Marco de adopción de la nube de AWS

Perspectiva de seguridad

Junio de 2016

Avisos

Este documento se ofrece solo con fines informativos. Representa la oferta actual de productos y prácticas de AWS a partir de la fecha de publicación de este documento. Dichas prácticas y productos pueden modificarse sin previo aviso. Los clientes son responsables de realizar sus propias evaluaciones independientes de la información contenida en este documento y de cualquier uso de los productos o servicios de AWS, cada uno de los cuales se ofrece “tal cual”, sin garantía de ningún tipo, ya sea explícita o implícita. Este documento no genera ninguna garantía, declaración, compromiso contractual, condición ni certeza por parte de AWS, sus filiales, proveedores o licenciantes. Las responsabilidades y obligaciones de AWS con respecto a sus clientes se controlan mediante los acuerdos de AWS y este documento no forma parte ni modifica ningún acuerdo entre AWS y sus clientes.

Contenido

Resumen 4
Introducción 4
Beneficios de seguridad de AWS 6
Diseñada para la seguridad 6
Altamente automatizada 7
Altamente disponible 7
Altamente acreditada 8
Componente directivo 8
Consideraciones 10
Componente preventivo 11
Consideraciones 12
Componente de detección 12
Consideraciones 13
Componente reactivo 14
Consideraciones 15
Realizar el viaje: definición de una estrategia 15
Consideraciones 18
Realizar el viaje: presentación de un programa 19
Las cinco principales 20
Ampliación de las epopeyas principales 22
Serie de sprints de ejemplo 24
Consideraciones 26
Realizar el viaje: desarrollo de operaciones de seguridad robustas 26
Conclusión 27
Apéndice A: Seguimiento del progreso de la perspectiva de seguridad del CAF de AWS 28
Habilitadores de seguridad clave 28
Modelo de progreso de epopeyas de seguridad 29
Taxonomía y terminología de CAF 32
Notas 32

Resumen

El marco de adopción de la nube[1] (CAF, Cloud Adoption Framework) de Amazon Web Services (AWS) proporciona pautas para coordinar las diferentes partes de las organizaciones que se van a migrar a la informática en la nube. Las pautas del CAF se desglosan en varias áreas de enfoque relevantes para la implementación de sistemas de TI basados en la nube. Estas áreas de enfoque reciben el nombre de *perspectivas*, y cada perspectiva se divide en *componentes*. Cada una de las siete perspectivas del CAF tiene su propio documento técnico.

En este documento técnico se analiza la perspectiva de seguridad, centrada en incorporar pautas y procesos para sus controles de seguridad existentes específicos para el uso de AWS en su entorno.

Introducción

La seguridad en AWS no requiere ninguna tarea. Todos los clientes de AWS se benefician de una arquitectura de red y un centro de datos diseñados para satisfacer los requisitos de seguridad de las organizaciones más exigentes. AWS y sus socios ofrecen cientos de herramientas y funciones para ayudarle a satisfacer sus objetivos de seguridad relacionados con la visibilidad, auditabilidad, capacidad de control y agilidad. Esto significa que puede disponer de la seguridad que necesita, pero sin desembolsos de capital y con mucha menos sobrecarga operativa que en un entorno local.

Figura 1: Perspectiva de seguridad del CAF de AWS

El objetivo de la perspectiva de seguridad es ayudarle a estructurar la selección e implementación de los controles adecuados para su organización. Como se muestra en la figura 1, los componentes de la perspectiva de seguridad organizan los principios que ayudarán a impulsar la transformación de la cultura de seguridad de su organización. En este documento se analizan las medidas específicas que puede adoptar para cada componente y la manera de medir el progreso:

- **Controles directivos**: estos controles establecen los modelos de gobierno, riesgo y conformidad en los que operará el entorno.
- **Controles preventivos**: son los controles que protegen sus cargas de trabajo y mitigan las amenazas y vulnerabilidades.
- **Controles de detección**: son controles que proporcionan visibilidad y transparencia completas sobre el funcionamiento de sus implementaciones en AWS.
- **Controles reactivos**: son controles diseñados para remediar las desviaciones posibles del marco de referencia de seguridad.

La seguridad en la nube es un concepto conocido. El aumento de la agilidad y de la capacidad de realizar acciones más rápidamente, a gran escala y a menor costo, no invalida los principios consolidados de la seguridad de la información.

Después de analizar los cuatros componentes de la perspectiva de seguridad, este documento técnico le mostrará los pasos que puede realizar en su viaje hacia la nube para garantizar que su entorno mantiene unos cimientos sólidos en materia de seguridad:

- Defina una **estrategia de seguridad** en la nube. Cuando inicie su viaje, contemple los objetivos empresariales de su organización, el enfoque de la administración de riesgos y el nivel de oportunidad que ofrece la nube.
- Presente un **programa de seguridad** para el desarrollo e implementación de las funcionalidades de seguridad, privacidad, conformidad y gestión de riesgos. Como el ámbito de este programa puede parecer en principio muy extenso, es importante que cree una estructura que permita a su organización abordar globalmente la seguridad en la nube. La implementación debería permitir un desarrollo iterativo para que las funcionalidades maduren conforme se desarrollan los programas. Esto permitirá convertir el componente de seguridad en un catalizador para el resto de las tareas de adopción de la nube de la organización.

- Desarrolle capacidades de **operaciones de seguridad** robustas que maduren y mejoren continuamente. El viaje de la seguridad continúa con el tiempo. Es recomendable que combine el rigor de las operaciones con la creación de nuevas capacidades, para que la iteración constante aporte mejoras continuas.

Beneficios de seguridad de AWS

La seguridad en la nube de AWS es la mayor prioridad. Como cliente de AWS, se beneficiará de una arquitectura de red y un centro de datos diseñados para satisfacer los requisitos de seguridad de las organizaciones más exigentes.

Una ventaja de la nube de AWS es que permite a los clientes escalar e innovar, manteniendo al mismo tiempo un entorno seguro. Los clientes pagan por los servicios que usan, lo que significa que puede disponer de la seguridad que necesita, pero sin gastos iniciales y a un costo menor que en un entorno local.

En esta sección se analizan algunos de los beneficios de seguridad de la plataforma de AWS.

Diseñada para la seguridad

La infraestructura de la nube de AWS se opera en centros de datos de AWS y se ha diseñado para satisfacer los requisitos de nuestros clientes más exigentes con la seguridad. La infraestructura de AWS se ha diseñado para proporcionar una alta disponibilidad, pero también con medidas de seguridad robustas para proteger la privacidad de los clientes. Todos los datos se almacenan en centros de datos de AWS con un alto nivel de seguridad. Los firewalls de red integrados en Amazon VPC y las capacidades de firewall de las aplicaciones web de AWS WAF le permiten crear redes privadas y controlar el acceso a sus instancias y aplicaciones.

Cuando implemente sistemas en la nube de AWS, AWS le ayudará compartiendo las responsabilidades de seguridad con usted. AWS diseña la infraestructura subyacente con principios de diseño seguro, y los clientes pueden implementar su propia arquitectura de seguridad para las cargas de trabajo implementadas en AWS.

Altamente automatizada

En AWS creamos herramientas de seguridad con un propósito específico y las adaptamos a nuestro entorno, tamaño y requisitos globales únicos. La creación de herramientas de seguridad desde cero permite a AWS automatizar muchas de las tareas rutinarias a las que los expertos de seguridad dedican normalmente su tiempo. Esto significa que los expertos de seguridad de AWS pueden emplear más tiempo en aplicar medidas para aumentar la seguridad de su entorno en la nube de AWS. Los clientes también automatizan las funciones de diseño y operaciones mediante un conjunto completo de API y herramientas. La gestión de identidad, la seguridad de la red, la protección de los datos y las capacidades de monitorización pueden automatizarse en su totalidad e implementarse mediante métodos de desarrollo de software conocidos que ya utiliza.Los clientes adoptan un enfoque automatizado para responder a los problemas de seguridad. Al automatizar la seguridad mediante los servicios de AWS, en lugar de tener empleados monitorizando su posición de seguridad y reaccionando a un evento, su sistema puede monitorizar, revisar e iniciar una respuesta.

Altamente disponible

AWS tiene centros de datos en varias regiones geográficas. En las regiones, existen varias zonas de disponibilidad para proporcionar capacidad de recuperación. AWS diseña los centros de datos con ancho de banda de sobra, por lo que si se produce una interrupción grave, se dispone de suficiente capacidad para equilibrar la carga de tráfico y dirigirla a los demás sitios, con el fin de minimizar la repercusión en nuestros clientes. Los clientes también utilizan esta estrategia de varias regiones y zonas de disponibilidad para crear aplicaciones muy resistentes sin apenas interrupciones, para replicar y crear backups de los datos fácilmente, y para implementar controles de seguridad globales de manera uniforme en toda la empresa.

Altamente acreditada

Los entornos de AWS se auditan continuamente, con certificaciones de entidades de acreditación de todo el mundo. Esto significa que los aspectos de su conformidad con las normativas ya están acreditados. Para obtener información adicional sobre las normas y regulaciones de seguridad que cumple AWS, consulte la página web de AWS Cloud Compliance[2]. Para ayudar a satisfacer las normas y regulaciones de seguridad gubernamentales, del sector y de la empresa, AWS proporciona informes de certificación en los que se describe cómo la infraestructura de la nube de AWS satisface los requisitos de una extensa lista de normas de seguridad globales. Puede obtener los informes de conformidad disponibles poniéndose en contacto con su representante de la cuenta de AWS. Los clientes heredan muchos de los controles operados por AWS en su propio programa de conformidad y certificación, lo que reduce el costo de mantener y aplicar medidas de control de seguridad además de mantener los propios controles. Con unas bases sólidas a su disposición, puede optimizar la seguridad de sus cargas de trabajo para aumentar la agilidad, resistencia y escala.

En el resto de este documento técnico se ofrece una introducción de cada uno de los componentes de la perspectiva de seguridad. Puede usar estos componentes para explorar los objetivos de seguridad que necesita para que su viaje a la nube sea un éxito.

Componente directivo

El componente directivo de la perspectiva de seguridad de AWS proporciona pautas sobre cómo planificar su enfoque de seguridad cuando migre a AWS. La clave para una planificación eficaz es definir las directrices que proporcionará a las personas que vayan a implementar y utilizar el entorno de seguridad. Esta información debe proporcionar instrucciones suficientes para determinar los controles que se necesitan y cómo se deben utilizar. Las áreas iniciales que debe considerar son las siguientes:

- **Gobierno de las cuentas**: dirija a la organización en el proceso de creación de procedimientos para gestionar las cuentas de AWS. Las áreas que deben definirse incluyen: qué inventarios de cuentas se van a recopilar y mantener, de qué acuerdos y enmiendas se dispone, y qué criterios se van a usar cuando se cree una cuenta de AWS. Desarrolle un proceso para crear cuentas de manera uniforme, asegurándose de que toda la configuración inicial sea correcta y de que quede claro quién es el propietario de cada una.

- **Titularidad de las cuentas e información de contacto**: establezca un modelo de gobierno adecuado de las cuentas de AWS que se use en toda la organización y prevea cómo se va a mantener la información de contacto de cada cuenta. Considere la posibilidad de crear cuentas de AWS asociadas a listas de distribución de correo electrónico en lugar de a direcciones de correo electrónico individuales. De esta forma, un grupo de personas podrá monitorizar la información de AWS sobre la actividad de las cuentas y responder a esta información. Además, este método es más robusto cuando se producen cambios internos de personal y proporciona un medio de asignar responsabilidades en materia de seguridad. Designe a su equipo de seguridad como un punto de contacto de seguridad para agilizar las comunicaciones prioritarias.
- **Marco de control**: establezca o aplique un marco de control estándar del sector y determine si necesita modificar o añadir algo para incorporar los servicios de AWS con los niveles de seguridad previstos. Realice un ejercicio de comparación de la conformidad para determinar cómo los requisitos de conformidad y los controles de seguridad reflejarán el uso de los servicios de AWS.
- **Titularidad de los controles**: consulte la información de Modelo de responsabilidad compartida de AWS[3] en el sitio web de AWS para determinar si deben realizarse modificaciones en la titularidad de los controles. Revise y actualice la matriz de asignación de responsabilidades (diagrama RACI) para incluir a los propietarios de los controles que operan en el entorno de AWS.
- **Clasificación de los datos**: revise las clasificaciones de datos actuales y determine cómo se van a gestionar estas clasificaciones en el entorno de AWS y qué controles serán los adecuados.
- **Gestión de cambios y recursos**: determine cómo se va a realizar la gestión de cambios y recursos en AWS. Cree un medio para determinar qué recursos existen, para qué sistemas se utilizan y cómo se administrarán los sistemas de forma segura. Esto se puede integrar con una base de datos de administración de la configuración (CMDB) existente. Plantéese crear una práctica de nomenclatura y etiquetado que permita que la identificación y administración tengan lugar en el nivel de seguridad necesario. Puede usar este enfoque para definir y controlar los metadatos que permiten la identificación y control.

- **Ubicación de los datos**: revise los criterios de ubicación de los datos para determinar qué controles se necesitarán para administrar la configuración y uso de los servicios de AWS en las distintas regiones. Los clientes de AWS eligen la región o regiones de AWS donde se alojará su contenido. De esta forma, los clientes que tengan requisitos geográficos específicos pueden establecer entornos en las ubicaciones que deseen. Los clientes pueden replicar y hacer backup del contenido en más de una región, pero AWS no mueve el contenido fuera de la región o las regiones elegidas por el cliente.
- **Acceso con privilegios mínimos**: establezca una cultura de seguridad en la organización basada en el principio de privilegios mínimos y autenticación robusta. Implemente protocolos para proteger el acceso a credenciales confidenciales y material clave asociado a cada cuenta de AWS. Defina las expectativas sobre cómo se delegará la autoridad a los ingenieros de software, equipo de operaciones y otros puestos involucrados en la adopción de la nube.
- **Manuales y libros de trabajo de operaciones de seguridad**: defina los patrones de seguridad para crear medidas de protección duraderas a las que la organización pueda recurrir con el paso del tiempo. Implemente las estrategias de automatización como libros de trabajo y documente la intervención humana en el proceso según corresponda.

Consideraciones

- **Cree** un modelo de responsabilidad compartida con AWS adaptado a su ecosistema.
- **Use** la autenticación robusta como parte del programa de protección para todas las partes involucradas en la cuenta.
- **Promueva** una cultura de titularidad de la seguridad para los equipos de aplicaciones.
- **Amplíe** su modelo de clasificación de datos para incluir los servicios de AWS.
- **Integre** los objetivos y las funciones del equipo de desarrolladores, operaciones y seguridad.
- **Considere** la posibilidad de crear una estrategia de nomenclatura y control de las cuentas usadas para gestionar los servicios de AWS.
- **Centralice** las listas de distribución de teléfono y correo electrónico para que se pueda monitorizar a los equipos.

Componente preventivo

El componente preventivo de la perspectiva de seguridad de AWS proporciona pautas sobre la implementación de la infraestructura de seguridad con AWS y en su organización.La clave para implementar el conjunto correcto de controles es permitir que sus equipos de seguridad consigan la confianza y capacidad que necesitan para desarrollar los conocimientos sobre automatización e implementación necesarios para proteger a la empresa en el entorno ágil y escalable de AWS.

Use el componente directivo para determinar los controles y las pautas que va a necesitar, y después use el componente preventivo para determinar cómo operará los controles eficazmente. AWS proporciona periódicamente directrices sobre las prácticas recomendadas de uso de los servicios de AWS y patrones de implementación de cargas de trabajo, que puede usar como referencia para la implementación de los controles. Visite el Centro de seguridad de AWS, el blog y la cumbre más reciente de AWS, y vea los vídeos sobre seguridad de la conferencia re:Invent.

Considere las siguientes áreas a la hora de determinar qué cambios (si hay alguno) necesita hacer en sus arquitecturas y prácticas de seguridad actuales. Esto le ayudará a definir una estrategia de adopción de AWS fluida y planificada.

- **Identidad y acceso**: integre el uso de AWS en el ciclo de vida de la plantilla de la organización, y en las fuentes de autenticación y autorización. Cree políticas y roles detallados asociados a usuarios y grupos apropiados. Cree medidas de protección que permitan cambios importantes únicamente a través de la automatización, y evite que se produzcan cambios no deseados o que estos cambios se reviertan automáticamente. Estos pasos reducirán el acceso humano a los sistemas y datos de producción.
- **Protección de la infraestructura**: implemente un marco de referencia de seguridad que incluya límites de confianza, configuración y mantenimiento de la seguridad del sistema (por ejemplo, medidas de refuerzo y parches) y otros puntos de aplicación de políticas adecuados (como grupos de seguridad, AWS WAF y Amazon API Gateway) para abordar las necesidades que ha identificado mediante el componente directivo.

- **Protección de los datos**: utilice medidas de seguridad adecuadas para proteger los datos en tránsito y en reposo. Las medidas de seguridad incluyen controles de acceso detallado a los objetos, la creación y control de las claves de cifrado usadas para cifrar los datos, la selección de métodos adecuados de cifrado y tokenización, la validación de la integridad y la retención adecuada de los datos.

Consideraciones

- **Trate** la seguridad como código para poder implementar y validar la infraestructura de seguridad de forma que admita el escalado y la capacidad de proteger la organización.
- **Cree** medidas de seguridad y valores predeterminados confidenciales, y ofrezca las plantillas y prácticas recomendadas en forma de código.
- **Cree** servicios de seguridad que la organización pueda usar para funciones de seguridad altamente repetitivas o especialmente confidenciales.
- **Defina** a las partes implicadas y confeccione un guion de su experiencia interactuando con los servicios de AWS.
- **Use** la herramienta AWS Trusted Advisor para evaluar continuamente su posición en materia de seguridad de AWS y considere la posibilidad de realizar una evaluación que demuestre una arquitectura adecuada de AWS.
- **Establezca** una base de referencia de seguridad viable mínima e itere continuamente para elevar el listón de las cargas de trabajo que protege.

Componente de detección

El componente de detección de la perspectiva de seguridad de CAF de AWS proporciona pautas para obtener visibilidad sobre el nivel de seguridad de su organización. Se puede reunir una gran cantidad de datos e información mediante servicios como AWS CloudTrail, logs específicos del servicio y valores devueltos por las API/CLI. La introducción de estas fuentes de información en una plataforma escalable para la administración y monitorización de logs, gestión de eventos, pruebas e inventario y auditoría le ofrecen la transparencia y agilidad operativa que necesita para poder confiar en la seguridad de sus operaciones.

- **Registro y monitorización**: AWS proporciona funciones de registro nativas, así como servicios que puede usar para obtener visibilidad casi en tiempo real de lo que sucede en el entorno de AWS. Puede usar estas herramientas para integrarlas en sus soluciones de registro y monitorización existentes. Integre el resultado de las fuentes de registro y monitorización en niveles profundos del flujo de trabajo de la organización de TI para la resolución integral de las actividades relacionadas con la seguridad.
- **Pruebas de seguridad**: pruebe el entorno de seguridad de AWS para garantizar que se satisfacen los estándares de seguridad definidos. Si realiza pruebas para determinar si sus sistemas responderán según lo previsto cuando se produzcan determinados eventos, estará mejor preparado para los eventos reales. Entre los ejemplos de pruebas de seguridad se incluye el análisis de vulnerabilidades, pruebas de intrusión e introducción de errores para probar que se satisfacen los estándares. El objetivo es determinar si el control responderá según lo previsto.
- **Inventario de los recursos**: saber qué cargas de trabajo se han implementado y están operativas le permitirá supervisar el entorno y asegurarse de que este funciona en los niveles de gobierno de seguridad previstos y exigidos por los estándares de seguridad.
- **Detección de cambios**: el uso de una base de referencia segura de controles preventivos exige también saber cuándo cambian estos controles. Implemente medidas para determinar las discrepancias entre la configuración segura y el estado actual.

Consideraciones

- **Determine** qué información de registro del entorno de AWS desea capturar, monitorizar y analizar.
- **Determine** cómo la capacidad empresarial del centro de operaciones de seguridad (SOC) integrará la monitorización y administración de la seguridad de AWS en las prácticas existentes.
- **Realice** continuamente análisis de vulnerabilidades y pruebas de intrusión de acuerdo con los procedimientos de AWS.

Componente reactivo

El componente reactivo de la perspectiva de seguridad de CAF de AWS proporciona pautas para la parte reactiva de la posición en materia de seguridad de su organización. Al incorporar su entorno de AWS en su posición de seguridad existente y después preparar y simular acciones que requieran una respuesta, estará mejor preparado para responder a los incidentes cuando estos ocurran.

Con la respuesta y recuperación automáticas de incidentes y la capacidad de mitigar partes de la recuperación de desastres, el equipo de seguridad puede centrarse en las investigaciones forenses y análisis de las causas raíz, en lugar de en proporcionar una respuesta. Algunos aspectos que debe considerar durante la adaptación de su posición en materia de seguridad son las siguientes:

- **Respuesta a incidentes**: durante un incidente, contener el evento y regresar a un estado de buen funcionamiento son elementos importantes de un plan de respuesta. Por ejemplo, la automatización de determinados aspectos de estas funciones mediante reglas de AWS Config y scripts de respuesta de AWS Lambda le ofrece la capacidad de escalar la respuesta a velocidades de Internet. Revise los procesos de respuesta a incidentes actuales y determine si y cómo la respuesta y recuperación automatizadas se aplicarán y se gestionarán para los recursos de AWS. Las funciones del centro de operaciones de seguridad deben estar estrechamente integradas con las API de AWS para ofrecer el mayor nivel de respuesta posible. De esta forma, dispondrá de la función de monitorización y administración de la seguridad para la adopción de la nube de AWS.
- **Simulaciones de respuesta a incidentes de seguridad**: mediante la simulación de eventos, puede validar que los controles y procesos implementados funcionan según lo previsto. Mediante este enfoque, puede determinar si de verdad es capaz de recuperarse de incidentes y responder a ellos cuando ocurran.

- **Investigación forense**: en muchos casos, sus herramientas de investigación forense funcionarán en el entorno de AWS. Los equipos forenses se beneficiarán de la implementación automatizada de herramientas en distintas regiones y de la capacidad de recopilar grandes volúmenes de datos rápidamente, con poca fricción y mediante los mismos servicios escalables robustos en los que se basan sus aplicaciones críticas, como Amazon Simple Storage Service (S3), Amazon Elastic Block Store (EBS), Amazon Kinesis, Amazon DynamoDB, Amazon Relational Database Service (RDS), Amazon RedShift y Amazon Elastic Compute Cloud (EC2).

Consideraciones

- **Actualice** sus procesos de respuesta a incidentes para que reconozcan el entorno de AWS.
- **Use** los servicios de AWS para preparar pericialmente sus implementaciones a través de la automatización y selección de características.
- **Automatice** la respuesta para ganar en robustez y capacidad de ampliación.
- **Use** los servicios de AWS para la recopilación y el análisis de datos como ayuda a la investigación.
- **Valide** su capacidad de respuesta a incidentes a través de la simulación de respuestas a incidentes de seguridad.

Realizar el viaje: definición de una estrategia

Revise su estrategia de seguridad actual para determinar si partes de la estrategia se beneficiarían del cambio como parte de una iniciativa de adopción de la nube. Compare la estrategia de adopción de la nube de AWS con el nivel de riesgo que su empresa está dispuesta a aceptar, con su enfoque para satisfacer los objetivos reglamentarios y de conformidad, y con sus definiciones sobre lo que es necesario para estar protegido y la manera de conseguirlo. En la tabla 1 se proporciona un ejemplo de una estrategia de seguridad que articula un conjunto de principios que se comparan con iniciativas específicas y flujos de trabajo.

Principio	Acciones de ejemplo
Infraestructura como código.	Mejorar los conocimientos de programación y automatización del equipo de seguridad; cambiar a DevSecOps.
Diseñar medidas de seguridad, no puertas de acceso.	Promover una conducta adecuada.
Usar la nube para proteger la nube.	Crear, operar y administrar herramientas de seguridad en la nube.
Permanecer actualizado; ejecución segura.	Usar nuevas características de seguridad; aplicar parches y reemplazar con frecuencia.
Reducir la dependencia en el acceso persistente.	Establecer catálogo de roles; automatizar KMI a través del servicio de secretos.
Visibilidad total.	Agregar logs y metadatos de AWS junto con los logs de SO y aplicaciones.
Conocimiento profundo.	Implementar un almacén de datos de seguridad con BI y análisis.
Respuesta a incidentes (RI) escalable.	Actualizar el procedimiento de operaciones estándar de RI e investigaciones forenses para el marco de responsabilidad compartida.
Reparación automática.	Automatizar la corrección y restauración a un estado de buen funcionamiento.

Tabla 1: Estrategia de seguridad de ejemplo

Conforme evolucione su estrategia, querrá empezar a iterar los marcos de garantías de terceros y requisitos de seguridad de la organización, e incorporarlos en un marco de gestión de riesgos que le guíe en su viaje a AWS. A menudo, una práctica eficaz es ampliar su mapa de conformidad cuando conozca mejor las necesidades de sus cargas de trabajo en la nube y las capacidades de seguridad proporcionadas por AWS.

Otro elemento clave de su estrategia es el cotejo del modelo de responsabilidad compartida con su ecosistema. Además de la "macrorrelación" que comparte con AWS, querrá explorar las responsabilidades compartidas internas de la organización, así como las de sus socios. Las empresas pueden dividir su modelo de responsabilidad compartida en tres grandes áreas: un marco de control, un modelo responsable, consultado y contrastado (RACI, por sus siglas en inglés) y un registro de riesgos. El marco de control describe cómo se espera que funcionen los aspectos de seguridad de la empresa y qué controles se aplicarán para gestionar el riesgo. Puede usar el modelo RACI para identificar y asignar a una persona la responsabilidad de los controles del marco. Por último, use un registro de riesgos para detectar controles sin la titularidad correcta. Clasifique los riesgos residuales que se han identificado, alineando su tratamiento con los nuevos flujos de trabajo e iniciativas implantados para resolverlos.

Cuando coteje estas responsabilidades compartidas, cabe esperar que encuentre nuevas oportunidades de automatizar las operaciones y mejorar el flujo de trabajo entre las partes implicadas críticas de su comunidad de seguridad, conformidad y gestión de riesgos. En la figura 2 se muestra un ejemplo de un modelo de responsabilidad compartida ampliado.

Figura 2: Modelo de responsabilidad compartida de ejemplo

Consideraciones

- **Cree** una estrategia personalizada que aborde el enfoque de implementación de la seguridad en la nube de su organización.
- **Promueva** la automatización como un aspecto subyacente en toda su estrategia.
- **Articule** claramente su enfoque de otorgar un papel preponderante a la nube.
- **Promueva** la agilidad y flexibilidad definiendo medidas de seguridad.
- **Considere** la estrategia como un breve ejercicio que define el enfoque de la seguridad de la información en la nube de su organización.
- **Itere** rápidamente mientras sienta las bases de la estrategia. Su objetivo es disponer de una serie de principios rectores que hagan avanzar la iniciativa; la estrategia no es un fin en sí mismo. Avance rápidamente y esté dispuesto a adaptarse y evolucionar.
- **Defina** principios estratégicos que impartan la cultura que desee en materia de seguridad y que definan las decisiones de diseño adoptadas, en lugar de una estrategia que implique soluciones específicas.

Realizar el viaje: presentación de un programa

Una vez definida la estrategia, es el momento de ponerla en práctica e iniciar la implementación que transformará su organización de seguridad y garantizará el viaje a la nube. Aunque dispone de un amplio abanico de opciones y características, la implementación no debería ser una tarea excesivamente larga. Este proceso de diseño e implementación de cómo las distintas capacidades funcionarán juntas representa una oportunidad de familiarizarse rápidamente y aprender a iterar sus diseños para satisfacer mejor sus requisitos. Aprenda de las primeras fases de la implementación y después vaya adaptando su diseño aplicando pequeños cambios a medida que aprende.

Figura 3: Epopeyas de seguridad del CAF de AWS

Para obtener ayuda con su implementación, puede usar las epopeyas de seguridad del CAF. (Véase la figura 3). Las epopeyas de seguridad son grupos de casos de usuario (casos de uso y casos de abuso) en los que puede trabajar durante los sprints. Cada una de estas epopeyas tiene varias iteraciones que abordan requisitos cada vez más complejos y van ganando en robustez. Aunque nuestra recomendación es agilizar la entrega, las epopeyas también pueden tratarse como flujos de trabajo o temas generales que ayuden a clasificar y estructurar la entrega mediante cualquier otro marco de trabajo. La estructura propuesta consta de las siguientes 10 epopeyas de seguridad (figura 4) para guiarle por la implementación.

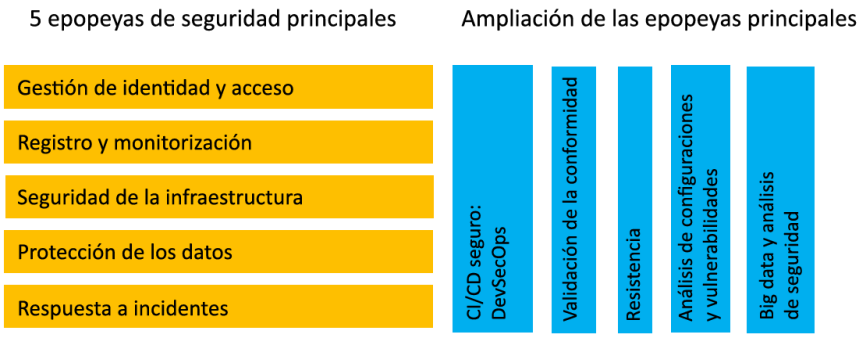

Figura 4: Diez epopeyas de seguridad de AWS

Las cinco principales

Las siguientes cinco epopeyas son las categorías principales de control y capacidad que debe considerar en las primeras fases, ya que son fundamentales para iniciar su viaje.

- **IAM**: AWS Identity and Access Management (IAM) constituye la columna vertebral de su implementación de AWS. En la nube, debe establecer una cuenta y disponer de privilegios para poder aprovisionar y organizar los recursos. Los casos típicos de automatización podrían incluir la asignación/concesión/auditoría de derechos, administración del material secreto, separación de las tareas y acceso con privilegios mínimos, administración de privilegios "just-in-time" y reducción de la dependencia en credenciales de larga duración.
- **Registro y monitorización**: los servicios de AWS proporcionan una gran variedad de datos de registro para ayudarle a monitorizar sus interacciones con la plataforma. El desempeño de los servicios de AWS se basa en las opciones de configuración elegidas y en la capacidad de introducir logs del sistema operativo y de las aplicaciones para crear un marco de referencia común. Los casos típicos de automatización podrían incluir agregación de logs, umbrales/alarmas/alertas, enriquecimiento, plataforma de búsqueda, visualización, acceso de las partes implicadas, y flujo de trabajo y registro de incidencias para iniciar una respuesta de la organización de circuito cerrado.

- **Seguridad de la infraestructura**: al tratar la infraestructura como código, la infraestructura de seguridad se convierte en una carga de trabajo de primer nivel que también debe implementarse como código. Este enfoque le ofrece la oportunidad de configurar los servicios de AWS mediante programación y de implementar la infraestructura de seguridad de socios de AWS Marketplace o soluciones de su propio diseño. Los casos típicos de automatización pueden incluir la creación de plantillas personalizadas para configurar los servicios de AWS de acuerdo con sus necesidades, la implementación de patrones de arquitectura de seguridad y libros de operaciones como código, la creación de soluciones de seguridad personalizadas a partir de los servicios de AWS, el uso de estrategias de gestión de parches como las implementaciones "blue-green", la reducción de la superficie de ataque expuesta y la validación de la eficacia de las implementaciones.
- **Protección de los datos**: proteger los datos importantes es un componente crítico de la creación y uso de sistemas de información, y AWS proporciona servicios y características que le ofrecen opciones robustas para proteger sus datos durante todo su ciclo de vida. Los casos típicos de automatización podrían incluir la toma de decisiones sobre la colocación de las cargas de trabajo, la implementación de un esquema de etiquetado, la creación de mecanismos para proteger los datos en movimiento como conexiones VPN y TLS/SSL (incluido AWS Certificate Manager), la creación de mecanismos para proteger los datos en reposo a través del cifrado en las capas correspondientes de su infraestructura, el uso de la implementación/ integración de AWS Key Management Service (AWS KMS), la implementación de AWS CloudHSM, la creación de esquemas de tokenización, y la implementación y uso de las soluciones de los socios de AWS Marketplace.
- **Respuesta a incidentes**: la automatización de aspectos de su proceso de gestión de incidentes mejora la fiabilidad y aumenta la velocidad de respuesta, y a veces crea un entorno más sencillo de evaluar en las revisiones posteriores. Los casos típicos de automatización podrían incluir el uso de "agentes de respuesta" de la función de AWS Lambda que reaccionen a cambios específicos en el entorno, la organización de eventos de autoescalado, el aislamiento de componentes del sistema sospechosos, la implementación de herramientas de investigación "just-in-time", y la creación de un flujo de trabajo y un sistema de registro de incidencias para poner fin a una respuesta de la organización de circuito cerrado y aprender de esta respuesta.

Ampliación de las epopeyas principales

Estas cinco epopeyas representan los temas que impulsarán una excelencia continuada de las operaciones a través de la disponibilidad, automatización y auditoría. Querrá integrar juiciosamente estas epopeyas en cada sprint. Si requieren mayor atención, tal vez le convenga tratarlas como sus propias epopeyas.

- **Robustez**: la alta disponibilidad, la continuidad de las operaciones, la robustez y resistencia, y la recuperación de desastres son las razones comunes de las implementaciones de la nube con AWS. Los casos típicos de automatización podrían incluir el uso de implementaciones en varias zonas de disponibilidad y regiones, el cambio de la superficie de ataque disponible, el escalado y modificación de la asignación de recursos para absorber los ataques, la protección de los recursos expuestos y la inducción deliberada de la interrupción de los recursos para validar la continuidad de las operaciones del sistema.

- **Validación de la conformidad**: la incorporación de un modelo de conformidad integral en su programa de seguridad impide que la conformidad se reduzca a un mero ejercicio de validación o a un proceso que tiene lugar después de la implementación. Esta epopeya proporciona la plataforma que consolida y racionaliza los elementos de cumplimiento generados por las otras epopeyas. Los casos típicos de automatización podrían incluir la creación de pruebas unitarias de seguridad asignadas a requisitos de conformidad, el diseño de servicios y cargas de trabajo que admitan la recopilación de pruebas de conformidad, la creación de procesos de notificación y visualización de la conformidad a partir de las características probatorias, la monitorización continua y la creación de equipos de DevSecOps orientados a la creación de herramientas de conformidad.

- **CI/CD seguro (DevSecOps)** : confiar en su cadena de suministro de software mediante el uso de cadenas de herramientas de implementación e integración continuas de confianza es un medio de desarrollar las prácticas de operaciones de seguridad en su migración a la nube. Los casos típicos de automatización podrían incluir el fortalecimiento y la revisión de la cadena de herramientas, el acceso con privilegios mínimos a la cadena de herramientas, el registro y monitorización del proceso de producción, la visualización de la integración/implementación de la seguridad y la comprobación de la integridad del código.

- **Análisis de configuraciones y vulnerabilidades**: el análisis de configuraciones y vulnerabilidades se beneficia considerablemente de la escala, agilidad y automatización que permite AWS. Los casos típicos de automatización podrían incluir la activación de AWS Config y creación de reglas de AWS Config para los clientes, el uso de Amazon CloudWatch Events y AWS Lambda para reaccionar a la detección de cambios, la implementación de Amazon Inspector, la selección e implementación de soluciones de monitorización continua de AWS Marketplace, la implementación de análisis desencadenados y la inserción de herramientas de evaluación en las cadenas de herramientas de CI/CD.
- **Análisis predictivos y de big data relacionados con la seguridad**: las operaciones de seguridad se benefician de los servicios y soluciones de big data como cualquier otro aspecto del negocio. El uso de big data le ofrece un conocimiento más detallado en el momento en que lo necesita, lo que mejora su agilidad y capacidad de aplicar a gran escala su posición en materia de seguridad. Los casos típicos de automatización podrían incluir la creación de "data lakes" de seguridad, el desarrollo de procesos de análisis, la creación de visualizaciones para impulsar la toma de decisiones sobre seguridad y el establecimiento de mecanismos de comentarios para una repuesta autónoma.

Una vez definida esta estructura, se puede esbozar un plan de implementación. Las capacidades cambian con el tiempo y las oportunidades de mejora se identificarán continuamente. Recuerde que los temas o categorías de capacidades arriba indicados se pueden tratar como epopeyas en una metodología ágil que contenga una serie de casos de usuario que incluyan tanto casos de uso como casos de abuso. Los distintos sprints irán aportando madurez, manteniendo la flexibilidad de adaptación al ritmo y demanda de la empresa.

Serie de sprints de ejemplo

Suponga que organiza una serie de seis sprints de dos semanas (un grupo de epopeyas a lo largo de un trimestre en un calendario de doce semanas), incluido un breve período de preparación, de la siguiente forma. Su enfoque dependerá de la disponibilidad de los recursos, la prioridad y el nivel de madurez deseado en cada capacidad conforme avance hacia una capacidad de producción viable mínima (PVM).

- **Sprint 0**: cartografía de la seguridad: mapas de conformidad, mapas de políticas, revisión del modelo inicial de amenazas, establecimiento de un registro de riesgos; creación de una cartera de casos de uso y abuso; planificación de las epopeyas de seguridad
- **Sprint 1**: IAM; registro y monitorización
- **Sprint 2**: IAM; registro y monitorización; protección de la infraestructura
- **Sprint 3**: IAM; registro y monitorización; protección de la infraestructura
- **Sprint 4**: IAM; registro y monitorización; protección de la infraestructura; protección de los datos
- **Sprint 5**: protección de los datos, automatización de las operaciones de seguridad, planificación/creación de herramientas de respuesta a incidentes; resistencia
- **Sprint 6**: automatización de las operaciones de seguridad; resistencia

Un elemento clave de la validación de conformidad es incorporar la validación en cada sprint a través de los casos de pruebas unitarias de seguridad y conformidad, y después llevar la promoción al proceso de producción. Cuando se requiera capacidad de validación de conformidad explícita, se pueden establecer los scripts para que se centren específicamente en esos casos de uso. Con el tiempo, se puede aprovechar la iteración para conseguir la validación e implementación continuas de la corrección automática de las desviaciones, si procede.

El objetivo general del enfoque es definir claramente qué es PVM o el marco de referencia, que se asignará al primer sprint de cada área. En las etapas iniciales, el objetivo final puede que esté menos definido, pero se creará una estrategia clara de los sprints iniciales. El tiempo, la experiencia y la iteración permitirán refinar y ajustar el estado final para que sea adecuado para su organización. En realidad, el estado final puede que cambie continuamente, pero en última instancia el proceso desembocará en una mejora continua a un ritmo más rápido. Este enfoque puede ser más eficaz y rentable que un enfoque radical basado en calendarios prolongados y en grandes desembolsos de capital.

Si profundizamos un poco más, el primer sprint de IAM podría consistir en definir la estructura de cuentas e implementar el conjunto principal de prácticas recomendadas. Un segundo sprint podría implementar la federación. Un tercer sprint podría ampliar la administración de cuentas para atender varias cuentas, y así sucesivamente. Los casos de uso de IAM que pueden abarcar uno o varios de estos sprints iniciales podrían incluir casos como los siguientes:

"Como administrador, quiero crear un conjunto inicial de usuarios para administrar el acceso con privilegios y las relaciones de confianza del proveedor de identidades".

"Como administrador, quiero asignar a los usuarios de mi directorio corporativo roles funcionales o conjuntos de derechos de acceso en la plataforma de AWS".

"Como administrador, quiero aplicar la autenticación multifactor en todas las interacciones con la consola de AWS realizadas por los usuarios interactivos".

En este ejemplo, los siguientes casos de uso de registro y monitorización podrían abarcar uno varios sprints iniciales:

"Como analista de operaciones de seguridad, quiero recibir los logs de nivel de plataforma de todas las regiones y cuentas de AWS".

"Como analista de operaciones de seguridad, quiero que todos los logs de nivel de plataforma se envíen a una ubicación compartida de todas las regiones y cuentas de AWS".

"Como analista de operaciones de seguridad, quiero recibir alertas de todas las operaciones que asocien políticas de IAM a usuarios, grupos o roles".

Puede crear capacidades en paralelo o en serie, y mantener la flexibilidad incluyendo los casos de uso de capacidades de seguridad en la cartera general de productos. También puede dividir los casos de uso entre los miembros de un equipo de DevOps centrado en la seguridad. Estas son decisiones que revisitará periódicamente para adaptar su entrega a las necesidades de la organización a lo largo del tiempo.

Consideraciones

- **Revise** su marco de control existente para determinar cómo los servicios de AWS operarán para satisfacer los estándares de seguridad exigidos.
- **Defina** a las partes implicadas y confeccione un guion de su experiencia interactuando con los servicios de AWS.
- **Defina** cuál será su primer sprint y cuál será el objetivo general inicial a largo plazo.
- **Establezca** una base de referencia de seguridad viable mínima e itere continuamente para elevar el listón de las cargas de trabajo y los datos que protege.

Realizar el viaje: desarrollo de operaciones de seguridad robustas

En un entorno donde la infraestructura es código, la seguridad debe tratarse también como código. El componente de operaciones de seguridad proporciona un medio de comunicar e instrumentar los preceptos fundamentales de la seguridad como código:

- Use la nube para proteger la nube.
- La infraestructura de seguridad debe depender de la nube.
- Exponga las características de seguridad como servicios mediante la API.
- Automatícelo todo para poder escalar la seguridad y la conformidad.

Para hacer viable este modelo de gobierno, las líneas de negocio se organizan a menudo como equipos de DevOps para crear e implementar la infraestructura y software empresarial. Puede ampliar los preceptos básicos del modelo de gobierno integrando la seguridad en su cultura o práctica de DevOps, lo que a veces recibe el nombre de DevSecOps. Cree un equipo en torno a los siguientes principios:

- El equipo de seguridad adopta las culturas y conductas de DevOps.
- Los desarrolladores contribuyen abiertamente al código usado para automatizar las operaciones de seguridad.
- El equipo de operaciones de seguridad puede participar en las pruebas y automatización del código de las aplicaciones.
- El equipo está orgulloso de la velocidad y frecuencia de sus implementaciones. Implementar más frecuentemente, con cambios más pequeños, reduce el riesgo operativo y muestra un rápido progreso en la estrategia de seguridad.

Los equipos integrados de desarrollo, seguridad y operaciones tienen tres misiones clave comunes:

- Fortalecer la cadena de herramientas de integración e implementación continuas
- Permitir y promover el desarrollo de software robusto conforme este atraviesa la cadena de herramientas
- Implementar toda la infraestructura y software de seguridad a través de la cadena de herramientas

Determinar los cambios (si los hubiera) en las prácticas de seguridad actuales le ayudará a planificar una estrategia de adopción de AWS fluida.

Conclusión

Cuando se embarque en el viaje de adopción de AWS, querrá actualizar su posición en materia de seguridad para incluir la parte de AWS de su entorno. Este documento técnico de perspectiva de la seguridad es una guía preceptiva sobre el enfoque que debe adoptar para aprovechar los beneficios que AWS ofrece a su posición en materia de seguridad. En el sitio web de AWS encontrará mucha más información sobre seguridad. Allí se describen detalladamente las características de seguridad y se ofrecen instrucciones preceptivas más detalladas para implementaciones comunes. También dispone de una lista extensa de contenido centrado en la seguridad[4] que deberían consultar varios miembros de su equipo de seguridad cuando prepare sus iniciativas de adopción de AWS.

Apéndice A: Seguimiento del progreso de la perspectiva de seguridad del CAF de AWS

Puede usar los principales habilitadores de seguridad y el modelo de progreso de epopeyas de seguridad descrito en este apéndice para medir el progreso y la madurez de la implementación de la perspectiva de seguridad del CAF de AWS. Los habilitadores y el modelo de progreso se pueden usar para fines de planificación del proyecto, para evaluar la robustez de las implementaciones o simplemente como un medio de favorecer la conversación sobre el camino por recorrer.

Habilitadores de seguridad clave

Los habilitadores de seguridad clave son hitos que le ayudan a seguir el plan previsto. Usamos un modelo de puntuación que consta de tres valores: no abordado, contemplado y completado.

- Estrategia de seguridad de la nube [no abordada, contemplada, completada]
- Plan de comunicación a las partes interesadas [no abordado, contemplado, completado]
- Cartografía de la seguridad [no abordada, contemplada, completada]
- Documentación del modelo de responsabilidad compartida [no abordada, contemplada, completada]
- Manual y libros de trabajo de operaciones de seguridad [no abordado, contemplado, completado]
- Plan de epopeyas de seguridad [no abordado, contemplado, completado]
- Simulación de respuesta a incidentes de seguridad [no abordada, contemplada, completada]

Modelo de progreso de epopeyas de seguridad

El modelo de progreso de epopeyas de seguridad le ayuda a evaluar su progreso en la implementación de las 10 epopeyas de seguridad descritas en este documento. Usamos un modelo de puntuación de 0 (cero) a 3 para medir la robustez. Hemos proporcionado ejemplos para las epopeyas de gestión de identidad y acceso y registro y monitorización para que vea cómo funciona esta progresión.

Cinco epopeyas de seguridad principales

0: no abordadas

1: abordadas en arquitectura y planes

2: implementación viable mínima

3: implementación en producción lista para la empresa

Epopeya de seguridad	0	1	2	3
Identity and Access Management	Ejemplo: No hay relación entre las identidades locales y de AWS.	Ejemplo: Se ha definido un enfoque de administración de identidades durante el ciclo de vida de la plantilla. Se ha documentado la arquitectura de IAM. Se han cotejado las funciones con las necesidades de políticas de IAM.	Ejemplo: Se ha implementado IAM tal como se ha definido en la arquitectura. Se han implementado políticas de IAM que corresponden a algunas funciones. Se ha validado la implementación de IAM.	Ejemplo: Automatización de los flujos de trabajo de ciclo de vida de IAM.
Registro y monitorización	Ejemplo: No se han usado las soluciones de registro y monitorización proporcionadas por AWS.	Ejemplo: Se ha definido un enfoque para la agregación, monitorización e integración de logs en los procesos de administración de eventos de seguridad.	Ejemplo: Se ha habilitado y centralizado el registro en el nivel de plataforma y servicio.	Ejemplo: Los eventos con implicaciones para la seguridad se ha integrando profundamente en el flujo de trabajo de seguridad y en los procesos y sistemas de gestión de incidentes.
Seguridad de la infraestructura				
Protección de los datos				
Administración de incidencias				

Ampliación de las cinco epopeyas principales

0: no abordada

1: abordadas en arquitectura y planes

2: implementación viable mínima

3: implementación en producción lista para la empresa

Epopeya de seguridad	0	1	2	3
Resistencia				
DevSecOps				
Validación de la conformidad				
Gestión de configuraciones y vulnerabilidades				
Big data de seguridad				

Taxonomía y terminología de CAF

El marco de adopción de la nube (CAF, Cloud Adoption Framework) es el marco que ha creado AWS para plasmar las pautas y las prácticas recomendadas de contratos con clientes anteriores. Una *perspectiva* del CAF de AWS representa un área de enfoque relevante para la implementación de sistemas de TI basados en la nube en las organizaciones. Por ejemplo, la perspectiva de seguridad proporciona pautas y procesos para evaluar y mejorar sus controles de seguridad existentes cuando migre al entorno de AWS.

Cada perspectiva del CAF está compuesta de componentes y actividades. Un *componente* es un área secundaria de una perspectiva que representa un aspecto específico que necesita atención.
En este documento técnico se analizan los componentes de la perspectiva de seguridad. Una *actividad* proporciona más orientación preceptiva para la creación de planes procesables que la organización puede usar para migrar a la nube y operar soluciones basadas en la nube de manera continuada.

Por ejemplo, el *componente directivo* es un elemento de la perspectiva de seguridad, y adaptar el modelo de responsabilidad compartida de AWS a su ecosistema podría ser una actividad de ese componente.

Cuando se combinan, el marco de adopción de la nube (CAF) y la metodología de adopción de la nube (CAM) pueden usarse como directrices durante el viaje a la nube de AWS.

Notas

[1] https://do.awsstatic.com/whitepapers/aws_cloud_adoption_framework.pdf

[2] https://aws.amazon.com/compliance/

[3] https://aws.amazon.com/compliance/shared-responsibility-model/

[4] https://aws.amazon.com/security/security-resources/