcepoint	Las soluciones de Forcepoint proporcionan una gestión e informes centralizados que ayudan a clasificar e investigar amenazas.
RS.MA-03	Los incidentes se clasifican y priorizan	Soluciones de seguridad de datos de Forcepoint Soluciones de red de Forcepoint	Los incidentes de Forcepoint se pueden clasificar según su origen, gravedad, política, etc. Se pueden priorizar por: más reciente, más grave, con mayor puntuación de riesgo, etc.
RS.MA-04	Los incidentes se escalan o derivan según sea necesario	Soluciones de seguridad de datos de Forcepoint Soluciones de red de Forcepoint	Forcepoint proporciona información detallada con niveles de gravedad/puntuaciones de riesgo sobre los incidentes, lo que puede ayudar a priorizar incidentes/casos para escalarlos.
RS.MA-05	Se aplican los criterios para iniciar la recuperación ante incidentes	Soluciones de seguridad de datos de Forcepoint Soluciones de red de Forcepoint	Forcepoint puede proporcionar información detallada sobre un incidente, lo que es útil en los procesos de recuperación ante incidentes.
RS.AN-03	Se realizan análisis para establecer qué ha ocurrido durante un incidente y cuál es su causa principal	Soluciones de seguridad de datos de Forcepoint Soluciones de red de Forcepoint	Forcepoint puede proporcionar información detallada sobre un incidente, como su origen, destino, canal y las reglas que infringió, junto con información forense sobre los eventos de seguridad de datos detectados.
RS.AN-06	Las acciones realizadas durante las investigaciones se registran, y se preservan la integridad y la procedencia de los registros	Soluciones de seguridad de datos de Forcepoint Soluciones de red de Forcepoint	Forcepoint mantiene un registro de auditoría de las actividades del administrador, junto con los detalles de los incidentes forenses, que se pueden almacenar en una ubicación cifrada.

Soluciones de Forcepoint asignadas al NIST CSF 2.0

FUNCIÓN Y SUBCATEGORÍA	DESCRIPCIÓN	PRODUCTOS DE FORCEPOINT	VALOR
RESPONDER			
RS.AN-07	Se recopilan datos y metadatos de incidentes y se preservan su integridad y procedencia	Soluciones de seguridad de datos de Forcepoint Soluciones de red de Forcepoint	Las soluciones de Forcepoint recopilan y almacenan información forense sobre incidentes que se almacena en un repositorio cifrado.
RS.AN-08	Se estima y valida la magnitud de un incidente	Soluciones de seguridad de datos de Forcepoint Soluciones de red de Forcepoint	Forcepoint proporciona información detallada con niveles de gravedad/puntuaciones de riesgo sobre los incidentes, lo que puede ayudar a priorizar incidentes/casos para escalarlos.
RS.CO-02	Los incidentes se notifican a las partes interesadas internas y externas	Soluciones de seguridad de datos de Forcepoint Soluciones de red de Forcepoint	Forcepoint puede proporcionar información sobre incidentes y enviar alertas a partes designadas. Con Forcepoint DSPM, el registro de activos puede avisar a varios propietarios de datos sobre detecciones y cambios en la clasificación o en el riesgo de los datos que están bajo su responsabilidad.
RS.CO-03	La información se comparte con las partes interesadas internas y externas designadas	Soluciones de seguridad de datos de Forcepoint Soluciones de red de Forcepoint	Las políticas de Forcepoint utilizan análisis contextuales e integraciones con otras fuentes (por ejemplo, SIEM o fuentes de inteligencia de terceros) para identificar eventos de riesgo o identificar y bloquear acciones de exfiltración de datos.
RS.MI-01	Los incidentes se controlan Forcepoint	Soluciones de seguridad de datos de Forcepoint Soluciones de red de Forcepoint	Las políticas de Forcepoint incluyen acciones proactivas y reactivas que se alinean con los planes de respuesta a incidentes de la organización. Forcepoint DLP puede bloquear o poner en cuarentena automáticamente datos para evitar su exfiltración.
RS.MI-02	Los incidentes se erradican Forcepoint	Soluciones de seguridad de datos de Forcepoint Soluciones de red de Forcepoint	Las políticas de Forcepoint incluyen acciones proactivas y reactivas que se alinean con los planes de respuesta a incidentes de la organización.

Soluciones de Forcepoint asignadas al NIST CSF 2.0

FUNCIÓN Y SUBCATEGORÍA	DESCRIPCIÓN	PRODUCTOS DE FORCEPOINT	VALOR
RECUPERAR			
RC.RP-01	La parte de recuperación del plan de respuesta a incidentes se lanza desde el proceso de respuesta a incidentes	Soluciones de seguridad de datos de Forcepoint Soluciones de red de Forcepoint	La revisión de los incidentes y las respuestas de Forcepoint DLP se puede integrar en los planes de recuperación y mejora de la organización.
RC.RP-06	La recuperación de incidentes se declara finalizada en función de criterios, y se rellena la documentación relacionada con el incidente	Soluciones de seguridad de datos de Forcepoint Soluciones de red de Forcepoint	Forcepoint puede proporcionar detalles de incidentes para ayudar a las organizaciones en este proceso.
RC.CO-04	Las actualizaciones públicas sobre recuperación de incidentes se comparten utilizando métodos y mensajes aprobados	Soluciones de seguridad de datos de Forcepoint Soluciones de red de Forcepoint	Forcepoint puede proporcionar detalles de incidentes de infracciones detectadas por sus soluciones, para que las organizaciones puedan crear mensajes y actualizaciones.

forcepoint.com/contact