# Marco de seguridad cibernética NIST (CSF, por sus siglas en inglés)

Alineación con el NIST CSF en la nube de AWS

*Enero del 2019*

[ Adopción segura de la nube ]

# Notas

Este documento solo tiene fines informativos. Representa las ofertas y prácticas actuales de productos de AWS a partir de la fecha de emisión de este documento, y que pueden ser modificadas sin previo aviso. Los clientes son responsables de realizar su propia evaluación independiente de la información contenida en este documento y cualquier uso de los productos o servicios de AWS, cada uno de los cuales se suministra "tal cual" y sin garantía de ningún tipo, ya sea explícita o implícita. Este documento no representa ninguna garantía, representación, compromiso contractual, condición o garantía de AWS, sus afiliados, proveedores o licenciantes. Las responsabilidades y obligaciones de AWS para con sus clientes están controladas por los acuerdos de AWS y este documento no forma parte, ni modifica, ningún acuerdo entre AWS y sus clientes.

# Contenido



# Resumen

Los gobiernos, los sectores de la industria y las organizaciones de todo el mundo están reconociendo cada vez más el Marco de seguridad cibernética (CSF) de NIST como una base de seguridad cibernética recomendada para ayudar a mejorar la gestión del riesgo de la seguridad cibernética y la resistencia de sus sistemas. Este documento evalúa el CSF de NIST y las numerosas ofertas de la nube de AWS que los clientes del sector público y empresarial pueden utilizar para cumplir con el CSF de NIST para mejorar su seguridad cibernética. También ofrece un certificado validado por terceros que confirma el cumplimiento de los servicios de AWS con las prácticas de gestión de riesgos del CSF de NIST, lo cual le permite proteger sus datos en AWS de forma adecuada.

# Personas a las que va dirigido

Este documento es para profesionales de la seguridad cibernética, funcionarios de gestión de riesgos u otros responsables de la empresa en su conjunto que desean implementar un marco de seguridad cibernética nuevo en la empresa o mejorar el marco actual. Para obtener detalles sobre cómo configurar los servicios de AWS identificados en este documento y en el libro de trabajo del clienteasociado (ver Apéndice A), póngase en contacto con su arquitecto de soluciones de AWS.

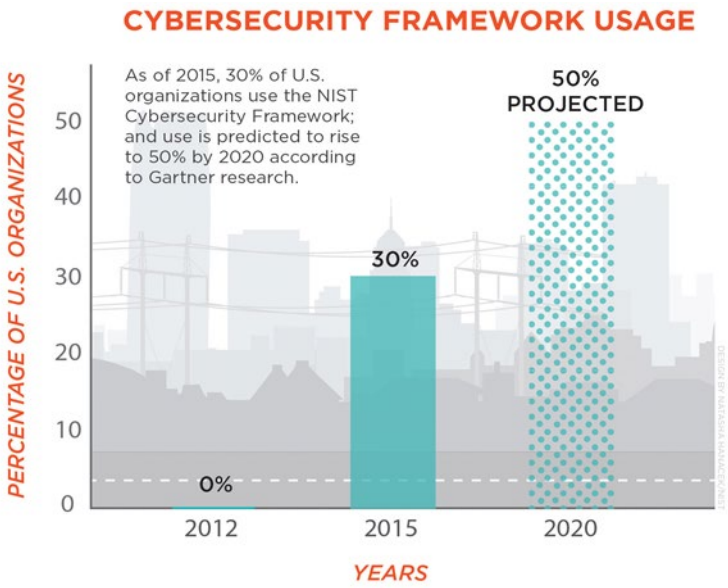
# Introducción

El marco del NIST para mejorar la seguridad cibernética de la infraestructura crítica (Marco de seguridad cibernética de NIST o CSF) se publicó originalmente en febrero del 2014, en respuesta a la Orden Ejecutiva Presidencial 13636 para la mejora de la ciberseguridad de infraestructuras críticas, "Improving Critical Infrastructure Cybersecurity"

Una "Infraestructura de seguridad cibernética", basada en el desarrollo de un marco voluntario para ayudar a las empresas a mejorar la seguridad cibernética, la gestión de riesgos y la resistencia de sus sistemas. El NIST consultó con varios socios del gobierno, la industria y el mundo académico durante más de un año para crear unas directrices y prácticas sólidas y basadas en el consenso. La Ley de mejora de la seguridad cibernética del 2014 reforzó la legitimidad y la autoridad del CSF al codificarlo y convertirse voluntariamente en ley y hasta que la Orden Ejecutiva Presidencial sobre el fortalecimiento de la seguridad cibernética de las redes federales y la infraestructura crítica, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure", firmada el 11 de mayo del 2017, obligó a todos los organismos federales de los EE.UU. a utilizar el CSF.

A pesar de que el objetivo era su adopción por el sector de infraestructuras críticas, el conjunto básico de disciplinas de seguridad cibernética contenidas en el CSF han contado con el apoyo del gobierno y la industria, como una base de referencia recomendada para ser utilizada por cualquier empresa, independientemente de su sector o tamaño. La industria hace cada vez más referencia al CSF como una norma de seguridad cibernética de hecho.

En febrero del 2018, la Organización Internacional de Normalización presentó "ISO/IEC 27103:2018 - Information technology — Security techniques". Esta norma sirve de guía para implementar un marco de seguridad cibernética y aprovechar las directrices actuales. De hecho, **la ISO 27103 fomenta los mismos conceptos y las mejores prácticas contenidas en el CSF de NIST**; específicamente, un marco enfocado en los resultados de seguridad organizados en torno a cinco funciones (Identificar, Proteger, Detectar, Responder, Recuperar) y actividades básicas que se cruzan con las directrices, acreditaciones y marcos actuales. Adoptar este enfoque puede ayudar a las empresas a conseguir resultados en materia de seguridad, ya que es preferible volver a utilizar y no volver a realizar.




Créditos: Natasha Hanacek/NIST https://www.nist.gov/industry-impacts/cybersecurity

Según Gartner, el CSF es utilizado por aproximadamente el 30 % de las empresas del sector privado de los EE. UU. y se prevé que alcance el 50 % en el año 2020.[1] A partir de la publicación de este informe, 16 sectores de infraestructura crítica de los EE. UU. utilizan el CSF y más de 21 estados ya lo han implementado.[2] Además de infraestructuras críticas y otras empresas del sector privado, otros países, como Italia e Israel, están aprovechando el CSF como base para sus directrices en seguridad cibernética nacional.

Desde el año fiscal 2016, la métrica de la agencia federal estadounidense para la Ley de modernización de la seguridad de la información federal (FISMA), se ha organizado en torno al CSF, y ahora se denomina un "estándar para gestionar y reducir los riesgos de la seguridad cibernética". Según el informe de la FISMA al Congreso para el año fiscal 2016, el Consejo de Inspectores Generales de Integridad y Eficiencia (CIGIE, por sus siglas en inglés) alineó las métricas de IG con las cinco funciones del CSF para evaluar el rendimiento de la agencia y promover métricas y criterios consistentes y comparables entre las evaluaciones del director de información (CIO, por sus siglas en inglés) y las del inspector general (IG, por sus siglas en inglés).

Las aplicaciones más comunes del CSF se han manifestado en tres situaciones diferentes:

1. La evaluación de la posición y la experiencia de la empresa en materia de seguridad cibernética mediante la evaluación del modelo CSF (perfil actual) determina la posición deseada en seguridad cibernética (perfil objetivo) y planifica y prioriza los recursos y los esfuerzos para conseguir el perfil objetivo.
2. La evaluación de los productos y los servicios actuales y propuestos para cumplir con los objetivos de seguridad junto con las categorías y subcategorías del CSF para identificar las deficiencias en la capacidad y las oportunidades de reducir el solapamiento/duplicado de las mismas y lograr una mayor eficiencia.
3. Una referencia para la reestructuración de sus equipos de seguridad, los procesos y la formación.

Este documento identifica las capacidades más importantes en la oferta de servicios de AWS disponibles a nivel mundial que las agencias federales, estatales y locales de los EE. UU.; los propietarios y los operadores de infraestructuras críticas a nivel mundial; así como empresas comerciales globales pueden implementar para cumplir con el CSF (es decir, la seguridad en la nube). También ofrece asistencia a la hora de establecer el cumplimiento de los servicios en la nube de AWS con el CSF y según lo validado por un asesor externo (es decir, la seguridad de la nube) basado en

1 https://www.nist.gov/industry-impacts/cybersecurity

2 Ibid.

normas de conformidad, incluyendo el FedRAMP Moderate[3] y la ISO 9001/27001/27017/27018[4]. Esto significa que puede confiar en los servicios de AWS a la hora de cumplir con los objetivos y los resultados de seguridad identificados en el CSF y que puede utilizar las soluciones de AWS para ayudarle a cumplir con el CSF y cualquier norma de cumplimiento obligatoria. Fomentar las soluciones de AWS puede facilitar el cumplimiento de las métricas de informes de la FISMA, especialmente para los organismos federales de los EE.UU. Esta combinación de resultados le permitirá confiar en la seguridad y la resistencia de sus datos a medida que vaya enviando cargas de trabajo críticas a la nube de AWS.

# Ventajas de seguridad al adoptar el CSF del NIST

El CSF ofrece una estructura, sencilla y efectiva, con tres elementos: Núcleo, Niveles y Perfiles. El núcleo representa un conjunto de prácticas de seguridad cibernética, resultados y controles de seguridad técnicos, operativos y de gestión (denominadas “referencias informativas”) que apoyan las cinco funciones de gestión de riesgos: Identificar, Proteger, Detectar, Responder y Recuperar. Los niveles hacen referencia a la aptitud y la experiencia de una empresa a la hora de administrar las funciones y los controles del CSF. Los perfiles sirven para transmitir la seguridad cibernética actual y futura de la empresa. Juntos, estos tres elementos permiten a las empresas priorizar y gestionar los riesgos de seguridad cibernética de acuerdo con sus necesidades empresariales.

Es importante tener en cuenta que la implementación del núcleo, los niveles y los perfiles corre a cuenta de la empresa que adopta el CSF (por ejemplo, una agencia gubernamental, una institución financiera, una empresa nueva comercial, etc.). Este documento analiza las soluciones y las capacidades de AWS que apoyan al núcleo a la hora de conseguir buenos resultados en seguridad (es decir, subcategorías) en el CSF. También describe los servicios de AWS que han sido acreditados en la FedRAMP Moderate y la ISO 9001/27001/27017/27018 como que cumplen con el CSF.

El núcleo hace referencia a los controles de seguridad de las normas ampliamente adoptadas y reconocidas internacionalmente, como la ISO/ IEC 27001, NIST 800-53, Objetivos de control para la información y tecnología relacionada (COBIT, por sus siglas en inglés), Consejo de seguridad cibernética (CCS, por sus siglas en inglés), Los 20 controles de seguridad más importantes (CSC, por sus siglas en inglés) y las normas de seguridad ANSI/ISA-62443 para la automatización industrial y los sistemas de control. A pesar de que esta lista representa algunas de las normas más prestigiosas, el CSF recomienda a las empresas el uso de catálogos de control para satisfacer de la mejor forma posible sus necesidades organizativas. El CSF también fue diseñado de manera que el tamaño, el sector y el país no fueran considerados; por lo tanto, las empresas del sector público y privado deben tener garantías de la aplicabilidad del CSF, independientemente del tipo de entidad o ubicación del estado o país.

El CSF anima a que las empresas hagan uso de catálogos de control para satisfacer mejor sus necesidades organizativas. El CSF también fue diseñado de manera que el tamaño, el sector y el país no fueran considerados; por lo tanto, las empresas del sector público y privado deben tener garantías de la aplicabilidad del CSF, independientemente del tipo de entidad o ubicación del estado o el país.

3 El Programa federal de gestión de riesgos y autorizaciones (FedRAMP en inglés) es el programa estandarizado a nivel federal del gobierno de los EE. UU. para la autorización de seguridad de los servicios en la nube. El enfoque de “hacer una vez, utilizar muchas veces” del FedRAMP se creó para ofrecer beneficios significativos, como aumentar la consistencia y la fiabilidad en la evaluación de los controles de seguridad, reducir los costes para los proveedores de servicios y los clientes de las agencias y agilizar las evaluaciones de autorización duplicadas entre las agencias que adquieren el mismo servicio.

4 La ISO 27001/27002 es una norma de seguridad ampliamente adoptada a nivel mundial que establece los requisitos y las mejores prácticas para realizar un enfoque sistemático para administrar la información de la compañía y del cliente en base a las evaluaciones de riesgos periódicas adecuadas para las situaciones de amenazas cambiantes. La ISO 27018 es un código de prácticas que se centra en la protección de los datos personales en la nube. Se basa en la norma de seguridad de la información ISO 27002 y ofrece una guía de implementación sobre los controles de la norma ISO 27002 aplicables a la información de identificación personal (PII, por sus siglas en inglés) de la nube pública. También ofrece un conjunto de controles adicionales y una guía asociada para abordar los requisitos de protección de la PII de la nube pública que no se abordan en el conjunto de control de la ISO 27002 existente.

# Casos de uso de implementación del CSF del NIST

## Atención sanitaria

El Departamento de Salud y Servicios Humanos de los EE. UU. completó la comparación de la Ley de portabilidad y responsabilidad de los seguros de la salud de 1996 (HIPAA)5 Regla de seguridad con el CSF del NIST. Según la HIPAA, las entidades y los socios comerciales cubiertos deben cumplir con la Regla de seguridad de HIPAA para garantizar la confidencialidad, integridad y disponibilidad de la información médica protegida.6 Teniendo en cuenta que la HIPAA no dispone de un conjunto de controles que pueden evaluarse ni de un proceso de acreditación formal, las entidades afectadas y los socios comerciales, como AWS, son elegibles para la HIPAA en función del cumplimiento con los controles de seguridad de NIST 800-53 que se pueden probar y verificar para colocar los servicios en la lista de elegibilidad de HIPAA. La correlación entre el CSF del NIST y la Regla de seguridad de la HIPAA ofrece un nivel de seguridad adicional, ya que las evaluaciones realizadas para ciertas categorías del CSF del NIST pueden ser más específicas y detalladas que las realizadas para el requisito de la Regla de seguridad de la HIPAA correspondiente.

## Servicios financieros

El Consejo de Coordinación del Sector de Servicios Financieros de los EE. UU.7 (FS-SCC, por sus siglas en inglés), compuesto por 70 asociaciones de servicios financieros, instituciones y empresas de servicios públicos/intercambio, desarrolló un perfil específico del sector: una versión personalizada del CSF del NIST que aborda aspectos únicos del sector y sus requisitos reglamentarios. El perfil de seguridad cibernética específico del sector de servicios financieros, redactado en colaboración con las agencias reguladoras, es un medio para armonizar los requisitos regulatorios relacionados con la seguridad cibernética. El FS-SCC, por ejemplo, detectó la correspondencia de la categoría "Estrategia de gestión de riesgos" con nueve requisitos regulatorios diferentes y determinó que el idioma y las definiciones, a pesar de ser diferentes, abordaban en gran medida el mismo objetivo de seguridad.

## Adopción internacional

Fuera de los EE. UU., muchos países han aprovechado el CSF del NIST para utilizarlo en el sector comercial y el público. Italia fue uno de los primeros países en adoptar el CSF del NIST y desarrolló una estrategia nacional de seguridad cibernética con base en las cinco funciones. En junio del 2018, el Reino Unido adaptó su Normativa de seguridad cibernética mínima (obligatoria para todos los departamentos gubernamentales) a las cinco funciones. Además, Israel y Japón localizaron el CSF del NIST en sus respectivos idiomas, e Israel creó una metodología de defensa cibernética basada en su propia adaptación del CSF del NIST. Uruguay realizó una comparación entre el CSF y las normas ISO para fortalecer las conexiones con los marcos internacionales. Suiza, Escocia, Irlanda y Bermudas también se encuentran en la lista de países que utilizan el CSF del NIST para mejorar la seguridad cibernética y la resistencia en todas las empresas del sector público y comercial.

---

5 La HIPAA incluye disposiciones para proteger la seguridad y la privacidad de la información médica protegida (PHI, por sus siglas en inglés). La PHI incluye un conjunto muy amplio de datos sanitarios personalmente identificables y relacionados con la salud, como la información sobre seguros y facturación, incluyendo los datos de diagnóstico, los datos de atención hospitalaria y los resultados de laboratorio, como las imágenes y los resultados de pruebas. Las reglas de la HIPAA se aplican a las entidades afectadas, incluyendo los hospitales, los proveedores de servicios médicos, los planes de salud patrocinados por el empleador, los centros de investigación y las compañías de seguros que tratan directamente con pacientes y datos de los mismos. El requisito de la HIPAA para proteger la PHI también se extiende a los socios comerciales.

6 La PHI incluye un conjunto muy amplio de datos sanitarios personalmente identificables y relacionados con la salud, incluyendo la información sobre seguros y facturación, los datos de diagnóstico, los datos de atención hospitalaria y los resultados de laboratorio, como las imágenes y los resultados de pruebas.

7 https://www.fsscc.org/About-FSSCC

# Servicios de AWS que permiten cumplir con el CSF del NIST

Esta sección proporciona una descripción general de las capacidades de AWS que puede aprovechar para cumplir con el núcleo del CSF y conseguir "seguridad en la nube". El apéndice A ofrece una lista completa de los servicios de AWS que cumplen con las categorías y subcategorías funcionales. La integración de estas herramientas como parte de su cartera tecnológica empresarial puede ayudarle a crear soluciones automatizadas, innovadoras y seguras para fortalecer su posición en la seguridad cibernética.

Cada “subcategoría” del núcleo del CSF fue evaluada y emitida por un asesor externo independiente para cumplir con los siguientes criterios:

- Correspondencia con los servicios de AWS aplicables
- Servicios de AWS aplicables acreditados según la FedRAMP Moderate y/o la ISO 9001/27001/27017/27018

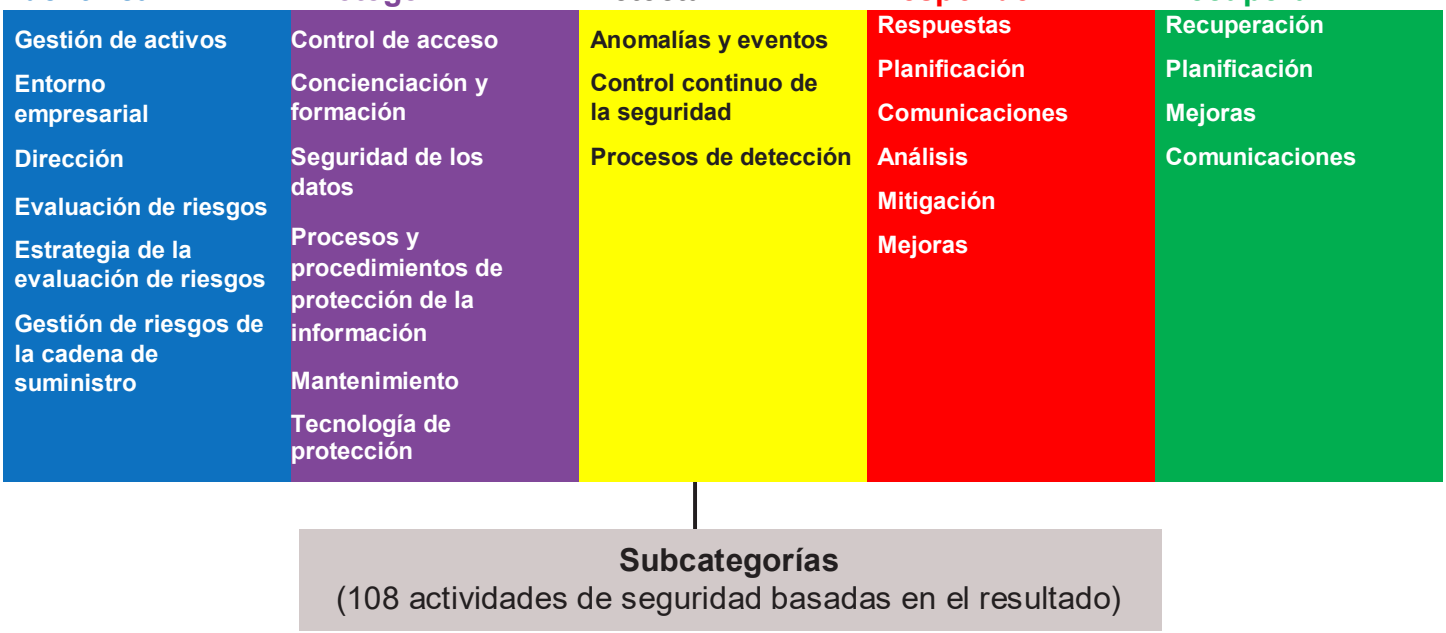
Además de tratar la "seguridad en la nube", esta sección también analiza cómo los servicios de AWS cumplen con el CSF para lograr la "seguridad de la nube". La certificación de terceros establece que los servicios de AWS cumplen con el CSF basándose en el cumplimiento de las normas que se han correlacionado con las subcategorías del CSF, específicamente, la FedRAMP Moderate y la ISO 9001/27001/27017/27018. Esto significa que puede confiar en que los servicios de AWS cumplan con los objetivos de seguridad del CSF y que puede utilizar estas soluciones de AWS para lograr también las mejores prácticas y resultados de seguridad y resistencia identificados en el CSF.

Si bien este documento sirve como un recurso para proporcionar una gestión de riesgos del ciclo de vida de la empresa que conecta los objetivos de la misión y el negocio con las actividades de la seguridad cibernética, AWS también proporciona otros recursos de mejores prácticas para los clientes que trasladan sus empresas a la nube (AWS Cloud Adoption Framework) y los clientes que diseñan, crean u optimizan soluciones en AWS (Well-Architected Framework).[8] Estos recursos proporcionan herramientas complementarias para ayudar a una empresa a desarrollar y obtener experiencia en sus programas, procesos y prácticas en la nube para la gestión de riesgos de la seguridad cibernética. Más específicamente, este documento técnico del CSF del NIST se puede usar junto con cualquiera de estas guías de mejores prácticas, sirviendo así como base para su programa de seguridad con el Cloud Adoption Framework o el Well-Architected Framework para poner en práctica los resultados de la seguridad del CSF en la nube.

Para los clientes que se trasladan a la nube, el AWS Cloud Adoption Framework (AWS CAF) proporciona una guía que respalda a cada unidad de su empresa para que cada área entienda cómo actualizar las habilidades, adaptar los procesos existentes e introducir nuevos procesos para aprovechar al máximo los servicios ofrecidos por la computación en la nube.
Miles de empresas en todo el mundo han migrado con éxito sus negocios a la nube, confiando en el CAF de AWS para guiar sus esfuerzos. AWS y nuestros socios proporcionan herramientas y servicios que pueden ayudarle en cada paso del camino para garantizar una comprensión y una transición completas.

https://d1.awsstatic.com/whitepapers/aws_cloud_adoption_framework.pdf

8 El AWS Well-Architected Framework documenta las mejores prácticas de arquitectura para diseñar y poner en funcionamiento sistemas fiables, seguros, eficientes y rentables en la nube. Proporciona un conjunto de preguntas básicas que le permiten comprender si una arquitectura específica cumple bien con las mejores prácticas de la nube. https://d1.awsstatic.com/whitepapers/architecture/AWS_Well-Architected_Framework.pdf




# Función del núcleo del CSF: Identificar

Esta sección analiza las seis categorías que conforman la función "Identificar": gestión de activos, entorno empresarial, dirección, evaluación de riesgos, estrategia de gestión de riesgos y gestión de riesgos de la cadena de suministro que "desarrolla una comprensión organizativa para gestionar el riesgo de la seguridad cibernética de los sistemas, las personas, los activos, los datos y las capacidades". En el apéndice A se puede encontrar un plano detallado que relaciona los servicios de AWS con "subcategorías" individuales y las declaraciones de responsabilidad del cliente y AWS.

**Subcategorías del núcleo de CSF para Identificar:**

**Gestión de activos (ID.AM):** Los datos, el personal, los dispositivos, los sistemas y las instalaciones que permiten a la empresa conseguir objetivos empresariales se identifican y gestionan de forma consistente con su importancia relativa para los objetivos empresariales y la estrategia de los riesgos de la empresa.

**Entorno empresarial (ID.BE):** La misión, los objetivos, las partes interesadas y las actividades de la empresa se entienden y priorizan. Esta información se utiliza para informar acerca de los roles, las responsabilidades y las decisiones de gestión de riesgos de la seguridad cibernética.

**Dirección (ID.GV)**: Las políticas, los procedimientos y los procesos para gestionar y controlar los requisitos regulatorios, legales, de riesgos, ambientales y operativos de la empresa se entienden e informan a la gestión del riesgo de la seguridad cibernética.

**Evaluación de riesgos (ID.RA):** La empresa entiende el riesgo de la seguridad cibernética en las operaciones de la misma (incluyendo la misión, las funciones, la imagen o la reputación), los activos de la empresa y las personas.

**Estrategia de gestión de riesgos (ID.RM):** Las prioridades, las restricciones, las tolerancias de los riesgos y las suposiciones de la empresa se establecen y utilizan para apoyar las decisiones del riesgo operativo.

**Gestión de riegos de la cadena de suministro (ID.SC):** Las prioridades, las restricciones, las tolerancias de los riesgos y las suposiciones de la empresa se establecen y utilizan para apoyar las decisiones del riesgo asociadas con la gestión en torno al riesgo de la cadena de suministro. La empresa ha establecido e implementado los procesos para identificar, evaluar y gestionar los riesgos de la cadena de suministro.

## Responsabilidad del cliente

Identificar y administrar los activos de la TI es el primer paso para una dirección y una seguridad de la TI efectivas aunque, sin embargo, ha sido uno de los más desafiantes. El Centro para la Seguridad de Internet (CIS)[9] reconoció la importancia fundamental del inventario de activos y asignó el inventario de activos físicos y lógicos como controles n.º 1 y n.º 2 de sus 20 principales. Sin embargo, ha sido difícil conseguir y mantener un inventario de la TI preciso, tanto de activos físicos como de activos lógicos, para empresas de todos los tamaños y recursos. Las soluciones de inventario se limitan a poder identificar e informar sobre todos los activos de TI en toda la empresa por varios motivos, como la segmentación de la red que impide que la solución "vea" e informe desde varias partes de la red empresarial, ya que los agentes de software del punto de enlace no se implementan o no funcionan completamente y existe incompatibilidad entre una amplia gama de tecnologías dispares. Desafortunadamente, los activos que se "pierden" o que no se contabilizan representan el mayor riesgo. Si no se rastrean, lo más probable es que no reciban los parches y actualizaciones más recientes, no se reemplacen durante las actualizaciones en el ciclo de vida y se permita que el malware pueda aprovecharse y mantener su efecto perjudicial sobre el activo.

El traslado a AWS ofrece dos beneficios fundamentales que pueden mitigar los desafíos que supone mantener inventarios de activos en un entorno local. En primer lugar, AWS asume la responsabilidad exclusiva de gestionar los activos físicos que conforman la infraestructura de la nube de AWS. Esto puede reducir significativamente la carga de la gestión de activos físicos para los clientes en aquellas cargas de trabajo que están alojadas en AWS. El cliente aún sería responsable de mantener inventarios de activos físicos para los equipos que se mantienen en su entorno (por ejemplo, centros de datos, oficinas, IoT implantado, personal móvil, etc.). La segunda ventaja es la capacidad de lograr una mayor visibilidad y un inventario de activos para los activos lógicos alojados en la cuenta de AWS de un cliente. Esto puede parecer un poco exagerado, pero se hace evidente rápidamente ya que no importa si una instancia EC2 (servidor virtual) está activada o desactivada, si el agente del punto de enlace está instalado y en funcionamiento, el segmento de red en el que esté activo ni cualquier otro factor. Ya sea utilizando la consola de AWS como una interfaz visual de fácil uso, a través de la interfaz de línea de comandos (CLI) o la interfaz programable de aplicaciones (API), los clientes pueden consultar y ver los activos de servicio de AWS. Esto reduce la carga de inventario del cliente a qué software instala en sus instancias EC2 y qué activos de datos almacena en AWS. AWS también tiene servicios que pueden realizar esta función, como Amazon Macie,[10] que puede identificar, clasificar, etiquetar y aplicar reglas a los datos almacenados en Amazon S3.

Una empresa que comprende su misión, a sus accionistas y sus actividades puede utilizar varios servicios de AWS para automatizar procesos, asignar riesgos empresariales a los sistemas de TI y gestionar las funciones de los usuarios. Por ejemplo, Identity and Access Management (IAM) se puede utilizar para asignar funciones de acceso basados en las funciones empresariales para las personas y los servicios. El uso de etiquetas para los servicios y los datos se puede utilizar para priorizar las tareas automáticas e incluir decisiones de riesgo predeterminadas o controles para que una persona evalúe los datos presentados y decida qué dirección debe tomar el sistema.

---

9 https://www.cisecurity.org/controls/

10 https://aws.amazon.com/macie/?sc_channel=PS&sc_campaign=acquisition_USsc_publisher=google&sc_medium=ACQ-P%7CPS-GO%7CBrand%7CDesktop%7CSU%7CSecurity%7CMacie%7CUS%7CEN%7CText&sc_content=macie_e&sc_detail=aws%20macie&sc_category=Security&sc_segment=293651803573&sc_matchtype=e&sc_country=US&s_kwcid=AL!4422!3!293651803573!e!!g!!aws%20macie&ef_id=WMf1pwAAALNCC8Y3:20180918152026:s

La dirección es el "héroe anónimo" de la seguridad cibernética. Sienta las bases y establece el estándar de calidad para las personas, los procesos y la tecnología. AWS ofrece varios servicios y capacidades, como AWS IAM, AWS Organizations, AWS Config, AWS Systems Manager, AWS Service Catalog y otros que los clientes pueden utilizar para implementar, controlar y hacer cumplir la normativa. Los clientes pueden aprovechar el cumplimiento de AWS con más de 50 estándares como FedRAMP, ISO y PCI DSS[11]. AWS ofrece información sobre su programa de riesgos y conformidad para permitir que los clientes incorporen los controles de AWS en su marco directivo. Esta información puede ayudar a los clientes a documentar un marco de control y dirección completo con AWS incluido como una parte importante de ese marco. Los servicios como Amazon Inspector identifican vulnerabilidades técnicas que se pueden incorporar en una posición de riesgo y un proceso de gestión.[12] La visibilidad mejorada que ofrece la nube aumenta la precisión de la posición de riesgo de un cliente, lo cual permite tomar decisiones relacionadas con el riesgo en datos más importantes.

## Responsabilidad de AWS

AWS mantiene una estricta gestión en el control de acceso al proporcionar solo acceso e información del centro de datos a los empleados y contratistas que tienen una necesidad empresarial legítima de recibir dichos privilegios. Cuando un empleado ya no tiene dicha necesidad empresarial de tales privilegios, su acceso se revoca inmediatamente, incluso si continúa siendo empleado de Amazon o de Amazon Web Services. Todo el acceso físico a los centros de datos por parte de los empleados de AWS se registra y audita de forma rutinaria. Los controles establecidos limitan el acceso a los sistemas y los datos y permiten que el acceso a los sistemas o los datos se dé de un modo restringido y controlado. Además, los datos del cliente y las instancias del servidor están aislados de forma lógica de otros clientes de manera predeterminada. El control de acceso de usuarios privilegiados es revisado por un auditor independiente durante las auditorías de AWS SOC 1, ISO 27001, PCI y FedRAMP.

Las actividades de gestión de riesgos de AWS incluyen nuestro ciclo de vida de desarrollo de sistemas (SDLC, por sus siglas en inglés), que incorpora las mejores prácticas de la industria y revisiones formales del diseño por parte del equipo de seguridad de AWS, el modelado de amenazas y la finalización de una evaluación de riesgos. Además, el entorno de control de AWS está sujeto a evaluaciones periódicas de riesgo internas y externas. AWS colabora con organismos de certificación externos y auditores independientes para revisar y probar el entorno de control general de AWS.

La administración de AWS ha desarrollado un plan empresarial estratégico que incluye la identificación de riesgos y la implementación de controles para mitigar o gestionar los mismos. La gestión de AWS vuelve a evaluar el plan empresarial estratégico al menos dos veces al año. Este proceso requiere que la administración identifique los riesgos dentro de sus áreas de responsabilidad y que implemente medidas apropiadas diseñadas para abordar esos riesgos. Además, el entorno de control de AWS está sujeto a varias evaluaciones de riesgos internas y externas. Los equipos de conformidad y seguridad de AWS han establecido un marco y políticas de la seguridad de la información basados en el marco de los objetivos de control para la tecnología de la información (COBIT, por sus siglas en inglés) y han integrado eficazmente la ISO 27001 en base a un marco certificable

11 La norma de seguridad de datos para la industria de tarjetas de pago (también denominada PCI DSS) es una norma de seguridad de la información patentada y administrada por el Consejo de normas de seguridad PCI https://www.pcisecuritystandards.org/), fundada por American Express, Discover Financial Services, JCB International, MasterCard Worldwide y Visa Inc. La PCI DSS se aplica a todos los organismos que almacenan, procesan o transmiten datos del titular de la tarjeta (CHD) y/o datos de autenticación confidencial (SAD), incluyendo comerciantes, procesadores, adquirentes, emisores y proveedores de servicios.

12 https://aws.amazon.com/inspector/?sc_channel=PS&sc_campaign=acquisition_USsc_publisher=google&sc_medium=ACQ- P%7CPS-GO%7CBrand%7CDesktop%7CSU%7CSecurity%7CInspector%7CUS%7CEN%7CText&sc_content=aws_inspector_e&sc_detail=aws%20inspector&sc_category=Security&sc_segment=293647559947&sc_matchtype=e&sc_country=US&s_kwcid=AL!4422!3!293647559947!e!!g!!aws%20inspector&ef_id=WMf1pwAAALNCC8Y3:20180918153103:s

sobre controles de la ISO 27002, principios de servicios fiduciarios del Instituto Americano de Contables Públicos Certificados (AICPA, por sus siglas en inglés), el PCI DSS v3.2 y la publicación 800-53 Rev del Instituto Nacional de Normas y Tecnología (NIST, por sus siglas en inglés) 4 (controles de seguridad recomendados para los sistemas de información federales). AWS mantiene la política de seguridad, ofrece formación de seguridad a los empleados y realiza revisiones de seguridad de la aplicación. Estas revisiones evalúan la confidencialidad, la integridad y la disponibilidad de los datos, así como el cumplimiento con la política de seguridad de la información. AWS Security analiza regularmente todas las direcciones IP de punto de enlace del servicio con acceso a Internet para detectar vulnerabilidades (estos análisis no incluyen las instancias de los clientes). AWS Security se lo notifica a las partes apropiadas para que subsanen cualquier vulnerabilidad que se haya detectado. Además, las empresas de seguridad independientes realizan evaluaciones externas de amenazas de vulnerabilidad. Los hallazgos y las recomendaciones resultantes de estas evaluaciones se clasifican y se entregan a los directivos de AWS. Estos análisis se realizan para garantizar el correcto estado y la viabilidad de la infraestructura subyacente de AWS y no están destinados a reemplazar los análisis de vulnerabilidad que debe realizar el cliente para cumplir con sus requisitos de conformidad específicos.

AWS mantiene acuerdos formales con proveedores externos clave e implementa mecanismos apropiados de gestión de relaciones de acuerdo con su relación con la empresa. Los procesos de gestión de terceros de AWS son revisados por auditores independientes como parte de la conformidad continua de AWS con el SOC y la ISO 27001. En consonancia con los estándares ISO 27001, a los activos de hardware de AWS se les asigna un propietario y el personal de AWS hace un seguimiento y los controla con herramientas de gestión de inventario patentadas de AWS. El equipo de la cadena de suministro y adquisiciones de AWS mantiene relaciones con todos los proveedores de AWS. Consulte los estándares ISO 27001; anexo A, dominio 8 para obtener más información. AWS ha sido validado y certificado por un auditor independiente para confirmar el cumplimiento del estándar de certificación ISO 27001.

# Función del núcleo del CSF: Proteger

Esta sección analiza las seis categorías que conforman la función "Proteger": Control de acceso, concienciación y formación, seguridad de los datos, procesos y procedimientos de protección de la información, mantenimiento y tecnología
de protección. La sección también destaca las soluciones de AWS que puede aprovechar para cumplir con esta función. En el apéndice A puede encontrar una lista detallada de los servicios de AWS en "subcategorías" individuales y las declaraciones de responsabilidad del cliente y AWS.

**Subcategoría del núcleo del CSF para Proteger:**

**Gestión de identidad, autenticación y control de acceso (PR.AC):** El acceso a los activos físicos y lógicos y las instalaciones asociadas se limita a los usuarios, los procesos y los dispositivos autorizados, y se gestiona de forma consistente con el riesgo evaluado del acceso no autorizado a actividades y transacciones autorizadas.

**Concienciación y formación (PR.AT):** El personal y los socios de la empresa reciben formación sobre la concienciación de la seguridad cibernética y están capacitados para cumplir con sus deberes y responsabilidades relacionadas con la seguridad cibernética conforme a las políticas, los procedimientos y los acuerdos relacionados con la misma.

**Seguridad de los datos (PR.DS):** La información y los registros (datos) se gestionan de acuerdo con la estrategia de riesgos de la empresa para proteger la confidencialidad, la integridad y la disponibilidad de la información.

**Procesos y procedimientos de protección de la información (PR.IP):** Las políticas de seguridad (que abordan el objetivo, el alcance, las funciones, las responsabilidades, el compromiso de gestión y la coordinación entre las entidades de la empresa), los procesos y los procedimientos se mantienen y utilizan para gestionar la protección de los sistemas y activos de la información.

**Mantenimiento (PR.MA):** El mantenimiento y las reparaciones de los componentes del sistema de control e información industrial se realizan de acuerdo a políticas y procedimientos.

**Tecnología de protección (PR.PT):** Las soluciones de seguridad técnica se gestionan para garantizar la seguridad y la resistencia de los sistemas y los activos, de acuerdo con las políticas, los procedimientos y los acuerdos relacionados con los mismos.

## Responsabilidad del cliente

Para cumplir con los tres objetivos de seguridad de confidencialidad, integridad y disponibilidad, lo último puede ser muy difícil de conseguir en un entorno local con solo uno o dos centros de datos. Esta es una de las mayores ventajas de los proveedores de servicios en la nube a gran escala y, de AWS en concreto, debido a nuestra exclusiva
arquitectura de infraestructuras. Puede distribuir su aplicación a lo largo de múltiples zonas de disponibilidad (AZ), es decir, zonas de aislamiento lógico de fallas dentro de una región. Si cuenta con el diseño apropiado con una gestión optimizada de la capacidad y de las capacidades de autoescalado, su aplicación y sus datos no se verían afectados por una sola interrupción del centro de datos. Si aprovecha todas las AZ de una región (donde haya más de tres), es posible que la pérdida de dos centros de datos tampoco tenga ningún impacto en su aplicación. Del mismo modo, servicios como Amazon Simple Storage Service (S3) duplican automáticamente sus datos en al menos tres AZ de la región, para conseguir una disponibilidad garantizada del 99,99 % y una durabilidad de los datos del 99,999999999 %.

La confidencialidad se puede conseguir mediante el cifrado en reposo y el cifrado en tránsito utilizando los servicios de cifrado de AWS, como el cifrado Elastic Block Store (EBS), el cifrado S3, el cifrado transparente de bases de datos para RDS

SQL Server y RDS Oracle y VPN Gateway o utilizando su solución de cifrado actual. AWS admite el cifrado TLS/SSL para todos sus puntos de enlace de API y la capacidad de crear túneles VPN para proteger los datos en tránsito. AWS también ofrece Key Management Service, un servicio de gestión de claves, y dispositivos de módulos de seguridad de hardware específicos para cifrar los datos en reposo. Puede elegir proteger sus datos utilizando las capacidades ofrecidas por AWS o utilizar sus propias herramientas de seguridad.

La integridad se puede implementar de varias formas. Amazon CloudWatch y Amazon CloudTrail disponen de controles de integridad, los clientes pueden utilizar firmas digitales para llamadas y registros de API, se pueden emplear sumas de comprobación MD5 en Amazon S3 y también existen numerosas soluciones externas de nuestros socios. Amazon Config incluso contribuye a la integridad del entorno AWS del cliente al monitorizar los cambios.

Dentro del entorno AWS del cliente, los servicios de AWS como AWS IAM, AWS Cognito, AWS Single Sign-On (SSO), AWS Cloud Directory, AWS Directory Service y funciones tales como la autenticación multifactorial le permiten implementar, gestionar, proteger, controlar e informar sobre las identidades de los usuarios, los estándares de autenticación y los derechos de acceso.

Es su responsabilidad formar al personal y a los usuarios finales sobre las políticas y los procedimientos para gestionar su entorno. Para la formación técnica, AWS y nuestros socios de formación ofrecen una formación integral para ejercer varias funciones, como los arquitectos de soluciones, el personal de SysOps, los desarrolladores y los equipos de seguridad.[13].

## Responsabilidad de AWS

AWS emplea el concepto de privilegio mínimo, según el cual el acceso de los empleados se concede en función de las necesidades empresariales y las responsabilidades laborales y, además, proporciona acceso temporal en base a las funciones para solo aquellos recursos y datos requeridos en ese momento.

AWS ofrece acceso al centro de datos físico solo a los empleados autorizados. Todos los empleados que necesitan acceder al centro de datos deben primero solicitar el acceso y ofrecer una justificación empresarial válida. Estas solicitudes se otorgan en base al principio de privilegio mínimo, por el que se debe especificar en las solicitudes a qué nivel del centro de datos necesita acceder la persona y están limitadas en el tiempo. El personal autorizado revisa y aprueba las solicitudes y el acceso se anula al finalizar el tiempo solicitado. Una vez otorgada la admisión, las personas solo pueden acceder a las zonas especificadas en sus permisos.

El acceso de terceros se solicita a través de empleados autorizados de AWS, que deben solicitar acceso para terceros y proporcionar una justificación empresarial válida. Estas solicitudes se otorgan en base al principio de privilegio mínimo, por el que se debe especificar en las solicitudes a qué nivel del centro de datos necesita acceder la persona y están limitadas en el tiempo. Estas solicitudes las aprueba el personal autorizado y el acceso se revoca cuando finaliza el tiempo de la solicitud. Una vez otorgada la admisión , las personas solo pueden acceder a las zonas especificadas en sus permisos. Cualquier persona a la que se le conceda acceso mediante una identificación de visitante debe presentar una identificación al llegar al lugar y será registrada y escoltada por personal autorizado.

AWS ha implementado políticas y procedimientos formales y documentados de concienciación y formación para nuestros

13 Puede encontrar la formación en clase y en línea disponible en: https://aws.amazon.com/training. También hay varios libros que tratan muchos aspectos de AWS y que se pueden encontrar en https://www.amazon.com buscando “AWS”. Los documentos técnicos de AWS se pueden encontrar en: https://aws.amazon.com/whitepapers

empleados y contratistas que gestionan el objetivo, el alcance, las funciones, las responsabilidades, el compromiso en la gestión, la coordinación entre las entidades de la empresa y la conformidad.

Las certificaciones FedRAMP e ISO 27001 de AWS documentan en detalle las políticas y los procedimientos mediante los cuales AWS utiliza, gestiona, controla, autoriza, implementa, informa y controla todos los cambios en su entorno e infraestructura, así como la forma en que AWS ofrece respuestas ante la redundancia y las emergencias para su infraestructura física. Además, las certificaciones documentan en detalle la forma en que se autoriza, realiza, registra y revisa todo el mantenimiento remoto de los servicios de AWS para evitar el acceso no autorizado. También abordan la forma en que AWS sanea los medios y destruye los datos. AWS utiliza productos y procedimientos que cumplen con las directrices de publicación especial del NIST 800-88 para el saneamiento de los medios. También es responsable de preparar las políticas, los procesos y los procedimientos para la protección de datos.

Para cumplir con los requisitos de facturación y mantenimiento, los activos de AWS se asignan a un propietario, se realiza un seguimiento y se controlan con herramientas de gestión de inventario patentadas de AWS. Los procedimientos de mantenimiento del propietario de activos de AWS se realizan con una herramienta patentada con verificaciones específicas que deben completarse de acuerdo con el programa de mantenimiento documentado. Los auditores externos prueban los controles de gestión de activos de AWS al validar que el propietario del activo está documentado y que la condición de los activos se inspecciona visualmente de acuerdo con la política de gestión de activos documentada.

Los servicios de AWS también pueden mejorar significativamente la gestión y el mantenimiento de los sistemas de nuestros clientes. En primer lugar, y en base a la infraestructura de AWS que se analizó antes con las zonas de disponibilidad (AZ), la aplicación que fue diseñada para una alta disponibilidad en múltiples AZ permite separar las actividades de mantenimiento. Puede disponer de activos en AZ sin conexión para su mantenimiento sin afectar el rendimiento de la aplicación en general, ya que los activos duplicados en las otras AZ aumentan y recuperan la carga. El mantenimiento se puede realizar con una AZ a la vez y se puede automatizar con paradas e informes cuando sea necesario. Además, se pueden pasar arquitecturas completas de un entorno DevTest (azul) a un entorno de operaciones (verde), y viceversa, según el método deseado.

# Función del núcleo del CSF: Detectar

Esta sección analiza las tres categorías que conforman la función "Detectar": Anomalías y eventos, control continuo de seguridad y procesos de detección. Resumimos las soluciones clave de AWS que puede aprovechar para cumplir con esta función. En el apéndice A puede encontrar una lista detallada de los servicios de AWS en "subcategorías" individuales y las declaraciones de responsabilidad del cliente y AWS.

**Subcategoría del núcleo del CSF para Detectar:**

**Anomalías y Eventos (DE.AE):** La actividad anómala se detecta de forma oportuna y se comprende el posible impacto de los eventos.

**Control continuo de la seguridad (DE.CM):** El sistema de información y los activos se controlan en intervalos discretos para identificar eventos de la seguridad cibernética y verificar la efectividad de las medidas de protección.

**Procesos de detección (DE.DP):** Los procesos y los procedimientos de detección se gestionan y se prueban para garantizar un conocimiento oportuno y adecuado de los eventos anómalos.

## Responsabilidad del cliente

La capacidad de recopilar, sintetizar y alertar sobre eventos relevantes para la seguridad es fundamental para cualquier programa de gestión de riesgos de seguridad cibernética. La naturaleza de la tecnología de nube basada en API ofrece un nuevo nivel de visibilidad y automatización que no era posible anteriormente. Con cada acción realizada y convertida en uno o más registros de auditoría, AWS proporciona una gran cantidad de información sobre la actividad disponible para los clientes dentro de su estructura de cuentas. Sin embargo, el volumen de datos puede presentar sus propios desafíos. Encontrar la famosa "aguja en el pajar" es un problema real, pero la capacidad y las capacidades que proporciona la nube son adecuadas para resolver estos desafíos. Con la infraestructura del procesamiento de registros, la automatización y el análisis de datos adecuados, es posible lograr una detección y respuesta casi en tiempo real para eventos críticos mientras se filtran falsos positivos y riesgos bajos/aceptados.

AWS tiene varios servicios que pueden utilizarse como parte de una estrategia integral de operaciones de seguridad para el control continuo y la detección de amenazas. En el nivel básico, hay servicios como AWS CloudTrail14 para registrar todas las llamadas API, donde los registros pueden firmarse y cifrarse digitalmente y luego almacenarse en un bucket seguro de Amazon S3. Los registros de flujo de Virtual Private Cloud (VPC)15 controlan toda la actividad de la red que entra y sale de su VPC. También está Amazon CloudWatch16, que controla el entorno de AWS y genera alertas similares a un sistema de gestión de eventos de información de seguridad (SIEM), y puede ser tomado en el SIEM local de un cliente.

También hay otros servicios avanzados como Amazon GuardDuty17 que relaciona la actividad dentro de su entorno de AWS con la inteligencia procedente de amenazas de múltiples fuentes que ofrece un contexto de riesgo adicional y detección de anomalías. Amazon Macie es otro servicio avanzado que puede identificar datos confidenciales, clasificarlos y etiquetarlos, así como rastrear su ubicación y su acceso. Algunos clientes pueden incluso optar por aprovechar los servicios de inteligencia artificial (AI) y de aprendizaje automático (ML) de AWS para modelar y analizar los datos del registro.

## Responsabilidad de AWS

AWS proporciona alertas casi en tiempo real cuando las herramientas de control de AWS muestran indicaciones de compromiso o posible compromiso, en función de los mecanismos de alarma de umbral determinados por el servicio de AWS y los equipos de seguridad.
AWS relaciona la información obtenida de los sistemas de control lógico y físico para mejorar la seguridad en función de sus necesidades. Tras la evaluación y el descubrimiento del riesgo, Amazon desactiva las cuentas que muestran un uso atípico que se ajusta a las características de los malos actores.

Los empleados de AWS están formados para reconocer los presuntos incidentes de seguridad y saber dónde informar sobre los mismos. Cuando es apropiado, los incidentes se denuncian a las autoridades correspondientes. AWS mantiene la página web del boletín de seguridad de AWS18 para notificar a los clientes sobre eventos de privacidad y seguridad que afecten a los servicios de AWS. Los clientes pueden registrarse en

14 https://aws.amazon.com/cloudtrail/

15 https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs.html

16 https://aws.amazon.com/cloudwatch/?sc_channel=PS&sc_campaign=acquisition_USsc_publisher=google&sc_medium=ACQ-P%7CPS-GO%7CBrand%7CDesktop%7CSU%7CManagement%20Tools%7CCloudWatch%7CUS%7CEN%7CText&sc_content=cloudwatch_e&sc_detail=aws%20cloudwatch&sc_category=Management%20Tools&sc_segment=293615620998&sc_matchtype=e&sc_country=US&s_kwcid=AL!4422!3!293615620998!e!!g!!aws%20cloudwatch&ef_id=WMf1pwAAALNCC8Y3:20180918153820:s

17 https://aws.amazon.com/guardduty/

18 https://aws.amazon.com/security/security-bulletins

Boletín de seguridad de la fuente RSS para mantenerse al tanto de los anuncios de seguridad en la página web del boletín de seguridad. El equipo de atención al cliente mantiene una web con el panel de estado del servicio[19] para alertar a los clientes sobre cualquier problema de disponibilidad que tenga una gran incidencia.

# Función del núcleo del CSF: Responder

Esta sección analiza las cinco categorías que conforman la función "Responder": Planificación de respuestas, comunicaciones, análisis, mitigación y mejoras. También resumimos las soluciones clave de AWS que puede utilizar para cumplir con esta función. En el apéndice A puede encontrar una lista detallada de los servicios de AWS en "subcategorías" individuales y las declaraciones de responsabilidad del cliente y AWS.

**Subcategoría del núcleo del CSF para Responder:**

**Planificación de respuestas (RS.RP):** Los procesos y los procedimientos de respuestas se ejecutan y mantienen para garantizar una respuesta oportuna a los eventos de seguridad cibernética detectados.

**Mitigación (RS.MI):** Los actividades se realizan para evitar la expansión de un evento, mitigar sus efectos y erradicar un incidente.

**Comunicaciones (RS.CO):** Las actividades de respuesta se coordinan con las partes interesadas internas y externas para, cuando sea adecuado, incluir la asistencia externa de las fuerzas del orden.

**Análisis (RS.AN):** El análisis se realiza para asegurar una respuesta adecuada y apoyar las actividades de recuperación.

**Mejoras (RS.IM):** Las actividades de respuesta organizativa mejoran al incorporar las lecciones aprendidas de las actividades de detección/respuesta actuales y anteriores.

## Responsabilidad del cliente

Es fundamental el tiempo que pasa entre la detección y la respuesta. Los planes de respuesta repetibles y bien ejecutados minimizan la exposición y aceleran la recuperación. La automatización habilitada por la nube permite la implementación de libros de tácticas sofisticados como códigos con tiempos de respuesta mucho más rápidos.

Al simplemente etiquetar una instancia de Amazon EC2, por ejemplo, la automatización puede aislar la instancia, tomar una instantánea forense, instalar herramientas de análisis, conectar la instancia sospechosa a una estación de trabajo forense y abrir una incidencia a un analista de seguridad cibernética. Las capacidades enumeradas a continuación facilitan la creación de procesos automatizados para agregar velocidad y consistencia a los procesos de respuesta ante incidentes. Además, estas herramientas le permiten mantener un historial de las comunicaciones para su uso en una revisión posterior al evento.

A pesar de que la nube ofrece capacidades para agilizar y acelerar la recopilación y difusión de información, siempre hay un elemento humano involucrado en la coordinación de la respuesta. El análisis de la seguridad cibernética requiere un proceso de investigación, análisis forense y comprensión del incidente. Estos necesariamente requieren algún nivel de interacción humana. Aunque los servicios de AWS no proporcionan análisis de incidentes directos, sí brindan servicios para ayudarle a ejecutar un proceso formalizado y evaluar la amplitud del impacto.

19 http://status.aws.amazon.com/

## Responsabilidad de AWS

AWS ha implementado una política y un programa formales y documentados de respuesta ante incidentes. La política aborda el objetivo, el alcance, las funciones, las responsabilidades y el compromiso de la administración.

AWS utiliza un enfoque trifásico para gestionar los incidentes:

1. Fase de activación y notificación
2. Fase de recuperación
3. Fase de reconstitución

Para garantizar la efectividad del plan de gestión de incidentes de AWS, AWS realiza pruebas de respuesta ante incidentes. Estas pruebas proporcionan una excelente cobertura para el descubrimiento de defectos y modos de fallos previamente desconocidos. Además, permite a los equipos de seguridad y servicios de Amazon probar los sistemas para detectar el posible impacto en el cliente y preparar aún más al personal para gestionar los incidentes como la detección y el análisis, la contención, la erradicación, la recuperación y las actividades posteriores al incidente.

El plan de prueba de respuesta ante incidentes se ejecuta anualmente, junto con el plan de respuesta ante incidentes. Los auditores externos revisan la planificación, las pruebas y los resultados de las pruebas de la gestión de incidentes de AWS.

# Función del núcleo del CSF: Recuperar

Esta sección analiza las tres categorías que conforman la función "Recuperar": Planificación de la recuperación, mejoras y comunicaciones. También resumimos las soluciones clave de AWS que puede utilizar para cumplir con esta función. En el apéndice A puede encontrar una lista detallada de los servicios de AWS en "subcategorías" individuales y las declaraciones de responsabilidad del cliente y AWS.

**Subcategoría del núcleo del CSF para Recuperar:**

**Planificación de la recuperación (RC.RP):** Los procesos y los procedimientos de recuperación se ejecutan y mantienen para garantizar la restauración oportuna de los sistemas o activos afectados por eventos de seguridad cibernética.

**Mejoras (RC.IM):** La planificación y los procesos de recuperación se mejoran al incorporar las lecciones aprendidas en actividades futuras.

**Comunicaciones (RC.CO):** Las actividades de restauración se coordinan con partes internas y externas, como centros coordinadores, proveedores de servicios de Internet, propietarios de sistemas de ataque, víctimas, otros CSIRT y vendedores.

## Responsabilidad del cliente

Los clientes son responsables de planificar, probar y realizar operaciones de recuperación para sus aplicaciones y datos, así como para mantener la continuidad de su negocio. La causa de un apagón puede provenir de muchas fuentes diferentes. Los servicios de AWS ofrecen muchas capacidades avanzadas de autorreparación y recuperación automática. El uso, por ejemplo, de grupos de escalado automático en múltiples zonas de disponibilidad permite que la infraestructura controle el estado de las instancias EC2

y cambiar rápidamente una instancia fallida con una nueva imagen de máquina de Amazon (AMI). Además, el uso de Amazon CloudWatch, AWS Lamda y otros servicios/capacidades de servicio pueden automatizar las acciones de recuperación para que incluya todo, desde la implementación de un entorno y una aplicación de AWS completos, hasta la conmutación por error a otra región de AWS, restaurar los datos desde copias de seguridad y mucho más.

Por último, las acciones que implican relaciones públicas, la gestión de la reputación y la comunicación de las actividades de recuperación corresponden a la forma en que la empresa gestiona el evento que afectó a su entorno y que, en este caso, es el cliente.

## Responsabilidad de AWS

La infraestructura resistente de AWS, la automatización fiable, los procesos disciplinados y las personas excepcionales pueden recuperarse de los eventos muy rápidamente y con una interrupción mínima (en caso de haberla) para nuestros clientes.

El plan de continuidad del negocio de AWS detalla el enfoque de tres fases que AWS ha desarrollado para recuperar y reconstituir la infraestructura de AWS:

- Fase de activación y notificación
- Fase de recuperación
- Fase de reconstitución

Este enfoque garantiza que AWS realice los esfuerzos de recuperación y reconstitución del sistema en una secuencia metódica, maximizando la efectividad de los esfuerzos de recuperación y reconstitución, así como minimizando el tiempo de interrupción del sistema debido a errores y omisiones.

AWS mantiene un entorno de control de seguridad universal que se aplica en todas las regiones. Todos los centros de datos han sido construidos en base a estándares físicos, ambientales y de seguridad en una configuración activa-activa, empleando un modelo de redundancia n+1 para garantizar la disponibilidad del sistema en caso de fallo de un componente. Los componentes (N) tienen al menos un componente de copia de seguridad independiente (+1), por lo que el componente de copia de seguridad está activo en la operación, incluso si todos los demás componentes son completamente funcionales. Para eliminar puntos únicos de fallo, este modelo se aplica en todo AWS, incluyendo la implementación de centros de datos y redes. Todos los centros de datos están en línea y están atendiendo al tráfico; ningún centro de datos está "frío". En caso de fallo, hay suficiente capacidad para permitir que el tráfico se equilibre con la carga en los sitios restantes.

# Cumplimiento de los servicios de AWS con el CSF

AWS evaluó el cumplimiento de nuestros servicios en la nube con el CSF para demostrar la "seguridad de la nube". En un mundo cada vez más interconectado, la aplicación de prácticas sólidas de gestión de riesgos de seguridad cibernética para cada sistema interconectado y para proteger la confidencialidad, la integridad y la disponibilidad de los datos es una necesidad. Nuestros clientes del sector público y privado esperan que utilicemos la mejor seguridad posible para proteger nuestros servicios en la nube y los datos procesados y almacenados en esos sistemas. Para proteger de una forma efectiva los datos y los sistemas en hiperescala, la seguridad no puede ser un último recurso, sino una parte integral de la gestión del ciclo de vida de nuestros sistemas. Esto significa que la seguridad comienza en la fase 0 (es decir, la concepción de los sistemas) y se suministra continuamente como parte inherente de nuestro modelo de prestación de servicios.

Según lo validado por nuestro asesor externo, las soluciones de AWS disponibles hoy para nuestros clientes del sector público y comercial cumplen con el CSF del NIST. Cada uno de estos servicios mantiene una acreditación actual según la FedRAMP Moderate y/o la ISO 27001. Al implementar las soluciones de AWS, las empresas pueden tener la seguridad de que los servicios de AWS mantienen las mejores prácticas de gestión de riesgos definidas en el CSF y pueden aprovechar estas soluciones para su propio cumplimiento del CSF.

AWS ejerce un enfoque riguroso y basado en la prevención de riesgos para la seguridad de nuestros servicios y la protección de los datos del cliente. Aplicamos nuestro propio proceso interno de garantía de seguridad para nuestros servicios, que evalúa la efectividad de los controles administrativos, técnicos y operativos necesarios para protegernos contra las amenazas de seguridad actuales y emergentes que afectan a la capacidad de recuperación de nuestros servicios. Los proveedores de servicios de la nube comercial a gran escala, como AWS, ya están sujetos a requisitos de seguridad sólidos en forma de certificaciones de seguridad específicas del sector, nacionales e internacionales (por ejemplo, FedRAMP, ISO 27001, PCI DSS, SOC , etc.) que abordan suficientemente las preocupaciones de riesgo identificadas por los clientes del sector público y privado en todo el mundo.

AWS adopta una seguridad alta en todos nuestros servicios basados en un enfoque de "marca de agua alta" para todos nuestros clientes. Esto significa que tomamos el nivel más alto de clasificación de los datos que se transfieren y almacenan en nuestros servicios en la nube y aplicamos esos mismos niveles de protección a todos nuestros servicios y para todos nuestros clientes. A continuación, estos servicios se ponen en cola para su certificación según el listo de conformidad más exigente, por lo que los clientes se benefician de niveles elevados de protección para los datos de los clientes procesados y almacenados en nuestra nube. Según ha validado nuestro asesor externo, las soluciones de AWS disponibles hoy para nuestros clientes del sector público y comercial cumplen con el núcleo del CSF. Cada uno de estos servicios mantiene una acreditación actual según la FedRAMP Moderate y/o la ISO 27001. Al implementar las soluciones de AWS, las empresas pueden tener la seguridad de que los servicios de AWS mantienen las mejores prácticas de gestión de riesgos definidas en el CSF y pueden aprovechar estas soluciones para su propio cumplimiento del CSF. Consulte el apéndice B para ver la carta de acreditación externa.

# Conclusión

Las entidades del sector público y privado reconocen el valor en cuanto a la seguridad en la adopción del CSF del NIST en sus entornos. En particular, las agencias federales de los EE. UU. están obligadas a cumplir con sus prácticas de informes y gestión de riesgos de la seguridad cibernética en el CSF. Como los gobiernos estatales y locales de los EE. UU., los gobiernos que no pertenecen a los EE. UU., los operadores de infraestructuras críticas y las empresas comerciales evalúan su propio cumplimiento del CSF y necesitan las herramientas y soluciones adecuadas para lograr un sistema seguro y compatible y evaluar su posicionamiento en cuanto a los riesgos de su organización.

Puede fortalecer su posicionamiento en cuanto a seguridad cibernética al aprovechar AWS como parte de la tecnología de su empresa para crear soluciones automatizadas, innovadoras y seguras para lograr resultados en materia de seguridad de acuerdo con el CSF. Conseguirá un nivel adicional de seguridad con la garantía de que los servicios de AWS también emplean prácticas de gestión de riesgos sólidas identificadas en el CSF y que han sido validadas por un asesor externo.

# Apéndice A: servicios de AWS y matriz de responsabilidad del cliente para el cumplimiento con el CSF

Las hojas de cálculo de la Matriz de responsabilidades del cliente y de los servicios de AWS para adaptarse al CSF ayudan a los clientes a evaluar su nivel de cumplimiento del CSF del NIST. Esta hoja de cálculo se encuentra en la pestaña Guías y libros de ejercicio dentro de la sección Recursos del sitio web de Cumplimiento de AWS.

# Apéndice B: validación del asesor externo

19 de septiembre del 2018
Amazon Web Services
A/A: Jennifer Gray
Seguridad – Estrategia de crecimiento | Dirección
Directora, Diseño de servicio

Kratos SecureInfo
14130 Sullyfield Circle,
Suite H
Chantilly, VA 20151
Tel.: (+1) 888 677 9351
www.kratossecureinfo.com

Estimada Sra. Gray:
Siguiendo sus órdenes, asumí la tarea de revisar los requisitos establecidos en el Marco de la seguridad cibernética (CSF) del Instituto Nacional de Normas y Tecnología (NIST), versión 1.1, con fecha del 16 de abril del 2018, y analicé los requisitos descritos en el Texto de función y regulación del CSF del NIST en relación con AWS y las arquitecturas de referencia de computación en la nube asociadas. Estos requisitos fueron implementados con los requisitos de control de seguridad establecidos por el NIST, documentados en la publicación especial del NIST (SP) 800-53.

Para mi revisión, validé la elaboración de las citaciones del CSF del NIST en base a los requisitos del control de seguridad SP 800-53 del NIST. Además, revisé los servicios de AWS que se han sometido a las acreditaciones de la FedRAMP Moderate y la ISO 9001/27001/27017/27018 que cumplen con el requisito de citación o control disponible para que los clientes lo puedan implementar. Durante la validación del servicio, identifiqué citaciones adicionales que pueden tener servicios de alcance disponibles que cumplen con el requisito. Todos los servicios recomendados para su inclusión se validaron como parte del alcance de las certificaciones de la FedRAMP Moderate y la ISO de AWS.

Los resultados del análisis revelaron que, a pesar de no ser obligatorio como marco de cumplimiento particular en este momento, AWS ha cumplido con la intención de estas citaciones a través de los servicios de AWS que incluyeron la FedRAMP y la ISO.

Basándonos en mi análisis del libro de trabajo de elaboración del núcleo del CSF desarrollado por AWS y nuestra comprensión del entorno de AWS, Kratos Secureinfo considera que AWS ha demostrado adecuadamente su cumplimiento del CSF del NIST a través de la implementación de los controles de seguridad de la FedRAMP y la ISO correspondientes.

Si tiene alguna duda en relación con la revisión del diseño que he realizado, póngase en contacto conmigo directamente en el (+1) 571 308 3397 o por correo electrónico:
Emily.Cummins@KratosSecureinfo.com

Atentamente, Emily Cummins
Asesora de seguridad principal
Kratos SecureInfo