Información general sobre el cumplimiento del RGPD en AWS

Diciembre de 2020

Aviso

Los clientes son responsables de evaluar personalmente la información contenida en este documento. Este documento (a) solo tiene fines informativos; (b) representa las prácticas y las ofertas de productos vigentes de AWS, que están sujetas a cambios sin previo aviso; y (c) no constituye ningún compromiso ni aseguramiento de AWS ni de sus empresas afiliadas, proveedores o licenciantes. Los productos o servicios de AWS se proporcionan “tal cual”, sin garantías, representaciones ni condiciones de ningún tipo, ya sean explícitas o implícitas. Las responsabilidades y obligaciones de AWS con respecto a sus clientes se controlan por medio de acuerdos de AWS; este documento no forma parte de ningún acuerdo entre AWS y sus clientes ni lo modifica.

Contenido

Resumen

Este documento informa sobre los servicios y los recursos que ofrece Amazon Web Services (AWS) a sus clientes para ayudarlos a cumplir los requisitos del Reglamento general de protección de datos (RGPD) que puedan afectar a sus actividades. Entre estos, se encuentran el cumplimiento de las normas de seguridad informática, las acreditaciones para el Cloud Computing Compliance Controls Catalog (C5, catálogo de controles de cumplimiento de computación en la nube) de AWS, el cumplimiento del código de conducta de Cloud Infrastructure Services Providers in Europe (CISPE, proveedores de servicios de infraestructura en la nube de Europa), el control de acceso a los datos, el uso de herramientas de seguimiento y registro, el cifrado y la gestión de las claves.

Resumen del Reglamento general de protección de datos

El Reglamento general de protección de datos (RGPD) europeo es una legislación sobre la privacidad[1] que entró en vigor el 25 de mayo de 2018 (Reglamento [UE] 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016[2]). El RGPD deroga a la Directiva europea de protección de datos (Directiva 95/46/CE) y tiene como objetivo armonizar las leyes de protección de datos de toda la Unión Europea (UE) mediante la instauración de una única ley de protección de datos que sea vinculante en todos los Estados miembros.

El RGPD se aplica a todas las organizaciones establecidas en la UE y a las organizaciones, ya estén o no establecidas en la UE, que procesen los datos personales de los interesados de la UE en relación con la oferta de bienes o servicios proporcionados a los interesados en la UE o el seguimiento de las actuaciones llevadas a cabo dentro de la UE. Los datos personales son cualquier información relacionada con una persona natural identificable o identificada.

Cambios que el RGPD introduce para las entidades que operan en la UE

Uno de los aspectos claves del reglamento es que unifica 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 protección de los datos que procesan y el cumplimiento del RGPD de manera continua mediante la implementación y la revisión frecuentes de medidas técnicas y organizativas, así como de las políticas de cumplimiento que afecten al tratamiento de los datos personales. En caso de incumplimiento del RGPD, las autoridades supervisoras europeas podrán imponer sanciones de hasta 20 millones de euros o el 4 % de la facturación anual mundial, según el importe que sea superior.

Preparación de AWS para el RGPD

Los expertos en cumplimiento, protección de datos y seguridad de AWS trabajan con clientes de todo el mundo para responder a sus dudas y ayudarlos a prepararse para ejecutar cargas de trabajo en la nube en conformidad con el RGPD. Estos equipos también analizan el nivel de preparación de AWS en relación con los requisitos del RGPD.

> *Podemos confirmar que todos los servicios de AWS pueden utilizarse en cumplimiento de lo estipulado en el RGPD.*

Anexo de procesamiento de datos (DPA) de AWS

AWS ofrece un Anexo de procesamiento de datos (DPA RGPD) que cumple con los requisitos del RGPD. El DPA para el RGPD de AWS está integrado en los términos de servicio de AWS y se aplica automáticamente a los clientes de todo el mundo que necesiten cumplir con el RGPD.

El 16 de julio de 2020, el Tribunal de Justicia de la Unión Europea (TJUE) emitió una sentencia relativa al Escudo de la Privacidad UE-EE. UU. y las Cláusulas Contractuales Tipo (SCC), también conocidas como “cláusulas modelo”. El TJUE dictaminó que el Escudo de Privacidad UE-EE. UU. ya no es válido para la transferencia de datos personales de la Unión Europea (UE) a los Estados Unidos (EE. UU.). Sin embargo, en la misma sentencia, el TJUE validó que las empresas pueden seguir utilizando SCC como mecanismo para transferir datos fuera de la UE.

Siguiendo esta sentencia, los clientes y socios de AWS pueden seguir utilizando AWS para transferir su contenido de Europa a Estados Unidos y a otros países, en cumplimiento de las leyes de protección de datos de la UE, incluido el Reglamento general de protección de datos (GDPR). Los clientes de AWS pueden confiar en los SCC incluidos en el Anexo de procesamiento de datos (DPA) de AWS si deciden transferir sus datos fuera de la Unión Europea en cumplimiento del RGPD. A medida que evolucione el panorama normativo y legislativo, trabajaremos para garantizar que nuestros clientes y socios puedan seguir disfrutando de los beneficios de AWS dondequiera que operen. Para obtener información adicional, consulte las preguntas frecuentes sobre el Escudo de Privacidad UE-EE. UU.

El rol de AWS con respecto al RGPD

Bajo el RGPD, AWS desempeña los roles de procesador y controlador de datos.

De conformidad con el artículo 32, los controladores y procesadores están obligados a “…aplicar medidas técnicas y organizativas apropiadas” que tengan en cuenta “el estado de la técnica, los costos de implementación y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas”. El RGPD ofrece sugerencias específicas sobre los tipos de medidas de seguridad que puedan ser necesarias, entre las que se incluyen las siguientes:

- La seudonimización y el cifrado de datos personales.
- La capacidad continuada para garantizar la confidencialidad, integridad, disponibilidad y tolerancia a fallos de los servicios y sistemas de procesamiento.
- La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en el evento de un incidente físico o técnico.
- Un proceso de verificación, evaluación y valoración habitual de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del procesamiento.

AWS como procesador de datos

Cuando los clientes y los socios de AWS Partner Network (APN) usan los servicios de AWS para procesar datos personales en su contenido, AWS se desempeña como procesador de datos. Los clientes y los socios de APN pueden utilizar los controles disponibles en los servicios de AWS, entre los que se incluyen los controles de configuración de la seguridad, para procesar datos personales. En estas circunstancias, el cliente o socio de APN puede desempeñarse como controlador o procesador de datos y AWS cumple el rol de procesador o subprocesador de datos. El Anexo de procesamiento de datos (DPA) de AWS incluye las obligaciones de AWS como procesador de datos.

AWS como controlador de datos

AWS actúa como controlador de datos cuando recopila datos personales y determina los objetivos y los medios a través de los que se procesarán dichos datos personales. Por ejemplo, AWS actúa como controlador de datos cuando procesa información de cuentas para el registro de cuentas, la gestión, el acceso a los servicios o la información de contacto de la cuenta de AWS para proporcionar asistencia mediante actividades de servicio de atención al cliente.

Modelo de seguridad de responsabilidad compartida

La seguridad y el cumplimiento son una responsabilidad compartida entre AWS y el cliente. Cuando los clientes migran los sistemas informáticos y datos a la nube, la responsabilidad en torno a la seguridad recae tanto en el cliente como en el proveedor de servicios en la nube. Cuando los clientes migran a la nube de AWS, AWS es responsable de proteger la infraestructura global en la que se ejecutan todos los servicios ofrecidos en la nube de AWS. Para servicios abstractos como Amazon S3 y Amazon DynamoDB, AWS también es responsable de la seguridad del sistema operativo y la plataforma. Los clientes y socios de APN actúan como controladores o procesadores de datos y son responsables de cualquier cosa que suban o conecten a la nube. Esta diferenciación de la responsabilidad suele denominarse seguridad *de* la nube en contraposición al término seguridad *en* la nube. Este modelo compartido puede ayudar a reducir la carga operativa de los clientes y les ofrece la flexibilidad y el control necesarios para implementar sus infraestructuras en la nube de AWS. Para obtener más información, visite la página web del modelo de responsabilidad compartida de AWS.

El RGPD no cambia el modelo de responsabilidad compartida de AWS, que sigue estando vigente para los clientes y socios de APN interesados en el uso de servicios de computación en la nube. El modelo de responsabilidad compartida es un enfoque útil para ilustrar las diferentes responsabilidades de AWS (como procesador o subprocesador de datos) y de los clientes o socios de APN (como controladores o procesadores de datos) en virtud del RGPD.

Normas de seguridad informática y marco de cumplimiento exhaustivos

En conformidad con el RGPD, es posible que las medidas técnicas y organizativas adecuadas deban incluir "…la capacidad para garantizar la confidencialidad, integridad, disponibilidad y tolerancia a fallos permanentes de los servicios y sistemas de procesamiento", así como procesos de gestión de riesgos general, de restauración y de pruebas de confianza.

Programa de cumplimiento de AWS

AWS mantiene continuamente un alto nivel de seguridad y cumplimiento en todas nuestras operaciones globales. La seguridad siempre ha sido nuestra prioridad más alta, nuestra tarea primordial. AWS se somete regularmente a auditorías independientes de certificación de terceros para garantizar que las actividades de control funcionan según lo previsto. Concretamente, AWS se audita de acuerdo con una variedad de marcos de seguridad mundiales y regionales según la región y el sector. Actualmente, AWS participa en más de 50 programas de auditoría diferentes.

El organismo evaluador documenta los resultados de estas auditorías y los pone a disposición de todos los clientes de AWS a través de AWS Artifact. AWS Artifact es un portal autoservicio gratuito para el acceso bajo demanda a los informes de cumplimiento de AWS. Cuando se publican nuevos informes, estos están disponibles en AWS Artifact, lo que permite a los clientes supervisar continuamente la seguridad y el cumplimiento de AWS y acceder de forma inmediata a nuevos informes.

Los clientes pueden beneficiarse de las certificaciones y acreditaciones reconocidas internacionalmente, que demuestran el cumplimiento de rigurosas normas internacionales como ISO 27017 para la seguridad en la nube, ISO 27018 para la privacidad en la nube, SOC 1, SOC 2 y SOC 3, PCI DSS de nivel 1 y más. AWS también ayuda a los clientes a cumplir las normas de seguridad informática locales, como la Common Cloud Computing Controls Catalogue (C5) de BSI, una certificación respaldada por el Gobierno alemán.

Para obtener información más detallada sobre los programas de certificación de AWS, los informes y las certificaciones de terceros, consulte los programas de cumplimiento de AWS. Para obtener información específica del servicio, consulte los Servicios de AWS en el ámbito del programa de conformidad.

Catálogo de controles de cumplimiento de la computación en la nube

El catálogo de controles de cumplimiento de la computación en la nube (C5) es un esquema de certificación respaldado por el Gobierno alemán e introducido en Alemania por el Servicio Federal de Seguridad de la Información (BSI). Se creó con el fin de ayudar a las organizaciones a demostrar la seguridad operativa frente a ciberataques comunes en el contexto de las *recomendaciones de seguridad para proveedores de la nube* del Gobierno alemán.

Las medidas técnicas y organizativas para proteger los datos y las medidas para la seguridad informática se centran en la seguridad informática de los datos para garantizar su confidencialidad, integridad y disponibilidad. El C5 define los requisitos de seguridad que también pueden ser de interés para proteger los datos. Los clientes de AWS y sus asesores en cumplimiento pueden utilizar la certificación del C5 como un recurso para conocer la gama de servicios de aseguramiento de la seguridad de TI que ofrece AWS a medida que migran sus cargas de trabajo a la nube. El C5 aporta el nivel de seguridad de TI definido por la normativa equivalente a la norma “IT-Grundschutz” alemana, con la incorporación de controles específicos de la nube.

El C5 agrega más controles 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, puede valorar la relación entre las regulaciones legales (como la privacidad de los datos), sus propias políticas o el entorno de amenazas y su uso de servicios de computación en la nube.

Código de conducta de CISPE

El RGPD contempla la aprobación de códigos de conducta para ayudar a los controladores y procesadores a demostrar el cumplimiento del reglamento. Uno de estos códigos a la espera de aprobación oficial es el *Código de conducta de CISPE para proveedores de servicios de computación en la nube* (de ahora en adelante, el *Código*).[3] El Código de conducta de CISPE ayuda a los clientes de la nube a garantizar que su proveedor de infraestructura en la nube esté utilizando estándares de protección de datos adecuados para proteger sus datos de conformidad con el RGPD. Estos son algunos de los beneficios principales del Código:

- **Aclara quién es responsable de cada aspecto de la protección de datos**: El Código explica tanto la función del proveedor de servicios en la nube como la del cliente de acuerdo con el RGPD específicamente en el contexto de los servicios de infraestructura en la nube.

- **Define los principios que deben seguir los proveedores**: El Código desarrolla los principios clave del RGPD en relación con las acciones concretas y las obligaciones que deben desempeñar los proveedores para demostrar el cumplimiento del RGPD y ayudar a los clientes a cumplirlo. Los clientes pueden utilizar estos beneficios concretos en sus propias estrategias de cumplimiento y protección de datos.
- **Les aporta a los clientes la privacidad y la información sobre seguridad necesarias para ayudarlos a lograr sus objetivos de cumplimiento**: El Código exige transparencia a los proveedores en relación con las medidas que llevan a cabo para cumplir las obligaciones relativas a la privacidad y la seguridad. Algunas de estas incluyen la implementación de medidas de seguridad y protección de la privacidad, la notificación de la violación de la seguridad de datos, la eliminación de datos y la transparencia de los subprocesamientos de los datos realizados por terceros. Todas estas obligaciones las verifican organismos independientes de vigilancia. Los clientes pueden utilizar esta información para comprender plenamente los altos niveles de seguridad que se proporcionan.

Para obtener más información, consulte CISPE Public Register, que ofrece a los clientes de AWS la tranquilidad de saber que, cuando utilizan AWS, controlan sus datos en un entorno seguro, protegido y que cumple con la normativa. El cumplimiento del Código por parte de AWS es un nuevo elemento en la lista de certificaciones y acreditaciones internacionales obtenidas por AWS. Esta lista incluye la ISO 27001, ISO 27018, ISO 9001, SOC 1, SOC 2, SOC 3 y el PCI DSS de nivel 1, entre otras.

Controles de acceso a los datos

El artículo 25 del RGPD establece que el responsable del tratamiento "…implementará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del proceso". Al permitir que solo obtengan acceso a los datos de clientes y recursos de AWS los administradores, usuarios y aplicaciones autorizados, los siguientes mecanismos de control de acceso de AWS pueden ayudar a los clientes a cumplir este requisito.

AWS Identity and Access Management

Cuando crea una cuenta en AWS, se genera una cuenta de usuario *raíz* automáticamente en su cuenta de AWS. Esta cuenta de usuario tiene acceso completo a todos los productos y recursos de AWS de su cuenta. En lugar de emplear esta cuenta para las tareas diarias, utilícela únicamente para crear roles o cuentas de usuario adicionales y para llevar a cabo las tareas administrativas que lo precisen. AWS le recomienda que aplique desde el primer momento el principio de los privilegios

mínimos: defina las distintas cuentas de usuario y los roles en relación con las distintas tareas y especifique el número mínimo de permisos necesarios para completar cada una. Este enfoque es un mecanismo para afinar un concepto clave introducido en el RGPD: la protección de datos desde el diseño. AWS Identity and Access Management (IAM) es un servicio web que puede utilizar para controlar de forma segura el acceso a sus recursos de AWS.

Los usuarios y los roles determinan las distintas identidades en IAM que tienen permisos concretos. Un usuario autorizado puede asumir un rol de IAM para realizar tareas específicas. Las credenciales temporales se crean cuando se asume el rol. Por ejemplo, puede utilizar roles de IAM para ofrecer de forma segura aplicaciones que se ejecutan en Amazon Elastic Compute Cloud (Amazon EC2) con credenciales temporales necesarias para acceder a otros recursos de AWS, como los buckets de Amazon S3 y bases de datos de Amazon Relational Database Service (Amazon RDS) o Amazon DynamoDB. Del mismo modo, los roles de ejecución conceden a las funciones de AWS Lambda los permisos necesarios para acceder a otros servicios y recursos de AWS, como Amazon CloudWatch Logs para la transmisión de registros o para leer un mensaje de una cola de Amazon Simple Queue Service (Amazon SQS). Al crear un rol, agregará políticas para definir autorizaciones.

Para ayudar a los clientes a supervisar las políticas de recursos e identificar recursos con acceso público o entre cuentas que no desean, puede habilitar IAM Access Analyzer para generar comprobaciones exhaustivas que identifiquen los recursos a los que se puede acceder desde fuera de una cuenta de AWS. IAM Access Analyzer evalúa las políticas de recursos utilizando la lógica y la inferencia matemáticas para determinar las posibles rutas de acceso permitidas por las políticas. IAM Access Analyzer supervisa continuamente las políticas nuevas o actualizadas y analiza los permisos concedidos mediante políticas para los roles de IAM, pero también para recursos de servicios como los buckets de Amazon S3, las claves de AWS Key Management Service (AWS KMS), las colas de Amazon SQS y las funciones de Lambda.

Access Analyzer para S3 le avisa cuando los buckets de S3 están configurados para permitir el acceso a cualquier usuario de Internet u otras cuentas de AWS, incluidas las cuentas de AWS ajenas a su organización. Al revisar un bucket en riesgo en Access Analyzer para S3, puede bloquear todo acceso público al bucket con un solo clic. AWS recomienda que bloquee todo el acceso a sus buckets a menos que necesite acceso público para permitir un caso de uso específico. Antes de bloquear todo el acceso público, asegúrese de que las aplicaciones seguirán funcionando correctamente sin ese acceso público. Para obtener más información, consulte el uso del bloqueo de acceso público de Amazon S3.

IAM también proporciona información de acceso reciente para ayudarlo a identificar los permisos que no utiliza, de modo que pueda eliminarlos para las entidades principales asociadas. Al utilizar la información de acceso reciente, puede refinar sus políticas y permitir el acceso solo a los servicios y acciones que necesite. Esto ayuda a cumplir

e implementar las prácticas recomendadas de los privilegios mínimos. Puede ver la información de acceso reciente a la que han accedido entidades o políticas existentes en IAM o en todo un entorno de AWS Organizations.

Credenciales temporales de acceso mediante AWS STS

Puede utilizar AWS Security Token Service (AWS STS) para crear credenciales de seguridad temporales que ofrezcan acceso a sus recursos de AWS y para proporcionarles esas credenciales a usuarios de confianza. Las credenciales de seguridad temporales funcionan de forma casi idéntica a las credenciales de clave de acceso a largo plazo que les proporciona a sus usuarios de IAM, con las siguientes diferencias:

- Las credenciales de seguridad temporales solamente son válidas durante un periodo corto concreto. Puede configurar la duración de su validez, desde los 15 minutos hasta un máximo de 12 horas. Una vez que las credenciales temporales caduquen, AWS ya no las reconocerá ni permitirá ningún acceso desde solicitudes de API realizadas con ellas.
- Las credenciales de seguridad temporales no se almacenan junto con la cuenta de usuario, sino que se generan de forma dinámica y se le proporcionan al usuario cuando se solicitan. Los usuarios pueden solicitar nuevas credenciales cuando caduquen las credenciales de seguridad temporales (o antes) si disponen de los permisos necesarios.

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

- No es necesario que distribuya ni incluya credenciales de seguridad de AWS a largo plazo en una aplicación.
- Las credenciales temporales son la base de los roles y de la identidad federada. Puede conceder acceso a sus recursos de AWS a los usuarios con solo definir una identidad temporal de AWS para ellos.
- Las credenciales de seguridad temporales tienen una duración limitada y personalizable, por lo que no es necesario que las cambie o retire por completo cuando dejen de ser necesarias. Una vez que las credenciales caduquen, ya no podrán volver a utilizarse. Puede especificar la duración máxima de su validez.

Multi-Factor Authentication

Para una mayor seguridad, puede agregar la autenticación con dos factores a su cuenta de AWS y a los usuarios de IAM. Una vez Multi-Factor Authentication (MFA) esté habilitado e inicie sesión en la consola de administración de AWS, se le solicitará el nombre de usuario y la contraseña (el primer factor), además de una respuesta de autenticación de su dispositivo MFA AWS (segundo factor). Puede habilitar MFA en su cuenta de AWS y en la de los usuarios individuales de IAM que haya creado en su cuenta. También puede utilizar MFA para controlar el acceso a las API de servicio de AWS.

Por ejemplo, puede definir una política que le permita total acceso a las operaciones de todas las API de AWS en EC2 y negar el acceso a algunas operaciones específicas de las API, como `StopInstances` y `TerminateInstances`, si el usuario no se ha autenticado con MFA.

```
        {
          "Version": "2012-10-17",
          "Statement": [
              {
                 "Sid": "AllowAllActionsForEC2",
                 "Effect": "Allow",
                 "Action": "ec2:*",
                 "Resource": "*"
              },
             {
                 "Sid": "DenyStopAndTerminateWhenMFAIsNotPResent",
                 "Effect": "Deny",
                 "Action": [
                     "ec2:StopInstances",
                     "ec2:TerminateInstances"
                ],
                 "Resource": "*",
                 "Conditions": {
                    "BoolIfExists":
{"aws:MultiFactorAuthPresent":false}
                 }
             }
        }
}
```

Para agregar una barrera adicional de seguridad a los buckets de S3, puede configurar la eliminación con MFA, que requiere una autenticación adicional para cambiar el estado de control de versiones de un bucket y eliminar permanentemente una versión

de un objeto. La eliminación con MFA proporciona seguridad adicional en caso de que sus credenciales de seguridad estén desprotegidas.

Para utilizar la eliminación con MFA, puede utilizar un hardware o un dispositivo MFA virtual para generar un código de autenticación. Consulte la página de Multi-factor Authentication para obtener una lista de dispositivos MFA virtuales o de hardware compatibles.

Acceso a los recursos de AWS

Para implementar un acceso pormenorizado a sus recursos de AWS, puede otorgar distintos niveles de permiso a distintas personas para que tengan acceso a distintos recursos. Por ejemplo, puede permitir que solo algunos usuarios tengan acceso completo a EC2, S3, DynamoDB, Amazon Redshift y otros servicios de AWS.

A otros usuarios puede otorgarles acceso de solo lectura a algunos buckets de Amazon S3, permiso para administrar algunas instancias de EC2 o acceso únicamente a su información de facturación.

La siguiente política es un ejemplo de uno de los métodos que puede utilizar para permitir todas las acciones en un bucket concreto de Amazon S3 y denegar explícitamente el acceso al resto de los servicios de AWS que no sean Amazon S3.

```
{
          "Version": "2012-10-17",
          "Statement": [
              {
                 "Effect": "Allow",
                 "Action": "s3:*",
                 "Resource": [
                      "arn:aws:s3:::bucket-name",
                      "arn:aws:s3:::bucket-name/*"
                  ],
               },
               {
                 "Effect": "Deny",
                 "NotAction": "s3:*",
                 "NotResource": [
                      "arn:aws:s3:::bucket-name",
                      "arn:aws:s3:::bucket-name/*"
                  ]
                }
            ]
}
```

Puede añadir una política a una cuenta de usuario o rol. Para conocer otros ejemplos de políticas de IAM, consulte los ejemplos de políticas basadas en identidad de IAM.

Definición de límites para el acceso a servicios regionales

Como cliente, mantiene la propiedad de su contenido y selecciona qué servicios de AWS pueden procesar, almacenar y alojar su contenido. AWS no accede a su contenido ni lo utiliza para ningún propósito sin su consentimiento. Según el modelo de responsabilidad compartida, puede elegir las regiones de AWS en las que se almacena el contenido, lo que le permite implementar servicios de AWS en las ubicaciones que desee, de acuerdo con sus requisitos geográficos específicos. Por ejemplo, si desea asegurarse de que su contenido se ubique solo en Europa, puede optar por implementar servicios de AWS exclusivamente en una de las regiones europeas de AWS.

Las políticas de IAM proporcionan un mecanismo simple para limitar el acceso a los servicios en regiones específicas. Puede agregar una condición global (*aws:RequestedRegion*) a las políticas asociadas a sus entidades principales de IAM para aplicarlo a todos los servicios de AWS. Por ejemplo, la siguiente política utiliza el elemento `NotAction` con el efecto `Deny`, que deniega explícitamente el acceso a todas las acciones no enumeradas en la instrucción si la región solicitada no es europea. Las acciones de los servicios CloudFront, IAM, Amazon Route 53 y AWS Support no deben denegarse porque se trata de servicios globales populares de AWS.

```
{
        "Version": "2012-10-17",
        "Statement": [
            {
               "Sid": "DenyAllOutsideRequestedRegions",
               "Effect": "Deny",
               "NotAction": [
                    "cloudfront:*",
                    "iam:*",
                    "route53:*",
                    "support:*"
                ],
                "Resource": "*",
                "Condition": {
                   "StringNotLike": {
                       "aws:RequestedRegion": [
                            "eu-*"
                       ]
                    }
```

```
                        }
                    }
                ]
}
```

Este ejemplo de política de IAM también se puede implementar como una Service Control Policy (SCP, Política de control de servicios) en AWS Organizations, que define los límites de los permisos aplicados a cuentas o unidades organizativas (OU) específicas de AWS dentro de una organización. Esto le permite controlar el acceso de los usuarios a servicios regionales en entornos complejos de varias cuentas.

Existen opciones de limitación geográfica para las nuevas regiones introducidas. Las regiones introducidas después del 20 de marzo de 2019 están deshabilitadas de forma predeterminada. Antes de poder utilizarlas, debe habilitar estas regiones. Si una región de AWS está deshabilitada por defecto, puede utilizar la consola de administración de AWS para habilitar o deshabilitar la región. Habilitar y deshabilitar regiones en AWS le permite controlar si los usuarios de su cuenta de AWS tendrán acceso a los recursos en dicha región.[4]

Control de acceso a aplicaciones web y móviles

AWS ofrece un servicio para gestionar el control de acceso a los datos en las aplicaciones de los clientes. Si necesita añadir un inicio de sesión y las funciones de control de acceso a las aplicaciones de su web y a sus aplicaciones móviles, puede utilizar Amazon Cognito. Los grupos de usuarios de Amazon Cognito ofrecen un directorio de usuarios seguro que puede albergar hasta cientos de millones de usuarios. Para proteger la identidad de los usuarios, puede añadir Multi-Factor Authentication (MFA) a sus grupos de usuarios. También puede utilizar la autenticación adaptativa, que permite usar un modelo basado en el riesgo para predecir cuándo necesitará otro factor de autenticación.

Con los grupos de identidades de Amazon Cognito (identidades federadas), puede ver quién ha accedido a sus recursos y desde dónde (aplicación móvil o aplicación web). Puede utilizar esta información para crear roles de IAM y políticas que le permitan conceder o denegar el acceso a un recurso en función del tipo de origen del acceso (aplicación móvil o web) y del proveedor de identidades.

Monitorización y registro

El artículo 30 del RGPD establece que "…cada responsable y, en su caso, su representante llevarán un registro de las actividades de tratamiento efectuadas bajo su responsabilidad". Este artículo también incluye información sobre qué tipo de datos deben registrarse cuando se monitoriza el procesamiento de todos los datos

personales. Los controladores y los procesadores también deben comunicar cualquier violación de manera oportuna, por lo que es importante detectar los incidentes rápidamente. Para ayudar a que los clientes puedan cumplir dichas obligaciones, AWS ofrece los siguientes servicios de registro y monitorización:

Gestión y configuración de activos con AWS Config

AWS Config ofrece una vista detallada de la configuración de los distintos recursos de AWS en su cuenta de AWS. La vista incluye la manera en la que los recursos se relacionan entre sí y cuál era su configuración anterior para que pueda ver las modificaciones implementadas en las configuraciones y relaciones con el transcurso del tiempo.

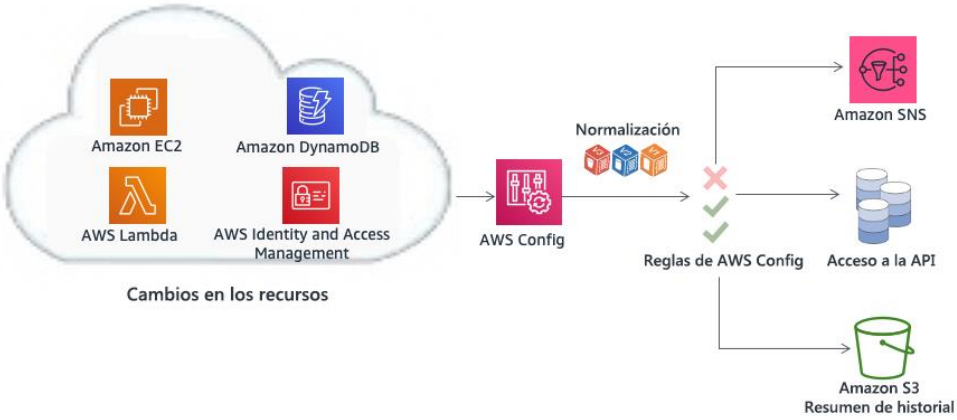

Figura 1: La configuración de la monitorización cambia a lo largo del tiempo con AWS Config

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

Con AWS Config, puede hacer lo siguiente:

- Evaluar las configuraciones de recursos de AWS para verificar si los valores son correctos.
- Obtener un resumen de las configuraciones actuales de los recursos admitidos asociados a su cuenta de AWS.
- Obtener las configuraciones de uno o más recursos existentes en su cuenta.
- Obtener las configuraciones históricas de uno o más recursos.
- Recibir una notificación cuando se cree, modifique o elimine un recurso.

- Ver las relaciones entre los recursos. Por ejemplo, puede ver todos los recursos que utilicen un grupo de seguridad determinado.

Auditoría de cumplimiento y análisis de seguridad

Con AWS CloudTrail, puede monitorizar de forma constante la actividad de su cuenta de AWS. Muestra el historial de llamadas a la API de AWS a su cuenta, incluidas las realizadas a través de la consola de administración de AWS y los kits de desarrollo de software (SDK) de AWS, las herramientas de línea de comandos y otros productos de mayor nivel de AWS. Puede identificar a los usuarios y las cuentas que llamaron a las API de AWS para solicitar servicios compatibles con CloudTrail, la dirección IP desde la que se efectuaron las llamadas y cuándo se realizaron. Puede integrar CloudTrail en las aplicaciones con la API, automatizar la creación de seguimientos en su organización, comprobar el estado de los seguimientos y controlar la manera en que los administradores habilitan y deshabilitan los registros de CloudTrail.

Los registros de CloudTrail pueden agregarse desde varias regiones y varias cuentas de AWS en un único bucket de S3. AWS recomienda escribir registros, especialmente los registros de AWS CloudTrail, en un bucket de S3 con acceso restringido en una cuenta de AWS designada para registros (archivo de registro). Los permisos del bucket deben impedir la eliminación de los registros, y también deben cifrarse en reposo mediante el cifrado en el lado del servidor con claves de cifrado gestionadas por Amazon S3 (SSE-S3) o por AWS KMS (SSE-KMS). La validación de la integridad del archivo de registro de CloudTrail se puede utilizar para determinar si un archivo de registro se modificó, eliminó o no se cambió después de que CloudTrail lo entregara. Esta característica está basada en algoritmos estándar del sector: SHA-256 para hash y SHA-256 con RSA para firmas digitales. Esto hace que computacionalmente sea difícil modificar, eliminar o falsificar archivos de registro de CloudTrail sin ser detectados. Puede utilizar la interfaz de línea de comandos (CLI) de AWS para validar los archivos en la ubicación a la que CloudTrail los entregó.

Los registros de CloudTrail agregados en un bucket de S3 pueden analizarse con fines de auditoría o para actividades de solución de problemas. Una vez centralizados los registros, puede integrarlos con las soluciones de gestión de eventos e información de seguridad (SIEM) o utilizar servicios de AWS, como Amazon Athena o CloudTrail Insights, para analizarlos y visualizarlos mediante Amazon QuickSight Dashboards. Una vez que haya centralizado los registros de CloudTrail, también puede utilizar la misma cuenta del archivo de registro para centralizar los registros de otros orígenes, como CloudWatch Logs y los balanceadores de carga de AWS.

Figura 2: Ejemplo de la arquitectura de las auditorías de cumplimiento y el análisis de la seguridad con AWS CloudTrail

Los registros de AWS CloudTrail también pueden emitir eventos preconfigurados de Amazon CloudWatch Events. Puede utilizar estos eventos para notificar a otros usuarios o sistemas que se ha producido un evento o para realizar correcciones. Por ejemplo, si quiere monitorizar las actividades de las instancias EC2, puede crear una regla de eventos de CloudWatch Events. Cuando se produce una actividad específica en la instancia de Amazon EC2 y el evento se guarda en los registros, la regla activa una función Lambda que envía un correo electrónico de notificación acerca del evento al administrador (consulte la Figura 3). El correo electrónico incluye detalles como cuándo ocurrió el evento, qué usuario realizó la acción, detalles de EC2 y mucho más. El siguiente diagrama muestra la arquitectura de la notificación de eventos.

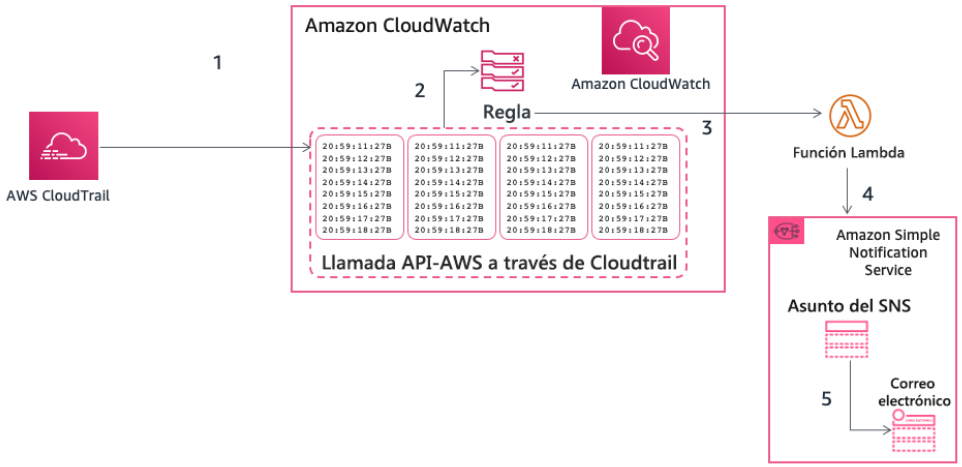

Figura 3: Ejemplo de la notificación de eventos en AWS CloudTrail

Recopilación y procesamiento de registros

Puede usar CloudWatch Logs para monitorizar y almacenar archivos de registro, así como acceder a ellos, desde instancias EC2, AWS CloudTrail, Route 53 y otros orígenes. Consulte la página de documentación de servicios de AWS que publican registros en CloudWatch Logs.

La información de registros incluye, por ejemplo:

- Un registro pormenorizado de acceso a objetos de S3.
- Información detallada sobre flujos en la red mediante VPC-Registros de flujo
- Acciones y verificaciones de la configuración basadas en las reglas de AWS Config.
- Filtrado y monitorización del acceso HTTP a aplicaciones por medio de las funciones del firewall de aplicaciones web (WAF) en CloudFront.

También puede publicar las métricas y los registros de aplicaciones personalizados en CloudWatch Logs al instalar CloudWatch Agent en instancias EC2 o servidores en las instalaciones.

Los registros pueden analizarse de forma interactiva mediante CloudWatch Logs Insights y realizan consultas para ayudarlo a responder de manera más eficiente y eficaz a los problemas operativos.

Los eventos de registro de CloudWatch Logs pueden procesarse casi en tiempo real al configurar filtros de suscripción y al entregarse a otros servicios como un clúster de Amazon Elasticsearch Service (Amazon ES), una transmisión de Amazon Kinesis, una transmisión de Amazon Kinesis Data Firehose o Lambda para un procesamiento, análisis o carga en otros sistemas de forma personalizada.

Los filtros de métricas de CloudWatch se pueden utilizar para definir patrones de búsqueda en los datos de registro, transformarlos en métricas numéricas de CloudWatch y configurar alarmas basadas en los requisitos de su sector. Por ejemplo, siguiendo la recomendación de AWS de no utilizar el usuario raíz para tareas diarias, es posible configurar un filtro de métricas de CloudWatch específico en un registro de CloudTrail (entregado a CloudWatch Logs) para crear una métrica personalizada y configurar una alarma para notificar a las partes interesadas pertinentes cuando se utilicen las credenciales raíz para acceder a su cuenta de AWS.

Se pueden entregar los registros de acceso al servidor de S3, los registros de acceso de Elastic Load Balancing, los registros de flujo de VPC y los registros de flujo de AWS Global Accelerator directamente a un bucket de S3. Por ejemplo, cuando habilite los registros de acceso al servidor de Amazon S3, puede obtener información detallada sobre las solicitudes que se realizan a su bucket de S3. Un registro de acceso contiene detalles sobre la solicitud, como el tipo de solicitud, los recursos especificados y la fecha y hora en la que fue procesada. Para obtener más información acerca del contenido de un registro, consulte el formato de registro de acceso al servidor de Amazon S3 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 forma predeterminada, S3 no recopila registros de acceso a servicios, pero cuando habilita el registro, S3 generalmente entrega registros de acceso a su bucket en unas pocas horas. Si necesita una entrega más rápida o necesita entregar registros a varios destinos, considere la posibilidad de utilizar registros de CloudTrail o una combinación de registros de CloudTrail y S3. Los registros se pueden cifrar en reposo al configurar el cifrado de objetos predeterminado en el bucket de destino. Los objetos se cifran mediante el cifrado en el lado del servidor con claves gestionadas por S3 (SSE-S3) o claves maestras del cliente (CMK) almacenadas en AWS Key Management Service (AWS KMS).

Los registros almacenados en un bucket de S3 se pueden consultar y analizar por medio de Amazon Athena. Amazon Athena es un servicio de consultas interactivo que le permite analizar datos en Amazon S3 con SQL estándar. Se puede usar Athena para ejecutar consultas ad-hoc con ANSI SQL, sin necesidad de combinar ni cargar datos en Athena. Athena puede procesar conjuntos de datos no estructurados, semiestructurados y estructurados y se integra con Amazon QuickSight para facilitar su visualización.

Los registros también son una fuente de información útil para la detección automatizada de amenazas. Amazon GuardDuty es un servicio de monitorización continua de seguridad que analiza y procesa eventos de varios orígenes, como los registros de flujo de VPC, los registros de eventos de gestión de CloudTrail, los registros de eventos de datos de S3 de CloudTrail y los registros de DNS. Utiliza fuentes de inteligencia contra amenazas, como listas de direcciones IP y dominios maliciosos y aprendizaje automático para identificar actividades inesperadas, potencialmente no autorizadas y maliciosas dentro de su entorno de AWS. Cuando habilita GuardDuty en una región, este comienza inmediatamente a analizar los registros de eventos de CloudTrail. Se beneficia de la gestión de CloudTrail y los eventos de datos de S3 directamente desde CloudTrail a través de un flujo de eventos independiente y duplicado.

Descubrimiento y protección de datos a escala con Amazon Macie

El artículo 32 del RGPD establece que “…el responsable y el encargado del tratamiento implementarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros: […]

(b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y tolerancia a fallos permanentes de los sistemas y servicios de tratamiento;

[…]

(d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento”.

Tener un proceso continuo de clasificación de datos es fundamental para ajustar el tratamiento de los datos de seguridad a la naturaleza de los datos. Si su organización gestiona datos confidenciales, supervise dónde residen, protéjalos adecuadamente y ofrezca evidencia de que está aplicando la seguridad y la privacidad informática de los datos según sea necesario para cumplir con los requisitos de cumplimiento normativo. Para ayudar al cliente a identificar y proteger sus datos confidenciales a escala, AWS ofrece Amazon Macie, un servicio de privacidad y seguridad informática de datos totalmente gestionado que utiliza modelos de correspondencia de patrones y el aprendizaje automático para identificar información de identificación personal (PII) y descubrir y proteger los datos confidenciales almacenados en buckets de S3. Amazon Macie evalúa estos buckets y proporciona una categorización de datos mediante identificadores de datos gestionados y diseñados para detectar distintas categorías de datos confidenciales. Macie puede detectar PII como nombres completos, direcciones de correo electrónico, fechas de nacimiento, números de identidad nacionales, identificaciones fiscales o números de referencia, etc.[5] El cliente puede definir identificadores de datos personalizados que reflejen los escenarios particulares de su organización (por ejemplo, números de cuenta de clientes o clasificación interna de datos).

Amazon Macie evalúa continuamente los objetos dentro de los buckets y proporciona automáticamente un resumen de las conclusiones (Figura 4) de los datos no cifrados o accesibles públicamente hallados que coinciden con la categoría de datos definida. Estos datos pueden incluir alertas para los objetos o buckets no cifrados y accesibles públicamente que son compartidos con cuentas de AWS fuera de las definidas en AWS Organizations. Amazon Macie se integra con otros servicios de AWS, como AWS Security Hub, para generar resultados de seguridad que se pueden procesar y proporcionar una acción automática y de respuesta ante los resultados (Figura 5).

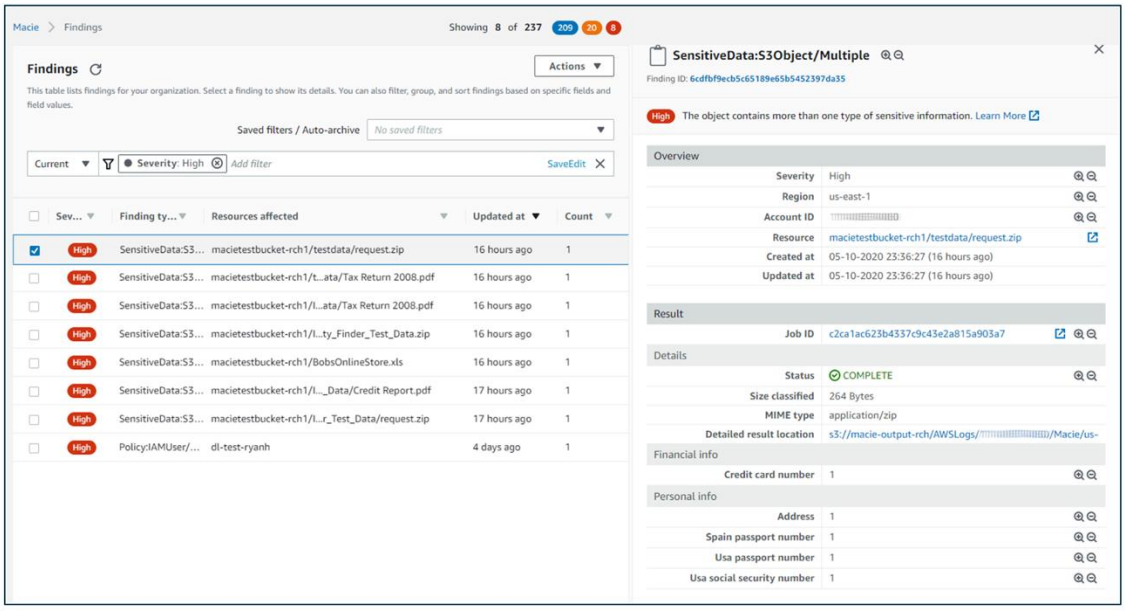

Figura 4: Inspecciones de datos y ejemplo de búsqueda

Gestión centralizada de la seguridad informática

Numerosas organizaciones deben hacer frente a desafíos relacionados con la visibilidad y la gestión centralizada de sus entornos. A medida que crece su huella operativa, este desafío puede acrecentarse a menos que sopese detenidamente diseños de seguridad. La falta de conocimientos y una gestión descentralizada y desigual de los procesos de gobierno y seguridad pueden provocar que su entorno sea vulnerable.

AWS ofrece herramientas que lo ayudan a afrontar algunos de los desafíos más importantes relacionados con la gestión y el gobierno de TI, así como herramientas para favorecer la protección de los datos con un enfoque basado en el diseño.

AWS Control Tower ofrece un método para configurar y controlar un nuevo entorno de AWS seguro con distintas cuentas. Automatiza la configuración de la zona de inicio[6], que es un entorno con distintas cuentas basado en prototipos de las prácticas recomendadas, y permite controlarlo con medidas de contención que puede seleccionar de una lista previamente empaquetada. Las medidas de contención implementan las reglas de gobierno relativas a la seguridad, el cumplimiento y las operaciones. AWS Control Tower permite la gestión de la identidad a través del directorio por defecto de AWS Single Sign-On (SSO) y la ejecución de auditorías entre cuentas con AWS SSO y AWS IAM. También centraliza los registros procedentes de CloudTrail y AWS Config, que se almacenan en S3.

AWS Security Hub es otro servicio que permite la centralización y ayuda a mejorar la visibilidad en una organización. Security Hub centraliza y prioriza los datos de seguridad y cumplimiento de las cuentas y servicios de AWS como Amazon GuardDuty y Amazon Inspector, y puede integrarse en el software de seguridad informática de terceros para ayudarlo a analizar las tendencias de seguridad e identificar los problemas de seguridad más prioritarios.

Amazon GuardDuty es un servicio inteligente de detección de amenazas que puede ayudar a los clientes a supervisar y proteger sus cuentas, cargas de trabajo y datos de AWS almacenados en S3 con mayor precisión y facilidad. GuardDuty analiza miles de millones de eventos en sus cuentas de AWS desde varios orígenes, incluidos los eventos de gestión de AWS CloudTrail, los eventos de datos de S3 de AWS CloudTrail, los registros de flujo de Amazon VPC y los registros DNS. Por ejemplo, detecta llamadas a la API inusuales, comunicaciones salientes sospechosas a direcciones IP maliciosas conocidas o posibles robos de datos mediante consultas DNS como mecanismo de transporte. GuardDuty es capaz de proporcionar resultados más precisos al utilizar la información acerca de amenazas basada en el aprendizaje automático y en los socios de seguridad externos.

Amazon Inspector es un servicio automático de evaluación de seguridad mediante el que se permite mejorar la seguridad y el cumplimiento de las aplicaciones

implementadas en las instancias EC2. Amazon Inspector evalúa automáticamente las aplicaciones para detectar exposiciones, vulnerabilidades y desviaciones de las prácticas recomendadas. Después de la evaluación, Amazon Inspector genera una lista detallada de problemas de seguridad ordenados por nivel de gravedad.

Amazon CloudWatch Events le permite configurar su cuenta de AWS para enviar eventos a otras cuentas de AWS o recibir los eventos de otras cuentas u organizaciones. Este mecanismo puede ser muy útil para implementar situaciones de respuesta a incidentes entre cuentas al llevarse a cabo acciones correctivas a su debido tiempo (por ejemplo, al llamar a la función Lambda o ejecutar un comando en una instancia EC2) si fueran necesarias cada vez que se produzca un incidente de seguridad informática.

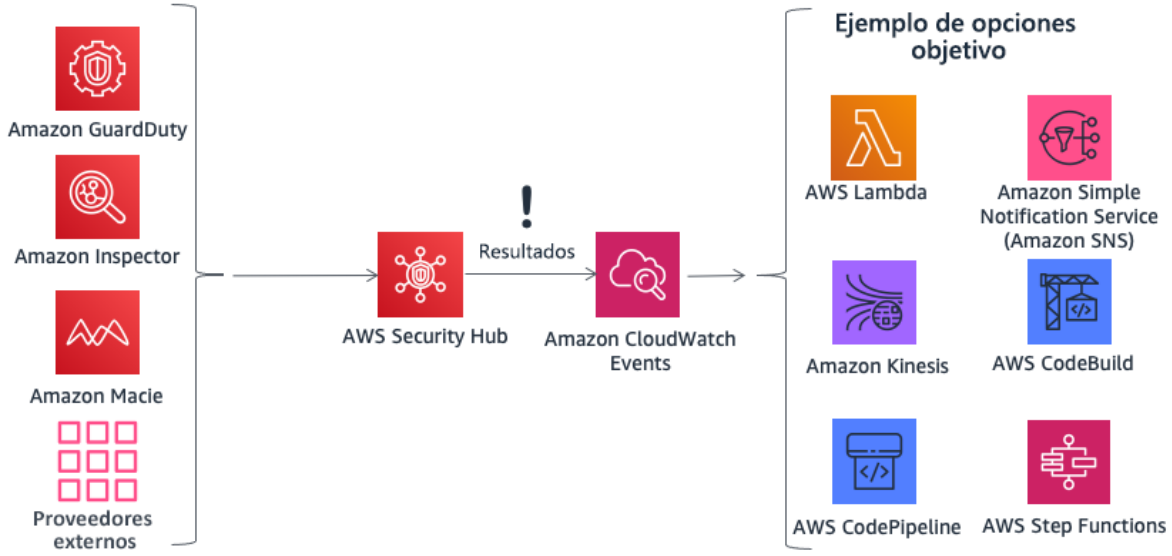

Figura 5: Ejecución de una acción con AWS Security Hub y AWS CloudWatch Events

AWS Organizations lo ayuda a gestionar y dirigir de forma centralizada entornos complejos. Asimismo, le permite controlar los accesos, el cumplimiento y la seguridad en un entorno con distintas cuentas. AWS Organizations es compatible con las políticas de control de servicios (SCP), que definen las acciones de los servicios de AWS que pueden usarse con cuentas o unidades organizativas (OU) específicas dentro de una organización.

AWS Systems Manager le proporciona visibilidad y control para su infraestructura en AWS. Puede ver los datos operativos de varios servicios de AWS desde una consola unificada y automatizar las tareas operativas en todos ellos. Puede obtener información sobre las actividades recientes de la API, los cambios en la configuración de los recursos, las alertas operativas, el inventario de software y el estado de cumplimiento de los parches. Mediante la integración con otros servicios de AWS, también puede

tomar medidas para los recursos en función de sus necesidades operativas para que su entorno logre un estado de cumplimiento.

Por ejemplo, al integrar Amazon Inspector con AWS Systems Manager, las evaluaciones de seguridad se simplifican y automatizan, ya que puede instalar el agente Amazon Inspector automáticamente mediante Amazon EC2 Systems Manager cuando se inicia una instancia EC2. También puede realizar correcciones de forma automática en los resultados de Amazon Inspector mediante las funciones System Manager y Lambda de EC2.

Protección de sus Datos en AWS

El artículo 32 del RGPD exige que las organizaciones "…implementen medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya… la seudonimización y el cifrado de datos personales…". Además, las organizaciones deben proteger ante la divulgación de datos personales o su acceso a ellos de forma no autorizada.

El cifrado reduce los riesgos asociados al almacenamiento de datos personales porque estos datos no pueden leerse sin la clave correcta. Una estrategia rigurosa de cifrado puede ayudar a mitigar el impacto de varios eventos relacionados con la seguridad, como algunas infracciones de seguridad.

Cifrado de datos en reposo

El cifrado de datos en reposo es esencial para el cumplimiento normativo y la protección de los datos. Ayuda a garantizar que ningún usuario ni aplicación puedan leer los datos confidenciales almacenados en discos sin una clave válida. AWS ofrece distintas opciones de cifrado en reposo y de gestión de las claves de cifrado. Por ejemplo, puede utilizar SDK de cifrado de AWS con una CMK creada y gestionada por AWS KMS para cifrar datos arbitrarios.

Los datos cifrados pueden almacenarse con seguridad en reposo y solo pueden descifrarlos los usuarios con acceso autorizado a la CMK. Como resultado, puede obtener datos confidenciales con cifrado de sobre, mecanismos de políticas para la autorización y autenticación del cifrado y registros de auditoría a través de AWS CloudTrail. Algunos de los servicios básicos de AWS cuentan con funciones integradas de cifrado en reposo, lo que ofrece la opción de cifrar datos antes de que se escriban en un almacenamiento no volátil. Por ejemplo, puede cifrar volúmenes de Amazon EBS y configurar buckets de S3 para el cifrado en el lado del servidor (SSE) mediante el cifrado AES-256. S3 también es compatible con el *cifrado del lado del cliente*, lo que le permite cifrar datos antes de enviarlos a S3. Los SDK de AWS admiten el cifrado del lado del cliente para facilitar las operaciones de cifrado y descifrado de objetos. Amazon RDS también admite el cifrado de datos transparente (TDE).

Es posible cifrar datos en almacenes de instancias EC2 de Linux mediante el uso de bibliotecas integradas de Linux. Mediante este método, se cifran los archivos de forma transparente, lo que protege los datos confidenciales. Como resultado, las aplicaciones que procesan los datos ignoran el cifrado a nivel del disco.

Puede utilizar dos métodos para cifrar archivos en almacenes de instancias:

- **Cifrado a nivel del disco**: con este método, todo el disco o un bloque dentro del disco se cifra utilizando 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.
- **Cifrado a nivel del sistema de archivos:** Con este método, se cifran los archivos y los directorios, pero no el disco entero ni una partición. El cifrado a nivel del sistema de archivos funciona sobre el sistema de archivos y se puede transferir a diversos sistemas operativos.

En el caso de los volúmenes de almacén de instancias SSD de las memorias no volátiles exprés (NVMe), *el cifrado a nivel de disco* es la opción predeterminada. Los datos en un almacenamiento de instancias basado en NVMe se cifran mediante un cifrado en bloque XTS-AES-256 implementado en un módulo de hardware de la instancia. Las claves de cifrado se generan mediante el módulo de hardware y son exclusivas para cada dispositivo de almacenamiento de la instancia basado en NVMe. Todas las claves de cifrado se destruyen cuando se detiene o se termina la instancia y no se pueden recuperar. No puede utilizar sus propias claves de cifrado.

Cifrado de datos en tránsito

AWS recomienda encarecidamente cifrar los datos en tránsito de un sistema a otro, incluidos los recursos dentro y fuera de AWS.

Cuando crea una cuenta en AWS, se le asigna Amazon Virtual Private Cloud (Amazon VPC), una sección aislada lógicamente de la nube de AWS. Desde aquí puede lanzar recursos de AWS en una red virtual que usted defina. Puede controlar todos los aspectos del entorno de red virtual, incluida la selección de su propio intervalo de direcciones IP, la creación de subredes y la configuración de tablas de rutas y gateways de red. También puede crear una conexión de redes virtuales privadas (VPN) de hardware entre el centro de datos corporativo y su Amazon VPC; de esta manera, puede utilizar la nube de AWS como una extensión del centro de datos corporativo.

Para proteger la comunicación entre su Amazon VPC y su centro de datos corporativo, puede seleccionar distintas opciones de conectividad de VPN y decidir cuál es la que mejor se ajusta a sus necesidades. Puede utilizar el cliente VPN de AWS para habilitar

el acceso seguro a sus recursos de AWS a través de los servicios del cliente VPN. También puede utilizar un dispositivo VPN por software de terceros disponible en AWS Marketplace, que puede instalar en una instancia EC2 en Amazon VPC. O bien, puede crear una conexión IPsec en la VPN para proteger la comunicación entre su VPC y su red remota. Para crear una conexión privada exclusiva desde una red remota a su VPC de Amazon puede utilizar AWS Direct Connect. Puede combinar esta conexión con una VPN sitio a sitio de AWS para crear una conexión privada y cifrada con IPsec.

AWS ofrece puntos de enlace HTTPS a través del protocolo TLS para llevar a cabo la comunicación, lo que ofrece un cifrado en tránsito cuando utilice las API de AWS. Puede utilizar el servicio AWS Certificate Manager (ACM) para generar, gestionar e implementar los certificados privados y públicos que utilice con vistas a establecer un transporte cifrado de sus cargas de trabajo entre los sistemas. Amazon Elastic Load Balancing está integrado en ACM y permite la compatibilidad con los protocolos HTTPS. Si se distribuye el contenido a través de Amazon CloudFront, este sistema será compatible con los puntos de enlace cifrados.

Herramientas de cifrado

AWS ofrece varios servicios de cifrado de datos escalables, herramientas y mecanismos para ayudarlo a proteger los datos almacenados y procesados en AWS. Para obtener más información sobre la privacidad y la funcionalidad del servicio de AWS, consulte las capacidades de los servicios de AWS para consideraciones de privacidad.[7]

Los servicios de criptografía de AWS utilizan una amplia gama de tecnologías de cifrado y almacenamiento que se han diseñado para conservar la integridad y confidencialidad de sus datos en reposo o tránsito. AWS ofrece cuatro servicios y herramientas principales para llevar a cabo las operaciones criptográficas:

- **AWS Key Management Service** (AWS KMS) es un servicio gestionado por AWS que genera y gestiona tanto las claves maestras como las claves de datos. AWS KMS está integrado en numerosos servicios de AWS para ofrecer el cifrado de datos en el lado del servidor con las claves de KMS pertenecientes a las cuentas de los clientes. Los módulos de seguridad de hardware (HSM) de KMS son FIPS 140-2 de nivel 2 validados.
- **AWS CloudHSM** proporciona HSM con validación FIPS 140-2 de nivel 3. Estos almacenan de forma segura las distintas claves criptográficas autoadministradas, entre las que se encuentran las claves maestras y los datos maestros.
- **Servicios y herramientas criptográficos de AWS**
  - **El SDK de cifrado de AWS** ofrece una biblioteca de cifrado en el lado del cliente para implementar las operaciones de cifrado y descifrado en *todos* los tipos de datos.

- **El cliente de cifrado de Amazon DynamoDB** ofrece una biblioteca de cifrado en el lado del cliente para cifrar tablas de datos antes de enviarlas a un servicio de base de datos, como Amazon DynamoDB.

AWS Key Management Service

AWS Key Management Service (AWS KMS) es un servicio gestionado que le facilita la creación y el control de las claves de cifrado empleadas para cifrar los datos y utiliza módulos de seguridad de hardware (HSM) a fin de proteger la seguridad de las claves. AWS KMS está integrado en otros productos de AWS para ayudarlo a proteger los datos que almacena con estos servicios. AWS KMS también está integrado en AWS CloudTrail para ofrecerle registros del uso de todas sus claves para satisfacer sus necesidades normativas y de cumplimiento.

Puede crear, importar claves maestras 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 CMK de AWS KMS, tanto si las ha importado como si AWS KMS las ha creado por usted, se almacenan cifradas en un almacén de larga duración para garantizar su uso cuando sea necesario. Puede decidir si AWS KMS cambiará automáticamente las CMK creadas en AWS KMS una vez al año sin necesidad de tener que volver a cifrar los datos que ya se han cifrado con la clave maestra. No necesita llevar un seguimiento de las versiones anteriores de las CMK porque AWS KMS las mantiene disponibles para descifrar los datos cifrados anteriormente de forma automática.

En relación con cualquier CMK en KMS, puede controlar quién tiene acceso a dichas claves y con qué servicios se pueden utilizar con una serie de controles de acceso, como concesiones y condiciones en las políticas clave o las de IAM. También puede importar claves de su infraestructura de gestión de claves y utilizarlas en KMS.

Por ejemplo, la siguiente política utiliza la condición `kms:ViaService` para permitir que un cliente gestione una CMK para utilizarla en acciones concretas solo cuando la petición proceda de EC2 o RDS en una región concreta (*us-west-2*) y en nombre de un usuario específico (`ExampleUser`).

```
{
          “Version”: “2012-10-17”,
          “Statement”: [
              {
                 “Effect”: “Allow”,
                 “Principal”: {
```

```
                    "AWS":
"arn:aws:iam::111122223333:user/ExampleUser"
                 }
                "Action": [
                     "kms:Encrypt*",
                     "kms:Decrypt",
                     "kms:ReEncrypt*",
                     "kms:GenerateDataKey*",
                     "kms:CreateGrant",
                     "kms:ListGrants",
                     "kms:DescribeKey"
                 ],
                 "Resource": "*",
                 "Condition": {
                    "ForAnyValue:StringEquals": {
                        "kms:ViaService": [
                              "ec2.us-west-2.amazonaws.com",
                              "rds.us-west-2.amazonaws.com"
                        ]
                     }
               }
}
```

Integración de los servicios de AWS

AWS KMS está integrado con otros servicios de AWS. Consulte el sitio web de KMS para obtener una lista completa de los servicios integrados. Esta integración le permite usar fácilmente las CMK de AWS KMS para cifrar los datos que almacene en estos servicios. Además de utilizar una CMK gestionada por el cliente, existen numerosos servicios integrados que le permiten utilizar una CMK gestionada por AWS y que se creará y gestionará automáticamente. Esta clave solo puede utilizarse en el servicio concreto que la ha generado.

Capacidades de auditoría

AWS CloudTrail registra cada uso de una clave que almacena en KMS en un archivo de registro y se entrega al bucket de S3 especificado en la configuración de CloudTrail. La información registrada incluye detalles del usuario, la hora, la fecha, la operación realizada y la clave utilizada.

Seguridad

AWS KMS está diseñado para garantizar que nadie pueda acceder a sus claves maestras. El servicio se basa en sistemas diseñados para proteger las claves maestras

con técnicas extensivas de seguridad reforzada, como no almacenar jamás claves maestras de texto plano en el disco, no mantenerlas en la memoria y limitar los sistemas que puedan conectarse a los hosts que usan claves. Todo el acceso al software de actualización del servicio lo dirige un control de acceso de varios niveles de cuya auditoría y revisión se encarga un grupo independiente dentro de AWS.

Para obtener más información sobre AWS KMS, consulte el documento técnico *AWS Key Management Service*.

AWS CloudHSM

AWS CloudHSM es un módulo de seguridad de hardware (HSM) basado en la nube que lo ayuda a cumplir los requisitos corporativos, contractuales y de cumplimiento normativo de seguridad informática de los datos, ya que le permite generar y utilizar sus claves de cifrado en un hardware validado por FIPS 140-2 de nivel 3.

Con CloudHSM controla las claves de cifrado y las operaciones criptográficas que ejecutan los 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 necesario incorporar protección adicional en las aplicaciones y los datos que estén sujetos a requisitos regulatorios o contractuales estrictos para la gestión de las claves de cifrado. Anteriormente, la única opción para almacenar datos sensibles (o de las claves de cifrado que protegían los datos sensibles) era hacerlo en centros de datos en las instalaciones. Esto podría haber impedido que usted migrara estas aplicaciones a la nube o hecho se redujera significativamente su rendimiento. Gracias a AWS CloudHSM, puede proteger sus claves de cifrado en los HSM estipulados y aprobados de acuerdo con los estándares gubernamentales para la gestión segura de claves. Puede crear, almacenar y gestionar de manera segura las claves utilizadas para el cifrado de datos para asegurarse de que solo usted pueda obtener acceso a ellos. AWS CloudHSM lo ayuda a cumplir los estrictos requisitos de gestión de claves sin reducir el rendimiento de la aplicación.

El servicio AWS CloudHSM funciona con Amazon VPC. Las instancias de CloudHSM se suministran en su Amazon VPC con la dirección IP que usted especifique, lo que proporciona una conectividad de red sencilla y privada a sus instancias EC2. Cuando sitúa las instancias de CloudHSM cerca de las instancias EC2, se reduce la latencia de la red, lo que a su vez puede mejorar el rendimiento de la aplicación. AWS proporciona acceso exclusivo y específico (instancia única) a las instancias de CloudHSM, que se encuentran aisladas de otros clientes de AWS. CloudHSM, disponible en varias regiones y zonas de disponibilidad, le permite añadir un almacenamiento de claves seguro y duradero a sus aplicaciones.

Integración con los productos de AWS y las aplicaciones de terceros

Puede utilizar CloudHSM con Amazon Redshift, Amazon RDS para Oracle o aplicaciones de terceros (como SafeNet Virtual KeySecure) para que funcionen como raíz de confianza, 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 criptográficas estándares, como PKCS#11, Java JCA/JCE y Microsoft CAPI/CNG.

Actividades de auditoría

Si tiene que hacer un seguimiento de los cambios realizados en los recursos o auditar actividades con fines de seguridad y cumplimiento, puede consultar las llamadas de gestión a la API en CloudHSM realizadas desde su cuenta mediante AWS CloudTrail. Además, puede auditar las operaciones en el dispositivo HSM a través de syslog o enviar mensajes de registro de syslog a su propio recopilador de registros.

Servicios y herramientas criptográficos de AWS

AWS ofrece mecanismos para cumplir un amplio número de normas de seguridad informática criptográficas que puede utilizar para implementar las prácticas recomendadas de cifrado. AWS Encryption SDK[8] es una biblioteca de cifrado en el lado del cliente disponible en Java, Python, C, JavaScript y la interfaz de línea de comandos compatible con Linux, macOs y Windows. Ofrece características avanzadas de protección de datos que incluyen conjuntos de algoritmos de claves seguros, autenticados y simétricos, como AES-GCM de 256 bits con derivación de claves y firma. Debido a que se ha diseñado específicamente para las aplicaciones que utilizan DynamoDB, el cliente de cifrado de DynamoDB[9] permite a los usuarios proteger sus tablas de datos antes de enviarlas a la base de datos. También verifica y descifra los datos cuando se recuperan. El cliente está disponible para Java y Python.

Infraestructura dm-crypt en Linux

Dm-crypt es un mecanismo de cifrado en el kernel de Linux que permite a los usuarios montar 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 ponerlo a disposición del sistema operativo. Tras el montaje, todos los archivos del sistema de archivos estarán disponibles para las aplicaciones, sin necesidad de ninguna interacción adicional. Sin embargo, estos archivos se cifran cuando se almacenan en el disco.

El Device mapper (mapeador de dispositivos) es una infraestructura del kernel de las versiones 2.6 y 3.x de Linux que proporciona un método genérico para crear capas virtuales de dispositivos de bloque. El destino de cifrado del mapeador de dispositivos 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 Logical

Volume Manager (LVM, administrador de volúmenes lógicos). EL LVM proporciona una gestión de volúmenes lógicos para el kernel de Linux.

Protección de datos desde el diseño y por defecto

Cada vez que un usuario o aplicación intente utilizar la consola de administración de AWS, la API de AWS o la AWS CLI, se enviará una solicitud a AWS. El servicio de AWS recibe la solicitud y realiza una serie de pasos para determinar si permitir o denegar la solicitud, según una lógica de evaluación de políticas concreta. A excepción de las solicitudes de credenciales raíz, todas las solicitudes de AWS se deniegan por defecto (se aplica la política de *negación* predeterminada). Esto significa que se denegarán todas las acciones que no se hayan permitido explícitamente en la política. En la definición de las políticas y, como práctica recomendada, AWS le recomienda aplicar el principio de privilegios mínimos, que implica que cada componente (es decir, usuarios, módulos o servicios) debe tener acceso únicamente a los recursos necesarios para completar sus tareas.

Este enfoque está en línea con el artículo 25 del RGPD, que establece que “el responsable del tratamiento implementará las medidas técnicas y organizativas apropiadas con miras a garantizar que, de forma predeterminada, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento”.

AWS también ofrece herramientas para implementar *infraestructura como código*, un potente mecanismo para incluir medidas de seguridad en el diseño de una arquitectura desde el principio. AWS CloudFormation ofrece un lenguaje común para describir y ofrecer todos los recursos de las infraestructuras, entre los que se incluyen políticas de seguridad y procesos. Con estas herramientas y prácticas, la seguridad se convierte en parte de su código y puede generar versiones, monitorizarla o modificarla (con un sistema de versiones) según las necesidades de su organización. Ello permite la *protección de los datos desde el diseño*, ya que los procesos de seguridad y las políticas pueden incluirse en la definición de la arquitectura. Además, desde su organización, las medidas de seguridad pueden monitorizarla de forma constante.

Cómo puede ayudarlo AWS

Tabla 1: Cómo puede ayudarlo AWS a transitar el camino al cumplimiento del RGPD

Área	Descripción	Servicios y herramientas de AWS
Marco de cumplimiento exhaustivo	Es posible que las medidas técnicas y organizativas adecuadas deban incluir “la capacidad de garantizar la confidencialidad, integridad, disponibilidad y tolerancia a fallos permanentes de los sistemas y servicios de tratamiento”.	SOC 1, SSAE 16, ISAE 3402 (anterior SAS 70), SOC 2, SOC 3 PCI DSS de nivel 1 ISO 9001, ISO 27001, ISO 27017, ISO 27018 FIPS 140-2 del NIST Catálogo de controles de cumplimiento de computación en la nube (C5)
Control de acceso a los datos	El responsable del tratamiento “…implementará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento”.	 AWS Identity and Access Management (IAM)  Amazon Cognito  AWS Shield y WAF  AWS Resource Access Manager  AWS Organizations  AWS CloudFormation  AWS CloudTrail
Monitorización y registro	“Cada responsable y, en su caso, su representante llevarán un registro de las actividades de tratamiento efectuadas bajo su responsabilidad”. “…el responsable y el encargado del tratamiento implementarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo […]”.	 AWS Config  Amazon CloudWatch  AWS Control Tower  Amazon GuardDuty  Amazon Inspector

Área	Descripción	Servicios y herramientas de AWS
		 Amazon Macie
		 AWS Systems Manager
		 AWS Security Hub
		 SDK y herramientas de AWS
Protección de sus datos en AWS	Las organizaciones deberán "implementar medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya la seudonimización y el cifrado de datos personales".	 AWS Certificate Manager
		 AWS CloudHSM
		 AWS Key Management Service

Colaboradores

Entre los colaboradores de este documento, se incluye a las siguientes personas:

- Tim Anderson, Technical Industry Specialist, Amazon Web Services
- Carmela Gambardella, Public Sector Senior Solutions Architect, Amazon Web Services
- Giuseppe Russo, Security Assurance Manager, Amazon Web Services
- Marta Taggart, Senior Program Manager, Amazon Web Services
- Luca Iannario, Public Sector Solutions Architect, Amazon Web Services

Revisiones del documento

Fecha	Descripción
Noviembre de 2017	Primera publicación

Fecha	Descripción
Diciembre de 2020	Actualización para añadir los nuevos servicios y funcionalidades de AWS.

Notes

[1] https://ec.europa.eu/info/law/law-topic/data-protection_es

[2] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

[3] https://cispe.cloud/

[4] https://docs.aws.amazon.com/es_es/general/latest/gr/rande-manage.html

[5] https://docs.aws.amazon.com/macie/latest/user/managed-data-identifiers.html#managed-data-identifiers-pii

[6] https://aws.amazon.com/solutions/aws-landing-zone/

[7] https://aws.amazon.com/es/compliance/data-privacy/service-capabilities/

[8] https://docs.aws.amazon.com/crypto/latest/userguide/awscryp-service-encrypt.html

[9] https://docs.aws.amazon.com/crypto/latest/userguide/awscryp-service-ddb-client.html