Prepararse para la conformidad con el GDPR en AWS

Noviembre de 2017

Avisos

Este documento se suministra únicamente 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

El Reglamento general de protección de datos (GDPR) entrará en vigor el 25 de mayo de 2018. AWS le ofrece los servicios y recursos necesarios para ayudarle a cumplir los requisitos del GDPR aplicables a su operación. Estos incluyen la adhesión por parte de AWS al Código de conducta de CISPE, controles de acceso a datos pormenorizados, herramientas de registro y monitorización, cifrado, administración de claves, servicio de auditoría, adhesión a los estándares de seguridad de TI y certificaciones de C5 de AWS.

Reglamento general de protección de datos: Información general

El GDPR es una nueva ley de privacidad europea que entrará en vigor el 25 de mayo de 2018. Su finalidad es armonizar las leyes de protección de datos en la Unión Europea (UE) por medio de la aplicación de una única ley de protección de datos vinculante en cada estado miembro.

El GDPR se aplica a todas las organizaciones creadas en la UE, o que ofrecen bienes o servicios a individuos de la UE, cuando procesan "datos personales" de residentes de la UE. Los datos personales son cualquier información relacionada con una persona natural identificable o identificada.

El GDPR reemplazará la Directiva europea de protección de datos existente (Directiva 95/46/CE). A partir del 25 de mayo de 2018, la Directiva de protección de datos existente y todas las leyes relacionadas con esta dejarán de tener vigencia.

Modificaciones que incorporará el GDPR para las organizaciones que operen en la UE

Uno de los aspectos claves del GDPR es que tiene la finalidad de unificar la forma en la que los datos personales se pueden procesar, utilizar e intercambiar de manera segura en los estados miembros de la UE. Las organizaciones deberán demostrar la seguridad de los datos que procesan y su conformidad con el GDPR de manera continua mediante la implementación y la revisión frecuente de medidas técnicas y organizativas sólidas, así como de políticas de conformidad. Las autoridades supervisoras podrán imponer sanciones de hasta 20 millones de euros o el 4% de la facturación anual mundial, el importe que sea superior.

Preparación de AWS para el GDPR

Los expertos en seguridad, protección de datos y conformidad de AWS han trabajado con clientes de todo el mundo para responder sus preguntas y ayudarlos a prepararse para la ejecución de cargas de trabajo en la nube una vez que el GDPR entre en vigor. Estos equipos también han estado revisando todos

los servicios que AWS ya ofrece para garantizar que cumplan con los requisitos del GDPR.

> Podemos confirmar que todos los servicios de AWS cumplirán con el GDPR cuando entre en vigor en mayo de 2018.

De conformidad con el artículo 32, los controladores y procesadores están obligados a “implementar medidas técnicas y organizativas adecuadas”, teniendo en cuenta “la tecnología y los costos de implementación, y la naturaleza, alcance, contexto y finalidad del procesamiento, así como el riesgo de las distintas posibilidades y gravedades de los derechos y libertades de las personas naturales”. El GDPR ofrece sugerencias específicas para toda acción de seguridad que pueda requerirse, incluidas:

- La seudonimización y el cifrado de datos personales.
- La capacidad de garantizar la confidencialidad, integridad, disponibilidad y adaptación continuas de los servicios y sistemas de procesamiento.
- La capacidad de restablecer la disponibilidad y el acceso a los datos personales de manera oportuna en caso de incidente técnico o físico.
- Un proceso para probar, valorar y evaluar periódicamente la efectividad de las medidas técnicas y organizativas a fin de garantizar la seguridad del procesamiento.

Código de conducta de CISPE

El GDPR contempla la aprobación de códigos de conducta para ayudar a los controladores y procesadores a demostrar conformidad con la normativa y las prácticas recomendadas. Uno de dichos códigos a la espera de aprobación oficial es el Código de conducta de CISPE para proveedores de servicios de infraestructura en la nube (el "Código"). El Código proporciona a los clientes la seguridad de que su proveedor de servicios en la nube utiliza los estándares de protección de datos adecuados, conformes al GDPR.

Estos son algunos de los beneficios claves del Código:

- **Definir quién es responsable de qué en lo referido a protección de datos.** El Código de conducta explica la función tanto del proveedor como del cliente de conformidad con el GDPR, dentro del contexto específico de los servicios de infraestructura en la nube.
- **El Código de conducta establece los principios a los cuales deben adherirse los proveedores.** El Código de conducta desarrolla los principios claves del GDPR acerca de las acciones y compromisos que deben asumir los proveedores para ayudar a los clientes a cumplir con la normativa. Los clientes pueden confiar en estos beneficios concretos para sus propias estrategias de conformidad y protección de datos.
- **El Código de conducta ofrece a los clientes la información de seguridad que necesitan para tomar decisiones sobre la conformidad**. El Código de conducta exige que los proveedores sean claros sobre los pasos que están siguiendo para ofrecer sus compromisos de seguridad. Por nombrar unos pocos, estos pasos incluyen notificaciones sobre violaciones de datos, eliminación de datos y subprocesamiento por terceros, así como solicitudes gubernamentales y de aplicación de la ley. Los clientes pueden utilizar esta información para comprender plenamente los altos niveles de seguridad proporcionados.

El 13 de febrero de 2017, AWS declaró que Amazon Elastic Compute Cloud (Amazon EC2), Amazon Simple Storage Service (Amazon S3), Amazon Relational Database Service (Amazon RDS), AWS Identity and Access Management (IAM), AWS CloudTrail y Amazon Elastic Block Store (Amazon EBS) están totalmente en conformidad con el Código (véase https://cispe.cloud/publicregister) Esto brinda a nuestros clientes una garantía adicional para controlar totalmente sus datos en un entorno protegido, seguro y conforme cuando utilizan AWS. Nuestra conformidad con el Código se suma a la larga lista de certificados y acreditaciones reconocidos internacionalmente con los que cuenta AWS, entre los que se incluyen ISO 27001, ISO 27018, ISO 9001, SOC 1, SOC 2, SOC 3, PCI DSS Level 1 y muchos más.

Controles de acceso a datos

El artículo 25 del GDPR establece que el controlador “deberá implementar las medidas técnicas y organizativas adecuadas para garantizar que, de forma predeterminada, solo se procesen los datos personales necesarios para cada finalidad específica del procesamiento”. Al permitir que solo accedan a los datos

de clientes y recursos de AWS los administradores, usuarios y aplicaciones autorizados, los siguientes mecanismos de control de acceso de AWS le ayudan a cumplir con este requisito.

- **Acceso pormenorizado a objetos de AWS en buckets de S3/SQS/SNS y otros**: puede conceder distintos permisos para distintos recursos a distintas personas. Por ejemplo, puede permitir a algunos usuarios un acceso completo a Amazon Elastic Compute Cloud (Amazon EC2), Amazon Simple Storage Service (Amazon S3), Amazon DynamoDB, Amazon Redshift y otros servicios de AWS. A otros usuarios puede otorgarles acceso de solo lectura a algunos buckets de S3, para administrar algunas instancias de EC2 o para acceder únicamente a su información de facturación.
- **Autenticación multifactor (MFA)**: puede añadir autenticación de doble factor a su cuenta y a usuarios particulares para una seguridad adicional. Con la MFA, tanto usted como sus usuarios deben proporcionar no solo una contraseña o clave de acceso que funcione con su cuenta, sino también un código de un dispositivo configurado para ello.
- **Autenticación de solicitud de API**: puede utilizar las características IAM para proporcionar de forma segura las credenciales necesarias para acceder a otros recursos de AWS, como buckets de S3 y bases de datos RDS o DynamoDB, a las aplicaciones que se ejecutan en instancias EC2.
- **Restricciones geográficas**: puede utilizar la restricción geográfica, también conocida como bloqueo geográfico, para evitar que los usuarios de una ubicación geográfica específica accedan a contenido que distribuye a través de la distribución web de CloudFront. Para utilizar la restricción geográfica, tiene dos opciones:
    - **Utilizar la característica de restricción geográfica CloudFront** Utilice esta opción para restringir el acceso a todos los archivos asociados con una distribución y según el país.
    - **Utilizar un servicio de geolocalización de terceros** Utilice esta opción para restringir el acceso a un subconjunto de los archivos asociados a una distribución o para restringirlo a un nivel más detallado que por país.
- **Tokens de acceso temporal a través de STS**: puede utilizar AWS Security Token Service (AWS STS) para crear y proporcionar a los

usuarios de confianza credenciales de seguridad temporales que puedan controlar el acceso a sus recursos de AWS. Las credenciales de seguridad temporales funcionan de forma casi idéntica a las credenciales de clave de acceso a largo plazo que utilizan sus usuarios de IAM, con las siguientes diferencias:

- **Las credenciales de seguridad temporales son a corto plazo, como su nombre indica:** Pueden configurarse para que tengan la duración que quiera, desde unos minutos hasta varias horas. Una vez que las credenciales hayan expirado, AWS ya no las reconocerá ni permitirá ningún acceso desde solicitudes de API realizadas con ellas.
- **El usuario no almacena las credenciales de seguridad temporales, sino que estas se generan de forma dinámica y se le proporcionan al usuario cuando este las solicita.** Cuando las credenciales de seguridad temporales expiren (o incluso antes), el usuario podrá solicitar unas credenciales nuevas, siempre que siga teniendo permiso para hacerlo.

Estas diferencias tienen las siguientes ventajas a la hora de utilizar credenciales temporales:

- No es necesario que distribuya o incluya credenciales de seguridad de AWS a largo plazo en una aplicación.
- Puede conceder acceso a los usuarios a sus recursos de AWS sin necesidad de definir una identidad de AWS para ellos. Las credenciales temporales son la base de las funciones y las identidades federadas.
- Las credenciales de seguridad temporales tienen una vida útil limitada, de modo que no tenga que asignarlas a otro usuario ni revocarlas de forma explícita cuando ya no las necesite. Una vez que las credenciales expiren, ya no pueden volver a utilizarse. Puede especificar el periodo de validez de las credenciales, hasta un límite máximo.

Monitorización y registro

El GDPR requiere que “cada controlador y, cuando proceda, el representante del controlador mantengan un registro de las actividades de procesamiento bajo su responsabilidad”. Este artículo también incluye detalles acerca de la

información que debe registrarse. Es decir, el GDPR requiere la monitorización del procesamiento de datos PII. Además, las obligaciones de notificación de violación oportunas hacen que los incidentes se detecten casi en tiempo real. Para ayudarle a cumplir con dichas obligaciones, AWS ofrece varios servicios de registro y monitorización:

- **Administración y configuración de activos con AWS Config**: AWS Config ofrece una vista detallada de la configuración de los recursos de AWS en su cuenta de AWS. Esto incluye cómo se relacionan los recursos entre sí y cómo estaban configurados en el pasado para que pueda ver el cambio que han sufrido las configuraciones y relaciones en el tiempo.

  Un recurso de AWS es una entidad que puede funcionar con un AWS, como una instancia de Amazon Elastic Compute Cloud (EC2), un volumen de Amazon Elastic Block Store (EBS), un grupo de seguridad, o una Amazon Virtual Private Cloud (VPC). Para obtener una lista completa de los recursos de AWS compatibles con AWS Config, consulte Tipos de recursos de AWS admitidos

  Con AWS Config, puede hacer lo siguiente:

  - Evaluar sus configuraciones de recursos de AWS para los ajustes deseados.
  - Obtener un resumen de las configuraciones actuales de los recursos admitidos asociados a su cuenta de AWS.
  - Recuperar las configuraciones de uno o más recursos existentes en su cuenta.
  - Recuperar las configuraciones históricas de uno o más recursos.
  - Recibir una notificación siempre que se cree, modifique o elimine un recurso.
  - Ver las relaciones entre los recursos. Por ejemplo, es posible que desee ver todos los recursos que utilicen un grupo de seguridad específico.

- **Auditoría de conformidad y análisis de seguridad con AWS CloudTrail**: con AWS CloudTrail, puede monitorizar las implementaciones de AWS en la nube a partir de un historial de las llamadas a la API de AWS en su cuenta, incluidas las llamadas a la API

realizadas a través de la consola de administración de AWS, los SDK de AWS, las herramientas de línea de comandos y otros servicios de AWS de alto nivel. También puede identificar a los usuarios y las cuentas que llamaron a las API de AWS para servicios compatibles con CloudTrail, la dirección IP desde la que se efectuaron las llamadas y cuándo se realizaron dichas llamadas. Puede integrar CloudTrail en las aplicaciones con la API. Automatice la creación de análisis en su organización, compruebe el estado de los análisis y controle la manera en que los administradores activan y desactivan CloudTrail.

- **Identificaciones de desafíos de documentación mediante TrustedAdvisor**: el registro ofrece una manera de obtener registros de acceso detallados en un bucket de S3. Un registro de acceso contiene detalles sobre la solicitud, como el tipo de solicitud, los recursos especificados en la solicitud con los que se ha trabajado y la fecha y hora en que se procesó la solicitud. Para obtener más información acerca de los contenidos de un registro, consulte Formato de registro[1] de acceso al servidor en la guía para desarrolladores del servicio Amazon Simple Storage.
- Los registros de acceso al servidor resultan útiles para muchas aplicaciones, ya que ofrecen a los propietarios del bucket información clave sobre la naturaleza de las solicitudes realizadas por clientes que no están bajo su control. De manera predeterminada, Amazon S3 no recopila registros de acceso al servicio, pero si habilita el registro, Amazon S3 envía registros de acceso a su bucket cada hora.
- Registro detallado de acceso a objetos de S3.
- Información detallada sobre flujos en la red mediante VPC-FlowLogs.
- Acciones y verificaciones de configuración basadas en reglas con AWS Config Rules.
- Filtrado y monitorización de acceso HTTP a aplicaciones con funciones de WAF en CloudFront.

Protección de sus datos en AWS

El GDPR requiere que las organizaciones tengan que “implementar medidas técnicas y organizativas adecuadas para garantizar un nivel de seguridad apropiado para el riesgo, entre las que se incluyen (…) la seudonimización y el cifrado de datos personales (…)”. Además, las organizaciones deben protegerse

ante la revelación no autorizada de datos personales o el acceso a ellos. Finalmente, en caso de que se haya producido una violación de datos personales que pueda constituir un riesgo para los derechos y las libertades de las personas naturales, pero el controlador haya establecido "las medidas de protección técnicas y organizativas adecuadas (...), como el cifrado", no es necesario que el controlador notifique el tipo de datos afectados por la violación, de modo que puede evitar los costes administrativos y daños reputacionales. AWS ofrece varios mecanismos escalables y seguros de cifrado de datos para ayudarle a proteger los datos de clientes almacenados y procesados en AWS:

- **Cifrado de sus datos en reposo con AES256 (EBS/S3/Glacier/RDS)**: el Cifrado de datos en reposo[2] es esencial para el cumplimiento de la normativa y garantizar que ningún usuario ni aplicación pueda leer los datos confidenciales almacenados en discos sin una clave válida. AWS proporciona opciones de datos en reposo y administración de claves como apoyo al proceso de cifrado. Por ejemplo, puede cifrar volúmenes de Amazon EBS y configurar buckets de Amazon S3 para el cifrado del lado del servidor (SSE) mediante el cifrado AES-256. Además, Amazon RDS es compatible con el cifrado transparente de datos (TDE).

  El almacén de instancias proporciona almacenamiento temporal a nivel de bloque para las instancias de Amazon EC2. Este almacén se encuentra en discos que están conectados físicamente a un equipo host. El almacén de instancias es perfecto para almacenar temporalmente información que cambia con frecuencia, como búferes, cachés y datos de borrador. Por defecto, los archivos almacenados en estos discos no están cifrados.

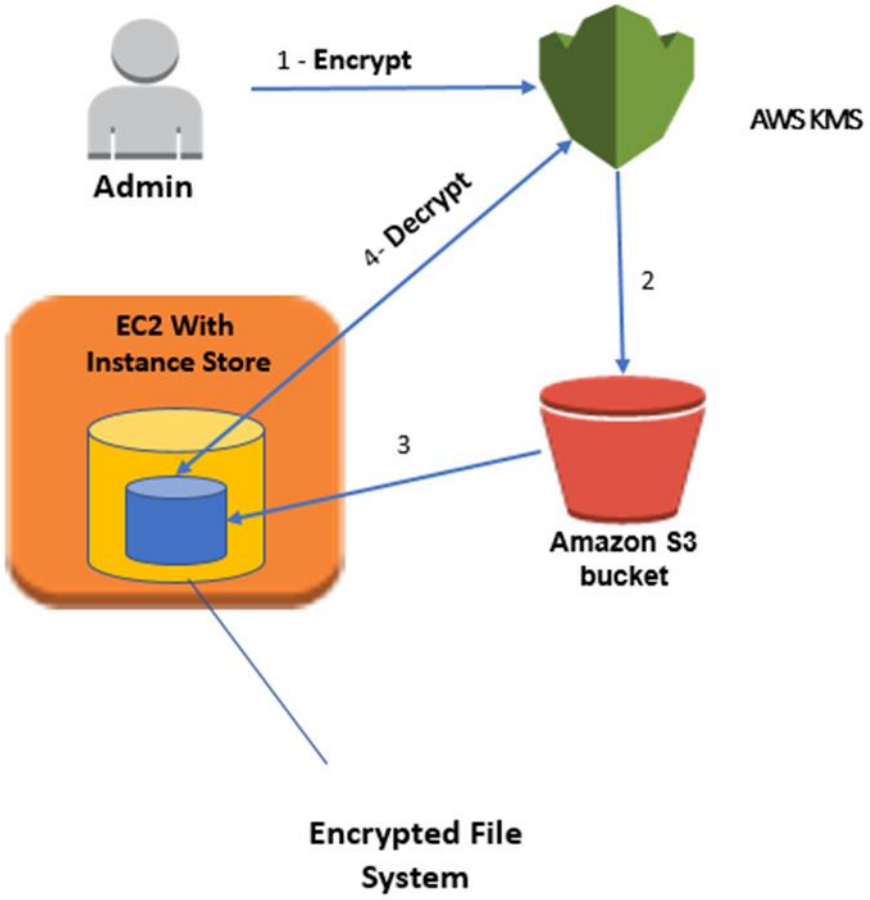
  - **Cifrado del sistema de archivos y disco**: puede utilizar dos métodos para cifrar archivos en almacenes de instancias. El primer método es el cifrado del disco, en el cual se cifra todo el disco o un bloque del mismo, mediante una o más claves de cifrado. El cifrado del disco funciona por debajo del nivel de sistema de archivos, es independiente del sistema operativo y oculta información sobre el archivo y el directorio, como el nombre y el tamaño. El Sistema de cifrado de archivos, por ejemplo, es una extensión de Microsoft para el sistema New Technology File System (NTFS) del sistema operativo Windows NT que proporciona cifrado del disco.

El segundo método es el cifrado del sistema de archivos. Se cifran los archivos y los directorios, pero no el disco entero ni una partición. El cifrado de archivos del sistema funciona sobre el sistema de archivos y se puede transferir a diversos sistemas operativos.

- **Infraestructura dm-crypt de Linux**: Dm-crypt es un mecanismo de cifrado en el kernel de Linux que permite que los usuarios monten un sistema de archivos cifrado. El montaje de un sistema de archivos es el proceso por el cual se incluye un sistema de archivos en un directorio (punto de montaje), para que esté disponible para el sistema operativo. Tras el montaje, todos los archivos del sistema de archivos están disponibles para las aplicaciones, sin necesidad de ninguna interacción adicional; sin embargo, estos archivos se cifran cuando se almacenan en el disco.

  El mapeador de dispositivos es una infraestructura del kernel de las versiones 2.6 y 3.x de Linux que proporciona una forma genérica para crear capas virtuales de dispositivos de bloque. El mapeador de dispositivos para objetivos de criptografía proporciona cifrado transparente de dispositivos de bloque mediante la API de criptografía del kernel. La solución de este artículo utiliza dm-crypt junto con un sistema de archivos respaldado en disco asociado con un volumen lógico mediante el Administrador de volúmenes lógicos (LVM). LVM proporciona una administración de volúmenes lógicos para el kernel de Linux.

- **Información general de la arquitectura**: el siguiente diagrama de arquitectura de alto nivel muestra la solución propuesta para habilitar el cifrado de almacenes de instancias EC2.



1. El administrador cifra una contraseña secreta con KMS. La contraseña cifrada se almacena en un archivo.
2. El administrador coloca el archivo que contiene la contraseña cifrada en un bucket de S3.
3. Al iniciar la instancia, esta copia los archivos cifrados en un disco interno.
4. A continuación, la instancia EC2 descifra el archivo mediante KMS y recupera la contraseña en texto plano. La contraseña se utiliza para configurar el sistema de archivos cifrado de Linux con LUKS. Todos los datos escritos en el sistema de archivos cifrado se cifran mediante el algoritmo de cifrado AES-256 al almacenarse en el disco.

- **Administración de claves gestionadas centralmente (por región)**: AWS Key Management Service (KMS) es un servicio administrado que facilita la creación y el control de claves de cifrado que se utilizan para cifrar los datos; este servicio usa los módulos de seguridad de hardware (HSM) para proteger la seguridad de las claves. AWS Key Management Service está integrado en otros servicios de AWS para ayudarle a proteger los datos que almacena con estos servicios. AWS Key Management Service también está integrado con AWS CloudTrail para ofrecerle los logs de uso de todas las claves a fin de que se ajusten a las necesidades normativas y de conformidad.
    - **Administración de claves centralizada**: AWS Key Management Service le permite ejercer un control centralizado de las claves de cifrado. Puede crear e importar claves y asignarlas a otros usuarios, así como definir políticas de uso y auditar el uso de forma sencilla desde la consola de administración de AWS o mediante el SDK o la CLI de AWS. Las claves principales de KMS, tanto si las ha importado como si las ha creado KMS, se almacenan cifradas en un almacén de larga duración para garantizar su recuperación cuando sea necesario. Puede optar por que KMS asigne automáticamente las claves principales creadas en KMS a otros usuarios una vez al año sin necesidad de tener que volver a cifrar los datos que ya se han cifrado con la clave principal. No necesita realizar un seguimiento de las versiones anteriores de las claves principales, porque KMS las mantiene disponibles para descifrar los datos cifrados anteriormente. Puede crear nuevas claves principales y controlar quién tiene acceso a ellas y con qué servicios se pueden usar cuando lo desee. También puede importar claves de su infraestructura de administración de claves y utilizarlas en KMS.
    - **Integración del servicio de AWS**: AWS Key Management Service se integra perfectamente con otros servicios de AWS. Esta integración le permite usar sin problemas las claves principales de AWS KMS para cifrar los datos que almacene en estos servicios. Puede usar una clave principal predeterminada que se crea automáticamente y solo se puede utilizar dentro del servicio integrado o puede seleccionar una clave principal personalizada que cree en KMS o que importe de su propia infraestructura de administración de claves y que tenga permiso para usar.

- **Capacidades de auditoría**: si tiene AWS CloudTrail[3] habilitado para la cuenta de AWS, cada uso que haga de alguna clave almacenada en KMS se registra en un archivo de registro que se entrega en el bucket de Amazon S3 especificado al habilitar AWS CloudTrail. La información registrada comprende los detalles del usuario, la hora, la fecha y la clave utilizada.
- **Escalabilidad, durabilidad y alta disponibilidad**: AWS Key Management Service es un servicio administrado. A medida que aumenta el uso de las claves de cifrado de AWS KMS, desaparece la necesidad de comprar infraestructura adicional para la administración de claves. AWS KMS se escala automáticamente para satisfacer sus necesidades de claves de cifrado.

  Las claves principales creadas en AWS KMS o importadas por usted no se pueden exportar desde el servicio. AWS KMS almacena varias copias de las versiones cifradas de las claves en sistemas diseñados para ofrecer una durabilidad del 99,999999999%, a fin de garantizar que las claves estarán disponibles siempre que necesite obtener acceso a ellas. Si importa claves en KMS, debe mantener una copia de las mismas en un lugar seguro para poder volver a importarlas en cualquier momento.

  AWS KMS se implementa en varias zonas de disponibilidad dentro de una región de AWS para ofrecer una alta disponibilidad de las claves de cifrado.
- **Seguro**: AWS KMS está diseñado para que nadie pueda obtener acceso a las claves principales. El servicio se basa en sistemas diseñados para proteger las claves principales con técnicas extensivas de seguridad reforzada, como no almacenar nunca claves principales no cifradas en el disco, no mantenerlas en la memoria y limitar los sistemas que pueden conectarse al dispositivo. Todo el acceso al software de actualización del servicio lo controla un servicio de aprobación de varios niveles de cuya auditoría y revisión se encarga un grupo independiente dentro de Amazon.

  Para obtener más información sobre cómo funciona AWS KMS, puede leer el documento técnico sobre AWS Key Management Service[4].

- **Túneles IPsec en AWS con gateways de VPN**: Amazon VPC le permite aprovisionar una sección de la nube de Amazon Web Services (AWS) aislada de forma lógica, donde podrá lanzar recursos de AWS en una red virtual que defina. Puede controlar todos los aspectos del entorno de red virtual, incluida la selección de su propio rango de direcciones IP, la creación de subredes y la configuración de tablas de ruteo y puertas de enlace de red. También puede crear una conexión de red privada virtual (VPN) de hardware entre el centro de datos de la empresa y la VPC, y utilizar la nube de AWS como una prolongación del centro de datos corporativo.

  Es fácil personalizar la configuración de red de Amazon VPC. Por ejemplo, puede crear una subred de cara al público para los servidores web con acceso a Internet y colocar los sistemas backend, como bases de datos o servidores de aplicaciones, en una subred de uso privado sin acceso a Internet. Puede aprovechar varias capas de seguridad, incluidos grupos de seguridad y listas de control de acceso a red, para ayudar a controlar el acceso a las instancias de Amazon EC2 desde cada subred.

- **Módulos HSM dedicados en la nube con CloudHSM**: el servicio AWS CloudHSM le ayuda a satisfacer los requisitos empresariales, contractuales y normativos para la seguridad de datos mediante el uso de módulos de seguridad de hardware (HSM) dedicados en la nube de AWS. Con CloudHSM, tiene el control de las claves de cifrado y las operaciones de cifrado que realiza el HSM.

  Los socios de AWS y AWS Marketplace ofrecen una gran variedad de soluciones para proteger la información confidencial dentro de la plataforma de AWS, pero puede ser necesaria una protección adicional para las aplicaciones y los datos que estén sujetos a estrictas condiciones contractuales o normativas para la administración de claves de cifrado. Hasta ahora, la única opción era almacenar la información confidencial (o las claves de cifrado que protegen la información confidencial) en sus centros de datos locales. Desafortunadamente, esto le impedía migrar estas aplicaciones a la nube o reducía significativamente su desempeño. El servicio AWS CloudHSM le permite proteger sus claves de cifrado dentro de los dispositivos HSM diseñados y aprobados de acuerdo con los estándares gubernamentales para la administración segura de claves. Puede crear, almacenar y administrar de manera segura las claves utilizadas para el cifrado de datos de modo que solo usted pueda acceder

a ellos. AWS CloudHSM le ayuda a cumplir los estrictos requisitos de administración de claves sin reducir el desempeño de la aplicación.

El servicio AWS CloudHSM funciona con Amazon Virtual Private Cloud (VPC). Las instancias de CloudHSM se suministran en su VPC con la dirección IP que usted especifique, lo que proporciona una conectividad de red sencilla y privada a sus instancias de Amazon Elastic Compute Cloud (EC2). Si sitúa las instancias de CloudHSM cerca de sus instancias de EC2, se reduce la latencia de la red, lo que a su vez puede mejorar el desempeño de la aplicación. AWS proporciona acceso exclusivo y específico (arrendatario único) a las instancias de CloudHSM, aislado de otros clientes de AWS. Disponible en varias regiones y zonas de disponibilidad, AWS CloudHSM le permite añadir un almacenamiento de claves seguro y duradero a sus aplicaciones.

- **Integrado**: puede utilizar CloudHSM con Amazon Redshift, Amazon Relational Database Service (RDS) Oracle o aplicaciones de otros fabricantes como SafeNet Virtual KeySecure para actuar a modo de raíz de confianza, Root of Trust, Apache (terminación SSL) o Microsoft SQL Server (cifrado transparente de datos). Asimismo, puede utilizar CloudHSM cuando escriba sus propias aplicaciones y seguir utilizando las bibliotecas de cifrado estándar con las que está familiarizado, como PKCS#11, Java JCA/JCE y Microsoft CAPI/CNG.
- **Auditable**: si tiene que hacer un seguimiento de los cambios en los recursos o auditar actividades con fines de seguridad y conformidad, puede consultar todas las llamadas a la API de CloudHSM realizadas desde su cuenta mediante CloudTrail. Además, puede auditar las operaciones en el dispositivo HSM a través de syslog o enviar mensajes de log syslog a su recopilador de datos.

Estándares de seguridad y marco de conformidad sólidos

De conformidad con el GDPR, es posible que las medidas técnicas y organizativas adecuadas deban incluir “la capacidad de garantizar la confidencialidad, integridad, disponibilidad y adaptación continuas de los servicios y sistemas de procesamiento”, así como procesos de confianza de

gestión del riesgo general, de restauración y de prueba. AWS le ofrece un sólido marco de conformidad y estándares de seguridad avanzados.

Modelo de responsabilidad compartida en cuanto a seguridad

Antes de adentrarnos en los detalles de cómo AWS protege sus datos, debemos hablar de cómo la seguridad en la nube es ligeramente diferente de la seguridad en los centros de datos locales. Cuando mueve sus sistemas informáticos y datos a la nube, las responsabilidades de seguridad se comparten entre usted y su proveedor de servicios en la nube. En este caso, AWS es responsable de proteger la infraestructura subyacente que respalda la nube, y de todo lo que ponga en la nube o conecte con ella. Este modelo de responsabilidad compartida en cuanto a seguridad puede reducir la carga operativa en muchos sentidos, y en algunos casos puede incluso mejorar su enfoque predeterminado hacia la seguridad sin ninguna acción adicional por su parte.

Responsabilidades de seguridad de AWS

Amazon Web Services es responsable de proteger la infraestructura global en la que se ejecutan todos los servicios ofrecidos en la nube de AWS. Esta infraestructura está compuesta por hardware, software, redes e instalaciones que ejecutan servicios de AWS. Proteger esta infraestructura es la mayor prioridad de AWS y, aunque no puede visitar nuestros centros de datos u oficinas para ver estas medidas de protección de primera mano, proporcionamos varios informes de auditores externos que han verificado que esta cumple una gran variedad de normas y regulaciones de seguridad informática. Para obtener más información, consulte https://aws.amazon.com/es/compliance/.

Tenga en cuenta que además de proteger su infraestructura global, AWS es responsable de la configuración de seguridad de sus productos que se consideran servicios administrados. Ejemplos de estos tipos de servicios son Amazon DynamoDB, Amazon RDS, Amazon Redshift, Amazon Elastic MapReduce y Amazon WorkSpaces, entre otros. Estos servicios proporcionan la escalabilidad y flexibilidad de los recursos basados en la nube con la ventaja añadida de que están administrados. Para estos servicios, AWS se ocupará de tareas de seguridad básicas como la aplicación de parches al sistema operativo (SO) invitado y a las bases de datos, la configuración del firewall y la

recuperación de desastres. Para la mayoría de estos servicios administrados, todo lo que tiene que hacer es configurar controles de acceso lógicos para los recursos y proteger las credenciales de sus cuentas. Algunos de ellos pueden requerir tareas adicionales, como configurar cuentas de usuario de base de datos, pero el servicio se encarga de la mayoría de las tareas de configuración de la seguridad.

Responsabilidades de seguridad del cliente

Con la nube de AWS, puede aprovisionar servidores virtuales, almacenamiento, bases de datos y escritorios en cuestión de minutos en lugar de semanas. También puede usar herramientas de análisis y flujo de trabajo basadas en la nube para procesar sus datos cuando lo necesite, y almacenar estos datos en sus propios centros de datos o en la nube. Los servicios de AWS que utilice determinarán la cantidad de trabajo de configuración que tendrá que realizar como parte de sus responsabilidades de seguridad.

Los productos de AWS correspondientes a la categoría ampliamente conocida como Infraestructura como servicio (IaaS) —como es el caso de Amazon EC2, Amazon VPC y Amazon S3— están completamente bajo su control y tendrá que realizar todas las tareas de configuración y administración de seguridad necesarias. Por ejemplo, para las instancias EC2, usted es responsable de administrar el sistema operativo invitado (incluidas las actualizaciones y parches de seguridad), todo el software de aplicación o utilidades que instale en las instancias y la configuración del firewall proporcionado por AWS (conocido como grupo de seguridad) en cada instancia. Estas son básicamente las mismas tareas de seguridad que suele realizar con independencia de dónde se encuentren los servidores.

Los servicios de AWS administrados como Amazon RDS o Amazon Redshift proporcionan todos los recursos necesarios para realizar una tarea específica, pero sin el trabajo de configuración que esta conlleva. Con los servicios administrados, no tiene que preocuparse de lanzar o mantener instancias, de aplicar parches al sistema operativo invitado o a la base de datos ni de replicar las bases de datos: AWS se ocupa de todo ello por usted. Pero al igual que con todos los servicios, debe proteger las credenciales de sus cuentas de AWS y configurar cuentas de usuario individuales con Amazon Identity and Access Management (IAM) para que cada usuario tenga sus propias credenciales y usted pueda implementar la división de tareas. También le recomendamos que

use la autenticación multifactor (MFA) con cada cuenta, lo que requiere el uso de SSL/TLS para comunicarse con sus recursos de AWS, y que configure el registro de actividades de las API y usuarios con AWS CloudTrail. Para obtener más información sobre las medidas adicionales que puede aplicar, consulte el documento técnico sobre prácticas recomendadas de seguridad de AWS y la lectura recomendada en la página web de recursos de seguridad de AWS.

Programa de conformidad de AWS

La conformidad de Amazon Web Services le permite conocer los potentes controles de AWS para mantener la seguridad y la protección de datos en la nube. A medida que se van creando sistemas en la infraestructura de nube de AWS, se deberán compartir las responsabilidades relativas a la conformidad. Mediante la combinación de características de servicio centradas en el control y la auditoría con los estándares aplicables de conformidad o auditoría, los habilitadores de conformidad de AWS crean programas tradicionales que le ayudan a establecerse y trabajar en un entorno de control de seguridad de AWS. La infraestructura de TI que AWS le ofrece está diseñada y se administra de acuerdo con las prácticas recomendadas de seguridad y diversos estándares de seguridad de TI, incluidos los siguientes:

- SOC 1/SSAE 16/ISAE 3402 (anteriormente SAS70)
- SOC 2
- SOC 3
- FISMA, DIACAP y FedRAMP
- DOD CSM niveles 1-5
- PCI DSS Nivel 1
- ISO 9001 / ISO 27001
- ITAR
- FIPS 140-2
- MTCS nivel 3

Asimismo, la flexibilidad y el control que ofrece la plataforma AWS le permiten implementar soluciones que cumplen los estándares específicos de diferentes sectores:

- CJIS (Criminal Justice Information Services)
- Cloud Security Alliance (CSA)
- Ley de derechos educativos de la familia y privacidad (Family Educational Rights and Privacy Act, FERPA)
- Ley de Portabilidad y Responsabilidad de Seguros Médicos (HIPAA)
- Motion Picture Association of America (MPAA)

AWS ofrece a los clientes una gran variedad de información con respecto al entorno de control de TI a través de documentos técnicos, informes, certificaciones y otras acreditaciones independientes. Para obtener más información, consulte el documento técnico sobre Riesgos y conformidad, disponible en https://aws.amazon.com/es/compliance/.

Catálogo de controles de conformidad de informática en la nube (C5, esquema de confirmación respaldado por el gobierno alemán)

El Catálogo de controles de conformidad de informática en la nube (C5)[5] es un esquema de certificación respaldado por el gobierno alemán e introducido en Alemania por el Servicio Federal de Seguridad de la Información (BSI) para ayudar a las organizaciones a mostrar la seguridad operativa frente a ciberataques comunes en el contexto de las Recomendaciones de seguridad para proveedores de la nube[6] del gobierno alemán.

Los clientes de AWS y sus asesores de conformidad pueden utilizar la certificación de C5 para comprender la gama de servicios de control de seguridad de TI que AWS ofrece a medida que trasladan sus cargas de trabajo a la nube. C5 agrega el nivel de seguridad de TI definido por la normativa equivalente al “IT-Grundschutz” con la incorporación de controles específicos de la nube.

C5 agrega controles adicionales que proporcionan información relativa a la ubicación de datos, aprovisionamiento de servicios, fuero jurisdiccional, certificación existente, obligaciones de divulgación de la información y una descripción del servicio completo. Con esta información, los clientes pueden evaluar cómo las normativas legales (es decir, la privacidad de los datos), sus

propias políticas o el entorno de amenazas se relaciona con su uso de servicios de informática en la nube.

Revisiones del documento

Fecha	Descripción
Noviembre de 2017	Publicación inicial

Notes

[1] https://docs.aws.amazon.com/es_es/AmazonS3/latest/dev/LogFormat.html

[2] https://do.awsstatic.com/whitepapers/AWS_Securing_Data_at_Rest_with_Encryption.pdf

[3] https://aws.amazon.com/es/cloudtrail/

[4] https://do.awsstatic.com/whitepapers/KMS-Cryptographic-Details.pdf

[5] https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/ComplianceControlsCatalogue.pdf;jsessionid=E5F009E49EB2689FAC3705578821BCB6.2_cid286?__blob=publicationFile&v=3

[6] https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CloudComputing/SecurityRecommendationsCloudComputingProviders.pdf?__blob=publicationFile&v=2