Protección de los Datos en la Nube

Guía para las Organizaciones de España

Contenido

Protección de los Datos en la Nube

Las organizaciones en España se encuentran entre los millones de clientes activos que utilizan Amazon Web Services (AWS) cada mes para transformar digitalmente los servicios y servir mejor a los ciudadanos, al tiempo que protegen sus activos más importantes y confidenciales: sus datos. En AWS, trabajamos estrechamente con los clientes para comprender sus necesidades de protección de datos. También ofrecemos el conjunto más completo de servicios, herramientas y experiencia para ayudar a proteger esos datos. Por ejemplo, estamos colaborando con el Centro Nacional de Inteligencia y el Centro Criptológico Nacional (CNI-CCN) ya han firmado un convenio de colaboración estratégico para impulsar conjuntamente la ciberseguridad y la innovación a través de la tecnología Nube de AWS. Nuestra colaboración abarca varias áreas de seguridad en la nube, desde capacitación en ciberseguridad y soporte de operaciones, hasta la creación de pautas de seguridad en la nube para ayudar a las organizaciones con los desafíos que enfrentan se enfrentan.

Además de ofrecer aún más opciones para ejecutar aplicaciones y prestar servicio a los usuarios finales desde centros de datos ubicados en España, nuestra infraestructura de AWS está diseñada para cumplir con los más altos niveles de seguridad y cumplimiento. Hemos obtenido la certificación en la categoría Alta del Esquema Nacional de Seguridad (ENS) y fuimos el primer proveedor de servicios en la nube (CSP) en acreditar varios servicios de seguridad en el Catálogo de Productos y Servicios de STIC (CPSTIC) del CCN. La obtención de esta acreditación demuestra que AWS puede prestar servicios de forma segura a la administración pública, así como a las empresas y organizaciones de interés estratégico en España. Para apoyar a España en su transformación digital, la infraestructura de AWS proporciona acceso a tecnologías avanzadas de AWS para impulsar la innovación y, al mismo tiempo, mantener los datos protegidos.

Con más de una década de experiencia trabajando con clientes en más de 425 países y territorios, incluidos decenas de miles de clientes en la Península Ibérica, nos comprometemos a elevar continuamente los estándares de protección y de los servicios. Siga leyendo para obtener ayuda a la hora de planificar despliegues en la nube de AWS que cumplan con los requisitos de protección de datos y descubra cómo adaptar su organización a las consideraciones de seguridad gubernamentales.

La Nube de AWS

A medida que el uso de la tecnología en la nube sigue aumentando en todo el mundo, las organizaciones deben garantizar que haya una seguridad adecuada a la hora de procesar los datos personales.

AWS comparte las responsabilidades en materia de seguridad y cumplimiento con sus clientes. Este modelo de responsabilidad compartida puede ayudar a aliviar la carga operativa de los clientes, ya que AWS es responsable de proteger la infraestructura que ejecuta todos los servicios que se ofrecen en la nube de AWS. No obstante, es responsabilidad del cliente gestionar los riesgos e implementar los controles adecuados en su entorno en la nube de AWS. Al utilizar los servicios de AWS, los clientes pueden diseñar una arquitectura que cumpla con sus requisitos de protección de datos.

Como se muestra en la **Figura 1**, esta diferenciación de responsabilidad se suele hacer mediante el término de seguridad de o en la nube.

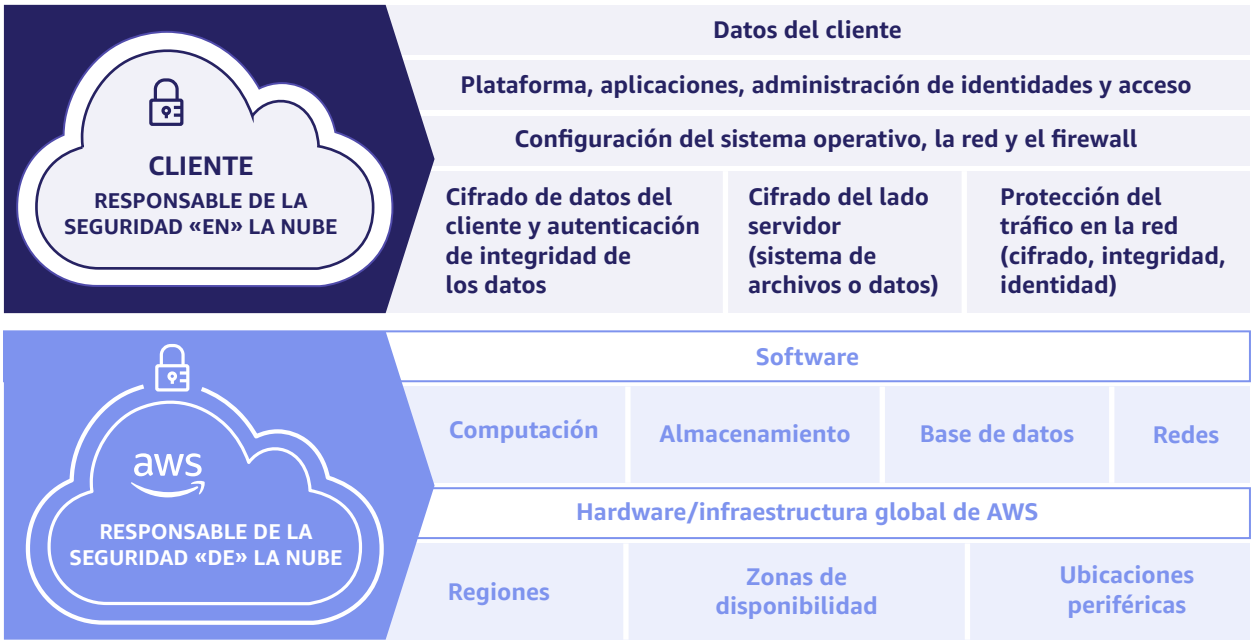

Figura 1. El Modelo de responsabilidad compartida de AWS

Encargados y Responsables del Tratamiento de Datos

AWS actúa como encargado y responsable del tratamiento de datos en virtud del Reglamento general de protección de datos (GDPR).

AWS como encargado del tratamiento de datos. Cuando los clientes utilizan servicios de AWS para procesar los datos personales del contenido que cargan a dichos servicios, AWS actúa como encargado del tratamiento de datos. Los clientes pueden utilizar los controles disponibles en los servicios de AWS, incluidos los controles de configuración de seguridad, para gestionar los datos personales. Un cliente puede actuar como responsable o encargado del tratamiento de datos, en cuyo caso, AWS actuaría como encargado o subencargado del tratamiento de dichos datos.

AWS como responsable del tratamiento de datos. Cuando AWS recopila datos personales y determina los fines y los medios de tratamiento de dichos datos (por ejemplo, cuando AWS almacena la información de contacto de la cuenta de AWS para facilitar las actividades de atención al cliente), actúa como responsable del tratamiento de datos.

Control Sobre la Ubicación y las Transferencias de Datos

AWS permite a los clientes cumplir con las consideraciones de ubicación y transferencia de datos, ya que los clientes mantienen el control de sus datos personales y determinan dónde se almacenarán, así como la región geográfica de ese almacenamiento. Los clientes eligen las regiones de AWS en las que almacenar sus datos. Despliegan los servicios de AWS solo en las ubicaciones que eligen, de acuerdo con los requisitos geográficos específicos. Por ejemplo, la región Europa (España) de AWS permite a los clientes almacenar y procesar su contenido en España con la seguridad de que mantendrán un control total sobre la ubicación de sus datos. Los clientes pueden utilizar múltiples zonas de disponibilidad (uno o más centros de datos discretos con energía, redes y conectividad redundantes en una región de AWS) para desarrollar aplicaciones altamente escalables, disponibles y tolerantes a fallas que puedan cumplir con los requisitos de soberanía y residencia de datos.

AWS no trasladará ni replicará los datos de los clientes de las regiones de AWS seleccionadas a menos que sea para cumplir con la ley, para la prestación de un servicio que no sea un servicio regional de AWS, o porque la transferencia sea una parte esencial del servicio (como en un servicio de entrega de contenido u otros que se encuentran aquí). Si los términos del servicio especifican una excepción, por ejemplo, el desarrollo y la mejora de esos servicios, los clientes pueden optar por no realizar transferencias de datos de clientes (consulte aquí ejemplos de estos servicios).

Cumplimiento del RGPD al Utilizar los Servicios de AWS

A medida que aumenta la cantidad de servicios en la nube, es importante garantizar que se aplica una seguridad adecuada a los datos personales que procesan los clientes que utilizan dichos servicios. Los clientes pueden utilizar todos los servicios de AWS para procesar datos personales de acuerdo con el RGPD. Todos los servicios y características de AWS que están disponibles de forma general cumplen con los altos estándares de privacidad y protección de datos que el RGPD exige a los encargados del tratamiento de datos. Esto significa que, además de beneficiarse de todas las medidas que AWS ya toma para mantener la seguridad de los servicios, los clientes pueden desplegar los servicios de AWS como parte de sus propios planes de cumplimiento del RGPD. El documento AWS GDPR Data Processing Addendum (Anexo del tratamiento de datos del RGPD de AWS o APD del RGPD de AWS) está incorporado en los términos de servicio de AWS y se aplica automáticamente a todos los clientes, lo que les permite cumplir con el RGPD.

La región Europa (España) de AWS ofrece a los clientes que crean aplicaciones conforme al RGPD acceso a una región segura de AWS de la Unión Europea (UE) que permite satisfacer los niveles más

altos de seguridad, cumplimiento y protección de datos. Si los clientes desean transferir datos fuera de España, la Agencia Española de Protección de Datos autoriza a AWS a realizar transferencias internacionales de datos.

Northius es una solución de educación digital líder con sede en España, que realiza operaciones en toda Europa y América Latina y ofrece más de 500 cursos de formación profesional general y vocacional. Sin embargo, la existencia de datos incoherentes en el software utilizado por los departamentos internos ralentizó la capacidad de la empresa para priorizar los proyectos y obstaculizó la visibilidad de las operaciones. Por este motivo, Northius buscó estandarizar y centralizar los datos y, al mismo tiempo, proteger la privacidad y la seguridad de la información personal de los clientes para cumplir con el RGPD.

Northius recurrió a AWS para crear una arquitectura de datos moderna y ágil basada en las prácticas recomendadas de AWS en materia de control de calidad y gobernanza de los datos en virtud del RGPD. La solución tenía que ofrecer datos de calidad a los equipos internos y, al mismo tiempo, cumplir con los requisitos del RGPD en materia de privacidad y seguridad de la información de identificación personal de los alumnos, como direcciones y números de teléfono. Northius trabajó junto con AWS Professional Services para crear un lago de datos con AWS Lake Formation y crear, administrar y proteger dicho lago rápidamente. Northius ha mejorado su gobernanza de datos al estandarizar las políticas internas sobre cómo se recopilan, almacenan y procesan los datos. La empresa tiene una mayor visibilidad sobre quién accede a la información personal de los usuarios. Así mismo, ofrece herramientas de toma de decisiones internas basadas en datos hasta tres veces más rápido y ha mejorado la coherencia de datos en un 35 por ciento, a la vez que ha aumentado la seguridad.

Consulte el estudio de caso aquí.

Los clientes pueden utilizar los servicios de AWS para transferir datos personales desde el Espacio Económico Europeo (EEE) a países no pertenecientes al mismo que no hayan recibido una decisión de adecuación de la Comisión Europea en cumplimiento con el RGPD. El Tribunal de Justicia de la Unión Europea (TJUE) emitió una sentencia que validó el uso de cláusulas contractuales tipo (SCC) como mecanismo para transferir datos de clientes fuera del EEE. Los clientes de AWS pueden seguir confiando en las SCC incluidas en el APD del RGPD de AWS si deciden transferir sus datos fuera del EEE en cumplimiento con el RGPD.

Los clientes deberán realizar una evaluación del impacto de la transferencia si eligen utilizar un servicio no regional o una región fuera del EEE. Los clientes pueden utilizar la página Características de privacidad de los servicios de AWS para determinar si el uso de un servicio de AWS individual implica la transferencia de datos del cliente y, en función de esto, optar por no utilizarlo o bien implementar medidas complementarias. En el documento técnico de AWS Navigating Compliance with EU Data Transfer Requirements (Gestión del cumplimiento de los requisitos de transferencia de datos de la UE) se proporciona información sobre los servicios y recursos que pueden ayudar a los clientes a realizar evaluaciones de transferencias de datos a la luz de las recientes sentencias del TJUE y las posteriores recomendaciones del Comité Europeo de Protección de Datos (CEPD).

AWS ofrece compromisos contractuales más estrictos que van más allá de lo que exigen las recientes sentencias del TJUE y lo que actualmente ofrecen otros CSP, para proteger los datos personales que los clientes confían a AWS para su tratamiento. Cabe destacar que estos compromisos se aplican a todos los datos de clientes procesados por AWS que estén sujetos al RGPD, tanto si se transfieren fuera del EEE como si no. Estos compromisos se aplican automáticamente a todos los clientes que utilizan AWS para procesar sus datos personales, mediante el anexo complementario al APD del RGPD de AWS.

AWS se ha comprometido con importantes programas de privacidad, portabilidad y soberanía digital de la UE, como el Código de conducta de la infraestructura como servicio de SWIPO, GAIA-X y el Código de conducta de protección de datos de CISPE (Código CISPE). El cumplimiento del Código CISPE por parte de AWS ofrece a los clientes garantías adicionales de que AWS ha implementado medidas contractuales y operativas que cumplen los requisitos aplicables a un encargado del tratamiento de datos, de conformidad con el artículo 28 del RGPD. EY CertifyPoint, un auditor externo acreditado por la autoridad francesa de protección de datos (CNIL), que actúa como principal autoridad de protección de datos, ha verificado el cumplimiento del Código CISPE por parte de AWS.

Para obtener más información sobre cómo AWS puede permitir el cumplimiento del RGPD, consulte los sitios Centro del RGPD de AWS y Preguntas frecuentes sobre el RGPD, además de los siguientes recursos: How AWS is helping EU customers navigate the new normal for data protection (Cómo ayuda AWS a los clientes de la UE a afrontar la nueva normalidad en materia de protección de datos) y Using AWS in the context of Common Privacy and Data Protection Considerations (Uso de AWS en el contexto de las consideraciones comunes de privacidad y protección de datos).

Para obtener una lista de los servicios de AWS que pueden ayudarle a gestionar el cumplimiento del RGPD, consulte el documento técnico Gestión del cumplimiento del RGPD en AWS.

Consideraciones de Seguridad

Los clientes que confían datos personales a un CSP deben cerciorarse de que los estándares de seguridad de este sean suficientes y apropiados para el tratamiento de datos personales que se lleva a cabo en su nombre.

La seguridad en la nube de AWS es nuestra máxima prioridad. Dado que AWS es tanto encargado como responsable del tratamiento de datos en virtud del RGPD, implementa controles y procesos técnicos y físicos, responsables y sofisticados diseñados para evitar el acceso o la divulgación no autorizados de los datos de los clientes (consulte el sitio Protección de datos en AWS). Supervisamos continuamente la evolución del panorama normativo y legislativo de la privacidad de los datos para identificar los cambios y determinar qué herramientas podrían necesitar nuestros clientes para satisfacer sus necesidades de cumplimiento (consulte el sitio Preguntas frecuentes sobre privacidad de los datos).

> Los datos confidenciales, como la información médica, están más seguros en un entorno en la nube que en uno local «si tenemos en cuenta varias perspectivas», como la disponibilidad de esta información, la prevención de redundancias y los propios sistemas de seguridad de los centros de datos de AWS.
>
> *- Santiago García Blanco, director general de Transformación Digital y Relaciones con los Usuarios de la Consejería de Salud del Gobierno de Cantabria. Consulte el estudio de caso aquí.*

Nuestro objetivo es ganarnos la confianza de los clientes simplificando las dificultades que suelen

asociarse a las actividades relacionadas con la protección de datos. Por ejemplo, para cumplir con el RGPD, es posible que los clientes deban realizar una evaluación de impacto relativa a la protección de datos (EIPD) para las actividades de tratamiento de datos. AWS Marketplace ofrece una amplia gama de soluciones de seguridad que combinan la experiencia en privacidad y el machine learning (ML) para simplificar este proceso y ayudar a mitigar el riesgo. Para obtener más orientación, incluidas las plantillas, los clientes pueden consultar el sitio web GDPR.EU: How to conduct a Data Protection Impact Assessment (Cómo realizar una evaluación de impacto relativa a la protección de datos).

AWS satisface 143 estándares de seguridad y certificaciones de cumplimiento, por lo que nos adherimos a los requisitos de cumplimiento de prácticamente todas las agencias reguladoras del mundo. Los clientes heredan estos estándares con los servicios de AWS que utilizan, lo que reduce su carga de trabajo en materia de cumplimiento. Ofrecemos orientación para mantener el cumplimiento y proporcionamos una amplia red de socios de AWS que pueden ayudar a gestionar el cumplimiento en nombre de un cliente, si así lo desea.

Cumplimiento del Esquema Nacional de Seguridad

La certificación del Esquema Nacional de Seguridad (ENS) define los estándares de seguridad que se aplican a todos los organismos gubernamentales y organismos públicos de España, así como a los proveedores de servicios de los que dependen los servicios públicos. Desarrollada por el Ministerio de Finanzas y Administración Pública y el CCN, comprende los principios básicos y los requisitos mínimos necesarios para la protección adecuada de la información.

Para conseguir la certificación en la categoría Alta del ENS, AWS superó satisfactoriamente una auditoría realizada por un asesor independiente acreditado. Además de la propia certificación de AWS, y de acuerdo con el modelo de responsabilidad compartida, los clientes deben diseñar sus cargas de trabajo para cumplir con el ENS. Para ayudar a los clientes, AWS ha colaborado con CCN para crear una serie de guías que los clientes pueden utilizar para adaptarse a los controles de seguridad descritos en la categoría Alta del ENS. Estas incluyen consejos sobre qué servicios y características se pueden utilizar para permitir el cumplimiento del ENS en diferentes escenarios, como el endurecimiento básico de las directrices, o en los casos más complejos, como entornos híbridos o de varias nubes.

Hemos desarrollado cursos de capacitación en seguridad en línea en colaboración con el Instituto Nacional de Administración Pública (INAP) y el CCN. Esta formación está disponible en el sitio web de Ángeles y apoya a las organizaciones en el cumplimiento de los requisitos de seguridad de acuerdo con la ENS.

Permitimos a los clientes verificar que sus controles de seguridad cumplen con las directrices 800 CCN STIC del ENS mediante Prowler, una herramienta de seguridad de código abierto que los clientes pueden integrar con AWS Security Hub para realizar comprobaciones de configuración de seguridad en su entorno de AWS.

Los clientes pueden iniciar paquetes de plantillas que cumplan con la normativa y de código abierto en AWS Config para crear controles de seguridad, lo que les permite personalizarlos y adaptarlos a los tres niveles del ENS.

Además, ofrecemos un acelerador de zona de aterrizaje de ENS en AWS. Esta solución implementa una base en la nube diseñada para alinearse con las mejores prácticas y requisitos de AWS necesarios para la protección adecuada de la información, de acuerdo con la ENS. Con esta solución, los clientes con cargas de trabajo altamente reguladas y requisitos de cumplimiento complejos pueden administrar y gobernar mejor su entorno de múltiples cuentas.

La Universidad Francisco de Vitoria (UFV) ofrece más de 50 grados y cuenta con más de 40 000 alumnos matriculados. Con un panorama tan vasto y cambiante, la UFV ha alojado sus datos en varios sistemas heredados, lo que ha creado silos que dificultan la extracción de datos significativos. Junto con AWS, la UFV creó una arquitectura de lake house de datos en AWS para mejorar el acceso, la calidad, la administración y la seguridad de los datos. En AWS, creó un flujo de trabajo común para la ingesta, transformación y visualización de datos y estableció procesos clave de gobernanza de datos para proteger la información confidencial.

La UFV puede controlar la seguridad del acceso a los datos de varias maneras. Para ello, puede permitir el acceso a determinados usuarios mediante las políticas de AWS IAM, lo cual permite a la UFV especificar quién o qué puede acceder a los servicios y recursos de AWS, administrar de forma centralizada los permisos detallados y analizar el acceso para ajustar los permisos en AWS. También puede proteger el acceso a los datos en AWS Lake Formation, un servicio que se utiliza para crear lagos de datos seguros con el uso de diferentes técnicas de catalogación de datos para conceder permisos mediante etiquetas.

Con un catálogo de datos unificado, la universidad puede controlar el acceso a sus datos y la publicación de los mismos y, a la vez, ofrecer los más altos niveles de confianza, seguridad y calidad. Dado que la UFV conserva instantáneas de sus informes de datos casi en tiempo real, la universidad puede supervisar que sus datos cumplan con los estándares de calidad, con los requisitos reglamentarios y con las prácticas recomendadas de AWS.

Consulte el estudio de caso aquí.

Protección de los Datos

Los clientes mantienen el control total de sus datos y determinan quién puede acceder a ellos. Ofrecemos el conjunto más completo de servicios, herramientas y conocimientos para ayudar a proteger los datos de los clientes. AWS puede ayudar a los clientes a mejorar su capacidad para cumplir con los requisitos básicos de seguridad y protección de datos, ya que se adapta a las normas gubernamentales, como el ENS, y a los reglamentos europeos más amplios en las siguientes áreas.

Identificación. Consulte el sitio Data Classification Overview (Descripción general de la clasificación de datos) para aprender a clasificar los datos y evaluar la confidencialidad y el impacto empresarial, evaluar los riesgos asociados a los diferentes tipos de datos y determinar la protección adecuada. Use herramientas como Amazon Macie, que utiliza ML

para reconocer automáticamente los datos confidenciales, como la información de identificación personal (PII) o la propiedad intelectual, y le proporciona paneles y alertas que dan visibilidad sobre cómo se accede a estos datos o cómo se trasladan.

Seudonimización y cifrad. Cifre los datos para reducir los riesgos asociados con el almacenamiento y el tratamiento de datos personales. AWS proporciona capacidades de cifrado de datos para muchos de sus servicios y ofrece publicaciones de blog para resaltar la importancia del cifrado y la forma en que AWS puede ayudarle. Utilice un almacenamiento de claves criptográficas, como AWS Key Management Service (AWS KMS), para generar y gestionar tanto las claves raíz como las claves de datos. Implemente operaciones de cifrado y descifrado en **todos los** tipos de datos de una biblioteca de cifrado del cliente con el SDK de cifrado de AWS. Utilice servicios como Amazon Athena para anonimizar los conjuntos de datos, y la tokenización para reemplazar los datos confidenciales.

Aislamiento de inquilinos. AWS proporciona capacidades de separación lógica y su arquitectura está diseñada para aislar a cada cliente de los demás (consulte el documento técnico Logical Separation on AWS [Separación lógica en AWS]). Use características como AWS Nitro Enclaves para crear entornos de computación aislados a fin de proteger y procesar de forma más segura datos altamente confidenciales (como información personal identificable [PII] y datos sanitarios, financieros y de propiedad intelectual) de sus instancias de Amazon Elastic Compute Cloud (Amazon EC2). Utilice Amazon Virtual Private Cloud (Amazon VPC) para iniciar los recursos de AWS en una red virtual aislada de forma lógica que pueda definir. Proporcione arquitecturas dedicadas basadas en hipervisor o bare metal, utilice arquitecturas de contenedores y sin servidor para aislar los entornos de ejecución y aplique la autenticación y la autorización. Para obtener más información, consulte el documento técnico SaaS Tenant Isolation Strategies (Estrategias de aislamiento de inquilinos de SaaS).

Medidas técnicas y organizativas. Diseñe aplicaciones seguras para garantizar la confidencialidad, la integridad y la disponibilidad de los datos personales. Gestione el acceso a los servicios y recursos de AWS de forma segura con AWS IAM. Puede crear y administrar grupos y usuarios de AWS, así como utilizar permisos para otorgarles o denegarles el acceso a los recursos de AWS. Utilice AWS CloudTrail para registrar, supervisar de forma continua y conservar información sobre la actividad de la cuenta relacionada con las acciones en AWS. De este modo, se simplifica el análisis de seguridad, el seguimiento de los cambios en los recursos y la solución de problemas. Utilice Amazon GuardDuty, un servicio gestionado de detección de amenazas, para supervisar de forma continua los comportamientos malintencionados o no autorizados a fin de proteger las cuentas y cargas de trabajo de AWS.

Copias de seguridad y restauración. Utilice AWS Backup para automatizar y desplegar de forma centralizada políticas de protección de datos a fin de configurar, administrar y controlar su actividad de copias de seguridad. Utilice AWS Elastic Disaster Recovery (AWS DRS) para minimizar el tiempo de inactividad y la pérdida de datos con una recuperación rápida y fiable. Además, Amazon Simple Storage Service (Amazon S3) ofrece replicación entre regiones para replicar datos en otras regiones de AWS con fines de cumplimiento, seguridad y recuperación de desastres.

Pruebas y evaluación. Realice análisis de vulnerabilidades y evaluaciones de seguridad, como, por ejemplo, pruebas de penetración, en su infraestructura. Utilice servicios como AWS Config para registrar y evaluar las configuraciones de sus recursos, AWS Security Hub para unificar la seguridad y el cumplimiento, y AWS Audit Manager para auditar continuamente el uso que hace de AWS y simplificar la evaluación del riesgo. Hemos desarrollado un programa de garantía de seguridad que utiliza las prácticas recomendadas en materia de privacidad y protección de datos a nivel mundial para ayudarle a llevar a cabo sus operaciones de forma segura en AWS. Estos procesos de control y medidas de seguridad se someten a múltiples evaluaciones independientes por parte de terceros y se pueden consultar en la página Programas de conformidad de AWS.

Vulneraciones de datos. Los clientes son responsables de supervisar su propio entorno para detectar vulneraciones de la privacidad. Utilice herramientas de supervisión como Amazon CloudWatch para realizar un seguimiento de cuándo se accede a los datos y de quién accede a estos. Utilice la guía Guía de respuesta a incidentes de seguridad de AWS para implementar un procedimiento de respuesta a incidentes de seguridad a fin de planificar la actuación en caso de que se produzcan dichos incidentes y garantizar que el personal sepa cómo reaccionar ante los problemas de seguridad. Notifique las vulneraciones a través de nuestra página web Informes sobre vulnerabilidades. Suscríbase a la fuente RSS de boletines de seguridad de AWS para mantenerse al tanto de los anuncios relacionados con la seguridad, así como al panel AWS Service Health Dashboard para que le avise de cualquier problema de disponibilidad que afecte de forma generalizada. Consulte la página Prácticas recomendadas en materia de seguridad, identidad y cumplimiento para obtener información adicional sobre cómo protegerse y detectar vulneraciones de seguridad.

Eliminación de datos. Los clientes controlan la eliminación de sus datos en AWS y mantienen las políticas y procedimientos de retención de datos adecuados. Proporcionamos instrucciones específicas del servicio sobre cómo puede eliminar los datos del sistema en la página Características de privacidad de los servicios de AWS. En caso de eliminación errónea, los servicios de AWS, como Amazon S3, admiten características que permiten mantener el control de las versiones de los datos, evitan eliminaciones accidentales y replican los datos en la misma región de AWS o en una diferente.

Inspecciones in situ. En lugar de permitir a los clientes llevar a cabo auditorías físicas, AWS cuenta con un tercero independiente que audita sus centros de datos. Los auditores redactan un informe SOC 1 de tipo 2 en relación con la auditoría. Las revisiones independientes de la seguridad física de los centros de datos también forman parte de una auditoría ISO 27001; una auditoría ENS; han calificado para los servicios en el Catálogo de Productos y Servicios de CCN STIC de España (CPSTIC) y en el marco de la asociación bancaria española Centro de Cooperación Interbancaria (CCI), Pinakes; una evaluación del Estándar de seguridad de datos (PCI) de la industria de tarjetas de pago (DSS); y una auditoría del Reglamento del tráfico internacional de armas (ITAR).

Transparencia Sobre el Tratamiento de Datos

La transparencia sobre el tratamiento de datos es fundamental. Somos transparentes en cuanto a la forma en que los servicios de AWS procesan los datos personales que los clientes pueden cargar en sus cuentas de AWS y ofrecemos capacidades que permiten a los clientes eliminar sus datos y supervisar su tratamiento.

AWS solo procesará los datos de los clientes según sus instrucciones documentadas y no utilizará ni compartirá el contenido del cliente ni tampoco accederá a este sin previo acuerdo, tal y como se describe en el Contrato de cliente de AWS y en el anexo AWS GDPR DPA (APD del RGPD de AWS). Ofrecemos herramientas en línea para ayudar a los clientes a cumplir con las obligaciones de protección de datos, como la página Centro de privacidad de datos y la página Características de privacidad de los servicios de AWS. Nuestro Aviso de privacidad en línea detalla cómo recopilamos y utilizamos la información personal en relación con los sitios web, aplicaciones, productos, servicios y eventos de AWS.

Nuestros compromisos reforzados con los clientes se basan en nuestra larga trayectoria de impugnación de las solicitudes de las fuerzas del orden. Si recibimos una solicitud legal por parte de organismos gubernamentales en relación con datos personales, ya sea dentro o fuera del EEE, nos comprometemos a impugnar las solicitudes que sean demasiado amplias o cuando tengamos motivos suficientes para hacerlo, incluso cuando la solicitud entre en conflicto con la legislación de la UE, tal como se describe en nuestro anexo complementario al APD del RGPD de AWS. Divulgamos solo la cantidad mínima de datos de los clientes necesaria para satisfacer la solicitud y proporcionamos informes de solicitud de información semestrales en los que se describen los tipos y la cantidad de solicitudes de información que AWS recibe de las fuerzas del orden.

Mantenemos la página Subencargados del tratamiento de datos de AWS para proporcionar una lista de los subencargados que AWS ha contratado para realizar actividades de tratamiento de los datos de los clientes, en nombre del cliente. Los subencargados del tratamiento de datos están sujetos a las mismas obligaciones contractuales que AWS tiene en virtud del APD del RGPD.

Proporcionamos una amplia variedad de documentos sobre prácticas recomendadas, formación y orientación que los clientes pueden utilizar para proteger sus datos, como lo ejemplifica el pilar de seguridad de AWS Well-Architected Framework.

BBVA es un grupo global de servicios financieros presente en 35 países, incluidos México, España y Turquía.

«Con la utilización del Modelo de responsabilidad compartida de AWS, redujimos considerablemente el tiempo y el alcance de la auditoría de PCI DSS... Todos los puntos relacionados con la seguridad física y el hardware, e incluso las bases de datos, quedaron fuera del alcance de la auditoría porque los servicios de AWS cuentan con la certificación PCI DSS». La solución GP2 tardó 2 meses en recibir la certificación PCI DSS, un proceso que habría tardado el doble con una solución local. «Con AWS, podemos cumplir con varios requisitos de certificación PCI DSS».

- Alfredo Sanz San Juan, director técnico de Global Payments y responsable de la plataforma GP2 de BBVA. Consulte el estudio de caso aquí.

Los CSP, como encargados del tratamiento de datos, pueden usar códigos de conducta o mecanismos de certificación aprobados para demostrar el cumplimiento de los elementos que procesan. Para validar nuestra conformidad con los estándares de privacidad y protección de datos, auditores independientes externos evalúan AWS y le permiten obtener certificaciones, informes de auditoría o atestados de conformidad, que se pueden consultar en AWS Artifact. Entre los estándares con los que cumplimos se incluyen la ISO 9001, la ISO 27001, la ISO 27701 y la ISO 27018; el SOC 1, el SOC 2 y el SOC 3; la categoría Alta del Esquema Nacional de Seguridad (ENS); el Catálogo de productos y servicios STIC (CPSTIC) del Centro Criptológico Nacional (CCN) de España; Ley de Portabilidad y Responsabilidad de los Seguros Médicos (HIPAA); el Estándar de seguridad de datos de la industria de tarjetas de pago (PCI DSS); Cloud Infrastructure Services Providers in Europe (CISPE); el Reglamento general de protección de datos (GDPR); el Catálogo de controles de cumplimiento de la computación en la nube (C5), y Escudo de privacidad entre la UE y los EE. UU.

Para ver la lista completa, consulte nuestra página Programas de cumplimiento de AWS.

Consideraciones Contractuales

Tal y como exige el RGPD, el tratamiento de datos debe regirse por un contrato y los responsables deben mantener el control sobre los datos personales con limitaciones y obligaciones claras y acordadas.

En AWS permitimos a los clientes cumplir estas consideraciones, ya que asumimos varios compromisos contractuales que se reflejan en el APD del RGPD de AWS y en el anexo complementario. Estos están relacionados con la ubicación de los datos, las medidas organizativas técnicas implementadas por AWS y las elegidas por el cliente, las medidas para proteger los datos de los clientes y la notificación de las solicitudes de divulgación de datos, las obligaciones en virtud del APD del RGPD de AWS en cumplimiento con la legislación aplicable en un tercer país en el que se procesen los datos de los clientes y los derechos legales de las personas en caso de infracción según el RGPD.

AWS puede contar con subencargados del tratamiento de datos que ayuden a procesar los datos de los clientes o presten servicios en nuestro nombre. Todas las interacciones con los subencargados del tratamiento de datos se rigen de acuerdo con el APD del RGPD de AWS. Los subencargados pertinentes de los clientes dependerán de la región de AWS que el cliente haya seleccionado y de los servicios de

AWS concretos que este utilice. AWS actualizará la página Subencargados del tratamiento de datos de AWS al menos 30 días antes de contratar a un nuevo subencargado de tratamiento de datos y, si los clientes se suscriben para recibir actualizaciones, AWS les notificará por correo electrónico los cambios que se hagan en esta página.

Resumen

Con la nube de AWS, los clientes pueden cumplir con los altos niveles de protección establecidos por el ENS nivel alto y el RGPD. Trabajamos en estrecha colaboración con los clientes para conocer sus necesidades de protección de datos. Así mismo, ofrecemos el conjunto más completo de servicios, herramientas y conocimientos para proteger los datos de los clientes. Nuestras protecciones de privacidad y controles de seguridad líderes del sector permiten a los clientes llevar a cabo operaciones con la confianza de que pueden lograr los requisitos de cumplimiento.

¿Quiere obtener más información?

AWS Experience Iberia es una plataforma de contenido y eventos ubicada en nuestras oficinas de AWS de Madrid. Además de proporcionar prácticas recomendadas y asistencia técnica para escalar de forma segura en la nube, ofrece lo siguiente:

- Asesoramiento en línea personalizado con expertos en temas tecnológicos y empresariales.
- Comunidades de profesionales tecnológicos, líderes empresariales y un ecosistema de startups.
- -Acceso instantáneo a eventos, talleres, mesas redondas y sesiones inspiradoras impartidas por expertos de AWS.

Reserve su plaza en cualquiera de las actividades y acceda a los recursos a través del sitio web.

También puede completar un formulario de solicitud y un experto de AWS se pondrá en contacto con usted lo antes posible.

Recursos adicionales

Generales

- El Centro Nacional de Inteligencia de España y AWS colaboran para impulsar la ciberseguridad del sector público
- Certificación de categoría Alta del Esquema Nacional de Seguridad
- Catálogo de productos y servicios STIC (CPSTIC) del CCN
- Marco Pinakes: La asociación bancaria española Centro de Cooperación Interbancaria (CCI)
- The National Intelligence Center of Spain and AWS Collaborate to Promote Public Sector Cybersecurity (El Centro Nacional de Inteligencia de España y AWS colaboran para promover la ciberseguridad del sector público)
- El libro electrónico: Acelerando la transformación digital en España
- El libro electrónico: Innovar, inspirar y construir
- El libro electrónico: Más rápido, más seguro, más fuerte: el futuro del transporte en la nube
- El libro electrónico: CAMBIANDO VIDAS: el futuro del cuidado de la salud en la nube
- Using AWS in the Context of Common Privacy and Data Protection Considerations (Uso de AWS en el contexto de las consideraciones habituales sobre privacidad y protección de datos)
- Características de privacidad de los servicios de AWS
- Protección de datos en AWS

Guías sobre 800 CCN STIC y el ENS

- CCN-STIC-887: Perfil de cumplimiento específico para el servicio en la nube corporativo de AWS
- CCN-STIC-887A: Guía de configuración segura de AWS
- CCN-STIC-887B: Guía rápida de Prowler
- CCN-STIC-887C: Guía de configuración de conectividad híbrida segura de AWS
- CCN-STIC-887D: Guía de configuración segura para entornos de varias cuentas de AWS
- CCN-STIC-887E: Guía de configuración segura de Amazon WorkSpaces
- Prácticas recomendadas operativas para el Esquema Nacional de Seguridad (ENS), categoría Baja
- Prácticas recomendadas operativas para el Esquema Nacional de Seguridad (ENS), categoría Media
- Prácticas recomendadas operativas para el Esquema Nacional de Seguridad (ENS), categoría Alta
- CCN-STIC-887F: Guía de respuesta a incidentes de seguridad de AWS
- CCN-STIC-887G: Guía de configuración segura para la supervisión y administración de AWS

RGPD

- Centro del Reglamento general de protección de datos (RGPD)
- Gestión del cumplimiento del RGPD en AWS
- AWS and the General Data Protection Regulation (GDPR) (AWS y el Reglamento general de protección de datos RGPD)
- Customer update: AWS and the EU-US Privacy Shield (Actualización para el cliente: AWS y el escudo de privacidad entre la UE y los EE. UU.)
- AWS and EU data transfers: strengthened commitments to protect customer data (Transferencias de datos entre AWS y la UE: compromisos reforzados para proteger los datos de los clientes)
- AWS GDPR Data Processing Addendum—Now Part of Service Terms (Anexo del tratamiento de datos del RGPD de AWS [ahora forma parte de las condiciones del servicio])
- La protección de datos es nuestro compromiso continuo con los clientes de España

Avisos

Los clientes son responsables de llevar a cabo su propia evaluación independiente de la información que se incluye en este documento. Este documento: (a) tiene únicamente fines informativos, (b) representa las ofertas y prácticas actuales de productos de Amazon Web Services (AWS), que están sujetas a cambios sin previo aviso, y (c) no crea compromisos ni garantías por parte de AWS y sus filiales, proveedores o licenciantes. Los productos o servicios de AWS se proporcionan «tal cual» sin garantías, declaraciones ni condiciones de ningún tipo, ya sean expresas o implícitas. Las responsabilidades y obligaciones de AWS respecto de sus clientes se rigen por acuerdos de AWS, y este documento no forma parte de ningún acuerdo entre AWS y sus clientes, ni lo modifica.