TERMS AND CONDITIONS

You hereby agree that you will not distribute, display, or otherwise make this document available to an *individual or entity*, unless expressly permitted herein. This document is AWS Confidential Information (as defined in the AWS Customer Agreement), and you may not remove these terms and conditions from this document, nor take excerpts of this document, without Amazon's express written consent. You may not use this document for purposes competitive with Amazon. You may distribute this document, in its complete form, upon the commercially reasonable request by (1) an end user of your service, to the extent that your service functions on relevant AWS offerings provided that such distribution is accompanied by documentation that details the function of AWS offerings in your service, provided that you have entered into a confidentiality agreement with the end user that includes terms not less restrictive than those provided herein and have named Amazon as an intended beneficiary, or (2) a regulator, so long as you request confidential treatment of this document (each (1) and (2) is deemed a "Permitted Recipient"). You must keep comprehensive records of all Permitted Recipient requests, and make such records available to Amazon and its auditors, upon request.

You further (i) acknowledge and agree that you do not acquire any rights against Amazon's Service Auditors in connection with your receipt or use of this document, and (ii) release Amazon's Service Auditor from any and all claims or causes of action that you have now or in the future against Amazon's Service Auditor arising from this document. The foregoing sentence is meant for the benefit of Amazon's Service Auditors, who are entitled to enforce it. "Service Auditor" means the party that created this document for Amazon or assisted Amazon with creating this document.

The Spanish report has been prepared by AWS for informational purposes only and has not been subject to any procedures by our service auditor, EY. The SOC report was originally prepared in English by EY, and the opinion is based on the System Description and the service auditor's tests of controls as presented in English. EY did not perform procedures or opine on the accuracy and fairness of the presentation of the Spanish translation we have prepared. As AWS controls have the same control number and wording in both the SOC 1 and SOC 2 reports, only one SOC report is translated each quarter for informational purposes.

AWS preparó el informe en español únicamente con fines informativos, sin intervenciones por parte del auditor de servicios, EY. Antes, EY preparaba en inglés el informe de los controles de organización de servicios (SOC), y se basaba en la descripción del sistema y las pruebas de control del auditor de servicios que estaban en inglés. EY no llevó a cabo ningún procedimiento ni dio su opinión respecto de la precisión y la imparcialidad de la presentación de la traducción al español. Debido a que los controles de AWS tienen el mismo número de control y redacción tanto en el informe de SOC 1 como en el de SOC 2, solo se traduce un informe de SOC cada trimestre con fines informativos.

Controles de organización y sistemas 2 (SOC 2) Informe tipo 2

Descripción del Sistema de Amazon Web Services en términos de seguridad, disponibilidad, confidencialidad y privacidad

Para el período comprendido entre el 1.° de octubre de 2023 y el 30 de septiembre de 2024

Descripción del Sistema de Amazon Web Services en términos de seguridad, disponibilidad, confidencialidad y privacidad

Índice

SECCIÓN I: Afirmación de Amazon Web Services

Amazon Web Services
410 Terry Avenue North
Seattle, WA 98109-5210

Afirmación de la gestión de Amazon Web Services

Hemos preparamos la descripción adjunta denominada "Descripción del sistema de Amazon Web Services en términos de seguridad, disponibilidad, confidencialidad y privacidad" (Descripción) de Amazon Web Services, Inc. ("AWS" u "Organización de servicios") conforme a los criterios para describir el sistema de una organización de servicios, según lo estipulado en la sección 200 de los Criterios de descripción DC de 2018, *Description Criteria for a Description of a Service Organization's System in a SOC 2 Report* (Criterios para la descripción del sistema de una organización de servicios en un informe de SOC 2) (Criterios de descripción). El propósito de la Descripción es proporcionar a los usuarios del informe datos sobre el sistema de Amazon Web Services (Sistema) que pueden ser útiles para evaluar los riesgos que surgen de las interacciones con el Sistema, puntualmente aquella información referida a los controles del sistema que la Organización de servicios diseñó, implementó y operó para proveer un aseguramiento razonable de que se alcanzaron sus compromisos de servicio y requisitos del sistema con base en los criterios de servicios de confianza relevantes para la seguridad, disponibilidad, confidencialidad y privacidad (criterios de servicios de confianza aplicables) estipuladas en la sección 100 de TSP de 2017: *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (Criterios de los servicios de confianza para la seguridad, disponibilidad, integridad de procesos, confidencialidad y privacidad) en los *criterios de servicios de confianza de AICPA*.

El alcance de esta descripción del sistema incluye los siguientes servicios:

- Amazon API Gateway
- Amazon AppFlow
- Controlador de recuperación de aplicaciones de Amazon
- Amazon AppStream 2.0
- Amazon Athena
- Amazon Augmented AI [excluye el personal público y el personal del proveedor para todas las características]
- Amazon Bedrock
- Amazon Braket
- Amazon Chime
- Amazon Chime SDK
- Amazon Cloud Directory
- Amazon CloudFront (excluye la entrega de contenido a través del punto de presencias integrado de Amazon CloudFront)
- Amazon CloudWatch
- Amazon CloudWatch Logs
- Amazon CodeWhisperer
- Amazon Cognito
- Amazon Comprehend
- Amazon Comprehend Medical
- Amazon WorkSpaces Secure Browser (anteriormente conocido como Amazon Workspaces Web)
- Cliente ligero de Amazon WorkSpaces
- AWS Amplify
- AWS App Mesh
- AWS App Runner
- AWS AppFabric
- AWS Application Migration Service
- AWS AppSync
- AWS Artifact
- AWS Audit Manager
- AWS Backup
- AWS Batch
- AWS Certificate Manager (ACM)
- AWS Chatbot
- AWS Clean Rooms
- AWS Cloud Map
- AWS Cloud9
- AWS CloudFormation
- AWS CloudHSM
- AWS CloudShell
- AWS CloudTrail

- Amazon Connect
- Amazon Data Firehose
- Amazon DataZone
- Amazon Detective
- Amazon DevOps Guru
- Amazon DocumentDB (compatible con MongoDB)
- Amazon DynamoDB
- Acelerador de Amazon DynamoDB (DAX)
- Amazon EC2 Auto Scaling
- Amazon Elastic Block Store (EBS)
- Amazon Elastic Compute Cloud (EC2)
- Amazon Elastic Container Registry (ECR)
- Amazon Elastic Container Service [los dos tipos de lanzamiento Fargate y EC2]
- Amazon Elastic File System (EFS)
- Amazon Elastic Kubernetes Service (EKS) (ambos tipos de lanzamiento: Fargate y EC2)
- Amazon Elastic MapReduce (EMR)
- Amazon ElastiCache
- Amazon EventBridge
- Amazon FinSpace
- Amazon Forecast
- Amazon Fraud Detector
- Amazon FSx
- Amazon GuardDuty
- Amazon Inspector
- Amazon Inspector Classic
- Amazon Kendra
- Amazon Keyspaces (para Apache Cassandra)
- Amazon Kinesis Data Streams
- Amazon Kinesis Video Streams
- Amazon Lex
- Amazon Location Service
- Amazon Macie
- Amazon Managed Grafana
- Amazon Managed Service para Apache Flink
- Amazon Managed Service para Prometheus
- Amazon Managed Streaming para Apache Kafka
- Amazon Managed Workflows para Apache Airflow (Amazon MWAA)
- AWS CodeBuild
- AWS CodeCommit
- AWS CodeDeploy
- AWS CodePipeline
- AWS Config
- AWS Control Tower
- AWS Data Exchange
- AWS Database Migration Service (DMS)
- AWS DataSync
- AWS Direct Connect
- AWS Directory Service [excluye Simple AD]
- AWS Elastic Beanstalk
- AWS Elastic Disaster Recovery
- AWS Elemental MediaConnect
- AWS Elemental MediaConvert
- AWS Elemental MediaLive
- AWS Entity Resolution
- Servicio de inyección de errores de AWS
- AWS Firewall Manager
- AWS Global Accelerator
- AWS Glue
- AWS Glue DataBrew
- Panel de AWS Health
- AWS HealthImaging
- AWS HealthLake
- AWS HealthOmics
- AWS IAM Identity Center
- AWS Identity and Access Management (IAM)
- AWS IoT Core
- AWS IoT Device Defender
- AWS IoT Device Management
- AWS IoT Events
- AWS IoT Greengrass
- AWS IoT SiteWise
- AWS IoT TwinMaker
- AWS Key Management Service (KMS)
- AWS Lake Formation
- AWS Lambda
- AWS License Manager
- AWS Mainframe Modernization
- AWS Managed Services
- AWS Network Firewall

- Amazon MemoryDB (anteriormente Amazon MemoryDB para Redis)
- Amazon MQ
- Amazon Neptune
- Amazon OpenSearch Service
- Amazon Personalize
- Amazon Pinpoint y End User Messaging (anteriormente Amazon Pinpoint)
- Amazon Polly
- Amazon Q Business
- Amazon Q Developer
- Amazon Quantum Ledger Database (QLDB)
- Amazon QuickSight
- Amazon Redshift
- Amazon Rekognition
- Amazon Relational Database Service (RDS)
- Amazon Route 53
- Amazon S3 Glacier
- Amazon SageMaker [excluye Studio Lab, al personal público y al personal del proveedor para todas las características]
- Amazon Security Lake
- Amazon Simple Email Service (SES)
- Amazon Simple Notification Service (SNS)
- Amazon Simple Queue Service (SQS)
- Amazon Simple Storage Service (S3)
- Amazon Simple Workflow Service (SWF)
- Amazon SimpleDB
- Amazon Textract
- Amazon Timestream
- Amazon Transcribe
- Amazon Translate
- Amazon Virtual Private Cloud (VPC)
- Amazon WorkDocs
- Amazon WorkMail
- Amazon WorkSpaces
- AWS OpsWorks [incluye Chef Automate, Puppet Enterprise]
- AWS OpsWorks Stacks
- AWS Organizations
- AWS Outposts
- AWS Payment Cryptography
- AWS Private Certificate Authority
- AWS Resilience Hub
- AWS Resource Access Manager (RAM)
- AWS Resource Groups
- AWS RoboMaker
- AWS Secrets Manager
- AWS Security Hub
- AWS Server Migration Service (SMS)
- AWS Serverless Application Repository
- AWS Service Catalog
- AWS Shield
- AWS Signer
- AWS Snowball
- AWS Snowball Edge
- AWS Snowmobile
- AWS Step Functions
- AWS Storage Gateway
- AWS Systems Manager
- AWS Transfer Family
- Notificaciones de usuarios de AWS
- Acceso verificado de AWS
- AWS WAF
- AWS Wickr
- AWS X-Ray
- EC2 Image Builder
- Elastic Load Balancing (ELB)
- FreeRTOS
- VM Import/Export

Encontrará más información sobre los servicios incluidos en el siguiente enlace https://aws.amazon.com/compliance/services-in-scope/

El alcance de las ubicaciones cubiertas en este informe incluye los centros de datos compatibles en las siguientes regiones:

- **Australia:** Asia-Pacífico (Sídney) (ap-southeast-2), Asia-Pacífico (Melbourne) (ap-southeast-4)
- **Baréin:** Medio Oriente (Baréin) (me-south-1)
- **Brasil:** América del Sur (São Paulo) (sa-east-1)
- **Canadá:** Canadá (centro) (ca-central-1), Oeste de Canadá (Calgary) (ca-west-1)*
- **Inglaterra:** Europa (Londres) (eu-west-2)
- **Francia:** Europa (París) (eu-west-3)
- **Alemania:** Europa (Fráncfort) (eu-central-1)
- **Hong Kong:** Asia-Pacífico (ap-east-1)
- **India:** Asia-Pacífico (Bombay) (ap-south-1), Asia-Pacífico (Hyderabad) (ap-south-2)
- **Indonesia:** Asia-Pacífico (Yakarta) (ap-southeast-3)
- **Irlanda:** Europa (Irlanda) (eu-west-1)
- **Israel:** Israel (Tel Aviv) (il-central-1)*
- **Italia:** Europa (Milán) (eu-south-1)
- **Japón:** Asia-Pacífico (Tokio) (ap-northeast-1), Asia-Pacífico (Osaka) (ap-northeast-3)
- **Singapur:** Asia-Pacífico (Singapur) (ap-southeast-1)
- **Sudáfrica:** África (Ciudad del Cabo) (af-south-1)
- **Corea del Sur:** Asia-Pacífico (Seúl) (ap-northeast-2)
- **España:** Europa (España) (eu-south-2)
- **Suecia:** Europa (Estocolmo) (eu-north-1)
- **Suiza:** Europa (Zúrich) (eu-central-2)
- **Emiratos Árabes Unidos:** Medio Oriente (EAU) (me-central-1)
- **Estados Unidos:** Este de EE. UU. (Norte de Virginia) (us-east-1), Este de EE. UU. (Ohio) (us-east-2), Oeste de EE. UU. (Oregón) (us-west-2), Oeste de EE. UU. (Norte de California) (us-west-1), AWS GovCloud (Este de EE. UU.) (us-gov-east-1), AWS GovCloud (Oeste de EE. UU.) (us-gov-west-1)

* La fecha de entrada en vigor para esta región es el 15 de febrero de 2024.

y las siguientes ubicaciones periféricas de AWS:

- CABA, Argentina
- General Pacheco, Argentina
- Brisbane, Australia
- Canberra, Australia
- Melbourne, Australia
- Perth, Australia
- Viena, Austria
- Bruselas, Bélgica
- Fortaleza, Brasil
- Rio de Janeiro, Brasil
- São Paulo, Brasil
- Sofía, Bulgaria
- Toronto, Canadá
- Haifa, Israel
- Milán, Italia
- Roma, Italia
- Inzai, Japón
- Nairobi, Kenia
- Kuala Lumpur, Malasia
- Santiago de Querétaro, México
- Ámsterdam, Países Bajos
- Diemen, Países Bajos
- Schiphol-Rijk, Países Bajos
- Auckland, Nueva Zelanda
- Rosedale, Nueva Zelanda
- Lagos, Nigeria
- Atlanta, Estados Unidos
- Aurora, Estados Unidos
- Bluffdale, Estados Unidos
- Boston, Estados Unidos
- Chandler, Estados Unidos
- Chicago, Estados Unidos
- Columbus, Estados Unidos
- Dallas, Estados Unidos
- Denver, Estados Unidos
- El Segundo, Estados Unidos
- Elk Grove Village, Estados Unidos
- Franklin, Estados Unidos

Amazon Web Services
410 Terry Avenue North
Seattle, WA 98109-5210

- Vancouver, Canadá
- Huechuraba, Chile
- Santiago, Chile
- Bogotá, Colombia
- Zagreb, Croacia
- Praga, República Checa
- Ballerup, Dinamarca
- El Cairo, Egipto
- Tallin, Estonia
- Helsinki, Finlandia
- Espoo, Finlandia
- Aubervilliers, Francia
- Marsella, Francia
- Berlín, Alemania
- Düsseldorf, Alemania
- Fráncfort, Alemania
- Hamburgo, Alemania
- Múnich, Alemania
- Koropi, Grecia
- Kropia, Grecia
- Budapest, Hungría
- Bangalore, India
- Chennai, India
- Calcuta, India
- Bombay, India
- Nueva Delhi, India
- Noida, India
- Pune, India
- Yakarta, Indonesia
- Clonshaugh, Irlanda
- Dublín, Irlanda
- Oslo, Noruega
- Barka, Omán
- Santiago de Surco, Perú
- Manila, Filipinas
- Ciudad Quezon, Filipinas
- Varsovia, Polonia
- Lisboa, Portugal
- Bucarest, Rumania
- Singapur, Singapur
- Ciudad del Cabo, Sudáfrica
- Johannesburgo, Sudáfrica
- Anyang-si, Corea del Sur
- Seúl, Corea del Sur
- Barcelona, España
- Madrid, España
- Estocolmo, Suecia
- Zúrich, Suiza
- Ciudad de Nuevo Taipei, Taiwán
- Taipei, Taiwán
- Bangkok, Tailandia
- Bang Chalong, Tailandia
- Estambul, Turquía
- Dubái, Emiratos Árabes Unidos
- Fujairah, Emiratos Árabes Unidos
- Londres, Reino Unido
- Manchester, Reino Unido
- Swinton, Reino Unido
- Ashburn, Estados Unidos
- Greenwood Village, Estados Unidos
- Hillsboro, Estados Unidos
- Houston, Estados Unidos
- Irvine, Estados Unidos
- Irving, Estados Unidos
- Kansas City, Estados Unidos
- Las Vegas, Estados Unidos
- Los Ángeles, Estados Unidos
- Lynnwood, Estados Unidos
- Miami, Estados Unidos
- Milpitas, Estados Unidos
- Mineápolis, Estados Unidos
- Ciudad de Nueva York, Estados Unidos
- Newark, Estados Unidos
- Las Vegas del Norte, Estados Unidos
- Filadelfia, Estados Unidos
- Phoenix, Estados Unidos
- Piscataway, Estados Unidos
- Pittsburgh, Estados Unidos
- Portland, Estados Unidos
- Reston, Estados Unidos
- Richardson, Estados Unidos
- Seattle, Estados Unidos
- Secaucus, Estados Unidos
- Tampa, Estados Unidos
- Tempe, Estados Unidos
- West Valley City, Estados Unidos
- Hanói, Vietnam
- Ho Chi Minh, Vietnam

y las siguientes ubicaciones de Wavelength en:

- Toronto, Canadá
- Berlín, Alemania
- Dortmund, Alemania
- Múnich, Alemania
- Osaka, Japón
- Alpharetta, Estados Unidos
- Annapolis Junction, Estados Unidos
- Aurora, Estados Unidos
- Azusa, Estados Unidos
- Mineápolis, Estados Unidos
- New Berlin, Estados Unidos
- Pembroke Pines, Estados Unidos
- Plant City, Estados Unidos

Amazon Web Services
410 Terry Avenue North
Seattle, WA 98109-5210

- Tama, Japón
- Daejeon, Corea del Sur
- Seúl, Corea del Sur
- Londres, Reino Unido
- Salford, Reino Unido
- Charlotte, Estados Unidos
- Euless, Estados Unidos
- Houston, Estados Unidos
- Knoxville, Estados Unidos
- Las Vegas, Estados Unidos
- Redmond, Estados Unidos
- Rocklin, Estados Unidos
- Southfield, Estados Unidos
- Tempe, Estados Unidos
- Municipio de Wall, Estados Unidos
- Westborough, Estados Unidos

así como ubicaciones de zona local:

- CABA, Argentina
- Perth, Australia
- Santiago, Chile
- Ballerup, Dinamarca
- Espoo, Finlandia
- Hamburgo, Alemania
- Calcuta, India
- Nueva Delhi, India
- Noida, India*
- Santiago de Querétaro, México
- Rosedale, Nueva Zelanda
- Lagos, Nigeria
- Barka, Omán
- Santiago de Surco, Perú
- Manila, Filipinas
- Varsovia, Polonia
- Singapur, Singapur*
- Ciudad de Nuevo Taipei, Taiwán
- Bang Chalong, Tailandia
- Atlanta, Estados Unidos
- Boston, Estados Unidos
- Chicago, Estados Unidos
- Doral, Estados Unidos
- El Segundo, Estados Unidos
- Garland, Estados Unidos
- Greenwood Village, Estados Unidos
- Hillsboro, Estados Unidos
- Houston, Estados Unidos
- Irvine, Estados Unidos
- Itasca, Estados Unidos
- Kansas City, Estados Unidos
- Kapolei, Estados Unidos
- Las Vegas, Estados Unidos
- Lee's Summit, Estados Unidos*
- Lithia Springs, Estados Unidos
- Mesa, Estados Unidos
- Miami, Estados Unidos
- Mineápolis, Estados Unidos
- Las Vegas del Norte, Estados Unidos
- Filadelfia, Estados Unidos
- Phoenix, Estados Unidos
- Piscataway, Estados Unidos
- Richardson, Estados Unidos
- Seattle, Estados Unidos

* Esta ubicación es una zona local dedicada y es posible que no esté disponible para todos los clientes.

La descripción también indica que, junto con los controles de AWS, se necesitan controles complementarios de la entidad usuaria que estén diseñados adecuadamente y que funcionen de manera eficaz para cumplir los compromisos de servicio y los requisitos del sistema. En la Descripción, se presentan los controles de AWS y los controles complementarios de entidad usuarias asumidos en el diseño de los controles de AWS.

Confirmamos, a nuestro leal saber y entender, lo siguiente:

a. En la Descripción, se presenta el Sistema que se diseñó e implementó durante todo el período comprendido entre el 1.° de octubre de 2023 y el 30 de septiembre de 2024 conforme a los Criterios de descripción.

Amazon Web Services
410 Terry Avenue North
Seattle, WA 98109-5210

b. Los controles enumerados en la Descripción se diseñaron adecuadamente durante todo el período comprendido entre el 1.° de octubre de 2023 y el 30 de septiembre de 2024 para proveer un aseguramiento razonable de que los compromisos de servicio y los requisitos del sistema de AWS se cumplirían con base en los criterios de servicios de confianza aplicables, si los controles funcionaron durante todo ese período, y si las entidades usuarias aplicaron los controles complementarios de las entidades usuarias asumidos en el diseño de los controles de AWS durante todo el período comprendido entre el 1.° de octubre de 2023 y el 30 de septiembre de 2024.

c. Los controles de AWS enumerados en la Descripción operaron de manera eficaz durante todo el período comprendido entre el 1.° de octubre de 2023 y el 30 de septiembre de 2024 para proveer un aseguramiento razonable de que los compromisos de servicio y los requisitos del sistema de AWS se alcanzaron con base en los criterios de servicios de confianza aplicables, si los controles complementarios de las entidades usuarias asumidos en el diseño de los controles de AWS funcionaron de forma eficaz durante todo ese período.

Gestión de Amazon Web Services

SECCIÓN II: Informe de aseguramiento del auditor de servicio independiente

Informe de aseguramiento del auditor de servicio independiente

A la Gestión de Amazon Web Services, Inc.

Alcance

Hemos evaluado la descripción de Amazon Web Services Inc. ("AWS") titulada "Descripción del sistema de Amazon Web Services en términos de seguridad, disponibilidad, confidencialidad y privacidad" (Descripción) que acompaña al sistema de AWS para la prestación de servicios de computación en la nube durante todo el período comprendido entre el 1.º de octubre de 2023 y el 30 de septiembre de 2024 para los siguientes servicios:

- Amazon API Gateway
- Amazon AppFlow
- Controlador de recuperación de aplicaciones de Amazon
- Amazon AppStream 2.0
- Amazon Athena
- Amazon Augmented AI [excluye el personal público y el personal del proveedor para todas las características]
- Amazon Bedrock
- Amazon Braket
- Amazon Chime
- Amazon Chime SDK
- Amazon Cloud Directory
- Amazon CloudFront (excluye la entrega de contenido a través del punto de presencias integrado de Amazon CloudFront)
- Amazon CloudWatch
- Amazon CloudWatch Logs
- Amazon CodeWhisperer
- Amazon Cognito
- Amazon Comprehend
- Amazon Comprehend Medical
- Amazon Connect
- Amazon Data Firehose
- Amazon DataZone
- Amazon Detective
- Amazon DevOps Guru
- Amazon DocumentDB (compatible con MongoDB)
- Amazon DynamoDB
- Acelerador de Amazon DynamoDB (DAX)
- Amazon EC2 Auto Scaling
- Amazon Elastic Block Store (EBS)
- Amazon WorkSpaces Secure Browser (anteriormente conocido como Amazon Workspaces Web)
- Cliente ligero de Amazon WorkSpaces
- AWS Amplify
- AWS App Mesh
- AWS App Runner
- AWS AppFabric
- AWS Application Migration Service
- AWS AppSync
- AWS Artifact
- AWS Audit Manager
- AWS Backup
- AWS Batch
- AWS Certificate Manager (ACM)
- AWS Chatbot
- AWS Clean Rooms
- AWS Cloud Map
- AWS Cloud9
- AWS CloudFormation
- AWS CloudHSM
- AWS CloudShell
- AWS CloudTrail
- AWS CodeBuild
- AWS CodeCommit
- AWS CodeDeploy
- AWS CodePipeline
- AWS Config
- AWS Control Tower
- AWS Data Exchange
- AWS Database Migration Service (DMS)
- AWS DataSync
- AWS Direct Connect
- AWS Directory Service [excluye Simple AD]

- Amazon Elastic Compute Cloud (EC2)
- Amazon Elastic Container Registry (ECR)
- Amazon Elastic Container Service [los dos tipos de lanzamiento Fargate y EC2]
- Amazon Elastic File System (EFS)
- Amazon Elastic Kubernetes Service (EKS) (ambos tipos de lanzamiento: Fargate y EC2)
- Amazon Elastic MapReduce (EMR)
- Amazon ElastiCache
- Amazon EventBridge
- Amazon FinSpace
- Amazon Forecast
- Amazon Fraud Detector
- Amazon FSx
- Amazon GuardDuty
- Amazon Inspector
- Amazon Inspector Classic
- Amazon Kendra
- Amazon Keyspaces (para Apache Cassandra)
- Amazon Kinesis Data Streams
- Amazon Kinesis Video Streams
- Amazon Lex
- Amazon Location Service
- Amazon Macie
- Amazon Managed Grafana
- Amazon Managed Service para Apache Flink
- Amazon Managed Service para Prometheus
- Amazon Managed Streaming para Apache Kafka
- Amazon Managed Workflows para Apache Airflow (Amazon MWAA)
- Amazon MemoryDB (anteriormente Amazon MemoryDB para Redis)
- Amazon MQ
- Amazon Neptune
- Amazon OpenSearch Service
- Amazon Personalize
- Amazon Pinpoint y End User Messaging (anteriormente Amazon Pinpoint)
- Amazon Polly
- Amazon Q Business
- Amazon Q Developer
- Amazon Quantum Ledger Database (QLDB)
- Amazon QuickSight
- AWS Elastic Beanstalk
- AWS Elastic Disaster Recovery
- AWS Elemental MediaConnect
- AWS Elemental MediaConvert
- AWS Elemental MediaLive
- AWS Entity Resolution
- Servicio de inyección de errores de AWS
- AWS Firewall Manager
- AWS Global Accelerator
- AWS Glue
- AWS Glue DataBrew
- Panel de AWS Health
- AWS HealthImaging
- AWS HealthLake
- AWS HealthOmics
- AWS IAM Identity Center
- AWS Identity and Access Management (IAM)
- AWS IoT Core
- AWS IoT Device Defender
- AWS IoT Device Management
- AWS IoT Events
- AWS IoT Greengrass
- AWS IoT SiteWise
- AWS IoT TwinMaker
- AWS Key Management Service (KMS)
- AWS Lake Formation
- AWS Lambda
- AWS License Manager
- AWS Mainframe Modernization
- AWS Managed Services
- AWS Network Firewall
- AWS OpsWorks [incluye Chef Automate, Puppet Enterprise]
- AWS OpsWorks Stacks
- AWS Organizations
- AWS Outposts
- AWS Payment Cryptography
- AWS Private Certificate Authority
- AWS Resilience Hub
- AWS Resource Access Manager (RAM)
- AWS Resource Groups
- AWS RoboMaker
- AWS Secrets Manager
- AWS Security Hub

- Amazon Redshift
- Amazon Rekognition
- Amazon Relational Database Service (RDS)
- Amazon Route 53
- Amazon S3 Glacier
- Amazon SageMaker [excluye Studio Lab, al personal público y al personal del proveedor para todas las características]
- Amazon Security Lake
- Amazon Simple Email Service (SES)
- Amazon Simple Notification Service (SNS)
- Amazon Simple Queue Service (SQS)
- Amazon Simple Storage Service (S3)
- Amazon Simple Workflow Service (SWF)
- Amazon SimpleDB
- Amazon Textract
- Amazon Timestream
- Amazon Transcribe
- Amazon Translate
- Amazon Virtual Private Cloud (VPC)
- Amazon WorkDocs
- Amazon WorkMail
- Amazon WorkSpaces
- AWS Server Migration Service (SMS)
- AWS Serverless Application Repository
- AWS Service Catalog
- AWS Shield
- AWS Signer
- AWS Snowball
- AWS Snowball Edge
- AWS Snowmobile
- AWS Step Functions
- AWS Storage Gateway
- AWS Systems Manager
- AWS Transfer Family
- Notificaciones de usuarios de AWS
- Acceso verificado de AWS
- AWS WAF
- AWS Wickr
- AWS X-Ray
- EC2 Image Builder
- Elastic Load Balancing (ELB)
- FreeRTOS
- VM Import/Export

Encontrará más información sobre los servicios incluidos en el siguiente enlace https://aws.amazon.com/compliance/services-in-scope/

El alcance de las ubicaciones cubiertas en este informe incluye los centros de datos compatibles en las siguientes regiones:

- **Australia:** Asia-Pacífico (Sídney) (ap-southeast-2), Asia-Pacífico (Melbourne) (ap-southeast-4)
- **Baréin:** Medio Oriente (Baréin) (me-south-1)
- **Brasil:** América del Sur (São Paulo) (sa-east-1)
- **Canadá:** Canadá (centro) (ca-central-1), Oeste de Canadá (Calgary) (ca-west-1)*
- **Inglaterra:** Europa (Londres) (eu-west-2)
- **Francia:** Europa (París) (eu-west-3)
- **Alemania:** Europa (Fráncfort) (eu-central-1)
- **Hong Kong:** Asia-Pacífico (ap-east-1)
- **India:** Asia-Pacífico (Bombay) (ap-south-1), Asia-Pacífico (Hyderabad) (ap-south-2)
- **Indonesia:** Asia-Pacífico (Yakarta) (ap-southeast-3)
- **Irlanda:** Europa (Irlanda) (eu-west-1)
- **Israel:** Israel (Tel Aviv) (il-central-1)*
- **Italia:** Europa (Milán) (eu-south-1)

- **Japón:** Asia-Pacífico (Tokio) (ap-northeast-1), Asia-Pacífico (Osaka) (ap-northeast-3)
- **Singapur:** Asia-Pacífico (Singapur) (ap-southeast-1)
- **Sudáfrica:** África (Ciudad del Cabo) (af-south-1)
- **Corea del Sur:** Asia-Pacífico (Seúl) (ap-northeast-2)
- **España:** Europa (España) (eu-south-2)
- **Suecia:** Europa (Estocolmo) (eu-north-1)
- **Suiza:** Europa (Zúrich) (eu-central-2)
- **Emiratos Árabes Unidos:** Medio Oriente (EAU) (me-central-1)
- **Estados Unidos:** Este de EE. UU. (Norte de Virginia) (us-east-1), Este de EE. UU. (Ohio) (us-east-2), Oeste de EE. UU. (Oregón) (us-west-2), Oeste de EE. UU. (Norte de California) (us-west-1), AWS GovCloud (Este de EE. UU.) (us-gov-east-1), AWS GovCloud (Oeste de EE. UU.) (us-gov-west-1)

* La fecha de entrada en vigor para esta región es el 15 de febrero de 2024.

y las siguientes ubicaciones periféricas de AWS:

- CABA, Argentina
- General Pacheco, Argentina
- Brisbane, Australia
- Canberra, Australia
- Melbourne, Australia
- Perth, Australia
- Viena, Austria
- Bruselas, Bélgica
- Fortaleza, Brasil
- Rio de Janeiro, Brasil
- São Paulo, Brasil
- Sofía, Bulgaria
- Toronto, Canadá
- Vancouver, Canadá
- Huechuraba, Chile
- Santiago, Chile
- Bogotá, Colombia
- Zagreb, Croacia
- Praga, República Checa
- Ballerup, Dinamarca
- El Cairo, Egipto
- Tallin, Estonia
- Helsinki, Finlandia
- Espoo, Finlandia
- Aubervilliers, Francia
- Marsella, Francia
- Haifa, Israel
- Milán, Italia
- Roma, Italia
- Inzai, Japón
- Nairobi, Kenia
- Kuala Lumpur, Malasia
- Santiago de Querétaro, México
- Ámsterdam, Países Bajos
- Diemen, Países Bajos
- Schiphol-Rijk, Países Bajos
- Auckland, Nueva Zelanda
- Rosedale, Nueva Zelanda
- Lagos, Nigeria
- Oslo, Noruega
- Barka, Omán
- Santiago de Surco, Perú
- Manila, Filipinas
- Ciudad Quezon, Filipinas
- Varsovia, Polonia
- Lisboa, Portugal
- Bucarest, Rumania
- Singapur, Singapur
- Ciudad del Cabo, Sudáfrica
- Johannesburgo, Sudáfrica
- Anyang-si, Corea del Sur
- Atlanta, Estados Unidos
- Aurora, Estados Unidos
- Bluffdale, Estados Unidos
- Boston, Estados Unidos
- Chandler, Estados Unidos
- Chicago, Estados Unidos
- Columbus, Estados Unidos
- Dallas, Estados Unidos
- Denver, Estados Unidos
- El Segundo, Estados Unidos
- Elk Grove Village, Estados Unidos
- Franklin, Estados Unidos
- Greenwood Village, Estados Unidos
- Hillsboro, Estados Unidos
- Houston, Estados Unidos
- Irvine, Estados Unidos
- Irving, Estados Unidos
- Kansas City, Estados Unidos
- Las Vegas, Estados Unidos
- Los Ángeles, Estados Unidos
- Lynnwood, Estados Unidos
- Miami, Estados Unidos
- Milpitas, Estados Unidos
- Mineápolis, Estados Unidos

- Berlín, Alemania
- Düsseldorf, Alemania
- Fráncfort, Alemania
- Hamburgo, Alemania
- Múnich, Alemania
- Koropi, Grecia
- Kropia, Grecia
- Budapest, Hungría
- Bangalore, India
- Chennai, India
- Calcuta, India
- Bombay, India
- Nueva Delhi, India
- Noida, India
- Pune, India
- Yakarta, Indonesia
- Clonshaugh, Irlanda
- Dublín, Irlanda
- Seúl, Corea del Sur
- Barcelona, España
- Madrid, España
- Estocolmo, Suecia
- Zúrich, Suiza
- Ciudad de Nuevo Taipei, Taiwán
- Taipei, Taiwán
- Bangkok, Tailandia
- Bang Chalong, Tailandia
- Estambul, Turquía
- Dubái, Emiratos Árabes Unidos
- Fujairah, Emiratos Árabes Unidos
- Londres, Reino Unido
- Manchester, Reino Unido
- Swinton, Reino Unido
- Ashburn, Estados Unidos
- Ciudad de Nueva York, Estados Unidos
- Newark, Estados Unidos
- Las Vegas del Norte, Estados Unidos
- Filadelfia, Estados Unidos
- Phoenix, Estados Unidos
- Piscataway, Estados Unidos
- Pittsburgh, Estados Unidos
- Portland, Estados Unidos
- Reston, Estados Unidos
- Richardson, Estados Unidos
- Seattle, Estados Unidos
- Secaucus, Estados Unidos
- Tampa, Estados Unidos
- Tempe, Estados Unidos
- West Valley City, Estados Unidos
- Hanói, Vietnam
- Ho Chi Minh, Vietnam

y las siguientes ubicaciones de Wavelength en:

- Toronto, Canadá
- Berlín, Alemania
- Dortmund, Alemania
- Múnich, Alemania
- Osaka, Japón
- Tama, Japón
- Daejeon, Corea del Sur
- Seúl, Corea del Sur
- Londres, Reino Unido
- Salford, Reino Unido
- Alpharetta, Estados Unidos
- Annapolis Junction, Estados Unidos
- Aurora, Estados Unidos
- Azusa, Estados Unidos
- Charlotte, Estados Unidos
- Euless, Estados Unidos
- Houston, Estados Unidos
- Knoxville, Estados Unidos
- Las Vegas, Estados Unidos
- Mineápolis, Estados Unidos
- New Berlin, Estados Unidos
- Pembroke Pines, Estados Unidos
- Plant City, Estados Unidos
- Redmond, Estados Unidos
- Rocklin, Estados Unidos
- Southfield, Estados Unidos
- Tempe, Estados Unidos
- Municipio de Wall, Estados Unidos
- Westborough, Estados Unidos

así como ubicaciones de zona local:

- CABA, Argentina
- Perth, Australia
- Santiago, Chile
- Ballerup, Dinamarca
- Espoo, Finlandia
- Hamburgo, Alemania
- Calcuta, India
- Nueva Delhi, India
- Noida, India*
- Santiago de Querétaro, México
- Rosedale, Nueva Zelanda
- Lagos, Nigeria
- Barka, Omán
- Santiago de Surco, Perú
- Manila, Filipinas
- Varsovia, Polonia
- Singapur, Singapur*
- Ciudad de Nuevo Taipei, Taiwán
- Bang Chalong, Tailandia
- Atlanta, Estados Unidos
- Boston, Estados Unidos
- Chicago, Estados Unidos
- Doral, Estados Unidos
- El Segundo, Estados Unidos
- Garland, Estados Unidos
- Greenwood Village, Estados Unidos
- Hillsboro, Estados Unidos
- Houston, Estados Unidos
- Irvine, Estados Unidos
- Itasca, Estados Unidos
- Kansas City, Estados Unidos
- Kapolei, Estados Unidos
- Las Vegas, Estados Unidos
- Lee's Summit, Estados Unidos*
- Lithia Springs, Estados Unidos
- Mesa, Estados Unidos
- Miami, Estados Unidos
- Mineápolis, Estados Unidos
- Las Vegas del Norte, Estados Unidos
- Filadelfia, Estados Unidos
- Phoenix, Estados Unidos
- Piscataway, Estados Unidos
- Richardson, Estados Unidos
- Seattle, Estados Unidos

* Esta ubicación es una zona local dedicada y es posible que no esté disponible para todos los clientes.

De acuerdo con los criterios para describir el sistema de una organización de servicios, según lo estipulado en la sección 200 de los Criterios de descripción DC de 2018, *Description Criteria for a Description of a Service Organization's System in a SOC 2 Report* (Criterios para la descripción del sistema de una organización de servicios en un informe SOC 2) (Criterios de descripción) y la idoneidad del diseño y la eficacia operativa de los controles incluidos en la Descripción durante todo el período comprendido entre el 1.º de octubre de 2023 y el 30 de septiembre de 2024 para proporcionar un aseguramiento razonable de que los compromisos de servicio y los requisitos del sistema se alcanzaron con base en los criterios de seguridad relevantes a la disponibilidad, confidencialidad y privacidad (criterios de servicios de confianza aplicables) establecidos en la sección 100 de TSP de 2017: *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (Criterios de los servicios de confianza en términos de seguridad, disponibilidad, integridad de procesos, confidencialidad y privacidad), en *Criterios de servicios de confianza* de AICPA.

La Descripción indica que los controles de AWS pueden proporcionar un aseguramiento razonable de que ciertos compromisos de servicio y requisitos del sistema se pueden lograr solo si los controles complementarios de las entidades usuarias asumidos en el diseño de los controles de AWS están adecuadamente diseñados y funcionan de forma eficaz, junto con los controles relacionados en la organización del servicio. Nuestra evaluación no incluyó dichos controles complementarios de las entidades usuarias, y no hemos evaluado la idoneidad del diseño o la eficacia operativa de dichos controles complementarios de la entidad usuaria.

La gestión de AWS proporciona la información de la sección adjunta “Otra información proporcionada por Amazon Web Services” para brindar información adicional, y no forma parte de la Descripción de AWS. No se ha sometido a dicha información a los procedimientos aplicados en nuestra evaluación y, por eso, no expresamos ninguna opinión al respecto.

Responsabilidades de AWS

AWS es responsable de sus compromisos de servicio y requisitos del sistema, así como del diseño**,** la implementación y el funcionamiento de controles efectivos dentro del sistema para proporcionar un aseguramiento razonable de que sus compromisos de servicio y los requisitos del sistema se hayan alcanzado. AWS proporcionó la afirmación adjunta, denominada “Afirmación de la gestión de Amazon Web Services” (Afirmación), sobre la presentación de la Descripción basada en los Criterios de descripción y la idoneidad del diseño y la eficacia operativa de los controles que se mencionan en el presente documento para proporcionar un aseguramiento razonable de que los compromisos de servicio y los requisitos del sistema se cumplirían con base en los criterios de servicios de confianza aplicables. AWS es responsable de (1) la preparación de la Descripción y la Afirmación; (2) la integridad, la exactitud y el método de presentación de la Descripción y la Afirmación; (3) la prestación de los servicios cubiertos por la Descripción; (4) la selección de las categorías de los servicios de confianza abordados por el compromiso y la mención de los criterios de servicios de confianza aplicables y los controles relacionados en la Descripción; (5) la identificación de los riesgos que amenazan la consecución de los compromisos de servicio y los requisitos del sistema de la organización de servicios; y (6) el diseño**,** la implementación y la documentación de los controles que están adecuadamente diseñados y que funcionan de forma eficaz para alcanzar sus compromisos de servicio y los requisitos del sistema.

Responsabilidades del auditor de servicios

Nuestra responsabilidad consiste en expresar una opinión sobre la presentación de la Descripción y sobre la idoneidad del diseño y la eficacia operativa de los controles mencionados en ella para cumplir los compromisos de servicio y los requisitos del sistema de la organización de servicios con base en nuestra evaluación.

Nuestra evaluación se llevó a cabo de acuerdo con los estándares de certificación establecidos por el Instituto Estadounidense de Contadores Públicos Certificados (AICPA) y de acuerdo con la Norma Internacional sobre Compromisos de Aseguramiento 3000 (revisada), *Assurance Engagements Other Than Audits or Reviews of Historical Financial Information* (Compromisos de aseguramiento que no sean auditorías ni revisiones de información financiera histórica), emitida por el Consejo de Normas Internacionales de Auditoría y Aseguramiento. Estos estándares exigen que planifiquemos y realicemos nuestra evaluación para obtener un aseguramiento razonable sobre si, en todos los aspectos materiales, (1) la Descripción se presenta de acuerdo con los Criterios de descripción, y (2) los controles mencionados en ella se diseñaron adecuadamente y funcionan de manera eficaz para proporcionar un aseguramiento razonable de que los compromisos de servicio y los requisitos del sistema de la organización de servicios se cumplieron con base en los criterios de servicios de confianza aplicables durante todo el período comprendido entre el 1.º de octubre de 2023 y el 30 de septiembre de 2024. La naturaleza, el momento y el alcance de los procedimientos seleccionados dependen de nuestro juicio, incluida la evaluación del riesgo de que se produzcan declaraciones erradas de importancia material, ya sea por fraude o por error. Consideramos que la evidencia que obtuvimos es suficiente y adecuada para proporcionar un fundamento razonable para nuestra opinión.

Una evaluación de la descripción del sistema de una organización de servicios y de la idoneidad del diseño y la eficacia operativa de los controles implica lo siguiente:

- Obtener una comprensión del sistema y de los compromisos de servicio y de los requisitos del sistema de la organización de servicios.
- Evaluar los riesgos de que la Descripción no se presente de acuerdo con los Criterios de descripción y de que los controles no estén adecuadamente diseñados o no funcionen de forma eficaz en función de los criterios de servicios de confianza aplicables.
- Realizar procedimientos para obtener evidencia sobre si la Descripción se presenta de acuerdo con los Criterios de la Descripción.
- Realizar procedimientos para obtener evidencia sobre si los controles indicados en la Descripción estaban adecuadamente diseñados para proporcionar un aseguramiento razonable de que la organización de servicios cumplía sus compromisos de servicio y los requisitos del sistema en función de los criterios de servicios de confianza aplicables.
- Comprobar la eficacia operativa de dichos controles para ofrecer un aseguramiento razonable de que se cumplieron los compromisos de servicio y los requisitos del sistema de la organización de servicios en función de los criterios de servicios de confianza aplicables.
- Evaluar la presentación general de la Descripción.

Nuestra evaluación también incluyó la realización de otros procedimientos que consideramos necesarios en las circunstancias.

Tenemos la obligación de ser independientes de AWS y de cumplir con nuestras otras responsabilidades éticas, de acuerdo con los requisitos éticos pertinentes relacionados con nuestro compromiso de evaluación.

Aplicamos la Normativa internacional sobre la gestión de la calidad 1, *gestión de la calidad para empresas que realizan auditorías o revisiones de estados financieros, u otros compromisos de aseguramiento o servicios relacionados*, que exige que diseñemos, implementemos y apliquemos un sistema de gestión de la calidad que incluya políticas o procedimientos relacionados con el cumplimiento de los requisitos éticos, las normas profesionales y los requisitos legales y regulatorios aplicables.

Limitaciones inherentes
La Descripción se elaboró para satisfacer las necesidades comunes de una amplia gama de usuarios del informe y, por tanto, es posible que no incluya todos los aspectos del sistema que cada usuario individual pueda considerar importantes para satisfacer sus necesidades de información.

Hay limitaciones inherentes a la eficacia de cualquier sistema de control interno, incluida la posibilidad de error humano y la elusión de controles. Debido a su naturaleza, es posible que los controles de una organización de servicios no siempre funcionen de forma eficaz para proporcionar un aseguramiento razonable de que los compromisos de servicio y los requisitos del sistema de la organización de servicios se cumplen en función de los criterios de servicios de confianza aplicables. Asimismo, la proyección a futuro de cualquier evaluación de la presentación de la Descripción o de las conclusiones sobre la idoneidad del diseño o de la eficacia operativa de los controles para cumplir los criterios de servicios de confianza aplicables está sujeta al riesgo de que el sistema pueda cambiar o de que los controles de una organización de servicios puedan volverse ineficaces.

Descripción de las pruebas de los controles
Los controles específicos sometidos a prueba, así como la naturaleza, el momento y los resultados de dichas pruebas, se enumeran en la "Descripción de criterios, controles, pruebas y resultados de las pruebas de AWS" (Descripción de las pruebas y los resultados) que se adjunta.

Opinión
En nuestra opinión, en todos los aspectos materiales:

a. En la Descripción, se presenta el Sistema de AWS que se diseñó e implementó durante todo el período comprendido entre el 1.° de octubre de 2023 y el 30 de septiembre de 2024 conforme a los Criterios de descripción.

b. Los controles mencionados en la Descripción se diseñaron adecuadamente durante todo el período comprendido entre el 1.º de octubre de 2023 y el 30 de septiembre de 2024 para proveer un aseguramiento razonable de que los compromisos de servicio y los requisitos del sistema de AWS se cumplirían con base en los criterios de servicios de confianza aplicables, si los controles funcionaron de forma eficaz durante todo ese período y si las entidades usuarias aplicaron los controles complementarios asumidos en el diseño de los controles de AWS durante todo ese período.

c. Los controles mencionados en la Descripción operaron de forma eficaz durante todo el período comprendido entre el 1.º de octubre de 2023 y el 30 de septiembre de 2024 para proveer un aseguramiento razonable de que los compromisos de servicio y los requisitos del sistema de AWS se alcanzaron con base en los criterios de servicios de confianza aplicables si los controles de las entidades usuarias asumidos en el diseño de los controles de AWS funcionaron de forma eficaz durante todo ese período.

Uso restringido
Este informe, incluida la descripción de las pruebas de los controles y los resultados de estas en la Descripción de las pruebas y los resultados, está destinado exclusivamente a la información y el uso de AWS, las entidades usuarias del sistema de AWS durante todo el período comprendido entre el 1.° de octubre de 2023 y el 30 de septiembre de 2024, o parte de este, y las posibles entidades usuarias, los auditores independientes y los profesionales que prestan servicios a dichas entidades usuarias, así como los reguladores que tengan suficiente conocimiento y comprensión de lo siguiente:

- la naturaleza del servicio prestado por la organización de servicios
- cómo interactúa el sistema de la organización de servicios con las entidades usuarias, las organizaciones de subservicios u otras partes
- el control interno y sus limitaciones
- controles complementarios de las entidades usuarias y cómo esos controles interactúan con los controles de la organización de servicios para cumplir los compromisos de servicio y los requisitos del sistema de la organización de servicios
- las responsabilidades de la entidad usuaria y cómo interactúan con los controles relacionados en la organización de servicios

- los criterios de los servicios de confianza aplicables
- los riesgos que pueden amenazar la consecución de los compromisos del servicio y los requisitos del sistema de la organización de servicios y cómo los controles abordan esos riesgos

El presente informe no está destinado a ser utilizado, ni debe serlo, por nadie más que por las partes mencionadas.

[Ver la versión en inglés para acceder a una opinión firmada por un auditor independiente]

13 de diciembre de 2024

SECCIÓN III: Descripción del sistema de Amazon Web Services en términos de seguridad, disponibilidad, confidencialidad y privacidad

Información general del Sistema de Amazon Web Services

Desde 2006, Amazon Web Services (AWS) proporciona infraestructura de TI flexible, escalable y segura a empresas de todos los tamaños a nivel mundial. Con AWS, los clientes pueden implementar soluciones en un entorno de computación en la nube que proporciona potencia de computación, almacenamiento y otros servicios de aplicación por Internet conforme a la demanda de las necesidades comerciales. AWS otorga a las empresas la flexibilidad para emplear los sistemas operativos, los programas de aplicación y las bases de datos que elijan.

El alcance de esta descripción del sistema incluye los siguientes servicios:

- Amazon API Gateway
- Amazon AppFlow
- Controlador de recuperación de aplicaciones de Amazon
- Amazon AppStream 2.0
- Amazon Athena
- Amazon Augmented AI [excluye el personal público y el personal del proveedor para todas las características]
- Amazon Bedrock
- Amazon Braket
- Amazon Chime
- Amazon Chime SDK
- Amazon Cloud Directory
- Amazon CloudFront (excluye la entrega de contenido a través del punto de presencias integrado de Amazon CloudFront)
- Amazon CloudWatch
- Amazon CloudWatch Logs
- Amazon CodeWhisperer
- Amazon Cognito
- Amazon Comprehend
- Amazon Comprehend Medical
- Amazon Connect
- Amazon Data Firehose
- Amazon DataZone
- Amazon Detective
- Amazon DevOps Guru
- Amazon DocumentDB (compatible con MongoDB)
- Amazon DynamoDB
- Acelerador de Amazon DynamoDB (DAX)
- Amazon EC2 Auto Scaling
- Amazon Elastic Block Store (EBS)
- Amazon Elastic Compute Cloud (EC2)
- Amazon Elastic Container Registry (ECR)
- Amazon WorkSpaces Secure Browser (anteriormente conocido como Amazon Workspaces Web)
- Cliente ligero de Amazon WorkSpaces
- AWS Amplify
- AWS App Mesh
- AWS App Runner
- AWS AppFabric
- AWS Application Migration Service
- AWS AppSync
- AWS Artifact
- AWS Audit Manager
- AWS Backup
- AWS Batch
- AWS Certificate Manager (ACM)
- AWS Chatbot
- AWS Clean Rooms
- AWS Cloud Map
- AWS Cloud9
- AWS CloudFormation
- AWS CloudHSM
- AWS CloudShell
- AWS CloudTrail
- AWS CodeBuild
- AWS CodeCommit
- AWS CodeDeploy
- AWS CodePipeline
- AWS Config
- AWS Control Tower
- AWS Data Exchange
- AWS Database Migration Service (DMS)
- AWS DataSync
- AWS Direct Connect
- AWS Directory Service [excluye Simple AD]
- AWS Elastic Beanstalk

- Amazon Elastic Container Service [los dos tipos de lanzamiento Fargate y EC2]
- Amazon Elastic File System (EFS)
- Amazon Elastic Kubernetes Service (EKS) (ambos tipos de lanzamiento: Fargate y EC2)
- Amazon Elastic MapReduce (EMR)
- Amazon ElastiCache
- Amazon EventBridge
- Amazon FinSpace
- Amazon Forecast
- Amazon Fraud Detector
- Amazon FSx
- Amazon GuardDuty
- Amazon Inspector
- Amazon Inspector Classic
- Amazon Kendra
- Amazon Keyspaces (para Apache Cassandra)
- Amazon Kinesis Data Streams
- Amazon Kinesis Video Streams
- Amazon Lex
- Amazon Location Service
- Amazon Macie
- Amazon Managed Grafana
- Amazon Managed Service para Apache Flink
- Amazon Managed Service para Prometheus
- Amazon Managed Streaming para Apache Kafka
- Amazon Managed Workflows para Apache Airflow (Amazon MWAA)
- Amazon MemoryDB (anteriormente Amazon MemoryDB para Redis)
- Amazon MQ
- Amazon Neptune
- Amazon OpenSearch Service
- Amazon Personalize
- Amazon Pinpoint y End User Messaging (anteriormente Amazon Pinpoint)
- Amazon Polly
- Amazon Q Business
- Amazon Q Developer
- Amazon Quantum Ledger Database (QLDB)
- Amazon QuickSight
- Amazon Redshift
- Amazon Rekognition
- Amazon Relational Database Service (RDS)
- Amazon Route 53
- AWS Elastic Disaster Recovery
- AWS Elemental MediaConnect
- AWS Elemental MediaConvert
- AWS Elemental MediaLive
- AWS Entity Resolution
- Servicio de inyección de errores de AWS
- AWS Firewall Manager
- AWS Global Accelerator
- AWS Glue
- AWS Glue DataBrew
- Panel de AWS Health
- AWS HealthImaging
- AWS HealthLake
- AWS HealthOmics
- AWS IAM Identity Center
- AWS Identity and Access Management (IAM)
- AWS IoT Core
- AWS IoT Device Defender
- AWS IoT Device Management
- AWS IoT Events
- AWS IoT Greengrass
- AWS IoT SiteWise
- AWS IoT TwinMaker
- AWS Key Management Service (KMS)
- AWS Lake Formation
- AWS Lambda
- AWS License Manager
- AWS Mainframe Modernization
- AWS Managed Services
- AWS Network Firewall
- AWS OpsWorks [incluye Chef Automate, Puppet Enterprise]
- AWS OpsWorks Stacks
- AWS Organizations
- AWS Outposts
- AWS Payment Cryptography
- AWS Private Certificate Authority
- AWS Resilience Hub
- AWS Resource Access Manager (RAM)
- AWS Resource Groups
- AWS RoboMaker
- AWS Secrets Manager
- AWS Security Hub
- AWS Server Migration Service (SMS)
- AWS Serverless Application Repository

- Amazon S3 Glacier
- Amazon SageMaker [excluye Studio Lab, al personal público y al personal del proveedor para todas las características]
- Amazon Security Lake
- Amazon Simple Email Service (SES)
- Amazon Simple Notification Service (SNS)
- Amazon Simple Queue Service (SQS)
- Amazon Simple Storage Service (S3)
- Amazon Simple Workflow Service (SWF)
- Amazon SimpleDB
- Amazon Textract
- Amazon Timestream
- Amazon Transcribe
- Amazon Translate
- Amazon Virtual Private Cloud (VPC)
- Amazon WorkDocs
- Amazon WorkMail
- Amazon WorkSpaces
- AWS Service Catalog
- AWS Shield
- AWS Signer
- AWS Snowball
- AWS Snowball Edge
- AWS Snowmobile
- AWS Step Functions
- AWS Storage Gateway
- AWS Systems Manager
- AWS Transfer Family
- Notificaciones de usuarios de AWS
- Acceso verificado de AWS
- AWS WAF
- AWS Wickr
- AWS X-Ray
- EC2 Image Builder
- Elastic Load Balancing (ELB)
- FreeRTOS
- VM Import/Export

Encontrará más información sobre los servicios incluidos en el siguiente enlace https://aws.amazon.com/compliance/services-in-scope/

El alcance de las ubicaciones cubiertas en este informe incluye los centros de datos compatibles en las siguientes regiones:

- **Australia:** Asia-Pacífico (Sídney) (ap-southeast-2), Asia-Pacífico (Melbourne) (ap-southeast-4)
- **Baréin:** Medio Oriente (Baréin) (me-south-1)
- **Brasil:** América del Sur (São Paulo) (sa-east-1)
- **Canadá:** Canadá (centro) (ca-central-1), Oeste de Canadá (Calgary) (ca-west-1)*
- **Inglaterra:** Europa (Londres) (eu-west-2)
- **Francia:** Europa (París) (eu-west-3)
- **Alemania:** Europa (Fráncfort) (eu-central-1)
- **Hong Kong:** Asia-Pacífico (ap-east-1)
- **India:** Asia-Pacífico (Bombay) (ap-south-1), Asia-Pacífico (Hyderabad) (ap-south-2)
- **Indonesia:** Asia-Pacífico (Yakarta) (ap-southeast-3)
- **Irlanda:** Europa (Irlanda) (eu-west-1)
- **Israel:** Israel (Tel Aviv) (il-central-1)*
- **Italia:** Europa (Milán) (eu-south-1)
- **Japón:** Asia-Pacífico (Tokio) (ap-northeast-1), Asia-Pacífico (Osaka) (ap-northeast-3)
- **Singapur:** Asia-Pacífico (Singapur) (ap-southeast-1)
- **Sudáfrica:** África (Ciudad del Cabo) (af-south-1)
- **Corea del Sur:** Asia-Pacífico (Seúl) (ap-northeast-2)
- **España:** Europa (España) (eu-south-2)
- **Suecia:** Europa (Estocolmo) (eu-north-1)

- **Suiza:** Europa (Zúrich) (eu-central-2)
- **Emiratos Árabes Unidos:** Medio Oriente (EAU) (me-central-1)
- **Estados Unidos:** Este de EE. UU. (Norte de Virginia) (us-east-1), Este de EE. UU. (Ohio) (us-east-2), Oeste de EE. UU. (Oregón) (us-west-2), Oeste de EE. UU. (Norte de California) (us-west-1), AWS GovCloud (Este de EE. UU.) (us-gov-east-1), AWS GovCloud (Oeste de EE. UU.) (us-gov-west-1)

* La fecha de entrada en vigor para esta región es el 15 de febrero de 2024.

y las siguientes ubicaciones periféricas de AWS:

- CABA, Argentina
- General Pacheco, Argentina
- Brisbane, Australia
- Canberra, Australia
- Melbourne, Australia
- Perth, Australia
- Viena, Austria
- Bruselas, Bélgica
- Fortaleza, Brasil
- Rio de Janeiro, Brasil
- São Paulo, Brasil
- Sofía, Bulgaria
- Toronto, Canadá
- Vancouver, Canadá
- Huechuraba, Chile
- Santiago, Chile
- Bogotá, Colombia
- Zagreb, Croacia
- Praga, República Checa
- Ballerup, Dinamarca
- El Cairo, Egipto
- Tallin, Estonia
- Helsinki, Finlandia
- Espoo, Finlandia
- Aubervilliers, Francia
- Marsella, Francia
- Berlín, Alemania
- Düsseldorf, Alemania
- Fráncfort, Alemania
- Hamburgo, Alemania
- Múnich, Alemania
- Koropi, Grecia
- Haifa, Israel
- Milán, Italia
- Roma, Italia
- Inzai, Japón
- Nairobi, Kenia
- Kuala Lumpur, Malasia
- Santiago de Querétaro, México
- Ámsterdam, Países Bajos
- Diemen, Países Bajos
- Schiphol-Rijk, Países Bajos
- Auckland, Nueva Zelanda
- Rosedale, Nueva Zelanda
- Lagos, Nigeria
- Oslo, Noruega
- Barka, Omán
- Santiago de Surco, Perú
- Manila, Filipinas
- Ciudad Quezon, Filipinas
- Varsovia, Polonia
- Lisboa, Portugal
- Bucarest, Rumania
- Singapur, Singapur
- Ciudad del Cabo, Sudáfrica
- Johannesburgo, Sudáfrica
- Anyang-si, Corea del Sur
- Seúl, Corea del Sur
- Barcelona, España
- Madrid, España
- Estocolmo, Suecia
- Zúrich, Suiza
- Ciudad de Nuevo Taipei, Taiwán
- Atlanta, Estados Unidos
- Aurora, Estados Unidos
- Bluffdale, Estados Unidos
- Boston, Estados Unidos
- Chandler, Estados Unidos
- Chicago, Estados Unidos
- Columbus, Estados Unidos
- Dallas, Estados Unidos
- Denver, Estados Unidos
- El Segundo, Estados Unidos
- Elk Grove Village, Estados Unidos
- Franklin, Estados Unidos
- Greenwood Village, Estados Unidos
- Hillsboro, Estados Unidos
- Houston, Estados Unidos
- Irvine, Estados Unidos
- Irving, Estados Unidos
- Kansas City, Estados Unidos
- Las Vegas, Estados Unidos
- Los Ángeles, Estados Unidos
- Lynnwood, Estados Unidos
- Miami, Estados Unidos
- Milpitas, Estados Unidos
- Mineápolis, Estados Unidos
- Ciudad de Nueva York, Estados Unidos
- Newark, Estados Unidos
- Las Vegas del Norte, Estados Unidos
- Filadelfia, Estados Unidos
- Phoenix, Estados Unidos

- Kropia, Grecia
- Budapest, Hungría
- Bangalore, India
- Chennai, India
- Calcuta, India
- Bombay, India
- Nueva Delhi, India
- Noida, India
- Pune, India
- Yakarta, Indonesia
- Clonshaugh, Irlanda
- Dublín, Irlanda
- Taipei, Taiwán
- Bangkok, Tailandia
- Bang Chalong, Tailandia
- Estambul, Turquía
- Dubái, Emiratos Árabes Unidos
- Fujairah, Emiratos Árabes Unidos
- Londres, Reino Unido
- Manchester, Reino Unido
- Swinton, Reino Unido
- Ashburn, Estados Unidos
- Piscataway, Estados Unidos
- Pittsburgh, Estados Unidos
- Portland, Estados Unidos
- Reston, Estados Unidos
- Richardson, Estados Unidos
- Seattle, Estados Unidos
- Secaucus, Estados Unidos
- Tampa, Estados Unidos
- Tempe, Estados Unidos
- West Valley City, Estados Unidos
- Hanói, Vietnam
- Ho Chi Minh, Vietnam

y las siguientes ubicaciones de Wavelength en:

- Toronto, Canadá
- Berlín, Alemania
- Dortmund, Alemania
- Múnich, Alemania
- Osaka, Japón
- Tama, Japón
- Daejeon, Corea del Sur
- Seúl, Corea del Sur
- Londres, Reino Unido
- Salford, Reino Unido
- Alpharetta, Estados Unidos
- Annapolis Junction, Estados Unidos
- Aurora, Estados Unidos
- Azusa, Estados Unidos
- Charlotte, Estados Unidos
- Euless, Estados Unidos
- Houston, Estados Unidos
- Knoxville, Estados Unidos
- Las Vegas, Estados Unidos
- Mineápolis, Estados Unidos
- New Berlin, Estados Unidos
- Pembroke Pines, Estados Unidos
- Plant City, Estados Unidos
- Redmond, Estados Unidos
- Rocklin, Estados Unidos
- Southfield, Estados Unidos
- Tempe, Estados Unidos
- Municipio de Wall, Estados Unidos
- Westborough, Estados Unidos

así como ubicaciones de zona local:

- CABA, Argentina
- Perth, Australia
- Santiago, Chile
- Ballerup, Dinamarca
- Espoo, Finlandia
- Hamburgo, Alemania
- Calcuta, India
- Nueva Delhi, India
- Noida, India*
- Santiago de Querétaro, México
- Varsovia, Polonia
- Singapur, Singapur*
- Ciudad de Nuevo Taipei, Taiwán
- Bang Chalong, Tailandia
- Atlanta, Estados Unidos
- Boston, Estados Unidos
- Chicago, Estados Unidos
- Doral, Estados Unidos
- El Segundo, Estados Unidos
- Garland, Estados Unidos
- Kansas City, Estados Unidos
- Kapolei, Estados Unidos
- Las Vegas, Estados Unidos
- Lee’s Summit, Estados Unidos*
- Lithia Springs, Estados Unidos
- Mesa, Estados Unidos
- Miami, Estados Unidos
- Mineápolis, Estados Unidos
- Las Vegas del Norte, Estados Unidos
- Filadelfia, Estados Unidos
- Phoenix, Estados Unidos

- Rosedale, Nueva Zelanda
- Lagos, Nigeria
- Barka, Omán
- Santiago de Surco, Perú
- Manila, Filipinas
- Greenwood Village, Estados Unidos
- Hillsboro, Estados Unidos
- Houston, Estados Unidos
- Irvine, Estados Unidos
- Itasca, Estados Unidos
- Piscataway, Estados Unidos
- Richardson, Estados Unidos
- Seattle, Estados Unidos

* Esta ubicación es una zona local dedicada y es posible que no esté disponible para todos los clientes.

Entorno de responsabilidad compartida

Trasladar la infraestructura de TI del cliente a AWS crea un modelo de responsabilidad compartida entre los clientes y AWS. AWS opera, administra y controla los componentes desde el sistema operativo del host y la capa de virtualización hasta la seguridad física de las instalaciones en las que funciona el servicio. A cambio, los clientes asumen la responsabilidad y la gestión del diseño, la implementación y la operación de su entorno de AWS, que puede incluir los sistemas operativos invitados (incluidas las actualizaciones y parches de seguridad), otro software de aplicaciones asociado, así como la configuración del firewall del grupo de seguridad que ofrece AWS. Los clientes deben examinar con cuidado los servicios que eligen, ya que sus responsabilidades varían en función de los servicios utilizados, la integración de los servicios en los entornos de TI y las leyes y regulaciones correspondientes. Es posible mejorar la seguridad o cumplir con requisitos de conformidad más exigentes gracias al aprovechamiento de tecnologías como firewalls basados en el host, detección o prevención de intrusiones basadas en el host y cifrado. AWS proporciona herramientas e información para asistir a los clientes en sus esfuerzos para valorar y validar el funcionamiento eficaz de los controles en sus entornos de TI ampliados. Para obtener más información, consulte el Centro de cumplimiento de AWS en https://aws.amazon.com/compliance.

AWS ofrece una variedad de servicios diferentes de plataforma e infraestructura. Para obtener más información sobre el Modelo de responsabilidad compartida de AWS, consulte https://aws.amazon.com/compliance/shared-responsibility-model/. Para brindar claridad sobre la seguridad y la responsabilidad compartida de los servicios de AWS, AWS ha clasificado sus servicios en tres categorías principales: abstraídos, de infraestructura y de contenedores. Cada categoría viene con un modelo de propiedad de seguridad ligeramente diferente basado en cómo los clientes interactúan y acceden a la funcionalidad. Los servicios en la nube de AWS que selecciona un cliente determinan su responsabilidad. Esto determina la cantidad de trabajo de configuración que el cliente debe realizar como parte de sus responsabilidades de seguridad.

Servicios de infraestructura: servicios como Amazon Elastic Compute Cloud (Amazon EC2) y Amazon Virtual Private Cloud (Amazon VPC) se clasifican como Servicios de infraestructura y, como tales, requieren que el cliente lleve a cabo las tareas de administración y configuración de seguridad necesarias. Si el cliente implementa una instancia de Amazon EC2, se debe encargar de administrar el sistema operativo huésped (incluidas las actualizaciones y los parches de seguridad), el software de aplicación o las utilidades que instale en las instancias y la configuración del firewall que proporciona AWS (denominado grupo de seguridad) en cada instancia.

Servicios de contenedor: los servicios de esta categoría suelen ejecutarse por separado en Amazon EC2 u otras instancias de infraestructura, pero, algunas veces, los clientes no deben administrar la capa del sistema operativo o de la plataforma. AWS proporciona un servicio administrado para estos "contenedores" de aplicaciones. Los CSC son responsables de configurar y administrar los controles de red, como las reglas de firewall, y de llevar a cabo la gestión de identidad y acceso a nivel de la plataforma fuera de la IAM. Los ejemplos de servicios de contenedor incluyen a Amazon Relational Database Service (Amazon RDS), Amazon Elastic Map Reduce (Amazon EMR), y AWS Elastic Beanstalk.

Servicios abstractos: esta categoría incluye servicios de alto nivel de almacenamiento, bases de datos y mensajería, como Amazon Simple Storage Service (Amazon S3), Amazon Glacier, Amazon DynamoDB, Amazon Simple Queue Service (SQS) y Amazon Simple Email Service (Amazon SES). Estos servicios abstraen la capa de plataforma o gestión en la que los clientes pueden crear y operar aplicaciones en la nube. Los clientes acceden a los puntos de conexión de estos servicios abstractos mediante las API de AWS, y AWS administra los componentes del servicio subyacente o el sistema operativo en el que residen.

Como cada cliente implementa su entorno de manera diferente en AWS, los clientes pueden aprovechar la transferencia de la gestión de determinados controles de TI a AWS, lo que da como resultado un (nuevo) entorno de control distribuido. Luego, los clientes pueden utilizar la documentación de control y cumplimiento de AWS disponible para llevar a cabo sus procedimientos de evaluación y verificación de control según sea necesario. Determinadas funciones de los servicios se identificaron como controles en la descripción del sistema y son denominadas como "específicas del servicio" ya que son únicas al servicio correspondiente.

Puede encontrar más información y ejemplos sobre las prácticas recomendadas de seguridad de AWS en https://aws.amazon.com/architecture/security-identity-compliance/.

Además, AWS publica blogs de seguridad que cubren las prácticas recomendadas sobre el uso de los servicios de AWS en https://aws.amazon.com/blogs/security/tag/best-practices/.

Aspectos relevantes de los controles internos

Según lo define el Instituto Americano de Contadores Públicos Autorizados (AICPA), el control interno es un proceso afectado por la junta directiva, la gerencia y otro personal de una entidad y consta de cinco componentes interrelacionados:

- Entorno de control: establece el tono de una organización, influyendo en la conciencia de control de su personal. Es la base de todos los demás componentes del control interno porque proporciona disciplina y estructura.
- Evaluación del riesgo: la identificación y el análisis de riesgos relevantes por parte de la entidad para el logro de sus objetivos, que forma una base para determinar cómo deben administrarse los riesgos.
- Información y comunicación: en torno a estas actividades se encuentran los sistemas de información y comunicación. Estos permiten al personal de la entidad capturar e intercambiar la información necesaria para realizar y controlar sus operaciones.

- Monitoreo: se debe monitorear todo el proceso y realizar las modificaciones necesarias. De esta manera, el sistema puede reaccionar dinámicamente al cambiar según lo requieran las condiciones.
- Actividades de control: se deben establecer y ejecutar políticas y procedimientos de control para ayudar a garantizar que las acciones que la gestión identifique como necesarias para abordar los riesgos para el logro de los objetivos de la entidad se lleven a cabo de manera efectiva.

Esta sección describe brevemente las características esenciales y otros componentes interrelacionados de los controles internos para cumplir con los compromisos de servicio y los requisitos del sistema para aquellos criterios de seguridad, disponibilidad, confidencialidad y privacidad de los servicios de confianza aplicables en lo que respecta a AWS, que pueden ser relevantes para los clientes en cinco áreas amplias:

- Políticas (entorno de control y gestión de riesgos): la entidad ha definido y documentado sus políticas relevantes para los criterios de servicios de confianza aplicables.
- Comunicaciones (información y comunicación): la entidad ha comunicado sus políticas definidas a las partes responsables y usuarios autorizados del sistema.
- Compromisos de servicio y requisitos del sistema (actividades de control): la entidad comunicó a los clientes sus compromisos de servicio y requisitos del sistema de conformidad con los acuerdos con los clientes.
- Procedimientos (actividades de control): la entidad ha puesto en funcionamiento procedimientos para lograr los compromisos de servicio y los requisitos del sistema de acuerdo con sus políticas definidas.
- Monitoreo: la entidad monitorea el sistema y toma medidas para mantener el cumplimiento de sus políticas definidas.

A. Políticas

A.1 Entorno de control

AWS es una unidad dentro de Amazon.com (“Amazon” o “la Empresa”) que se alinea organizativamente en torno a cada uno de los servicios web, como Amazon EC2, Amazon S3, Amazon VPC, Amazon EBS y Amazon RDS. AWS aprovecha algunos aspectos del entorno de control general de Amazon en la entrega de estos servicios web. El entorno de control colectivo abarca los esfuerzos de la dirección y los empleados para establecer y mantener un entorno que respalde la eficacia de controles específicos. AWS mantiene sitios web informativos internos que describen el entorno de AWS, sus límites, las responsabilidades del usuario y los servicios **(Control AWSCA-9.1)**.

El entorno de control en Amazon comienza en el nivel más alto de la Empresa. El liderazgo ejecutivo y el sénior juegan un papel importante en el establecimiento de los valores fundamentales y el tono de la empresa en la cima. El Código de conducta y ética empresarial de la Empresa, que establece los principios rectores, está a disposición de todos los empleados.

Amazon se compromete a contar con miembros altamente calificados como parte de la junta directiva **(Control AWSCA-1.7)**. Anualmente, el Comité de gobierno corporativo de Amazon proporciona a cada miembro de la junta un cuestionario que establece si son independientes y si están calificados para formar parte de cada junta o comité según las reglas aplicables. El Comité de gobierno corporativo revisa y evalúa periódicamente la composición de la junta y su desempeño general durante la evaluación anual de sus miembros individuales. El Comité de Compensación y Desarrollo de Liderazgo, con la presencia de todos los miembros de la junta, evalúa anualmente el plan de sucesión de cada miembro del equipo de Senior Management **(Control AWSCA-1.8)**. Esto incluye el plan anual de sucesión y desempeño de la empresa y el director ejecutivo (CEO).

AWS se compromete a proteger los datos de sus clientes y a mantener el cumplimiento de los requisitos regulatorios aplicables. Esto se demuestra en el plan operativo anual consolidado que incluye requisitos y objetivos regulatorios y de cumplimiento para permitir la identificación y evaluación de los riesgos relacionados con esos objetivos **(Control AWSCA-1.9)**. Las políticas y los procedimientos de AWS describen la guía necesaria para la seguridad de la información y la operación que admite entornos de AWS, el uso aceptable de dispositivos móviles y el acceso al contenido de datos y dispositivos de red **(Control AWSCA-3.16)**. Los empleados de AWS deben revisar las políticas y procedimientos aplicables, ya que se actualizan periódicamente.

Amazon ha creado una línea directa de ética para que los empleados o contratistas externos puedan denunciar las conductas indebidas o infracciones de las políticas, prácticas, reglas, requisitos o procedimientos de AWS **(Control AWSCA-9.6).** Las infracciones importantes del Código de Conducta y Ética Empresarial de la empresa o de cualquier otra política similar se gestiona de forma adecuada, lo que puede incluir medidas disciplinarias o el despido. Amazon comunica las infracciones que cometan los vendedores o los contratistas externos a sus empleadores para que adopten medidas disciplinarias, retiren su asignación a Amazon o rescindan el contrato **(Control AWSCA-9.7).**

La administración de AWS ha implementado un programa de auditoría formal que monitorea y audita los controles diseñados para la protección frente a los riesgos de la organización y la salvaguarda del contenido de los clientes. Esto incluye evaluaciones externas independientes con respecto a los marcos de control reglamentarios, internos y externos. Las auditorías internas y externas se planifican, se realizan y se informan al Comité de Auditoría. El equipo de conformidad de AWS realiza y revisa el plan de auditoría de acuerdo con el calendario de auditoría documentado y comunica los requisitos de auditoría basados en criterios estándar que verifican el cumplimiento de los requisitos reglamentarios y el riesgo notificado al Comité de Auditoría.

AWS Artifact es el recurso principal para que los clientes obtengan información relacionada con la conformidad de AWS. Proporciona acceso a los informes de seguridad y conformidad de AWS y a determinados contratos en línea. Los informes disponibles en AWS Artifact incluyen: informes de controles de organización y sistemas (SOC) de servicios de AWS, Certificación de conformidad del Sector de pagos con tarjeta (PCI) y certificaciones de los organismos de acreditación en distintas regiones geográficas y sectores verticales de la industria que validan la implementación y la eficacia operativa de los controles de seguridad de AWS. Entre otras cosas, los informes de conformidad se ponen a disposición de los clientes para que puedan evaluar la conformidad de AWS con los controles de seguridad y las obligaciones de cumplimiento asociadas **(Control AWSCA-9.8).**

La estructura organizacional de AWS proporciona un marco para planificar, ejecutar y controlar las operaciones empresariales **(Control AWSCA-1.1).** Los líderes de AWS asignan roles y responsabilidades en función de la estructura organizativa de AWS para garantizar una dotación de personal adecuada, la eficacia de las operaciones y la división de funciones. La dirección también ha establecido la autoridad y las líneas de información adecuadas para el personal clave. La empresa sigue un proceso estructurado de incorporación para ayudar a los nuevos empleados a familiarizarse con las herramientas, procesos, sistemas, políticas y procedimientos de Amazon.

AWS realiza una evaluación formal de la dotación de recursos y personal adecuada para alinear las cualificaciones de los empleados con los objetivos empresariales de la entidad para apoyar la consecución de los objetivos empresariales de la entidad. Durante el proceso de revisión anual del rendimiento, el empleado recibe retroalimentación adecuada sobre los puntos fuertes y las áreas de crecimiento. El administrador del empleado comparte las evaluaciones de fortaleza y crecimiento del empleado con el empleado **(Control AWSCA-9.3).**

Los entornos GovCloud (este de EE. UU.) y GovCloud (oeste de EE. UU.) son regiones de AWS situadas en los Estados Unidos (EE. UU.) que están diseñadas para mantener controles de acceso físicos y lógicos que limitan el acceso del personal de AWS a la red de AWS para las regiones GovCloud (EE. UU.) a los ciudadanos estadounidenses. El entorno de control de AWS que se describe en este documento también es aplicable a las regiones de GovCloud (EE. UU.). El entorno de control de AWS está sujeto a varias evaluaciones de riesgo internas y externas.
AWS estableció un marco de seguridad de la información. Como parte de este marco, AWS revisa y actualiza periódicamente las políticas de seguridad e imparte formación sobre seguridad a sus empleados, que incluye instrucciones sobre clasificación de datos. Además, el equipo de seguridad de las aplicaciones de AWS (AppSec) realiza revisiones de seguridad de sus aplicaciones. Estas revisiones evalúan la disponibilidad, confidencialidad e integridad de los datos, así como la conformidad con las políticas de seguridad. Cuando es necesario, AWS Security aprovecha el marco de seguridad y las políticas de seguridad establecidas y mantenidas por Amazon Corporate Information Security.

AWS cuenta con un proceso para revisar los riesgos medioambientales y geopolíticos antes de lanzar una nueva región **(Control AWSCA-1.10)**. Las evaluaciones de riesgo abarcan la revisión de catástrofes naturales (por ejemplo, fenómenos meteorológicos extremos), tecnológicas (por ejemplo, incendios, radiaciones nucleares, contaminación industrial) y de origen humano (por ejemplo, colisiones de vehículos, actos intencionados, geopolíticos), incluidas las exposiciones que presentan las entidades cercanas; según proceda. Además de las consideraciones específicas de cada sitio, AWS evalúa las situaciones que pueden afectar a las distintas zonas de disponibilidad (AZ) dentro de una región.

A.2 Administración de riesgos

AWS mantiene un programa de administración de riesgos formal para identificar, analizar, gestionar y monitorear de manera continua los riesgos que afectan los objetivos de negocio, los requisitos regulatorios y a los clientes de AWS, e informar sobre tales riesgos. El equipo de administración de riesgos de AWS (ARM) identifica los riesgos, los documenta en un registro de riesgos e informa los resultados a los líderes al menos una vez por semestre. El programa de gestión de riesgos consta de las siguientes fases:

1) Identificar los riesgos

ARM ha desarrollado un enfoque a medida para identificar los riesgos en toda la empresa. El enfoque es:

- Ascendente para identificar las actividades de gestión de riesgos existentes
- Descendente para recoger información de los líderes clave
- Contacto proactivo por parte de los responsables de los riesgos para recopilar información de otros equipos internos, eventos externos y tendencias de la industria.

Cuando corresponde, ARM lleva a cabo interacciones ad hoc con la empresa a raíz de las solicitudes entrantes o de un contacto proactivo por parte del equipo sobre cuestiones específicas.

2) Analizar los riesgos

ARM revisa los riesgos identificados con los líderes séniores para calibrarlos, evaluarlos y priorizarlos. Esto se consigue evaluando:

- Probabilidad (posibilidad de que ocurra en un período definido)
- Impacto (grado de gravedad en términos de clientes, empleados, costos, operaciones, cumplimiento normativo y reglamentario, y reputación)
- Eficacia de la administración de riesgos actual (existencia de prácticas o controles que reducen el riesgo inherente)

3) Tratar los riesgos

ARM adopta el tratamiento de riesgos (en lugar de la mitigación del riesgo) como estrategia y colabora con los expertos en la materia (SME) empresariales para desarrollar planes de respuesta basados en la opción de tratamiento adecuada. Estos podrían incluir:

- Eliminar o evitar el riesgo (por ejemplo, detener la actividad)
- Reducir el riesgo (por ejemplo, aplicar controles)
- Transferir el riesgo (por ejemplo, a un tercero)
- Aceptar el riesgo (cuando hay ganas y capacidad)

4) Monitoreo e informe de riesgos

ARM monitorea activamente los riesgos materiales y sus planes de tratamiento. Se proporcionan informes al liderazgo sénior al menos de forma semestral. Los informes pueden incluir información importante sobre los principales riesgos y tratamientos, así como tendencias emergentes y actualizaciones generales del programa **(Control AWSCA-1.5)**.

Además de la evaluación del riesgo de ARM, la auditoría interna realiza una evaluación del riesgo independiente para identificar y priorizar los riesgos significativos de AWS y utiliza esta información para definir el plan de auditoría. La evaluación del riesgo incorpora información de múltiples fuentes, como los cambios en el negocio, las auditorías internas, los eventos operativos y los riesgos emergentes. El plan de auditoría y los cambios en el plan durante el año se presentan al Comité de auditoría. La auditoría interna también comunica al comité de auditoría los resultados significativos de las auditorías y los planes de acción asociados.

Además, al menos mensualmente, la administración de AWS revisa las métricas operativas de AWS y la corrección de errores (COE) para mejorar la disponibilidad general de los servicios de AWS e identificar áreas de mejora mientras se mitigan los riesgos para los entornos de AWS. Los documentos "COE" se utilizan para realizar un análisis profundo de la causa raíz de determinados incidentes en AWS, documentar las medidas adoptadas y asignar elementos de acción de seguimiento y propietarios para realizar un seguimiento hasta su resolución.

B. Comunicaciones

AWS ha implementado distintos métodos de comunicación interna a nivel global para ayudar a los empleados a comprender sus roles y responsabilidades individuales, y a comunicar eventos importantes de manera oportuna**.** Estos métodos incluyen programas de orientación y formación para los empleados recién contratados; programas de formación anuales adaptados en función de los roles y las responsabilidades de los empleados, que pueden incluir Amazon Security Awareness (ASA) **(Control AWSCA-1.4)**, Software Developer Engineer (SDE) Bootcamp, International Traffic in Arms Regulations (ITAR) Secure Coding Training, la formación Threat Modeling the Right Way for Amazon Builders Fraud/Bribery/Foreign Corrupt Practices, la formación Privacy Engineering Foundations for AWS Service Teams, las formaciones Managing Third Parties Using the Third-Party Risk Management Lifecycle, Export Compliance; reuniones periódicas de administración para obtener información actualizada sobre el rendimiento empresarial y otros asuntos; y medios electrónicos, como videoconferencias, mensajes de correo electrónico y la publicación de información a través de la Intranet de Amazon sobre temas como la notificación de incidentes de seguridad de la información y las directrices que describen la administración del cambio. La Política de privacidad interna de AWS informa a los empleados de AWS y a los proveedores/contratistas aplicables sobre los requisitos de AWS en relación con la privacidad de la información personal del cliente de conformidad con la legislación aplicable y otras obligaciones de AWS.

C. Compromisos de servicio y requisitos del sistema

C.1 Compromisos de servicio

AWS comunica los compromisos de servicio a las entidades usuarias (clientes de AWS) en forma de Acuerdos de nivel de servicio (SLA), acuerdos de cliente (https://aws.amazon.com/agreement/), contratos o a través de la descripción de las ofertas de servicio proporcionadas en línea a través del sitio web de AWS. Puede encontrar más información sobre los Acuerdos de nivel de servicio en https://aws.amazon.com/legal/service-level-agreements/.

AWS también ha implementado diferentes métodos de comunicación externa para respaldar a sus clientes y la comunidad. Existen mecanismos que permiten informar al equipo de AWS Support Escalation y Event Management (E2M) y notificar a los clientes de los posibles problemas operativos que podrían afectar a la experiencia del cliente. El panel de AWS Health está disponible para alertar a los clientes sobre "Eventos de servicios generales", que muestran el estado de todos los servicios de AWS y "Los eventos de su cuenta", que muestran eventos específicos de su cuenta. El cliente puede consultar la información sobre el estado actual en este sitio o aprovechar Amazon EventBridge Integrations o fuentes RSS para recibir notificaciones sobre las interrupciones de cada servicio individual. También se pueden obtener detalles relacionados con la seguridad y el cumplimiento con AWS en los sitios web Centro de seguridad de AWS y Cumplimiento de AWS.

Los clientes pueden ponerse en contacto con AWS a través de la página "Contacte con nosotros" para resolver problemas relacionados con los servicios de AWS. AWS proporciona mecanismos disponibles públicamente para que las partes externas se pongan en contacto con AWS para reportar eventos de seguridad y publica información que incluye una descripción del sistema e información de seguridad y conformidad que aborda los compromisos y responsabilidades de AWS **(Control AWSCA-9.5)**. También puede suscribirse a las ofertas de Premium Support que incluyen comunicación directa con el equipo de atención al cliente y alertas proactivas sobre todo tipo de problema que afecte al cliente. AWS también implementa mecanismos de monitoreo y alarma que configuran los propietarios de los servicios de AWS para identificar y notificar al personal operativo y de gestión acerca de los incidentes cuando se superen límites tempranos de advertencia en las métricas operativas clave (**Control AWSCA-8.1**). Además, los incidentes se registran en un sistema de boletaje, se les asigna una calificación de gravedad y se hace un seguimiento hasta su resolución **(Control AWSCA-8.2)**.

C.2 Requisitos del Sistema

La selección y el uso de los servicios por parte de los clientes de AWS deben establecerse y operarse bajo un modelo de responsabilidad compartida para que la funcionalidad de los servicios y la seguridad asociada se administren adecuadamente. AWS se hace cargo de proteger la infraestructura que ejecuta los servicios que se ofrecen en la nube de AWS. La responsabilidad del cliente viene determinada por los servicios en la nube de AWS que seleccione el cliente y las interdependencias de dichos servicios dentro de la nube de AWS y su propio entorno de red. Los clientes deben evaluar los objetivos de su red de servicios en la nube de AWS e identificar los riesgos y los controles correspondientes que deben implementarse para abordar dichos riesgos al utilizar los servicios de AWS, el software y los controles operativos. Los clientes deben evaluar cuidadosamente los servicios específicos de AWS que eligen, ya que sus responsabilidades de seguridad pueden variar en función del servicio o servicios que seleccionen, así como el tipo de configuración y los controles operativos requeridos para estos servicios.

A la hora de diseñar y desarrollar sus servicios, la gestión de AWS ha creado políticas internas que son relevantes para los servicios y sistemas disponibles para los clientes. El desarrollo de estas políticas y procedimientos ayuda a respaldar la toma de decisiones de la administración y proporciona a los equipos operativos requisitos empresariales claros y orientación para administrar cada servicio y sistema de AWS. Como cada servicio de AWS es único, los requisitos del sistema para utilizar los distintos servicios varían en función del servicio y del entorno de cada cliente.

Como se explica en la sección Disponibilidad del informe, AWS cuenta con procesos e infraestructura a fin de poner los servicios de AWS a disposición de los clientes para satisfacer sus necesidades. AWS comunica a los clientes los requisitos de su sistema y cómo empezar a utilizar los servicios de AWS en forma de guías de usuario, guías para desarrolladores, referencias a la API, tutoriales específicos del servicio o kits de herramientas del SDK. Puede encontrar más información sobre la Documentación de AWS en https://docs.aws.amazon.com/. Estos recursos ayudan a los clientes a diseñar los servicios de AWS para satisfacer sus necesidades empresariales.

AWS identificó los siguientes objetivos para apoyar la seguridad, el cambio y los procesos operativos subyacentes a sus compromisos de servicio y requisitos empresariales. Estos objetivos ayudan a garantizar el funcionamiento del sistema y a mitigar los riesgos que amenazan la consecución de los compromisos

de servicio y los requisitos del sistema. Los objetivos que se indican a continuación proporcionan una garantía razonable de lo siguiente:

- La integridad de los datos se mantiene en todas las fases, incluida la transmisión, el almacenamiento y el procesamiento.
- Existen políticas y mecanismos para restringir adecuadamente el acceso no autorizado a sistemas y datos, y los datos de los clientes están debidamente separados de los de otros clientes.
- Los incidentes del sistema se registran y analizan puntualmente y se hace un seguimiento hasta su resolución.
- Los cambios (incluidos los de emergencia o no rutinarios y los cambios en la configuración) que se les realizan a los recursos de TI existentes se documentan, autorizan, prueban, aprueban e implementan por personal autorizado.
- Los componentes críticos del sistema se replican en varias AZ y se mantienen y supervisan las copias de seguridad autorizadas para garantizar una replicación correcta que permita cumplir los compromisos de servicio.
- Se aplican controles para proteger los datos dentro y fuera de los límites de los entornos que almacenan el contenido de un cliente para cumplir los compromisos de servicio.
- Se establecieron procedimientos para que la recopilación, el uso, la retención, la divulgación y la eliminación del contenido del cliente dentro de los servicios de AWS estén en conformidad con los compromisos de servicio.

D. Procedimientos

D.1 Organización de la seguridad

AWS cuenta con una organización de seguridad de la información establecida, administrada por el equipo de AWS Security y dirigida por el Chief Information Security Officer (CISO) de AWS. Las responsabilidades del equipo de AWS Security se definen y asignan en toda la organización. El equipo de AWS Security trabaja con los equipos de los servicios de AWS, otros equipos de seguridad interna y terceros, que se esfuerzan por garantizar la mitigación de los riesgos de seguridad. AWS Security establece y mantiene políticas y procedimientos para delinear los estándares de acceso lógico en el sistema de AWS y hosts de infraestructura. Las políticas también identifican responsabilidades funcionales para la administración de la seguridad, la privacidad y del acceso lógico. Cuando corresponda, la seguridad de AWS aprovecha el marco y las políticas del sistema de información establecidos y mantenidos por Amazon Corporate Information Security. AWS Security Leadership revisa y aprueba las políticas de AWS y Amazon Corporate Information Security de forma anual, las cuales se utilizan para apoyar a AWS en el cumplimiento de los compromisos de servicio asumidos con el cliente **(Control AWSCA-1.1**, **AWSCA -1.2**, y **AWSCA-1.3)**.

En el marco de esta evaluación anual, se inspeccionaron las siguientes políticas para comprobar que se habían aprobado en el último año:

Política de control de acceso de AWS	Política de protección de medios de AWS
Política de gestión de la configuración de AWS	Política de contraseñas de AWS
Política de planificación de contingencia de AWS	Política de seguridad del personal de AWS
Norma del grupo de permisos críticos de AWS	Política de protección física y medioambiental de AWS
Norma de seguridad del centro de datos: Manejo, Almacenamiento y Destrucción de medios	Política de desarrollo de software seguro
Política de clasificación y manejo de datos de AWS	Norma de evaluación y certificación de la seguridad de AWS
Norma de uso y de gestión de las credenciales de las instalaciones de AWS	Política de formación sobre concienciación de la seguridad informática de AWS
Política de identificación y autenticación de AWS	Política de protección de sistemas y comunicaciones de AWS
Política de respuesta a incidentes de AWS	Política de integridad del sistema y de la información de AWS
Política de gestión de riesgos de seguridad de la información de AWS	Política de mantenimiento del sistema de AWS
Política de privacidad interna de AWS	Política de intercambio de información de terceros de AWS
Política de administración de riesgos de AWS	

AWS cuenta con una política de concienciación y formación en materia de seguridad informática que se difunde a través de un portal de comunicación interno de Amazon a todos los empleados. Esta política aborda el propósito, el alcance, los roles y las responsabilidades. AWS mantiene e imparte anualmente una formación de concientización sobre la seguridad informática a todos los usuarios del sistema de información. La formación también incluye componentes, como la privacidad, la formación en protección de datos y las prácticas principales de tratamiento de datos **(Control AWSCA-1.4)**.

Como parte de sus responsabilidades dentro del modelo de responsabilidad compartida, AWS implementa el modelo de tres líneas de defensa establecido por el Instituto de Auditores Internos (IIA), tratado en el documento técnico del IIA *Three Lines Model* (Modelo de tres líneas) "https://www.theiia.org/en/content/position-papers/2020/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense/". En este modelo, la administración operativa es la primera línea de defensa, las diversas funciones de control de riesgos y supervisión del cumplimiento establecidas por la administración son la segunda línea de defensa **(Control AWSCA-1.5)** y la garantía independiente es la tercera. Como tercera línea de defensa, Amazon cuenta con una función de auditoría interna para evaluar periódicamente los riesgos y evaluar la conformidad con los procesos de seguridad de AWS con debido cuidado profesional **(Control AWSCA-9.8)**.

Además, AWS Security Assurance trabaja con evaluadores externos para obtener una evaluación independiente de los contenidos/procesos de gestión de riesgos mediante la realización de evaluaciones periódicas de seguridad y auditorías o exámenes de conformidad (por ejemplo, SOC, FedRAMP, ISO, PCI) para evaluar la seguridad, integridad, confidencialidad y disponibilidad de la información y los recursos. La administración de AWS también colabora con Auditoría Interna para determinar el estado del entorno de control de AWS y aprovecha esta información para presentar de forma justa las afirmaciones realizadas en los informes.

D.2 Seguridad lógica

AWS ha establecido políticas y procedimientos para delinear las normas de acceso lógico a los sistemas y hosts de infraestructura de AWS. Las políticas también identifican responsabilidades funcionales para la administración de la seguridad y del acceso lógico. Cuando la ley lo permita, AWS exige que los empleados se sometan, en el momento de la contratación, a una investigación de antecedentes proporcional a su puesto y nivel de acceso y de acuerdo con la Política de Seguridad del Personal de AWS **(Control AWSCA-9.2)**.

Los empleados de AWS que tengan acceso a sistemas que podrían afectar la confidencialidad, la integridad, la disponibilidad o la privacidad del contenido de los clientes están obligados a completar una investigación de antecedentes posterior a la contratación en el plazo de un año desde su última comprobación de antecedentes. La investigación posterior a la contratación incluye requisitos de investigación de antecedentes penales coherentes con la investigación de antecedentes previa a la contratación. El acceso a los sistemas que podría afectar a la confidencialidad, integridad, disponibilidad o privacidad del contenido de los clientes se administra mediante la pertenencia a grupos de permisos. Los empleados que prestan soporte a los servicios internos o tienen acceso a los recursos de la red no están obligados a completar la investigación de antecedentes posterior a la contratación. La investigación de antecedentes posterior a la contratación se lleva a cabo cuando la ley local lo permite y de acuerdo con la Política de Seguridad del Personal de AWS **(Control AWSCA-9.9)**.

Aprovisionamiento de cuentas

La responsabilidad de proporcionar acceso a los usuarios, que incluye el acceso de los empleados y contratistas, es compartida por Recursos Humanos (RR. HH.), Operaciones Corporativas y Propietarios de Servicios.

Una cuenta estándar de empleado o contratista con privilegios mínimos se suministra en estado deshabilitado cuando un gerente de contratación envía su solicitud de incorporación de un nuevo empleado o contratista en el sistema de RR. HH. de Amazon. La cuenta se habilita automáticamente tras la activación del registro del empleado en el sistema de RR. HH. de Amazon. Las contraseñas nuevas se establecen con un valor único y deben cambiarse durante el primer uso **(Control AWSCA-2.1)**.

Gestión del acceso

AWS emplea el concepto de privilegio mínimo, lo que permite solo el acceso necesario para que los usuarios realicen su función de trabajo. Las cuentas de usuario se crean para tener un acceso mínimo. El acceso por encima de estos privilegios mínimos requiere una autorización adecuada y por separado.

El propietario o administrador correspondiente aprueba el acceso a los recursos, incluidos los servicios, los hosts, los dispositivos de redes y los grupos de Windows y UNIX en el sistema de administración de permisos de propiedad exclusiva de Amazon. Las solicitudes de cambios en el acceso se capturan en el registro de auditoría de la herramienta de administración de permisos de Amazon. Cuando se produce un cambio en la función laboral de un empleado, se debe aprobar el acceso continuo al recurso; de lo contrario, dicho acceso se revocará automáticamente **(Control AWSCA-2.2).**

Revisión de acceso periódico

Las listas de control de acceso o los grupos de permisos que conceden acceso a las infraestructuras críticas se revisan periódicamente para comprobar su idoneidad. Trimestralmente, el personal de administración de AWS correspondiente revisa el acceso de los usuarios a los sistemas de AWS que respaldan la infraestructura y la red; se requiere una reaprobación explícita o se revoca el acceso al recurso. Semestralmente, AWS revisa el acceso a las cuentas de AWS. Cuando un usuario interno deja de tener una necesidad comercial que requiere acceder al sistema de gestión operativa, se revocan los privilegios del usuario y el acceso a los sistemas pertinentes (**Control AWSCA-2.3**).

Eliminación del acceso

El acceso se revoca de manera automática cuando se termina el registro de un empleado en el sistema de Recursos Humanos de Amazon. Se desactivan las cuentas de Windows y UNIX. Además, el sistema de gestión de permisos de Amazon elimina al usuario de todos los sistemas **(Control AWSCA-2.4)**.

Política de contraseñas

El acceso y la administración de la seguridad lógica de Amazon se basan en los ID de usuario, las contraseñas y Kerberos para autenticar a los usuarios en los servicios, recursos y dispositivos, así como para autorizar el nivel de acceso adecuado para el usuario. La seguridad de AWS ha establecido una política de contraseñas con las configuraciones y los intervalos de caducidad necesarios. AWS cuenta con un proceso de monitoreo y respuesta de credenciales para controlar las credenciales comprometidas de los empleados de Amazon. Las credenciales de los usuarios afectados se identifican, rastrean y rotan oportunamente **(Control AWSCA-2.5).**

Acceso remoto

AWS requiere una autenticación de dos factores a través de un canal criptográfico aprobado para la autenticación en la red interna de AWS desde ubicaciones remotas **(Control AWSCA-2.6).**

Las API permiten a los clientes seleccionar quién tiene acceso a los servicios y recursos de AWS (si los permisos a nivel de recursos son aplicables al servicio) que poseen. AWS impide que los clientes accedan a los recursos de AWS que no tienen asignados mediante permisos de acceso. El contenido de los usuarios está segregado por el software del servicio. El contenido solo se devuelve a las personas autorizadas a acceder al servicio o recurso de AWS especificado (si los permisos a nivel de recurso son aplicables al servicio) **(Control AWSCA-3.5)**.

AWS realiza revisiones de la seguridad de las aplicaciones (AppSec) cuando es necesario para los productos y servicios lanzados externamente y las adiciones de características significativas antes del lanzamiento para identificar riesgos de seguridad y privacidad y determinar si están mitigados. Como parte de la revisión de AppSec, el equipo de Application Security recopila información detallada necesaria para la revisión. El equipo de Application Security realiza un seguimiento de las revisiones con respecto a un inventario gestionado de forma independiente de los productos y las funciones que se van a lanzar para garantizar que ninguno se lance inadvertidamente antes de una revisión completa. Como parte de la revisión de seguridad, también se revisan las políticas de IAM recién creadas o modificadas que permiten a los usuarios finales interactuar con las actualizaciones lanzadas. A continuación, el equipo de Application Security determina la granularidad de la revisión necesaria en función del diseño, el modelo de amenazas y el impacto en el perfil de riesgo de AWS. Durante este proceso, trabajan con el equipo de servicio para identificar, priorizar y solucionar los problemas de seguridad. El equipo de Application Security proporciona su aprobación final para el lanzamiento solo después de completar la revisión **(Control AWSCA-3.6)**. Se realizan pruebas de penetración según sea necesario.

Seguridad de la red de AWS

La red de AWS está conformada por las instalaciones de los centros de datos internos, los servidores, los equipos de red y los sistemas de software de host que están bajo el control de AWS y que se utilizan para prestar los servicios de AWS.

La red de AWS ofrece una importante protección contra los problemas tradicionales de seguridad de la red. A continuación, se muestran algunos ejemplos:

- **Ataques de denegación de servicio distribuidos (DDoS).** Los puntos de conexión de la API de AWS están alojados en una gran infraestructura a escala de Internet y utilizan técnicas propias de mitigación de DDoS. Además, las redes de AWS son multiproveedor a través de varios proveedores para lograr la diversidad de acceso a Internet (**Control AWSCA-8.1**).
- **Ataques de intermediario (MITM).** Todas las API de AWS están disponibles a través de puntos de conexión protegidos por TLS/SSL, que proporcionan autenticación del servidor. Las imágenes de máquina de Amazon (AMI) de Amazon EC2 generan automáticamente nuevos certificados de host SSH en el primer arranque y los registran en la consola de la instancia. Así, los clientes pueden utilizar las API seguras para llamar a la consola y acceder a los certificados del host antes de iniciar la sesión en la instancia por primera vez. Los clientes pueden utilizar TLS/SSL para todas sus interacciones con AWS **(Control AWSCA-3.11).**
- ***Spoofing* de IP.** La infraestructura de cortafuegos (*firewall*) basada en el *host* y controlada por AWS no permitirá que una instancia envíe tráfico con una dirección IP o MAC de origen que no sea la suya **(Control AWSCA-3.10)**.
- **Escaneo de puertos.** Los análisis de puertos no autorizados por parte de los clientes de Amazon EC2 constituyen una infracción de la Política de uso aceptable de AWS. Las infracciones de la Política de uso aceptable de AWS se toman en serio y se investigan todas las que se denuncian. Los clientes pueden denunciar las sospechas de abuso a través de los contactos disponibles en nuestra página web: https://aws.amazon.com/contact-us/report-abuse/. Los escaneos de puertos de las instancias de Amazon EC2 suelen ser ineficaces porque, por defecto, todos los puertos de entrada de las instancias de Amazon EC2 están cerrados y solo el cliente puede abrirlas. La gestión estricta de los grupos de seguridad por parte de los clientes puede mitigar aún más la amenaza de los análisis de puertos. Los clientes pueden pedir permiso para llevar a cabo análisis de vulnerabilidad según sea necesario para cumplir con los requisitos de cumplimiento específicos. Estos escaneos deben limitarse a las instancias propias de los clientes y no deben infringir la Política de Uso Aceptable de AWS. La aprobación anticipada de este tipo de análisis puede iniciarse presentando una solicitud a través del sitio web de AWS en: https://aws.amazon.com/security/penetration-testing/.
- **Captura de paquetes a través de la escucha de la red por parte de otros usuarios.** Las instancias virtuales están diseñadas para evitar que otras instancias que se ejecutan en modo promiscuo reciban o que capturen el tráfico que está destinado a una instancia virtual diferente a través de la escucha de la red. Aunque los clientes pueden poner las instancias en modo promiscuo, el hipervisor no les entregará ningún tráfico que no esté dirigido a ellas. Incluso dos instancias virtuales del mismo cliente ubicadas en el mismo *host* físico no pueden escuchar el tráfico de la otra. Aunque Amazon EC2 ofrece protección contra el intento inadvertido o malicioso de un cliente de ver los datos de otro, los clientes pueden cifrar el tráfico confidencial como práctica estándar **(Control AWSCA-3.10).**

- ***Software* antivirus instalado en las estaciones de trabajo.** El software antivirus se implementa y ejecuta en las estaciones de trabajo corporativas de Amazon. Los equipos de Client Engineering y Enterprise Engineering implementan software antivirus en la generación de imágenes de las estaciones de trabajo corporativas de Amazon. AWS implementó comprobaciones para garantizar que el software antivirus esté instalado, se ejecute y pueda poner en cuarentena cualquier estación de trabajo que no cumpla con las normas. Esta funcionalidad de cuarentena aísla esas estaciones de trabajo de la red hasta que se hayan realizado las acciones de remediación necesarias **(Control AWSCA-3.18)**.

Los dispositivos de firewall están configurados para limitar el acceso a las redes de producción **(Control AWSCA-3.1).** Las configuraciones de estas políticas de firewall se mantienen a través de un push automático desde un servidor principal **(Control AWSCA-3.2).** El personal de administración correspondiente de AWS revisa y aprueba todos los cambios en las políticas del firewall **(Control AWSCA-3.3).**

Con regularidad, AWS Security realiza análisis de vulnerabilidad en los sistemas operativos del host, las aplicaciones web y las bases de datos en el entorno de AWS con una variedad de herramientas **(Control AWSCA-3.4).** Los equipos de Seguridad de AWS también se suscriben a fuentes de noticias para detectar errores aplicables de proveedores y monitorean de manera proactiva los sitios web de los proveedores y otros medios relevantes en busca de nuevos parches. Los clientes de AWS tienen la posibilidad de informar los problemas a AWS a través del sitio web Informes de vulnerabilidad de AWS en: https://aws.amazon.com/security/vulnerability-reporting/.
AWS emplea técnicas de virtualización que incluyen dispositivos de red virtuales y cortafuegos (*firewall*) basados en el *host*, que controlan las restricciones del flujo de tráfico mediante listas de control de acceso (ACL) en EC2 y VPC, y como instancias de EC2 que presentan una variedad de sistemas operativos. Es responsabilidad de los clientes configurar adecuadamente los recursos del servidor dentro de la VPC del cliente.

Control de acceso externo

Los clientes pueden configurar el acceso externo a los servicios a través de AWS Identity and Access Management (IAM). IAM permite a los clientes controlar de forma segura el acceso de sus usuarios a los servicios y recursos de AWS. Mediante IAM, los clientes pueden crear y administrar usuarios, roles y grupos de AWS y crear y adjuntar políticas a esas entidades con permisos granulares que permiten o deniegan el acceso a los recursos de AWS. Los grupos de seguridad actúan como dispositivos de firewall y también pueden utilizarse para controlar el acceso a algunas aplicaciones del alcance, como VPC, EFS, ElastiCache y DMS. Estos grupos de seguridad establecen el modo de acceso “denegar todos” como valor predeterminado, por lo que los clientes deben autorizar específicamente la conectividad de la red. Esto puede lograrse autorizando un rango de IP de red o un Grupo de Seguridad existente **(Control AWSCA-3.5)**.

Interactuar con el servicio

AWS ofrece varios métodos para interactuar con sus servicios en forma de API, kits de desarrollo de software (SDK), la consola de administración de AWS y la interfaz de la línea de comandos de AWS. Todos los métodos dependen, en última instancia, de las API públicas y siguen las prácticas estándar de autenticación y autorización de AWS.

Las llamadas autenticadas a los servicios de AWS están firmadas por un certificado X.509 o la clave de acceso secreta de AWS del cliente. Cuando se utiliza la interfaz de la línea de comandos de AWS (AWS CLI) o uno de los SDK de AWS para realizar solicitudes a AWS, estas herramientas firman automáticamente las

solicitudes con la clave de acceso especificada por el cliente cuando se configuraron las herramientas. Las solicitudes creadas manualmente deben firmarse con la versión 4 o la versión 2 de Signature. Todos los servicios de AWS admiten la versión 4 de Signature, excepto Amazon SimpleDB, que requiere la versión 2 de Signature. Para los servicios de AWS que admiten ambas versiones, se recomienda utilizar la versión 4 de Signature.

Registro interno

AWS mantiene repositorios centralizados que proporcionan la funcionalidad principal de archivo de registros disponible para el uso interno de los equipos de servicio de AWS. El aprovechamiento de S3 para una alta escalabilidad, durabilidad y disponibilidad permite a los equipos de servicio recopilar, archivar y ver los registros de servicio en un servicio de registro central.

Los hosts de producción en AWS se implementan a través de imágenes de referencia maestra **(Control AWSCA-9.4)**. Las imágenes de referencia se equipan con un conjunto estándar de configuraciones y funciones que incluyen registro y monitoreo por razones de seguridad.

Estos registros se almacenan y son accesibles para los equipos de AWS Security para el análisis de la causa raíz en caso de un supuesto incidente de seguridad. Los registros para un *host* determinado también están disponibles para el equipo que posee ese *host* en caso de que el equipo necesite buscar sus registros para análisis operacional y de seguridad.

Cifrado

La política criptográfica de Amazon define la implementación criptográfica adecuada a través de la norma de criptografía de Amazon. La norma de criptografía se basa en las normas FIPS, las normas NIST o el conjunto de algoritmos de seguridad nacional comercial (conjunto B). Los equipos de servicio reciben orientaciones sobre la aplicación, incluida la longitud adecuada de la clave y los parámetros específicos del algoritmo para el cifrado, a través de las revisiones de seguridad de la aplicación. Además, los AWS Security Engineers, dentro del programa de revisión de criptografía, revisan el uso apropiado de la criptografía dentro de AWS. Además, las llamadas a la API se pueden cifrar con TLS/SSL a fin de mantener la confidencialidad. Es responsabilidad del cliente configurar y administrar adecuadamente el uso y la implementación de las opciones de cifrado disponibles para cumplir con los requisitos de conformidad.

Cada versión de firmware de producción del módulo de seguridad de hardware (HSM) de AWS Key Management Service se ha validado con el NIST según el estándar de nivel 3 del FIPS 140-2 más reciente, o está en proceso de certificarse conforme a dicho estándar **(Control AWSCA-4.14)**. El equipo de AWS KMS trabaja junto con un laboratorio asesor de FIPS certificado con el Programa voluntario nacional de acreditación de laboratorios (NVLAP) (por ejemplo: Acumen), el cual, a su vez, trabaja con el NIST para obtener las nuevas versiones de firmware del HSM certificadas. Cada versión nueva de firmware que se implementa en producción se ha enviado al laboratorio para su validación y, luego de validarse, se enviará al Programa de Validación de Módulos Criptográficos (CMVP) del NIST a fin de solicitar la revisión y certificación del estándar FIPS 140-3.

Eliminación del contenido creado por los clientes

AWS permite que los clientes eliminen el contenido creado. Una vez que se eliminan los datos con éxito, estos se vuelven ilegibles **(Control AWSCA-7.7).** En los servicios con almacenamiento efímero, como EC2, esta característica ya no está disponible tras eliminar la instancia de EC2.

D.3 Descripciones del servicio de AWS

Amazon API Gateway

Amazon API Gateway es un servicio que facilita a los desarrolladores la publicación, el mantenimiento, el monitoreo y la protección de las API a cualquier escala. Con él, se puede crear una API personalizada para el código que se ejecuta en AWS Lambda y, luego, solicitar el código Lambda desde la API de los clientes. Amazon API Gateway puede ejecutar un código AWS Lambda en la cuenta de los clientes, iniciar las máquinas de estado AWS Step Functions o realizar llamadas a AWS Elastic Beanstalk, Amazon EC2 o servicios web ajenos a AWS con puntos de conexión HTTP de acceso público. Mediante la consola Amazon API Gateway, los clientes pueden definir las API de REST y los recursos y métodos asociados, administrar el ciclo de vida de las API, generar los SDK y visualizar las métricas para las API.

Amazon AppFlow

Amazon AppFlow es un servicio de integración que habilita a los clientes transferir datos de forma segura entre aplicaciones de software como servicio (SaaS, Software-as-a-Service) como Salesforce, SAP, Zendesk, Slack y ServiceNow, y servicios de AWS como Amazon S3 y Amazon Redshift. Con AppFlow, los clientes pueden ejecutar flujos de datos a escala empresarial con la frecuencia que elijan: de forma programada, en respuesta a un evento empresarial o bajo demanda. Los clientes pueden configurar las capacidades de transformación de datos, como el filtrado y la validación, con el fin de generar datos de calidad listos para usar como parte del propio flujo, sin necesidad de pasos adicionales.

Controlador de recuperación de aplicaciones de Amazon (en vigor desde el 15 de agosto de 2024)

El Controlador de recuperación de aplicaciones de Amazon ofrece información sobre si las aplicaciones y los recursos de los clientes están listos para la recuperación. El Controlador de recuperación de aplicaciones también ayuda a administrar y coordinar la recuperación de las aplicaciones de los clientes en todas las regiones y zonas de disponibilidad (AZ) de AWS. Estas capacidades simplifican y hacen más fiable la recuperación de aplicaciones al reducir los pasos manuales que requieren las herramientas y los procesos tradicionales.

Amazon AppStream 2.0

Amazon AppStream 2.0 es un servicio de streaming que brinda a los clientes un acceso inmediato y desde cualquier parte a sus aplicaciones de escritorio. Además, agiliza la gestión, mejora la seguridad y reduce los costos, ya que permite subir a la nube de AWS las aplicaciones de los clientes desde los dispositivos físicos de los usuarios. El protocolo de streaming de Amazon AppStream 2.0 brinda a los clientes un rendimiento eficaz y fluido que es casi idéntico al de una aplicación nativa. Gracias a Amazon AppStream 2.0, los clientes pueden cumplir con un gran número de requisitos de almacenamiento y de cómputo exigido por sus aplicaciones.

Amazon Athena

Amazon Athena es un servicio de consultas interactivo que facilita el análisis de datos en Amazon S3 con SQL estándar. Dado que es sin servidor, los clientes no deben administrar ninguna infraestructura. Athena tiene una alta disponibilidad y ejecuta las consultas mediante recursos informáticos en diversos servicios y dispositivos de cada instalación. Además, emplea Amazon S3 como sistema de almacenamiento de datos principal, por lo que toda la información de los clientes cuenta con una gran disponibilidad y permanencia.

Amazon Augmented AI (excluye al personal público y al personal del proveedor para todas las características)

Amazon Augmented AI (A2I) es un servicio de machine learning que facilita la creación de los flujos de trabajo necesarios para la revisión humana. Amazon A2I acerca la revisión humana a todos los desarrolladores, ya que elimina las tareas complicadas e indiferenciadas relacionadas con la creación de sistemas de revisión humana o la administración de un gran número de profesionales en tal área (al margen de que funcione o no con AWS). Tanto el personal público como los proveedores de este servicio son opciones que no están contempladas en el presente informe.

Amazon Bedrock

Amazon Bedrock es un servicio totalmente administrado que permite que los modelos fundacionales (FM) de Amazon y las principales empresas de inteligencia artificial (IA) estén disponibles a través de una API, de modo que los clientes pueden elegir entre varios FM para encontrar el modelo que mejor se adapte a su caso de uso. Con la experiencia sin servidor de Amazon Bedrock, los clientes pueden comenzar rápidamente, experimentar de manera sencilla con FM, personalizar los FM de forma privada con sus propios datos, e integrarlos y desplegarlos sin problemas en las aplicaciones de los clientes con las herramientas y capacidades de AWS. Los agentes para Amazon Bedrock están totalmente administrados y facilitan a los desarrolladores la creación de aplicaciones de IA generativa que pueden ofrecer respuestas actualizadas que se basan en fuentes de conocimiento patentadas y completar tareas para una amplia gama de casos de uso. Los modelos fundacionales (FM) de Amazon y de las empresas de IA líderes, disponibles a través de Amazon Bedrock, no se incluyen en el diseño de los controles descritos en este informe de SOC.

Amazon Braket

Amazon Braket, el servicio de computación cuántica de AWS, está diseñado para ayudar a acelerar la investigación científica y el desarrollo de software para la computación cuántica. Amazon Braket proporciona todo lo que los clientes necesitan para crear, probar y ejecutar programas cuánticos en AWS, incluido el acceso a diferentes tipos de computadoras cuánticas y simuladores de circuitos clásicos, y un entorno de desarrollo unificado para crear y ejecutar circuitos cuánticos. Amazon Braket también gestiona la infraestructura clásica necesaria para la ejecución de algoritmos híbridos cuántico-clásicos. Cuando los clientes deciden interactuar con computadoras cuánticas proporcionadas por terceros, Amazon Braket anonimiza el contenido, de modo que solo se envía al proveedor de hardware cuántico el contenido necesario para procesar la tarea cuántica. No se comparte información de la cuenta de AWS y los datos de los clientes no se almacenan fuera de AWS.

Amazon Chime

Amazon Chime es un servicio de comunicación que permite a los clientes reunirse, chatear y realizar llamadas de negocios dentro y fuera de las organizaciones; todo esto gracias a una sola aplicación. Con Amazon Chime, los clientes pueden organizar y asistir a reuniones en línea con video HD, audio, pantalla compartida, chat para reuniones, números de acceso telefónico y soporte para videoconferencias en la sala. El cliente puede utilizar el chat y las salas de chat para mantener una comunicación constante a través de dispositivos móviles y de escritorio. Los clientes también pueden administrar usuarios empresariales, gestionar políticas y configurar SSO u otras características avanzadas en cuestión de minutos mediante la consola de administración de Amazon Chime.

Amazon Chime SDK

Amazon Chime SDK es un conjunto de componentes de comunicación en tiempo real que los clientes pueden utilizar para agregar rápidamente funciones de mensajería, audio, video y pantalla compartida a sus aplicaciones web o móviles. Los clientes pueden utilizar Amazon Chime SDK para crear aplicaciones multimedia en tiempo real que puedan enviar y recibir audio y video, y permitan compartir contenido. Amazon Chime SDK funciona independientemente de cualquier cuenta de administrador de Amazon Chime y no afecta a las reuniones alojadas en Amazon Chime.

Amazon Cloud Directory

Con Amazon Cloud Directory, los clientes pueden crear directorios flexibles y nativos en la nube para organizar la jerarquía de los datos en varias dimensiones. Estos directorios pueden ser útiles en una variedad de casos de uso, como organigramas, catálogos de cursos y registros de dispositivos. Por ejemplo, los clientes pueden crear un organigrama dirigido a distintas jerarquías para informar la estructura, la ubicación y el centro de costos.

Amazon CloudFront (excluye la entrega de contenido a través del punto de presencias integrado de Amazon CloudFront)

Amazon CloudFront es un servicio web rápido de red de entrega de contenido (CDN) que distribuye de forma segura datos, videos, aplicaciones y API a clientes de todo el mundo con baja latencia y gran velocidad de transferencia. CloudFront ofrece la capacidad en materia de seguridad más avanzada, como codificación a nivel de campo y soporte HTTPS integrado a la perfección con AWS Shield, AWS Web Application Firewall y Route 53 como protección contra varios tipos de ataques, entre ellos, ataques DDoS a la red y a la capa de aplicación. Estos servicios residen en ubicaciones periféricas de redes (de escala global y conectadas a través de la red troncal de AWS) y brindan a los usuarios una experiencia más segura, eficiente y libre.

CloudFront distribuye contenido de los clientes gracias a una red global de ubicaciones periféricas. Al solicitar contenido compartido por cualquier cliente en CloudFront, se redirecciona al usuario final a la ubicación periférica que proporciona la latencia más baja para que se distribuya el contenido con el mejor rendimiento posible. Si el contenido ya es parte de tal ubicación periférica, CloudFront lo distribuye de inmediato.

Amazon CloudWatch

Amazon CloudWatch es un servicio de monitoreo y gestión para desarrolladores, operadores del sistema, site reliability engineers (SRE, ingenieros de fiabilidad de sitio) y IT managers. CloudWatch proporciona a los clientes datos e información práctica para monitorear aplicaciones, comprender y responder a los cambios en el rendimiento de todo el sistema, optimizar la utilización de recursos y obtener una visión unificada del estado operativo. CloudWatch recopila datos operativos y de monitoreo en forma de registros, métricas y eventos, lo que les ofrece a los clientes una visión unificada de los recursos, las aplicaciones y los servicios que se ejecutan en AWS y en los servidores en las instalaciones.

Amazon CloudWatch Logs

Amazon CloudWatch Logs es un servicio que sirve para monitorear y almacenar archivos de registro y acceder a estos desde instancias de Amazon Elastic Compute Cloud (EC2), AWS CloudTrail, Route 53 y otras fuentes. CloudWatch Logs permite a los clientes centralizar los registros de los sistemas, las aplicaciones y los servicios de AWS utilizados en un solo servicio altamente escalable. Los clientes pueden verlos fácilmente, buscarlos según patrones, filtrarlos según campos específicos o archivarlos de manera segura para futuros análisis. Los registros de CloudWatch permiten a los clientes visualizar registros, independientemente de la fuente, como un flujo de eventos único, uniforme y con un orden cronológico, como así también consultarlos en función de criterios específicos.

Amazon CodeWhisperer (obsoleto el 15 de agosto de 2024)

Amazon CodeWhisperer es una herramienta de productividad que genera sugerencias de código en tiempo real, de una sola línea o con funciones completas, en el entorno de desarrollo integrado (IDE) de los clientes y en la línea de comandos para ayudar a crear software de forma rápida. Los clientes pueden aceptar rápida y fácilmente la sugerencia principal, ver más sugerencias o continuar escribiendo su propio código.

Amazon Cognito

Amazon Cognito permite a los clientes y usuarios registrarse, iniciar sesión y administrar permisos para las aplicaciones móviles y web. Los clientes pueden crear su propio directorio de usuario dentro de Amazon Cognito. Los clientes también pueden elegir autenticar a los usuarios a través de proveedores de identidad social como Facebook, Twitter o Amazon, con soluciones de identidad SAML o mediante el uso del propio sistema de identidad de los clientes. Además, Amazon Cognito permite a los usuarios guardar datos de forma local en los dispositivos de los usuarios, lo que hace posible que las aplicaciones de los clientes funcionen inclusive cuando están sin conexión. En consecuencia, los clientes pueden sincronizar datos en todos los dispositivos de los usuarios, para que su experiencia de la aplicación no sufra alteraciones, independientemente del dispositivo que utilicen.

Amazon Comprehend

Amazon Comprehend es un servicio de procesamiento de lenguaje natural (NLP) que utiliza el machine learning para buscar información y relaciones en los textos. Amazon Comprehend emplea machine learning para ayudar a los clientes a revelar información y relaciones en sus datos no estructurados sin la experiencia de machine learning. El servicio identifica el idioma del texto; extrae frases clave, lugares, personas, marcas o eventos; entiende si el texto es positivo o negativo y lo analiza mediante tokenización y partes del habla; y organiza de forma automática una colección de archivos de texto por tema.

Amazon Comprehend Medical

Amazon Comprehend Medical es un servicio de procesamiento de lenguaje natural (NLP) que facilita el uso de machine learning para extraer información médica pertinente de texto no estructurado. A través de Amazon Comprehend Medical, los clientes pueden recolectar datos críticos (como enfermedades médicas, medicamentos, dosis, potencia y frecuencia) con rapidez y precisión de una serie de fuentes, como notas de los médicos, informes de ensayos clínicos e historiales clínicos de pacientes. Amazon Comprehend Medical emplea modelos de machine learning avanzados para identificar con precisión y rapidez información médica, como afecciones médicas y medicamentos, y determinar su interrelación, por ejemplo, la dosis y la concentración de un medicamento.

Amazon Connect

Amazon Connect es una solución omnicanal unificada creada para ofrecer experiencias personalizadas, eficientes y proactivas a través de los canales preferidos de los clientes. El cliente puede asegurarse de que los problemas de los usuarios se resuelven rápidamente y, si se necesitan varios contactos, puede mantener el contexto de manera fluida a medida que cambian las necesidades del cliente. Amazon Connect también ayuda a los clientes a interactuar proactivamente con sus usuarios a gran escala mediante información relevante, como recordatorios de citas, recomendaciones de productos y promociones de marketing.

Amazon Data Firehose

Amazon Data Firehose es un medio confiable para cargar los datos de streaming en almacenes de datos y herramientas de análisis. Permite capturar, transformar y cargar datos de streaming en Amazon S3, Amazon Redshift y Amazon OpenSearch Service, lo que permite un análisis casi en tiempo real con los paneles y las herramientas de inteligencia empresarial que ya están en uso. El servicio escala de forma automática para ajustarse al rendimiento de los datos de los clientes y no requiere administración continua. También permite lotear, comprimir, transformar y cifrar los datos antes de cargarlos, con lo que se minimiza la cantidad de almacenamiento requerida en el destino y se aumenta la seguridad.

Amazon DataZone (en vigor a partir del 15 de febrero de 2024)

Amazon DataZone es un servicio de administración de datos que agiliza y facilita a los clientes la catalogación, el descubrimiento, el uso compartido y la gobernanza de los datos almacenados en AWS, en las instalaciones y en fuentes de terceros. Con Amazon DataZone, los ingenieros, los científicos de datos, los administradores de productos, los analistas y los usuarios empresariales pueden acceder rápidamente a los datos de toda la organización para descubrirlos, utilizarlos y colaborar en la obtención de información basada en datos. Los administradores y propietarios de datos que supervisan los activos de datos de una organización pueden administrar y gobernar con facilidad el acceso a los datos. Amazon DataZone proporciona flujos de trabajo integrados para que los consumidores de datos soliciten acceso a estos y para que los propietarios aprueben el acceso.

Amazon Detective

Amazon Detective permite a los clientes analizar, investigar e identificar con facilidad y sin demoras la causa raíz de los potenciales problemas de seguridad o de las actividades sospechosas. Amazon Detective recolecta de forma automática datos de registro de los recursos de AWS y emplea machine learning, análisis estadístico y teoría de grafos para crear un conjunto de datos asociados que les permite a los clientes realizar investigaciones en materia de seguridad con más eficiencia y rapidez. Los servicios de AWS Security sirven para identificar posibles problemas de seguridad o resultados.

Con Amazon Detective, se pueden analizar millones de eventos desde varios orígenes de datos y crear automáticamente una vista unificada e interactiva de los recursos, los usuarios y las interacciones entre estos a lo largo del tiempo. Gracias a esta vista unificada, los clientes pueden visualizar todos los detalles y el contexto en un solo lugar para identificar los motivos subyacentes de los resultados, explorar a fondo las actividades históricas pertinentes y determinar con rapidez la causa principal.

Amazon DevOps Guru

Amazon DevOps Guru es un servicio que funciona con machine learning (ML) que está diseñado para mejorar el rendimiento y la disponibilidad operativas de una aplicación. DevOps Guru permite detectar los comportamientos que no siguen los patrones operativos normales para que los clientes puedan identificar los problemas operativos antes de que los afecten.

DevOps Guru utiliza modelos de ML que cuentan con años de excelencia operativa de Amazon.com y AWS para identificar comportamientos anómalos en las aplicaciones (por ejemplo, más latencia, tasas de errores, recursos limitados, entre otros) y ayuda a descubrir problemas críticos que podrían dar lugar a interrupciones de servicio. Cuando DevOps Guru identifica un problema crítico, envía de manera automática una alerta y brinda un resumen de las anomalías relacionadas, la posible causa raíz y el contexto de cuándo y dónde se produjo el problema. Si es posible, DevOps Guru también ayuda a proporcionar recomendaciones sobre cómo solucionar el problema.

Amazon DocumentDB (con compatibilidad con MongoDB)

Amazon DocumentDB (con compatibilidad con MongoDB) es un servicio de base de datos de documentos escalable, rápido y con alta disponibilidad que admite cargas de trabajo de MongoDB. Amazon DocumentDB está diseñado desde cero para brindar a los clientes el rendimiento, la escalabilidad y la disponibilidad que necesitan para trabajar con cargas de trabajo esenciales de MongoDB a escala. Amazon DocumentDB implementa la API MongoDB 3.6 de código abierto de Apache 2.0 a través de la emulación de las respuestas que espera un cliente de MongoDB desde un servidor de MongoDB, lo que permite a los clientes usar sus controladores y herramientas existentes de MongoDB con Amazon DocumentDB. Amazon DocumentDB utiliza un sistema de almacenamiento distribuido, tolerante a errores y autorreparable que escala verticalmente de forma automática hasta 64 TB por clúster de base de datos.

Amazon DynamoDB

Amazon DynamoDB es un servicio de base de datos NoSQL administrado. Permite a los clientes delegar a AWS las cargas administrativas de operar y escalar bases de datos distribuidas como aprovisionamiento de hardware, ajustes y configuración, replicación, aplicación de parches de software y escalado de clústeres.

Los clientes pueden crear una tabla de base de datos que almacene y recupere datos y abarque el tráfico solicitado. Amazon DynamoDB distribuye automáticamente los datos y el tráfico de la tabla en una cantidad apropiada de servidores con el fin de controlar la capacidad de solicitudes especificada y la cantidad de datos almacenados, al mismo tiempo que mantiene un rendimiento constante y rápido. Todos los elementos de los datos se almacenan en unidades de estado sólido (SSD) y se replican automáticamente en múltiples AZ de una región.

Acelerador de Amazon DynamoDB (DAX) (en vigor a partir del 15 de febrero de 2024)

El acelerador de Amazon DynamoDB (DAX) es un servicio de almacenamiento en caché totalmente administrado y de alta disponibilidad creado para Amazon DynamoDB. El DAX multiplica por 10 el rendimiento, de milisegundos a microsegundos, incluso con millones de solicitudes por segundo. El DAX realiza el trabajo pesado necesario para agregar aceleración en memoria a sus tablas de DynamoDB, sin necesidad de que los desarrolladores administren la invalidación de la caché, la propagación automática de datos o la administración de clústeres.

Amazon EC2 Auto Scaling

Amazon EC2 Auto Scaling ejecuta/cancela las instancias en representación de los clientes según las condiciones que definan (por ejemplo, horarios) al modificar las métricas como el tiempo promedio de CPU o el estado de una instancia de acuerdo con las comprobaciones de estado de ELB o EC2. Además, permite que los cómputos de los clientes estén equilibrados en múltiples AZ y que escalen su flota según la frecuencia de uso.

Amazon Elastic Block Store (EBS)

Amazon Elastic Block Store (EBS) ofrece volúmenes de almacenamiento en bloques persistentes para utilizar con las instancias de Amazon EC2 en la nube de AWS. Cada volumen de Amazon EBS se replica automáticamente dentro de su AZ para proteger a los clientes de los errores de componente. Amazon EBS permite a los clientes crear volúmenes de almacenamiento desde 1 GB hasta 16 TB, que las instancias de Amazon EC2 pueden montar como dispositivos. Los volúmenes de almacenamiento se comportan como dispositivos de bloque sin procesar y sin formato, con nombres de dispositivos proporcionados por el usuario y una interfaz de dispositivos de bloque. Los clientes pueden crear un sistema de archivos sobre los volúmenes de Amazon EBS o utilizarlos de cualquier otra manera en la que utilizaría un dispositivo de bloques (como un disco duro).

Los volúmenes de Amazon EBS se presentan como dispositivos de bloque sin procesar y sin formato cuyo contenido se ha eliminado antes de ponerse a disposición para su uso. El contenido se elimina antes de la reutilización. Si los clientes tienen procedimientos que exigen eliminar todos los datos con un método específico, los clientes pueden aplicar dicho procedimiento antes de borrar el volumen a fin de cumplir con los requisitos del cliente. Amazon EBS incluye Data Lifecycle Manager, que proporciona una manera simple y automatizada para crear copias de respaldo de los datos almacenados en los volúmenes de Amazon EBS.

Amazon Elastic Compute Cloud (EC2)

Amazon Elastic Compute Cloud (EC2) es una oferta de infraestructura como servicio (IaaS) de Amazon, que provee capacidad de computación escalable a través de instancias de servidor en centros de datos de AWS. Amazon EC2 está diseñado para facilitar la informática a escala de la Web al permitirles a los clientes obtener y configurar la capacidad con un nivel mínimo de fricción. Los clientes crean y lanzan instancias, que son máquinas virtuales disponibles en una amplia variedad de configuraciones de hardware y software.

La seguridad dentro de Amazon EC2 se proporciona en varios niveles: el sistema operativo de la capa host, el sistema operativo de la instancia virtual o el sistema operativo huésped, el firewall y las llamadas a la API firmadas. Cada uno de estos elementos se basa en las capacidades de los demás. De esta manera, se ayuda a evitar que los datos contenidos en Amazon EC2 sean interceptados por sistemas o usuarios no autorizados y a proveer seguridad en las mismas instancias de Amazon EC2 sin sacrificar la flexibilidad de la configuración. El servicio Amazon EC2 utiliza un hipervisor que aísla la memoria y la CPU entre las máquinas virtuales; controla el acceso a la red, al almacenamiento y a otros dispositivos, y mantiene un fuerte aislamiento entre las máquinas virtuales huéspedes. De forma regular, los auditores independientes evalúan la seguridad de Amazon EC2 y los equipos de penetración buscan vulnerabilidades y vectores de ataque nuevos y existentes.

AWS evita que los clientes accedan a *hosts* físicos o instancias no asignadas a ellos gracias a la aplicación de filtros con el *software* de virtualización **(Control AWSCA-3.12)**.

Amazon EC2 ofrece una solución de firewall completa denominada grupo de seguridad. Este firewall de entrada obligatorio está configurado de forma predeterminada con un modo de denegación de todo, por lo que los clientes de Amazon EC2 deben abrir de forma explícita los puertos necesarios para permitir el tráfico de entrada **(Control AWSCA-3.9).**

Amazon proporciona la función Time Sync, que permite sincronizar el tiempo de las instancias de EC2 de Linux con el tiempo universal coordinado (UTC, Coordinated Universal Time). Se envía por el Network Time Protocol (NTP) y utiliza una flota de relojes atómicos conectados a satélites redundantes en cada región para proveer una hora de referencia muy precisa a través de la dirección IPv4 local 169.254.169.123 o una dirección IPv6 fd00:ec2::123. Las irregularidades de la velocidad de rotación de la Tierra que causan desviaciones del UTC con respecto al Marco de Referencia Celestial Internacional (ICRF), por un segundo adicional, se llaman segundo intercalar. Para corregir esta desviación de los relojes, Time Sync atenúa los segundos intercalares en un período (proceso denominado corrimiento de los segundos intercalares), lo que facilita el procesamiento de los segundos intercalares en las aplicaciones del cliente. La sincronización del reloj de Amazon EC2 para las regiones de Este de EE. UU. (Norte de Virginia) y Asia-Pacífico (Tokio) se ha mejorado para lograr una precisión dentro de los 100 microsegundos frente a 1 milisegundo para las demás regiones en las instancias de EC2 compatibles. Los tipos de instancias que no admitan esto seguirán teniendo una precisión de 1 milisegundo **(Control AWSCA-7.10).**

<u>Amazon Elastic Container Registry (ECR)</u>
Amazon Elastic Container Registry es un registro de imagen de contenedor Docker que permite a los desarrolladores almacenar, administrar e implementar imágenes de contenedores Docker. Amazon Elastic Container Registry está integrado con Amazon Elastic Container Service (ECS) y Amazon Elastic Kubernetes Service (EKS).

<u>Amazon Elastic Container Service [los dos tipos de lanzamiento Fargate y EC2]</u>
Amazon Elastic Container Service es un servicio de gestión de contenedores escalable y de alto rendimiento que es compatible con contenedores Docker y permite a los clientes ejecutar aplicaciones con facilidad en un clúster administrado de instancias de Amazon EC2. Gracias a Amazon Elastic Container Service, los clientes ya no necesitan instalar, operar y escalar su propia infraestructura de gestión de clústeres. Con simples llamadas a la API, los clientes pueden lanzar y detener aplicaciones compatibles con Docker, consultar el estado completo de los clústeres de los clientes y acceder a muchas características familiares como grupos de seguridad, Elastic Load Balancing, volúmenes de EBS y roles de IAM. Además, pueden emplear Amazon Elastic Container Service para programar la ubicación de contenedores en los clústeres de los clientes según los recursos que necesiten y sus requisitos de disponibilidad.

<u>Amazon Elastic File System (EFS)</u>
Amazon Elastic File System (EFS) provee almacenamiento de archivos para las instancias de Amazon EC2. EFS presenta una interfaz de sistema de archivos adjunta a la red a través del protocolo NFS v4. Los sistemas de archivos EFS crecen y se encogen elásticamente a medida que los usuarios agregan y borran datos. Amazon EFS distribuye los datos en múltiples AZ. De esta manera, si una AZ se vuelve inaccesible, la estructura permite a los clientes seguir accediendo al conjunto completo de sus datos. El cliente es responsable de elegir desde cuáles de sus Virtual Private Clouds (VPC) quiere acceder a un sistema de

archivos, para lo cual crea recursos llamados destinos de montaje. Hay un destino de montaje por cada AZ, que expone una dirección IP y un nombre DNS para montar el sistema de archivos del cliente en las instancias de EC2. A continuación, los clientes registran sus instancias de EC2 y emiten un comando 'mount', que apunta a la dirección IP o al nombre de DNS del destino de montaje. Se asigna al destino de montaje uno o más grupos de seguridad de VPC a los que pertenece. Los grupos de seguridad de VPC definen las reglas sobre qué tráfico de VPC puede alcanzar los destinos de montaje y, a su vez, el sistema de archivos.

Amazon Elastic Kubernetes Service (EKS) (ambos tipos de lanzamiento: Fargate y EC2)

Amazon Elastic Kubernetes Service (EKS) facilita la implementación, la administración y la escalabilidad de aplicaciones con contenedores que emplean Kubernetes en AWS. Amazon EKS ejecuta la infraestructura de administración de Kubernetes para que los clientes eliminen un único punto de error en múltiples AZ de AWS. Amazon EKS tiene un certificado de conformidad con Kubernetes, por lo que los clientes pueden usar herramientas y complementos existentes de los socios y la comunidad de Kubernetes. Las aplicaciones que se ejecutan en cualquier entorno de Kubernetes estándar son totalmente compatibles y se pueden migrar sin dificultades a Amazon EKS.

Amazon Elastic MapReduce (EMR)

Amazon Elastic MapReduce (EMR) es un servicio web que provee clústeres Hadoop administrados en instancias de Amazon EC2 que se ejecutan en el sistema operativo Linux. Amazon EMR utiliza el procesamiento de Hadoop junto con varios productos de AWS para realizar diversas tareas, como la indexación web, la minería de datos, el análisis de archivos de registro, el machine learning, la simulación científica y el almacenamiento de datos. Amazon EMR no solo administra de forma activa los clústeres para los clientes, sino que reemplaza los nodos con errores y ajusta la capacidad según se solicite. Amazon EMR gestiona de forma segura y confiable una amplia gama de casos de uso de macrodatos, como análisis de registros, indexación web, transformaciones de datos (ETL), machine learning, análisis financiero, simulación científica y bioinformática.

Amazon ElastiCache

Amazon ElastiCache automatiza las tareas de gestión en los entornos de caché en memoria, como la gestión de revisiones, la detección de errores y la recuperación. Funciona en conjunto con otros servicios de AWS para proveer una caché en memoria administrada. Por ejemplo, una aplicación que se ejecuta en Amazon EC2 puede acceder de forma segura al clúster de Amazon ElastiCache que se ubica en la misma región con una latencia muy baja.

A través del servicio Amazon ElastiCache, los clientes pueden crear un clúster de caché, es decir, una colección de uno o más nodos de caché en la que cada uno de ellos ejecuta una instancia de Memcached, Redis Engine o DAX Engine. Un nodo de caché es un entorno autónomo que provee una porción de tamaño fijo de RAM segura conectada a la red. Cada nodo de caché ejecuta una instancia de Memcached, Redis Engine o DAX Engine, y tiene nombre de DNS y puerto propios. Se admiten varios tipos de nodos de caché, cada uno de ellos presentan diferentes cantidades de memoria asociada.

Amazon EventBridge

Amazon EventBridge es un servicio que ofrece una transmisión casi en tiempo real de los eventos que describen los cambios en los recursos de AWS. Los clientes pueden configurar reglas de enrutamiento a fin de determinar dónde enviar los datos recopilados para crear arquitecturas de aplicaciones que reaccionen en tiempo real a los orígenes de los datos. Amazon EventBridge detecta cambios operativos

cuando ocurren y responde a estos mediante acciones correctivas si es necesario. Estas medidas consisten en enviar mensajes para responder al entorno, activar funciones, implementar cambios y capturar información del estado.

Amazon FinSpace

Amazon FinSpace es un servicio de gestión y análisis de datos que permite almacenar, catalogar y preparar datos de la industria financiera con más facilidad y a escala. Amazon FinSpace reduce el tiempo que demoran los clientes de la financial services industry (FSI, industria de servicios financieros) en buscar todos los tipos de datos financieros y acceder a estos para el análisis.

Amazon Forecast

Amazon Forecast emplea machine learning para combinar datos de serie temporal con variables adicionales a fin de elaborar pronósticos. Con Amazon Forecast, los clientes pueden importar datos de serie temporal y datos asociados a Amazon Forecast desde la base de datos de Amazon S3. A continuación, Amazon Forecast carga los datos de forma automática, los inspecciona e identifica los atributos claves necesarios para elaborar los pronósticos. Luego, forma y optimiza un modelo personalizado del cliente y lo aloja en un entorno de alta disponibilidad donde se pueda usar para generar pronósticos empresariales.

Amazon Forecast está protegido con cifrado. Todo el contenido que se procesa con Amazon Forecast está cifrado con claves del cliente a través de Amazon Key Management Service y cifrado en reposo en la región de AWS donde el cliente está usando el servicio. Los administradores también pueden controlar el acceso a Amazon Forecast a través de la política de permisos de AWS Identity and Access Management (IAM), lo que garantiza la protección y privacidad de la información confidencial.

Amazon Fraud Detector

Amazon Fraud Detector ayuda a detectar actividades en línea sospechosas, como la creación de cuentas falsas y los fraudes en los pagos en línea. Amazon Fraud Detector utiliza machine learning (ML) y los 20 años de experiencia en la detección de fraudes que poseen AWS y Amazon.com para identificar automáticamente la actividad fraudulenta y atrapar más fraudes con mayor rapidez. Con Amazon Fraud Detector, los clientes pueden crear un modelo de ML para la detección de fraudes con solo un par de clics y usarlo para evaluar las actividades en línea en milisegundos.

Amazon FSx

Amazon FSx provee sistemas de archivos de terceros. Amazon FSx provee a los clientes compatibilidad nativa de sistemas de archivos de terceros con conjuntos de características para cargas de trabajo como almacenamiento basado en Windows, high-performance computing (HPC, computación de alto rendimiento), machine learning y Electronic Design Automation (EDA). Los clientes no deben preocuparse por gestionar los servidores de archivos y el almacenamiento, ya que Amazon FSx automatiza las tareas administrativas que consumen tiempo, como el aprovisionamiento de hardware, la configuración del software, la aplicación de parches y las copias de seguridad. Amazon FSx integra los sistemas de archivos con servicios de AWS nativos en la nube, por lo que se amplía su utilidad para una gran variedad de cargas de trabajo.

Amazon GuardDuty

Amazon GuardDuty es un servicio de detección de amenazas que monitorea de forma continua para encontrar actividad maliciosa y comportamiento no autorizado a fin de proteger las cuentas y las cargas de trabajo de AWS de los CSC. Con la nube, se simplifica la recopilación y el agregado de actividades de red y de cuenta. No obstante, analizar de manera continua los datos de registros de eventos para detectar amenazas potenciales puede requerir mucho tiempo de parte de los equipos de seguridad. Con GuardDuty, los clientes ahora cuentan con una opción rentable e inteligente para realizar detecciones de amenazas continuas en la nube de AWS.

Amazon Inspector

Amazon Inspector es un servicio automatizado de administración de vulnerabilidades que analiza de forma continua las cargas de trabajo de AWS en busca de vulnerabilidades de software y la exposición involuntaria de la red. Amazon Inspector elimina la sobrecarga operativa asociada al despliegue y la configuración de una solución de administración de vulnerabilidades, ya que permite a los clientes desplegar Amazon Inspector en todas las cuentas en un solo paso.

Amazon Inspector Classic

Amazon Inspector Classic es un servicio automatizado de evaluación de seguridad para aquellos clientes que buscan mejorar el nivel de seguridad y cumplimiento de las aplicaciones que se implementan en AWS. Amazon Inspector Classic evalúa de forma automática las aplicaciones en busca de vulnerabilidades y desviaciones en relación con las prácticas recomendadas. Después de realizar una evaluación, Amazon Inspector Classic genera una lista detallada de resultados de seguridad priorizados por nivel de severidad.

Amazon Kendra

Amazon Kendra es un servicio de búsqueda inteligente impulsado por machine learning. Kendra reimagina la manera en que las empresas buscan sitios web y aplicaciones del cliente para que los empleados y clientes puedan hallar contenido con facilidad, incluso cuando se distribuye en varios lugares y repositorios de contenido.

Amazon Keyspaces (para Apache Cassandra)

Amazon Keyspaces (for Apache Cassandra) es un servicio de base de datos compatible con Apache Cassandra, de alta disponibilidad y escalable. Con Amazon Keyspaces, los clientes pueden ejecutar cargas de trabajo de Cassandra en AWS con el mismo código de aplicación de Cassandra y las mismas herramientas para desarrolladores que usan actualmente. Amazon Keyspaces es un servicio sin servidor que ofrece a los clientes las características de rendimiento, elasticidad y empresariales que necesitan para operar a escala cargas de trabajo de Cassandra esenciales para la empresa.

Amazon Kinesis Data Streams

Amazon Kinesis Data Streams es un servicio de streaming de datos en tiempo real duradero y de gran escalabilidad. Kinesis Data Streams puede capturar gigabytes de datos por segundo de forma continua desde cientos de miles de orígenes como las secuencias de clics en sitios web, secuencias de eventos de bases de datos, transacciones financieras, fuentes de redes sociales, registros de TI y eventos de seguimiento y localización. Los datos recopilados están disponibles en milisegundos, lo que habilita casos de uso de análisis en tiempo real como paneles en tiempo real, detección de anomalías en tiempo real, fijación de precios dinámica y mucho más.

Amazon Kinesis Video Streams

Amazon Kinesis Video Streams facilita la transmisión de video segura desde dispositivos conectados a AWS para el análisis, el machine learning (ML), la reproducción y el procesamiento de otros tipos. Aprovisiona de manera automática y escala elásticamente la infraestructura necesaria para capturar datos de video de streaming desde millones de dispositivos. También almacena de forma duradera, cifra e indexa datos de video en las transmisiones y permite a los clientes acceder a sus datos a través de API fáciles de usar. Kinesis Video Streams también les permite reproducir videos para la visualización en vivo y bajo demanda y crear rápidamente aplicaciones que aprovechan la visión artificial y el análisis de video.

Amazon Lex

Amazon Lex es un servicio para crear interfaces conversacionales en cualquier aplicación mediante el uso de voz y texto. Proporciona las funcionalidades avanzadas de aprendizaje profundo de automatic speech recognition (ASR, reconocimiento de voz automático) a fin de convertir la conversación de voz en texto y de natural language understanding (NLU, comprensión del lenguaje natural) a fin de reconocer la intención del texto. De esta manera, los clientes pueden crear aplicaciones con experiencias del usuario muy participativas e interacciones conversacionales similares a las de la vida real. Amazon Lex escala automáticamente para que los clientes no tengan que preocuparse por la administración de la infraestructura.

Amazon Location Service

Amazon Location Service facilita la tarea de los desarrolladores de agregar funcionalidades de ubicación a las aplicaciones sin comprometer la seguridad de los datos y la privacidad del usuario. Con Amazon Location Service, el cliente puede crear aplicaciones que proporcionen mapas y puntos de interés, conviertan las direcciones de las calles en coordenadas geográficas, calculen rutas, hagan un seguimiento de los recursos y activen acciones basadas en la ubicación. Amazon Location Service utiliza datos geoespaciales de alta calidad para proporcionar mapas, lugares, rutas, seguimiento y geoperimetraje.

Amazon Macie

Amazon Macie es un servicio de seguridad y privacidad de datos que emplea machine learning y concordancia de patrones para ayudar a los clientes a descubrir, monitorear y proteger la información confidencial en AWS.

Macie automatiza el descubrimiento de información confidencial, como información de identificación personal (PII) y datos financieros, para proveer a los clientes una mejor comprensión de los datos que almacena la organización en Amazon Simple Storage Service (Amazon S3). También provee a los clientes un inventario de buckets de S3 y los evalúa y monitorea de forma automática para fines de seguridad y control de acceso. En minutos, Macie puede identificar e informar buckets con permisos excesivos o descifrados para la organización.

Si Macie detecta información confidencial u otros posibles problemas en la seguridad o la privacidad del contenido de los clientes, crea resultados en detalle para revisarlos o tomar medidas correctivas según sea necesario. Los clientes pueden revisar y analizar estos resultados directamente en Macie o monitorearlos y procesarlos con otros servicios, aplicaciones y sistemas.

Amazon Managed Grafana

Amazon Managed Grafana es un servicio para Grafana de código abierto, que proporciona visualización interactiva de datos para datos operativos y de monitoreo. Con Amazon Managed Grafana, los clientes pueden visualizar, analizar y crear alarmas sobre sus métricas, registros y rastros recopilados de varios orígenes de datos en su sistema de observabilidad, incluidos AWS, ISV de terceros y otros recursos de su cartera de TI. Amazon Managed Grafana descarga la gestión operativa de Grafana escalando automáticamente la infraestructura informática y de base de datos a medida que aumenta la demanda de uso, con actualizaciones de versión y parches de seguridad automatizados. Amazon Managed Grafana se integra de forma nativa con los servicios de AWS para que los clientes puedan agregar, consultar, visualizar y analizar de forma segura sus datos de AWS en varias cuentas y regiones con tan solo unos clics en la consola de AWS. Amazon Managed Grafana se integra en AWS IAM Identity Center y es compatible con Security Assertion Markup Language (SAML) 2.0, por lo que los clientes pueden configurar el acceso de los usuarios a paneles y orígenes de datos específicos solo para determinados usuarios de su directorio corporativo.

Amazon Managed Service para Apache Flink

Amazon Managed Service para Apache Flink ofrece una manera sencilla a los clientes de analizar los datos de transmisión, obtener información útil y responder a las necesidades de la empresa y de los clientes en tiempo real. Amazon Managed Service para Apache Flink reduce la complejidad que implica crear, administrar e integrar aplicaciones de transmisión en otros servicios de AWS. Los usuarios de SQL pueden consultar datos de streaming o crear aplicaciones de streaming completas con facilidad usando plantillas y un editor de SQL interactivo. Los desarrolladores de Java pueden crear con rapidez aplicaciones de streaming sofisticadas que utilizan bibliotecas Java de código abierto e integraciones de AWS para transformar y analizar datos en tiempo real.

Amazon Managed Service para Prometheus

Amazon Managed Service para Prometheus es un servicio de monitoreo y alerta compatible con Prometheus que facilita el monitoreo de aplicaciones e infraestructuras en contenedores a escala. El proyecto Prometheus de Cloud Native Computing Foundation es una solución de código abierto de monitoreo y alerta optimizada para los entornos de contenedores. Con Amazon Managed Service para Prometheus, los clientes pueden utilizar el lenguaje de consultas de Prometheus (PromQL) de código abierto para monitorear y alertar sobre el rendimiento de las cargas de trabajo en contenedores sin la necesidad de escalar y operar en la infraestructura subyacente. Amazon Managed Service para Prometheus escala de forma automática la ingestión, el almacenamiento, la alerta y la consulta de métricas operativas a medida que las cargas de trabajo aumentan o disminuyen, y está integrado con los servicios de seguridad de AWS para acceder a los datos de forma segura y rápida.

Amazon Managed Streaming para Apache Kafka

Amazon Managed Streaming for Apache Kafka es un servicio que facilita a los clientes la creación y ejecución de aplicaciones que utilizan Apache Kafka para procesar datos de streaming. Apache Kafka es una plataforma de código abierto para crear aplicaciones y canalizaciones de datos de streaming en tiempo real. Con Amazon MSK, los clientes pueden utilizar las API nativas de Apache Kafka para rellenar los lagos de datos, transferir los cambios hacia y desde las bases de datos y hacer funcionar las aplicaciones de análisis y machine learning.

Amazon Managed Workflows para Apache Airflow (Amazon MWAA)

Amazon Managed Workflows para Apache Airflow es un servicio para Apache Airflow que permite a los clientes utilizar su plataforma Apache Airflow actual y conocida para orquestar sus flujos de trabajo. Los clientes obtienen mayor escalabilidad, disponibilidad y seguridad sin la carga operativa que supone la administración de la infraestructura subyacente. Amazon Managed Workflows para Apache Airflow organiza los flujos de trabajo de los clientes mediante grafos acíclicos dirigidos (DAG) escritos en Python. Los clientes proporcionan a Amazon Managed Workflows para Apache Airflow un bucket de Amazon Simple Storage Service (S3) en el que residen los DAG, los complementos y los requisitos de Python del cliente. Luego, los clientes pueden ejecutar y monitorizar sus DAG desde la consola de administración de AWS, una interfaz de línea de comandos (CLI), un kit de desarrollo de software (SDK) o la interfaz de usuario (UI) de Apache Airflow.

Amazon MemoryDB (anteriormente Amazon MemoryDB para Redis)

Amazon MemoryDB es un servicio de base de datos en memoria duradero y compatible con Redis. Está diseñado para las aplicaciones modernas con arquitecturas de microservicios.

Amazon MemoryDB es compatible con Redis, un almacén de datos de código abierto, que permite a los clientes crear aplicaciones de forma rápida mediante las mismas estructuras de datos, API y comandos flexibles de Redis que ya utilizan en la actualidad. Con Amazon MemoryDB, todos los datos de los clientes se almacenan en la memoria, lo que permite al cliente conseguir un alto rendimiento y una latencia de escritura de un solo dígito de milisegundo y de lectura de microsegundo. Amazon MemoryDB también almacena los datos de forma duradera en múltiples AZ mediante un registro de transacciones distribuido que permite mayor velocidad para el reinicio de nodos, la recuperación de bases de datos y la conmutación por error. Al ofrecer tanto rendimiento en memoria como durabilidad Multi-AZ, Amazon MemoryDB puede utilizarse como una base de datos principal de alto rendimiento para aplicaciones de microservicios, lo que elimina la necesidad de administrar por separado tanto una caché como una base de datos duradera.

Amazon MQ

Amazon MQ es un servicio de agente de mensajes administrado para Apache ActiveMQ y RabbitMQ que configura y opera agentes de mensajes en la nube. Los agentes de mensajes permiten que distintos sistemas de software (que generalmente utilizan lenguajes de programación diferentes en distintas plataformas) se comuniquen e intercambien información. La mensajería es la red troncal de las comunicaciones que conecta e integra los componentes de las aplicaciones distribuidas, como el procesamiento de pedidos, la gestión de inventario y el cumplimiento de los pedidos en el comercio electrónico. Amazon MQ se ocupa de administrar y mantener dos agentes de mensajes de código abierto, ActiveMQ y RabbitMQ.

Amazon Neptune

Amazon Neptune es un servicio de base de datos de gráficos confiable y rápido que facilita la creación y la ejecución de aplicaciones que funcionan con conjuntos de datos altamente conectados. El núcleo de Amazon Neptune es un motor de base de datos de gráficos con alto rendimiento y un diseño exclusivo y optimizado para almacenar miles de millones de relaciones y consultar el gráfico con una latencia de milisegundos. Amazon Neptune es compatible con modelos de grafos populares (Property Graph y RDF de W3C) y sus respectivos lenguajes de consulta como Apache, TinkerPop Gremlin y SPARQL, lo que permite a los clientes crear con facilidad consultas que navegan con eficiencia los conjuntos de datos altamente conectados. Neptune potencia los casos de uso de gráficos, como los motores de recomendaciones, la detección de fraudes, los gráficos de conocimiento, la investigación de medicamentos y la seguridad de redes.

Amazon OpenSearch Service

Amazon OpenSearch Service es un servicio que facilita que el cliente implemente, asegure y opere OpenSearch de forma rentable a escala. Además, permite a los clientes pagar solo por lo que usan, sin costos iniciales ni requisitos de uso. Con Amazon OpenSearch Service, los clientes obtienen la pila de ELK que necesitan, sin los gastos generales operativos.

Amazon Personalize

Amazon Personalize es un servicio de machine learning que facilita a los desarrolladores la creación de recomendaciones individualizadas para los clientes que utilizan sus aplicaciones. Amazon Personalize permite a los desarrolladores crear aplicaciones que puedan ofrecer una amplia variedad de experiencias de personalización, como recomendaciones específicas de productos, una reclasificación de productos personalizada y marketing directo personalizado. Amazon Personalize trasciende los sistemas de recomendaciones basados en reglas estáticas y rígidas y entrena, sintoniza e implementa modelos de machine learning personalizados para ofrecer recomendaciones muy personalizadas a los clientes en una variedad de industrias, como comercios minoristas, medios de comunicación y entretenimiento.

Amazon Pinpoint y End User Messaging (anteriormente Amazon Pinpoint)

Amazon Pinpoint y End User Messaging ayudan a los clientes a interactuar con otros clientes a través del envío de correos electrónicos, SMS y mensajes push móviles. Los clientes pueden usar Amazon Pinpoint y End User Messaging para enviar mensajes dirigidos (como alertas sobre promociones y campañas de retención de clientes), así como mensajes directos (como confirmaciones de pedidos y mensajes de restablecimiento de contraseñas) a sus clientes.

Amazon Polly

Amazon Polly es un servicio que convierte el texto en habla verosímil, lo que les permite a los clientes crear aplicaciones que puedan hablar y categorías completamente nuevas de productos con esta capacidad. Amazon Polly es un servicio que convierte el texto en voz y utiliza tecnologías avanzadas de aprendizaje profundo a fin de sintetizar habla que se asemeja a una voz humana.

Amazon Q Business (en vigor desde el 15 de agosto de 2024)

Amazon Q Business es un servicio que implementa un experto en IA generativa para los datos de su empresa. Cuenta con una interfaz de usuario integrada en la que los usuarios pueden hacer preguntas complejas en lenguaje natural, crear o comparar documentos, generar resúmenes de documentos e interactuar con aplicaciones de terceros. La funcionalidad de IA proporcionada por Amazon Q Business no está incluida en el diseño de los controles descritos en este informe SOC.

Amazon Q Developer (en vigor desde el 15 de agosto de 2024)

Amazon Q Developer es un asistente conversacional basado en inteligencia artificial (IA) generativa que puede ayudar a los clientes a comprender, crear, ampliar y utilizar las aplicaciones de AWS. Los clientes pueden hacer preguntas sobre la arquitectura de AWS, los recursos de AWS, las prácticas recomendadas, la documentación, la asistencia técnica y mucho más. Cuando se utiliza en un entorno de desarrollo integrado (IDE), Amazon Q proporciona asistencia para el desarrollo de software. Amazon Q puede conversar sobre código, proporcionar complementos de código en línea, generar código nuevo neto, analizar su código en busca de vulnerabilidades de seguridad y realizar actualizaciones y mejoras en el código, como actualizaciones de lenguaje, depuración y optimización. La funcionalidad de IA proporcionada por Amazon Q Developer no está incluida en el diseño de los controles descritos en este informe SOC.

Amazon Quantum Ledger Database (QLDB)

Amazon Quantum Ledger Database (QLDB) es una base de datos de libro mayor que ofrece un registro de transacción transparente, inmutable y verificable mediante cifrado a cargo de una autoridad central confiable. Amazon QLDB realiza un seguimiento de todos los cambios de los datos de aplicación y mantiene un historial de cambios completo y verificable a lo largo del tiempo.

Amazon QuickSight

Amazon QuickSight es un servicio de análisis empresarial rápido y basado en la nube que facilita la creación de visualizaciones, la realización de análisis *ad hoc* y la obtención rápida de información de la empresa a partir de los datos de los clientes. Con este servicio basado en la nube, los clientes pueden conectarse a sus datos, realizar análisis avanzados y crear visualizaciones y paneles a los que se puede acceder desde cualquier navegador o dispositivo móvil.

Amazon Redshift

Amazon Redshift es un servicio de almacenamiento de datos que sirve para analizar datos con las herramientas de inteligencia empresarial (BI) existentes del cliente. También incluye Redshift Spectrum, que permite a los clientes ejecutar directamente consultas SQL sobre exabytes de datos sin estructurar en Amazon S3.

Amazon Rekognition

La API Rekognition es fácil de usar y permite a los clientes identificar de forma automática objetos, personas, textos, escenas y actividades, así como detectar contenido inadecuado. Los desarrolladores pueden crear rápidamente una biblioteca de contenido apta para la búsqueda a fin de optimizar los flujos de trabajo de medios de comunicación, enriquecer los motores de recomendaciones mediante la extracción de texto en imágenes o integrar autenticación secundaria en aplicaciones existentes para incrementar la seguridad del usuario final. Con una amplia variedad de casos de uso, Amazon Rekognition permite a los clientes agregar fácilmente los beneficios de la visión artificial a la empresa.

Amazon Relational Database Service (RDS)

Amazon Relational Database Service (RDS) permite a los clientes configurar, operar y escalar una base de datos relacional en la nube. Amazon RDS administra copias de seguridad, parches de software, detección automática de errores y recuperación. Además, proporciona capacidad rentable y de tamaño modificable, a la vez que automatiza las tareas administrativas que consumen mucho tiempo, como el aprovisionamiento del hardware, la configuración de las bases de datos, la aplicación de parches y la creación de copias de seguridad.

Amazon Route 53

Amazon Route 53 provee el servicio web administrado de sistema de nombres de dominio (DNS). Conecta las solicitudes del usuario con la infraestructura que se ejecuta dentro y fuera de AWS. Los clientes pueden usar Amazon Route 53 para configurar las comprobaciones de estado de DNS a fin de enrutar el tráfico a puntos de conexión en buen estado o monitorear de forma independiente el estado de sus aplicaciones y puntos de conexión. Amazon Route 53 permite a los clientes administrar el tráfico de forma global a través de una variedad de tipos de enrutamiento, como el enrutamiento basado en la latencia, Geo DNS y WRR, todos tipos de enrutamiento que se pueden combinar con la conmutación por error de DNS. Amazon Route 53 también ofrece el registro de nombre de dominio, por lo que los clientes pueden comprar y administrar nombres de dominio como example.com y Amazon Route 53 configura de manera

automática los ajustes de DNS de sus dominios. Amazon Route 53 envía solicitudes automatizadas por Internet a un recurso, como un servidor web, para verificar si es alcanzable, funcional y está disponible. Los clientes también pueden elegir recibir notificaciones cuando un recurso pierde disponibilidad y desviar el tráfico de Internet lejos de los recursos en mal estado.

Amazon S3 Glacier

Amazon S3 Glacier es una solución de almacenamiento de archivo para datos a los que se accede con poca frecuencia y admiten tiempos de recuperación de varias horas. Los datos en Amazon S3 Glacier se almacenan como un archivo. Los archivos en Amazon S3 Glacier se pueden crear o borrar, pero no modificar. Los archivos de Amazon S3 Glacier se organizan en bóvedas. Todas las bóvedas creadas tienen una política de permisos predeterminada que solo otorga acceso al creador de la cuenta o los usuarios a los que explícitamente se otorgó permiso. Amazon S3 Glacier permite a los clientes configurar las políticas de acceso en sus bóvedas para los usuarios dentro de sus cuentas de AWS. Las políticas del usuario pueden expresar los criterios de acceso para Amazon S3 Glacier según la bóveda. Los clientes pueden ejecutar una semántica de tipo Write Once Read Many (WORM, escritura única, lecturas múltiples) para los usuarios a través de políticas de usuario que prohíben eliminar archivos.

Amazon SageMaker (excluye Studio Lab, el personal público y el personal del proveedor para todas las características)

Amazon SageMaker es una plataforma que permite a los desarrolladores y los científicos de datos crear, entrenar e implementar modelos de machine learning a cualquier escala con facilidad y rapidez. Elimina las barreras que suelen “desacelerar” a los desarrolladores que desean usar machine learning.

Amazon SageMaker elimina la complejidad que restringe el éxito del desarrollador con el proceso de crear, formar e implementar modelos de machine learning a escala. Incluye módulos que pueden usarse, en conjunto o por separado, para crear, formar e implementar modelos de machine learning del cliente.

Amazon Security Lake (en vigor desde el 15 de agosto de 2024)

Amazon Security Lake centraliza automáticamente los datos de seguridad de los entornos de AWS, los proveedores de SaaS, las instalaciones y las fuentes en la nube en un lago de datos personalizado almacenado en una cuenta de cliente. Con Security Lake, los clientes pueden obtener conocimientos más completos de los datos de seguridad de toda su organización. También pueden mejorar la protección de las cargas de trabajo, las aplicaciones y los datos.

Amazon Simple Email Service (SES)

Amazon Simple Email Service (SES) es un servicio de correo electrónico rentable, flexible y escalable que permite a los desarrolladores enviar correos desde cualquier aplicación. Los clientes pueden configurar Amazon SES para que sea compatible con varios casos de uso de correo electrónico, como comunicaciones transaccionales, de marketing o correos electrónicos masivos. Las opciones de implementación de IP flexible y autenticación de correos electrónicos que ofrece Amazon SES ayudan a impulsar una mayor capacidad de entrega y a proteger la reputación del remitente, al mismo tiempo que se envían análisis para medir el impacto de cada correo electrónico. Con Amazon SES, los clientes pueden enviar correos electrónicos de forma segura, global y a escala.

Amazon Simple Notification Service (SNS)

Amazon Simple Notification Service (SNS) es un servicio web que sirve para configurar, operar y enviar notificaciones. Permite a los desarrolladores publicar mensajes desde una aplicación y entregarlos a los suscriptores o a otras aplicaciones. Amazon SNS sigue un paradigma de mensajería del tipo "publish-subscribe" (pub-sub), en el que las notificaciones se envían a los clientes con un mecanismo "push". Para usar SNS, se requiere definir un "Tema", configurar las políticas referidas al acceso y la entrega del Tema, suscribir a los clientes, designar los puntos de conexión de entrega y publicar mensajes en un Tema. Los administradores definen un Tema como un punto de acceso para publicar mensajes y permitir a los clientes que se suscriban a las notificaciones. Se aplican políticas de seguridad en los Temas para determinar quién puede publicar, quién puede suscribirse y para designar los protocolos compatibles.

Amazon Simple Queue Service (SQS)

Amazon Simple Queue Service (SQS) es un servicio de cola de mensajes que ofrece una cola alojada y distribuida para almacenar mensajes mientras se transportan entre computadoras. Gracias a Amazon SQS, los desarrolladores pueden trasladar datos entre componentes distribuidos de sus aplicaciones que realizan distintas tareas, pero sin perder mensajes ni requerir que cada componente esté siempre disponible. Amazon SQS permite a los clientes crear un flujo de trabajo automatizado, en estrecha colaboración con Amazon EC2 y otros servicios web de infraestructura de AWS.

Los componentes principales de Amazon SQS son una flota de enrutadores de solicitudes de frontend, una flota de almacenamiento de datos de backend, una flota de caché de metadatos y una flota de gestión de cargas de trabajo dinámica. Las colas de los usuarios se asignan a uno o más clústeres de backend. Las solicitudes para leer, escribir o borrar mensajes ingresan a los frontends. Los frontends se contactan con la caché de metadatos para determinar qué clúster de backend aloja esa cola y, luego, conectar los nodos en ese clúster para atender la solicitud.

Para la autorización, Amazon SQS tiene su propio sistema de permisos basados en recursos que se rige por políticas escritas en el mismo lenguaje utilizado en las políticas de IAM de AWS. Los permisos del usuario para cualquier recurso de Amazon SQS se pueden otorgar a través del sistema de política de Amazon SQS o del sistema de políticas de IAM de AWS, que está autorizado mediante el AWS Identity and Access Management Service. Estas políticas se utilizan para especificar qué cuentas de AWS tienen acceso a la cola, así como el tipo de acceso y las condiciones.

Amazon Simple Storage Service (S3)

Amazon Simple Storage Service (S3) proporciona una interfaz de servicios web que se puede utilizar para almacenar y recuperar datos de cualquier lugar en la Web. Para brindarles a los clientes flexibilidad a fin de determinar cómo, cuándo y a quién desean exponer la información que almacenan en AWS, las API de Amazon S3 ofrecen controles de acceso de *bucket* y de objeto con valores predeterminados que solo permiten el acceso autenticado del creador del *bucket* o del objeto. A menos que el cliente conceda un acceso anónimo, el primer paso antes de que el usuario pueda acceder a Amazon S3 es recibir la autenticación con una solicitud firmada con la clave de acceso secreta del usuario.

Un usuario autenticado puede leer un objeto solo si se le otorgaron permisos de lectura en una Lista de control de acceso (ACL) a nivel del objeto. Un usuario autenticado puede enumerar las claves y crear o sobrescribir objetos en un bucket solo si se le concedieron permisos de escritura y lectura en una ACL a nivel del bucket. Las ACL a nivel de bucket y de objeto son independientes. Un objeto no hereda las ACL de su bucket. Los permisos para leer o modificar las ACL de bucket u objeto están controlados por ACL

con valores predeterminados que solo admiten el acceso del creador. En consecuencia, el cliente mantiene el control total de quién tiene acceso a sus datos. Los clientes pueden conceder acceso a sus datos de Amazon S3 a otros usuarios de AWS mediante el ID o el correo electrónico de la cuenta de AWS o el ID del producto DevPay. Los clientes también pueden otorgar acceso a sus datos de Amazon S3 a todos los usuarios de AWS o a cualquier persona (si habilitan el acceso anónimo).

Las configuraciones de los dispositivos de red compatibles con Amazon S3 permiten el acceso solo a puertos específicos en otros sistemas de servidores dentro de Amazon S3 **(Control AWSCA-3.7).** El acceso externo a los datos almacenados en Amazon S3 se registra y preserva por lo menos durante 90 días. Entre los registros, se incluye la información de solicitud de acceso pertinente, como el acceso a los datos o la dirección IP, el objeto y la operación **(Control AWSCA-3.8).**

Amazon Simple Workflow Service (SWF)

Amazon Simple Workflow Service (SWF) es un servicio de orquestación para crear aplicaciones distribuidas escalables. En general, una aplicación está formada por varias tareas diferentes que se deben realizar en una secuencia determinada impulsada por un conjunto de condiciones dinámicas. Amazon SWF permite a los desarrolladores crear e implementar estas tareas, ejecutarlas en la nube o en las instalaciones y coordinar sus flujos. Amazon SWF administra el flujo de ejecución para que las tareas posean equilibrio de carga entre los empleados, se respeten las dependencias entre las tareas, se manipule la concurrencia de forma correcta y se ejecuten flujos de trabajo complementarios.

Amazon SWF habilita la creación de aplicaciones a través de la orquestación de tareas coordinadas por un proceso de decisiones. Las tareas representan unidades lógicas de trabajo y se realizan con componentes de aplicación que pueden adoptar cualquier forma, como código ejecutable, *scripts*, llamadas de servicio web y acciones humanas.

Los desarrolladores implementan empleados para que realicen tareas. Ejecutan los empleados en una infraestructura en la nube, como Amazon EC2, o fuera de esta. Las tareas pueden tener una ejecución prolongada, fallar, caducar o completarse con distintos rendimientos y latencias. Amazon SWF almacena tareas para los empleados, las asigna cuando están listos, sigue su progreso, las mantiene actualizadas e incluye detalles sobre la finalización. Para orquestar las tareas, los desarrolladores escriben programas que permiten obtener el último estado de las tareas de Amazon SWF para iniciar tareas posteriores en forma continua. Amazon SWF mantiene el estado de ejecución de una aplicación de manera duradera para que esta pueda resistir los errores en cada uno de sus componentes.

Amazon SWF provee auditabilidad, ya que los clientes pueden visibilizar la ejecución de cada paso en la aplicación. La consola de administración y las API permiten a los clientes monitorear todas las ejecuciones en proceso de la aplicación. Además, pueden ampliar cualquier ejecución para visualizar el estado de cada tarea y sus datos de entrada y salida. Para facilitar la resolución de problemas y el análisis histórico, Amazon SWF retiene el historial de ejecuciones durante la cantidad de días que el cliente especifique (con un máximo de 90 días).

El proceso real de las tareas ocurre en recursos de computación que le pertenecen al cliente final. Los clientes son responsables de asegurar estos recursos de computación, por ejemplo, si un cliente utiliza Amazon EC2 para los empleados, puede restringir el acceso a sus instancias en Amazon EC2 a determinados usuarios de AWS IAM. Además, los clientes son responsables de cifrar la información confidencial antes de enviarla a sus flujos de trabajo y descifrarla en sus empleados.

Amazon SimpleDB

Amazon SimpleDB es un almacén de datos no relacional que permite a los clientes almacenar y consultar datos a través de solicitudes de servicios web. Crea y administra varias réplicas de datos distribuidas en distintas zonas geográficas de manera automática para ofrecer una alta disponibilidad y durabilidad de los datos.

Los datos en Amazon SimpleDB se almacenan en dominios, que son similares a las tablas de bases de datos, excepto que no se pueden ejecutar funciones en varios dominios. Las API de Amazon SimpleDB proveen controles en el nivel del dominio que solo permiten el acceso autenticado de su creador.

Los datos almacenados en Amazon SimpleDB se guardan de forma redundante en múltiples ubicaciones físicas como parte de la operación normal de esos servicios. Amazon SimpleDB provee durabilidad de objetos mediante la protección de datos en múltiples AZ en la escritura inicial y la replicación posterior activa ante el caso de falta de disponibilidad del dispositivo o detección de degradación de datos.

Amazon Textract

Amazon Textract extrae automáticamente datos y texto de documentos escaneados. Con Textract, los clientes pueden automatizar con rapidez flujos de trabajo de documentos, lo que les permite procesar grandes volúmenes de páginas en poco tiempo. Una vez captada la información, los clientes pueden realizar acciones sobre ella en sus aplicaciones empresariales para iniciar los pasos siguientes en el procesamiento de aplicaciones de préstamos o reclamos médicos. Además, pueden crear índices de búsqueda, generar flujos de trabajo de aprobación automatizados y mantener mejor la conformidad con las normas de archivado de documentos a partir del marcado de los datos que puedan requerir redacción.

Amazon Timestream

Amazon Timestream es un servicio de base de datos de serie temporal escalable, rápido y sin servidor para IoT y aplicaciones operativas que facilita el almacenamiento y el análisis de billones de eventos por día, hasta 1000 veces más rápido y con solo 1/10 del costo de las bases de datos relacionales. Amazon Timestream ahorra tiempo y costos para los clientes en la gestión del ciclo de vida de los datos de serie temporal, gracias a que retiene los datos recientes en la memoria y traslada los datos históricos a un nivel de almacenamiento de costo optimizado, de acuerdo con las políticas que define el usuario. Amazon Timestream cuenta con un motor de consulta diseñado específicamente para permitir a los clientes acceder a datos recientes e históricos y analizarlos juntos sin tener que especificar de forma explícita en la consulta si los datos están en la memoria o en el nivel de costo optimizado. Amazon Timestream ofrece funciones de análisis de serie temporal e integradas que ayudan a los clientes a identificar tendencias y patrones en los datos en tiempo real.

Amazon Transcribe

Amazon Transcribe facilita la incorporación de capacidad de conversión de voz a texto en las aplicaciones de los clientes. Para las computadoras, es prácticamente imposible buscar y analizar datos de audio. Por esta razón, es necesario convertir las conversaciones de voz grabadas en texto antes de usarlas en las aplicaciones.

Amazon Transcribe aplica un proceso de aprendizaje profundo llamado automatic speech recognition (ASR, reconocimiento automático de voz) para convertir la voz a texto con rapidez. Se puede usar para transcribir las llamadas de servicio al cliente, automatizar subtítulos (incluso del tipo ocultos) y generar metadatos para que los activos de medios de comunicación creen un archivo que permita búsquedas completas.

De forma automática, Amazon Transcribe agrega puntuación y formato para que el producto se asemeje bastante a la calidad de la transcripción manual, pero con solo una fracción del tiempo y los gastos involucrados.

Amazon Translate

Amazon Translate es un servicio de traducción automática neuronal que ofrece traducciones rápidas, de alta calidad y asequibles. La traducción automática neuronal es una forma de automatización de la traducción de idiomas que utiliza modelos de aprendizaje profundo para ofrecer una traducción más precisa y natural que aquella que proviene de los algoritmos de traducción tradicionales, estadísticos y basados en reglas. Amazon Translate permite a los clientes localizar contenido, como los sitios web y las aplicaciones, para los usuarios internacionales y traducir grandes volúmenes de texto de forma eficiente y con facilidad.

Amazon Virtual Private Cloud (VPC)

Amazon Virtual Private Cloud (VPC) permite a los clientes aprovisionar una sección aislada lógicamente de la nube de AWS en la que se pueden lanzar recursos de AWS en una red virtual definida por el cliente. Los clientes pueden conectar su infraestructura vigente con las instancias de Amazon EC2 aisladas de la red dentro de Amazon VPC, ampliar sus capacidades de gestión ya existentes, como servicios de seguridad, firewalls y sistemas de detección de intrusos, y así agregar sus instancias a través de una conexión a una red privada virtual (VPN). El servicio de VPN provee aislamiento en la red de extremo a extremo a través de una gama de direcciones IP que eligen los clientes y el enrutamiento de todo el tráfico de red entre Amazon VPC y otra red que designan los clientes mediante una VPN de seguridad con protocolo de Internet cifrado (IPsec).

De forma opcional, los clientes pueden conectar su VPC a Internet añadiendo una Internet Gateway (IGW, puerta de enlace de Internet) o puerta de enlace de NAT. La IGW permite el acceso bidireccional desde y hacia Internet para algunas instancias en la VPC según las rutas que definen los clientes. En ellas se especifica qué tráfico de qué dirección IP debe enrutarse desde Internet, los grupos de seguridad y las ACL de red (NACLS), que limitan qué instancias pueden aceptar o enviar este tráfico. Asimismo, los clientes tienen la opción de configurar una puerta de enlace de NAT que permite que el tráfico solo saliente iniciado desde una instancia de VPC alcance Internet, pero impide que el tráfico iniciado desde Internet llegue a las instancias de VPC. Esto se logra mediante la asignación de direcciones IP privadas a una dirección pública en la salida y la asignación de la dirección IP pública a la dirección privada en el retorno.

El objetivo de esta arquitectura es aislar los recursos y datos de AWS en una Amazon VPC de otra Amazon VPC y prevenir que se transfieran datos desde afuera de la red de Amazon, excepto cuando el cliente configura específicamente opciones de conectividad a Internet o a través de una conexión de VPN IPsec a la red fuera de la nube.

A continuación, se muestran más detalles:

- **Nube virtual privada (VPC):** una nube virtual privada de Amazon es una porción aislada de la nube de AWS en la que los clientes pueden implementar instancias de Amazon EC2 en subredes que segmentan el rango de direcciones IP de la VPC (tal como lo designa el cliente) y aislar las instancias de Amazon EC2 en una subred de otra subred. Las instancias de Amazon EC2 dentro de una Amazon VPC son accesibles para los clientes a través de la puerta de enlace de Internet (IGW), la puerta de enlace virtual (VGW), la puerta de enlace de tránsito (TGW) o los emparejamientos de VPC establecidos en Amazon VPC **(Control AWSCA-3.13** y **AWSCA-3.15).**

- **IPsec VPN:** una conexión de VPN IPsec conecta la Amazon VPC de un cliente a otra red que este designe. IPsec es un conjunto de protocolos que protegen las comunicaciones de Internet Protocol (IP, Protocolo de Internet) gracias a la autenticación y el cifrado de cada paquete de IP de un flujo de datos. Para crear una conexión de VPN IPsec a su Amazon VPC, los clientes de Amazon VPC primero deben establecer una asociación de seguridad de Internet Key Exchange (IKE, intercambio de clave de Internet) entre la puerta de enlace de VPN de Amazon VPC y la puerta de enlace de otra red usando como autenticador una clave compartida con anterioridad. Una vez establecido, el IKE negocia con una clave efímera para proteger los mensajes futuros de IKE. Una asociación de seguridad IKE no se puede establecer, a menos que haya una concordancia total entre los parámetros. A continuación, con la clave efímera de IKE, se establecen dos claves en total entre la puerta de enlace de VPN y la puerta de enlace de cliente para formar una asociación de seguridad IPsec. El tráfico entre las puertas de enlace se cifra y descifra con esa asociación de seguridad. IKE rota automáticamente las claves efímeras utilizadas para cifrar el tráfico dentro de la asociación de seguridad IPsec con regularidad a fin de garantizar la confidencialidad de las comunicaciones **(Control AWSCA-3.14** y **AWSCA-4.3)**.

Amazon WorkDocs

Amazon WorkDocs es un servicio seguro de creación de contenido, almacenamiento y colaboración. Los usuarios pueden compartir archivos, hacer comentarios enriquecedores y acceder a su contenido alojado en WorkDocs desde cualquier dispositivo. WorkDocs cifra datos en tránsito y en reposo y ofrece poderosos controles de gestión, integración con Active Directory y visibilidad casi en tiempo real de los archivos y las acciones de los usuarios. El SDK de WorkDocs permite a los usuarios utilizar las mismas herramientas de AWS que ya conocen e integrar WorkDocs con los productos y servicios de AWS, sus soluciones ya existentes, aplicaciones de terceros o propias.

Amazon WorkMail

Amazon WorkMail es un servicio administrado de correo electrónico y calendario empresariales que es compatible con escritorios existentes y clientes de correo electrónico para dispositivos móviles. Permite acceder a correos electrónicos, contactos y calendarios mediante Microsoft Outlook, un navegador o aplicaciones nativas de iOS y Android. Amazon WorkMail puede integrarse al directorio corporativo actual de los clientes para que puedan controlar las claves que cifran los datos y la ubicación (región de AWS) en la que se almacenan.

Los clientes pueden crear una organización en Amazon WorkMail, seleccionar el Active Directory con el que desean integrarse y elegir su clave de cifrado para aplicarla a todos los contenidos del cliente. Después de configurar y validar su dominio de correo, desde Active Directory se seleccionan o agregan usuarios, se habilitan para Amazon WorkMail y se les otorga la identidad de dirección de correo electrónico dentro del dominio de correo electrónico que le pertenece al cliente.

Amazon WorkSpaces

Amazon WorkSpaces es un servicio de computación en la nube administrado desde el escritorio. Amazon WorkSpaces permite a los clientes entregar una experiencia de escritorio de alta calidad a los usuarios finales, así como ayudar a cumplir los requisitos de conformidad y políticas de seguridad. Cuando se usa Amazon WorkSpaces, los datos de una organización no se envían ni se almacenan en los dispositivos del usuario final. Los protocolos PCoIP y WSP empleados por Amazon WorkSpaces utilizan una transmisión de video interactiva para brindar la experiencia de escritorio al usuario mientras los datos permanecen en la nube de AWS o en el entorno fuera de la nube de la organización.

Cuando se integra Amazon WorkSpaces al Active Directory corporativo, cada WorkSpace se une al dominio de Active Directory y puede administrarse como cualquier otro escritorio en la organización. Esto significa que los clientes pueden usar las Políticas de Grupos de Active Directory para administrar su Amazon WorkSpaces y especificar las opciones de configuración que controlan el escritorio, incluso aquellas que restringen las capacidades de los usuarios para utilizar almacenamiento local en sus dispositivos. Amazon WorkSpaces también se integra con el servidor RADIUS vigente de los clientes para habilitar la autenticación multifactor (MFA).

Amazon WorkSpaces Secure Browser (anteriormente Amazon Workspaces Web)

Amazon WorkSpaces Secure Browser es un servicio administrado bajo demanda, diseñado para facilitar el acceso seguro del explorador a sitios web internos y aplicaciones de software como servicio (SaaS). Los clientes pueden acceder al servicio desde exploradores web existentes sin administración de infraestructura, software cliente especializado o soluciones de redes privadas virtuales (VPN).

Cliente ligero de Amazon WorkSpaces (en vigor desde el 15 de agosto de 2024)

Cliente ligero de Amazon WorkSpaces reduce los costos de computación del usuario final y simplifica la logística de los dispositivos al enviarlos directamente desde los centros de distribución de Amazon a los usuarios finales o a las ubicaciones de la empresa. Los usuarios finales pueden configurar un dispositivo en cuestión de minutos, sin asistencia de TI. También ayuda a mejorar la seguridad al evitar que los usuarios almacenen datos o carguen aplicaciones en el dispositivo local e incluye un servicio sencillo de administración de dispositivos. Cliente ligero de WorkSpaces proporciona una consola para monitorear, administrar y mantener de forma centralizada los dispositivos y su conectividad con los servicios de escritorio virtual de AWS.

AWS Amplify

AWS Amplify es un conjunto de herramientas y servicios con tecnología de AWS que se puede emplear de forma conjunta o individual. Su objetivo es ayudar a los desarrolladores de interfaces de usuario y móviles a crear aplicaciones escalables de pila completa. Además, los clientes pueden configurar el backend de las aplicaciones y conectarlas en minutos, implementar aplicaciones web estáticas en solo unos clics y administrar sin problemas el contenido de las aplicaciones que no pertenecen a la consola de AWS. Amplify es compatible con marcos web populares, entre ellos, JavaScript, React, Angular, Vue, Next.js y plataformas móviles como Android, iOS, React Native, Ionic y Flutter.

AWS App Mesh

AWS App Mesh es una malla de servicios que brinda redes de nivel de aplicación y permite que los servicios de los clientes se comuniquen entre sí mediante diferentes tipos de infraestructuras informáticas. App Mesh otorga a los clientes una visibilidad total y una alta disponibilidad para las aplicaciones. AWS App Mesh facilita la ejecución de servicios seguros ofreciendo una visibilidad consistente y controles de tráfico de red. Permite prescindir de las actualizaciones de código de las aplicaciones para cambiar la forma en que se recopilan los datos de monitoreo o se dirige el tráfico entre los servicios. Asimismo, configura cada servicio para exportar los datos de monitoreo e implementa una lógica uniforme de control de las comunicaciones en todas las aplicaciones.

<u>AWS App Runner</u>
AWS App Runner es un servicio que facilita la tarea de los desarrolladores en la implementación rápida de aplicaciones web y API en contenedores, a escala y sin necesidad de experiencia previa en infraestructura. El servicio proporciona una abstracción simplificada sin infraestructura para aplicaciones web multiconcurrentes y servicios basados en API. Con App Runner, los componentes de la infraestructura, como la compilación, los equilibradores de carga, los certificados y las réplicas de aplicaciones, están administrados por AWS. Los clientes solo proporcionan su código fuente (o una imagen de contenedor creada previamente) y obtienen a cambio una URL de punto de conexión de servicio en la que se pueden realizar solicitudes.

<u>AWS AppFabric</u>
AWS AppFabric es un servicio sin código que conecta varias aplicaciones de Software como un Servicio (SaaS) para mejorar la seguridad, la administración y la productividad. AppFabric agrega y normaliza los datos de SaaS (p. ej., registros de eventos de usuarios, acceso de usuarios) en todas las aplicaciones de SaaS sin necesidad de escribir integraciones de datos personalizadas.

<u>AWS Application Migration Service</u>
AWS Application Migration Service es el principal servicio que AWS recomienda para migrar las aplicaciones a AWS. El servicio minimiza los procesos manuales, que requieren mucho tiempo y son propensos a errores, al adaptar automáticamente los servidores fuente de los clientes desde una infraestructura física, virtual o en la nube para que se ejecuten de forma nativa en AWS. Los clientes pueden utilizar el mismo proceso automatizado para migrar una amplia gama de aplicaciones a AWS sin realizar cambios en las aplicaciones, su arquitectura o los servidores migrados.

<u>AWS AppSync</u>
AWS AppSync es un servicio que permite a los clientes desarrollar y administrar con facilidad las API GraphQL. Una vez que se implementa, AWS AppSync escala de forma automática y por completo su motor de ejecución para satisfacer los volúmenes de solicitudes de las API. AWS AppSync permite configurar, administrar y preservar el lenguaje GraphQL gracias a una infraestructura sin servidor, pero con una gran disponibilidad incorporada.

<u>AWS Artifact</u>
AWS Artifact es un portal de recuperación de artefactos de auditoría de autoservicio que brinda a los clientes acceso bajo demanda a la documentación de conformidad de AWS y a sus acuerdos. Los clientes pueden utilizar AWS Artifact Reports para descargar documentos de seguridad y conformidad de AWS, como las certificaciones ISO de AWS, los informes del sector de tarjetas de pago (PCI) y los de control de sistemas y organizaciones (SOC). Los clientes pueden usar AWS Artifact Agreements para revisar, aceptar y hacer un seguimiento del estado de los acuerdos de AWS.

<u>AWS Audit Manager</u>
Con la ayuda de AWS Audit Manager, los clientes auditan de manera continua el uso de AWS para simplificar cómo administran el riesgo y la conformidad con las regulaciones y los estándares del sector. Con AWS Audit Manager, es fácil evaluar si las políticas, los procedimientos y las actividades (también llamados controles) funcionan según lo previsto. El servicio no solo brinda marcos predefinidos con controles que se ajustan a los estándares y regulaciones reconocidos del sector, sino que también ofrece marcos y controles según requisitos particulares y una colección y organización automática de la evidencia de acuerdo con el diseño de cada requisito de control.

AWS Backup

AWS Backup es un servicio de copias de seguridad que facilita la centralización y automatización de los datos de respaldo incluidos en los servicios de AWS en la nube, como así también en aquellos en las instalaciones y que requieren AWS Storage Gateway. Si se utiliza AWS Backup, los clientes pueden configurar de forma centralizada las políticas de copia de seguridad de los recursos de AWS, como los volúmenes de Amazon EBS, las bases de datos de Amazon RDS, las tablas de Amazon DynamoDB, los sistemas de archivos de Amazon EFS y los volúmenes de AWS Storage Gateway. AWS Backup automatiza y consolida las tareas de copia de seguridad que anteriormente se realizaban servicio por servicio, por lo que se elimina la necesidad de elaborar *scripts* y procesos manuales personalizados.

AWS Batch

AWS Batch permite que los desarrolladores, científicos e ingenieros ejecuten trabajos de computación por lotes en AWS. Además, aprovisiona de forma dinámica la cantidad y el tipo de recursos informáticos óptimos (por ejemplo, instancias optimizadas para memoria o CPU) según los requerimientos de volumen y recursos específicos de los trabajos por lote enviados. AWS Batch planifica, programa y ejecuta las cargas de trabajo de computación de cada lote de los clientes en toda la gama de características y servicios de computación de AWS, como Amazon EC2 y las instancias de spot.

AWS Certificate Manager (ACM)

AWS Certificate Manager (ACM) es un servicio que permite aprovisionar, administrar e implementar con facilidad los certificados de la capa de conexión segura (SSL) o de Transport Layer Security (TLS), sean públicos o privados, para utilizarlos con los servicios de AWS y los recursos internos conectados. Los certificados de SSL/TLS se utilizan para asegurar las comunicaciones de la red y establecer la identidad de los sitios web en Internet, así como los recursos de las redes privadas. Con AWS Certificate Manager, ya no es necesario adquirir, cargar y renovar los certificados de SSL y TLS de forma manual.

AWS Chatbot

Con AWS Chatbot, un servicio de AWS, los equipos de desarrollo de software y DevOps pueden utilizar las salas de chat de Slack o Amazon Chime para monitorear los eventos operativos y responder a ellos en la nube de AWS. AWS Chatbot procesa las notificaciones del servicio de AWS desde Amazon Simple Notification Service (Amazon SNS) y las envía a las salas de chat de Slack o Amazon Chime para que los equipos los analicen e intervengan en consecuencia. Los equipos pueden responder a los eventos de servicio de AWS desde una sala de chat donde todos los miembros colaboran sin importar su ubicación.

AWS Clean Rooms

AWS Clean Rooms ayuda a los clientes y a sus socios a colaborar y analizar sus conjuntos de datos colectivos de forma más fácil y segura, sin necesidad de compartir ni copiar los datos subyacentes de los demás. Con AWS Clean Rooms, los clientes pueden crear una sala limpia de datos segura en cuestión de minutos y colaborar con cualquier otra empresa en la nube de AWS para obtener información exclusiva sobre campañas publicitarias, decisiones de inversión, e investigación y desarrollo. Los clientes pueden usar AWS Clean Rooms para analizar los datos con hasta cuatro partes en una sola colaboración. También pueden obtener información de forma segura de varias empresas sin tener que escribir código. Por otro lado, pueden crear una sala limpia, invitar a las empresas con las que desean colaborar y seleccionar qué participantes pueden ejecutar análisis dentro de la colaboración.

AWS Cloud Map

AWS Cloud Map es un servicio de descubrimiento de recursos en la nube con el que los clientes pueden definir nombres para los recursos de sus aplicaciones. Cloud Map conserva la ubicación de estos recursos en constante cambio para incrementar la disponibilidad de las aplicaciones.

Los clientes pueden registrar cualquier recurso de las aplicaciones, como las bases de datos, las colas, los microservicios y otros recursos de la nube, con nombres personalizados. Así, Cloud Map comprueba el estado de los recursos para asegurarse de que la ubicación está actualizada y, luego, consultar el registro de la ubicación de los recursos requeridos según la versión de la aplicación en el entorno de implementación.

AWS Cloud9

AWS Cloud9 es un entorno de desarrollo integrado (IDE, en inglés). AWS Cloud9 IDE tiene una terminal incorporada que ofrece una experiencia valiosa de edición de código y es compatible con varios lenguajes de programación y depuradores de tiempo de ejecución. Contiene una colección de herramientas para que los clientes codifiquen, creen, ejecuten y depuren distintos tipos de software, y también para que lo suban a la nube. Los clientes acceden al IDE de AWS Cloud9 mediante un navegador web, donde pueden configurarlo según sus preferencias. Además, pueden cambiar la paleta de colores, combinar las teclas de acceso directo, habilitar el uso de colores para la sintaxis y el formateo del código específicos del lenguaje de programación y mucho más.

AWS CloudFormation

AWS CloudFormation es un servicio con el que se puede simplificar el aprovisionamiento de los recursos de AWS, como los grupos de Auto Scaling, los ELB, Amazon EC2, Amazon VPC, Amazon Route 53 y más. Las plantillas creadas por los clientes sobre la infraestructura y las aplicaciones que desean usar en AWS, así como el servicio AWS CloudFormation, aprovisiona de forma automática los recursos de AWS requeridos y sus relaciones según lo establecido en tales documentos.

AWS CloudHSM

AWS CloudHSM es un servicio que permite a los clientes utilizar HSM exclusivos dentro de la nube de AWS. AWS CloudHSM está diseñado para aplicaciones en las que es obligatorio utilizar HSM para el cifrado y el almacenamiento de claves.

AWS adquiere estos dispositivos de HSM de producción de manera segura a través de bolsas autentificables con sellos inviolables (TEA) que ofrecen los proveedores. El fabricante compara los números de serie de estas TEA y de los HSM de producción con los datos provistos fuera de banda y las personas aprobadas los registran en los sistemas de seguimiento **(Control AWSCA-4.15)**.

AWS CloudHSM permite a los clientes almacenar y usar claves de cifrado dentro de HSM en los centros de datos de AWS. Con AWS CloudHSM, los clientes conservan la propiedad total, el control y el acceso con respecto a las claves y la información confidencial, mientras que Amazon administra los HSM más próximos a las aplicaciones y datos del cliente. Todos los medios HSM se ponen fuera de servicio de forma segura y se destruyen físicamente, bajo la verificación de dos empleados, antes de retirarlos del control de AWS **(Control AWSCA-5.13)**.

AWS CloudShell

AWS CloudShell es un entorno de *shell* basado en explorador que se usa para administrar y explorar sus recursos de AWS, además de interactuar con ellos de manera segura. CloudShell requiere autenticación previa con las credenciales de la consola del cliente. Las herramientas de desarrollo y operaciones comunes ya están instaladas, por lo que no se requiere ni instalación ni configuración locales. Con CloudShell, los clientes pueden ejecutar *scripts* con la interfaz de la línea de comandos de AWS (AWS CLI), experimentar con las API de servicios de AWS mediante AWS SDK o utilizar unas diversas otras herramientas para ser productivos. Los clientes pueden usar CloudShell directamente desde sus exploradores.

AWS CloudTrail

AWS CloudTrail es un servicio web que registra la actividad de AWS para los clientes y provee archivos de registro a un bucket de Amazon S3 específico. La información registrada incluye la identidad del intermediario de la API, la hora a la que se realiza la llamada a la API, la dirección IP de origen del intermediario, los parámetros de la solicitud y los elementos de respuesta devueltos por el servicio de AWS.

AWS CloudTrail brinda un historial de llamadas a la API de AWS para las cuentas del cliente, incluidas las llamadas a la API que se realizan a través de la consola de administración de AWS, los SDK de AWS, las herramientas de la línea de comandos y los servicios de AWS de nivel superior (como AWS CloudFormation). El historial de llamadas a la API de AWS que produce AWS CloudTrail permite el análisis seguro, el seguimiento de cambios de recursos y la auditoría de conformidad.

AWS CodeBuild

AWS CodeBuild es un servicio de creación que compila códigos fuente, ejecuta pruebas y produce paquetes de software listos para su implementación. CodeBuild escala de manera continua y procesa varias creaciones al mismo tiempo para que las creaciones de los clientes no queden en una cola de espera. Los clientes pueden usar entornos de creación ya empaquetados o diseñar entornos de creación personalizados que utilicen sus propias herramientas de creación. AWS CodeBuild elimina la necesidad de configurar, arreglar con parches, actualizar y administrar los servidores de compilación y el software del cliente.

AWS CodeCommit

AWS CodeCommit es un servicio de control de código fuente que aloja repositorios Git privados. Permite a los equipos colaborar con el código en un ecosistema seguro y altamente escalable. Con CodeCommit, los clientes no necesitan operar su propio sistema de control de fuente o preocuparse por el escalado de sus infraestructuras. CodeCommit se puede utilizar para almacenar de forma segura cualquier elemento, desde código fuente hasta archivos binarios, y funciona a la perfección con las herramientas de Git existentes.

AWS CodeDeploy

AWS CodeDeploy es un sistema de implementación que automatiza las implementaciones de software en una variedad de servicios de computación como Amazon EC2, AWS Fargate, AWS Lambda y los servicios en las instalaciones del cliente. AWS CodeDeploy permite a los clientes lanzar características nuevas con rapidez, ayuda a evitar tiempos de inactividad durante la implementación de la aplicación y gestiona la complejidad de actualizar las aplicaciones.

AWS CodePipeline

AWS CodePipeline es un servicio de entrega continua que ayuda a los clientes a automatizar las canalizaciones de lanzamientos para lograr actualizaciones rápidas y confiables de la aplicación e infraestructura. CodePipeline automatiza las fases de crear, probar e implementar en el proceso de lanzamiento del cliente cada vez que ocurre un cambio de código, con base en el modelo de lanzamiento que defina el cliente. Esto permite a los clientes entregar características y actualizaciones de forma rápida y confiable. Los clientes pueden integrar fácilmente AWS CodePipeline en servicios de terceros como GitHub o en su propio complemento personalizado.

AWS Config

AWS Config permite a los clientes estimar, auditar y evaluar las configuraciones de los recursos de AWS. AWS Config monitorea y registra de forma continua las configuraciones de los recursos de AWS y les permite a los clientes automatizar la evaluación de las configuraciones registradas en función de las configuraciones deseadas. Además, pueden revisar los cambios en las configuraciones y relaciones entre los recursos de AWS, profundizar en los historiales detallados de la configuración de los recursos y determinar la conformidad general según las configuraciones especificadas en las directrices internas. Esto permite simplificar la auditoría del cumplimiento, el análisis de seguridad, la gestión de los cambios y la resolución de los problemas operativos.

AWS Control Tower

AWS Control Tower proporciona la forma más fácil de configurar y gobernar un entorno de AWS nuevo, seguro y de varias cuentas de acuerdo con las prácticas recomendadas establecidas gracias a la experiencia que ha obtenido AWS ayudando a miles de empresas a trasladarse a la nube. Con AWS Control Tower, los creadores pueden aprovisionar cuentas de AWS nuevas que cumplen con las políticas del cliente. Si los clientes necesitan crear un nuevo entorno de AWS y, a la vez, iniciar su camino junto a AWS y comenzar una nueva iniciativa de nube, o bien si no saben absolutamente nada sobre cómo trabajar con AWS, Control Tower los ayudará a comenzar sin demora con el gobierno y las prácticas recomendadas integradas.

AWS Data Exchange

AWS Data Exchange facilita la búsqueda, la suscripción y el uso de datos de terceros en la nube. Los proveedores de datos calificados incluyen marcas líderes de la categoría. Una vez suscritos a un producto de datos, los clientes pueden usar la API de AWS Data Exchange para cargar datos directamente en Amazon S3 y, luego, analizarlos con la variedad de servicios de análisis y machine learning que ofrece AWS. Para los proveedores de datos, AWS Data Exchange facilita el alcance a millones de clientes de AWS que migran hacia la nube gracias a que ya no es necesario crear y mantener una infraestructura de almacenamiento de datos, entrega, facturación y concesión de derechos.

AWS Database Migration Service (DMS)

AWS Database Migration Service (DMS) es un servicio en la nube que habilita a los clientes a migrar bases de datos relacionales, almacenes de datos, bases de datos NoSQL y otros tipos de almacenamientos de datos. AWS DMS se puede usar para migrar datos en la nube de AWS, entre instancias en las instalaciones (a través de la configuración de la nube de AWS) o entre combinaciones de configuraciones en la nube y en las instalaciones. El servicio es compatible con migraciones homogéneas dentro de una plataforma de bases de datos, así como migraciones heterogéneas entre distintas plataformas de bases de datos. AWS Database Migration Service también se puede utilizar para la replicación de datos continua con alta disponibilidad.

AWS DataSync

AWS DataSync es un servicio de transferencia de datos en línea que simplifica, automatiza y acelera el movimiento de datos entre el almacenamiento en las instalaciones y los servicios de AWS Storage, así como entre los servicios de AWS Storage. Con DataSync, se pueden copiar datos entre el Network File System (NFS), los servidores de archivos Server Message Block (SMB), el almacenamiento de objetos autoadministrado, AWS Snowcone, los buckets de Amazon Simple Storage Service (Amazon S3), los sistemas de archivos de Amazon EFS y los sistemas de archivo de Amazon FSx para Windows File Server. DataSync gestiona de forma automática muchas de las tareas relacionadas con las transferencias de datos que pueden desacelerar las migraciones o cargar las operaciones de TI de los clientes, incluidas la ejecución de las instancias propias de los clientes, la manipulación del cifrado, la administración de *scripts*, la optimización de la red y la validación de la integridad de datos.

AWS Direct Connect

AWS Direct Connect permite a los clientes establecer una conexión de red exclusiva entre sus redes y una de las ubicaciones de AWS Direct Connect. Utilizando AWS Direct Connect, los clientes pueden establecer una conexión privada entre AWS y su centro de datos, oficina o entorno de coubicación.

AWS Directory Service (excluye Simple AD)

AWS Directory Service for Microsoft Active Directory, también conocido como AWS Managed Microsoft AD, permite que las cargas de trabajo de directorio y los recursos de AWS utilicen Active Directory (AD) administrado en la nube de AWS. AWS Managed Microsoft AD almacena contenido de directorio en volúmenes de Amazon Elastic Block Store cifrados mediante el uso de claves de cifrado. Los datos en tránsito a los clientes de Active Directory y desde estos están cifrados cuando viajan a través del Lightweight Directory Access Protocol (LDAP) por la red de Amazon Virtual Private Cloud (VPC) de los clientes. Si un cliente de Active Directory está ubicado en una red fuera de la nube, el tráfico viaja hasta la VPC de los clientes a través de un enlace de red privada virtual o un enlace de AWS Direct Connect.

AWS Elastic Beanstalk

AWS Elastic Beanstalk es un programa de lanzamiento de contenedores de aplicación que permite a los clientes lanzar y escalar sus aplicaciones sobre AWS. Los clientes pueden usar AWS Elastic Beanstalk para crear entornos nuevos con los programas seleccionados de Elastic Beanstalk y sus aplicaciones, implementar versiones de las aplicaciones, actualizar las configuraciones de las aplicaciones, recrear entornos, actualizar configuraciones de AWS, monitorear el estado y la disponibilidad del entorno y crear sobre la infraestructura escalable que proveen servicios preexistentes como Auto Scaling, Elastic Load Balancing, Amazon EC2, Amazon VPC y Amazon Route 53, entre otros.

AWS Elastic Disaster Recovery

AWS Elastic Disaster Recovery minimiza el tiempo de inactividad y la pérdida de datos con recuperación de aplicaciones en las instalaciones y basadas en la nube que usa almacenamiento asequible, computación mínima y recuperación a un momento dado. Los clientes pueden configurar AWS Elastic Disaster Recovery en sus servidores de origen para iniciar la replicación segura de los datos. Los datos de los clientes se replican en una subred de área provisional en sus cuentas de AWS, en la región de AWS que seleccionen. El diseño del área provisional reduce los costos gracias al uso de almacenamiento asequible y recursos mínimos de computación para mantener la replicación en curso. Los clientes pueden realizar pruebas que no interrumpen las actividades para confirmar que se haya completado la implementación. En el curso de las operaciones normales, los clientes pueden mantenerse preparados por medio del control de la replicación y la ejecución periódica de

simulacros de conmutación por recuperación que no interrumpan las actividades. Si los clientes necesitan recuperar aplicaciones, pueden lanzar instancias de recuperación en AWS en solo minutos, con el estado de servidor más actualizado o a un momento determinado anterior.

AWS Elemental MediaConnect

AWS Elemental MediaConnect es un servicio de alta calidad que permite transportar videos en vivo. MediaConnect habilita a los clientes a crear flujos de trabajo esenciales de videos en vivo empleando una fracción del tiempo y el costo de los servicios de satélite o fibra. Los clientes pueden usar MediaConnect para capturar videos en vivo de un sitio de eventos remoto (como un estadio), compartir videos con socios (como un distribuidor de televisión por cable) o replicar una transmisión de video para su procesamiento (como un servicio de libre transmisión). MediaConnect combina el transporte de video confiable, el intercambio de transmisiones de alta seguridad y el monitoreo de tráfico de la red y videos en tiempo real que permiten a los clientes concentrarse en el contenido y no en su infraestructura de transporte.

AWS Elemental MediaConvert

AWS Elemental MediaConvert es un servicio de transcodificación de video basado en archivos que posee características con calidad de difusión. Permite a los clientes crear contenido de video-on-demand (VOD, video bajo demanda) para la difusión y entrega en múltiples pantallas a escala. El servicio combina capacidades de video y audio avanzadas con una interfaz de servicios web sencilla. Con AWS Elemental MediaConvert, los clientes pueden concentrarse en proporcionar experiencias de medios de comunicación sin preocuparse por la complejidad de crear y operar infraestructura de procesamiento de video.

AWS Elemental MediaLive

AWS Elemental MediaLive es un servicio de procesamiento de video en vivo. Los clientes pueden crear transmisiones de video de alta calidad para su entrega a televisores de difusión y dispositivos de múltiples pantallas conectados a Internet, como televisores conectados, tabletas, smartphones y decodificadores. El funcionamiento del servicio consiste en codificar transmisiones de video en vivo en tiempo real, tomar un origen de video en vivo de gran tamaño y comprimirlo en versiones más pequeñas para su distribución a los espectadores. AWS Elemental MediaLive permite a los clientes centrarse en crear experiencias de video en vivo para los espectadores sin la complejidad de crear y operar la infraestructura de procesamiento de videos.

AWS Entity Resolution (en vigor a partir del 15 de febrero de 2024)

AWS Entity Resolution es un servicio que ayuda a los clientes a hacer coincidir, vincular y mejorar sus registros relacionados y almacenados en varias aplicaciones, canales y almacenes de datos. AWS Entity Resolution ofrece técnicas de coincidencia, como la coincidencia basada en reglas, la coincidencia impulsada por modelos de machine learning (ML) y la coincidencia de proveedores de servicios de datos, que sirven de ayuda para vincular con mayor precisión conjuntos relacionados de información de clientes, códigos de productos o códigos de datos empresariales.

Servicio de inyección de errores de AWS

El servicio de inyección de errores de AWS es un servicio totalmente administrado para ejecutar experimentos de inyección de errores a fin de mejorar el rendimiento, la observabilidad y la resiliencia de las aplicaciones. FIS simplifica el proceso de configuración y ejecución de experimentos de inyección de errores controlados en una gama de servicios de AWS, de modo que los equipos puedan generar confianza en el comportamiento de sus aplicaciones.

AWS Firewall Manager

AWS Firewall Manager es un servicio de gestión de seguridad que facilita la configuración y gestión centralizadas de las reglas de AWS WAF en las cuentas y aplicaciones. Con Firewall Manager, los clientes pueden desplegar las reglas de AWS WAF para sus equilibradores de carga de aplicación y distribuciones de Amazon CloudFront en todas las cuentas de AWS Organizations. A medida que se crean nuevas aplicaciones, Firewall Manager también permite a los clientes que las nuevas aplicaciones y recursos estén en conformidad con un conjunto común de reglas de seguridad desde el primer día.

AWS Global Accelerator

AWS Global Accelerator es un servicio de redes que mejora la disponibilidad y el rendimiento de las aplicaciones que los clientes ofrecen a sus usuarios globales. AWS Global Accelerator también facilita la administración de las aplicaciones globales de los clientes mediante la provisión de direcciones IP estáticas que actúan como un punto de entrada fijo a las aplicaciones de los clientes alojadas en AWS, lo que elimina la complejidad de administrar direcciones IP específicas para distintas AZ y regiones de AWS.

AWS Glue

AWS Glue es un servicio de extracción, transformación y carga (ETL) que facilita a los clientes la preparación y la carga de los datos para su análisis. Los clientes pueden crear y ejecutar un trabajo de ETL con solo unos clics en la consola de administración de AWS.

AWS Glue DataBrew

AWS Glue DataBrew es una herramienta de preparación de datos visual que pueden utilizar los analistas de datos y científicos de datos para limpiar y normalizar los datos con facilidad a fin de prepararlos para el análisis y el machine learning. Los clientes pueden elegir desde transformaciones estandarizadas hasta tareas de preparación de datos automatizadas, sin la necesidad de escribir ningún código.

Panel de AWS Health

El panel de AWS Health proporciona alertas y una orientación de corrección cuando AWS experimenta eventos que podrían afectar a los clientes. Mientras que el panel de AWS Health muestra el estado general de los servicios de AWS, ofrece a los clientes una vista personalizada del rendimiento y la disponibilidad de los servicios de AWS subyacentes a los recursos de AWS del cliente.

En el panel, se muestra información pertinente y oportuna para ayudar a los clientes a administrar los eventos en curso. Además, se brindan notificaciones proactivas que los ayudan a planificar las actividades programadas. Con el panel de AWS Health, se activan alertas a partir de los cambios en el estado de los recursos de AWS, lo que proporciona visibilidad de los eventos y orientación para ayudar a diagnosticar y resolver rápidamente los problemas.

AWS HealthImaging

AWS HealthImaging es un servicio que ayuda a las organizaciones del sector de la salud y las ciencias biológicas, así como a sus socios de software, a almacenar, analizar y compartir datos de diagnóstico por imagen a una escala de petabytes. Con HealthImaging, los clientes pueden reducir el costo total de propiedad (TCO) de sus aplicaciones de generación de imágenes médicas hasta en un 40 % mediante la ejecución de sus aplicaciones de generación de imágenes médicas desde una copia única de los datos de generación de imágenes de los pacientes en la nube. Con latencias de recuperación de imágenes de menos de un segundo para los datos activos y archivados, los clientes pueden obtener los ahorros de costos de la nube sin sacrificar el rendimiento en el punto de atención. HealthImaging elimina la carga que implica

administrar la infraestructura para los flujos de trabajo de generación de imágenes de los clientes, de modo que puedan centrarse en brindar una atención de calidad a los pacientes.

AWS HealthLake

AWS HealthLake es un servicio que ofrece a las empresas de atención médica y de ciencias biológicas una visión completa de los datos sanitarios individuales o de la población de pacientes para su consulta y análisis a escala. Mediante las API de HealthLake, las organizaciones sanitarias pueden copiar fácilmente los datos de salud, como los informes médicos de imágenes o las notas de los pacientes, de los sistemas en las instalaciones a un lago de datos seguro en la nube. HealthLake utiliza modelos de machine learning (ML) para comprender y extraer automáticamente información médica significativa de los datos sin procesar, como medicamentos, procedimientos y diagnósticos. HealthLake organiza e indexa la información y la almacena en el formato estándar del sector, recursos rápidos de interoperabilidad sanitaria (FHIR), para ofrecer una visión completa de la historia clínica de cada paciente.

AWS HealthOmics

AWS HealthOmics ayuda a las organizaciones de atención médica y de ciencias biológicas a procesar, almacenar y analizar datos genómicos y otros datos ómicos a escala. El servicio admite una amplia gama de casos de uso, incluida la secuenciación de ADN y ARN (genómica y transcriptómica), la predicción de la estructura de proteínas (proteómica) y más. Gracias a que simplifica la administración de la infraestructura para los clientes y elimina el trabajo pesado indiferenciado, HealthOmics permite a los clientes obtener información más profunda a partir de sus datos ómicos, mejorar los resultados de la atención médica y lograr avances en descubrimientos científicos.

HealthOmics se basa en tres componentes de servicio. El almacenamiento de Omics ingiere de manera eficiente datos genómicos sin procesar en la nube y utiliza la compresión específica del dominio para ofrecer precios de almacenamiento atractivos a los clientes. También les ofrece la posibilidad de acceder sin problemas a sus datos desde varios entornos de computación. Los flujos de trabajo de Omics ejecutan flujos de trabajo bioinformáticos a escala en un entorno de computación completamente administrado. Es compatible con tres lenguajes de flujo de trabajo comunes específicos del dominio de la bioinformática. El análisis de Omics almacena datos de variantes y anotaciones genómicas y permite a los clientes realizar consultas y análisis a escala de manera eficiente.

AWS IAM Identity Center

AWS IAM Identity Center es un servicio basado en la nube que simplifica la administración del acceso SSO a las cuentas de AWS y a las aplicaciones empresariales. Los clientes pueden controlar el acceso SSO y los permisos de usuario en todas sus cuentas de AWS en AWS Organizations. Además, pueden administrar el acceso a aplicaciones populares de la empresa y aplicaciones personalizadas que son compatibles con Security Assertion Markup Language (SAML) 2.0. Además, AWS IAM Identity Center ofrece un portal de usuario en el que se pueden buscar todas las cuentas de AWS asignadas, aplicaciones empresariales y aplicaciones personalizadas en un solo lugar.

AWS Identity and Access Management (IAM)

AWS Identity and Access Management es un servicio web que ayuda a los clientes a controlar de forma segura el acceso a los recursos de AWS para sus usuarios. Con IAM, los clientes pueden controlar quién puede utilizar sus recursos de AWS (autenticación), y qué recursos pueden utilizar y de qué forma (autorización). Los clientes pueden permitir a otras personas administrar y usar recursos en sus cuentas de AWS sin tener que compartir sus contraseñas o claves de acceso. Además, pueden otorgar distintos

permisos a personas diferentes para recursos diferentes. Los clientes pueden usar las características de IAM para dar de forma segura a las aplicaciones que se ejecutan en instancias de EC2 las credenciales necesarias para acceder a otros recursos de AWS, como buckets de S3 y bases de datos de RDS o DynamoDB.

AWS IoT Core

AWS IoT Core es un servicio en la nube administrado que permite a los dispositivos conectados interactuar de manera fácil y segura con las aplicaciones en la nube y otros dispositivos. Provee comunicación segura y procesamiento de datos en distintos tipos de ubicaciones y dispositivos conectados, de modo que los clientes puedan crear aplicaciones de IoT con facilidad, como soluciones industriales y soluciones de hogar conectado.

AWS IoT Device Defender

AWS IoT Device Defender es un servicio de seguridad que permite a los clientes auditar la configuración de sus dispositivos, supervisar los dispositivos conectados para detectar comportamientos anormales y mitigar los riesgos de seguridad. Ofrece a los clientes la capacidad de aplicar políticas de seguridad coherentes en toda su flota de dispositivos de AWS IoT y responder con rapidez cuando los dispositivos se ven comprometidos. AWS IoT Device Defender proporciona herramientas para identificar problemas de seguridad y desviaciones de las prácticas recomendadas. AWS IoT Device Defender puede auditar flotas de dispositivos para garantizar que cumplan las prácticas recomendadas de seguridad y detectar comportamientos anormales en los dispositivos.

AWS IoT Device Management

AWS IoT Device Management provee a los clientes la capacidad de presentar, organizar y administrar de forma remota y segura dispositivos de IoT a escala. Con AWS IoT Device Management, los clientes pueden registrar sus dispositivos conectados de manera individual o masiva, así como administrar los permisos para que los dispositivos permanezcan seguros.

También pueden organizar los dispositivos, monitorear y solucionar los problemas de su funcionalidad, consultar el estado de cualquier dispositivo IoT de su flota y enviar actualizaciones de firmware por vía inalámbrica (OTA, over-the-air). AWS IoT Device Management es independiente de cualquier tipo de dispositivo y sistema operativo, por lo que los clientes pueden administrar dispositivos de todo tipo, desde microcontroladores restringidos hasta autos conectados, todo con el mismo servicio. AWS IoT Device Management permite a los clientes escalar sus flotas y reducir el costo y el esfuerzo de administrar implementaciones de dispositivos de IoT grandes y diversas.

AWS IoT Events

AWS IoT Events es un servicio que detecta eventos en miles de sensores de IoT que envían distintos datos de telemetría, como la temperatura de un congelador, la humedad de un equipo de protección respiratorio y la velocidad de la correa de un motor. Los clientes pueden seleccionar los orígenes de datos pertinentes que desean capturar, definir la lógica de cada evento usando afirmaciones simples del tipo 'if-then-else' y seleccionar la alerta o personalizar la acción de respuesta cuando ocurre un evento. De manera continua, IoT Events monitorea datos de varios sensores y aplicaciones de IoT y se integra con otros servicios, como AWS IoT Core, para habilitar la detección precoz e información única sobre los eventos. IoT Events desencadena alertas y acciones de forma automática en respuesta a eventos con base en la lógica definida para resolver problemas con rapidez, reducir los costos de mantenimiento y aumentar la eficiencia operativa.

AWS IoT Greengrass

AWS IoT Greengrass amplía sin interrupciones AWS a los dispositivos periféricos para que puedan actuar de forma local y conforme a los datos que generan, a la vez que utiliza la nube para la gestión, el análisis y el almacenamiento duradero. Con AWS IoT Greengrass, los dispositivos conectados pueden ejecutar funciones de AWS Lambda, ejecutar predicciones con base en los modelos de machine learning, mantener los datos de los dispositivos sincronizados y comunicarse con otros dispositivos de forma segura, incluso cuando no están conectados a Internet.

AWS IoT SiteWise

AWS IoT SiteWise es un servicio que habilita a las empresas industriales a recopilar, almacenar, organizar y visualizar miles de flujos de datos de sensores en múltiples instalaciones industriales. AWS IoT SiteWise incluye un software que se ejecuta en un dispositivo de puerta de enlace que se encuentra en una instalación, recopila continuamente los datos de un servidor historiador o industrial especializado y los envía a la nube de AWS. Con este servicio, los clientes pueden evitar meses de desarrollo de soluciones no diferenciadas de recopilación y catalogación de datos y centrarse en el uso de sus datos para detectar y solucionar problemas en los equipos, detectar ineficiencias y mejorar el rendimiento de la producción.

AWS IoT TwinMaker

AWS IoT TwinMaker facilita a los desarrolladores la creación de gemelos digitales de sistemas reales, como edificios, fábricas, equipos industriales y líneas de producción. AWS IoT TwinMaker proporciona las herramientas que los clientes necesitan para crear gemelos digitales que ayudan a optimizar las operaciones de los edificios, aumentar la producción y mejorar el rendimiento de los equipos. Con la capacidad de utilizar los datos existentes de varias fuentes, crear representaciones virtuales de cualquier entorno físico y combinar los modelos 3D existentes con datos reales, los clientes ahora pueden aprovechar los gemelos digitales para crear una visión integral de sus operaciones de forma más rápida y con menos esfuerzo.

AWS Key Management Service (KMS)

AWS Key Management Service (KMS) permite a los usuarios crear y administrar claves criptográficas. Una clase de claves, las claves de KMS, están diseñadas para nunca quedar expuestas en texto plano fuera del servicio. Las claves KMS se pueden usar para cifrar datos enviados directamente al servicio. Las claves de KMS también sirven para proteger otros tipos de claves, como las claves de datos, que el servicio crea y devuelve a la aplicación del usuario para el uso local. AWS KMS solo crea y devuelve claves de datos a los usuarios, pero no las almacena ni administra.

AWS KMS está integrado con varios servicios de AWS para que los usuarios puedan solicitar que los recursos en esos servicios estén cifrados con claves de datos únicas que aprovisiona KMS y que están protegidas con una clave de KMS que el usuario elige cuando se crea el recurso **(Control AWSCA-4.6).** Consulte los servicios incluidos e integrados con KMS en https://aws.amazon.com/kms/. Los servicios integrados utilizan las claves de datos de AWS KMS. Las claves de datos que aprovisiona AWS KMS están cifradas con una clave maestra de 256 bits única para la cuenta del cliente en un modo definido de AES: Advanced Encryption Standard **(Control AWSCA-4.7)**.

Cuando un cliente solicita a AWS KMS crear una clave de KMS, el servicio crea un ID de clave para la clave KMS y un material de clave, denominado clave de respaldo, que se vincula con el ID de clave de la clave KMS. El servicio solo puede utilizar la clave de respaldo de 256 bits para cifrar o descifrar operaciones **(Control AWSCA-4.10).** KMS generará un ID de clave asociado si un cliente decide importar su propia

clave. Si el cliente elige habilitar la rotación de claves para una clave de KMS con una clave de respaldo que generó el servicio, AWS KMS creará una versión nueva de la clave de respaldo para cada evento de rotación, pero el ID de clave seguirá siendo el mismo **(Control AWSCA-4.11).** Todas las operaciones de cifrado futuras con el ID de clave usarán la clave de respaldo más reciente, mientras que todas las versiones anteriores de las claves de respaldo se retienen para descifrar textos cifrados con la versión anterior de la clave. Las claves de respaldo y las claves que importa el cliente están cifradas con claves controladas por AWS cuando se crean o importan y solo se almacenan en el disco en forma cifrada.

Todas las solicitudes a las API de AWS KMS se registran y ponen a disposición en AWS CloudTrail del solicitante y del propietario de la clave. Las solicitudes registradas proporcionan información acerca de quién hizo la solicitud y con qué clave de KMS, y detallan información sobre el recurso de AWS que se protegió mediante el uso de la clave KMS. El cliente puede ver estos eventos de registro una vez que activa AWS CloudTrail en la cuenta **(Control AWSCA-4.8).**

AWS KMS crea y administra varias réplicas distribuidas de las claves de KMS y los metadatos de claves de forma automática para permitir una alta disponibilidad y durabilidad de los datos. Las claves KMS son objetos regionales; las claves KMS solo se pueden usar en la región de AWS donde fueron creadas. Para garantizar la durabilidad, las claves KMS solo se almacenan de forma cifrada en discos persistentes y en dos sistemas de almacenamiento separados. Cuando se requiere una clave de KMS para cumplir con la solicitud de un cliente autorizado, esta se recupera del almacenamiento, se descifra en uno de los numerosos módulos de seguridad reforzados (HSM) de AWS KMS de la región y se usa solo en la memoria para poner en marcha la operación criptográfica (p. ej., cifrar o descifrar). Para cada solicitud de uso de la clave de KMS en el futuro, se requerirá el descifrado de la clave de KMS en la memoria para otro uso único.

Los puntos de conexión de AWS KMS solo son accesibles a través de TLS mediante los siguientes paquetes de algoritmos de cifrado que son compatibles con la propiedad del secreto hacia delante **(Control AWSCA-4.9)**:

- TLS_AES_128_GCM_SHA256
- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES256-SHA384
- ECDHE-RSA-AES256-SHA
- ECDHE-RSA-AES128-SHA256
- DHE-RSA-AES256-SHA256
- DHE-RSA-AES128-SHA256
- DHE-RSA-AES256-SHA
- DHE-RSA-AES128-SHA
- PQ-TLS-1-2-2023-11-29

Por su diseño, nadie puede acceder al material clave de KMS. Las claves de KMS solo están presentes en módulos de seguridad reforzados durante el tiempo necesario para realizar las operaciones criptográficas correspondientes. Los empleados de AWS no tienen ninguna herramienta para recuperar las claves de KMS de esos módulos de seguridad reforzados. Además, se implementan controles de acceso de varias partes en las

operaciones de esos módulos de seguridad reforzados que implican cambiar la configuración del software o incorporar módulos de seguridad reforzados nuevos en el servicio. Estos controles de acceso de varias partes minimizan la posibilidad de que ocurra un cambio no autorizado en los módulos de seguridad reforzados, que se exponga el material de clave fuera del servicio o que se permita el uso no autorizado de las claves del cliente **(Control AWSCA-4.5).** Además, el material de clave utilizado para los procesos de recuperación de desastres con KMS está físicamente protegido para que ningún empleado de AWS pueda obtener acceso **(Control AWSCA-4.12).** Con regularidad, un grupo de operadores autorizados revisan los intentos de acceder a los materiales de claves de recuperación **(Control AWSCA-4.13).** Los roles y las responsabilidades de los custodios criptográficos con acceso a los sistemas que almacenan o utilizan material de clave están formalmente documentados y reconocidos **(Control AWSCA-1.6).**

AWS Lake Formation

AWS Lake Formation es un servicio de lago de datos integrado que facilita la tarea de los clientes en la incorporación, limpieza, catalogación, transformación y protección de sus datos y su disponibilidad para el análisis y el ML. AWS Lake Formation ofrece a los clientes una consola central en la que pueden descubrir orígenes de datos, configurar trabajos de transformación para mover datos a un lago de datos de Amazon Simple Storage Service (S3), eliminar duplicados y hacer coincidir registros, catalogar datos para que las herramientas de análisis puedan acceder a ellos, configurar políticas de acceso y seguridad a los datos, y auditar y controlar el acceso desde los servicios de análisis y ML de AWS. Lake Formation administra automáticamente el acceso a los datos registrados en Amazon S3 a través de servicios como AWS Glue, Amazon Athena, Amazon Redshift, Amazon QuickSight y Amazon EMR para garantizar el cumplimiento de las políticas definidas por el cliente. Con AWS Lake Formation, los clientes pueden configurar y administrar sus lagos de datos sin tener que integrar manualmente varios servicios subyacentes de AWS.

AWS Lambda

AWS Lambda permite a los clientes ejecutar el código sin aprovisionar ni administrar servidores por su cuenta. AWS Lambda utiliza una flota de computación de instancias de Amazon Elastic Compute Cloud (Amazon EC2) en múltiples AZ de una región, lo que ofrece la alta disponibilidad, seguridad, rendimiento y escalabilidad de la infraestructura de AWS.

AWS License Manager

AWS License Manager facilita la administración de licencias en AWS y los servidores en las instalaciones de los proveedores de software. AWS License Manager permite que los administradores de los clientes creen normas personalizadas de otorgamiento de licencias para emular los términos de sus acuerdos de licencia y, luego, ejecuta esas normas cuando se lanza una instancia de EC2. Los administradores del cliente pueden emplear esas normas para limitar las violaciones en el otorgamiento de licencias, como usar más licencias que lo estipulado en el acuerdo o reasignar licencias a distintos servidores a corto plazo. La creación de normas en AWS License Manager también permite a los clientes limitar las vulneraciones de los acuerdos de licencias mediante la detención del lanzamiento de instancias o la notificación de la violación a los administradores del cliente. Los administradores de los clientes obtienen el control de todas sus licencias y también pueden visualizarlas con el panel de AWS License Manager. De esta manera, pueden reducir los riesgos de incumplimientos, errores en los informes y costos adicionales provocados por los excesos con las licencias.

AWS License Manager se integra con los servicios de AWS para simplificar la gestión de las licencias en varias cuentas de AWS, catálogos de TI y en las instalaciones a través de una única cuenta de AWS.

AWS Mainframe Modernization (en vigor a partir del 15 de febrero de 2024)

AWS Mainframe Modernization es un servicio de equipo central elástico y un conjunto de herramientas de desarrollo para migrar y modernizar cargas de trabajo del equipo central y heredadas. Con Mainframe Modernization, los integradores de sistemas pueden ayudar a descubrir sus cargas de trabajo del equipo central y heredadas, evaluar y analizar la preparación para la migración, y planificar proyectos de migración y modernización. Una vez finalizada la planificación, los clientes pueden utilizar las herramientas de desarrollo integradas de Mainframe Modernization para redefinir la plataforma o refactorizar sus cargas de trabajo del equipo central y heredadas, probar el rendimiento y la funcionalidad de las cargas de trabajo y migrar sus datos a AWS.

AWS Managed Services

AWS Managed Services provee gestión continua de una infraestructura de AWS del cliente. AWS Managed Services automatiza actividades habituales como las solicitudes de cambio, el monitoreo, la gestión de parches, la seguridad y los servicios de copias de seguridad, y también brinda servicios durante todo el ciclo de vida para aprovisionar, ejecutar y respaldar la infraestructura de los clientes.

AWS Network Firewall

AWS Network Firewall es un servicio de detección y prevención de intrusos administrado con estado y Network Firewall para las Virtual Private Cloud (VPC) del cliente. Con este servicio, los clientes pueden filtrar el tráfico en el perímetro de sus VPC. Esto incluye filtrar el tráfico de entrada y salida de una puerta de enlace de Internet, una puerta de enlace de NAT o a través de una VPN o AWS Direct Connect.

AWS OpsWorks (incluye Chef Automate, Puppet Enterprise)

AWS OpsWorks para Chef Automate es un servicio de gestión de la configuración que aloja Chef Automate, un paquete de herramientas de automatización de Chef para la gestión de la configuración, el cumplimiento y seguridad y la implementación continua. OpsWorks también mantiene el servidor Chef de los clientes mediante la aplicación de parches, la actualización y la creación de copias de seguridad automáticas de sus servidores. Con OpsWorks, los clientes ya no necesitan operar sus propios sistemas de gestión de la configuración o preocuparse por mantener su infraestructura. Da a los clientes acceso a todas las características de Chef Automate, como gestión de la configuración y conformidad, donde los clientes administran a través de la consola de Chef o herramientas de la línea de comandos como Knife. También funciona de forma ininterrumpida con los libros de recetas de Chef existentes.

AWS OpsWorks para Puppet Enterprise es un servicio de gestión de la configuración que aloja Puppet Enterprise, un conjunto de herramientas de automatización de Puppet para gestionar infraestructuras y aplicaciones. OpsWorks también mantiene el servidor maestro Puppet de los clientes mediante la aplicación de parches, la actualización y la creación de copias de seguridad automáticas de los servidores de los clientes. Con OpsWorks, los clientes ya no necesitan operar sus propios sistemas de gestión de la configuración o preocuparse por mantener su infraestructura. Otorga a los clientes acceso a todas las características de Puppet Enterprise, que los clientes administran a través de la consola de Puppet. También funciona de forma ininterrumpida con el código de Puppet existente.

AWS OpsWorks Stacks

AWS OpsWorks Stacks es un servicio de gestión de aplicaciones y servidores. Permite a los clientes administrar las aplicaciones y los servidores en AWS y en las instalaciones. Con OpsWorks Stacks, los clientes pueden modelar sus aplicaciones como una pila que contiene distintas capas, como el balanceador de carga, la base de datos y el servidor de la aplicación. Pueden implementar y configurar las instancias de Amazon EC2 en cada capa o conectar con otros recursos como bases de datos de Amazon RDS. OpsWorks Stacks también permite a los clientes configurar el escalado automático para sus servidores con base en cronogramas ya configurados o en respuesta a cambios en los niveles de tráfico. Además, utiliza enlaces de ciclo de vida para orquestar cambios a medida que el entorno escala.

AWS Organizations

AWS Organizations ayuda a los clientes a controlar de forma centralizada sus entornos a medida que crecen y escalan las cargas de trabajo en AWS. Ya sea que formen parte de una empresa emergente en crecimiento o de una empresa grande, Organizations los ayudará a administrar la facturación; controlar el acceso, la conformidad y la seguridad; y compartir los recursos entre todas las cuentas de AWS de forma centralizada.

Con AWS Organizations, los clientes pueden automatizar la creación de cuentas, crear grupos de cuentas para reflejar las necesidades de la empresa y aplicar políticas para esos grupos con el fin de controlarlos. Los clientes también pueden simplificar la facturación a través de la configuración de un único método de pago para todas sus cuentas de AWS. A través de las integraciones con otros servicios de AWS, los clientes pueden usar Organizations para definir configuraciones centrales y compartir recursos en las cuentas en sus organizaciones.

AWS Outposts

AWS Outposts es un servicio que lleva la infraestructura de AWS, los servicios de AWS, las API y las herramientas a cualquier centro de datos, lugar de coubicación o instalación física para una experiencia híbrida verdaderamente coherente. AWS Outposts es ideal para cargas de trabajo que requieren un acceso de baja latencia a los sistemas en las instalaciones, al procesamiento de datos local o al almacenamiento de datos local. Outposts ofrece los mismos servicios, infraestructura de hardware, API y herramientas de AWS para crear y ejecutar aplicaciones en las instalaciones y en la nube. La computación, el almacenamiento, las bases de datos y otros servicios de AWS se ejecutan de forma local en Outposts y los clientes pueden acceder al rango total de servicios de AWS disponibles en la región para crear, administrar y escalar aplicaciones en las instalaciones. Service Link se establece entre Outposts y la región de AWS a través de una conexión de VPN protegida en la Internet pública o AWS Direct Connect **(Control AWSCA-3.17)**.

AWS Outposts está configurado con una Nitro Security Key (NSK, clave de seguridad Nitro), que está diseñada para cifrar el contenido del cliente y permitirle eliminar de forma mecánica el contenido del dispositivo. El contenido del cliente se destruye por vía criptográfica si el cliente elimina la NSK de un dispositivo Outpost **(Control AWSCA-7.9)**.

Para obtener información adicional sobre seguridad en AWS Outposts, incluido el modelo de responsabilidad compartida, consulte la Guía del usuario de AWS Outposts.

AWS Payment Cryptography (en vigor a partir del 15 de febrero de 2024)

AWS Payment Cryptography es un servicio administrado que puede utilizarse para sustituir las funciones de criptografía y administración de claves específicas de los pagos que suelen proporcionar los harware security modules (HSM, módulos de seguridad de hardware) de pago en las instalaciones. Este servicio API de AWS, elástico y de pago por uso, permite que las aplicaciones de procesamiento de créditos, débitos y pagos se trasladen a la nube sin necesidad de HSM de pago dedicados.

AWS Private Certificate Authority

AWS Private Certificate Authority (CA) es un servicio de CA privado administrado que habilita a los clientes a administrar de forma fácil y segura el ciclo de vida de sus certificados privados. Private CA permite que los desarrolladores sean más ágiles al proporcionarles API para crear e implementar certificados privados de forma programática. Los clientes también tienen la flexibilidad de crear certificados privados para las aplicaciones que requieren tiempos de vida de certificados o nombres de recursos personalizados. Con Private CA, los clientes pueden crear y administrar certificados privados para sus recursos conectados en un solo lugar con un servicio de CA privado administrado, seguro y de pago por uso.

AWS Resilience Hub

AWS Resilience Hub ayuda a los clientes a mejorar la resiliencia de sus aplicaciones y a reducir las interrupciones de ellas mediante la detección de debilidades relacionadas con la resiliencia y la evaluación y validación continua de esta. AWS Resilience Hub también puede proporcionar procedimientos operativos estándar (SOP) para ayudar a recuperar las aplicaciones en AWS cuando se producen interrupciones no planificadas debido a problemas de software, despliegue u operaciones. El servicio está diseñado para aplicaciones nativas en la nube que utilizan servicios de AWS de alta disponibilidad y tolerantes a errores como componentes básicos.

AWS Resource Access Manager (RAM)

AWS Resource Access Manager ayuda a los clientes a compartir de forma segura sus recursos entre las cuentas de AWS, dentro de su organización o en unidades organizativas (OU, organizational units) en AWS Organizations, y con los roles y usuarios de IAM para los tipos de recursos compatibles. Los clientes pueden utilizar AWS Resource Access Manager para compartir puertas de enlace de tránsito, subredes, configuraciones de licencias de AWS License Manager, reglas de Amazon Route 53 Resolver y otros tipos de recursos.

AWS Resource Groups

AWS Resource Groups es un servicio que ayuda a los clientes a organizar los recursos de AWS en grupos lógicos. Estos grupos pueden representar una aplicación, un componente de software o un entorno. Los Resource Groups pueden incluir más de cincuenta tipos de recursos adicionales, por lo que la cantidad total de tipos de recursos compatibles alcanza los setenta y siete. Algunos de estos tipos de recursos nuevos incluyen tablas de Amazon DynamoDB, funciones de AWS Lambda, trazas de AWS CloudTrail y muchos más. Ahora los clientes pueden crear grupos de recursos que reflejan de forma precisa sus aplicaciones y actuar en función de esos grupos y no de recursos individuales.

AWS RoboMaker

AWS RoboMaker es un servicio que facilita el desarrollo, la prueba y la implementación de aplicaciones de robótica inteligentes a escala. RoboMaker amplía el marco de software de robótica con código abierto más utilizado, Robot Operating System (ROS), gracias a la conectividad con los servicios en la nube. Esto incluye servicios de machine learning de AWS, servicios de monitoreo y servicios de análisis que permiten

a un robot transmitir datos, navegar, comunicar, entender y aprender. RoboMaker provee un entorno de desarrollo de robótica para desarrollar aplicaciones, un servicio de simulación de robótica para acelerar las pruebas de las aplicaciones y un servicio de gestión de flotas de robots para implementar, actualizar y administrar aplicaciones de forma remota.

AWS Secrets Manager

AWS Secrets Manager ayuda a los clientes a proteger los secretos necesarios para acceder a sus aplicaciones, servicios y recursos de TI. El servicio permite a los clientes rotar, administrar y recuperar con facilidad las credenciales de la base de datos, las claves de API y otros secretos a lo largo de su ciclo de vida. Los usuarios y las aplicaciones recuperan secretos con una llamada a las API de Secrets Manager, lo que elimina la necesidad de crear códigos rígidos para la información confidencial en texto plano. Secrets Manager ofrece rotación de secretos con integración incorporada para Amazon RDS, Amazon Redshift y Amazon DocumentDB. El servicio también se extiende a otros tipos de secretos, como claves de API y tokens OAuth. Además, Secrets Manager permite a los clientes controlar el acceso a los secretos usando permisos detallados y auditar la rotación de secretos de manera centralizada para los recursos en la nube de AWS, servicios de terceros y en las instalaciones.

AWS Security Hub

AWS Security Hub brinda a los clientes una vista integral de las alertas de seguridad de alta prioridad y el estado de conformidad en todas las cuentas de AWS. Hay una gama de herramientas de seguridad potentes a disposición de los clientes, desde firewalls y protección de puntos de conexión hasta escáneres de vulnerabilidades y cumplimiento. Con Security Hub, los clientes ahora cuentan con un lugar único que agrupa, organiza y prioriza las alertas de seguridad o los resultados de diferentes servicios de AWS, como Amazon GuardDuty, Amazon Inspector Classic y Amazon Macie, así como también soluciones de socios de AWS. Los resultados se resumen de forma visual en paneles integrados con gráficos y tablas accionables.

AWS Server Migration Service (SMS) (obsoleto el 1 de abril de 2024)

AWS Server Migration Service (SMS) es un servicio sin agentes que facilita y agiliza para los clientes la migración de miles de cargas de trabajo en las instalaciones de AWS. AWS SMS permite a los clientes automatizar, programar y hacer un seguimiento de las replicaciones progresivas de los volúmenes de servidores en vivo, lo que facilita la coordinación de migraciones de servidores a gran escala.

AWS Serverless Application Repository

AWS Serverless Application Repository es un repositorio administrado para aplicaciones sin servidor. Permite a los equipos, las organizaciones y los desarrolladores almacenar y compartir aplicaciones reutilizables, como así también armar e implementar con facilidad arquitecturas sin servidor de una manera novedosa y eficaz. Con Serverless Application Repository, los clientes no necesitan clonar, crear, empaquetar ni publicar código fuente en AWS antes de la implementación. En cambio, utilizan aplicaciones ya armadas de Serverless Application Repository en sus arquitecturas sin servidor, lo que los ayuda a reducir el trabajo duplicado, garantizar las prácticas recomendadas de la organización y salir al mercado más rápido. La integración con AWS Identity and Access Management (IAM) provee control al nivel del recurso de cada aplicación, lo que permite a los clientes compartir las aplicaciones de manera pública con todos o de forma privada con cuentas de AWS específicas.

AWS Service Catalog

AWS Service Catalog permite a los clientes crear y administrar catálogos de servicios de TI que están aprobados para su uso en AWS. Estos servicios de TI pueden incluir de todo, desde imágenes de máquinas virtuales, servidores, software y bases de datos hasta arquitecturas completas de aplicaciones de varios niveles. AWS Service Catalog no solo permite a los clientes administrar de manera centralizada los servicios de TI comúnmente implementados, sino que también los ayuda a lograr un gobierno consistente y cumplir sus requisitos de conformidad, a la vez que les permite a los usuarios implementar con rapidez los servicios de TI aprobados que necesitan.

AWS Shield

AWS Shield es un servicio de protección administrado contra Distributed Denial of Service (DDoS, denegaciones de servicio distribuidas) que protege las aplicaciones web que se ejecutan en AWS. AWS Shield proporciona detección siempre activa y mitigación automática incorporada que minimizan el tiempo de inactividad y la latencia de las aplicaciones, para que no tenga que contratar AWS Support para beneficiarse de la protección ante los DDoS.

AWS Signer

AWS Signer es un servicio de firma de código administrado que asegura la confianza y la integridad del código del cliente. Los clientes validan el código en función de una firma digital para confirmar que el código no ha sido alterado y proviene de un publicador de confianza. Con AWS Signer, los administradores de seguridad de los clientes tienen un sitio único para definir el entorno de firma, lo que incluye qué rol de AWS Identity and Access Management (IAM) puede firmar el código y en qué regiones. AWS Signer administra las claves públicas y privadas del certificado de firma del código y permite la gestión central del ciclo de vida de la firma del código.

AWS Snowball

Snowball es una solución de traslado de datos a escala de petabytes que utiliza aparatos seguros para transferir grandes cantidades de datos dentro y fuera de la nube de AWS. Con Snowball, se abordan los desafíos comunes que presentan las transferencias de datos a gran escala, incluidos los altos costos de la red, los largos tiempos de transferencia y los problemas de seguridad. Transferir datos con Snowball es simple y seguro.

AWS Snowball Edge (obsoleto el 1 de julio de 2024)

AWS Snowball Edge es un dispositivo de 100 TB para transferir datos con capacidades de almacenamiento y computación integradas. Los clientes pueden usar Snowball Edge para transferir grandes cantidades de datos dentro y fuera de AWS, como una capa de almacenamiento transitorio para conjuntos de datos locales grandes o para admitir cargas de trabajo locales en ubicaciones remotas o sin conexión. Snowball Edge se conecta con las aplicaciones y la infraestructura existentes de los clientes mediante interfaces de almacenamiento estándar, lo que optimiza el proceso de transferencia de datos y minimiza la configuración y la integración. Snowball Edge permite formar clústeres que conforman un nivel de almacenamiento local y procesar los datos de los clientes en las instalaciones, lo que ayuda a garantizar que sus aplicaciones continúen ejecutándose incluso cuando no pueden acceder a la nube.

AWS Snowmobile (obsoleto el 1 de abril 2024)

AWS Snowmobile es un servicio de transferencia de datos a escala de exabytes, que se utiliza para transferir cantidades de datos extremadamente grandes a AWS. Los clientes pueden transferir sus exabytes de datos a través de un contenedor de envío reforzado de 13,71 metros de longitud,

transportado por un camión semirremolque. Snowmobile facilita el traspaso de volúmenes de datos masivos a la nube, lo que incluye bibliotecas de videos, repositorios de imágenes e incluso la migración de un centro de datos completo. Una vez cargados los datos del cliente, Snowmobile regresa a AWS, donde los datos se importan a Amazon S3 o Amazon Glacier.

AWS Step Functions

AWS Step Functions es un servicio web que permite que los clientes coordinen los componentes de microservicios y aplicaciones distribuidas mediante el uso de flujos de trabajo visuales. Los clientes pueden crear aplicaciones a partir de componentes individuales que realizan una función o tarea discretas, lo que permite escalar y cambiar las aplicaciones con rapidez. Step Functions proporciona una manera confiable de coordinar los componentes y navegar las funciones de la aplicación de un cliente. Proporciona una consola gráfica para visualizar los componentes de la aplicación de un cliente en una serie de pasos. De forma automática, Step Functions desencadena cada paso y realiza un seguimiento de ellos. Cuando se produce un error, vuelve a intentarlo de modo que la aplicación de los clientes siempre se ejecute en orden y de la manera esperada. Dado que registra el estado de cada paso, cuando algo sale mal, los clientes pueden diagnosticar los problemas y depurarlos con rapidez.

AWS Storage Gateway

El servicio AWS Storage Gateway conecta los dispositivos de software fuera de la nube de los clientes con el almacenamiento basado en la nube. El servicio permite a las organizaciones almacenar datos en los servicios de almacenamiento en la nube de larga duración de AWS, como Amazon S3 y Amazon Glacier.

AWS Storage Gateway realiza una copia de seguridad de los datos fuera de las instalaciones en Amazon S3 en la forma de instantáneas de Amazon EBS. Además, transfiere datos a AWS y los almacena en Amazon S3 o Amazon Glacier, según el caso de uso y el tipo de puerta de enlace utilizada. Hay tres tipos de puertas de enlace: de volumen, de cinta y de archivo. La puerta de enlace de cinta permite a los clientes almacenar datos a los que se accede con más frecuencia en Amazon S3 y con menos frecuencia en Amazon Glacier.

La puerta de enlace de archivo permite a los clientes copiar datos a S3 y hacerlos aparecer como objetos individuales en S3. Las puertas de enlace de volumen almacenan datos directamente en Amazon S3 y permiten a los clientes sacar una instantánea de sus datos para poder acceder a las versiones anteriores de estos. Estas instantáneas se capturan como Amazon EBS Snapshots, que también se almacenan en Amazon S3. Tanto Amazon S3 como Amazon Glacier almacenan de manera redundante estas instantáneas de diversos dispositivos en varias instalaciones, lo que contribuye a la detección de cualquier pérdida de redundancia y a su correspondiente reparación. La instantánea de Amazon EBS proporciona una copia de seguridad en un momento dado que puede volver a almacenarse fuera de la nube o en una puerta de enlace que se ejecuta en Amazon EC2, o usarse para crear instancias de nuevos volúmenes de Amazon EBS. Los datos se almacenan dentro de una única región que especifican los clientes.

AWS Systems Manager

AWS Systems Manager otorga a los clientes visibilidad y control sobre sus infraestructuras en AWS. Además, les brinda una interfaz de usuario unificada para que puedan visualizar sus datos operativos desde diversos servicios de AWS. Por otra parte, los clientes pueden automatizar tareas operativas en todos los recursos de AWS.

Con AWS Systems Manager, los clientes pueden agrupar recursos por aplicación, como las instancias de Amazon EC2, los buckets de Amazon S3 o las instancias de Amazon RDS, ver los datos operativos para monitorear los grupos de recursos, solucionar sus problemas y tomar medidas sobre ellos.

AWS Transfer Family

AWS Transfer Family permite transferir archivos directamente a Amazon S3 y sacarlos. Con el respaldo del Secure File Transfer Protocol (SFTP), también conocido como Secure Shell (SSH) File Transfer Protocol, el File Transfer Protocol over SSL (FTPS) y el File Transfer Protocol (FTP), AWS Transfer Family ayuda a los clientes a migrar sin interrupciones sus flujos de trabajo de transferencia de archivos a AWS gracias a la integración con sistemas de autenticación existentes y la provisión de enrutamiento de DNS con Amazon Route 53.

Notificaciones de usuarios de AWS

Notificaciones de usuarios de AWS permite a los usuarios configurar y visualizar de forma centralizada las notificaciones de los servicios de AWS, como los eventos de AWS Health, las alarmas de Amazon CloudWatch o los cambios de estado de las instancias de EC2, en un formato coherente y fácil de usar. Los usuarios pueden ver las notificaciones de todas las cuentas, regiones y servicios en un centro de notificaciones de la consola y configurar los canales de entrega, como el correo electrónico, el chat y las notificaciones push en la aplicación para dispositivos móviles de la Consola de AWS, donde pueden recibir estas notificaciones. Las notificaciones proporcionan direcciones URL para dirigir a los usuarios a los recursos de la consola de administración a fin de habilitar la toma de medidas y soluciones.

Acceso verificado de AWS (en vigor desde el 15 de agosto de 2024)

Acceso verificado de AWS es un servicio que permite asegurar el acceso a las aplicaciones sin necesidad de utilizar una red privada virtual (VPN). Acceso verificado evalúa cada solicitud de aplicación y ayuda a garantizar que los usuarios puedan acceder a cada aplicación solo cuando cumplen los requisitos de seguridad especificados.

AWS WAF

AWS WAF es un firewall de aplicaciones web que ayuda a proteger las aplicaciones web frente a ataques web comunes que pueden afectar la disponibilidad de la aplicación, poner en riesgo la seguridad o consumir demasiados recursos.

Los clientes pueden usar AWS WAF para crear reglas personalizadas que bloqueen patrones de ataque comunes, como inyección de código SQL o scripting entre sitios, y reglas diseñadas para aplicaciones específicas. Se pueden implementar estas reglas en cuestión de minutos, lo que permite a los clientes responder con rapidez a los cambios en los patrones del tráfico. Además, AWS WAF incluye una API con todas las características, la cual pueden utilizar los clientes para automatizar la creación, la implementación y el mantenimiento de las reglas de seguridad.

AWS Wickr

AWS Wickr es un servicio cifrado de extremo a extremo que ayuda a las organizaciones a colaborar de forma segura mediante mensajes individuales y grupales, llamadas de voz y video, uso compartido de archivos y de pantallas, y mucho más. AWS Wickr cifra los mensajes, las llamadas y los archivos con un protocolo de cifrado de extremo a extremo de 256 bits. Solo los destinatarios previstos y la organización del cliente pueden descifrar estas comunicaciones, lo que reduce el riesgo de ataques de adversarios intermedios.

AWS X-Ray

AWS X-Ray ayuda a los desarrolladores a analizar y depurar las aplicaciones distribuidas de producción, como las creadas con una arquitectura de microservicios. Con X-Ray, los clientes o desarrolladores pueden comprender cómo funcionan sus aplicaciones y los servicios subyacentes para identificar y solucionar la causa raíz de los problemas y los errores de rendimiento. X-Ray ofrece una vista integral de las solicitudes a medida que se trasladan a través de su aplicación y muestra un mapa de los componentes subyacentes de su aplicación. Los clientes o desarrolladores pueden usar X-Ray para analizar las aplicaciones tanto en desarrollo como en producción.

EC2 Image Builder

Con EC2 Image Builder, es más fácil automatizar la creación, gestión e implementación de imágenes de servidor "doradas" personalizadas, seguras y actualizadas que se instalan y configuran previamente con software y configuración para cumplir con estándares de TI específicos.

Elastic Load Balancing (ELB)

Elastic Load Balancing (ELB) ofrece a los clientes un equilibrador de carga que distribuye de manera automática el tráfico entrante de la aplicación en varias instancias de Amazon EC2 en la nube. Permite a los clientes alcanzar niveles superiores de tolerancia a errores para sus aplicaciones, lo que proporciona ininterrumpidamente la cantidad requerida de capacidad balanceadora de carga que se precisa para distribuir el tráfico de la aplicación.

FreeRTOS

FreeRTOS es un sistema operativo para microcontroladores que facilita la programación, la implementación, la protección, la conexión y la administración de dispositivos periféricos pequeños y de baja potencia. FreeRTOS amplía el kernel de FreeRTOS, un sistema operativo de código abierto popular para microcontroladores, con bibliotecas de software que facilitan la conexión segura de dispositivos pequeños de baja potencia a los servicios en la nube de AWS como AWS IoT Core o a dispositivos periféricos más potentes que ejecutan AWS IoT Greengrass.

VM Import/Export

VM Import/Export es un servicio que permite a los clientes importar imágenes de máquinas virtuales de su entorno existente a instancias de Amazon EC2 y exportarlas de nuevo al entorno en las instalaciones. Esta oferta permite a los clientes aprovechar sus inversiones actuales en las máquinas virtuales que crearon para cumplir con sus requisitos de seguridad de TI, gestión de la configuración y conformidad, dado que las máquinas virtuales se trasladan a Amazon EC2 como instancias listas para usar. Los clientes también pueden exportar las instancias importadas en su infraestructura de virtualización fuera de la nube, lo que les permite implementar cargas de trabajo en toda su infraestructura de TI.

D.4 Manejo seguro de datos

AWS proporciona muchos métodos para que los clientes manejen sus datos de forma segura. En Controles complementarios de las entidades usuarias (CUEC) al final de esta sección, se detallan los métodos adicionales. AWS permite a los clientes abrir un canal seguro y cifrado en los servidores de AWS mediante HTTPS (TLS/SSL).

Amazon S3 proporciona un mecanismo que permite a los usuarios utilizar sumas de comprobación MD5 para verificar que los datos enviados a AWS son idénticos a los recibidos a nivel de bit, y que los datos que envía Amazon S3 son idénticos a los que recibe el usuario. Cuando los clientes eligen proporcionar sus propias claves para el cifrado y el descifrado de los objetos de Amazon S3 (S3 SSE-C), Amazon S3 no almacena la clave de cifrado que provee el cliente. Amazon S3 genera y almacena un HMAC salado unidireccional de la clave de cifrado del cliente y ese valor de HMAC salado no se registra **(Control AWSCA-4.4).**

Tras iniciar la comunicación con una AMI de Windows provista por AWS, AWS habilita una comunicación segura mediante la configuración de los Terminal Services en la instancia mediante la generación de un certificado de servidor autofirmado único X.509 y la entrega de la huella digital del certificado al usuario a través de un canal seguro **(Control AWSCA-4.2).**

Luego, AWS habilita la comunicación segura con las AMI de Linux, mediante la configuración de SSH en la instancia, la generación de una clave de host única y la entrega de la clave de huella digital al usuario a través de un canal seguro **(Control AWSCA-4.1).**

Las conexiones entre las aplicaciones del cliente y las instancias MySQL de Amazon RDS se pueden cifrar con TLS/SSL. Amazon RDS genera un certificado TLS/SSL para cada instancia de base de datos, que puede usarse para establecer una conexión cifrada usando el cliente MySQL predeterminado. Una vez que se establezca una conexión cifrada, los datos transferidos entre la instancia de base de datos y la aplicación del cliente se cifrarán durante la transferencia. Si los clientes requieren que los datos estén cifrados mientras están “en reposo” en la base de datos, su aplicación debe administrar el cifrado y el descifrado de los datos. Además, los clientes pueden configurar controles para que las instancias de sus bases de datos solo acepten conexiones cifradas para cuentas específicas del usuario.

D.5 Seguridad física y protección ambiental

Amazon tiene considerable experiencia en el diseño, la creación y el manejo de centros de datos a gran escala. Esta experiencia se aplicó al sistema y la infraestructura de AWS. Consulte la sección “Información general del sistema de Amazon Web Services” para ver el listado de centros de datos dentro del alcance.

<u>Seguridad física</u>
AWS solo ofrece acceso físico a sus centros de datos a los empleados y contratistas cuyas necesidades comerciales de poseer tales privilegios sean legítimas. El acceso a los centros de datos debe recibir la aprobación de una persona autorizada **(Control AWSCA-5.1).** Todos los visitantes deberán presentar una identificación, y el personal autorizado los registrará y acompañará.

Cuando un empleado o contratista ya no requiere acceso al centro de datos, su acceso se revoca de inmediato, incluso si sigue siendo empleado o contratista de Amazon o AWS. Además, el acceso se revoca automáticamente cuando finaliza el registro de un empleado o contratista en el sistema de RR. HH. de Amazon **(Control AWSCA-5.2)**. El acceso de los titulares a los centros de datos se revisa trimestralmente. A los titulares de tarjetas marcados para su eliminación, se les revoca automáticamente el acceso como parte de la revisión **(Control AWSCA-5.3).**

El acceso físico se controla tanto en el perímetro como en los puntos de entrada del edificio, donde hay personal de seguridad profesional que utiliza vigilancia por video, sistemas de detección de intrusos y medios electrónicos de identificación con credencial o pin. El personal autorizado emplea mecanismos de

autenticación multifactorial para acceder a las plantas donde están los centros de datos **(Control AWSCA-5.4**, **AWSCA-5.5** y **AWSCA-5.6)**.

Además de los controles de seguridad física, el acceso físico a los centros de datos en la región GovCloud (EE. UU.) está restringido a los empleados o contratistas que fueron validados como residentes de EE. UU. (titulares de una Green Card o ciudadanos según la definición del Departamento de Estado de Estados Unidos).
Amazon es propietario y operador de muchos de sus centros de datos, mientras que otros centros están alojados en espacios de coubicación de diversas empresas prestigiosas bajo contrato con Amazon. AWS también implementa en los espacios de coubicación el acceso físico y los controles de seguridad descritos con anterioridad.

Las zonas locales de AWS son un tipo de implementación de infraestructura administrada y respaldada por AWS que acerca los servicios de computación, almacenamiento, base de datos y otros servicios selectos de AWS a las grandes poblaciones, industrias, centros de TI o a los clientes donde actualmente no existe ninguna región de AWS. Con las zonas locales de AWS, los clientes pueden ejecutar porciones sensibles a la latencia de aplicaciones locales para usuarios finales y recursos en una geografía específica, y ofrecer latencias de milisegundos de un solo dígito para casos de uso específico. Las zonas locales dedicadas se implementan en las instalaciones y se entregan de acuerdo con un contrato específico y exclusivo de un cliente. La seguridad física de estas zonas locales dedicadas cumple los requisitos establecidos por AWS.

AWS ofrece infraestructura de Wavelength en asociación con proveedores de telecomunicaciones, que se optimiza para las aplicaciones de computación de periferia móvil. Las zonas Wavelength son implementaciones de infraestructura de AWS que integran servicios de computación y almacenamiento de AWS dentro de los centros de datos de los proveedores de servicios de comunicaciones (CSP o proveedores de telecomunicaciones) en la periferia de la red 5G, de modo que el tráfico de la aplicación de los dispositivos 5G pueda alcanzar los servidores de la aplicación que se ejecutan en zonas Wavelength sin dejar la red de telecomunicaciones. Esto evita la latencia que se originaría si el tráfico de la aplicación tuviera que atravesar varios saltos en internet para llegar a destino, lo que permite a los clientes aprovechar al máximo los beneficios de latencia y ancho de banda que ofrecen las redes 5G modernas.

Los contratos con proveedores externos de coubicación incluyen disposiciones para respaldar la protección de los activos de AWS y la comunicación a AWS de incidentes o eventos que afecten los activos o a los clientes de Amazon **(Control AWSCA-5.11)**. Además, AWS provee monitoreo del cumplimiento de los estándares de seguridad y operación a través de revisiones periódicas de los proveedores de servicios de coubicación **(Control AWSCA-5.12).** La frecuencia de las revisiones de coubicación se basa en una categorización que depende de los contratos y del nivel de participación con el proveedor de servicios de coubicación.

Los espacios de AWS dentro de los centros de coubicación se instalan con cámaras de televisión de circuito cerrado (CCTV), sistemas de detección de intrusos, y dispositivos de control de acceso que alertan al personal de AWS sobre los accesos y los incidentes, cuyas implementaciones están operadas por AWS. El acceso físico a los espacios de AWS dentro de los centros de coubicación está controlado por AWS y sigue los procesos de gestión del acceso estándar de AWS.

Redundancia

Los centros de datos están diseñados para anticipar y tolerar errores mientras mantienen los niveles de servicio. Cada región de AWS cuenta con varios centros de datos. Todos los centros de datos se encuentran en línea y a disposición de los clientes; ninguno de ellos está "inactivo". En caso de error, los procesos automatizados alejan el tráfico del área afectada. Las aplicaciones centrales se implementan en un estándar N+1, de forma que, en el caso de que se produzca un error en el centro de datos, haya capacidad suficiente como para permitir que se equilibre la carga de tráfico entre los demás sitios.

Detección y extinción de incendios

Se han instalado equipos automáticos de detección y extinción de incendios para reducir los riesgos. El sistema de detección de incendios utiliza sensores de detección de humo (por ejemplo, detección de humo por aspiración multipunto [VESDA], detección de punto de origen) en todos los entornos de centros de datos propiedad de Amazon, así como también en espacios de infraestructura mecánica y eléctrica, salas de refrigeración y salas de equipos generadores. Estas áreas están protegidas por sistemas de rociadores de húmedos, de acción previa con interbloqueo doble o de sistema gaseoso **(Control AWSCA-5.7).**

Energía

Los sistemas de electricidad de los centros de datos que utiliza AWS están diseñados para ser totalmente redundantes y sostenibles sin generar ningún impacto en las operaciones las 24 horas del día. Además, las unidades de Sistema de alimentación ininterrumpida (UPS) proveen alimentación de respaldo en caso de una falla eléctrica para cargas críticas y esenciales en los centros de datos de Amazon y los sitios de coubicación de terceros donde Amazon conserva las unidades de UPS. Los centros de datos propiedad de Amazon utilizan generadores para proveer energía de respaldo a las instalaciones. **(Control AWSCA-5.9** y **AWSCA-5.10)**.

Clima y temperatura

Se debe controlar el clima a fin de mantener una temperatura operativa regulada para los servidores y otro hardware, lo que evita el sobrecalentamiento y reduce la posibilidad de interrupciones en el servicio. Los centros de datos propiedad de Amazon están climatizados para mantener las condiciones ambientales en niveles específicos. El personal y los sistemas monitorean y controlan la temperatura y la humedad en niveles apropiados. Esto se proporciona en N+1 y utiliza la refrigeración libre como fuente primaria de refrigeración cuando esté disponible en función de las condiciones ambientales locales **(Control AWSCA-5.8)**.

Gestión del entorno

En los centros de datos de Amazon, AWS monitorea los sistemas y equipos eléctricos, mecánicos y de asistencia vital para que todos los problemas se identifiquen de inmediato. Esto se lleva a cabo mediante rondas y lecturas diarias, junto con información general de nuestros centros de datos que se proporciona a través del Sistema de Gestión de Edificios (BMS) y el Sistema de Monitoreo Eléctrico (EMS) de AWS. El mantenimiento preventivo se lleva a cabo para mantener la operatividad continua del equipamiento mediante la herramienta de Gestión de Activos Empresariales (EAM), el seguimiento de incidentes y el sistema de Gestión de cambios. El objetivo principal de este proceso es proporcionar una visión holística de los Activos Mecánicos, Eléctricos y de Plomería (MEP), propiedad de los equipos de infraestructura de AWS. Esto incluye la provisión de un repositorio centralizado para los equipos, la optimización del mantenimiento planificado y no planificado, y el manejo de los repuestos críticos del centro de datos.

Gestión de Medios

Cuando un dispositivo de almacenamiento ha llegado al final de su vida útil, los procedimientos de AWS incluyen un proceso de retiro que está diseñado para evitar el acceso no autorizado a los activos. AWS utiliza las técnicas detalladas en la publicación NIST 800-88 ("Directrices para el saneamiento del contenido multimedia") como parte del proceso de retiro. Todos los medios de producción se retiran de forma segura de acuerdo con las prácticas estándar del sector **(Control AWSCA-5.13).** Los medios de producción no se retiran del control de AWS hasta que se hayan retirado de forma segura.

D.6 Administración de cambios

Software

AWS aplica un enfoque sistemático para gestionar los cambios a fin de revisar, probar, aprobar y comunicar los cambios introducidos en los servicios que repercutan en los clientes. Los procesos de gestión de cambios se basan en las directrices de gestión de cambios de Amazon y se adaptan a las especificidades de cada servicio de AWS **(Control AWSCA-6.1).** Estos procesos se documentan y la gestión de equipos de servicio se los comunica al personal necesario.

El objetivo del proceso de gestión de cambios de AWS es evitar interrupciones involuntarias del servicio y mantener la integridad del servicio que se presta al cliente. Los detalles de los cambios se documentan en una de las herramientas de gestión de cambios o de implementación de Amazon **(Control AWSCA-6.2)**.

Antes de la implementación en los entornos de producción, se realiza lo siguiente en los cambios:

- Se desarrollan en un entorno de desarrollo segregado del entorno de producción **(Control AWSCA-6.4)**.
- Se revisan por parte de colegas para comprobar los aspectos técnicos y la idoneidad **(Control AWSCA-6.5)**.
- Se prueban para confirmar que los cambios se comportarán como se espera cuando se apliquen y no afectarán negativamente al rendimiento **(Control AWSCA-6.3)**.
- Reciben la aprobación de los miembros del equipo autorizados para ofrecer la supervisión y el conocimiento adecuados sobre el impacto empresarial **(Control AWSCA-6.5)**.

Los cambios suelen enviarse a la fase de producción con una implementación gradual, empezando por los sitios con el menor nivel de impacto. Las implementaciones son monitoreadas minuciosamente para que pueda evaluarse el impacto. Los propietarios del servicio cuentan con una serie de métricas configurables que miden el estado de las dependencias ascendentes del servicio. Estas métricas son monitoreadas minuciosamente mediante límites y alarmas (por ejemplo, latencia, disponibilidad, errores fatales, uso de CPU, etc.). La información del cliente, incluida su información personal, y el contenido del cliente no son utilizados en entornos de evaluación y desarrollo **(Control AWSCA-6.7).** Los procedimientos de reversión se documentan para que los miembros del equipo puedan revertir al estado anterior de ser necesario.

Cuando es posible, los cambios se programan durante períodos de cambio regulares. Los cambios de emergencia en los sistemas de producción que requieren desviaciones de los procedimientos estándar de gestión de cambios se asocian a un incidente y se registran y aprueban según corresponda.

AWS realiza validaciones de implementación y revisiones de cambios para detectar cambios no autorizados en su entorno, y un seguimiento de los problemas identificados hasta su resolución. La gestión de AWS revisa y realiza mensualmente un seguimiento de las infracciones de implementación de los servicios inscritos en el programa de Monitoreo de Implementaciones como parte de la revisión empresarial de AWS Security. En el caso de los servicios que no están inscritos en el programa de monitoreo de implementación, se lleva a cabo una revisión mensual secundaria de las implementaciones en los 60 días siguientes al mes en que se realizaron. Si se detectan cambios no autorizados o que se desvían del proceso estándar de revisión y aprobación, se hace un seguimiento hasta su resolución **(Control AWSCA-6.6).**

Infraestructura

Cuando se aprovisiona hardware nuevo, se instala un software desarrollado internamente por AWS para administrar la configuración. Estas herramientas se ejecutan en todos los host de UNIX para validar que están configurados y que el software se instaló de manera estándar con base en el tipo de host y se actualiza de manera regular.

Solo los usuarios aprobados con necesidades empresariales verificadas que están autorizados a través del servicio de permisos pueden acceder a los servidores centrales de gestión de la configuración. La configuración de los host se monitorea para comprobar el cumplimiento de los estándares de seguridad de AWS y se envía automáticamente a la flota de hosts **(Control AWSCA-9.4)**.

Los cambios no rutinarios, de emergencia y otros cambios de configuración en la infraestructura existente de AWS están sujetos a autorización, registro, prueba, aprobación y documentación de acuerdo con las normas del sector establecidas para sistemas similares. Las actualizaciones de la infraestructura de AWS se realizan de forma tal que el impacto al cliente y su uso del servicio sea el mínimo posible. AWS se comunica con los clientes, ya sea por correo electrónico o a través del panel de AWS Health (https://status.aws.amazon.com/), en caso de que el uso del servicio pueda verse afectado negativamente.

D.7 Integridad de datos, disponibilidad, redundancia y retención de datos

AWS trata de mantener la integridad de los datos en todas las fases, incluida la transmisión, el almacenamiento y el procesamiento.

Amazon S3 utiliza sumas de comprobación internamente para confirmar la integridad continua de los datos en tránsito dentro del sistema y en reposo. Amazon S3 provee una instalación para que los clientes puedan enviar sumas de comprobación junto con los datos transferidos al servicio. El servicio valida las sumas de comprobación una vez que se hayan recibido los datos para determinar que ninguna corrupción tuvo lugar durante el tránsito. Independientemente de si se envía una suma de comprobación con un objeto a Amazon S3, el servicio usa sumas de comprobación internamente para confirmar la integridad continua de los datos en tránsito dentro del sistema y en reposo. Cuando se detecta corrupción del disco o error del dispositivo, el sistema automáticamente intenta restaurar los niveles normales de redundancia de almacenamiento de objetos **(Control AWSCA-7.1, AWSCA-7.2** y **AWSCA-7.3).**

Los servicios y sistemas de AWS que alojan el contenido de los clientes están diseñados para retener el contenido del cliente hasta que este lo elimine o el acuerdo con el cliente finalice **(Control AWSCA-7.8)**. Una vez que termina la obligación contractual de retener el contenido o tras una acción iniciada por el cliente para remover o eliminar el contenido, los servicios de AWS poseen procesos y procedimientos

para detectar una eliminación y hacer que el contenido sea inaccesible. AWS utiliza Amazon Simple Storage Service (S3), Amazon Elastic Compute Cloud (EC2), Amazon Elastic Block Store (EBS), Amazon DynamoDB, AWS Key Management Service (KMS) y AWS CloudHSM como los servicios principales para almacenar el contenido de los clientes, que de forma individual o combinada, también se utilizan en muchos de los demás servicios de AWS enumerados en la Información general del sistema para el almacenamiento de contenido del cliente. Amazon S3 Glacier, Amazon Relational Database Service (RDS) Aurora, SimpleDB, Amazon Simple Queue Service (SQS), Amazon Cloud Directory, Amazon Pinpoint y End User Messaging, AWS Secrets Manager, Amazon Elastic File System (EFS) y Amazon CloudFront utilizan el almacenamiento local para almacenar el contenido de los clientes, pero no se utilizan para funcionalidades de almacenamiento de contenido de otros servicios, de forma similar a los servicios principales de almacenamiento de contenido de AWS. Cuando los clientes solicitan la eliminación de datos, se inician procesos automatizados para eliminar los datos y hacer que el contenido sea ilegible **(Control AWSCA-7.7).**

Disponibilidad

El Programa de resiliencia de AWS abarca los procesos y procedimientos mediante los cuales AWS identifica, responde y se recupera de un evento o incidente de disponibilidad importante dentro del entorno de los servicios de AWS. Este programa se basa en el enfoque tradicional de abordar la gestión de contingencias, que incorpora elementos de los planes de continuidad de negocio y recuperación de desastres, y lo amplía para tener en cuenta elementos esenciales de las estrategias proactivas de mitigación de riesgos, como la ingeniería de zonas de disponibilidad (AZ) físicamente separadas y la planificación continua de la capacidad de la infraestructura.

Los planes de contingencia de AWS y los manuales de respuesta a incidentes se mantienen y actualizan para reflejar los riesgos emergentes y las lecciones aprendidas de incidentes anteriores. Los planes de respuesta de los equipos de servicio se prueban y actualizan durante el transcurso de la actividad empresarial, y el liderazgo sénior prueba, revisa y aprueba anualmente el Plan de resiliencia de AWS **(Control AWSCA-10.3)**.

AWS ha identificado los componentes críticos del sistema necesarios para mantener la disponibilidad del sistema y recuperar el servicio en caso de interrupción. Los componentes críticos del sistema (por ejemplo, las bases de código) se respaldan en múltiples ubicaciones aisladas conocidas como zonas de disponibilidad. Cada zona de disponibilidad se ejecuta en su propia infraestructura física e independiente, y está diseñada para ser altamente fiable. Los puntos comunes de error, como los generadores y los equipos de refrigeración, no se comparten entre las zonas de disponibilidad. Además, las zonas de disponibilidad están físicamente separadas y diseñadas de manera tal que incluso las catástrofes extremadamente infrecuentes, como los incendios, los tornados o las inundaciones, solo deberían afectar a una única zona de disponibilidad. AWS replica los componentes críticos del sistema en varias zonas de disponibilidad y se mantienen y monitorean las copias de seguridad autorizadas para garantizar una replicación correcta **(Control AWSCA-10.1** y **AWSCA-10.2)**.

Copia de seguridad de datos

Los servicios de almacenamiento centrales de AWS tienen la capacidad de almacenarse de forma redundante en múltiples ubicaciones físicas como parte de las operaciones normales. Los clientes deben habilitar copias de seguridad de sus datos en todos los servicios de AWS.

Amazon S3 está diseñado para que los objetos tengan un grado de durabilidad del 99,999999999 % y un grado de disponibilidad del 99,99 % durante un período de un año. Los objetos se almacenan de forma redundante en múltiples dispositivos e instalaciones en una región de Amazon S3. Para contribuir a la durabilidad, las operaciones PUT y COPY de Amazon S3 almacenan de forma sincronizada el contenido de los clientes en varias instalaciones antes de comunicar el estado SUCCESS. Después del almacenamiento, Amazon S3 ayuda a mantener la durabilidad de los objetos mediante la detección y la corrección rápidas de la pérdida de redundancia. Además, Amazon S3 corrobora periódicamente la integridad de los datos almacenados con sumas de comprobación. En el caso de que se detecte corrupción, se corrige con los datos almacenados de forma redundante. Asimismo, Amazon S3 usa sumas de comprobación en todo el tráfico de red para detectar la corrupción en los paquetes de datos al almacenar o recuperar datos **(Control AWSCA-7.3**, **AWSCA-7.4** y **AWSCA-7.5)**.

La replicación de Amazon EBS se almacena dentro de la misma AZ, no a través de varias zonas, pero los clientes pueden realizar instantáneas periódicas de Amazon Simple Storage Service (S3) para proporcionar una durabilidad de los datos a largo plazo. En el caso de los clientes que han diseñado bases de datos transaccionales complejas con Amazon EBS, las copias de seguridad en Amazon S3 se pueden realizar a través del sistema de gestión de bases de datos, de manera que las transacciones y los registros distribuidos se puedan comprobar. AWS no efectúa copias de seguridad de los datos que se mantengan en discos virtuales asociados a las instancias en ejecución de Amazon EC2.

Amazon RDS ofrece dos métodos diferentes para realizar copias de seguridad y restaurar sus instancias de base de datos: las copias de seguridad automatizadas y las instantáneas de base de datos (DB Snapshots). Por defecto, la característica de copias de seguridad automatizadas de Amazon RDS permite que su instancia de base de datos se someta a una recuperación a un momento dado. Amazon RDS realizará una copia de seguridad de su base de datos y de los registros de transacciones, y los almacenará durante un período de retención especificado por el usuario. Esto permite la restauración de una instancia de base de datos a cualquier segundo durante el período de retención definido, hasta los últimos cinco minutos. El período de retención de las copias de seguridad automatizadas puede configurarse hasta un máximo de 35 días. Durante el período de copia de seguridad, es posible que la entrada/salida del almacenamiento (E/S) se suspenda durante unos segundos, mientras se realiza la copia de seguridad de los datos. Esta suspensión se puede evitar con las implementaciones Multi-AZ de base de datos, ya que las copias de seguridad se toman de la instancia de reserva. Las instantáneas de base de datos son copias de seguridad iniciadas por el usuario de las instancias de base de datos. Amazon RDS almacenará estas copias de seguridad completas de base de datos hasta que los clientes las eliminen explícitamente. Los clientes pueden crear una nueva instancia de base de datos a partir de una instantánea de base de datos según sea necesario **(Control AWSCA-7.6)**.

El equipo de AWS responsable de la administración de la capacidad monitorea continuamente el uso de los servicios para proyectar las necesidades de infraestructura según los compromisos y requisitos de disponibilidad. AWS mantiene un modelo de planificación de la capacidad para evaluar el uso y la demanda de la infraestructura al menos una vez al mes, y normalmente con más frecuencia (por ejemplo, semanalmente). Además, el modelo de planificación de la capacidad de AWS apoya la planificación de las demandas futuras para adquirir e implementar recursos adicionales basados en los recursos actuales y los requisitos previstos **(Control AWSCA-10.4)**.

D.8 Confidencialidad

AWS se compromete a proteger la seguridad y la confidencialidad del contenido de sus clientes, definido como "Su contenido" en https://aws.amazon.com/agreement/ **(Control AWSCA-11.3)**. Los sistemas y servicios de AWS están diseñados para permitir a los clientes autentificados de AWS acceder y administrar su contenido. AWS notifica a los clientes el acceso de terceros al contenido de un cliente en la página de acceso de terceros ubicada en https://aws.amazon.com/compliance/third-party-access. AWS puede eliminar el contenido de un cliente cuando se vea obligado a hacerlo por una orden legal, o cuando haya pruebas de fraude o abuso, tal y como se describe en el Contrato de cliente (https://aws.amazon.com/agreement/) y la Política de uso aceptable (https://aws.amazon.com/aup/). Cuando se ejecute la retirada de los contenidos de un cliente por los motivos indicados anteriormente, los empleados pueden hacerlos inaccesibles según lo requiera la situación. Para mayor claridad, esta capacidad de hacer inaccesibles los contenidos de los clientes se extiende también a los contenidos cifrados.

Durante el proceso de diseño, generación y prueba de las características del producto del sistema y del *software* de AWS, el contenido del cliente no se utiliza y permanece en el entorno de producción. El contenido de un cliente no es necesario para el ciclo de vida de desarrollo de software de AWS. Cuando se necesita contenido para desarrollar o probar el software de un servicio, los equipos de servicio de AWS disponen de herramientas para generar datos simulados y aleatorios.

AWS sabe que los clientes se preocupan por la privacidad y la seguridad de los datos. Por este motivo, AWS ofrece a los clientes la propiedad y el control de su contenido mediante herramientas que permiten a los clientes determinar dónde se almacena su contenido, asegurar su contenido en tránsito o en reposo y administrar el acceso a los servicios y recursos de AWS. AWS también implementa controles técnicos y físicos diseñados para evitar el acceso no autorizado o la divulgación del contenido de un cliente. Como se describe en las áreas de Seguridad física y Gestión de cambios en la Sección III de este informe, AWS emplea una serie de controles para salvaguardar los datos desde dentro y fuera de los límites de los entornos que almacenan el contenido de un cliente. Gracias a estas medidas, el acceso a los contenidos de los clientes está restringido a las partes autorizadas.

Los planes de contingencia y los manuales de respuesta a incidentes de AWS han definido y probado herramientas y procesos para detectar, mitigar, investigar y evaluar los incidentes de seguridad. Estos planes y manuales incluyen directrices para responder a posibles infracciones de datos de acuerdo con los requisitos contractuales y regulatorios. Los ingenieros de AWS Security siguen un protocolo documentado cuando responden a posibles incidentes de seguridad de datos. El protocolo implica pasos que incluyen la validación de la presencia del contenido del cliente dentro del servicio de AWS (sin ver realmente los datos), la determinación del estado de cifrado del contenido de un cliente y la determinación del acceso indebido al contenido de un cliente en la medida de lo posible.

En el transcurso de su respuesta, los ingenieros de seguridad documentan los resultados relevantes en las herramientas internas utilizadas para el seguimiento del problema de seguridad. Se informa a los líderes de AWS Security con regularidad de todas las investigaciones de problemas de seguridad de datos. En el caso de que haya indicadores positivos de que una parte no intencionada haya accedido de forma potencial al contenido del cliente, un ingeniero de seguridad se compromete con los líderes de AWS Security y el equipo legal de AWS para revisar los resultados. Los líderes de AWS Security y el equipo legal revisan los resultados y determinan si se ha producido una vulneración de datos notificable de acuerdo

con las obligaciones contractuales o reglamentarias. Si se confirma, se notifica a los clientes afectados de acuerdo con el requisito de notificación aplicable.

Los proveedores y terceros con acceso restringido que realizan negocios con Amazon están sujetos a compromisos de confidencialidad como parte de sus acuerdos con Amazon. Los compromisos de confidencialidad se incluyen en los acuerdos con proveedores y terceros con acceso restringido, y AWS y el tercero los revisan en el momento de la redacción o la firma del contrato **(Control AWSCA-11.1).** AWS monitorea el rendimiento de los terceros mediante revisiones periódicas con un enfoque basado en los riesgos, que evalúa el rendimiento con respecto a las obligaciones contractuales **(Control AWSCA-11.2).**

Internamente, los requisitos de confidencialidad se comunican a los empleados a través de la formación y las políticas. Los empleados están obligados a asistir a la formación sobre Concienciación de la seguridad informática de Amazon (ASA), que incluye políticas y procedimientos relacionados con la protección de los contenidos de los clientes. Los requisitos de confidencialidad se incluyen en la Política de clasificación y manejo de datos. Las políticas se revisan y actualizan al menos una vez al año.

AWS implementa políticas y controles para monitorear el acceso a los recursos que procesan o almacenan el contenido del cliente. Además, un Acuerdo maestro de servicios (MSA) o un Acuerdo de no divulgación (NDA) obligan a un subcontratista a la confidencialidad en el improbable caso de que estén expuestos al contenido de un cliente. El MSA hace referencia tanto a un NDA como a la obligación de proteger el contenido de un cliente en caso de que no tenga un NDA. AWS Legal mantiene el MSA más actualizado en un portal de documentos legales. El portal sirve de repositorio para almacenar los contratos con los compromisos más actuales, el propietario del documento y la fecha de modificación. También se lleva a cabo una revisión legal cuando se ejecuta el MSA con un proveedor.

Los servicios y sistemas alojados por AWS están diseñados para retener y proteger el contenido de un cliente durante el período del contrato con el cliente y, en algunos casos, hasta 30 días después de la terminación. El contrato de cliente, https://aws.amazon.com/agreement/, especifica los términos y condiciones. Los servicios de AWS están diseñados para retener el contenido de un cliente hasta que la obligación contractual de retener el contenido de un cliente termine, o tras una acción iniciada por el cliente para eliminar o borrar su contenido.

Una vez que la obligación contractual de retener el contenido de un cliente termina, o tras una acción iniciada por el cliente para eliminar o borrar su contenido, los servicios de AWS tienen procesos y procedimientos para detectar una eliminación y hacer que el contenido sea inaccesible. Después de un evento de eliminación, las acciones automatizadas actúan sobre el contenido borrado para hacerlo inaccesible **(Control AWSCA-7.7).**

D.9 Privacidad

AWS clasifica los datos de los clientes en dos categorías: contenido del cliente e información de la cuenta. AWS define el contenido del cliente como software (incluidas imágenes de máquina), datos, texto, audio, video o imágenes que un cliente o cualquier usuario final transfiere a AWS para su procesamiento, almacenamiento o alojamiento mediante los servicios de AWS en relación con la cuenta de dicho cliente, y cualquier resultado computacional que un cliente o cualquier usuario final obtenga de lo anterior a través de su uso de los servicios de AWS. Por ejemplo, el contenido del cliente incluye el contenido que un cliente o cualquier usuario final almacena en Amazon Simple Storage Service (S3). Los términos del

Contrato de cliente de AWS (https://aws.amazon.com/agreement/) y los Términos de Servicio de AWS (https://aws.amazon.com/service-terms/) se aplican al contenido del cliente.

La información de cuenta es información sobre un cliente que este proporciona a AWS en relación con la creación o administración de una cuenta de cliente. Por ejemplo, la información de cuenta incluye nombres, nombres de usuario, números de teléfono, direcciones de correo electrónico e información de facturación asociados a una cuenta de cliente. Cualquier información enviada por el cliente que AWS necesite para prestar servicios al cliente o en relación con la administración de cuentas de clientes, no está incluida en este informe.

El Aviso de privacidad de AWS está disponible en el sitio web de AWS en https://aws.amazon.com/privacy/. El equipo legal de AWS revisa el Aviso de privacidad de AWS y lo actualiza según sea necesario para reflejar las prácticas empresariales actuales de Amazon y los requisitos regulatorios globales. El Aviso de privacidad describe cómo AWS recopila y utiliza la información personal de un cliente en relación con los sitios web, aplicaciones, productos, servicios, eventos y experiencias de AWS. El Aviso de privacidad no se aplica a los contenidos de los clientes.

Como parte del proceso de creación y activación de la cuenta de AWS, se informa a los clientes de AWS del Aviso de privacidad de AWS y se les exige que acepten el Acuerdo de cliente, incluidos los términos y condiciones relacionados con la recopilación, el uso, la conservación, la divulgación y la eliminación de sus datos. Los clientes son responsables de determinar qué contenido almacenar en AWS, que puede incluir información personal. Sin la aceptación del Contrato de cliente, los clientes no pueden inscribirse para utilizar los servicios de AWS.

El Contrato de cliente de AWS informa a los clientes de los compromisos de seguridad y privacidad de los datos de AWS antes de activar una cuenta de AWS y se pone a disposición de los clientes para que lo revisen en cualquier momento en el sitio web de AWS **(Control AWSCA-12.1)**.

El cliente determina qué datos se introducen en los servicios de AWS y tiene la capacidad de configurar los ajustes de seguridad y privacidad adecuados para los datos, incluido quién puede acceder a ellos y utilizarlos. Además, el cliente puede optar por no facilitar determinados datos. Además, el cliente administra los requisitos de notificación o consentimiento y mantiene la exactitud de los datos.

Asimismo, el Contrato de cliente de AWS indica cómo AWS comparte, protege y retiene el contenido del cliente. AWS también informa a los clientes de las actualizaciones del Contrato de cliente poniéndolo a su disposición en su sitio web e indicando la última fecha de actualización. Los clientes deben consultar con frecuencia el sitio web del Contrato de cliente para comprobar si se realizaron cambios en él **(Control AWSCA-12.2)**.

AWS no almacena ningún dato del titular de la tarjeta obtenido de los clientes. En su lugar, AWS pasa los datos del titular de la tarjeta del cliente y los envía inmediatamente a la plataforma de pagos de Amazon, la plataforma con certificación PCI que Amazon utiliza para todo el procesamiento de pagos. Esta plataforma devuelve un identificador único que AWS almacena y utiliza para todo procesamiento futuro. La plataforma de pagos de Amazon se sitúa completamente fuera de los límites de AWS y está gestionada por la entidad mayor Amazon. No es un servicio de AWS, pero lo utiliza la entidad mayor Amazon para el procesamiento de pagos. Por lo tanto, la plataforma de pagos de Amazon no entra en el ámbito de este informe.

AWS ofrece a los clientes la posibilidad de actualizar sus preferencias de comunicación a través de la consola de AWS o mediante el Centro de preferencias de correo electrónico de AWS **(Control AWSCA-12.3)**. Cuando los clientes actualizan sus preferencias de comunicación utilizando su correo electrónico, se guardan sus preferencias actualizadas. Los clientes pueden darse de baja de los correos electrónicos de marketing de AWS en la consola de AWS. Los clientes de AWS seguirán recibiendo notificaciones importantes de AWS relacionadas con la cuenta, como los estados de facturación mensuales, o si se producen cambios significativos en un servicio que utilicen.

AWS ofrece a los clientes autenticados la posibilidad de acceder a sus datos, actualizarlos y confirmarlos. La denegación de acceso se comunicará mediante la consola de AWS **(Control AWSCA-12.6)**. Los clientes pueden iniciar sesión en sus cuentas de AWS a través de la consola de AWS para ver y actualizar sus datos.

AWS (o Amazon) no revela información de clientes en respuesta a demandas gubernamentales a menos que se le exija hacerlo para cumplir con una orden legalmente válida y vinculante. El Departamento Legal de AWS revisa y mantiene registros de todas las solicitudes de información, en los que figura información sobre los tipos y el volumen de información solicitada. A menos que AWS tenga prohibido hacerlo o existan indicios claros de conducta ilegal en relación con el uso de productos o servicios de Amazon, AWS notifica a los clientes antes de divulgar el contenido de los clientes para que puedan solicitar protección contra la divulgación. AWS comparte el contenido de los clientes únicamente como se describe en el Contrato de cliente de AWS **(Control AWSCA-12.8)**.

AWS puede producir información no relacionada con el contenido o sobre el contenido en respuesta a solicitudes válidas y vinculantes de las fuerzas del orden y gubernamentales, como citaciones, órdenes judiciales y órdenes de registro. “Información no relacionada con el contenido” significa información del cliente como nombre, dirección, dirección de correo electrónico, información de facturación, fecha de creación de la cuenta e información de uso del servicio. “Información sobre el contenido” incluye el contenido que un cliente transfiere para su procesamiento, almacenamiento o alojamiento en relación con los servicios de AWS y cualquier resultado computacional. AWS registra las solicitudes de información de los clientes para mantener un registro completo, preciso y oportuno de dichas solicitudes **(Control AWSCA-12.7)**.

Si es necesario, los clientes son responsables de notificar a las personas cuyos datos el cliente recopila y utiliza en AWS. AWS no es responsable de proporcionar dicha notificación ni de obtener el consentimiento de estas personas y solo es responsable de comunicar sus compromisos de privacidad a los clientes de AWS, que se proporciona durante el proceso de creación y activación de la cuenta.

AWS ha documentado una política y un plan de respuesta a incidentes que describe un enfoque organizado para responder a las violaciones e incidentes de seguridad. El equipo de AWS Security es responsable de monitorear los sistemas, hacer un seguimiento de los inconvenientes y documentar los resultados de los eventos relacionados con la seguridad. Se mantienen registros de los incidentes y las vulneraciones de seguridad, que incluyen información sobre el estado necesaria para respaldar las actividades forenses, el análisis de tendencias y la evaluación de los detalles del incidente.

Como parte del proceso, se investigan las posibles vulneraciones al contenido del cliente y se las eleva a los equipos de AWS Security y AWS Legal. Los clientes pueden suscribirse a la página Boletines de seguridad de AWS, que proporciona información sobre los problemas de seguridad identificados. AWS

notifica a los clientes afectados y a los reguladores las vulneraciones e incidentes tal y como exige la ley de acuerdo con los procesos del equipo **(Control AWSCA-12.5)**.

AWS retiene y dispone del contenido del cliente de conformidad con el Contrato de cliente y la Política de clasificación y manejo de datos de AWS. Cuando un cliente cierra su cuenta o rescinde el contrato con AWS, la cuenta se pone bajo aislamiento; tras lo cual, en un plazo de 90 días, los clientes pueden restaurar sus cuentas y el contenido relacionado. Los servicios de AWS que alojan contenido del cliente están diseñados para retener su contenido hasta que finalice la obligación contractual de hacerlo o hasta que el cliente inicie una acción para eliminar o borrar el contenido **(Control AWSCA-7.8)**. Cuando un cliente solicita que se eliminen datos, AWS utiliza procesos automatizados para detectar esa solicitud y hacer que el contenido sea inaccesible. Una vez completado el borrado, se llevan a cabo acciones automatizadas sobre el contenido borrado para hacerlo ilegible **(Control AWSCA-7.7)**.

AWS tiene una lista publicada externamente de subprocesadores de terceros que actualmente están contratados por AWS para procesar los datos del cliente en función de la región de AWS y el servicio de AWS que el cliente seleccione en https://aws.amazon.com/compliance/sub-processors/. Antes de que AWS autorice y permita a cualquier nuevo subprocesador de terceros acceder a cualquier contenido del cliente, AWS actualizará el sitio web para informar a los clientes **(Control AWSCA-12.12)**. AWS mantiene contratos con subprocesadores de terceros que definen cómo se limita el acceso al contenido del cliente a los niveles mínimos necesarios para prestar el servicio descrito en la página y que además contienen protección de datos, compromisos de confidencialidad y requisitos de seguridad **(Control AWSCA-12.9 y 12.10).** AWS realiza revisiones de seguridad de las aplicaciones para cada proveedor de subprocesadores de terceros antes de la integración con AWS para identificar y mitigar los riesgos de seguridad **(Control AWSCA-12.4)**. En las revisiones de seguridad frecuentes, se tienen en cuenta componentes de privacidad, como el período de retención, el uso y la recopilación de datos, según corresponda. La revisión comienza cuando el propietario de un sistema envía una solicitud de revisión al equipo dedicado de seguridad de proveedores de AWS (AVS) y proporciona la información detallada necesaria para la revisión.

Durante este proceso, el equipo de AVS determina la granularidad de la revisión necesaria en función del tipo de contenido del cliente que se compartirá, el diseño, el modelo de amenaza y el impacto en el perfil de riesgo de AWS. Proporcionan orientación en materia de seguridad, validan el material de aseguramiento de seguridad y se reúnen con terceros para hablar de sus pruebas de penetración, el ciclo de vida de desarrollo de software, los procesos de gestión de cambios y otros controles de seguridad operativos. Trabajan con el propietario del sistema para identificar, priorizar y corregir los resultados de seguridad. El equipo de AVS colabora con el Departamento Legal de AWS según sea necesario para validar que el contenido de las revisiones de AVS se ajusta a las políticas de privacidad de AWS. El equipo de AVS da su aprobación final al sistema del tercero después de haber evaluado adecuadamente los riesgos y trabajado con el solicitante para implementar controles de seguridad que mitiguen los riesgos identificados. Estas revisiones de seguridad de las aplicaciones no solo se ejecutan para los nuevos subprocesadores de terceros, sino que también se renuevan anualmente con cada subprocesador de terceros **(Control AWSCA-12.10 and AWSCA-12.11)**.

E. Monitoreo

E.1 Actividades de monitoreo

AWS utiliza una gran variedad de sistemas de monitoreo automatizado para facilitar un elevado nivel de rendimiento y disponibilidad en los servicios. AWS define al incidente de seguridad informática como un evento adverso relacionado con la seguridad, en el que haya habido una pérdida de confidencialidad de los datos, ruptura de la integridad de los datos o sistemas, o interrupción o denegación de la disponibilidad. Las herramientas de monitoreo de AWS se han diseñado para detectar actividades y condiciones inusuales o no autorizadas en los puntos de comunicación de entrada y salida. Estas herramientas monitorean el uso de los servidores y la red, las actividades de escaneo de puertos, el uso de las aplicaciones y los intentos de intrusión no autorizados.

Los sistemas dentro de AWS están diseñados para monitorear las métricas operativas clave, y se configuran alarmas para notificar automáticamente al personal de operaciones y administración cuando se superan los valores de umbral de alerta temprana. Se utiliza un horario de guardia a fin de que el personal esté siempre disponible para solucionar los problemas operativos. Esto incluye un sistema de localización para que las notificaciones se envíen al personal de operaciones de forma rápida y confiable **(Control AWSCA-8.1)**.

La documentación se mantiene actualizada para ayudar e informar al personal de operaciones sobre el tratamiento de incidentes o problemas. Se utiliza un sistema de tickets compatible con la comunicación, las actualizaciones de progreso, la colaboración necesaria entre los equipos y las capacidades de registro. Los coordinadores de las llamadas cualificados facilitan la comunicación y el progreso durante el tratamiento de los problemas operativos que precisan de colaboración. Después de un problema operativo importante, se convoca a una revisión después de la acción, independientemente del impacto externo. Además, se redactan documentos de corrección de errores (COE) para identificar la causa raíz y tomar medidas preventivas para el futuro. Se hace un seguimiento de la implementación de las medidas preventivas durante reuniones semanales de operaciones.

El equipo de AWS Security Operations emplea procedimientos de diagnóstico según estándares industriales tales como identificación, registro y verificación de incidentes, clasificación inicial de incidentes y priorización de acciones, para avanzar hacia una resolución durante eventos que impacten a la empresa. Los operadores del personal en EE. UU., Europa, Medio Oriente y África (EMEA), y Asia-Pacífico (APAC) brindan cobertura continua las 24 horas del día, los 7 días de la semana, para detectar incidentes, manejar el impacto y hallar una resolución **(Control AWSCA-8.2)**.

E.2 Notificación de incidentes

AWS ha documentado una política y un plan de respuesta a incidentes que describe un enfoque organizado para responder a las vulneraciones e incidentes de seguridad **(AWSCA-1.2)**. El equipo de AWS Security es responsable de monitorear los sistemas, hacer un seguimiento de los inconvenientes y documentar los resultados de los eventos relacionados con la seguridad. Se mantienen registros de los incidentes y las vulneraciones de seguridad, que incluyen información sobre el estado necesaria para respaldar las actividades forenses, el análisis de tendencias y la evaluación de los detalles del incidente.

Como parte del proceso, se investigan las posibles vulneraciones al contenido del cliente y se las eleva a los equipos de AWS Security y AWS Legal. Cuando la ley lo exige, se notifica a los clientes y reguladores afectados sobre las vulneraciones e incidentes. Los clientes pueden suscribirse a la página Boletines de seguridad de AWS, que proporciona información sobre los problemas de seguridad identificados.

Controles complementarios de las entidades usuarias

Los servicios de AWS se diseñaron con la presunción de que sus entidades usuarias (o clientes) implementan ciertas políticas, procedimientos y controles. En determinadas situaciones, es necesaria la aplicación de políticas, procedimientos y controles específicos por parte del cliente para alcanzar los compromisos de servicio y los requisitos del sistema que se basan en los criterios aplicables a los servicios de confianza incluidos en este informe. Esta sección describe las políticas, los procedimientos y los controles adicionales que los clientes pueden tener que implementar para satisfacer los compromisos de servicio y los requisitos del sistema para los casos de uso específicos de los clientes.

CC1.0: criterios comunes relacionados con el entorno de control

CC2.0: criterios comunes relacionados con la comunicación e información

CC3.0: criterios comunes relacionados con la evaluación del riesgo

CC4.0: criterios comunes relacionados con las actividades de monitoreo

- Los clientes deben asegurarse de que existe un registro adecuado de eventos para respaldar los procesos de monitoreo y respuesta a incidentes. Los clientes deben registrar eventos que incluyan, entre otros, actividades del administrador, errores del sistema, comprobaciones de autenticación y eliminaciones de datos.
- Los clientes deben habilitar y configurar las funciones de registro específicas del servicio cuando estén disponibles para todos los servicios e implementar procesos adecuados de monitoreo y respuesta a incidentes.

CC5.0: criterios comunes relacionados con las actividades de control

CC6.0: criterios comunes relacionados con los controles de acceso lógicos y físicos

- Los clientes deben utilizar pares de claves asimétricas o autenticación multifactor para acceder a sus hosts y evitar la autenticación basada en una contraseña simple.
- Los clientes deben implementar controles de acceso, como grupos de seguridad, roles de IAM y Listas de control de acceso (ACL), para segmentar y aislar instancias con funciones similares.
- Específicos de S3: los clientes deben utilizar las reglas administradas y las ACL para asegurar sus buckets de S3 y, así, controlar el acceso a los buckets de S3 y evitar que sean accesibles al público.
- Específico de AppStream 2.0: los clientes son responsables de administrar el acceso de los usuarios a las instancias de streaming y deben mantener controles para aprobar y conceder el acceso, eliminarlo de forma oportuna cuando un empleado deja la organización o cambia de responsabilidades laborales, y revisar de forma periódica los niveles de acceso adecuados para los usuarios existentes.

- Los clientes deben utilizar la autenticación multifactor para controlar el acceso a las credenciales de su cuenta raíz y deben evitar utilizar las credenciales de la cuenta raíz si no es para ajustar la configuración inicial de la cuenta de AWS Identity and Access Management (IAM), excepto en el caso de los servicios para los que IAM no está disponible. Los clientes deben eliminar las claves de acceso para la cuenta raíz cuando no esté en uso.
- Específico de Outpost: los clientes deben restringir y monitorear el acceso físico a los centros de datos y a las instalaciones que albergan los dispositivos de Outpost al personal en función de sus responsabilidades en el trabajo.
- Específico de Outpost: los clientes son responsables de verificar que su sitio cumple con los requisitos de Outpost en cuanto a las instalaciones, las redes y la energía, tal como se describe en https://docs.aws.amazon.com/outposts/latest/userguide/outposts-requirements.html.
- Específico de Outpost: los clientes son responsables de quitar la clave de seguridad Nitro (NSK) para garantizar que el contenido del cliente se destruya de manera criptográfica de Outpost antes de devolverlo a AWS.
- Los clientes son responsables de administrar y revisar el acceso de los usuarios a su instancia de los servicios de AWS de conformidad con sus políticas de administración de acceso.

CC7.0: criterios comunes relacionados con las operaciones de sistema

- Los clientes también pueden suscribirse a las ofertas de Premium Support, que incluyen comunicación directa con el equipo de atención al cliente y alertas proactivas sobre cualquier tipo de inconveniente que pueda afectar al cliente.
- Específico de VPC: los clientes son responsables de los requisitos de seguridad de su red y de conectar su Amazon Virtual Private Cloud a un punto apropiado de su red interna.
- Específico de EC2: los clientes son responsables de configurar la funcionalidad de Time Sync y monitorear la sincronización para lograr la exactitud a través de sus instancias EC2, como AWS ha publicado en la documentación de la guía del usuario https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/set-time.html#configure-amazon-time-service-amazon-linux.

CC8.0: criterios comunes relacionados con la gestión de cambios

- Los clientes son responsables de mantener la aplicación de los parches en las instancias de Amazon del cliente. Los clientes pueden aprovechar las herramientas automatizadas de aplicación de parches, como el AWS Systems Manager Patch Manager para poder implementar parches de software y sistema operativo automáticamente en grandes grupos de instancias.
- Los clientes deben establecer cuentas de desarrollo y producción separadas para aislar el sistema de producción del trabajo de desarrollo.
- Específico de App Mesh: los clientes que utilicen su propia imagen de Envoy deben seguir un proceso documentado de gestión de cambios para garantizar que las configuraciones actualizadas

se documenten, prueben y aprueben antes de la implementación en las instancias de producción del cliente.

CC9.0: criterios comunes relacionados con la mitigación del riesgo

- Los clientes deben mantener políticas y procedimientos que proporcionen formación y orientación para la seguridad de la información dentro de la organización, el entorno de TI y el uso de los servicios de AWS.
- Los clientes deben evaluar los objetivos de su red de servicios en la nube de AWS e identificar los riesgos y los controles correspondientes que deben implementarse para abordar dichos riesgos al utilizar los servicios de AWS, el software y los controles operativos.

A: criterios de disponibilidad

- Específico de EC2: los clientes que utilicen el servicio EC2 deben aumentar los firewalls de las instancias de AWS con uno basado en un host para obtener redundancia y filtrado de salida.
- Específico de EC2/VPC: los datos almacenados en los discos virtuales de Amazon EC2 deben copiarse de forma proactiva a otra opción de almacenamiento para que haya redundancia.
- Los clientes deben garantizar que sus recursos de AWS, tales como el servidor y las instancias de bases de datos, posean los niveles adecuados de redundancia y aislamiento. La redundancia puede obtenerse mediante el uso de la opción de implementación Multi-AZ y Multi-Region donde esté disponible.
- Específico de EBS: la replicación de Amazon EBS se almacena dentro de la misma AZ, no en múltiples zonas, por lo que los clientes deben enviar instantáneas periódicamente a Amazon S3 para preservar la durabilidad de los datos a largo plazo.
- Los clientes deben habilitar copias de seguridad de sus datos en todos los servicios de AWS.

C: criterios de confidencialidad

- Los clientes deben utilizar la opción de Amazon S3 para especificar una suma de comprobación MD5 como parte de una operación REST PUT para los datos enviados a Amazon S3. Cuando la solicitud llega a Amazon S3, se recalcula una suma de comprobación MD5 de los datos de objeto recibidos y se compara a la suma de comprobación MD5 provista. Si existe incompatibilidad, el PUT se rechaza para evitar que los datos corruptos se transfieran a Amazon S3. Los clientes deben usar las sumas de comprobación MD5 devueltas luego de usar REST GET para confirmar que los datos devueltos por el GET no se corrompieron en tránsito.
- Cualquier código que los clientes escriban para llamar a las API de Amazon deben esperar recibir y manejar errores del servicio. En la guía del usuario y en la documentación de la API correspondientes se puede encontrar orientación específica para cada servicio.
- Específico de AWS Snowball: los clientes no deben eliminar ninguna copia local de sus datos hasta que hayan verificado que se han copiado en AWS.

- Específico de AWS Snowball: todos los datos se cifran antes de su persistencia. Con AWS Snowball, hay breves períodos en los que el contenido de los clientes está en texto sin formato antes del cifrado y la persistencia. Si al cliente le preocupa este período corto, debe cifrar sus datos antes de enviarlos al dispositivo.
- Los clientes deben transmitir las claves secretas a través de canales seguros. Los clientes deben evitar integrar claves secretas en páginas web u otro código fuente en donde se pueda acceder de forma pública. Los clientes deben cifrar la información confidencial tanto en reposo como en tránsito por la red.
- Los clientes deben configurar y administrar apropiadamente el uso y la implementación de opciones de cifrado disponibles para cumplir con sus requisitos.
- Los clientes deben utilizar conexiones cifradas (TLS/SSL) para todas sus interacciones con AWS. Se recomienda el uso de TLS 1.2. Los clientes pueden optar por un programa de rotación de claves que cumpla con sus necesidades para cualquier clave de KMS que quisieran rotar.

P – Criterios de privacidad

P1 – Información y comunicación

P2 - Elección y consentimiento

- Los clientes deben consultar con frecuencia el sitio web del Contrato de cliente y el Aviso de privacidad para comprobar si se produjeron cambios.
- Los clientes son responsables de actualizar sus preferencias de comunicación.
- Los clientes son responsables de administrar los requisitos de divulgación y notificación de los datos almacenados en los servicios de AWS, cuando proceda, ya que AWS no es responsable de proporcionar la notificación, obtener el consentimiento o tener conocimiento de lo que se ha notificado a los individuos o el consentimiento que estos han otorgado.

P3 – Recopilación

P4 – Uso, retención y eliminación

- Los clientes son responsables de cumplir cualquier normativa o ley que exija una justificación de los fines para los que se recopila, utiliza, retiene y divulga la información personal.

P5 - Acceso

- Los clientes son responsables de proporcionar a las personas su información personal, que el cliente haya almacenado en los servicios de AWS, si así lo exige la ley.

P6 - Divulgación y notificación

P7 - Calidad

- Los clientes son responsables de mantener la información personal, que el cliente haya almacenado en los servicios de AWS, exacta, completa y relevante, tal y como lo requiera cualquier normativa o ley.

P8 - Monitoreo y aplicación

La lista de consideraciones de control mencionada no representa todos los controles que debe emplear el cliente. Pueden ser necesarios otros controles. Los clientes deben consultar la documentación adicional de los servicios de AWS en el sitio web de AWS.

SECCIÓN IV: Descripción de los criterios, los controles de AWS, las pruebas y los resultados de las pruebas

Pruebas realizadas y resultados de los controles a nivel de la entidad

En la planificación de la naturaleza, el tiempo y la extensión de las pruebas de los controles, EY tuvo en cuenta los aspectos del entorno de control de AWS y realizó pruebas de los controles que consideró necesarios.

Además de las pruebas de eficacia operativa de los controles específicos que se describen a continuación, en los procedimientos se incluyeron las pruebas de los siguientes componentes del entorno de control interno de AWS:

- Controles de gestión y estructura organizacional
- Proceso de evaluación del riesgo
- Información y comunicación
- Actividades de control
- Monitoreo

Las pruebas del entorno de control incluyeron los siguientes procedimientos, de acuerdo con el alcance que EY consideró necesario: (a) la revisión de la estructura organizacional de AWS, que incluye la división de las responsabilidades funcionales, las declaraciones de política, los manuales de procedimiento y los controles de personal, (b) debates con el personal de gestión, operaciones y administrativo, entre otros, responsable del desarrollo, el cumplimiento y la aplicación de los controles, y (c) observaciones del personal en el rendimiento de sus funciones asignadas.

El entorno de control se consideró en la determinación de la naturaleza, el tiempo y la extensión de las pruebas de los controles y los controles importantes para lograr los objetivos de control.

Procedimientos para evaluar la totalidad y precisión de la información proporcionada por la entidad (Information Provided by the Entity, IPE)

En el caso de las pruebas de los controles que requerían la IPE (por ejemplo, los controles que necesitan poblaciones generadas por un sistema para pruebas con muestras), EY realizó la combinación de los siguientes procedimientos, siempre que fue posible, según la naturaleza de la IPE, para abordar la totalidad, precisión e integridad de los datos o informes que se utilizaron: (1) inspeccionar el origen de la IPE, (2) inspeccionar la consulta, el script o los parámetros que se utilizaron para generar la IPE, (3) relacionar los datos entre la IPE y el origen, o (4) inspeccionar la IPE en caso de brechas anómalas en las secuencias o el tiempo para determinar si los datos están completos, son precisos y si mantienen su integridad. Además de los procedimientos anteriores, para las pruebas de controles que requieren el uso de la gestión de la IPE en la ejecución de los controles (por ejemplo, las revisiones frecuentes de las listas de acceso de los usuarios), EY inspeccionó los procedimientos de gestión para evaluar la validez del origen de la IPE y la completitud, precisión e integridad de los datos o informes.

Criterios sobre los servicios de confianza y los controles relacionados para los sistemas y las aplicaciones

En las siguientes páginas, AWS ha especificado la descripción de los objetivos de control y los controles para alcanzar los objetivos, los cuales son su responsabilidad. Las “Pruebas realizadas por EY” y los “Resultados de las pruebas” son responsabilidad del auditor del servicio.

Nota: En la sección V de este informe, “Otra información proporcionada por Amazon Web Services”, se proporciona una comparación de los controles de AWS que se revisaron durante el período de evaluación a fines informativos.

Entorno de control del sistema de información

Los siguientes controles se aplican a los servicios que se enumeran en la Descripción del sistema y sus centros de datos disponibles, excepto en los que los controles son solo para uno de los servicios. En esos casos, los controles se indican como “Específico de S3”, “Específico de EC2”, “Específico de VPC”, “Específico de KMS”, “Específico de RDS”, “Específico de Outposts” o según se indique como específico para un servicio o conjunto de servicios en particular.

Controles de AWS asignados a los criterios de seguridad, disponibilidad, confidencialidad y privacidad

Criterios	Compatible con la actividad de control de AWS (AWSCA)	Descripción de los criterios
CC1.0: criterios comunes relacionados con el entorno de control		
CC1.1	AWSCA-1.1; AWSCA-1.2; AWSCA-9.2; AWSCA-9.3; AWSCA-9.7; AWSCA-9.9; AWSCA-11.1; AWSCA-11.2	Principio 1 de COSO: la entidad demuestra compromiso con la integridad y los valores éticos.
CC1.2	AWSCA-1.7; AWSCA-1.8; AWSCA-9.8	Principio 2 de COSO: la junta directiva demuestra independencia de la gestión y supervisa el desarrollo y rendimiento del control interno.
CC1.3	AWSCA-1.1; AWSCA-1.2	Principio 3 de COSO: la gestión establece, con la supervisión de la junta, estructuras, líneas jerárquicas, autoridades adecuadas y responsabilidades en el cumplimiento de los objetivos.
CC1.4	AWSCA-1.2; AWSCA-1.4; AWSCA-1.7; AWSCA-1.8; AWSCA-9.2; AWSCA-9.3; AWSCA-9.9: AWSCA-11.1; AWSCA-11.2	Principio 4 de COSO: la entidad demuestra compromiso para atraer, desarrollar y retener a las personas capacitadas en consonancia con los objetivos.

Controles de AWS asignados a los criterios de seguridad, disponibilidad, confidencialidad y privacidad

Criterios	Compatible con la actividad de control de AWS (AWSCA)	Descripción de los criterios
CC1.5	AWSCA-1.1; AWSCA-1.2; AWSCA-1.3; AWSCA-9.3; AWSCA-9.7	Principio 5 de COSO: la entidad hace que las personas se hagan cargo de sus responsabilidades de control interno para alcanzar los objetivos.
CC2.0: criterios comunes relacionados con la comunicación e información		
CC2.1	AWSCA-1.2; AWSCA-1.5; AWSCA-1.9; AWSCA-1.10; AWSCA-3.6; AWSCA-8.1; AWSCA-8.2; AWSCA-9.8	Principio 13 de COSO: la entidad obtiene o genera y utiliza información importante y de calidad para brindar apoyo al funcionamiento del control interno.
CC2.2	AWSCA-1.2; AWSCA-1.4; AWSCA-1.6; AWSCA-1.9; AWSCA-9.1; AWSCA-9.5; AWSCA-9.6; AWSCA-10.3; AWSCA-11.1; AWSCA-11.3	Principio 14 de COSO: la entidad comunica la información de manera interna, lo que incluye los objetivos y las responsabilidades de control interno, necesarios para brindar apoyo al funcionamiento del control interno.
CC2.3	AWSCA-1.4; AWSCA-1.6; AWSCA-9.1; AWSCA-9.5; AWSCA-11.1; AWSCA-11.2; AWSCA-11.3; AWSCA-12.1; AWSCA-12.2; AWSCA-12.3; AWSCA-12.4;	Principio 15 de COSO: la entidad se comunica con los usuarios externos con respecto a los asuntos que afectan el funcionamiento del control interno.

Controles de AWS asignados a los criterios de seguridad, disponibilidad, confidencialidad y privacidad

Criterios	Compatible con la actividad de control de AWS (AWSCA)	Descripción de los criterios
	AWSCA-12.5	
CC3.0: criterios comunes relacionados con la evaluación del riesgo		
CC3.1	AWSCA-1.5; AWSCA-1.9; AWSCA-1.10; AWSCA-9.8	Principio 6 de COSO: la entidad identifica los objetivos con suficiente claridad, lo que permite la identificación y evaluación de riesgos relacionados con los objetivos.
CC3.2	AWSCA-1.5; AWSCA-1.9; AWSCA-1.10; AWSCA-3.4; AWSCA-5.12; AWSCA-10.3	Principio 7 de COSO: la entidad identifica los riesgos para los logros de sus objetivos en toda la entidad y analiza los riesgos como una base para determinar cómo se deberían abordar.
CC3.3	AWSCA-1.5; AWSCA-1.10; AWSCA-3.4; AWSCA-5.12; AWSCA-10.3	Principio 8 de COSO: la entidad tiene en cuenta las posibilidades de fraude en la evaluación de riesgos con respecto al logro de los objetivos.
CC3.4	AWSCA-1.5; AWSCA-1.10; AWSCA-3.4; AWSCA-5.12; AWSCA-10.3	Principio 9 de COSO: la entidad identifica y evalúa los cambios que podrían impactar en gran medida el sistema de control interno.
CC4.0: criterios comunes relacionados con las actividades de monitoreo		

Controles de AWS asignados a los criterios de seguridad, disponibilidad, confidencialidad y privacidad

Criterios	Compatible con la actividad de control de AWS (AWSCA)	Descripción de los criterios
CC4.1	AWSCA-1.10; AWSCA-3.4; AWSCA-5.12; AWSCA-9.8; AWSCA-11.2	Principio 16 de COSO: la entidad selecciona, desarrolla y realiza evaluaciones continuas o individuales para determinar si los componentes del control interno están presentes y en funcionamiento.
CC4.2	AWSCA-1.5; AWSCA-1.10; AWSCA-9.8	Principio 17 de COSO: la entidad evalúa y comunica las deficiencias del control interno de manera oportuna a las partes responsables de realizar la acción correctiva, lo que incluye a los directivos superiores y a la junta directiva, según corresponda.
CC5.0: criterios comunes relacionados con las actividades de control		
CC5.1	AWSCA-1.2; AWSCA-1.3; AWSCA-1.5; AWSCA-1.10	Principio 10 de COSO: la entidad selecciona y desarrolla las actividades de control que contribuyen con la mitigación de los riesgos para el logro de los objetivos a niveles aceptables.
CC5.2	AWSCA-1.2; AWSCA-1.3; AWSCA-1.5; AWSCA-1.10	Principio 11 de COSO: la entidad también selecciona y desarrolla las actividades de control general relacionadas con la tecnología para asistir en el logro de los objetivos.
CC5.3	AWSCA-1.1; AWSCA-1.2; AWSCA-1.3; AWSCA-1.5; AWSCA-1.10; AWSCA-10.3	Principio 12 de COSO: la entidad implementa actividades de control a través de las políticas que establecen lo que se espera y en los procedimientos que ponen en marcha estas políticas.
CC6.0: criterios comunes relacionados con los controles de acceso lógicos y físicos		
CC6.1	AWSCA-1.2; AWSCA-2.1; AWSCA-2.2; AWSCA-2.3; AWSCA-2.4; AWSCA-2.5; AWSCA-2.6; AWSCA-3.1;	La entidad implementa el software, la infraestructura y las arquitecturas de seguridad de acceso lógico sobre los activos de información protegida para resguardarlos de eventos de seguridad a fin de cumplir con los objetivos de la entidad.

Controles de AWS asignados a los criterios de seguridad, disponibilidad, confidencialidad y privacidad

Criterios	Compatible con la actividad de control de AWS (AWSCA)	Descripción de los criterios
	AWSCA-3.2; AWSCA-3.3; AWSCA-3.5; AWSCA-3.6; AWSCA-3.7; AWSCA-3.8; AWSCA-3.9; AWSCA-3.10; AWSCA-3.11; AWSCA-3.12; AWSCA-3.13; AWSCA-3.14; AWSCA-3.15; AWSCA-3.17; AWSCA-4.4; AWSCA-4.5; AWSCA-4.6; AWSCA-4.7; AWSCA-4.8; AWSCA-4.9; AWSCA-4.10; AWSCA-4.11; AWSCA-4.12; AWSCA-4.13; AWSCA-4.14; AWSCA-4.15; AWSCA-6.1; AWSCA-8.1; AWSCA-8.2; AWSCA-9.4	
CC6.2	AWSCA-2.1; AWSCA-2.2; AWSCA-2.3; AWSCA-2.4	Antes de emitir las credenciales del sistema y brindar el acceso al sistema, la entidad registra y autoriza a nuevos usuarios internos y externos cuyo acceso lo administra la entidad. En el caso del acceso de los usuarios que administra la entidad, las credenciales del sistema del usuario se eliminan cuando el usuario ya no tiene acceso autorizado.
CC6.3	AWSCA-2.1; AWSCA-2.2; AWSCA-2.3;	La entidad autoriza, modifica o elimina el acceso a los datos, el software, las funciones y otros activos de información protegida según los roles, la responsabilidad o el diseño y los cambios del sistema, teniendo en cuenta

Controles de AWS asignados a los criterios de seguridad, disponibilidad, confidencialidad y privacidad

Criterios	Compatible con la actividad de control de AWS (AWSCA)	Descripción de los criterios
	AWSCA-2.4; AWSCA-2.5; AWSCA-2.6	los conceptos de privilegio mínimo y división de los deberes con el fin de alcanzar los objetivos de la entidad.
CC6.4	AWSCA-3.16; AWSCA-4.12; AWSCA-4.13; AWSCA-4.15; AWSCA-5.1; AWSCA-5.2; AWSCA-5.3; AWSCA-5.4; AWSCA-5.5	La entidad restringe el acceso físico autorizado a las instalaciones y a los activos de información protegidos (por ejemplo, las instalaciones de los centros de datos, el almacenamiento de medios con copia de seguridad y otras ubicaciones importantes) al personal con el fin de alcanzar los objetivos de la entidad.
CC6.5	AWSCA-5.13; AWSCA-7.7; AWSCA-7.8; AWSCA-7.9	La entidad discontinúa la protección física y lógica sobre los activos físicos solo después de que la capacidad de leer y recuperar los datos y el software de los activos ha mermado y ya no son necesarios para alcanzar los objetivos de la entidad.
CC6.6	AWSCA-2.6; AWSCA-3.1; AWSCA-3.2; AWSCA-3.3; AWSCA-3.7; AWSCA-3.8; AWSCA-3.9; AWSCA-4.14; AWSCA-8.1; AWSCA-8.2	La entidad implementa medidas de seguridad para el acceso lógico con el fin de protegerse contra amenazas de orígenes externos a los límites de su sistema.
CC6.7	AWSCA-1.2; AWSCA-1.4; AWSCA-1.6; AWSCA-2.2; AWSCA-2.3; AWSCA-3.16; AWSCA-3.17; AWSCA-3.18; AWSCA-4.1; AWSCA-4.2;	La entidad restringe la transmisión, el movimiento y la eliminación de información a los usuarios y procesos internos y externos autorizados, y la protege durante su transmisión, movimiento o eliminación para alcanzar los objetivos de la entidad.

Controles de AWS asignados a los criterios de seguridad, disponibilidad, confidencialidad y privacidad

Criterios	Compatible con la actividad de control de AWS (AWSCA)	Descripción de los criterios
	AWSCA-4.3; AWSCA-4.4; AWSCA-4.6; AWSCA-4.7; AWSCA-4.9; AWSCA-4.11; AWSCA-4.14; AWSCA-4.15; AWSCA-5.1; AWSCA-5.2; AWSCA-5.3; AWSCA-5.13; AWSCA-7.1	
CC6.8	AWSCA-2.2; AWSCA-2.3; AWSCA-3.4; AWSCA-3.18; AWSCA-6.1; AWSCA-6.2; AWSCA-6.3; AWSCA-6.4; AWSCA-6.5; AWSCA-6.6; AWSCA-8.1; AWSCA-8.2; AWSCA-9.4	La entidad implementa controles para evitar o detectar y actuar sobre la introducción de un software malicioso o no autorizado a fin de alcanzar los objetivos de la entidad.
CC7.0: criterios comunes relacionados con las operaciones de sistema		
CC7.1	AWSCA-3.1; AWSCA-3.2; AWSCA-3.3; AWSCA-3.4; AWSCA-3.6; AWSCA-6.6; AWSCA-7.10; AWSCA-9.4	Con el fin de cumplir con sus objetivos, la entidad utiliza procedimientos de detección y monitoreo para identificar (1) cambios en las configuraciones que impliquen la introducción de nuevas vulnerabilidades, y (2) la susceptibilidad ante las vulnerabilidades que se descubran recientemente.

Controles de AWS asignados a los criterios de seguridad, disponibilidad, confidencialidad y privacidad

Criterios	Compatible con la actividad de control de AWS (AWSCA)	Descripción de los criterios
CC7.2	AWSCA-1.2; AWSCA-3.4; AWSCA-5.6; AWSCA-8.1; AWSCA-8.2; AWSCA-9.6	La entidad monitorea los componentes del sistema y la operación de esos componentes para detectar anomalías que sean indicio de actos maliciosos, desastres naturales y errores que afecten la capacidad de la entidad para cumplir con sus objetivos. Las anomalías se analizan para determinar si representan o no eventos de seguridad.
CC7.3	AWSCA-1.1; AWSCA-5.6; AWSCA-5.11; AWSCA-5.12; AWSCA-8.1; AWSCA-8.2; AWSCA-9.6; AWSCA-10.3; AWSCA-12.5	La entidad evalúa los eventos de seguridad para determinar si podrían causar o si causaron errores que eviten que la entidad cumpla sus objetivos (incidentes de seguridad) y, de ser así, toma medidas para prevenir o abordar esos errores.
CC7.4	AWSCA-1.1; AWSCA-1.2; AWSCA-3.4; AWSCA-5.11; AWSCA-5.12; AWSCA-8.1; AWSCA-8.2; AWSCA-9.6; AWSCA-9.7; AWSCA-10.3; AWSCA-12.5	La entidad responde a los incidentes de seguridad identificados ejecutando el programa definido de respuesta a incidentes para comprender, contener, remediar y comunicar los incidentes de seguridad, según corresponda.
CC7.5	AWSCA-5.11; AWSCA-5.12; AWSCA-6.1; AWSCA-8.2; AWSCA-9.6; AWSCA-10.3	La entidad identifica, desarrolla e implementa actividades para recuperarse de los incidentes de seguridad identificados.
CC8.0: criterios comunes relacionados con la gestión de cambios		

Controles de AWS asignados a los criterios de seguridad, disponibilidad, confidencialidad y privacidad

Criterios	Compatible con la actividad de control de AWS (AWSCA)	Descripción de los criterios
CC8.1	AWSCA-3.1; AWSCA-3.2; AWSCA-3.3; AWSCA-3.6; AWSCA-3.16; AWSCA-6.1; AWSCA-6.2; AWSCA-6.3; AWSCA-6.4; AWSCA-6.5; AWSCA-6.6; AWSCA-6.7; AWSCA-8.2; AWSCA-9.4; AWSCA-10.3; AWSCA-12.4	La entidad autoriza, diseña, desarrolla o adquiere, configura, documenta, prueba, aprueba e implementa cambios en la infraestructura, los datos, el software y los procedimientos a fin de cumplir sus objetivos.
CC9.0: Mitigación del riesgo		
CC9.1	AWSCA-1.2; AWSCA-1.5; AWSCA-1.10; AWSCA-10.3	La entidad identifica, selecciona y desarrolla actividades de mitigación del riesgo para los riesgos que surgen de posibles interrupciones comerciales.
CC9.2	AWSCA-1.5; AWSCA-1.10; AWSCA-5.11; AWSCA-5.12; AWSCA-9.7; AWSCA-11.1; AWSCA-11.2; AWSCA-11.3; AWSCA-12.4	La entidad evalúa y administra los riesgos asociados con los proveedores y los socios empresariales.

Controles de AWS asignados a los criterios de seguridad, disponibilidad, confidencialidad y privacidad

Criterios	Compatible con la actividad de control de AWS (AWSCA)	Descripción de los criterios
Criterios adicionales sobre la disponibilidad		
A1.1	AWSCA-8.1; AWSCA-10.3; AWSCA-10.4	La entidad mantiene, monitorea y evalúa la capacidad de procesamiento actual y el uso de los componentes del sistema (infraestructura, datos y software) para administrar la demanda de capacidad y habilitar la implementación de capacidad adicional para ayudar a cumplir con sus objetivos.
A1.2	AWSCA-1.2; AWSCA-1.5; AWSCA-1.10; AWSCA-5.7; AWSCA-5.8; AWSCA-5.9; AWSCA-5.10; AWSCA-5.11; AWSCA-5.12; AWSCA-7.3; AWSCA-7.4; AWSCA-7.5; AWSCA-7.6; AWSCA-8.1; AWSCA-8.2; AWSCA-10.1; AWSCA-10.2; AWSCA-10.3; AWSCA-10.4	La entidad autoriza, diseña, desarrolla o adquiere, implementa, opera, aprueba, mantiene y monitorea la protección ambiental, el software, los procesos de copia de seguridad de los datos y la infraestructura de recuperación para cumplir con sus objetivos.
A1.3	AWSCA-1.2; AWSCA-10.2; AWSCA-10.3	La entidad prueba los procedimientos del plan de recuperación que apoyan la recuperación del sistema para cumplir con sus objetivos.

Controles de AWS asignados a los criterios de seguridad, disponibilidad, confidencialidad y privacidad

Criterios	Compatible con la actividad de control de AWS (AWSCA)	Descripción de los criterios
Criterios adicionales sobre la confidencialidad		
C1.1	AWSCA-1.2; AWSCA-7.2; AWSCA-7.3; AWSCA-7.4; AWSCA-7.5; AWSCA-7.6; AWSCA-7.8; AWSCA-10.2	La entidad identifica y mantiene información confidencial para cumplir con los objetivos de la entidad relacionados con la confidencialidad.
C1.2	AWSCA-5.13; AWSCA-7.7; AWSCA-7.9	La entidad se deshace de información confidencial para cumplir con los objetivos de la entidad relacionados con la confidencialidad.
Criterios adicionales relacionados con la privacidad		
P1.1	AWSCA-12.1; AWSCA-12.2; AWSCA-12.4	La entidad notifica a los interesados sus prácticas de protección de la intimidad para cumplir los objetivos de la entidad en materia de protección de la intimidad. El aviso se actualiza y se comunica a los interesados de manera oportuna en caso de cambios en las prácticas de privacidad de la entidad, incluidos los cambios en el uso de la información personal, para cumplir los objetivos de la entidad relacionados con la privacidad.
P2.1	AWSCA-12.1; AWSCA-12.3	La entidad comunica a los interesados las opciones disponibles en relación con la recopilación, el uso, la retención, la divulgación y la eliminación de información personal y las consecuencias, en su caso, de cada opción. El consentimiento explícito para la recopilación, el uso, la retención, la divulgación y la eliminación de información personal se obtiene de los interesados o de otras personas autorizadas, si es necesario. Dicho consentimiento se obtiene únicamente para la finalidad prevista de la información a fin de cumplir los objetivos de la entidad relacionados con la privacidad. La base de la entidad para determinar el consentimiento implícito para la recolección, el uso, la retención, la divulgación y la eliminación de información personal está documentada.
P3.1	AWSCA-1.4; AWSCA-3.6; AWSCA-12.1; AWSCA-12.4	La información personal se recopila de forma coherente con los objetivos de la entidad relacionados con la privacidad.

Controles de AWS asignados a los criterios de seguridad, disponibilidad, confidencialidad y privacidad

Criterios	Compatible con la actividad de control de AWS (AWSCA)	Descripción de los criterios
P3.2	No aplicable: los clientes mantienen la propiedad de su contenido y seleccionan qué servicios de AWS pueden procesar, almacenar y alojar su contenido. AWS no accede ni utiliza el contenido del cliente para ningún fin sin el consentimiento explícito del cliente. Los clientes son responsables de la conformidad con cualquier norma o ley relativa a la recopilación de información personal.	En el caso de la información que requiere el consentimiento explícito, la entidad comunica la necesidad de dicho consentimiento, así como las consecuencias de la falta de consentimiento para la solicitud de información personal, y obtiene el consentimiento antes de la recopilación de la información a fin de cumplir los objetivos de la entidad relacionados con la privacidad.
P4.1	AWSCA-1.2; AWSCA-1.4; AWSCA-3.6; AWSCA-7.7; AWSCA-11.2; AWSCA-12.4	La entidad limita el uso de la información personal a los fines identificados en los objetivos de la entidad relacionados con la privacidad.

Controles de AWS asignados a los criterios de seguridad, disponibilidad, confidencialidad y privacidad

Criterios	Compatible con la actividad de control de AWS (AWSCA)	Descripción de los criterios
P4.2	AWSCA-1.2; AWSCA-3.6; AWSCA-7.7; AWSCA-7.8; AWSCA-7.9; AWSCA-12.4	La entidad retiene la información personal de forma coherente con los objetivos de la entidad relacionados con la privacidad.
P4.3	AWSCA-1.2; AWSCA-5.13; AWSCA-7.7; AWSCA-7.8; AWSCA-7.9	La entidad elimina de forma segura la información personal para cumplir los objetivos de la entidad relacionados con la privacidad.
P5.1	AWSCA-9.5; AWSCA-12.1; AWSCA-12.5; AWSCA-12.6; AWSCA-12.7;	La entidad concede a los interesados identificados y autenticados la posibilidad de acceder a su información personal almacenada para revisarla y, previa solicitud, proporciona copias físicas o electrónicas de dicha información a los interesados para cumplir los objetivos de la entidad relacionados con la privacidad. Si se deniega el acceso, se informa a los interesados de la denegación y del motivo de esta, según sea necesario, para cumplir los objetivos de la entidad relacionados con la privacidad.
P5.2	AWSCA-9.5; AWSCA-12.1; AWSCA-12.5; AWSCA-12.6; AWSCA-12.7	La entidad corrige, modifica o agrega información personal con base en la información facilitada por los interesados y comunica dicha información a terceros, según se comprometa o sea necesario, para cumplir los objetivos de la entidad relacionados con la privacidad. Si se deniega una solicitud de corrección, se informa a los interesados de la denegación y del motivo de esta para cumplir los objetivos de la entidad relacionados con la privacidad.
P6.1	AWSCA-11.2; AWSCA-12.1; AWSCA-12.4; AWSCA-12.7; AWSCA-12.9; AWSCA-12.11	La entidad revela información personal a terceros con el consentimiento explícito de los interesados y dicho consentimiento se obtiene antes de la divulgación para cumplir los objetivos de la entidad relacionados con la privacidad.
P6.2	AWSCA-12.7	La entidad crea y retiene un registro completo, preciso y oportuno de las divulgaciones autorizadas de información personal para cumplir los objetivos de la entidad relacionados con la privacidad.

Controles de AWS asignados a los criterios de seguridad, disponibilidad, confidencialidad y privacidad

Criterios	Compatible con la actividad de control de AWS (AWSCA)	Descripción de los criterios
P6.3	AWSCA-8.1; AWSCA-8.2; AWSCA-9.5; AWSCA-10.3; AWSCA-12.5	La entidad crea y retiene un registro completo, preciso y oportuno de las divulgaciones no autorizadas detectadas o notificadas (incluidas las violaciones) de información personal para cumplir los objetivos de la entidad relacionados con la privacidad.
P6.4	AWSCA-11.1; AWSCA-11.2; AWSCA-11.3; AWSCA-12.4; AWSCA-12.5	La entidad obtiene compromisos de privacidad de proveedores y otros terceros que tienen acceso a información personal para cumplir los objetivos de la entidad relacionados con la privacidad. La entidad evalúa la conformidad de esas partes de forma periódica y en función de las necesidades y adopta medidas correctoras, si es necesario.
P6.5	AWSCA-8.1; AWSCA-8.2; AWSCA-11.1; AWSCA-11.2; AWSCA-11.3; AWSCA-12.5	La entidad obtiene el compromiso de los proveedores y otros terceros con acceso a la información personal de notificar a la entidad en caso de divulgación real o presunta no autorizada de información personal. Dichas notificaciones se comunican al personal adecuado y se actúa en consecuencia de acuerdo con los procedimientos establecidos de respuesta a incidentes para cumplir los objetivos de la entidad relacionados con la privacidad.
P6.6	AWSCA-8.2; AWSCA-12.5	La entidad notifica las violaciones y los incidentes a los interesados afectados, a los reguladores y a otros para cumplir los objetivos de la entidad relacionados con la privacidad.
P6.7	AWSCA-1.2; AWSCA-8.2; AWSCA-12.5; AWSCA-12.7; AWSCA-12.8; AWSCA-12.10; AWSCA-12.12	La entidad proporciona a los interesados una relación de la información personal que posee y la divulgación de la información personal de los interesados, a petición de estos, para cumplir los objetivos de la entidad relacionados con la privacidad.
P7.1	AWSCA-1.2; AWSCA-12.6	La entidad recopila y mantiene información personal precisa, actualizada, completa y relevante para cumplir los objetivos de la entidad relacionados con la privacidad.

Controles de AWS asignados a los criterios de seguridad, disponibilidad, confidencialidad y privacidad

Criterios	Compatible con la actividad de control de AWS (AWSCA)	Descripción de los criterios
P8.1	AWSCA-1.5; AWSCA-8.2; AWSCA-9.5; AWSCA-9.7; AWSCA-9.8; AWSCA-12.1; AWSCA-12.5	La entidad aplica un proceso para recibir, abordar, resolver y comunicar la resolución de consultas, reclamaciones y litigios de los interesados y otras personas, y monitorea periódicamente la conformidad para alcanzar los objetivos de la entidad relacionados con la privacidad. Las correcciones y otras medidas necesarias relacionadas con las deficiencias detectadas se realizan o adoptan a su debido tiempo.

Criterios de seguridad, disponibilidad, confidencialidad y privacidad asignados a las pruebas y controles del auditor de servicios de AWS realizados y a sus resultados

Controles establecidos por AWS	Criterios	Pruebas realizadas por EY	Resultados de las pruebas
AWSCA-1.1: la organización de AWS estableció las estructuras, las líneas jerárquicas con autoridades asignadas y las responsabilidades para cumplir de manera adecuada con los requisitos importantes sobre seguridad, disponibilidad, confidencialidad y privacidad.	CC1.1; CC1.3; CC1.5; CC5.3; CC7.3; CC7.4	Se consultó a un Program Manager de AWS Security Assurance para comprobar si la organización de AWS estableció las estructuras, las líneas jerárquicas con autoridades asignadas y las responsabilidades para cumplir con los requisitos de la empresa de manera adecuada, incluida la función de seguridad informática.	No se observaron desviaciones.
		Se inspeccionó el organigrama y el documento de procedimientos del gobierno de la seguridad informática para comprobar si la organización de AWS estableció las estructuras, las líneas jerárquicas con autoridades asignadas y las responsabilidades para cumplir adecuadamente los requisitos de seguridad, disponibilidad, confidencialidad y privacidad, lo que incluye la función de seguridad informática.	No se observaron desviaciones.

Criterios de seguridad, disponibilidad, confidencialidad y privacidad asignados a las pruebas y controles del auditor de servicios de AWS realizados y a sus resultados

Controles establecidos por AWS	Criterios	Pruebas realizadas por EY	Resultados de las pruebas
		Se inspeccionó la política del sistema integrado de gestión de la seguridad informática para comprobar si los líderes encargados de la seguridad aprobaron todo el documento en el último año y si los miembros correspondientes del equipo de Security aprobaron los cambios menores.	No se observaron desviaciones.
AWSCA-1.2: AWS mantiene políticas formales que proporcionan orientación para la seguridad informática dentro de la organización y el entorno de TI de respaldo.	CC1.1; CC1.3; CC1.4; CC1.5; CC2.1; CC2.2; CC5.1; CC5.2; CC5.3; CC6.1; CC6.7; CC7.2; CC7.4; CC9.1; P4.1; P4.2; P4.3; P6.7; P7.1; A1.2; A1.3; C1.1	Se consultó a un administrador de programa de AWS Security Assurance para comprobar que existen las políticas de seguridad oficiales, incluidas la designación de la responsabilidad y la rendición de cuentas para la administración del sistema y los controles, y se brindó orientación para la seguridad informática dentro de la organización y el entorno de TI de respaldo.	No se observaron desviaciones.
		Se inspeccionaron las políticas de seguridad informática enumeradas en la Descripción del sistema y la herramienta interna de políticas de Amazon para comprobar que incluían los procedimientos de seguridad para toda la organización como orientación para el entorno de AWS y el entorno de TI de respaldo.	No se observaron desviaciones.
AWSCA-1.3: los líderes de Security controlan y aprueban las políticas de	CC1.5; CC5.1; CC5.2; CC5.3	Se consultó a un Program Manager de AWS Security Assurance para comprobar si los líderes encargados de la seguridad controlaban y aprobaban las políticas de seguridad al menos una vez al año.	No se observaron desviaciones.

Criterios de seguridad, disponibilidad, confidencialidad y privacidad asignados a las pruebas y controles del auditor de servicios de AWS realizados y a sus resultados

Controles establecidos por AWS	Criterios	Pruebas realizadas por EY	Resultados de las pruebas
seguridad una vez al año.		Se inspeccionaron las políticas de seguridad listadas en la Descripción del sistema y en la herramienta interna de políticas de Amazon para comprobar que fueron aprobadas en el último año natural completo por los líderes de Security.	No se observaron desviaciones.
AWSCA-1.4: AWS preserva los programas de formación para empleados a fin de promover la concientización de los requisitos de seguridad informática de AWS, como se define en la Política de formación de concientización de la seguridad de AWS.	CC1.4; CC2.2; CC2.3; CC6.7; P3.1; P4.1	Se consultó a un Security Program Manager para comprobar si se habían establecido los programas de formación para empleados a fin de promover la concientización acerca de los requisitos de seguridad informática de AWS.	No se observaron desviaciones.
		Sobre una muestra de empleados de AWS seleccionados de la lista de empleados activos y contratistas de RR. HH., se inspeccionó la transcripción de la formación para comprobar si los empleados completaron el curso de formación de Amazon Security Awareness (ASA) dentro de los 60 días de la asignación de roles y que el curso de formación incluía los requisitos de seguridad informática y los requisitos de privacidad de los datos como se define en la Política de concientización de la seguridad informática de AWS.	No se observaron desviaciones.
AWSCA-1.5: AWS mantiene un programa de gestión de riesgos formal para identificar, analizar, gestionar, monitorear e informar de manera continua acerca de los riesgos que afectan los objetivos de negocio y los	CC2.1; CC3.1; CC3.2; CC3.3; CC3.4; CC4.2; CC5.1; CC5.2; CC5.3; CC9.1; CC9.2; A1.2;	Se consultó a un administrador sénior de riesgos regulatorios de AWS para comprobar que se mantenía un programa formal de administración de riesgos para identificar, analizar, tratar, monitorear e informar de manera continua acerca de los riesgos que afectan a los objetivos empresariales, los requisitos regulatorios y a los clientes de AWS. El programa identifica los riesgos, los documenta en un registro de riesgos según corresponda e informa de los resultados a los líderes al menos una vez por semestre.	No se observaron desviaciones.

Criterios de seguridad, disponibilidad, confidencialidad y privacidad asignados a las pruebas y controles del auditor de servicios de AWS realizados y a sus resultados

Controles establecidos por AWS	Criterios	Pruebas realizadas por EY	Resultados de las pruebas
requisitos regulatorios de AWS. El programa identifica los riesgos, los documenta en un registro de riesgos según corresponda e informa de los resultados a los líderes al menos una vez por semestre.	P8.1	Se inspeccionó la política de administración de riesgos de AWS para comprobar que estaba diseñada para describir cómo identificar, analizar, tratar, monitorear e informar de forma continua sobre los riesgos que afectan a los objetivos empresariales, los requisitos regulatorios y a los clientes de AWS, así como las opciones detalladas de tratamiento de riesgos, como la aceptación, la prevención, la mitigación y la transferencia.	No se observaron desviaciones.
		En el caso de una muestra de los riesgos seleccionados del registro de riesgos, se inspeccionó la documentación pertinente a fin de comprobar si la administración había identificado, analizado, tratado y monitoreado el riesgo.	No se observaron desviaciones.
AWSCA-1.6: específico de KMS. Los guardianes criptográficos de KMS documentan formalmente sus roles y responsabilidades y llegan a un acuerdo cuando asumen un rol o cuando las responsabilidades cambian.	CC2.2; CC2.3; CC6.7	Se consultó a un Cryptography Software Development Manager para comprobar si las personas documentaron y confirmaron de manera formal los roles y las responsabilidades de los guardianes de la criptografía KMS cuando asumieron o cambiaron las responsabilidades.	No se observaron desviaciones.
		Se seleccionó un grupo de personas del grupo de guardianes criptográficos de KMS con acceso a los sistemas que almacenan o usan material clave, y se inspeccionaron los documentos de los roles y las responsabilidades para comprobar si las responsabilidades de los usuarios se documentaron de manera formal y si las personas firmaron el documento.	No se observaron desviaciones.

Criterios de seguridad, disponibilidad, confidencialidad y privacidad asignados a las pruebas y controles del auditor de servicios de AWS realizados y a sus resultados

Controles establecidos por AWS	Criterios	Pruebas realizadas por EY	Resultados de las pruebas
AWSCA-1.7: la Junta y sus Comités cuentan con la cantidad de miembros independientes obligatoria, y cada miembro de la Junta y del Comité está calificado para desempeñar esa función. Todos los años, los miembros de la Junta completan cuestionarios para establecer si son independientes y están calificados o no para integrar el Comité de la Junta de acuerdo con las normas aplicables.	CC1.2; CC1.4	Se consultó al vicepresidente del Consejo general para comprobar si la junta y sus comités contaban con la cantidad necesaria de miembros de la junta independientes, y si todos los miembros de la junta y los comités estaban calificados para desempeñar esa función.	No se observaron desviaciones.
		Se inspeccionaron los estatutos de la empresa de Amazon y las directrices del gobierno corporativo de la empresa para comprobar que definían el número y las funciones de los miembros de la Junta directiva y sus responsabilidades.	No se observaron desviaciones.
		Se inspeccionó el cuestionario anual de los miembros de la Junta para comprobar que todos los miembros de la Junta completaron los cuestionarios y si incluían preguntas para determinar si los miembros eran independientes o estaban calificados para integrar cada parte del Comité de la Junta de acuerdo con los estatutos y las directrices aplicables.	No se observaron desviaciones.

Criterios de seguridad, disponibilidad, confidencialidad y privacidad asignados a las pruebas y controles del auditor de servicios de AWS realizados y a sus resultados

Controles establecidos por AWS	Criterios	Pruebas realizadas por EY	Resultados de las pruebas
AWSCA-1.8: la junta directiva realiza una evaluación anual de los miembros individuales de la junta y del rendimiento general de la junta. El Comité de gobierno corporativo y de nominación revisa y evalúa con frecuencia la composición de la junta. El Comité de Compensación y Desarrollo de Liderazgo, con la presencia de la Junta en pleno, evalúa anualmente el plan de sucesión de cada miembro del equipo de Senior Management. Como parte de la revisión de rendimiento anual del director ejecutivo (CEO) y la empresa la Junta revisa el plan de sucesión para el director.	CC1.2; CC1.4	Se consultó al vicepresidente del Consejo General para comprobar si la Junta directiva llevó a cabo la evaluación anual de los miembros individuales de la Junta y el rendimiento general de la Junta, si el Comité de gobierno corporativo de nominación revisó y analizó con frecuencia la composición de la Junta, y si el Comité de Compensación y Desarrollo de Liderazgo evaluó el plan de sucesión de cada miembro del equipo de gestión sénior, que incluye al director ejecutivo (CEO).	No se observaron desviaciones.
		Se inspeccionaron las actas de las reuniones del Gobierno Corporativo y de Nominación para comprobar si se analizó y completó la evaluación y revisión anual de la composición de la Junta Directiva.	No se observaron desviaciones.
		Se revisaron las actas de las reuniones de la Junta Directiva para comprobar si la Junta revisa el plan de sucesión del CEO y el equipo de gerencia sénior como parte de la revisión anual del desempeño de la empresa y el CEO.	No se observaron desviaciones.

Criterios de seguridad, disponibilidad, confidencialidad y privacidad asignados a las pruebas y controles del auditor de servicios de AWS realizados y a sus resultados

Controles establecidos por AWS	Criterios	Pruebas realizadas por EY	Resultados de las pruebas
AWSCA-1.9: AWS prepara y consolida el documento de planificación operativa de manera anual. El plan operativo incluye los objetivos de rendimiento y operativos, los requisitos de cumplimiento normativo con suficiente claridad para habilitar la identificación y evaluación de los riesgos relacionados con los objetivos.	CC2.1; CC2.2; CC3.1; CC3.2	Se consultó al administrador sénior de análisis y planificación financiera para comprobar si AWS preparó y consolidó de manera anual el documento de planificación operativa, que incluye los objetivos operativos y de rendimiento, así como los requisitos regulatorios y de cumplimiento con la suficiente claridad para habilitar la identificación y evaluación de los riesgos relacionados con los objetivos.	No se observaron desviaciones.
		Se inspeccionó el seguimiento de los entregables y las invitaciones a reuniones relacionados con la creación del documento de planificación operativa para comprobar que incluía los objetivos operativos y de rendimiento, así como los requisitos regulatorios y de conformidad que identificaban y evaluaban los riesgos relacionados con estos objetivos.	No se observaron desviaciones.
AWSCA-1.10: AWS cuenta con un proceso para revisar los riesgos medioambientales y geopolíticos antes de lanzar una nueva región.	CC2.1; CC3.1; CC3.2; CC3.3; CC3.4; CC4.1; CC4.2; CC5.1; CC5.2; CC5.3; CC9.1; CC9.2; A1.2	Se consultó al administrador sénior de riesgos y resiliencia para comprobar que los riesgos medioambientales y geopolíticos se revisaban antes de lanzar nuevas regiones de centros de datos.	No se observaron desviaciones.
		Para todas las regiones de centros de datos nuevas dentro del alcance seleccionadas del sistema de inventario del centro de datos, se realizó una inspección de la documentación de revisión para comprobar si se realizaba una revisión de los riesgos medioambientales y geopolíticos antes de lanzar la nueva región de centro de datos.	No se observaron desviaciones.
AWSCA-2.1: el acceso de los usuarios a la red interna de Amazon no se proporciona, a	CC6.1; CC6.2; CC6.3	Se consultó a un ingeniero sénior de desarrollo de software de evaluación y autorización de trabajo para comprobar si el acceso de los usuarios a la red interna de Amazon no se activaba, a menos que	No se observaron desviaciones.

Criterios de seguridad, disponibilidad, confidencialidad y privacidad asignados a las pruebas y controles del auditor de servicios de AWS realizados y a sus resultados

Controles establecidos por AWS	Criterios	Pruebas realizadas por EY	Resultados de las pruebas
menos que Recursos Humanos cree un registro activo en el Sistema de RR. HH. El acceso se aprovisiona de forma automática con privilegio mínimo por función de trabajo. Las primeras contraseñas se establecen con un valor único y se cambian de manera inmediata después del primer uso.		Recursos Humanos creara un registro activo en el sistema de RR. HH., si el acceso se concedía automáticamente con privilegio mínimo por función de trabajo y si las primeras contraseñas se establecían con un valor único y se cambiaban de manera inmediata después del primer uso.	
		Se inspeccionaron las configuraciones de los sistemas responsables de aprovisionar acceso a la red interna de Amazon para comprobar que el acceso a las cuentas de usuario de Windows y UNIX no se podía aprovisionar, a menos que Recursos Humanos creara un registro activo en el Sistema de RR. HH., que el acceso se aprovisionara automáticamente con el privilegio mínimo por función de trabajo antes de las fechas de inicio de los empleados, y que las primeras contraseñas se configuraran para crear un valor único y debieran cambiarse inmediatamente después del primer uso.	No se observaron desviaciones.
		Se seleccionó a un nuevo empleado de la empresa y a un nuevo empleado socio a partir de un listado de nuevas contrataciones generado por el sistema de RR. HH. y se inspeccionó el registro del empleado en el sistema de RR. HH. para comprobar si dicho sistema activaba el registro antes de la creación de las cuentas de Windows y UNIX de un empelado y si las contraseñas de primera vez se cambiaban de inmediato después de que el empleado utilizara la cuenta por primera vez.	No se observaron desviaciones.

Criterios de seguridad, disponibilidad, confidencialidad y privacidad asignados a las pruebas y controles del auditor de servicios de AWS realizados y a sus resultados

Controles establecidos por AWS	Criterios	Pruebas realizadas por EY	Resultados de las pruebas
AWSCA-2.2: el acceso de TI por encima del privilegio mínimo, incluidas las cuentas de administrador, lo aprueba el personal adecuado antes del aprovisionamiento del acceso.	CC6.1; CC6.2; CC6.3; CC6.7; CC6.8	Se preguntó a los Software Development Managers para comprobar si el acceso de TI por encima de los privilegios mínimos, incluidas las cuentas de administrador, lo había aprobado el personal adecuado antes del aprovisionamiento del acceso.	No se observaron desviaciones.
		Se inspeccionaron las configuraciones del sistema responsables del proceso de aprovisionamiento de acceso para comprobar que el acceso de TI por encima de los privilegios mínimos, incluidas las cuentas de administrador, debía ser aprobado por el personal adecuado antes de la provisión automática de acceso.	No se observaron desviaciones.
		Se seleccionó a un empleado activo y se inspeccionó el proceso de aprovisionamiento del acceso para comprobar si el personal adecuado aprobaba el acceso antes del aprovisionamiento automático del acceso.	No se observaron desviaciones.
AWSCA-2.3: el personal adecuado revisa de forma periódica los privilegios de acceso de TI.	CC6.1; CC6.2; CC6.3; CC6.7; CC6.8	Se les consultó a los Software Development Managers para comprobar si el personal adecuado revisaba y aprobaba el acceso a los sistemas de apoyo a la infraestructura y a la red por encima de los privilegios mínimos de manera trimestral.	No se observaron desviaciones.
		Se les consultó a los Software Development Managers para comprobar si el personal adecuado revisaba y aprobaba el acceso a las cuentas internas de AWS por encima de los privilegios mínimos de manera semestral.	No se observaron desviaciones.
		Se inspeccionaron las configuraciones de los sistemas responsables del proceso de revisión de los accesos para comprobar que el personal adecuado revisaba trimestralmente los privilegios de acceso a la infraestructura de TI y a la red de forma	No se observaron desviaciones.

Criterios de seguridad, disponibilidad, confidencialidad y privacidad asignados a las pruebas y controles del auditor de servicios de AWS realizados y a sus resultados

Controles establecidos por AWS	Criterios	Pruebas realizadas por EY	Resultados de las pruebas
		automatizada o que el acceso se eliminaba automáticamente.	
		Se inspeccionaron las configuraciones de los sistemas responsables del proceso de revocación de acceso temporal para comprobar si, cuando los privilegios temporales a los recursos caducaban, el acceso a los recursos se eliminaba automáticamente.	No se observaron desviaciones.
		Se inspeccionaron las configuraciones de los sistemas responsables del proceso de revocación interno de transferencias para comprobar si, cuando un usuario realizaba una transferencia interna, el acceso a los recursos anteriores se eliminaba automáticamente.	No se observaron desviaciones.
		Se seleccionó a un grupo de acceso activo de privilegios de acceso a la infraestructura de TI y a la red marcados para su eliminación como parte del proceso de revisión del acceso de los usuarios y se inspeccionó el registro para comprobar si el acceso se revocaba de forma automática.	No se observaron desviaciones.
		Se observó cómo un Software Development Manager marcaba una cuenta interna activa de AWS para su eliminación como parte del proceso de revisión del acceso de los usuarios y se inspeccionó la cuenta después de la revisión para comprobar que el acceso se revocaba de forma automática.	No se observaron desviaciones.
		Se seleccionó un usuario con acceso temporal a la infraestructura de TI y privilegios de acceso a la red para comprobar que, cuando los privilegios temporales del	No se observaron desviaciones.

Criterios de seguridad, disponibilidad, confidencialidad y privacidad asignados a las pruebas y controles del auditor de servicios de AWS realizados y a sus resultados

Controles establecidos por AWS	Criterios	Pruebas realizadas por EY	Resultados de las pruebas
		recurso se vencieron, el acceso se revocó automáticamente.	
		Se seleccionó a un grupo de acceso activo de privilegios de acceso a la infraestructura de TI y a la red que no se revisó durante el trimestre, y se inspeccionaron los registros de acceso para comprobar si los privilegios se revocaban de forma automática.	No se observaron desviaciones.
		Se seleccionó un grupo de acceso activo y se inspeccionó el proceso de revisión del acceso para comprobar que el personal adecuado revisaba de manera trimestral la infraestructura de TI y los privilegios de acceso a la red.	No se observaron desviaciones.
		Se seleccionó una muestra de cuentas de AWS a partir de un listado generado por el sistema de cuentas internas activas de AWS y se inspeccionó el proceso de revisión del acceso para comprobar que el personal adecuado revisaba los privilegios de acceso a las cuentas internas de AWS semestralmente.	No se observaron desviaciones.
AWSCA-2.4: el acceso de los usuarios a los sistemas de Amazon se revoca en un plazo de 24 horas a partir de la cancelación (desactivación) del registro del empleado en el sistema de RR. HH.	CC6.1; CC6.2; CC6.3	Se consultó a un ingeniero sénior de desarrollo de software de evaluación y autorización de trabajo para comprobar si el acceso a los sistemas se revocó de manera automática en un plazo de 24 horas a partir de la cancelación (desactivación) del registro del empleado en el sistema de RR. HH.	No se observaron desviaciones.
		Se inspeccionaron las configuraciones del sistema responsable de terminar el acceso a los sistemas de Amazon para comprobar si el acceso a las cuentas de usuarios de Windows y UNIX se configuró para que se revoque de manera automática en un plazo de 24 horas	No se observaron desviaciones.

Criterios de seguridad, disponibilidad, confidencialidad y privacidad asignados a las pruebas y controles del auditor de servicios de AWS realizados y a sus resultados

Controles establecidos por AWS	Criterios	Pruebas realizadas por EY	Resultados de las pruebas
por parte de Recursos Humanos.		después de que se terminara (desactivara) el registro de un empleado en el sistema de RR. HH.	
		Se inspeccionó el registro del sistema de RR. HH. de un empleado despedido para comprobar si el acceso a los sistemas de Amazon se revocó de manera automática en un plazo de 24 horas en las cuentas Unix/LDAP y Windows/AD.	No se observaron desviaciones.
AWSCA-2.5: las configuraciones se administran de conformidad con la Política de contraseñas de Amazon.com.	CC6.1 CC6.3;	Se le consultó a un Corporate Systems Manager y a un Corporate Response Manager para comprobar si se aplicó la complejidad de la contraseña, la longitud, la antigüedad máxima, el historial, el bloqueo y el monitoreo de la credencial de acuerdo con la Política de contraseñas de Amazon.com.	No se observaron desviaciones.
		Se inspeccionaron las configuraciones de la contraseña en el dominio de Active Directory para comprobar si se configuraron a fin de aplicar la Política de contraseñas de Amazon.com, que incluye lo siguiente: • Las contraseñas deben tener al menos ocho (8) caracteres. • Las contraseñas deben contener una combinación de letras, números y caracteres especiales • Las contraseñas no deben contener el nombre real del usuario ni el nombre del usuario. • Las contraseñas no deben ser modificaciones o incrementos de una contraseña utilizada recientemente para la cuenta.	No se observaron desviaciones.

Criterios de seguridad, disponibilidad, confidencialidad y privacidad asignados a las pruebas y controles del auditor de servicios de AWS realizados y a sus resultados

Controles establecidos por AWS	Criterios	Pruebas realizadas por EY	Resultados de las pruebas
		• Las cuentas se bloquean después de 6 intentos no válidos	
		Se observó que las siguientes configuraciones de las contraseñas se aplicaban de acuerdo con la política de contraseñas de Amazon.com después de intentar establecer una combinación de contraseñas que no cumplían la política utilizando la herramienta de contraseñas en el entorno de producción: • Las contraseñas deben tener al menos ocho caracteres • Las contraseñas deben contener una combinación de letras, números y caracteres especiales • Las contraseñas no deben contener el nombre real del usuario ni el nombre del usuario. • Las contraseñas no deben ser iguales ni similares a una contraseña utilizada recientemente. • Las contraseñas no deben contener la palabra “Amazon” ni ningún otro nombre comercial.	No se observaron desviaciones.
		Se inspeccionó la configuración del monitoreo del compromiso de la credencial para comprobar si los tickets de incidentes se creaban de manera automática y se registraban en el sistema de tickets según la Política de contraseñas de Amazon.com.	No se observaron desviaciones.

Criterios de seguridad, disponibilidad, confidencialidad y privacidad asignados a las pruebas y controles del auditor de servicios de AWS realizados y a sus resultados

Controles establecidos por AWS	Criterios	Pruebas realizadas por EY	Resultados de las pruebas
		Se inspeccionó un ticket de incidente creado para las credenciales del usuario afectadas para comprobar si se identificaron, rotaron y rastrearon las credenciales de las cuentas de Amazon marcadas.	No se observaron desviaciones.
AWSCA-2.6: AWS requiere una autenticación de dos factores sobre un canal criptográfico aprobado para la autenticación de la red interna de AWS desde ubicaciones remotas.	CC6.1; CC6.3; CC6.6	Se le consultó a un Corporate Systems Manager para comprobar si se solicitaba la autenticación de dos factores sobre un canal criptográfico aprobado para acceder a la red de la empresa de Amazon desde ubicaciones remotas.	No se observaron desviaciones.
		Se inspeccionó la configuración del protocolo de autenticación de los servidores RADIUS y SAML para comprobar si la autenticación de la red interna de AWS desde ubicaciones remotas requería una autenticación de dos factores sobre un canal criptográfico aprobado.	No se observaron desviaciones.
		Se intentó iniciar sesión en la red de la empresa de Amazon desde una ubicación remota para comprobar si se solicitaba un token físico y una contraseña para acceder a la red de la empresa de Amazon sobre un canal criptográfico aprobado.	No se observaron desviaciones.

Criterios de seguridad, disponibilidad, confidencialidad y privacidad asignados a las pruebas y controles del auditor de servicios de AWS realizados y a sus resultados

Controles establecidos por AWS	Criterios	Pruebas realizadas por EY	Resultados de las pruebas
AWSCA-3.1: los dispositivos de firewall se configuran para restringir el acceso al entorno informático y aplicar límites en los clústeres de computación.	CC6.1; CC6.6; CC7.1; CC8.1	Se consultó a un Infrastructure Security Engineer de AWS para comprobar que los dispositivos de firewall se configuraron para restringir el acceso al entorno de computación y reforzar los límites de los clústeres informáticos.	No se observaron desviaciones.
		Se seleccionó una muestra de firewalls a partir de un listado generado por el sistema de firewalls dentro del alcance y se inspeccionaron las listas de control de acceso para comprobar si los dispositivos estaban configurados para denegar todos los accesos al entorno computacional y aplicar límites a los clústeres computacionales, a menos que se autorizara de forma explícita.	No se observaron desviaciones.
AWSCA-3.2: las políticas de firewall (archivos de configuración) se envían de manera automática a los dispositivos de firewall de producción.	CC6.1; CC6.6; CC7.1; CC8.1	Se consultó a un Infrastructure Security Engineer de AWS para comprobar si las políticas de firewall se enviaban de manera automática a los dispositivos de firewall de producción.	No se observaron desviaciones.
		Se seleccionó una muestra de dispositivos de firewall a partir de un listado generado por el sistema de firewalls dentro del alcance y se inspeccionó la salida del registro de despliegue para comprobar si las políticas se enviaban automáticamente a los dispositivos de firewall de producción.	No se observaron desviaciones.
AWSCA-3.3: se revisan y aprueban las actualizaciones	CC6.1; CC6.6; CC7.1; CC8.1	Se consultó a un Infrastructure Security Engineer de AWS para comprobar si se revisaban y aprobaban las actualizaciones de las políticas de firewall del centro de datos.	No se observaron desviaciones.

Criterios de seguridad, disponibilidad, confidencialidad y privacidad asignados a las pruebas y controles del auditor de servicios de AWS realizados y a sus resultados

Controles establecidos por AWS	Criterios	Pruebas realizadas por EY	Resultados de las pruebas
de las políticas de firewall.		Se seleccionó una muestra de actualizaciones de la política de firewall a partir de un listado generado por el sistema de firewall incluida dentro del alcance y en las que se aplicaran las actualizaciones de las políticas de firewall, y se inspeccionaron las evidencias de aprobación para comprobar si el personal adecuado las había revisado y aprobado antes de su aplicación.	No se observaron desviaciones.
		Se seleccionó una muestra de empleados a partir de un listado generado por el sistema de individuos elegibles para aprobar solicitudes de ACL y se inspeccionó el puesto y el equipo del empleado para comprobar si las aprobaciones y los derechos de acceso de los usuarios eran apropiados.	No se observaron desviaciones.
AWSCA-3.4: AWS realiza evaluaciones de vulnerabilidad externas al menos una vez por trimestre y los problemas identificados se investigan y se rastrean hasta su resolución de forma oportuna.	CC3.2; CC3.3; CC3.4; CC4.1; CC6.8; CC7.1; CC7.2; CC7.4	Se le consultó a un Technical Program Manager de AWS Security para comprobar si se realizaron las evaluaciones de vulnerabilidad externa y si se investigaron los problemas identificados y se realizó un seguimiento hasta sus resoluciones.	No se observaron desviaciones.
		Se inspeccionó la lista de los puntos finales de producción de las herramientas de evaluación de vulnerabilidad de las evaluaciones de vulnerabilidad externas trimestrales que se realizaron para comprobar si los hosts de producción de los servicios incluidos (compatibles con los puntos finales públicos) formaban parte de los análisis trimestrales.	No se observaron desviaciones.

Criterios de seguridad, disponibilidad, confidencialidad y privacidad asignados a las pruebas y controles del auditor de servicios de AWS realizados y a sus resultados

Controles establecidos por AWS	Criterios	Pruebas realizadas por EY	Resultados de las pruebas
		Se seleccionó una muestra de trimestres y se inspeccionó la evidencia de las evaluaciones de vulnerabilidades externas para comprobar si se realizaron las evaluaciones, si se documentaron los resultados y si existía un proceso para el seguimiento, el tratamiento y la resolución oportunos de los problemas identificados.	No se observaron desviaciones.
AWSCA-3.5: AWS habilita a los clientes para que seleccionen quién tiene acceso a los servicios y recursos de AWS (si los permisos a nivel de recursos son aplicables al servicio) que poseen. AWS impide que los clientes accedan a los recursos de AWS que no tienen asignados mediante permisos de acceso. El contenido solo se devuelve a las personas autorizadas a acceder al servicio o recurso de AWS especificado (si los permisos a nivel de recurso son aplicables al servicio).	CC6.1	Se consultó a los administradores de desarrollo de software para asegurarse de que los clientes habilitados de AWS pudieran seleccionar quiénes tienen acceso a los servicios y recursos de AWS que poseen, que se evitó el acceso de los clientes a los recursos de AWS que no estaban asignados a ellos a través de los permisos de acceso, y que el contenido solo se devolvía a las personas que tenían autorización para acceder al servicio o recurso específico de AWS.	No se observaron desviaciones.
		Se inspeccionaron las configuraciones existentes para los servicios de AWS que administraban el acceso externo a los servicios y recursos de AWS (si los permisos a nivel de recursos eran aplicables al servicio), para comprobar si los servicios estaban diseñados para devolver el contenido solo a las personas autorizadas a acceder al servicio o recurso de AWS específico, y si AWS impedía que los clientes accedieran a recursos que no se les habían asignado mediante permisos de acceso.	No se observaron desviaciones.
		Se observó a un usuario con permisos de acceso autorizados intentar acceder a los servicios y recursos de AWS para comprobar que los servicios devolvían contenido solo a personas con acceso autorizado al servicio o recurso de AWS específico.	No se observaron desviaciones.

Criterios de seguridad, disponibilidad, confidencialidad y privacidad asignados a las pruebas y controles del auditor de servicios de AWS realizados y a sus resultados

Controles establecidos por AWS	Criterios	Pruebas realizadas por EY	Resultados de las pruebas
		Se observó a un usuario sin permisos de accesos autorizados que intentó acceder a los servicios y recursos de AWS para comprobar si los servicios no devolvían contenido a personas con acceso no autorizado al servicio o recurso de AWS especificado.	No se observaron desviaciones.
AWSCA-3.6: AWS realiza revisiones de seguridad informática de las aplicaciones para los productos y servicios lanzados externamente y las adiciones de características significativas antes del lanzamiento para evaluar si se identifican y mitigan los riesgos de seguridad.	CC2.1; CC6.1; CC7.1; CC8.1; P3.1; P4.1; P4.2	Se consultó a un Technical Program Manager de Application Security para comprobar si AWS realizó las revisiones de la seguridad informática de las aplicaciones para los productos y servicios lanzados externamente y las adiciones de características significativas antes del lanzamiento para evaluar si se identifican y mitigan los riesgos de seguridad.	No se observaron desviaciones.
		Se seleccionó una muestra de productos, servicios y adiciones de características significativas a partir de un listado generado por el sistema de representaciones de tickets de problemas lanzados durante el período y se inspeccionó la revisión del equipo de Application Security para comprobar si los productos, servicios y adiciones de características significativas se revisaron antes del lanzamiento.	No se observaron desviaciones.
AWSCA-3.7: específico de S3. AWS configura los dispositivos de red para permitir el acceso solo a puertos específicos en otros sistemas de servidores dentro de Amazon S3.	CC6.1; CC6.6;	Se consultó a un Software Development Manager de S3 para comprobar si los dispositivos de red se configuraron para permitir el acceso solo a puertos específicos en sistemas de servidores dentro de Amazon S3.	No se observaron desviaciones.
		Se seleccionó una muestra de dispositivos de red de S3 a partir de un listado de dispositivos de red de S3 generado con el repositorio de códigos de S3 y se inspeccionaron los ajustes de configuración con el fin de comprobar si los dispositivos estaban configurados para permitir el acceso solo a puertos específicos.	No se observaron desviaciones.

Criterios de seguridad, disponibilidad, confidencialidad y privacidad asignados a las pruebas y controles del auditor de servicios de AWS realizados y a sus resultados

Controles establecidos por AWS	Criterios	Pruebas realizadas por EY	Resultados de las pruebas
AWSCA-3.8: específico de S3. El acceso a datos externos se registra con la dirección IP de acceso a los datos, el objeto y la operación. Los registros se retienen durante al menos 90 días.	CC6.1; CC6.6;	Se consultó a un Software Development Engineer de S3 para comprobar si el acceso a datos externos se registraba con la dirección IP de acceso a los datos, el objeto y la operación, y si los registros se retenían durante al menos 90 días.	No se observaron desviaciones.
		Se inspeccionaron los ajustes de configuración que se envían a los servidores web S3 para comprobar si los servidores se configuraron para registrar la dirección IP de acceso a los datos, el objeto y la operación.	No se observaron desviaciones.
		Se seleccionó una muestra de las zonas de disponibilidad (AZ) de AWS a partir de un listado de AZ generado con el repositorio de códigos de AZ y se inspeccionaron las configuraciones operativas del entorno para la retención de registros de acceso externo a datos con el fin de comprobar que los registros estaban configurados para retenerse durante 90 días.	No se observaron desviaciones.
		Se observó a un ingeniero de desarrollo de software realizar una operación de acceso a un objeto S3 y se inspeccionó el resultado del registro del acceso a datos externos luego de 90 días para comprobar si se registró la siguiente información durante 90 días como mínimo: la dirección IP del descriptor de acceso de datos que accede a los datos, el objeto al que se accedió y la operación que se realizó.	No se observaron desviaciones.
AWSCA-3.9: específico de EC2. Los host físicos poseen firewalls basados en un host	CC6.1; CC6.6	Se consultó a un Security Manager de EC2 para comprobar si los hosts físicos de EC2 contaban con firewall basados en un host o si el acceso se restringió de manera lógica para prevenir el acceso sin autorización.	No se observaron desviaciones.

Criterios de seguridad, disponibilidad, confidencialidad y privacidad asignados a las pruebas y controles del auditor de servicios de AWS realizados y a sus resultados

Controles establecidos por AWS	Criterios	Pruebas realizadas por EY	Resultados de las pruebas
para prevenir el acceso sin autorización.		Se inspeccionaron las configuraciones automatizadas responsables de configurar un nuevo host para comprobar que los firewalls basados en un host se agregaban automáticamente durante el proceso de creación de nuevos hosts.	No se observaron desviaciones.
		Se inspeccionaron las configuraciones de monitoreo de los hosts físicos para comprobar si se había establecido un monitoreo para notificar a los miembros del equipo de servicio en caso de que un host físico no tuviera un firewall activo.	No se observaron desviaciones.
		Se observó a un ingeniero de seguridad de EC2 realizar una solicitud de API con y sin el token correcto para comprobar si se solicitaba el token de acceso basado en un host para autorizar el acceso al host.	No se observaron desviaciones.
		Se seleccionó una muestra de hosts físicos de EC2 compatibles con las regiones de AWS que están dentro del alcance a partir de los listados de hosts de producción de cada región y se inspeccionó la configuración del firewall basado en un host para comprobar si contaba con firewalls basados en un host y si funcionaba para prevenir el acceso sin autorización.	No se observaron desviaciones.
AWSCA-3.10: específico de EC2. Los hosts virtuales están detrás de los firewalls del software que se configuran para	CC6.1	Se consultó a un Security Manager de EC2 para comprobar si los hosts virtuales estaban detrás de los firewall del software, que evitaba el spoofing de TCP/IP, la búsqueda (sniffing) de paquetes y restringía las conexiones entrantes a los puertos de un cliente específico.	No se observaron desviaciones.

Criterios de seguridad, disponibilidad, confidencialidad y privacidad asignados a las pruebas y controles del auditor de servicios de AWS realizados y a sus resultados

Controles establecidos por AWS	Criterios	Pruebas realizadas por EY	Resultados de las pruebas
prevenir la *spoofing* de TCP/IP, la búsqueda (*sniffing*) de paquetes y restringir las conexiones entrantes a los puertos de un cliente específico.		Se observó a un Security Engineer de EC2 mientras creaba un host virtual de EC2 con un firewall configurado para comunicarse solo con direcciones IP específicas y se comprobó que las comunicaciones con la dirección IP específica tuvieron éxito.	No se observaron desviaciones.
		Se observó a un Security Engineer de EC2 intentar comunicarse con una dirección IP no especificada para comprobar si se rechazaban los intentos.	No se observaron desviaciones.
		Se observó a un Security Engineer de EC2 crear un host EC2 virtual y se inspeccionaron las configuraciones de la tabla de IP para comprobar si el tráfico estaba dirigido para prevenir el spoofing de TCP/IP.	No se observaron desviaciones.
		Se observó a un Security Engineer de EC2 mientras creaba dos instancias de EC2 en un solo host de EC2 físico y generaba tráfico de red en cada instancia para comprobar que ninguna de las instancias pudiese capturar el paquete a través de la escucha de la red del tráfico de la otra instancia.	No se observaron desviaciones.
AWSCA-3.11: específico de EC2. AWS evita que los clientes accedan a las AMI personalizadas que	CC6.1	Se le preguntó a un ingeniero de seguridad EC2 para comprobar si AWS evitaba que los clientes accedan a las AMI personalizadas que no tienen asignadas mediante los permisos de lanzamiento de manera predeterminada.	No se observaron desviaciones.

Criterios de seguridad, disponibilidad, confidencialidad y privacidad asignados a las pruebas y controles del auditor de servicios de AWS realizados y a sus resultados

Controles establecidos por AWS	Criterios	Pruebas realizadas por EY	Resultados de las pruebas
no tienen asignadas mediante una propiedad de la AMI llamada permisos de lanzamiento. De manera predeterminada, los permisos de lanzamiento de una AMI restringen su uso al cliente o cuenta que la creó y la registró.		Se inspeccionó la configuración de permisos de lanzamiento de AMI en la consola de AWS para comprobar que, de manera predeterminada, el permiso de lanzamiento de una AMI restringe su uso a la cuenta que la creó, a menos que el cliente conceda permisos de acceso.	No se observaron desviaciones.
		Se creó una AMI, se intentó acceder a la AMI sin los permisos de lanzamiento designados y, según la inspección del mensaje del error dentro de la consola de administración de AWS, se comprobó que el acceso estaba restringido.	No se observaron desviaciones.
AWSCA-3.12: específico de EC2. AWS evita que los clientes accedan a hosts físicos o instancias que no tienen asignados mediante el filtro del software de virtualización.	CC6.1	Se consultó a un Security Manager de EC2 para comprobar si los clientes tenían el acceso restringido a los host físicos o instancias que no tienen asignados mediante el filtro del software de virtualización.	No se observaron desviaciones.
		Se observó que un Security Engineer de EC2 intentó realizar un *ping* IP a un *host* físico EC2 desde una instancia de EC2 dentro del *host* para comprobar si el *host* físico estaba aislado de las instancias.	No se observaron desviaciones.
		Se observó que un Security Engineer de EC2 intentó acceder a un archivo almacenado en una instancia EC2 desde el host EC2 físico en el que se encontraba la instancia, para comprobar que no se podía acceder a las instancias ubicadas en un host físico.	No se observaron desviaciones.

Criterios de seguridad, disponibilidad, confidencialidad y privacidad asignados a las pruebas y controles del auditor de servicios de AWS realizados y a sus resultados

Controles establecidos por AWS	Criterios	Pruebas realizadas por EY	Resultados de las pruebas
		Se observó a un Security Engineer de EC2 realizar el intento de acceder a un archivo almacenado en una instancia de EC2 desde una instancia diferente en el mismo host físico EC2 para comprobar si las instancias en los mismos hosts físicos estaban aisladas entre sí.	No se observaron desviaciones.
AWSCA-3.13: específico de VPC. Las comunicaciones de red dentro de una VPC están aisladas de las comunicaciones de red dentro de otras VPC.	CC6.1	Se le preguntó a un ingeniero de desarrollo de *software* de red EC2 para comprobar si las comunicaciones de red entre las diferentes VPC estaban aisladas entre sí.	No se observaron desviaciones.
		Se observó a un Networking Software Development Engineer de EC2 configurar la infraestructura de VPC para dos VPC e intentar comunicarse entre instancias a través de las dos VPC a fin de comprobar que las comunicación de red entre las dos VPC estaba aislada.	No se observaron desviaciones.
AWSCA-3.14: específico de VPC. Las comunicaciones de red dentro de una puerta de enlace VPN están aisladas de las comunicaciones de red dentro de otras puertas de enlace VPN.	CC6.1	Se le preguntó a un ingeniero de desarrollo de *software* de red EC2 para comprobar si las comunicaciones de red entre las puertas de enlace VPC estaban aisladas entre sí.	No se observaron desviaciones.
		Se observó a un ingeniero de desarrollo de software de redes de EC2 configurar una infraestructura de VPC con dos puertas de enlace de VPN e intentar comunicarse entre las instancias en las dos puertas de enlace de VPN a fin de comprobar que la comunicación de red entre las dos puertas de enlace de VPN estaba aislada.	No se observaron desviaciones.

Criterios de seguridad, disponibilidad, confidencialidad y privacidad asignados a las pruebas y controles del auditor de servicios de AWS realizados y a sus resultados

Controles establecidos por AWS	Criterios	Pruebas realizadas por EY	Resultados de las pruebas
AWSCA-3.15: específico de VPC. El tráfico de Internet mediante una puerta de enlace de Internet se reenvía a una instancia en una VPC solo cuando una puerta de enlace de Internet se adjunta a una VPC y una IP pública se asigna a una instancia en la VPC.	CC6.1	Se consultó a un ingeniero de seguridad de EC2 para comprobar si el tráfico de Internet mediante una puerta de enlace de Internet solo se reenviaba a una instancia en una VPC cuando se conectaba una puerta de enlace de Internet a una VPC y una IP pública se asignaba a la instancia en la VPC.	No se observaron desviaciones.
		Se creó una VPC, se conectó una puerta de enlace de Internet, se asignó una IP pública y, según la inspección del tráfico en una instancia, se comprobó que el tráfico se reenvió con éxito.	No se observaron desviaciones.
		Se eliminó la puerta de enlace de Internet y la IP pública de la VPC y, según la inspección del tráfico en la instancia, se comprobó que se evitaba el reenvío del tráfico.	No se observaron desviaciones.

Criterios de seguridad, disponibilidad, confidencialidad y privacidad asignados a las pruebas y controles del auditor de servicios de AWS realizados y a sus resultados

Controles establecidos por AWS	Criterios	Pruebas realizadas por EY	Resultados de las pruebas
AWSCA-3.16: AWS mantiene políticas y procedimientos formales que proporcionan orientación para las operaciones y la seguridad de la información dentro de la organización y los entornos de respaldo de AWS. La política de	CC6.4; CC6.7; CC8.1	Se consultó a un Risk Management Program Manager de AWS para comprobar si existían las políticas y procedimientos formales para el uso de los dispositivos móviles y si se incluyó la orientación para las operaciones y la seguridad informática de las organizaciones que apoyan los entornos de AWS.	No se observaron desviaciones.
		Se inspeccionó el sitio web interno de AWS para comprobar si los empleados de AWS disponían de políticas y procedimientos formales para el uso de dispositivos móviles.	No se observaron desviaciones.

Criterios de seguridad, disponibilidad, confidencialidad y privacidad asignados a las pruebas y controles del auditor de servicios de AWS realizados y a sus resultados

Controles establecidos por AWS	Criterios	Pruebas realizadas por EY	Resultados de las pruebas
dispositivos móviles proporciona orientación sobre lo siguiente: • El uso de los dispositivos móviles. • La protección de los dispositivos que acceden al contenido del cual Amazon es responsable. • La capacidad de borrado remoto. • Las restricciones de protección contra la averiguación de contraseñas. • Los requisitos de sincronización remota. • Los requisitos de revisión de seguridad. • Los métodos aprobados para acceder a los datos de Amazon.		Se inspeccionó la política sobre los dispositivos móviles para comprobar que incluya los procedimientos de seguridad en toda la organización como orientación sobre el entorno de AWS con respecto a lo siguiente: • El uso de los dispositivos móviles • La protección de los dispositivos que acceden al contenido del cual Amazon es responsable • La capacidad de borrado remoto • Las restricciones de protección contra la averiguación de contraseñas • Los requisitos de sincronización remota • Los requisitos de revisión de seguridad. • Los métodos aprobados para acceder a los datos de Amazon.	No se observaron desviaciones.
AWSCA-3.17: específico de Outpost. Service Link se establece entre Outpost y la región	CC6.1; CC6.7;	Se consultó a un Senior Security Engineer de AWS para comprobar si Service Link se estableció entre Outposts y la región de AWS a través de una conexión de VPN protegida en Internet público o AWS Direct Connect.	No se observaron desviaciones.

Criterios de seguridad, disponibilidad, confidencialidad y privacidad asignados a las pruebas y controles del auditor de servicios de AWS realizados y a sus resultados

Controles establecidos por AWS	Criterios	Pruebas realizadas por EY	Resultados de las pruebas
de AWS a través de una conexión de VPN protegida en Internet público o AWS Direct Connect.		Se inspeccionaron las configuraciones de los Outposts para comprobar si Service Link se estableció entre el Outpost y la región de AWS a través de una conexión de VPN protegida en Internet público o AWS Direct Connect.	No se observaron desviaciones.
		Se inspeccionaron los paneles de un Outpost para comprobar si se rastreó y monitoreó el estado de la conexión de VPN protegida entre el Outpost y la región de AWS.	No se observaron desviaciones.
		Se inspeccionaron las configuraciones del monitoreo de un Outpost activo para comprobar si se configuró la alarma para la conexión de VPN protegida a fin de informar a los miembros del equipo del servicio en el caso de problemas en la red.	No se observaron desviaciones.
AWSCA-3.18: se instaló, actualizó y ejecutó el software antivirus en las estaciones de trabajo.	CC6.7; CC6.8;	Se consultó a un Senior Security Engineer de AWS para comprobar si el software antivirus se instaló, actualizó y ejecutó en las estaciones de trabajo.	No se observaron desviaciones.
		Se inspeccionaron las configuraciones del antivirus en la consola del administrador para la generación de imágenes en las estaciones de trabajo con el fin de comprobar si existe el software antivirus para monitorear el código malicioso, se actualiza automáticamente con las nuevas versiones o definiciones de virus e impide que los usuarios finales desactiven el servicio.	No se observaron desviaciones
		Se inspeccionó una estación de trabajo que había deshabilitado el software antivirus para comprobar que la estación de trabajo estaba en proceso de ser aislada de la red.	No se observaron desviaciones.

Criterios de seguridad, disponibilidad, confidencialidad y privacidad asignados a las pruebas y controles del auditor de servicios de AWS realizados y a sus resultados

Controles establecidos por AWS	Criterios	Pruebas realizadas por EY	Resultados de las pruebas
		Se inspeccionó una estación de trabajo para comprobar que el software antivirus estaba instalado, actualizado y en funcionamiento de acuerdo con la política de integridad del sistema y la información de AWS.	No se observaron desviaciones.
AWSCA-4.1: específico de EC2. Tras iniciar la comunicación con una AMI de Linux provista por AWS, AWS habilita una comunicación segura con la configuración SSH en la instancia, mediante la generación de una clave de host única y la entrega de la huella digital de la clave al usuario a través de un canal de confianza.	CC6.7	Se consultó a un Security Engineer de EC2 para comprobar si después de iniciar la comunicación con una AMI de Linux provista por AWS, AWS habilitó una comunicación segura por la configuración SSH en la instancia, mediante la generación de una clave de host única y la entrega de la huella digital de la clave al usuario a través de un canal de confianza.	No se observaron desviaciones.
		Se lanzó una instancia de EC2 pública de una AMI de Linux y se inspeccionó la consola EC2 para comprobar si se podía acceder a la huella de la clave del host única desde el registro del sistema.	No se observaron desviaciones.
		Con la instancia de EC2 pública de una AMI de Linux, se conectó a la instancia a través de SSH utilizando la huella digital de clave de host única y se inspeccionaron los registros de conexión para comprobar si se enumeró esta huella de clave.	No se observaron desviaciones.
		Se lanzó una segunda instancia de EC2 pública de una AMI de Linux y se inspeccionaron la consola de EC2 y los registros de conexión de instancias para comprobar si la huella de la clave de host única era diferente a la de la primera instancia.	No se observaron desviaciones.

Criterios de seguridad, disponibilidad, confidencialidad y privacidad asignados a las pruebas y controles del auditor de servicios de AWS realizados y a sus resultados

Controles establecidos por AWS	Criterios	Pruebas realizadas por EY	Resultados de las pruebas
		Con la segunda instancia de EC2 pública de una AMI de Linux, se intentó conectar a la instancia a través de SSH utilizando la huella digital de la clave de host única de la primera instancia y se observó que el sistema rechazaba el intento, para comprobar que la conexión a una instancia de EC2 de una AMI de Linux solo se puede realizar utilizando la huella digital de la clave de host única de la instancia.	No se observaron desviaciones.
AWSCA-4.2: específico de EC2. Tras iniciar la comunicación con una AMI de Windows provista por AWS, AWS habilita una comunicación segura al configurar Windows Terminal Services en la instancia, al generar un certificado de servidor autofirmado único y al entregar la huella digital del certificado al usuario a través de un canal seguro.	CC6.7	Se le consultó a un Security Engineer de EC2 para comprobar si tras iniciar la comunicación con Windows AMI provista por AWS, AWS habilitó una comunicación segura al configurar Windows Terminal Service en la instancia, al generar un certificado de servidor autofirmado único y al entregar la huella digital del certificado al usuario a través de un canal seguro.	No se observaron desviaciones.
		Se lanzó una instancia de EC2 pública de una AMI de Windows y se inspeccionó la consola EC2 y el registro del sistema para comprobar si se podía acceder al certificado del servidor autofirmado.	No se observaron desviaciones.
		Con el lanzamiento de la instancia de EC2 pública de una AMI de Windows, se conectó a la instancia utilizando el certificado del servidor autofirmado único para comprobar si los registros de conexión coincidían con este certificado desde el registro del sistema de consola EC2 de la instancia.	No se observaron desviaciones.
		Se lanzó una segunda instancia de EC2 pública de una AMI de Windows y se inspeccionó la consola EC2 y los registros de conexión de la instancia para comprobar si el certificado del servidor autofirmado único era diferente al de la primera instancia.	No se observaron desviaciones.

Criterios de seguridad, disponibilidad, confidencialidad y privacidad asignados a las pruebas y controles del auditor de servicios de AWS realizados y a sus resultados

Controles establecidos por AWS	Criterios	Pruebas realizadas por EY	Resultados de las pruebas
		Con la segunda instancia de EC2 pública de una AMI de Windows, se intentó conectar a la instancia utilizando el certificado del servidor autofirmado único de la primera instancia y se observó que el sistema rechazaba el intento, para comprobar que la conexión a una instancia de EC2 de una AMI de Windows solo se puede realizar utilizando el certificado del servidor autofirmado único de la instancia.	No se observaron desviaciones.
AWSCA-4.3: específico de VPC. Amazon habilita la comunicación segura de la VPN a una puerta de enlace de VPN, para lo cual proporciona una clave secreta compartida que se utiliza a fin de establecer asociaciones IPSec.	CC6.7	Se consultó a un Manager of Software Development de VPC para comprobar si Amazon habilitaba la comunicación de VPN segura con una puerta de enlace de VPN mediante una clave secreta que establecía asociaciones IPSec.	No se observaron desviaciones.
		Se observó que un Manager of Software Development de VPC utilizó la clave secreta compartida para establecer asociaciones IPSec y comprobar que la conexión era satisfactoria.	No se observaron desviaciones.
		Se observó que un Manager of Software Development de VPC modificó la clave secreta compartida para establecer asociaciones IPSec y comprobar que la conexión era satisfactoria.	No se observaron desviaciones.
AWSCA-4.4: específico de S3. S3 genera y almacena un HMAC salado unidireccional de la clave de cifrado del	CC6.1; CC6.7	Se consultó a un Software Development Engineer de S3 para comprobar que S3 generaba y almacenaba un HMAC salado unidireccional de la clave de cifrado del cliente, y que el valor HMAC salado no se registraba.	No se observaron desviaciones.

Criterios de seguridad, disponibilidad, confidencialidad y privacidad asignados a las pruebas y controles del auditor de servicios de AWS realizados y a sus resultados

Controles establecidos por AWS	Criterios	Pruebas realizadas por EY	Resultados de las pruebas
cliente. Este valor HMAC salado no se registra.		Se observó que un Software Development Engineer de S3 cargó un objeto cifrado en S3 y se inspeccionaron los metadatos del objeto almacenado para comprobar si la información de cifrado incluía un HMAC salado unidireccional de la clave de cifrado del cliente.	No se observaron desviaciones.
		Se observó a un Software Development Engineer de S3 cargar un objeto cifrado a S3 y se buscó en los registros del host de S3 el valor HMAC salado unidireccional para comprobar que no se había registrado.	No se observaron desviaciones.
		Se observó a un ingeniero de desarrollo de software de S3 intentar descifrar un objeto en S3 con una clave de cifrado incorrecta para comprobar que la función de descifrado fallara y el objeto fuera ilegible.	No se observaron desviaciones.
AWSCA-4.5: específico de KMS. Las claves de KMS que se usan para las operaciones criptográficas en KMS se protegen de forma lógica para que ningún empleado de AWS pueda acceder al material de claves.	CC6.1	Se consultó a un Cryptography Technical Program Manager de AWS para comprobar que ningún empleado de AWS pudiera obtener acceso lógico a los módulos de seguridad reforzados en los que se utilizaban claves del cliente para operaciones criptográficas.	No se observaron desviaciones.
		Se inspeccionaron las configuraciones para obtener acceso lógico al módulo de seguridad reforzado para comprobar si las claves de KMS utilizadas para las operaciones criptográficas en KMS estaban protegidas lógicamente de modo que ningún empleado de AWS pudiera acceder al material de las claves.	No se observaron desviaciones.

Criterios de seguridad, disponibilidad, confidencialidad y privacidad asignados a las pruebas y controles del auditor de servicios de AWS realizados y a sus resultados

Controles establecidos por AWS	Criterios	Pruebas realizadas por EY	Resultados de las pruebas
		Se observó a un Cryptography Software Development Engineer de AWS intentar obtener acceso lógico al módulo de seguridad reforzado en el que se usan las claves del cliente en la memoria para comprobar que no era posible.	No se observaron desviaciones.
		Se inspeccionaron las configuraciones de acceso al material de claves de KMS para comprobar que ningún empleado de AWS pudiera modificar los conjuntos de reglas, los hosts ni la membresía del operador del dominio del dispositivo de seguridad reforzado.	No se observaron desviaciones.
		Se observó a un Cryptography Software Development Engineer de AWS intentar eliminar un host u operador sin cumplir las reglas de quórum para comprobar que las acciones daban lugar a un error de regla de quórum.	No se observaron desviaciones.
AWSCA-4.6: específico de KMS. Los servicios de AWS que se integran en AWS KMS para la gestión de claves utilizan una clave de datos de 256 bits a nivel local para proteger el contenido del cliente.	CC6.1; CC6.7	Se consultó a los Software Development Engineers para comprobar si los servicios de AWS que se integran en AWS KMS para la gestión de claves utilizaban una clave de datos AES de 256 bits a nivel local para proteger el contenido del cliente.	No se observaron desviaciones.
		Se inspeccionaron las configuraciones de las llamadas a la API de los servicios que se integran en KMS para los servicios que almacenan el contenido de los clientes con el fin de comprobar que cada servicio estaba configurado para enviar solicitudes de claves AES de 256 bits a KMS.	No se observaron desviaciones.

Criterios de seguridad, disponibilidad, confidencialidad y privacidad asignados a las pruebas y controles del auditor de servicios de AWS realizados y a sus resultados

Controles establecidos por AWS	Criterios	Pruebas realizadas por EY	Resultados de las pruebas
AWSCA-4.7: específico de KMS. La clave proporcionada por KMS a los servicios integrados es una clave de 256 bits cifrada con una clave AES única de 256 bits para la cuenta de AWS del cliente.	CC6.1; CC6.7	Se consultó a un Cryptography Technical Program Manager de AWS para comprobar si las claves proporcionadas por KMS a los servicios integrados eran claves AES de 256 bits y estaban cifradas con claves AES de 256 bits únicas de la cuenta de AWS de cada cliente.	No se observaron desviaciones.
		Se inspeccionó la configuración de creación de claves de KMS para comprobar que las claves de KMS creadas por KMS utilizaban el algoritmo criptográfico AES-256.	No se observaron desviaciones.
		Se inspeccionó la configuración de la actividad de cifrado de KMS para comprobar que se devolvían claves AES de 256 bits para las solicitudes de claves AES de 256 bits procedentes de los servicios integrados de KMS para cifrar los datos del cliente.	No se observaron desviaciones.
		Se observó a un AWS Cryptography Software Development Engineer crear un recurso con contenido habilitado para el cifrado mediante KMS con el fin de comprobar que se utilizaba una clave de KMS para cifrar una clave de cifrado de datos AES de 256 bits (que se utilizaba para cifrar el contenido) como se solicitaba al servicio.	No se observaron desviaciones.
		Se observó a un AWS Cryptography Software Development Engineer crear un recurso con contenido habilitado para el cifrado mediante KMS y, a continuación, intentar acceder a los datos sin descifrarlos para comprobar que eran ilegibles.	No se observaron desviaciones.

Criterios de seguridad, disponibilidad, confidencialidad y privacidad asignados a las pruebas y controles del auditor de servicios de AWS realizados y a sus resultados

Controles establecidos por AWS	Criterios	Pruebas realizadas por EY	Resultados de las pruebas
		Se observó a un Cryptography Software Development Engineer de AWS mientras creaba un recurso con contenido habilitado para el cifrado mediante KMS y, a continuación, intentaba descifrar los datos con la clave de cifrado de datos AES de 256 bits necesaria para comprobar si los datos se habían descifrado correctamente.	No se observaron desviaciones.
		Se cargaron datos de prueba con un servicio integrado en KMS cifrado con una clave de cifrado de datos, cifrada por una clave de KMS relacionada con una cuenta de AWS y se intentó realizar la misma actividad, con otra cuenta de AWS, con la misma clave de KMS para observar que se había producido un error de carga debido a un error de autorización causado por una falta de coincidencia entre el propietario de la clave de KMS y la cuenta de AWS.	No se observaron desviaciones.
AWSCA-4.8: específico de KMS. Las solicitudes en KMS se registran en AWS CloudTrail.	CC6.1	Se consultó a un Technical Program Manager de AWS Cryptography para comprobar que las llamadas a la API realizadas por los servicios de AWS que se integran con KMS se capturaban cuando la característica de registro estaba habilitada.	No se observaron desviaciones.
		Se inspeccionó la configuración del registro de KMS para comprobar que las solicitudes en KMS se diseñaron para ser registradas en AWS CloudTrail.	No se observaron desviaciones.
		Se habilitó el registro de CloudTrail en un servicio que se integra en KMS, se cargaron datos con una clave de KMS para el cifrado y se descargó el mismo archivo para el descifrado y se inspeccionaron los registros en AWS CloudTrail para comprobar que se registraba la actividad de las llamadas a la API de cifrado y descifrado.	No se observaron desviaciones.

Criterios de seguridad, disponibilidad, confidencialidad y privacidad asignados a las pruebas y controles del auditor de servicios de AWS realizados y a sus resultados

Controles establecidos por AWS	Criterios	Pruebas realizadas por EY	Resultados de las pruebas
AWSCA-4.9: específico de KMS. Solo los clientes que utilicen TLS con conjuntos de algoritmos de cifrado que admitan la confidencialidad directa pueden acceder a los puntos de conexión de KMS.	CC6.1; CC6.7	Se consultó a un Technical Program Manager de AWS Cryptography para comprobar que solo se podía acceder a los puntos de conexión de KMS mediante TLS con conjuntos de algoritmos de cifrado para admitir la confidencialidad directa.	No se observaron desviaciones.
		Se inspeccionó la configuración de la comunicación TLS de KMS para comprobar que los conjuntos de algoritmos de cifrado enumerados admitían la confidencialidad directa.	No se observaron desviaciones.
		Se observó a un AWS Cryptography Software Development Engineer intentar conectarse a un punto de conexión del servicio KMS público con un algoritmo de cifrado no admitido para comprobar que no se podía acceder a los puntos de conexión.	No se observaron desviaciones.
		Se observó a un AWS Cryptography Software Development Engineer intentar conectarse a un punto de conexión del servicio KMS público con un conjunto de algoritmo de cifrado compatible con la confidencialidad directa para comprobar que el punto de conexión fuera exitoso.	No se observaron desviaciones.
AWSCA-4.10: específico de KMS. Las claves utilizadas en AWS KMS solo se utilizan para un único fin, tal y como	CC6.1	Se le consultó a un Technical Program Manager de AWS Cryptography para comprobar que las claves utilizadas en AWS KMS solo se utilizaban para un único fin como se define en el parámetro de uso de cada clave.	No se observaron desviaciones.

Criterios de seguridad, disponibilidad, confidencialidad y privacidad asignados a las pruebas y controles del auditor de servicios de AWS realizados y a sus resultados

Controles establecidos por AWS	Criterios	Pruebas realizadas por EY	Resultados de las pruebas
se define en el parámetro de uso de cada clave.		Se inspeccionó el código fuente responsable del uso de la clave de AWS KMS, para comprobar que el parámetro de uso estaba configurado a nivel de clave y que las operaciones requerían el uso de las claves designadas por el sistema para esa operación.	No se observaron desviaciones.
		Se creó una clave de AWS KMS y se intentó realizar una operación de clave en línea con el parámetro de uso de clave para comprobar que la operación se realizaba de acuerdo con el parámetro configurado.	No se observaron desviaciones.
		Se creó una clave de AWS KMS y se intentó realizar una operación de clave que no se ajustaba al parámetro de uso de clave para comprobar que la operación generaba un error de uso de clave.	No se observaron desviaciones.
AWSCA-4.11: específico de KMS. Las claves de KMS creadas por KMS se rotan con una frecuencia definida si el cliente las habilita.	CC6.1; CC6.7	Se consultó a un Technical Program Manager de AWS Cryptography para comprobar que el servicio KMS incluyera la funcionalidad para que las claves de KMS se rotaran con una frecuencia definida, si el cliente lo habilitaba.	No se observaron desviaciones.
		Se inspeccionó el código fuente responsable de la rotación de las claves de KMS para comprobar que se crearía una nueva rotación de claves de acuerdo con la frecuencia definida por el cliente, si se habilitaba.	No se observaron desviaciones.
		Se inspeccionó el registro de eventos de rotación de claves bajo demanda de una clave interna de AWS para comprobar que la clave se rotó de inmediato y se registró el evento.	

Criterios de seguridad, disponibilidad, confidencialidad y privacidad asignados a las pruebas y controles del auditor de servicios de AWS realizados y a sus resultados

Controles establecidos por AWS	Criterios	Pruebas realizadas por EY	Resultados de las pruebas
		Se inspeccionó el registro de eventos de rotación de claves de una clave interna de AWS para comprobar que la clave de respaldo se había rotado de acuerdo con la frecuencia definida.	No se observaron desviaciones.
AWSCA-4.12: específico de KMS. Los materiales de claves de recuperación utilizados para los procesos de recuperación de desastres por KMS están protegidos de manera física sin conexión para que ningún empleado de AWS pueda acceder al material de claves.	CC6.1; CC6.4	Se le consultó a un Technical Program Manager de AWS Cryptography para comprobar que los materiales de claves de recuperación utilizados para los procesos de recuperación de desastres por KMS estuvieran protegidos de manera física sin conexión para que ningún empleado de AWS pudiera acceder al material de claves.	No se observaron desviaciones.
		Se inspeccionó la lista de empleados con acceso físico a los recursos de material de claves de recuperación utilizados para los procesos de recuperación de desastres por KMS para comprobar que los empleados eran adecuados en función de su puesto y sus responsabilidades.	No se observaron desviaciones.
		Se inspeccionó un registro de acceso físico de los intentos de acceso a los materiales clave de recuperación para comprobar que ningún empleado de AWS pudiera acceder por su cuenta.	No se observaron desviaciones.
AWSCA-4.13: específico de KMS; los operadores autorizados revisan los intentos de acceso a los	CC6.1; CC6.4	Se consultó a un Technical Program Manager de AWS Cryptography para comprobar que los operadores autorizados revisaron los intentos de acceso a los materiales de claves de recuperación con la frecuencia definida en la documentación del equipo.	No se observaron desviaciones.

Criterios de seguridad, disponibilidad, confidencialidad y privacidad asignados a las pruebas y controles del auditor de servicios de AWS realizados y a sus resultados

Controles establecidos por AWS	Criterios	Pruebas realizadas por EY	Resultados de las pruebas
materiales de claves de recuperación con una frecuencia definida en la documentación del equipo.		Se inspeccionaron las revisiones de los intentos de acceso o las solicitudes a los materiales de clave de recuperación para comprobar que los operadores autorizados realizaban y documentaban las revisiones con la frecuencia definida en la documentación del equipo.	No se observaron desviaciones.
AWSCA-4.14: cada versión de firmware de producción del módulo de seguridad de hardware (HSM) de AWS Key Management Service se ha validado con el NIST según el estándar de nivel 3 de FIPS 140-2 o está en proceso de certificarse conforme al estándar de nivel 3 de FIPS 140-3.	CC6.1; CC6.6; CC6.7	Se le consultó a un Cryptography Technical Program Manager de AWS para comprobar si la versión del firmware de producción de AWS Key Management Service HSM estaba certificada por el NIST según el estándar de nivel 3 del FIPS 140-2 o está en proceso de certificarse conforme al estándar de nivel 3 de FIPS 140-3.	No se observaron desviaciones.
		Para todas las regiones que están dentro del alcance, se inspeccionó la versión del firmware que se ejecutaba en dispositivos de producción de HSM de AWS Key Management Service para comprobar que la versión del firmware de producción de HSM de AWS Key Management Service estuviera certificada por el certificado del Programa de Validación de Módulos Criptográficos del NIST según el estándar de nivel 3 de FIPS 140-2 o el firmware actualizado estuviera en proceso de certificarse conforme al estándar de nivel 3 de FIPS 140-3.	No se observaron desviaciones.

Criterios de seguridad, disponibilidad, confidencialidad y privacidad asignados a las pruebas y controles del auditor de servicios de AWS realizados y a sus resultados

Controles establecidos por AWS	Criterios	Pruebas realizadas por EY	Resultados de las pruebas
AWSCA-4.15: específico de CloudHSM. Los dispositivos HSM de producción se reciben en bolsas autentificables a prueba de manipulaciones. Los números de serie de las bolsas autentificables a prueba de manipulaciones y los números de serie de los HSM de producción se verifican con los datos proporcionados fuera de banda por el fabricante y se registran en los sistemas de seguimiento por parte de personas autorizadas.	CC6.1; CC6.4; CC6.7;	Se le consultó a un CloudHSM Technical Program Manager para comprobar si los dispositivos de HSM de producción se recibían en bolsas autenticables a prueba de manipulaciones, y si los números de serie de las bolsas autenticables a prueba de manipulaciones y los números de serie de los HSM de producción se comparaban con los datos proporcionados fuera de banda por el fabricante y los registraban personas autorizadas para acceder a los sistemas de seguimiento en función de sus roles y responsabilidades, de conformidad con los estándares de operación y seguridad de AWS.	No se observaron desviaciones.
		Se inspeccionó la configuración de las verificaciones automatizadas realizadas antes de mover un dispositivo de HSM de producción para comprobar si los números de serie de los HSM se verificaban con los datos proporcionados fuera de banda antes de ingresar en producción.	No se observaron desviaciones.
		Se inspeccionaron los registros de validación de un dispositivo de HSM que no superó la validación para comprobar si se prohibía automáticamente su entrada en producción cuando el número de serie del HSM no podía verificarse con los datos facilitados fuera de banda por el fabricante.	No se observaron desviaciones.
		Se inspeccionaron los registros de validación de un dispositivo de HSM de producción para comprobar si el número de serie del dispositivo de HSM se verificaba con los datos proporcionados fuera de banda antes de ingresar en producción.	No se observaron desviaciones.

Criterios de seguridad, disponibilidad, confidencialidad y privacidad asignados a las pruebas y controles del auditor de servicios de AWS realizados y a sus resultados

Controles establecidos por AWS	Criterios	Pruebas realizadas por EY	Resultados de las pruebas
AWSCA-5.1: el acceso físico a los centros de datos está aprobado por una persona autorizada.	CC6.4; CC6.7	Se consultó a un Technical Program Manager de AWS Security para comprobar que el acceso físico a los centros de datos estaba aprobado por una persona autorizada.	No se observaron desviaciones.
		Se inspeccionó la configuración para ejecutar la aprobación del acceso físico y el aprovisionamiento dentro del sistema de gestión de acceso al centro de datos para comprobar que el acceso físico a los centros de datos estaba diseñado para ser concedido después de la aprobación de una persona autorizada.	No se observaron desviaciones.
		Se seleccionó un acceso a los centros de datos aprovisionado por un usuario durante el período y se inspeccionaron los registros de aprovisionamiento de acceso físico a los centros de datos para comprobar si el acceso físico se concedía después de ser aprobado por una persona autorizada.	No se observaron desviaciones.
AWSCA-5.2: el acceso físico se revoca en un plazo de 24 horas a partir de la desactivación del registro del empleado o del proveedor.	CC6.4; CC6.7	Se le consultó a un Technical Program Manager de AWS Security para comprobar si el acceso físico se revocaba automáticamente en un plazo de 24 horas a partir de la desactivación del registro del empleado o del proveedor.	No se observaron desviaciones.
		Se inspeccionaron las configuraciones del sistema de gestión de acceso al centro de datos para comprobar que el acceso físico se revocaba automáticamente en un plazo de 24 horas desde la desactivación del registro del empleado o del proveedor en el sistema de RR. HH.	No se observaron desviaciones.

Criterios de seguridad, disponibilidad, confidencialidad y privacidad asignados a las pruebas y controles del auditor de servicios de AWS realizados y a sus resultados

Controles establecidos por AWS	Criterios	Pruebas realizadas por EY	Resultados de las pruebas
		Se seleccionó a un empleado despedido y se inspeccionó el registro del sistema de RR. HH. para comprobar si el acceso físico se revocaba de manera sistemática en un plazo de 24 horas a partir de la desactivación del registro del empleado en el sistema de RR. HH. por el sistema de aprovisionamiento de acceso.	No se observaron desviaciones.
AWSCA-5.3: el personal adecuado revisa el acceso físico a los centros de datos trimestralmente.	CC6.4; CC6.7	Se consultó a un Technical Program Manager de AWS Security para comprobar si el personal adecuado revisaba el acceso físico a los centros de datos trimestralmente.	No se observaron desviaciones.
		Se inspeccionaron las configuraciones del sistema dentro del sistema de gestión de acceso a los centros de datos para comprobar que el acceso marcado para ser retirado se eliminaba automáticamente una vez que la revisión se marcaba como completa.	No se observaron desviaciones.
		Se seleccionó a un usuario marcado para ser eliminado durante la revisión trimestral más reciente del acceso físico y se inspeccionaron los registros de CloudWatch para la revocación de actividades a fin de comprobar si el acceso del usuario se había eliminado adecuadamente del sistema de gestión de acceso al centro de datos.	No se observaron desviaciones.
		Se seleccionó una muestra de usuarios activos que tenían acceso al centro de datos a partir de una lista de los niveles de acceso al centro de datos activos dentro del periodo y se inspeccionaron las revisiones de acceso para comprobar si estas se habían realizado trimestralmente y si el personal adecuado había aprobado el acceso.	No se observaron desviaciones.

Criterios de seguridad, disponibilidad, confidencialidad y privacidad asignados a las pruebas y controles del auditor de servicios de AWS realizados y a sus resultados

Controles establecidos por AWS	Criterios	Pruebas realizadas por EY	Resultados de las pruebas
AWSCA-5.4: se utilizan cámaras de circuito cerrado de televisión (CCTV) para monitorear las ubicaciones de los servidores en los centros de datos. Las imágenes se retienen durante 90 días, a menos que estén limitadas por obligaciones legales o contractuales.	CC6.4	Se consultó a un Technical Program Manager de AWS Security y a los Data Center Operations Managers para comprobar que los puntos de acceso físico a las ubicaciones de los servidores estaban vigilados por una cámara de circuito cerrado de televisión (CCTV) y que las imágenes se conservaban durante 90 días, a menos que estuvieran limitadas por obligaciones legales o contractuales.	No se observaron desviaciones.
		Se seleccionó una muestra de los centros de datos de la herramienta de administración de activos y se observaron las grabaciones de CCTV o se inspeccionaron capturas de pantalla de las grabaciones de CCTV de las áreas cercanas a los puntos de acceso a las ubicaciones de los servidores, para comprobar que se habían grabado los puntos de acceso físicos a las ubicaciones de los servidores.	No se observaron desviaciones.
		Se seleccionó una muestra de los centros de datos de la herramienta de administración de activos y se inspeccionó la configuración de los grabadores de video en red para comprobar si las imágenes de CCTV de las ubicaciones de los servidores se retenían durante 90 días, a menos que estuvieran limitadas por obligaciones legales o contractuales.	No se observaron desviaciones.

Criterios de seguridad, disponibilidad, confidencialidad y privacidad asignados a las pruebas y controles del auditor de servicios de AWS realizados y a sus resultados

Controles establecidos por AWS	Criterios	Pruebas realizadas por EY	Resultados de las pruebas
AWSCA-5.5: el acceso a las ubicaciones de los servidores se administra mediante dispositivos electrónicos de control de acceso.	CC6.4	Se consultó a un Technical Program Manager de AWS Security y a los Data Center Operations Managers para comprobar que los puntos de acceso físico a las ubicaciones de los servidores se administraban mediante dispositivos de control de acceso electrónico.	No se observaron desviaciones.
		Se seleccionó una muestra de los centros de datos de la herramienta de administración de activos, se observaron los dispositivos de control de acceso electrónico en los puntos de acceso físico a las ubicaciones de los servidores o se inspeccionaron las configuraciones de control de acceso a la seguridad física para comprobar que los dispositivos de control de acceso electrónico estaban instalados en los puntos de acceso físico a las ubicaciones de los servidores y que requerían credenciales de identificación de Amazon autorizadas con los PIN correspondientes para ingresar en las ubicaciones de los servidores.	No se observaron desviaciones.
AWSCA-5.6: se instalan sistemas electrónicos de detección de intrusos en las ubicaciones de los servidores de datos para monitorear, detectar y alertar automáticamente al personal adecuado	CC7.2; CC7.3	Se consultó a un Technical Program Manager de AWS Security y a los Data Center Operations Managers para comprobar que los sistemas electrónicos de detección de intrusos estuvieran instalados y fueran capaces de detectar vulneraciones en las ubicaciones de los servidores de los centros de datos.	No se observaron desviaciones.

Criterios de seguridad, disponibilidad, confidencialidad y privacidad asignados a las pruebas y controles del auditor de servicios de AWS realizados y a sus resultados

Controles establecidos por AWS	Criterios	Pruebas realizadas por EY	Resultados de las pruebas
de los incidentes de seguridad informática.		Se seleccionó una muestra de los centros de datos de la herramienta de administración de activos, se observaron los sistemas electrónicos de detección de intrusos en las instalaciones o se inspeccionaron las configuraciones de control de acceso a la seguridad física para comprobar que los sistemas electrónicos de detección de intrusos estaban instalados, que eran capaces de detectar intentos de intrusión y que alertaban automáticamente al personal de seguridad de los eventos detectados para su investigación y resolución.	No se observaron desviaciones.
AWSCA-5.7: los centros de datos de Amazon están protegidos por sistemas de detección y extinción de incendios.	A1.2	Se consultó a los Data Center Operations Managers para comprobar que los centros de datos de Amazon estuvieran protegidos por sistemas de detección y extinción de incendios.	No se observaron desviaciones.
		Se seleccionó una muestra de los centros de datos de Amazon a partir de la herramienta de administración de activos y se observaron los sistemas de detección de incendios en las instalaciones para comprobar que se encontraban en todas las áreas de los centros de datos.	No se observaron desviaciones.
		Se seleccionó una muestra de centros de datos de Amazon y se observaron los dispositivos de extinción de incendios en las instalaciones para comprobar si se encontraban en todas las áreas de los centros de datos.	No se observaron desviaciones.

Criterios de seguridad, disponibilidad, confidencialidad y privacidad asignados a las pruebas y controles del auditor de servicios de AWS realizados y a sus resultados

Controles establecidos por AWS	Criterios	Pruebas realizadas por EY	Resultados de las pruebas
AWSCA-5.8: los centros de datos de Amazon están climatizados para mantener unas condiciones ambientales adecuadas. El personal y los sistemas monitorean y controlan la temperatura y la humedad del aire a niveles adecuados.	A1.2	Se consultó a los administradores de operaciones de los centros de datos para comprobar que los centros de datos de Amazon estaban climatizados para mantener las condiciones ambientales adecuadas y que las unidades estaban monitoreadas por personal y sistemas para controlar la temperatura y la humedad del aire a niveles adecuados.	No se observaron desviaciones.
		Se seleccionó una muestra de los centros de datos de Amazon a partir de la herramienta de administración de activos y se observaron los sistemas de aire acondicionado de las instalaciones para comprobar que monitoreaban y controlaban la temperatura y la humedad a niveles adecuados.	No se observaron desviaciones.
AWSCA-5.9: las unidades de sistema de alimentación ininterrumpida (UPS) proporcionan energía de reserva en caso de una falla eléctrica en los centros de datos de Amazon y en los sitios de coubicación de terceros donde Amazon mantiene las unidades de UPS.	A1.2	Se consultó a los Data Center Operations Managers para comprobar si las unidades de UPS proporcionaban energía de reserva en caso de falla eléctrica en los centros de datos de Amazon o en los sitios de coubicación donde Amazon administra las unidades de UPS.	No se observaron desviaciones.
		Se inspeccionó la configuración del sistema responsable de incorporar automáticamente y monitorear de forma continua el estado de las unidades de UPS mantenidas por Amazon para comprobar que las unidades de UPS se monitoreaban y enviaban una alerta en caso de falla eléctrica.	No se observaron desviaciones.
		Se seleccionó un centro de datos y se inspeccionó la evidencia para comprobar que las unidades de UPS se monitoreaban y que se enviaba una alerta en caso de falla eléctrica.	No se observaron desviaciones.

Criterios de seguridad, disponibilidad, confidencialidad y privacidad asignados a las pruebas y controles del auditor de servicios de AWS realizados y a sus resultados

Controles establecidos por AWS	Criterios	Pruebas realizadas por EY	Resultados de las pruebas
		Se seleccionó una muestra de los centros de datos a partir de la herramienta de administración de activos y se observaron los equipos de UPS en las instalaciones para comprobar si las unidades de UPS estaban configuradas para proporcionar energía de respaldo en caso de una falla eléctrica.	No se observaron desviaciones.
AWSCA-5.10: los centros de datos de Amazon tienen generadores para proporcionar energía de reserva en caso de falla eléctrica.	A1.2	Se consultó a los administradores de operaciones de centros de datos para comprobar que los centros de datos de Amazon tuvieran generadores para proporcionar energía de respaldo en caso de falla eléctrica.	No se observaron desviaciones.
		Se seleccionó una muestra de los centros de datos de Amazon a partir de la herramienta de administración de activos y se observaron los equipos generadores en las instalaciones para comprobar si estos estaban configurados para proporcionar energía de respaldo en caso de una falla eléctrica.	No se observaron desviaciones.
AWSCA-5.11: existen contratos con proveedores de servicios de coubicación de terceros que incluyen disposiciones para proporcionar sistemas de	CC7.3; CC7.4; CC7.5; CC9.2; A1.2	Se consultó al asesor legal de AWS para comprobar si los contratos de los proveedores de servicios de coubicación incluían disposiciones sobre los sistemas de extinción de incendios, aire acondicionado, unidades de UPS y fuentes de alimentación redundantes, así como disposiciones que exigen la comunicación a AWS de incidentes o eventos que afecten a los activos o clientes de Amazon.	No se observaron desviaciones.

Criterios de seguridad, disponibilidad, confidencialidad y privacidad asignados a las pruebas y controles del auditor de servicios de AWS realizados y a sus resultados

Controles establecidos por AWS	Criterios	Pruebas realizadas por EY	Resultados de las pruebas
extinción de incendios, aire acondicionado para mantener las condiciones atmosféricas adecuadas, unidades de Sistema de alimentación ininterrumpida (UPS) (a menos que sean mantenidas por Amazon) y fuentes de alimentación redundantes. Los contratos también incluyen disposiciones que exigen la comunicación de incidentes o eventos que impactan en los activos o clientes de Amazon a AWS.		Se seleccionó una muestra de los centros de datos administrados por los proveedores de servicios de coubicación a partir de la herramienta de administración de activos y se inspeccionaron los acuerdos contractuales vigentes entre los proveedores de servicios y AWS para comprobar que incluían disposiciones sobre sistemas de extinción de incendios, aire acondicionado, unidades de UPS y fuentes de alimentación redundantes, así como disposiciones que exigían a los proveedores de servicios de coubicación notificar inmediatamente a Amazon sobre el descubrimiento de cualquier uso o divulgación no autorizados de información confidencial o cualquier otra vulneración.	No se observaron desviaciones.
AWSCA-5.12: AWS realiza revisiones periódicas de los proveedores de servicios de coubicación para	CC3.2; CC3.3; CC3.4; CC4.1; CC7.3; CC7.4;	Se consultó a un Vendor Performance Manager para comprobar que se realizaban las revisiones periódicas de las relaciones con los proveedores de coubicación para validar el cumplimiento de los estándares de operación y seguridad de AWS.	No se observaron desviaciones.

Criterios de seguridad, disponibilidad, confidencialidad y privacidad asignados a las pruebas y controles del auditor de servicios de AWS realizados y a sus resultados

Controles establecidos por AWS	Criterios	Pruebas realizadas por EY	Resultados de las pruebas
validar el cumplimiento de los estándares de operación y seguridad de AWS.	CC7.5; CC9.2; A1.2	Se seleccionó una muestra de los centros de datos administrados por los proveedores de servicios de coubicación a partir de la herramienta de administración de activos y se inspeccionaron las revisiones del proveedor correspondiente para comprobar si se realizaron en virtud de la programación de revisión empresarial de coubicación y si se incluyó la evaluación del cumplimiento de los estándares de operación y seguridad de AWS.	No se observaron desviaciones.
AWSCA-5.13: antes de abandonar el control de AWS, todos los medios de producción de AWS se retiran de forma segura y se destruyen físicamente bajo la verificación de dos empleados.	CC6.5; CC6.7; C1.2; P4.3	Se consultó a los administradores de operaciones de los centros de datos para comprobar si los medios de producción de AWS se retiraban de manera segura y se destruían físicamente antes de abandonar el control de AWS.	No se observaron desviaciones.
		Se inspeccionó el documento Procedimientos operativos estándar de la destrucción de medios de AWS para comprobar si incluía los procedimientos para que el personal de los centros de datos retire de manera segura los medios de producción antes de dejar el control de AWS.	No se observaron desviaciones.
		Se seleccionó una muestra de los centros de datos a partir de la herramienta de administración de activos y se observaron las prácticas de seguridad en las instalaciones para comprobar que los medios de producción estaban restringidos al control de AWS, a menos que se retiraran de forma segura y se destruyeran físicamente.	No se observaron desviaciones.

Criterios de seguridad, disponibilidad, confidencialidad y privacidad asignados a las pruebas y controles del auditor de servicios de AWS realizados y a sus resultados

Controles establecidos por AWS	Criterios	Pruebas realizadas por EY	Resultados de las pruebas
		Se seleccionó una muestra de los centros de datos a partir de la herramienta de administración de activos y se observó el equipo y los medios en las instalaciones o se inspeccionaron los registros de destrucción de medios para el retiro y la destrucción física seguros a fin de comprobar que los medios de producción se retiraron de forma segura, se destruyeron físicamente y fueron verificados por dos personas antes de salir del control de AWS.	No se observaron desviaciones.
AWSCA-6.1: AWS aplica un enfoque sistemático a la administración del cambio para garantizar que los cambios en los aspectos de un servicio que afectan a los clientes se revisen, prueben y aprueben. Las normas de la gestión de cambios se basan en las directrices y se adaptan según las características de cada servicio de AWS.	CC6.1; CC6.8; CC7.5; CC8.1	Se consultó a los Software Development Managers para comprobar que los cambios de servicio que afectan a los clientes en el entorno de producción se revisaban, probaban y aprobaban, que seguían las directrices de gestión de cambios relevantes y que se mantenían, seguían y comunicaban a los equipos de servicio los procesos de gestión de cambios específicos del servicio.	No se observaron desviaciones.
		Se seleccionó una muestra de servicios y se inspeccionó el documento de directrices de gestión de cambios relevantes para comprobar que comunicaban orientaciones específicas sobre los procesos de gestión de cambios, incluidos el inicio, la prueba y la aprobación, y que los equipos documentaron y mantuvieron los pasos específicos del equipo de servicio.	No se observaron desviaciones.
AWSCA-6.2: los detalles de los cambios están documentados en una de las	CC6.8; CC8.1	Se consultó a los Software Development Managers para comprobar que los cambios estuvieran documentados en una de las herramientas de gestión de cambios o de implementación de Amazon.	No se observaron desviaciones.

Criterios de seguridad, disponibilidad, confidencialidad y privacidad asignados a las pruebas y controles del auditor de servicios de AWS realizados y a sus resultados

Controles establecidos por AWS	Criterios	Pruebas realizadas por EY	Resultados de las pruebas
herramientas de gestión de cambios o de implementación de Amazon.		Se seleccionó una muestra de cambios a partir de una lista generada por el sistema de cambios implementados en la producción y se inspeccionó la documentación pertinente para comprobar si los detalles de los cambios se documentaban en una de las herramientas de gestión de cambios o de implementación de Amazon y se comunicaban a la dirección del equipo de servicio.	No se observaron desviaciones.
AWSCA-6.3: los cambios se prueban de acuerdo con los estándares de gestión de cambios del equipo de servicio antes de la migración a producción.	CC6.8; CC8.1	Se le consultó a los Software Development Managers para comprobar si los cambios se probaron de acuerdo con los estándares de gestión de cambios del equipo de servicio antes de la migración a la producción.	No se observaron desviaciones.
		Se seleccionó una muestra de cambios a partir de una lista generada por el sistema de cambios migrados a producción y se inspeccionó la documentación pertinente para comprobar si los cambios se probaban de acuerdo con los estándares de gestión de cambios del equipo de servicios y si las pruebas se habían realizado en un entorno de desarrollo antes de la migración a producción.	No se observaron desviaciones.
		Se inspeccionó una política de Identity and Access Management administrada por AWS para comprobar si las políticas administradas por AWS se probaban antes de su traslado a producción.	No se observaron desviaciones.
AWSCA-6.4: AWS mantiene entornos de producción y	CC6.8; CC8.1	Se le consultó a los Software Development Managers para comprobar si AWS mantenía entornos de producción y desarrollo separados.	No se observaron desviaciones.

Criterios de seguridad, disponibilidad, confidencialidad y privacidad asignados a las pruebas y controles del auditor de servicios de AWS realizados y a sus resultados

Controles establecidos por AWS	Criterios	Pruebas realizadas por EY	Resultados de las pruebas
desarrollo separados.		Se seleccionó una muestra de cambios de una lista generada por el sistema de cambios implementados en producción y se inspeccionaron las canalizaciones de implementación relacionadas para comprobar que los entornos de producción y desarrollo estaban separados.	No se observaron desviaciones.
AWSCA-6.5: los cambios son revisados por el impacto en el negocio y aprobados por el personal autorizado antes de la migración a producción de acuerdo con los estándares de gestión de cambios del equipo de servicio.	CC6.8; CC8.1	Se le consultó a los Software Development Managers para comprobar si los cambios se revisaban a fin de determinar el impacto en el negocio y si el personal autorizado los aprobaba antes de la migración a la producción de acuerdo con los estándares de gestión de cambios del equipo de servicio.	No se observaron desviaciones.
		Se seleccionó una muestra de cambios a partir de un listado de cambios migrados a producción generado por el sistema y se inspeccionó la documentación relevante para comprobar si el personal autorizado revisó y aprobó los cambios antes de la migración a producción de acuerdo con las normas de gestión de cambios del equipo de servicios.	No se observaron desviaciones.
		Se inspeccionaron las configuraciones existentes para publicar las políticas de IAM administradas por AWS con el fin de comprobar si las políticas se diseñaban para requerir aprobaciones antes de ser trasladadas a producción.	No se observaron desviaciones.
		Se inspeccionó una política de IAM administrada por AWS para comprobar si las políticas administradas por AWS se aprobaban antes de su traslado a producción.	No se observaron desviaciones.

Criterios de seguridad, disponibilidad, confidencialidad y privacidad asignados a las pruebas y controles del auditor de servicios de AWS realizados y a sus resultados

Controles establecidos por AWS	Criterios	Pruebas realizadas por EY	Resultados de las pruebas
AWSCA-6.6: AWS realiza validaciones de implementación y revisiones de cambios para detectar cambios no autorizados en su entorno y realiza un seguimiento de los problemas identificados hasta su resolución.	CC6.8; CC7.1; CC8.1	Se consultó a los Software Development Managers para comprobar que AWS realizaba validaciones de implementación y revisiones de cambios a fin de detectar cambios que no seguían el proceso de gestión de cambios y que se tomaban las medidas adecuadas para hacer un seguimiento de los problemas identificados hasta su resolución.	No se observaron desviaciones.
		Se inspeccionó la documentación pertinente de una muestra de cambios a partir de un listado de cambios migrados a producción generado por el sistema para comprobar si AWS realizaba validaciones de implementación y revisiones de cambios para detectar cambios no autorizados, y si se tomaban las medidas de seguimiento necesarias para solucionar los problemas identificados.	No se observaron desviaciones.
		Se inspeccionaron las revisiones trimestrales de seguridad empresarial y el contenido del panel de infracciones de implementación de una muestra trimestral para comprobar si la gestión de AWS realizó un seguimiento de los cambios no autorizados hasta su resolución.	No se observaron desviaciones.
		Se inspeccionó la documentación de una muestra de meses y servicios que utilizan monitoreo de implementación manual para comprobar si el equipo de servicios de AWS relacionado generaba una lista de todos los cambios implementados en producción durante el mes, evaluaba los cambios para comprobar su idoneidad y si se tomaban medidas de seguimiento necesarias para solucionar los problemas identificados.	No se observaron desviaciones.

Criterios de seguridad, disponibilidad, confidencialidad y privacidad asignados a las pruebas y controles del auditor de servicios de AWS realizados y a sus resultados

Controles establecidos por AWS	Criterios	Pruebas realizadas por EY	Resultados de las pruebas
		Se inspeccionó el contenido del panel de infracciones de implementación de una muestra de meses y servicios que utilizan monitoreo de implementación manual para comprobar si la administración de AWS realizó un seguimiento de los cambios no autorizados hasta su resolución.	No se observaron desviaciones.
AWSCA-6.7: la información del cliente, incluida su información personal, y el contenido del cliente no se utilizan en entornos de desarrollo y pruebas.	CC8.1	Se preguntó a los administradores de desarrollo de software para comprobar si los datos de producción, incluidos el contenido de los clientes y los datos de los empleados de AWS, no se utilizaban en entornos de prueba o desarrollo.	No se observaron desviaciones.
		Se inspeccionó el contenido de la Política de desarrollo de software seguro destinada a los software development engineers y a los software development managers en todo AWS para comprobar si proporcionaba instrucciones de no utilizar datos de producción en entornos de prueba o desarrollo.	No se observaron desviaciones.
AWSCA-7.1: específico de S3. S3 compara las sumas de comprobación provistas por el usuario para validar la integridad de los datos en tránsito. Si la suma de comprobación MD5 proporcionada por el	CC6.7	Se consultó a un administrador de desarrollo de software de S3 para determinar las sumas de comprobación proporcionadas por el usuario comparadas con S3 para validar la integridad de los datos en tránsito y que la suma de comprobación MD5 proporcionada por el cliente coincida con la suma de comprobación MD5 calculada por S3 en los datos recibidos. De lo contrario, la solicitud REST PUT fallaría, lo que evitaría que se escribieran datos dañados en S3.	No se observaron desviaciones.

Criterios de seguridad, disponibilidad, confidencialidad y privacidad asignados a las pruebas y controles del auditor de servicios de AWS realizados y a sus resultados

Controles establecidos por AWS	Criterios	Pruebas realizadas por EY	Resultados de las pruebas
cliente no coincide con la suma de comprobación MD5 calculada por S3 en los datos recibidos, el REST PUT fallará, lo que evitará que los datos dañados en el cable se escriban en S3.		Se inspeccionaron las configuraciones de las sumas de comprobación MD5 para comprobar si S3 estaba configurado para comparar de manera continua las sumas de comprobación provistas por el usuario a fin de validar la integridad de los datos en tránsito.	No se observaron desviaciones.
		Se observó a un Software Development Engineer cargar un archivo con una suma de comprobación MD5 no válida para comprobar si la transferencia se anulaba y se mostraba un mensaje de error.	No se observaron desviaciones.
		Se observó a un Software Development Engineer cargar un archivo con una suma de comprobación MD5 válida que coincide con la suma de comprobación calculada por S3 para comprobar si la transferencia de datos se completaba con éxito.	No se observaron desviaciones.
AWSCA-7.2: específico de S3. S3 realiza pruebas de integridad continuas de los datos en reposo. Los objetos se validan de manera continua con las sumas de comprobación para evitar la corrupción de los objetos.	C1.1	Se consultó a un Software Development Engineer de S3 para comprobar que S3 realizaba comprobaciones continuas de integridad de los datos en reposo y que los objetos se validaban automáticamente con sus sumas de comprobación para evitar la corrupción de los objetos.	No se observaron desviaciones.
		Se inspeccionaron las configuraciones de las comprobaciones de integridad para asegurarse de que S3 estaba configurado para realizar continuamente comprobaciones de integridad de los datos en reposo y validarlas con sus sumas de comprobación.	No se observaron desviaciones.

Criterios de seguridad, disponibilidad, confidencialidad y privacidad asignados a las pruebas y controles del auditor de servicios de AWS realizados y a sus resultados

Controles establecidos por AWS	Criterios	Pruebas realizadas por EY	Resultados de las pruebas
		Se observó a un Software Development Engineer de S3 localizar un objeto cuya suma de comprobación no se había validado con su localizador de objetos, para comprobar que el servicio S3 detectaba automáticamente el objeto y evitar su corrupción.	No se observaron desviaciones
		Se inspeccionaron los archivos de registro del sistema de un objeto en reposo para comprobar que las sumas de comprobación se utilizaban para evaluar las comprobaciones continuas de la integridad de los datos.	No se observaron desviaciones.
		Se inspeccionaron los registros de S3 para comprobar si S3 está diseñado para restaurar automáticamente los niveles normales de redundancia del almacenamiento de objetos cuando se detecta una corrupción en el disco o una falla en el dispositivo.	No se observaron desviaciones.
AWSCA-7.3: específico de S3. Cuando se detecta la corrupción del disco o el error del dispositivo, el sistema automáticamente intenta restaurar los niveles normales de redundancia de almacenamiento de objetos.	A1.2; C1.1	Se consultó a un Software Development Manager de S3 para comprobar que, cuando se detecta la corrupción del disco o el error del dispositivo, el sistema automáticamente intenta restaurar los niveles normales de redundancia de almacenamiento de objetos.	No se observaron desviaciones.
		Se inspeccionaron las configuraciones de reparación del sistema para comprobar si S3 estaba configurado para intentar restaurar automáticamente la redundancia de almacenamiento de objetos al detectarse una corrupción en el disco o un error en el dispositivo.	No se observaron desviaciones

Criterios de seguridad, disponibilidad, confidencialidad y privacidad asignados a las pruebas y controles del auditor de servicios de AWS realizados y a sus resultados

Controles establecidos por AWS	Criterios	Pruebas realizadas por EY	Resultados de las pruebas
		Se inspeccionaron los registros de S3 para comprobar si S3 está diseñado para restaurar automáticamente los niveles normales de redundancia del almacenamiento de objetos cuando se detecta una corrupción en el disco o una falla en el dispositivo.	No se observaron desviaciones
		Se observó a un Software Development Engineer localizar un objeto que estaba corrompido o que había sufrido un error de dispositivo para comprobar que el objeto se reescribía en una ubicación conocida, lo que restablecía los niveles normales de redundancia del almacenamiento de objetos.	No se observaron desviaciones.
AWSCA-7.4: específico de S3. Los objetos se almacenan de forma redundante en múltiples instalaciones aisladas de fallos.	A1.2; C1.1	Se consultó a un Software Development Manager de S3 para comprobar que los objetos se almacenaran de forma redundante en múltiples instalaciones aisladas de fallos.	No se observaron desviaciones.
		Se inspeccionaron las configuraciones de partición de objetos para comprobar que los objetos se almacenan de forma redundante en varias instalaciones aisladas de fallos.	No se observaron desviaciones.
		Se cargó un objeto y se observó a un Software Development Engineer acceder a la configuración de la ubicación del objeto para comprobar que el objeto se almacenaba de forma redundante en múltiples instalaciones aisladas de fallos.	No se observaron desviaciones.
AWSCA-7.5: específico de S3. El diseño de los sistemas es lo suficientemente	A1.2; C1.1	Se consultó a un Software Development Manager de S3 con el fin de comprobar si los sistemas estaban diseñados para soportar la pérdida de las instalaciones de un centro de datos sin interrumpir el servicio.	No se observaron desviaciones.

Criterios de seguridad, disponibilidad, confidencialidad y privacidad asignados a las pruebas y controles del auditor de servicios de AWS realizados y a sus resultados

Controles establecidos por AWS	Criterios	Pruebas realizadas por EY	Resultados de las pruebas
redundante como para soportar la pérdida de las instalaciones de un centro de datos sin interrumpir el servicio.		Se inspeccionó la configuración del sistema utilizado por S3 en los objetos almacenados para comprobar que los servicios críticos estaban diseñados para soportar la pérdida de una instalación sin interrupción del servicio.	No se observaron desviaciones.
AWSCA-7.6: específico de RDS. Si el cliente lo habilita, RDS realiza copias de seguridad de las bases de datos del cliente, almacena las copias de seguridad durante períodos de retención definidos por el usuario y admite la recuperación en un momento dado.	A1.2; C1.1	Se consultó a un Systems Engineer Manager de RDS para comprobar que, si el cliente lo había habilitado, RDS realizaba copias de seguridad de las bases de datos del cliente, almacenaba copias de seguridad por períodos de retención definidos por el usuario y admitía la recuperación en un momento dado.	No se observaron desviaciones.
		Se inspeccionaron las configuraciones de copia de seguridad de RDS para comprobar, en caso de que el cliente lo hubiera habilitado, si RDS realizaba una copia de seguridad de la base de datos del cliente y si almacenaba las copias de seguridad durante los períodos de retención definidos por el usuario.	No se observaron desviaciones.
		Se creó una base de datos RDS, se habilitaron las copias de seguridad, se hizo una copia de seguridad de la base de datos para comprobar que RDS realizaba copias de seguridad de las bases de datos del cliente mediante copias de seguridad programadas de acuerdo con un período de retención definido por el usuario.	No se observaron desviaciones.

Criterios de seguridad, disponibilidad, confidencialidad y privacidad asignados a las pruebas y controles del auditor de servicios de AWS realizados y a sus resultados

Controles establecidos por AWS	Criterios	Pruebas realizadas por EY	Resultados de las pruebas
		Se creó una base de datos RDS, se capturó una instantánea de la base de datos en un momento determinado y se restauró la base de datos RDS mediante el uso de la instantánea capturada, para comprobar si las bases de datos RDS podían recuperarse en un momento determinado mediante el uso de las instantáneas de la base de datos.	No se observaron desviaciones
		Se restauró una base de datos RDS mediante una copia de seguridad de la base de datos, para comprobar que las bases de datos RDS pueden recuperarse en un momento dado.	No se observaron desviaciones.
AWSCA-7.7: AWS permite a los clientes eliminar su contenido. Una vez que se eliminan los datos con éxito, se vuelven ilegibles.	CC6.5; C1.2; P4.1; P4.2; P4.3	Se consultó a los Software Development Managers para comprobar si AWS ofrecía a los clientes la posibilidad de eliminar su contenido y hacerlo ilegible.	No se observaron desviaciones.
		Se observó a un Security Manager de EC2 crear un host virtual, cargar contenido, eliminar el volumen de almacenamiento subyacente y, a continuación, crear una instancia diferente dentro de la misma ranura de memoria virtual y consultar el contenido original para comprobar que se había eliminado el volumen de almacenamiento subyacente y los datos en memoria.	No se observaron desviaciones.
		En el caso de los servicios que proveen almacenamiento de contenidos tal y como se describe en la Descripción del sistema, se inspeccionaron las configuraciones diseñadas para eliminar automáticamente los contenidos de los buckets, volúmenes, instancias y otros medios de almacenamiento de contenidos, para comprobar que estaban diseñados a fin de eliminar y hacer ilegibles los datos.	No se observaron desviaciones.

Criterios de seguridad, disponibilidad, confidencialidad y privacidad asignados a las pruebas y controles del auditor de servicios de AWS realizados y a sus resultados

Controles establecidos por AWS	Criterios	Pruebas realizadas por EY	Resultados de las pruebas
		Para los servicios que proporcionan almacenamiento de contenido, tal como se describe en la Descripción del sistema, se creó de forma independiente una cuenta en la nube de AWS registrada con una dirección de correo electrónico independiente y se creó contenido de muestra en buckets, volúmenes, instancias u otros medios de almacenamiento de contenido, y se comparó la marca de tiempo de creación con la fecha y hora actuales. Se observó a los administradores de desarrollo de software consultar los objetos para comprobar que los objetos existían y estaban en estado activo.	No se observaron desviaciones.
		Para los servicios centrales de almacenamiento que proporcionan almacenamiento de contenido, tal como se describe en la Descripción del sistema, se creó una cuenta en la nube de AWS registrada con una dirección de correo electrónico independiente y se creó contenido de muestra en buckets, volúmenes, instancias u otros medios de almacenamiento de contenido, y se comparó la marca de tiempo de creación con la fecha y hora actuales. Se observó la consulta de los administradores de desarrollo de software sobre el backend para comprobar que los objetos existieran y estuvieran en estado activo.	No se observaron desviaciones.

Criterios de seguridad, disponibilidad, confidencialidad y privacidad asignados a las pruebas y controles del auditor de servicios de AWS realizados y a sus resultados

Controles establecidos por AWS	Criterios	Pruebas realizadas por EY	Resultados de las pruebas
		En el caso de los servicios que proporcionan almacenamiento de contenido, tal como se describe en la Descripción del sistema, se eliminaron el contenido o los buckets, los volúmenes, las instancias u otros medios de almacenamiento de contenido subyacentes, y se inspeccionó si se eliminaron los identificadores de datos o si los datos en sí se pusieron en cero después de eliminarlos para comprobar que no se podían leer.	No se observaron desviaciones.
		En el caso de los servicios centrales de almacenamiento que proporcionan almacenamiento de contenido, tal como se describe en la Descripción del sistema, se observó a los administradores de desarrollo de software consultar los metadatos de objetos eliminados para comprobar que se haya devuelto un error que indicaba que no se podía encontrar el objeto.	No se observaron desviaciones.
AWSCA-7.8: AWS retiene el contenido de los clientes según los acuerdos con estos.	CC6.5; C1.1; P4.2	Se consultó a un Technical Program Manager de AWS Security Assurance para comprobar que AWS retenía el contenido de los clientes según los acuerdos con estos.	No se observaron desviaciones.
		Se inspeccionó la copia más reciente del Contrato de cliente de AWS para comprobar que se había comunicado externamente a los clientes y que contenía una fecha de entrada en vigor, que era la versión más reciente del contrato.	No se observaron desviaciones.

Criterios de seguridad, disponibilidad, confidencialidad y privacidad asignados a las pruebas y controles del auditor de servicios de AWS realizados y a sus resultados

Controles establecidos por AWS	Criterios	Pruebas realizadas por EY	Resultados de las pruebas
		Se inspeccionó el Contrato de cliente de AWS para comprobar que el lenguaje contractual de la sección 7.3b establecía que AWS no borrará la información del cliente durante un máximo de 30 días en caso de cancelación de la cuenta de AWS, y que el lenguaje establecía explícitamente que el cliente aceptaba las responsabilidades relacionadas con la eliminación de la información confidencial.	No se observaron desviaciones.
		Se inspeccionó la configuración de la retención del contenido de la cuenta del cliente para comprobar que se había diseñado un servicio de cuenta centralizado para enviar notificaciones a los servicios a fin de eliminar el contenido del cliente 90 días después del cierre de la cuenta.	No se observaron desviaciones.
		Se seleccionó un servicio que almacena el contenido del cliente integrado en el servicio de cuenta centralizado, se creó una unidad de almacenamiento de contenido, se cerró la cuenta de AWS y se inspeccionó el contenido a lo largo del ciclo de vida de 90 días para comprobar si el contenido del cliente se conservaba hasta su eliminación 90 días después del cierre de la cuenta del cliente.	No se observaron desviaciones.
		En el caso de un servicio de muestra que almacenaba el contenido del cliente durante más de 30 días, se creó una unidad de almacenamiento de contenido, se cerró la cuenta de AWS, se volvió a abrir la cuenta de AWS 30 días después de la finalización y, por observación, se comprobó que se conservaba el contenido.	No se observaron desviaciones.

Criterios de seguridad, disponibilidad, confidencialidad y privacidad asignados a las pruebas y controles del auditor de servicios de AWS realizados y a sus resultados

Controles establecidos por AWS	Criterios	Pruebas realizadas por EY	Resultados de las pruebas
AWSCA-7.9: específico de Outpost. La clave de seguridad Nitro está configurada en Outpost para cifrar el contenido del cliente y permitir que este disponga de un medio mecánico para realizar la trituración criptográfica del contenido.	CC6.5; C1.2; P4.2; P4.3	Se consultó a un Senior Security Engineer de AWS para comprobar si la clave de seguridad de Nitro estaba configurada en Outpost para cifrar el contenido del cliente y permitir que el cliente disponga de un medio mecánico para realizar la destrucción criptográfica del contenido.	No se observaron desviaciones.
		Se inspeccionaron las configuraciones de Outposts con el fin de comprobar si el Outpost estaba configurado para cifrar el contenido del cliente con la clave de seguridad de Nitro.	No se observaron desviaciones.
		Se inspeccionó el documento de Procedimientos operativos estándar para la recuperación de Outposts a fin de comprobar que la clave de seguridad Nitro se destruye mecánicamente en el momento de la recuperación.	No se observaron desviaciones.
		Se inspeccionaron los registros de un Outpost con una clave de seguridad Nitro válida para comprobar que se cifró correctamente el contenido del Outpost con una clave de seguridad Nitro válida.	No se observaron desviaciones.
		Se inspeccionaron los registros de un Outpost sin una clave de seguridad Nitro válida para comprobar que no se podía descifrar el contenido del Outpost sin la clave de seguridad Nitro válida.	No se observaron desviaciones.

Criterios de seguridad, disponibilidad, confidencialidad y privacidad asignados a las pruebas y controles del auditor de servicios de AWS realizados y a sus resultados

Controles establecidos por AWS	Criterios	Pruebas realizadas por EY	Resultados de las pruebas
AWSCA-7.10: específico de EC2. Amazon EC2 habilita la sincronización del reloj con base en el Protocolo de tiempo de red en las instancias Linux de EC2 para lograr una precisión de 1 milisegundo respecto al tiempo universal coordinado.	CC7.1	Se consultó a un ingeniero de desarrollo de software de AWS que comprobara si Amazon EC2 permitía la sincronización del reloj basada en el protocolo de hora de red en las instancias de EC2, para lograr una precisión dentro de 1 milisegundo del tiempo universal coordinado para las regiones heredadas y dentro de los 100 microsegundos del tiempo universal coordinado para dos regiones mejoradas: Este de EE. UU. (Norte de Virginia) y Asia-Pacífico (Tokio).	No se observaron desviaciones.
		Se inspeccionaron las configuraciones de sincronización del reloj para comprobar que las diferentes capas de la infraestructura estaban vinculadas para garantizar la sincronización del reloj.	No se observaron desviaciones.
		Se observó a un Software Development Engineer de EC2 crear una instancia de EC2 y habilitar la sincronización del reloj para comprobar que la sincronización alcanzara una precisión dentro de 1 milisegundo del tiempo universal coordinado para las regiones heredadas y dentro de los 100 microsegundos del tiempo universal coordinado para dos regiones mejoradas: la región Este de EE. UU. (Norte de Virginia) y Asia-Pacífico (Tokio).	No se observaron desviaciones.
		Para las regiones mejoradas Este de EE. UU. (Norte de Virginia) y Asia-Pacífico (Tokio) se inspeccionaron los dispositivos de reloj Grandmaster administrados por AWS para comprobar si estos dispositivos estaban activos y si el monitoreo estaba habilitado para asegurar una precisión dentro de los 100 milisegundos del tiempo universal coordinado.	No se observaron desviaciones

Criterios de seguridad, disponibilidad, confidencialidad y privacidad asignados a las pruebas y controles del auditor de servicios de AWS realizados y a sus resultados

Controles establecidos por AWS	Criterios	Pruebas realizadas por EY	Resultados de las pruebas
		Se seleccionó una muestra de zonas de disponibilidad (AZ) de AWS a partir de un listado de AZ generado desde un repositorio de código de AZ y se inspeccionaron los dispositivos de reloj Grandmaster administrados por AWS para comprobar si estos dispositivos estaban activos y si el monitoreo estaba habilitado para asegurar que se lograba una precisión dentro de un 1 milisegundo del tiempo universal coordinado.	No se observaron desviaciones.
AWSCA-8.1: los propietarios de los servicios configuran el monitoreo y las alarmas para identificar y notificar al personal operativo y de gestión los incidentes cuando se cruzan los límites de alerta temprana en las métricas operativas clave.	CC2.1; CC6.1; CC6.6; CC6.8; CC7.2; CC7.3; CC7.4; A1.1; A1.2; P6.3; P6.5	Se consultó a los Software Development Managers para comprobar si el entorno de producción se monitoreaba y si los propietarios de los servicios habían configurado las alarmas para notificar al personal operativo y de gestión cuando se cruzaban los límites de alerta temprana en las métricas operativas clave.	No se observaron desviaciones.
		Se seleccionó una muestra de las métricas operativas clave a partir de un listado de alarmas críticas y se inspeccionaron sus configuraciones para comprobar si existían el monitoreo y la alarma relacionados para notificar al personal adecuado cuando se alcanzaba o superaba un límite.	No se observaron desviaciones.
AWSCA-8.2: los incidentes se registran en un sistema de tickets, se les asigna una calificación de gravedad y se les	CC2.1; CC6.1; CC6.6; CC6.8; CC7.2; CC7.3; CC7.4;	Se consultó a un director de respuesta de seguridad de TI de AWS y a un director de desarrollo de software de red transfronteriza de AWS si los incidentes se registraban en un sistema de tickets, se les asignaba un nivel de gravedad y se realizaba un seguimiento hasta su resolución.	No se observaron desviaciones.

Criterios de seguridad, disponibilidad, confidencialidad y privacidad asignados a las pruebas y controles del auditor de servicios de AWS realizados y a sus resultados

Controles establecidos por AWS	Criterios	Pruebas realizadas por EY	Resultados de las pruebas
realiza un seguimiento hasta su resolución.	CC7.5; CC8.1; A1.2; P6.3; P6.5; P6.6; P6.7; P8.1	Se inspeccionaron las configuraciones de la herramienta de monitoreo de la red que crea automáticamente los tickets para los incidentes de monitoreo de la red a fin de comprobar si los incidentes se registraban en un sistema de tickets, se les asignaba un nivel de gravedad y se realizaba un seguimiento hasta su resolución.	No se observaron desviaciones.
		Se seleccionó una muestra de incidentes a partir de un listado generado por el sistema de las principales métricas operativas clave y alertas de seguridad, y se inspeccionaron las entradas asociadas en el sistema de tickets para comprobar si se asignaba un nivel de gravedad a los incidentes y se realizaba un seguimiento hasta su resolución.	No se observaron desviaciones.
AWSCA-9.1: AWS mantiene sitios web informativos internos que describen el entorno de AWS, sus límites, las responsabilidades de los usuarios y los servicios.	CC2.2; CC2.3	Se le consultó al Technical Program Manager de AWS Security Assurance para comprobar si AWS mantenía sitios web informativos internos que describen el entorno de AWS, sus límites, las responsabilidades de los usuarios y los servicios.	No se observaron desviaciones.
		Se inspeccionaron los sitios web informativos internos de AWS para cada servicio de AWS incluido para comprobar que describían el entorno de AWS, sus límites, las responsabilidades de los usuarios y los servicios.	No se observaron desviaciones.
AWSCA-9.2: AWS realiza una investigación previa a la contratación de los candidatos acorde con el puesto	CC1.1; CC1.4	Se consultó al Compliance Manager de Recursos Humanos para comprobar si AWS realizó una selección previa a la contratación de los candidatos a tiempo completo antes de la fecha de inicio de los empleados, de acuerdo con la legislación local.	No se observaron desviaciones.

Criterios de seguridad, disponibilidad, confidencialidad y privacidad asignados a las pruebas y controles del auditor de servicios de AWS realizados y a sus resultados

Controles establecidos por AWS	Criterios	Pruebas realizadas por EY	Resultados de las pruebas
y el nivel del empleado, de acuerdo con la legislación local y la política de seguridad del personal de AWS.		Se seleccionó una muestra de nuevos empleados a tiempo completo de AWS a partir de un listado de empleados activos y se inspeccionaron sus registros de control previo a la contratación, para comprobar si se había realizado un control previo a la contratación antes de la fecha de inicio de cada empleado.	No se observaron desviaciones.
AWSCA-9.3: AWS realiza una evaluación formal anual de los recursos y la dotación de personal, incluida la evaluación de la alineación de las calificaciones de los empleados con los objetivos de la entidad. Los empleados reciben comentarios sobre sus fortalezas e ideas de crecimiento anualmente.	CC1.1; CC1.4; CC1.5	Se consultó a un Director of Talent Management para comprobar si existía un proceso para realizar una evaluación formal de la dotación de recursos y personal anualmente, incluida una evaluación de la alineación de las calificaciones de los empleados con los objetivos de la entidad y que los empleados recibieran comentarios sobre sus fortalezas e ideas de crecimiento.	No se observaron desviaciones.
		Se seleccionó una muestra de empleados de AWS a partir de un listado generado por el sistema de RR. HH., y se inspeccionaron sus registros de evaluación del rendimiento para comprobar si se había evaluado formalmente a cada empleado con respecto a los objetivos de la entidad durante la evaluación formal anual más reciente de recursos y dotación de personal.	No se observaron desviaciones.
AWSCA-9.4: los ajustes de configuración de los hosts de AWS se monitorean para validar la conformidad con los	CC6.1; CC6.8; CC7.1; CC8.1	Se consultó a un System Engineering Manager y a un Software Development Manager para comprobar si los ajustes de configuración del host de AWS se monitoreaban para validar la conformidad con las normas de seguridad de AWS y si se enviaban automáticamente a la flota.	No se observaron desviaciones.

Criterios de seguridad, disponibilidad, confidencialidad y privacidad asignados a las pruebas y controles del auditor de servicios de AWS realizados y a sus resultados

Controles establecidos por AWS	Criterios	Pruebas realizadas por EY	Resultados de las pruebas
estándares de seguridad de AWS y se envían automáticamente a la flota de hosts.		Se inspeccionaron las configuraciones de monitoreo para comprobar que los hosts de producción se configuraron para monitorear la conformidad con los estándares de seguridad de AWS y para solicitar e instalar automáticamente las actualizaciones de los ajustes de configuración de los hosts enviadas a la flota.	No se observaron desviaciones.
		Se seleccionaron hosts de producción y se inspeccionaron los registros de implementación automatizados para comprobar que los hosts de producción solicitaban e instalaban automáticamente las actualizaciones de los ajustes de configuración del host enviadas a la flota.	No se observaron desviaciones.
		Se inspeccionaron lo detalles de un ticket de incidencia creado por un intento de implementación fallido, para comprobar si la instalación fallida de los ajustes de configuración del host se había identificado, seguido y resuelto a tiempo.	No se observaron desviaciones.
AWSCA-9.5: AWS proporciona mecanismos disponibles públicamente para que los clientes se comuniquen con AWS para reportar eventos de seguridad e información publicada, lo que incluye una	CC2.2; CC2.3; P5.1; P5.2; P6.3; P8.1	Se consultó a un administrador de controles de seguridad de AWS Security Assurance y a un administrador sénior de programas técnicos de marketing técnico para comprobar que AWS proporcionaba mecanismos disponibles públicamente para que los clientes se comuniquen con AWS con el objetivo de informar sobre eventos de seguridad e información publicada, que incluye una descripción del sistema e información de seguridad y cumplimiento que aborda los compromisos y las responsabilidades de AWS.	No se observaron desviaciones.

Criterios de seguridad, disponibilidad, confidencialidad y privacidad asignados a las pruebas y controles del auditor de servicios de AWS realizados y a sus resultados

Controles establecidos por AWS	Criterios	Pruebas realizadas por EY	Resultados de las pruebas
descripción del sistema e información de seguridad y conformidad que aborda los compromisos y las responsabilidades de AWS.		Se inspeccionaron los sitios web informativos de AWS para comprobar que proporcionaban mecanismos disponibles públicamente a fin de que los clientes se pusieran en contacto con AWS para informar eventos de seguridad.	No se observaron desviaciones.
		Se inspeccionaron los documentos técnicos y los sitios web públicos de AWS para comprobar que proporcionaban información, incluida una descripción del sistema e información sobre seguridad y conformidad que abordaba los compromisos y las responsabilidades de AWS.	No se observaron desviaciones.
		Se inspeccionó un ticket resultante de una consulta de un cliente para comprobar que existe un proceso para abordar, seguir y resolver las consultas de los clientes en el momento oportuno.	No se observaron desviaciones.
		En el caso de una muestra de consultas de cumplimiento enviadas por clientes y seleccionadas del portal de soporte de cumplimiento de Contacte con nosotros de AWS, se inspeccionó la documentación de apoyo para comprobar que un representante de marketing realizó un seguimiento puntual de cada consulta mediante correo electrónico o llamada telefónica.	No se observaron desviaciones
AWSCA-9.6: la empresa ofrece una línea directa para que los empleados informen de forma anónima sobre	CC2.2; CC7.2; CC7.3; CC7.4; CC7.5	Se le consultó al Vice President de Litigation Legal si la empresa proporcionaba una línea directa para que los empleados informaran de forma anónima sobre posibles violaciones de la conducta.	No se observaron desviaciones.

Criterios de seguridad, disponibilidad, confidencialidad y privacidad asignados a las pruebas y controles del auditor de servicios de AWS realizados y a sus resultados

Controles establecidos por AWS	Criterios	Pruebas realizadas por EY	Resultados de las pruebas
posibles violaciones de la conducta.		Se inspeccionó el manual del propietario y la guía de la política de empleo para comprobar que los empleados tenían acceso a la línea directa de ética en todas las zonas geográficas durante la orientación.	No se observaron desviaciones.
		Se llamó al número de la línea directa de fraude para comprobar que estaba disponible para que los empleados informaran de forma anónima sobre posibles violaciones de la conducta.	No se observaron desviaciones.

Criterios de seguridad, disponibilidad, confidencialidad y privacidad asignados a las pruebas y controles del auditor de servicios de AWS realizados y a sus resultados

Controles establecidos por AWS	Criterios	Pruebas realizadas por EY	Resultados de las pruebas
AWSCA-9.7: las infracciones importantes del Código de conducta y ética empresarial y de políticas similares de la empresa se tratan adecuadamente en términos de comunicación y de posibles medidas disciplinarias o de	CC1.1; CC1.5; CC9.2; P8.1	Se consultó al Director de Recursos Humanos para comprobar que las infracciones materiales del Código de conducta y ética empresarial de la empresa y políticas similares se trataban adecuadamente en términos de comunicación y posibles medidas disciplinarias o despido, y que las infracciones que implicaban a terceros o contratistas se comunicaban a sus respectivos empleadores, que se encargaban de cualquier posible medida disciplinaria, remoción de la asignación con Amazon o despido.	No se observaron desviaciones.

Criterios de seguridad, disponibilidad, confidencialidad y privacidad asignados a las pruebas y controles del auditor de servicios de AWS realizados y a sus resultados

Controles establecidos por AWS	Criterios	Pruebas realizadas por EY	Resultados de las pruebas
despido. Las violaciones que implican a terceros o contratistas se comunican a sus respectivos empleadores, que realizarán cualquier posible acción disciplinaria, remoción de la asignación con Amazon o despido.		Se inspeccionó la política del Código de conducta y ética empresarial de la empresa para comprobar que las expectativas de los empleados estaban publicadas en la Intranet para que los empleados las revisaran y que las consecuencias de determinadas infracciones estaban documentadas en la política.	No se observaron desviaciones.
		Se inspeccionó la wiki del proceso de investigación del equipo de RR. HH. y el sistema Enterprise Case Management para comprobar que se detallaban los procedimientos operativos estándar para el tratamiento de una posible infracción sustancial del Código de conducta y ética empresarial de la empresa, tanto para los empleados como para los proveedores, incluido el tratamiento de la comunicación y las posibles medidas disciplinarias.	No se observaron desviaciones.
AWSCA-9.8: AWS estableció un programa de auditoría formal que incluye evaluaciones internas y externas continuas e independientes para validar la implementación y la eficacia operativa del entorno de control de AWS.	CC1.2; CC2.1; CC3.1; CC4.1; CC4.2; P8.1	Se consultó a un Business Risk Management Director para comprobar si AWS había establecido un programa de auditoría formal que incluía evaluaciones internas y externas continuas e independientes para validar la implementación y la eficacia operativa del entorno de control de AWS.	No se observaron desviaciones.
		Se inspeccionó el marco de auditoría y el listado de entrevistados para comprobar si las áreas funcionales de AWS, incluidos los equipos de AWS Security y de AWS Service, estaban cubiertas por la creación de la evaluación del riesgo de la auditoría interna.	No se observaron desviaciones.

Criterios de seguridad, disponibilidad, confidencialidad y privacidad asignados a las pruebas y controles del auditor de servicios de AWS realizados y a sus resultados

Controles establecidos por AWS	Criterios	Pruebas realizadas por EY	Resultados de las pruebas
		Se inspeccionó el plan de auditoría anual creado por la auditoría interna y enviado al comité de auditoría para comprobar que la auditoría interna había formalizado y esbozado su plan de auditoría específico como respuesta a la evaluación del riesgo realizada, y que el plan de auditoría incluía la organización de AWS.	No se observaron desviaciones.
AWSCA-9.9: AWS tiene un proceso para evaluar si los empleados de AWS que tienen acceso a los recursos que almacenan o procesan los datos de los clientes a través de grupos de permisos están sujetos a una verificación de antecedentes después de la contratación, según la legislación local. Los empleados de AWS que tienen acceso a recursos que almacenan o procesan datos de clientes serán sometidos a una verificación de antecedentes de acuerdo con la Política de seguridad del personal de AWS.	CC1.1; CC1.4;	Se consultó a un Security Assurance Program Manager para comprobar si los empleados con acceso a recursos que almacenan o procesan datos de clientes a través de grupos de permisos recibían una verificación de antecedentes, según la legislación local, una vez por año natural como mínimo.	No se observaron desviaciones.
		Se seleccionó una muestra de empleados de AWS a partir de una lista generada por el sistema de cuentas que tienen acceso a recursos que almacenan o procesan datos de clientes, y se inspeccionó el estado de su comprobación de antecedentes para verificar si se completaban las comprobaciones de antecedentes una vez por año calendario o si se eliminaba el acceso a recursos que almacenan o procesan datos de clientes, según corresponda.	No se observaron desviaciones.

Criterios de seguridad, disponibilidad, confidencialidad y privacidad asignados a las pruebas y controles del auditor de servicios de AWS realizados y a sus resultados

Controles establecidos por AWS	Criterios	Pruebas realizadas por EY	Resultados de las pruebas
AWSCA-10.1: los componentes del sistema crítico de AWS se replican en varias zonas de disponibilidad y se realiza el mantenimiento de las copias de respaldo.	A1.2	Se le preguntó a los administradores de desarrollo de *software* repositorio para comprobar que los componentes del sistema crítico de AWS se replicaron en varias zonas de disponibilidad y se realizó el mantenimiento de las copias de seguridad.	No se observaron desviaciones.
		Se inspeccionaron las configuraciones de replicación a fin de comprobar que los componentes del sistema crítico de AWS se configuraron para que se repliquen en varias zonas de disponibilidad.	No se observaron desviaciones.
		Se inspeccionaron las configuraciones de las copias de seguridad para comprobar si se realizaba la copia de seguridad de los componentes del sistema crítico de AWS a medida que se implementaban los cambios o de acuerdo con los trabajos configurados de manera periódica a lo largo del día.	No se observaron desviaciones.
		En el caso de los archivos del componente del sistema, se inspeccionaron los registros de la replicación del entorno de producción y la copia de seguridad del servicio de AWS relacionado para comprobar si los datos se replicaban en varias zonas de disponibilidad.	No se observaron desviaciones.
AWSCA-10.2: las copias de respaldo de los componentes del sistema crítico de AWS se monitorean para realizar la reproducción exitosa en varias zonas de disponibilidad.	A1.2; A1.3; C1.1	Se le preguntó a los Repository Software Development Managers a fin de comprobar que los componentes del sistema crítico de AWS se monitorearon para la replicación en varias zonas de disponibilidad.	No se observaron desviaciones.
		Se inspeccionó la configuración del monitoreo de copias de seguridad para comprobar si los tickets de incidentes de error se generaban automáticamente en caso de fallas en las copias de seguridad.	No se observaron desviaciones.

Criterios de seguridad, disponibilidad, confidencialidad y privacidad asignados a las pruebas y controles del auditor de servicios de AWS realizados y a sus resultados

Controles establecidos por AWS	Criterios	Pruebas realizadas por EY	Resultados de las pruebas
		En el caso de una alarma crítica, se inspeccionaron los paneles de monitoreo y las configuraciones de las alarmas a fin de determinar si existía un mecanismo de alarma para notificar al personal adecuado sobre los éxitos y fallas de la replicación y de la copia de seguridad, y cuando los archivos no se replicaron lo suficiente en varias zonas de disponibilidad.	No se observaron desviaciones.
		Se inspeccionaron las notificaciones de cuando una copia de seguridad no se completó y cuando los archivos no estaban suficientemente representados en varias zonas de disponibilidad para asegurarse de que el equipo de servicio inició el proceso de corrección y rastreó los problemas hasta su resolución.	No se observaron desviaciones.

Criterios de seguridad, disponibilidad, confidencialidad y privacidad asignados a las pruebas y controles del auditor de servicios de AWS realizados y a sus resultados

Controles establecidos por AWS	Criterios	Pruebas realizadas por EY	Resultados de las pruebas
AWSCA-10.3: la planificación de contingencia de AWS y las guías de respuesta a incidentes se mantienen y actualizan para reflejar los riesgos de	CC2.2; CC3.2; CC3.3; CC3.4; CC5.3; CC7.3; CC7.4; CC7.5; CC8.1;	Se le preguntó a un Technical Program Manager de cumplimiento de AWS si AWS mantenía un procedimiento de planificación de contingencia general que refleje los riesgos de continuidad emergentes e incorpore las lecciones aprendidas de incidentes pasados, y si el plan de contingencia de AWS se prueba al menos una vez al año.	No se observaron desviaciones.

Criterios de seguridad, disponibilidad, confidencialidad y privacidad asignados a las pruebas y controles del auditor de servicios de AWS realizados y a sus resultados

Controles establecidos por AWS	Criterios	Pruebas realizadas por EY	Resultados de las pruebas
continuidad emergentes y las lecciones aprendidas de incidentes anteriores. El plan de contingencia de AWS se prueba al menos una vez al año.	CC9.1; A1.1; A1.2; A1.3; P6.3	Se solicitó a los Software Development Managers que determinaran la planificación de contingencia de AWS y las guías de respuesta a incidentes específicos para cada equipo de servicio, que se mantienen y actualizan para reflejar los riesgos de continuidad emergentes y las lecciones aprendidas de incidentes anteriores.	No se observaron desviaciones.
		Se inspeccionó la documentación del plan de contingencia de AWS para asegurarse de que se revisó y aprobó al menos una vez al año, y que las guías de cada servicio existentes se mantuvieron y se actualizaron para reflejar los riesgos de continuidad emergentes y las lecciones aprendidas de incidentes pasados.	No se observaron desviaciones.
		En una prueba anual más reciente del plan de contingencia de AWS, se inspeccionó el ticket para comprobar que el plan de contingencia se probó durante el último año y que se resolvieron los simulacros realizados para imitar los incidentes y se restableció la disponibilidad del servicio.	No se observaron desviaciones.
AWSCA-10.4: AWS mantiene un modelo de planificación de la capacidad para evaluar el uso y la demanda de la infraestructura al menos una vez al mes, y normalmente	A1.1; A1.2	Se le preguntó a un administrador sénior de planificación de la capacidad del centro de datos y a un administrador de programas técnicos de borde para determinar si AWS mantenía un modelo de planificación de capacidad que evaluaba el uso de la infraestructura, la demanda prevista y los recursos adicionales necesarios para cumplir con los requisitos de disponibilidad.	No se observaron desviaciones.

Criterios de seguridad, disponibilidad, confidencialidad y privacidad asignados a las pruebas y controles del auditor de servicios de AWS realizados y a sus resultados

Controles establecidos por AWS	Criterios	Pruebas realizadas por EY	Resultados de las pruebas
con más frecuencia (por ejemplo, semanalmente). Además, el modelo de planificación de la capacidad de AWS apoya la planificación de las demandas futuras para adquirir e implementar recursos adicionales basados en los recursos actuales y los requisitos previstos.		Se le preguntó a los administradores de desarrollo de software para asegurarse de que los servicios incluidos en el alcance cuentan con programas de capacidad establecidos para monitorear el uso y enviar necesidades de capacidad adicional al equipo central de planificación de capacidad.	No se observaron desviaciones.
		Se seleccionó una muestra de regiones y ubicaciones periféricas, y se inspeccionó el modelo de planificación de capacidad para determinar si la capacidad se evaluó según la frecuencia definida y si el modelo contenía previsiones de demandas futuras y disponibilidad de recursos.	No se observaron desviaciones.
AWSCA-11.1: los proveedores y terceros con acceso restringido, que realizan negocios con Amazon, están sujetos a compromisos de confidencialidad como parte de sus acuerdos con Amazon. AWS y terceros revisan los compromisos de confidencialidad incluidos en los acuerdos con proveedores y terceros, con acceso restringido, en el momento de la redacción o la firma del contrato.	CC1.1; CC1.4; CC2.2; CC2.3; CC9.2; P6.4; P6.5	Se le preguntó al Legal Corporate Counsel de AWS si los proveedores o terceros con acceso restringido, que realizan negocios con AWS, han estado sujetos a acuerdos de confidencialidad como parte de sus acuerdos con Amazon y si AWS y el tercero revisaron estos acuerdos en el momento de la redacción o la firma del contrato.	No se observaron desviaciones.
		Para una muestra de proveedores externos y terceros con acceso restringido que realizan negocios con Amazon, se inspeccionaron los acuerdos con los proveedores para comprobar si contenían compromisos de confidencialidad.	No se observaron desviaciones.
		Se seleccionó una muestra de proveedores externos y terceros con acceso restringido que realizan negocios con Amazon, y se inspeccionaron los acuerdos con los proveedores para comprobar si el proveedor y AWS los habían firmado y aprobado.	No se observaron desviaciones.

Criterios de seguridad, disponibilidad, confidencialidad y privacidad asignados a las pruebas y controles del auditor de servicios de AWS realizados y a sus resultados

Controles establecidos por AWS	Criterios	Pruebas realizadas por EY	Resultados de las pruebas
AWSCA-11.2: AWS tiene un programa vigente para evaluar el desempeño de los proveedores y la conformidad con las obligaciones contractuales.	CC1.1; CC1.4; CC2.3; CC4.1; CC9.2; P4.1; P6.1; P6.4; P6.5	Se le preguntó al equipo de Servicios globales del centro de datos si AWS cuenta con un programa implementado para evaluar el desempeño de los proveedores y el cumplimiento de las obligaciones contractuales.	No se observaron desviaciones.
		Se inspeccionaron los calendarios del programa de evaluación de AWS para evaluar el desempeño del proveedor y el cumplimiento de las obligaciones contractuales y determinar que las revisiones para los proveedores con acceso restringido se programaron con una frecuencia sujeta al riesgo general de hacer negocios con cada proveedor.	No se observaron desviaciones.
		Se seleccionó una muestra de proveedores a partir de una lista de proveedores terceros y se inspeccionaron las evaluaciones de desempeño y cumplimiento de los proveedores con las obligaciones contractuales para comprobar que las revisiones se realizaban de acuerdo con la frecuencia estipulada en la política y que servían como medio para evaluar el desempeño de los proveedores con respecto a las obligaciones contractuales, en función del riesgo.	No se observaron desviaciones.
AWSCA-11.3: AWS comunica los requisitos de confidencialidad en los acuerdos cuando se renuevan con proveedores y terceros con acceso restringido. Los cambios en los	CC2.2; CC2.3; CC9.2; P6.4; P6.5	Se le preguntó a un Technical Program Manager de AWS Security Assurance para comprobar que AWS comunicó los requisitos de confidencialidad al renovar los contratos con proveedores y terceros con acceso restringido y que los cambios en los compromisos de confidencialidad estándar con los clientes se comunicaron en el sitio web de AWS a través del Contrato de cliente de AWS.	No se observaron desviaciones.

Criterios de seguridad, disponibilidad, confidencialidad y privacidad asignados a las pruebas y controles del auditor de servicios de AWS realizados y a sus resultados

Controles establecidos por AWS	Criterios	Pruebas realizadas por EY	Resultados de las pruebas
compromisos de confidencialidad estándar con los clientes se comunican en el sitio web de AWS a través del Contrato de cliente de AWS.		Para una muestra de proveedores externos y terceros con acceso restringido que realizan negocios con Amazon, se inspeccionaron los acuerdos vigentes con proveedores para comprobar si AWS comunicó los compromisos de confidencialidad y privacidad como parte de los acuerdos.	No se observaron desviaciones.
		Se inspeccionó el Contrato de cliente de AWS público que se encuentra en el sitio web de AWS para determinar los cambios en los compromisos de confidencialidad estándar que se comunicaron a través del Contrato de cliente de AWS y se pusieron a disposición del público a través de un registro de cambios integrado.	No se observaron desviaciones.
AWSCA-12.1: AWS informa a los clientes de los compromisos de seguridad y privacidad de los datos de AWS en el Contrato de cliente de AWS antes de activar una cuenta de AWS y lo pone a disposición de los clientes para que lo revisen en cualquier momento en el sitio web de AWS.	P1.1; P2.1; P3.1; P5.1; P5.2; P6.1; P8.1	Se solicitó al Consejo corporativo de AWS que se asegurara de que AWS informa a los clientes los compromisos de privacidad y seguridad informática de los datos de AWS en el Contrato de cliente de AWS antes de activar una cuenta de AWS y lo pone a disposición de los clientes para que lo revisen en cualquier momento en el sitio web de AWS.	No se observaron desviaciones.
		Se intentó crear una cuenta de AWS sin aceptar el Contrato de cliente de AWS y se observó que el sistema impedía continuar con la apertura de la cuenta.	No se observaron desviaciones.
		Se reconoció el Contrato de cliente de AWS y se creó correctamente una cuenta de AWS para comprobar que se requería el reconocimiento del Contrato de cliente de AWS antes de abrir una cuenta de AWS.	No se observaron desviaciones.

Criterios de seguridad, disponibilidad, confidencialidad y privacidad asignados a las pruebas y controles del auditor de servicios de AWS realizados y a sus resultados

Controles establecidos por AWS	Criterios	Pruebas realizadas por EY	Resultados de las pruebas
		Se inspeccionó el Contrato de cliente de AWS en el sitio web de AWS para comprobar que el Contrato de cliente de AWS está disponible públicamente para que los clientes lo revisen y que informa a los clientes sobre los compromisos de seguridad y privacidad de los datos de AWS.	No se observaron desviaciones.
AWSCA-12.2: AWS informa a los clientes de los cambios realizados en el Contrato de cliente de AWS a través del sitio web público de AWS.	CC2.3; P1.1	Se preguntó al Consejo corporativo de AWS si AWS informa a los clientes de los cambios realizados en el Contrato de cliente de AWS a través del sitio web público de AWS.	No se observaron desviaciones.
		Se inspeccionó el Contrato de cliente de AWS a través del sitio web de AWS para comprobar que se mostraba a los clientes la fecha de la última actualización.	No se observaron desviaciones.
		Se inspeccionó el Contrato de cliente de AWS para comprobar que contenía un compromiso de la administración de poner a disposición de los clientes cualquier cambio aplicado en el Contrato de cliente de AWS.	No se observaron desviaciones.
AWSCA-12.3: AWS ofrece a los clientes la posibilidad de actualizar las preferencias de comunicación a través de la consola de AWS.	P2.1	Se consultó a un administrador de programas sénior para comprobar que Amazon ofrece a los clientes la capacidad de actualizar sus preferencias de comunicación a través de la consola de AWS.	No se observaron desviaciones.
		Se observó a un administrador de programas sénior actualizar las preferencias de comunicación de una cuenta de AWS a través de la consola de AWS, se inspeccionó la actualización en el repositorio backend y se inspeccionó la notificación de confirmación de actualización de las preferencias de comunicación para comprobar que Amazon ofrece a los clientes la posibilidad de actualizar las preferencias de comunicación a través de la consola de AWS.	No se observaron desviaciones.

Criterios de seguridad, disponibilidad, confidencialidad y privacidad asignados a las pruebas y controles del auditor de servicios de AWS realizados y a sus resultados

Controles establecidos por AWS	Criterios	Pruebas realizadas por EY	Resultados de las pruebas
AWSCA-12.4: AWS realiza revisiones de seguridad de las aplicaciones para sistemas de terceros que recopilan contenido de clientes de acuerdo con los procesos del equipo, para garantizar que se identifican y mitigan los riesgos de seguridad.	CC2.3; P1.1; P3.1; P4.1; P4.2; P6.1; P6.4	Se preguntó a un Technical Program Manager si AWS realiza revisiones de seguridad informática de la aplicación para sistemas de terceros que recopilan contenido de clientes de acuerdo con los procesos del equipo, para garantizar que se identifican y mitigan los riesgos de seguridad.	No se observaron desviaciones.
		Se inspeccionó la documentación del equipo de incorporación de terceros a los proveedores de sistemas de terceros que recopilan contenidos de clientes para comprobar que se evaluaba a los terceros en relación con la recopilación de contenidos de clientes y se los remitía a revisiones de seguridad adicionales.	No se observaron desviaciones.
		Se seleccionó una muestra de revisiones de seguridad de sistemas de terceros que recopilan contenido de los clientes que se implementó durante el periodo de evaluación para comprobar que el sistema se evaluó antes de su lanzamiento a fin de verificar si se identificaron y mitigaron los riesgos de seguridad.	No se observaron desviaciones.
AWSCA-12.5: AWS notifica a los Titulares de los Datos afectados y a los reguladores las infracciones e incidentes tal y como exige la ley de acuerdo con los procesos del equipo.	P5.1; P5.2; P6.3; P6.4; P6.6; P6.7; P8.1; CC2.3; CC7.4	Se consultó a un Consejo corporativo sénior de AWS para comprobar si AWS notifica a los titulares de los datos afectados y a los reguladores sobre las vulneraciones e incidentes tal y como exige la ley de acuerdo con los procesos del equipo.	No se observaron desviaciones.
		Se inspeccionó la política de privacidad interna de AWS para comprobar que AWS notifica a los Titulares de los datos afectados y a los reguladores las infracciones e incidentes tal y como exige la ley de acuerdo con los procesos del equipo.	No se observaron desviaciones.

Criterios de seguridad, disponibilidad, confidencialidad y privacidad asignados a las pruebas y controles del auditor de servicios de AWS realizados y a sus resultados

Controles establecidos por AWS	Criterios	Pruebas realizadas por EY	Resultados de las pruebas
		Se inspeccionaron los detalles de la respuesta a incidentes de una muestra de tickets de incidentes de alertas de seguridad para comprobar si se habían realizado las evaluaciones necesarias para determinar si era obligatorio informar a los titulares de datos afectados y a los reguladores sobre las infracciones, y si la información requerida se había comunicado de forma adecuada según la documentación de respuesta a incidentes.	No se observaron desviaciones
AWSCA-12.6: AWS ofrece a los clientes autenticados la posibilidad de acceder a sus datos, actualizarlos y confirmarlos. La denegación de acceso se comunicará mediante la consola de AWS.	P5.1; P5.2; P7.1	Se consultó a un Consejo corporativo sénior para comprobar si AWS ofrece a los clientes autenticados la posibilidad de acceder a sus datos, actualizarlos y confirmarlos. Además, se consultó a un Consejo corporativo sénior para determinar qué condiciones desencadenarían una denegación de acceso y que la denegación se comunicaría mediante la consola de AWS.	No se observaron desviaciones.
		Se inspeccionó el Contrato de cliente de AWS para comprobar que AWS se compromete a notificar a los clientes antes de denegarles el acceso.	No se observaron desviaciones.
		Se actualizó la información de las cuentas personales en la Consola de AWS para comprobar que AWS ofrece a los clientes autenticados la posibilidad de acceder a sus datos, actualizarlos y confirmarlos.	No se observaron desviaciones.
AWSCA-12.7: AWS registra las solicitudes de información de los clientes para	P5.1; P5.2; P6.1; P6.2; P6.7;	Se preguntó al Consejo corporativo de AWS si AWS registra las solicitudes de información de los clientes para mantener un registro completo, preciso y oportuno de dichas solicitudes.	No se observaron desviaciones.

Criterios de seguridad, disponibilidad, confidencialidad y privacidad asignados a las pruebas y controles del auditor de servicios de AWS realizados y a sus resultados

Controles establecidos por AWS	Criterios	Pruebas realizadas por EY	Resultados de las pruebas
mantener un registro completo, preciso y oportuno de dichas solicitudes.		Se inspeccionaron las configuraciones para el registro de solicitudes de información de los clientes a través del sistema de seguimiento de solicitudes de aplicación de la ley de Amazon a fin de comprobar que AWS registra las solicitudes de información de los clientes para mantener un registro completo, exacto y oportuno de dichas solicitudes.	No se observaron desviaciones.
		Se observó el repositorio de solicitudes de información de los clientes de AWS para comprobar que AWS registra las solicitudes de información de los clientes.	No se observaron desviaciones.
AWSCA-12.8: a menos que se prohíba hacerlo o exista una indicación clara de conducta ilegal en relación con el uso de los productos o servicios de AWS, AWS hace un intento razonable de notificar a los clientes antes de divulgar el Contenido del cliente en respuesta a solicitudes válidas o vinculantes de la ley.	P6.7	Se solicitó al Consejo corporativo de AWS que se asegurara de que AWS hace un intento razonable de notificar a los clientes antes de divulgar el Contenido del cliente en respuesta a solicitudes válidas o vinculantes de la ley, a menos que esté legalmente prohibido hacerlo.	No se observaron desviaciones.
		Se inspeccionó la política pública de las Directrices de aplicación de la ley de Amazon para comprobar si AWS no divulga información de clientes en respuesta a demandas del Gobierno, a menos que se le exija a AWS legalmente mediante una orden vinculante. En tales casos, AWS notifica a los clientes antes de la divulgación, a menos que la ley lo prohíba.	No se observaron desviaciones.
		En el caso de una divulgación de Contenido del cliente en respuesta a una solicitud vinculante de la ley, se inspeccionó una notificación por correo electrónico enviada desde AWS Legal a un cliente de AWS y un acuse de recibo del cliente de AWS para comprobar que AWS notificó al cliente antes de divulgar el contenido del cliente.	No se observaron desviaciones.

Criterios de seguridad, disponibilidad, confidencialidad y privacidad asignados a las pruebas y controles del auditor de servicios de AWS realizados y a sus resultados

Controles establecidos por AWS	Criterios	Pruebas realizadas por EY	Resultados de las pruebas
AWSCA-12.9: AWS mantiene contratos con subprocesadores de terceros que incluyen protección de datos, compromisos de confidencialidad y requisitos de seguridad.	P6.1	Se consultó a un Consejo corporativo de AWS para comprobar si AWS mantenía contratos con subprocesadores de terceros que incluyeran pe protección de datos, compromisos de confidencialidad y requisitos de seguridad.	No se observaron desviaciones.
		En el caso de una muestra de subprocesadores de terceros seleccionados del sitio web público de subprocesadores de AWS, se inspeccionaron los contratos para comprobar que incluyeran protección de datos, compromisos de confidencialidad y requisitos de seguridad.	No se observaron desviaciones.
AWSCA-12.10: se realiza una revisión formal de los subprocesadores de terceros antes de que AWS permita cualquier procesamiento por parte de los subprocesadores de terceros, con el fin	P6.7	Se consultó a un Consejo corporativo de AWS para comprobar si se había realizado una revisión formal de los subprocesadores de terceros antes de que AWS permitiera cualquier procesamiento por parte de subprocesadores de terceros.	No se observaron desviaciones.

Criterios de seguridad, disponibilidad, confidencialidad y privacidad asignados a las pruebas y controles del auditor de servicios de AWS realizados y a sus resultados

Controles establecidos por AWS	Criterios	Pruebas realizadas por EY	Resultados de las pruebas
de determinar que se implementaron las restricciones adecuadas para limitar el procesamiento del contenido del cliente por parte de los subprocesadores de terceros únicamente al contenido del cliente que es necesario para proporcionar o mantener los servicios de AWS seleccionados por el cliente.		En el caso de una muestra de subprocesadores de terceros seleccionada del sitio web público de subprocesadores de AWS, se inspeccionó la revisión de seguridad de las aplicaciones realizada por el equipo de seguridad de proveedores de aplicaciones (AVS) para comprobar que se evaluaron las restricciones que limitan el procesamiento del contenido del cliente por parte de subprocesadores de terceros únicamente al contenido del cliente que es necesario para proporcionar o mantener los servicios de AWS seleccionados por el cliente, antes de que AWS permitiera cualquier procesamiento por parte del subprocesador de terceros.	No se observaron desviaciones.
AWSCA-12.11: AWS realiza reevaluaciones anuales de los subprocesadores de terceros, o después de incidentes importantes o cambios significativos.	P6.1	Se consultó a un Consejo corporativo de AWS para comprobar si AWS cuenta con un proceso para realizar reevaluaciones anuales de los subprocesadores de terceros, o después de incidentes importantes o cambios significativos.	No se observaron desviaciones.
		En el caso de una muestra de subprocesadores de terceros seleccionados del sitio web público de subprocesadores de AWS, se inspeccionó la revisión de seguridad de las aplicaciones realizada por el equipo de seguridad de proveedores de aplicaciones (AVS) para comprobar que se realizaban reevaluaciones de los subprocesadores de terceros anualmente o tras incidentes graves o cambios significativos.	No se observaron desviaciones.

Criterios de seguridad, disponibilidad, confidencialidad y privacidad asignados a las pruebas y controles del auditor de servicios de AWS realizados y a sus resultados

Controles establecidos por AWS	Criterios	Pruebas realizadas por EY	Resultados de las pruebas
AWSCA-12.12: el proceso de lanzamiento de nuevos subprocesadores de terceros requiere la adición a la lista publicada externamente de subprocesadores de terceros que actualmente están contratados por AWS para procesar los datos del cliente en función de la región de AWS y el servicio de AWS que el cliente seleccione.	P6.7	Se consultó a un Consejo corporativo de AWS para comprobar el proceso de lanzamiento de nuevos subprocesadores de terceros que se requieren agregar a la lista pública de subprocesadores de terceros que actualmente están contratados por AWS.	No se observaron desviaciones.
		Se inspeccionó el manual de lanzamiento para comprobar que incluyera los requisitos de notificación al equipo correspondiente y la adición de subprocesadores de terceros a la lista de subprocesadores publicada externamente para la divulgación pública del uso de nuevos subprocesadores de terceros antes de que AWS permitiera cualquier procesamiento por parte de estos.	No se observaron desviaciones.

SECCIÓN V: Otra información proporcionada por Amazon Web Services

Para el informe SOC de otoño actual (del 1/10/2023 al 30/09/2024) AWS agregó nuevos controles y realizó mejoras en los controles actuales y en la información relacionada presentada en comparación con el informe SOC anterior. Estos cambios fueron impulsados por nuestro compromiso con la mejora continua, el deseo de ajustar mejor nuestros controles documentados con nuestros procesos operativos en evolución, las guía SOC del AICPA y los comentarios recibidos de nuestros clientes. Las secciones a continuación ofrecen una visión general de los cambios:

Sección I: Modificaciones de los controles existentes

Se realizaron cambios menores en la redacción de las siguientes descripciones de control para reflejar con mayor precisión los procesos existentes.

ANTIGUO: primavera 2024	NUEVO: otoño 2024
AWSCA-3.5: AWS habilita a los clientes para que articulen quién tiene acceso a los servicios y recursos de AWS (si los permisos a nivel de recursos son aplicables al servicio) que poseen. AWS impide que los clientes accedan a los recursos de AWS que no tienen asignados mediante permisos de acceso. El contenido solo se devuelve a las personas autorizadas a acceder al servicio o recurso de AWS especificado (si los permisos a nivel de recurso son aplicables al servicio).	**AWSCA-3.5:** AWS habilita a los clientes para que seleccionen quién tiene acceso a los servicios y recursos de AWS (si los permisos a nivel de recursos son aplicables al servicio) que poseen. AWS impide que los clientes accedan a los recursos de AWS que no tienen asignados mediante permisos de acceso. El contenido solo se devuelve a las personas autorizadas a acceder al servicio o recurso de AWS especificado (si los permisos a nivel de recurso son aplicables al servicio).
AWSCA-5.8: los centros de datos de Amazon están climatizados para mantener las condiciones atmosféricas adecuadas. El personal y los sistemas monitorean y controlan la temperatura y la humedad del aire a niveles adecuados.	**AWSCA-5.8:** los centros de datos de Amazon están climatizados para mantener unas condiciones ambientales adecuadas. El personal y los sistemas monitorean y controlan la temperatura y la humedad del aire a niveles adecuados.
AWSCA-5.13: antes de abandonar las zonas seguras de AWS, todos los medios de producción de AWS se retiran de forma segura y se destruyen físicamente bajo la verificación de dos empleados.	**AWSCA-5.13:** antes de abandonar el control de AWS, todos los medios de producción de AWS se retiran de forma segura y se destruyen físicamente bajo la verificación de dos empleados.

Sección II: Adición de nuevos controles y revisiones de los controles de AWS asignados a los Criterios de los servicios de confianza

Se agregaron nuevos controles al alcance del informe SOC de AWS para ajustarse mejor con los puntos de atención asociados a los criterios SOC 2 del AICPA. Se revisó la asignación de los Controles de AWS con los Criterios de los servicios de confianza de AWS. Consulte la subsección “Controles de AWS asignados a los criterios de seguridad, disponibilidad, confidencialidad y privacidad” en la Sección III.

Controles nuevos	Asignado a los Criterios
AWSCA-12.8: a menos que se prohíba hacerlo o exista una indicación clara de conducta ilegal en relación con el uso de los productos o servicios de AWS, AWS hace un intento razonable de notificar a los clientes antes de divulgar el Contenido del cliente en respuesta a solicitudes válidas o vinculantes de la ley.	P6.7
AWSCA-12.9: AWS mantiene contratos con subprocesadores de terceros que incluyen protección de datos, compromisos de confidencialidad y requisitos de seguridad.	P6.1
AWSCA-12.10: se realiza una revisión formal de los subprocesadores de terceros antes de que AWS permita cualquier procesamiento por parte de los subprocesadores de terceros, con el fin de determinar que se implementaron las restricciones adecuadas para limitar el procesamiento del contenido del cliente por parte de los subprocesadores de terceros únicamente al contenido del cliente que es necesario para proporcionar o mantener los servicios de AWS seleccionados por el cliente.	P6.7
AWSCA-12.11: AWS realiza reevaluaciones anuales de los subprocesadores de terceros, o después de incidentes importantes o cambios significativos.	P6.1
AWSCA-12.12: el proceso de lanzamiento de nuevos subprocesadores de terceros requiere la adición a la lista publicada externamente de subprocesadores de terceros que actualmente están contratados por AWS para procesar los datos del cliente en función de la región de AWS y el servicio de AWS que el cliente seleccione.	P6.7

Sección III: Actualizaciones de los controles complementarios de las entidades usuarias

Se actualizaron los CUEC existentes y se agregaron nuevos CUEC para ajustarse mejor al alcance del informe, el entorno de control de la evolución y para ofrecer una orientación más clara a los clientes sobre sus responsabilidades. Consulte la subsección “Controles complementarios de las entidades usuarias” de la Sección III para obtener la lista más actualizada.

APÉNDICE: Glosario de términos

Apéndice: Glosario de términos

AMI: una imagen de máquina de Amazon (AMI) es una imagen de máquina cifrada almacenada en Amazon S3. Contiene toda la información necesaria para arrancar instancias del software de un cliente.

API: la interfaz de programación de aplicaciones (API) es una interfaz en informática que define las formas en que un programa de aplicación puede solicitar servicios de las bibliotecas o los sistemas operativos.

Autenticación: la autenticación es el proceso de determinar si alguien o algo es, de hecho, quien o lo que declara ser.

Zona de disponibilidad: las ubicaciones de Amazon EC2 se componen de regiones y zonas de disponibilidad. Las zonas de disponibilidad son ubicaciones distintas que están diseñadas para estar aisladas de los errores de otras zonas de disponibilidad y proporcionan una conectividad de red barata y de baja latencia a otras zonas de disponibilidad de la misma región.

Bucket: un contenedor de objetos almacenados en Amazon S3. Cada objeto está contenido en un bucket. Puede encontrar más información en https://docs.aws.amazon.com/AmazonS3/latest/dev/Introduction.html #BasicsBucket

Contenido de AWS: "Contenido de AWS" significa el Contenido que nosotros o cualquiera de nuestras filiales ponemos a disposición en relación con los Servicios o en el Sitio de AWS para permitir el acceso a los Servicios y su uso, incluidas las API; WSDL; Documentación; código de muestra; bibliotecas de software; herramientas de línea de comandos; techos de concepto; plantillas; y otra tecnología relacionada (incluida cualquiera de las anteriores que sean proporcionadas por nuestro personal). El Contenido de AWS no incluye los Servicios ni el Contenido de Terceros.

Contenido del cliente: definido como "Su contenido" en https://aws.amazon.com/agreement/

HMAC: en criptografía, un Código de autenticación de mensajes hash con clave (HMAC o KHMAC), es un tipo de código de autenticación de mensajes (MAC) calculado mediante un algoritmo específico que implica una función hash criptográfica en combinación con una clave secreta. Como cualquier MAC, puede utilizarse para verificar de forma simultánea la integridad de los datos y la autenticidad de un mensaje. Cualquier función hash criptográfica iterativa, como MD5 o Algoritmo hash seguro 1, puede utilizarse en el cálculo de un HMAC; el algoritmo MAC resultante se denomina HMAC-MD5 o HMAC-SHA1, según corresponda. La solidez criptográfica del HMAC depende de la solidez criptográfica de la función hash subyacente, del tamaño y la calidad de la clave y del tamaño de la longitud de salida del hash en bits.

Información personal: la información personal que AWS recopila en el curso de la prestación de las ofertas de AWS incluye:

- **Información que nos facilita:** recopilamos cualquier información que nos facilite en relación con las Ofertas de AWS. Haga clic aquí para ver ejemplos de la información que nos facilita.
- **Información automática:** recopilamos automáticamente determinados tipos de información cuando interactúa con las Ofertas de AWS. Haga clic aquí para ver ejemplos de la información que recopilamos automáticamente.
- **Información de otras fuentes:** podríamos recopilar información sobre usted de otras fuentes, incluidos proveedores de servicios, socios y fuentes disponibles públicamente. Haga clic aquí para ver ejemplos de la información que recopilamos de otras fuentes.

Hipervisor: un hipervisor, también llamado Virtual Machine Monitor (VMM), es un software de virtualización de computadoras/hardware que permite que se ejecuten múltiples sistemas operativos en una computadora anfitriona de forma simultánea.

Dirección IP: una dirección de Protocolo de Internet (IP) es una etiqueta numérica que se asigna a los dispositivos que participan en una red informática que utiliza el Protocolo de Internet para la comunicación entre sus nodos.

IP Spoofing: creación de paquetes del Protocolo de Internet (IP) con una dirección IP de origen falsificada, llamada spoofing, con el propósito de ocultar la identidad del remitente o suplantar la identidad de otro sistema informático.

Sumas de comprobación MD5: en criptografía, MD5 (Message-Digest algorithm 5) es una función hash criptográfica ampliamente utilizada con un valor hash de 128 bits. Como estándar de Internet (RFC 1321), MD5 se ha empleado en una amplia variedad de aplicaciones de seguridad y también se utiliza habitualmente para comprobar la integridad de los archivos.

Objeto: las entidades fundamentales almacenadas en Amazon S3. Los objetos constan de datos y metadatos. La parte de datos es opaca para Amazon S3. Los metadatos son un conjunto de pares nombre-valor que describen el objeto. Estos incluyen algunos metadatos por defecto, como la fecha de última modificación, y metadatos HTTP estándar, como Content-Type. El desarrollador también puede especificar metadatos personalizados al momento de almacenar el Objeto.

Escaneo de puertos: un escaneo de puertos es una serie de mensajes enviados por alguien que intenta entrar en una computadora para saber qué servicios de red informática, cada uno asociado a un número de puerto "conocido", proporciona la computadora.

Política de privacidad: "Política de privacidad" significa la política de privacidad ubicada en https://aws.amazon.com/privacy/ (y cualquier ubicación posterior o relacionada designada por nosotros), ya que puede ser actualizada por AWS de vez en cuando.

Entidad usuaria: las entidades que utilizan los servicios de una organización de servicios durante una parte o todo el período de revisión.

Servicio: software o capacidad informática que se proporciona a través de una red (por ejemplo, Amazon EC2, Amazon S3).

Organización de servicios: una organización o segmento de una organización que presta servicios a entidades usuarias que pueden ser relevantes para el control interno de dichas entidades usuarias sobre los informes financieros.

Versión 4 de la firma: la versión 4 de la firma es el proceso para añadir información de autenticación a las solicitudes de AWS. Por seguridad, la mayoría de las solicitudes a AWS deben ser firmadas con una clave de acceso, que consiste en un ID de clave de acceso y una clave de acceso secreta.

Organización de subservicio: una organización de servicios utilizada por otra organización de servicios para realizar algunos de los servicios prestados a las entidades usuarias que pueden ser relevantes para el control interno de dichas entidades usuarias sobre los informes financieros.

Instancia virtual: una vez lanzada una AMI, el sistema en ejecución resultante se denomina instancia virtual. Todas las instancias con base en la misma AMI empiezan siendo idénticas y cualquier información sobre ellas se pierde cuando las instancias se terminan o fallan.

X.509: en criptografía, X.509 es un estándar de UIT-T para una infraestructura de clave pública (PKI) para el inicio de sesión único (SSO) y la infraestructura de gestión de privilegios (PMI). X.509 especifica, entre otras cosas, formatos estándar para certificados de clave pública, listas de revocación de certificados, certificados de atributos y un algoritmo de validación de la ruta de certificación.