Consideraciones sobre el uso de productos de AWS en sistemas GxP

Enero de 2016

Avisos

Este documento se suministra únicamente con fines informativos. Representa la oferta de productos y las prácticas actuales de AWS a partir de la fecha de publicación de este documento. Los productos y prácticas pueden modificarse sin previo aviso. Los clientes son responsables de realizar sus propias evaluaciones independientes de la información contenida en este documento y de cualquier uso de los productos o servicios de AWS, cada uno de los cuales se ofrece "como es", sin garantía de ningún tipo, ya sea explícita o implícita. Este documento no genera ninguna garantía, representaciones, compromisos contractuales, condiciones ni garantías de AWS, sus filiales, proveedores ni licenciantes.
Las responsabilidades y obligaciones de AWS con respecto a sus clientes se controlan mediante los acuerdos de AWS, y este documento no forma parte ni modifica ningún acuerdo entre AWS y sus clientes.

Índice

1 RESUMEN

En 2006, Amazon Web Services (AWS) comenzó a proporcionar productos de infraestructura de TI a los clientes en forma de servicios web, más conocido hoy como "cloud computing". Actualmente, AWS ofrece una plataforma de infraestructura escalable de alta fiabilidad y de bajo costo que permite operar a cientos de miles de empresas en 190 países de todo el mundo. Algunos de los principales beneficios del cloud computing son la oportunidad de reemplazar los gastos de capital de infraestructura iniciales por costos variables de bajo importe que se amplían con el uso y permiten a los clientes dedicar más tiempo a sus actividades principales y menos a tareas de TI sin valor añadido.

Con la cloud, las organizaciones ya no necesitan planificar y aprovisionar dispositivos e infraestructura de TI con semanas o meses de antelación. Pueden poner en marcha al instante cientos o miles de máquinas virtuales con herramientas y métodos de implementación automatizados que proporcionan resultados más rápidamente y garantizan controles con mayor coherencia y menos errores manuales. Para aprovechar los beneficios de la adopción de productos de AWS, las organizaciones con requisitos de cumplimiento de "buenas prácticas de laboratorio, clínicas o de fabricación" (GxP) y sus auditores necesitarán adquirir nuevas habilidades y considerar cambiar sus políticas y procedimientos de GxP para permitir que el cumplimiento de los requisitos de TI sea más ágil, esté automatizado y se centre en la seguridad.

En este documento técnico se proporcionan directrices para usar los productos de AWS en el contexto de GxP. El contenido se ha desarrollado junto con clientes de dispositivos médicos y farmacéuticos de AWS, además de socios de software, que usan actualmente productos de AWS en sus sistemas GxP validados. Para garantizar la idoneidad del contenido, AWS se ha tomado la molestia de contratar a Lachman Consultant Services Inc. (Lachman Consultants) para que revise el enfoque descrito en este documento e incluya sus aportaciones. Lachman Consultants es una de las firmas de consultoría más prestigiosas en FDA y asuntos de cumplimiento de leyes internacionales que afectan al sector de dispositivos médicos y farmacéuticos en la actualidad. Lachman Consultants cuenta con una amplia experiencia trabajando con empresas en asuntos relacionados con el establecimiento y desarrollo de sistemas GxP, incluidas las directrices GxP para respaldar el mantenimiento de datos regulados en un entorno en la cloud. Para obtener información adicional sobre Lachman Consultants, visite www.lachmanconsultants.com.

No obstante, sigue siendo conveniente que los clientes de AWS consulten con sus propios asesores para garantizar que sus políticas y procedimientos GxP son adecuados para su sistema de TI, software y prácticas de seguridad actuales en los que se emplean productos de AWS.

2 INTRODUCCIÓN

Amazon Web Services (AWS) proporciona productos de software de infraestructura en la cloud que se usan cada vez más para almacenar y procesar cargas de trabajo confidenciales y reguladas en prácticamente todos los sectores industriales que existen en el mundo. Las organizaciones sanitarias y de ciencias de la salud son conocedoras de los beneficios de la cloud de AWS y están usando productos de AWS como componentes de sus sistemas de TI regulados, incluidos sistemas informatizados que respaldan las "Buenas prácticas de laboratorio, buenas prácticas clínicas y buenas prácticas de fabricación (“GxP”) para los dispositivos médicos, los productos farmacéuticos y otros sectores de productos alimentarios y médicos.

En este documento se proporciona información para ayudar a los clientes que desean usar los productos de AWS para crear sistemas informatizados que almacenen o procesen registros electrónicos teniendo en cuenta los requisitos comunes de cumplimiento de GxP e integridad de los datos.

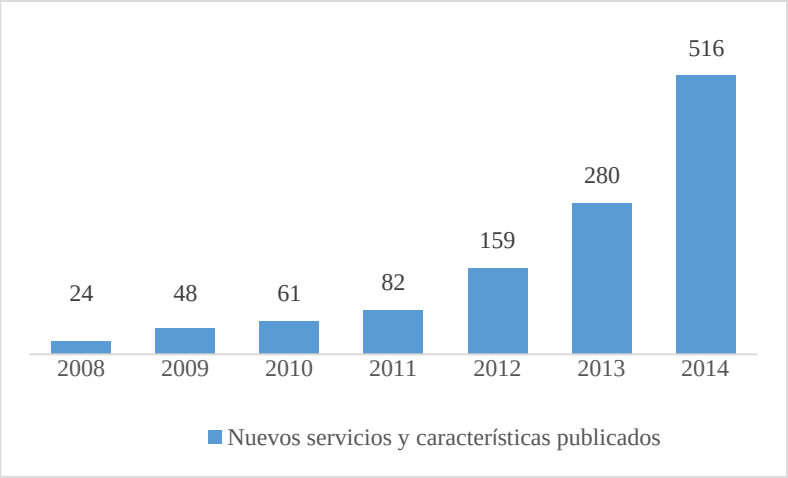
Este documento ayudará a los clientes a entender lo siguiente:

- El ámbito y la base tecnológica de los productos de AWS
- Las consideraciones del sistema de calidad que los clientes podrían tener en cuenta a la hora de usar productos comerciales de AWS en la cloud
- Las consideraciones sobre el ciclo de vida del desarrollo del sistema para los clientes que desarrollan, validan o utilizan sistemas GxP que incorporan productos de AWS como un componente
- Las consideraciones sobre los aspectos legales para los clientes que deben enviar o proporcionar información relativa al sistema a los organismos reguladores

En https://aws.amazon.com/compliance/ encontrará otros documentos técnicos con información más específica sobre los productos de AWS, la privacidad y la protección de los datos.

2.1.1 Acerca de AWS

Fundado en 2006 por Amazon.com (NYSE: AMZN), Amazon Web Services es un proveedor de servicios en la cloud consolidado que ofrece un catálogo de productos de infraestructura basados en suscripción y suministrados bajo petición a través de Internet desde centros de datos emplazados en EE. UU., Australia, Brasil, Alemania, Irlanda, Japón, Corea y Singapur. Desde su creación, AWS ha apostado por la innovación en su definición de la cloud computing como un medio de distribuir rápidamente nuevos productos a los clientes y después iterar y mejorar estos productos con gran rapidez en función de las aportaciones de los clientes. El ritmo de innovación y las mejoras continuas en el servicio son una de las principales razones por las que cada vez más organizaciones eligen usar los productos de AWS para sus sistemas críticos.



La obsesión por el cliente y la confianza de los clientes son los principios fundamentales que rigen la cultura del equipo de Amazon. Aunque los clientes conservan la propiedad y el control de sus datos y sistemas cuando usan productos de AWS, AWS trabaja sin descanso para proporcionar seguridad y transparencia a los clientes coordinando sus plataformas de privacidad y protección de datos actuales. Consulte el apéndice de privacidad de datos (página 33) para obtener más información.

- Información de AMZN Corp.: http://phx.corporate-ir.net/phoenix.zhtml?c=97664&p=irol-irhome
- Principios de dirección: http://www.amazon.jobs/principles
- Informes de los analistas: https://aws.amazon.com/resources/analyst-reports/

2.1.2 Clientes de AWS

AWS tiene más de un millón de clientes activos en más de 190 países que representan prácticamente a todos los sectores y tipos de organización, desde empresas de nueva creación de propiedad particular y pequeñas empresas a grandes corporaciones y organismos gubernamentales. En las organizaciones de nuestros clientes, los usuarios principales de los productos de AWS son desarrolladores de software, ingenieros de red y administradores de sistemas que crean y mantienen la infraestructura de TI y las aplicaciones de la organización. AWS tiene una amplia lista de casos de éxito de clientes que ponen de manifiesto la gran variedad de sectores y mercados que se benefician de nuestros productos en la cloud: https://aws.amazon.com/solutions/case-studies/all/.

Las organizaciones sanitarias y de ciencias de la salud figuran entre aquellas que usan productos de AWS en sus sistemas informatizados, y en el sitio web de AWS Health se incluyen algunos casos de estos clientes: https://aws.amazon.com/health/.

2.1.3 Tecnología de AWS

Amazon Web Services (AWS) debe su nombre a la tecnología básica integrada en todos los productos de AWS: los servicios web. Un servicio web es un módulo de software autónomo y reutilizable que pone su funcionalidad al servicio de otros módulos de software a través de protocolos de Internet que utilizan formatos de mensajes

estandarizados como XML[1] y JSON[2]. Los productos de AWS, disponibles online y a través de la consola de administración de autoservicio, https://aws.amazon.com/account/, se basan en dos tipos de servicios web, cada uno con varios tipos de interfaces:

Tipos de servicios web:

- Protocolo simple de acceso a objetos (SOAP)
- Transferencia de estado representacional (REST)

Interfaces de los productos de AWS:

- Interfaz de programación de aplicaciones (API)
- Interfaz de línea de comandos (CLI)
- Interfaz gráfica de usuario (GUI)

Los servicios web no están vinculados a ningún sistema operativo o lenguaje de programación, lo que significa que las aplicaciones escritas en diferentes lenguajes de programación y ejecutadas en diferentes plataformas pueden intercambiar fácilmente datos a través de Internet (o de una intranet) mediante las acciones predefinidas permitidas por la interfaz de cada servicio web. Una ventaja importante del enfoque de servicios web, denominado a veces "arquitectura orientada a la Web", es que las aplicaciones de software que usan servicios web no necesitan saber cómo se ha creado el servicio o cómo se almacenan los datos subyacentes; solo necesitan saber a qué acciones responderá la interfaz del servicio web. Siempre que las acciones estén disponibles en la interfaz, los cambios en los componentes subyacentes de un servicio web o la incorporación de nuevas acciones no afectarán al comportamiento ni a la fiabilidad de la aplicación. La lista de acciones de servicios web permitidas por los productos de AWS está totalmente documentada y disponible online: https://aws.amazon.com/documentation/.

Además de la tecnología de servicios web, las tecnologías de infraestructura definidas por software como la virtualización y las redes definidas por software (SDN) son fundamentales en los productos de AWS.
Los componentes de infraestructura que anteriormente solo estaban disponibles como equipo físico especializado, como es el caso de los balanceadores de carga de la red y los firewalls, ahora están disponibles como recursos definidos por software a petición, lo que reduce los plazos y los gastos de desarrollo del sistema y permite un grado mayor de estandarización y control de la infraestructura a través de la automatización del software.

La expansión del software para incluir componentes de la infraestructura anteriormente físicos, combinada con los beneficios de la arquitectura orientada a la Web y las metodologías de programación modernas, están generando una transición a escala global del SDLC de TI[3], las aptitudes del personal y el cumplimiento de las normativas de TI en todos los sectores. Las organizaciones que estén preparadas para aprovechar al máximo los productos de AWS en sus sistemas GxP serán las que reconozcan esta transición y se adapten a ella.

1 Lenguaje de marcado extensible
2 Notación de objetos JavaScript
3 Ciclo de vida de desarrollo del sistema

Ventajas de la tecnología de AWS:

- **Independencia e interoperabilidad de la plataforma:** los productos de AWS admiten aplicaciones escritas en muchos lenguajes de programación y no restringen las aplicaciones a determinados sistemas operativos o componentes de hardware.
- **Escalabilidad:** la combinación de infraestructura definida por software con productos de AWS con métodos de programación modernos permite a los clientes de AWS diseñar sus sistemas informatizados para ampliar o reducir rápidamente los recursos (y sus costos) en función de las demandas reales del sistema.
- **Tolerancia a errores:** los productos de AWS permiten un bajo acoplamiento entre ellos y las aplicaciones de software y, por tanto, los clientes pueden diseñar sus sistemas GxP para que sigan funcionando correctamente aunque un componente del sistema o producto de AWS deje de estar disponible temporalmente.
- **Separación de las tareas:** la separación de las responsabilidades de la infraestructura física de las responsabilidades del software y la infraestructura virtuales del cliente proporciona un control crítico de integridad de los datos al garantizar que aquellos usuarios con acceso físico estén totalmente aislados de los que tienen acceso lógico a los datos de GxP.
- **Auditabilidad:** la interoperabilidad basada en los mensajes de los servicios web permite que los clientes configuren y usen los productos de AWS de forma que se registren, monitoreen y auditen uniformemente.
- **Enfocada en las competencias básicas:** la ventaja definitiva de los productos de AWS reside en que nuestros clientes pueden dedicar menos tiempo a realizar tareas que no aportan valor añadido y más a sus atribuciones básicas que añaden valor a su organización.

2.1.4 Productos de AWS

AWS crea productos comerciales de software de infraestructura en la cloud y aplicaciones de ofimática que son configurables por el usuario y de propósito general por naturaleza, y que se distribuyen de acuerdo con los estándares de TI comerciales como ISO, NIST y SOC, entre otros. Son similares a otros productos y servicios de TI de propósito general, como motores de base de datos, sistemas operativos, lenguajes de programación, proveedores de Internet, etc. Muchas organizaciones clasifican los productos de AWS como productos comerciales de software de infraestructura de distribución general (COTS, por sus siglas en inglés), lo que concuerda con el uso de productos de AWS como artículos COTS por parte del gobierno federal de EE. UU. a través de un programa de compras federal denominado FedRAMP. Según FedRAMP, que recoge las definiciones de la Normativa Federal de Adquisiciones de EE. UU. (FAR, por sus siglas en inglés), los artículos COTS son 1) productos o servicios que se ofrecen o venden en grandes cantidades en los mercados comerciales a partir de un catálogo consolidado, 2) productos o servicios que se ofrecen sin modificación ni personalización y 3) productos y servicios que se ofrecen sujetos a términos y condiciones comerciales estándar. Los clientes de AWS con requisitos de GxP son responsables de clasificar los productos de AWS de acuerdo con las designaciones del sector pertinentes como Categoría 1, en virtud de las directrices de Buenas prácticas de la fabricación automatizada (GAMP) y el Programa de Cooperación de Inspección Farmacéutica (PIC/S) para los sistemas informatizados en entornos GxP regulados, o en virtud de las plataformas de calidad de dispositivos médicos, Software de procedencia desconocida (SOUP), componentes OTS de “caja negra” o recursos informáticos de propósito general.

AWS ofrece más de 50 productos pertenecientes a varios grupos:

Grupo	Productos de AWS
Computación	Amazon EC2, Amazon EC2 Container Service, AWS Elastic Beanstalk, AWS Lambda, Auto Scaling
Almacenamiento	Amazon S3, Amazon CloudFront, Amazon EBS, Amazon EFS, Amazon Glacier, AWS Storage Gateway, AWS Snowball
Base de datos	Amazon RDS, Amazon DynamoDB, Amazon ElastiCache, Amazon Redshift
Redes	Amazon VPC, AWS Direct Connect, Elastic Load Balancing, Amazon Route 53
Herramientas para desarrolladores	AWS CodeCommit, AWS CodePipeline, AWS CodeDeploy, herramientas y SDK de AWS
Herramientas de gestión	Amazon CloudWatch, AWS CloudFormation, AWS CloudTrail, AWS Config, AWS Management Console, AWS OpsWorks, AWS Service Catalog, Trusted Advisor, herramientas de AWS para Windows PowerShell
Seguridad e identidad	Identity & Access Management, AWS Directory Service, Amazon Inspector, AWS CloudHSM, AWS KMS, AWS WAF
Análisis	Amazon EMR, AWS Data Pipeline, Amazon Elastisearch Service, Amazon Kinesis, Amazon Kinesis Firehose, Amazon Machine Learning, Amazon QuickSight
Tecnología móvil e Internet de las cosas (IOT)	AWS IoT, AWS Mobile Hub, Amazon API Gateway, Amazon Cognito, AWS Device Farm, Amazon Mobile Analytics, AWS Mobile SDKs, Amazon SNS
Servicios de aplicaciones	Amazon API Gateway, Amazon AppStream, Amazon CloudSearch, Amazon Elastic Transcoder, Amazon FPS, Amazon SES, Amazon, SNS, Amazon SQS, Amazon SWF
Aplicaciones de productividad empresarial	Amazon WorkSpaces, Amazon WAM, Amazon WorkDocs, Amazon WorkMail

Los detalles y las especificaciones de los productos de AWS, de la infraestructura global y de la suscripción de los clientes están disponibles online:

- https://aws.amazon.com/account/
- https://aws.amazon.com/products/
- https://aws.amazon.com/documentation/
- https://aws.amazon.com/about-aws/global-infrastructure/

3 USO DE PRODUCTOS DE AWS EN SISTEMAS GXP

Aunque el modelo de distribución de los productos de AWS se basa en la entrega virtual online en lugar de productos locales físicos, las responsabilidades de usarlos como componentes en sistemas GxP son las mismas. En este modelo consolidado, los clientes que configuran y usan productos comerciales de infraestructura como componentes de sus sistemas GxP tienen responsabilidades en varias áreas clave:

- Sistemas de calidad
- Ciclo de vida de desarrollo del sistema
- Cuestiones legales

3.1 Sistemas de calidad

Las organizaciones que deseen usar productos de AWS en sistemas GxP deben revisar y actualizar la documentación de su sistema de calidad. En esta sección se proporcionan directrices sobre algunas de las áreas clave que deben considerar.

3.1.1 Responsabilidad de administración

Antes de usar productos de AWS en sistemas GxP en producción, los clientes deben considerar cómo van a administrar la creación y mantenimiento de sus cuentas de AWS. Como la creación de cuentas de AWS se basa en el autoservicio y a los creadores de las cuentas se les otorgan credenciales de la cuenta raíz con control pleno sobre la configuración de los productos de AWS y controles de acceso, los directivos con responsabilidad ejecutiva de la organización del cliente deben definir y comunicar una política de gobierno de las cuentas de AWS, con el fin de garantizar que se realiza un seguimiento de las cuentas usadas en sistemas GxP y que las credenciales de la cuenta raíz están controladas por personas cualificadas autorizadas por la organización. Asimismo, debe aplicarse una política de contraseñas a la cuenta de AWS que requiera que todos los usuarios con cuenta cambien sus contraseñas.

Los clientes deberían actualizar los siguientes documentos para respaldar el uso de productos de AWS en sistemas GxP:

- Política de gobierno de cuentas de AWS
- Memorando dirigido a todo el personal con la autoridad responsable de las compras de la organización
- Procedimiento de creación de cuentas de AWS
- Política de contraseñas de usuarios con cuentas de AWS

3.1.2 Personal

Los clientes de AWS son responsables de garantizar que su personal tiene los conocimientos, la capacitación y la experiencia necesarios para realizar las funciones asignadas. Cuando las funciones incluyen el uso de productos de AWS en sistemas GxP, debe tenerse en cuenta el grado de experiencia con productos de AWS a la hora de contratar o entrenar al personal. El nivel de acceso al sistema y las funciones realizadas son importantes para determinar el grado de experiencia necesario, y hay una serie de funciones que pueden resultar afectadas:

- Ingenieros de software
- Evaluadores de software
- Ingenieros de red
- Administradores del sistema
- Ingenieros de seguridad
- Ingenieros de validación
- Personal de compras
- Personal de control de calidad
- Auditores
- Nota: normalmente, los usuarios finales de la aplicación GxP no interactúan directamente con los productos de AWS y probablemente no necesitarán capacitación específica en AWS

La capacitación puede consistir en dar a conocer al producto, en capacitación *per se* o en calificación de los empleados a partir de una prueba. AWS y la red de socios de Amazon (APN) proporcionan capacitación inicial y continua y certificaciones con productos de AWS, incluidos los siguientes:

- Documentación online: https://aws.amazon.com/documentation/
- Vídeos educativos: https://aws.amazon.com/training/intro series/
- Laboratorios autoguiados: https://aws.amazon.com/training/self-paced-labs/
- Eventos y seminarios web: https://aws.amazon.com/about-aws/events/
- Clases y talleres: https://aws.amazon.com/training/course- descriptions/
- Capacitación dirigida por socios: https://aws.amazon.com/partners/training/
- Certificaciones profesionales: https://aws.amazon.com/certification/

Los clientes deberían actualizar los siguientes documentos para respaldar el uso de productos de AWS en sistemas GxP:

- Planes y procedimientos de capacitación
- Descripciones de tareas
- Solicitudes de empleo y currículos
- Registros de capacitación
- Certificaciones con productos de AWS

3.1.3 Auditorías

Es importante que los clientes que auditen su uso de productos de AWS en sistemas GxP evalúen la eficacia continuada de los controles de seguridad del sistema y la integridad de datos en el SDLC. Para realizar auditorías eficaces del uso de productos de AWS, los auditores de TI deben estar familiarizados con la tecnología de servicios básicos, los productos de AWS y las secuencias de comandos básicas como JSON.

Lo ideal sería que los auditores tuvieran acceso directo a los recursos de las cuentas de AWS pertinentes a través de políticas de acceso de solo lectura. En la cuenta de AWS, los auditores y asesores deberían revisar las configuraciones de las características de productos pertinentes y los datos de registro, como los siguientes:

- Credenciales de la cuenta de AWS
- Contactos de la organización
- Usuarios, grupos y funciones de IAM
- Proveedores de IAM para SAML y OpenID Connect
- Configuraciones de seguridad de Amazon EC2
- Políticas basadas en recursos en otros servicios como S3
- Reglas de configuración de AWS
- Logs de actividad del sistema en CloudTrail
- Historial de cambios en AWS Config
- Casos de soporte técnico del sistema

AWS ofrece un conjunto de herramientas de auditoría y recursos didácticos para ayudar a los auditores a preparar la auditoría del uso de productos de AWS en sistemas GxP:

- Documento técnico de auditoría de AWS: https://d0.awsstatic.com/whitepapers/compliance/AWS Auditing Security Checklist.pdf
- Documento técnico de listas de comprobación operativas para AWS https://s3.amazonaws.com/awsmedia/AWS_Operational_Checklists.pdf
- Directivas de auditoría de seguridad de AWS: https://docs.aws.amazon.com/general/latest/gr/aws-security-audit-guide.html
- Página del producto AWS CloudTrail: https://aws.amazon.com/cloudtrail/
- Página del producto AWS Config: https://aws.amazon.com/config/
- Página de AWS Trusted Advisor: https://aws.amazon.com/premiumsupport/trustedadvisor/
- qwikLAB de auditoría autoguiada: https://www.qwiklab.com/focuses/preview/1250?locale=en
- Capacitación de auditores presencial: awsauditttraining@amazon.com

Los clientes deberían actualizar los siguientes documentos para respaldar el uso de productos de AWS en sistemas GxP:

- Programación de auditoría de TI
- Procedimientos y listas de comprobación de cuentas de AWS
- Informes de auditoría de cuentas de AWS
- Calificaciones, currículo y registros de capacitación de los auditores de TI para productos de AWS

3.1.4 Control de compras

La compra de productos de infraestructura de TI consistía anteriormente en un proceso de pedido de compra (PO) de productos físicos contabilizados como gasto de capital. Con los productos de AWS, sin embargo, la compra requiere un proceso de facturación medida similar al de los servicios públicos para productos de software por suscripción que se contabilizan como un gasto de explotación variable. Muchas organizaciones de ciencias de la salud tienen procedimientos de compra de productos de TI para sistemas GxP creados para un proceso de pedido de compra que posiblemente no se correspondan con la compra de un modelo de precios de productos por suscripción de pago por uso como AWS.

Compra de infraestructura mediante el pedido de compra tradicional

1. TI especifica los requisitos del servidor
2. TI abastece el servidor y el sistema operativo correspondientes
3. TI envía una solicitud al departamento de compras
4. El departamento de compras envía el pedido de compra al proveedor
5. El proveedor envía el servidor
6. El departamento de materiales recibe el envío
7. TI instala el servidor y el sistema operativo
8. TI configura el sistema operativo
9. TI califica manualmente el servidor y el sistema operativo
10. El departamento de cuentas paga y amortiza el recurso de hardware como gasto de capital (CapEx)

Proceso de compra de infraestructura mediante AWS

1. TI especifica los requisitos del servidor
2. TI selecciona el tipo de instancia EC2 correspondiente y su propia imagen del sistema operativo calificada
3. TI lanza la instancia EC2 con la imagen calificada y el registro automático activado
4. TI paga el uso medido de la instancia EC2 mediante una tarjeta de crédito de gastos de explotación (OpEx)

Los clientes que usen productos de AWS en sistemas GxP deben revisar sus procedimientos de compra de TI para garantizar que pueden acomodar gastos de suscripción y un modelo de distribución online. En esta revisión deben participar los equipos de TI, compras y control de calidad de la organización, y debe incluir la creación de pedidos, la recepción y los pagos, así como la administración de cuentas de AWS. AWS proporciona documentación para ayudar a las organizaciones a entender y administrar la facturación de las cuentas de AWS.

- Documento técnico sobre facturación de administración de costos de AWS: https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/awsaccountbilling-aboutv2.pdf
- Identificación del uso con informes detallados de facturación: https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/detailed-billing-reports.html
- Calculadora sencilla de facturación mensual de AWS http://calculator.s3.amazonaws.com/index.html

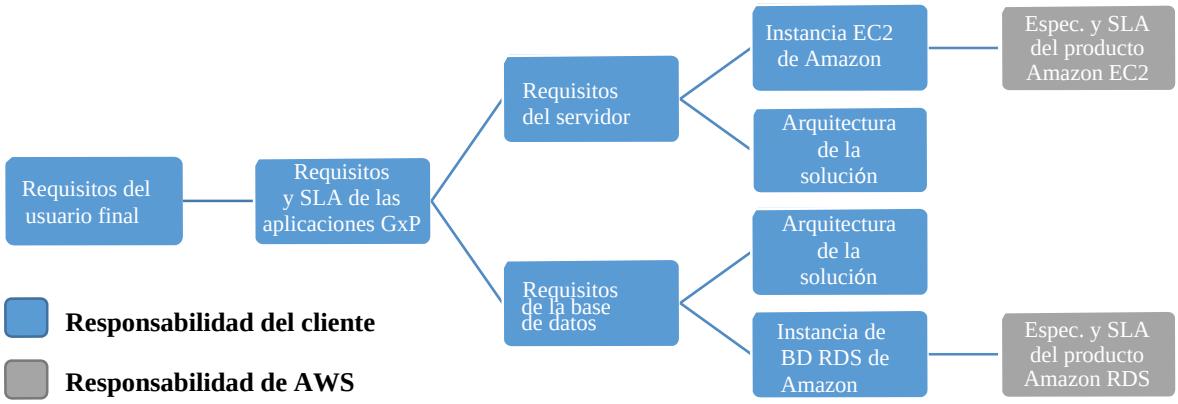
- Los clientes deberían actualizar los siguientes documentos para respaldar el uso de productos de AWS:

Los clientes deberían actualizar los siguientes documentos para respaldar el uso de productos de AWS en sistemas GxP:

- Procedimientos de compra
- Informes detallados de facturación de AWS
- Factura en PDF por correo electrónico

3.1.5 Evaluación del producto

Garantizar que los productos y servicios comprados satisfacen los requisitos especificados es un requisito clave de los controles de GxP. En el caso de los componentes de infraestructura comercialmente disponibles como los productos de AWS, es muy sencillo garantizar que las especificaciones del producto satisfacen los requisitos de los usuarios, porque las especificaciones de la interfaz y los contratos de los productos de AWS están ampliamente documentados y disponibles para su revisión por parte del cliente. Como AWS no personaliza los productos de AWS ni los SLA para los distintos clientes, estos pueden simplemente aplicar los requisitos de sus aplicaciones GxP a las especificaciones y SLA de productos de AWS correspondientes. Por ejemplo, un cliente que desee ejecutar una aplicación de software COTS configurable mediante los productos Amazon EC2 y Amazon RDS de AWS debería primero documentar los requisitos del servidor de la aplicación (CPU, memoria, etc.) y los requisitos de la base de datos, y visitar después las páginas de los productos Amazon EC2 y Amazon RDS para identificar la familia de servidores virtuales (por ejemplo, el tipo de instancia EC2) y el tipo de base de datos (por ejemplo, el tipo de instancia de base de datos) que satisfagan los requisitos de la aplicación.



Es importante tener en cuenta que el SLA del sistema GxP no es una función directa de los SLA del producto de AWS; por el contrario, el SLA del sistema GxP es una función de la configuración y uso de los productos de AWS por parte del cliente (es decir, la arquitectura de su solución). Por ejemplo, si una aplicación GxP necesita tener un mayor nivel de disponibilidad que el que proporciona el producto de AWS en concreto, el cliente puede diseñar su solución para conseguir ese mayor nivel de disponibilidad. Por tanto, al evaluar la idoneidad de los productos de AWS para un sistema GxP en particular, debe tenerse en cuenta la arquitectura total de la solución.

Para la evaluación de productos de AWS para aplicaciones personalizadas (categoría 5 de GAMP) o dispositivos médicos, será necesario que los clientes del sistema GxP analicen al mismo tiempo el contexto del sistema, las posibles arquitecturas y diseños y los productos de AWS disponibles durante la fase de planificación de su SDLC. Para ayudar a los clientes existentes y potenciales a determinar si los productos de AWS satisfacen los requisitos de su aplicación, AWS publica documentación técnica del producto online y proporciona a los clientes la capacidad de probar los productos de AWS antes de aprobar el diseño de su sistema GxP.

- Documentación de productos de AWS: https://aws.amazon.com/documentation/

Los clientes deberían actualizar los siguientes documentos para respaldar el uso de productos de AWS en sistemas GxP:

- Procedimientos de SDLC
- Requisitos y evaluación del riesgo de los sistemas GxP
- Arquitectura de la solución de los sistemas GxP
- Evaluación de los productos de AWS

3.1.6 Evaluación de los proveedores

Las organizaciones con requisitos de GxP necesitan evaluar y seleccionar a sus posibles proveedores, contratistas y consultores en función de su capacidad de satisfacer los requisitos especificados. Una vez que el cliente haya realizado la evaluación de un producto y haya determinado que los productos de AWS pueden satisfacer los requisitos de la arquitectura del sistema GxP, puede realizarse una evaluación del proveedor para determinar que AWS es capaz de distribuir sin problemas los productos de AWS de acuerdo con las especificaciones de la interfaz y los SLA publicados.

AWS utiliza una plataforma de control de la administración líder del sector que satisface los estándares actuales de calidad, seguridad y confianza de las organizaciones de TI comerciales.
Periódicamente, auditores cualificados independientes realizan evaluaciones de cumplimiento de los controles de AWS, y los informes de cumplimiento de estas evaluaciones se ponen a disposición de los clientes para que evalúen a AWS como proveedor. Los informes de cumplimiento de AWS identifican el ámbito de los productos de AWS y las regiones evaluadas, así como la certificación de conformidad del asesor.

Controles	**Criterios de evaluación**	**Auditor**	**Informe de cumplimiento**
ISO 27001	ISO/IEC 17021 y 27006	EY CertifyPoint	https://aws.amazon.com/compliance/iso-27001-faqs/
ISO 27017	ISO/IEC 17021 y 27006	EY CertifyPoint	https://aws.amazon.com/compliance/iso-27017-faqs/
ISO 9001	ISO/IEC 17021	EY CertifyPoint	https://aws.amazon.com/compliance/iso-9001-faqs/
SOC 1 SOC 2	AT 801 y	EY	https://aws.amazon.com/compliance/soc-faqs/

Controles	Criterios de evaluación	Auditor	Informe de cumplimiento
SOC 3	AT 101 Controls, TSP Sec. 100 Trust & Attestation		
FedRAMP/ N IST 800-53r4	NIST 800-53a	Veris Group	https://www.fedramp.gov/marketplace/co mpliant-systems/amazon-web-services-aws-eastwest-us-public-cloud/
PCI-DSS v3.1 Nivel 1	Procedimiento de auditoría de seguridad PCI DSS	Coalfire	https://aws.amazon.com/compliance/pci-dss-level-1-faqs/

Disponemos de recursos online adicionales para que los clientes conozcan los procesos de seguridad de AWS y el historial de desempeño presente y pasado de los productos de AWS:

- Documento técnico de riesgos y cumplimiento de AWS, apéndice A: cuestionario de CSA https://d0.awsstatic.com/whitepapers/compliance/AWS_Risk_and_Compliance_Whitepaper.pdf
- Documento técnico de descripción general de los procesos de seguridad de AWS https://d0.awsstatic.com/whitepapers/aws-security-whitepaper.pdf
- Panel de estado del servicio de AWS e historial de estado http://status.aws.amazon.com/

Los clientes GxP deberían actualizar sus procedimientos de evaluación de proveedores para garantizar que todos los tipos de proveedores pueden acomodar productos de AWS. Para los clientes de GxP que tengan una experiencia previa con productos de AWS en sistemas que no son GxP, la evaluación de los proveedores de GxP de AWS debería incluir también un examen del historial de desempeño de esos sistemas, incluidos todos los problemas relacionados con el sistema atribuibles a AWS *y* que el cliente no pudo resolver a través de la arquitectura de su solución.

Los clientes deberían actualizar los siguientes documentos para respaldar el uso de productos de AWS en sistemas GxP:

- Procedimiento de clasificación y evaluación de proveedores GxP
- Examen del desempeño de sistemas que no son GxP
- Datos de evaluación de proveedores de AWS, incluidos cuestionarios de los proveedores
- Informe de aprobación de proveedores de AWS
- Informes y documentos técnicos de cumplimiento de AWS
- Consulte también los contratos con proveedores (página 17)

3.1.7 Contrato con proveedores

Los contratos con proveedores de TI son importantes para las organizaciones con sistemas GxP. Estos contratos deben incluir declaraciones claras y documentadas de las responsabilidades compartidas y los compromisos del proveedor de TI de notificar a la organización los cambios importantes en el producto del proveedor.
Como los productos de AWS están estandarizados y son idénticos para todos los clientes, los contratos de los productos de AWS también están estandarizados e incluyen definiciones de las obligaciones de AWS y del cliente, así como mecanismos de notificación de los cambios realizados en dichos productos.

Los contratos de AWS se indican a continuación, y el apéndice (página 37) incluye una tabla de algunas de las responsabilidades relacionadas con GxP encontradas en estos contratos de AWS.

- Contrato del cliente https://aws.amazon.com/agreement/
- Contrato empresarial póngase en contacto con el departamento de ventas de AWS
- Anexo de seguridad póngase en contacto con el departamento de ventas de AWS
- Servicio de atención al cliente https://aws.amazon.com/premiumsupport/
- Condiciones del servicio https://aws.amazon.com/service-terms/
- Política de uso aceptable https://aws.amazon.com/aup/
- Acuerdos de nivel de servicios (SLA) específicos del producto:

Amazon S3	https://aws.amazon.com/s3/sla/
Amazon EC2 y EBS	https://aws.amazon.com/ec2/sla/
Amazon RDS	https://aws.amazon.com/rds/sla/
Route53	https://aws.amazon.com/route53/sla/
CloudFront	https://aws.amazon.com/cloudfront/sla/

- Anexo de procesamiento de datos
  https://aws.amazon.com/compliance/eu-data-protection/

Los clientes que usen productos de AWS en GxP deberán prestar especial atención al nivel de soporte técnico que necesitan de AWS. Hay cuatro niveles de soporte técnico de AWS, Basic, Developer, Business y Enterprise, cada uno con un nivel diferente de clasificación de gravedad de los casos y tiempos de respuesta. En función del caso concreto de soporte técnico del cliente, como solucionar un problema relacionado con el sistema identificado a través de una inspección reglamentaria justificada (véase la página 30), el nivel de soporte técnico de AWS determinará los tiempos de respuesta de la solicitud del cliente. Muchos de los clientes de sistemas GxP actuales de AWS mantienen un soporte de nivel Business o Enterprise para dar cuenta de estos escenarios.

Los clientes deben revisar y, si es necesario, actualizar sus políticas de contratación de proveedores de TI para garantizar que son compatibles con el modelo de funcionamiento y contratación estandarizados de AWS. Esto es especialmente necesario para las organizaciones que hayan contratado previamente proveedores de servicios administrados, servicios GxP especializados o proveedores de co-location que personalicen sus servicios y realicen actividades de desarrollo, validación y mantenimiento de la aplicación en nombre de su cliente.

Los clientes deberían actualizar los siguientes documentos para respaldar el uso de productos de AWS en sistemas GxP:

- Política de contratación de proveedores de TI
- Contratos aplicables indicados arriba

3.1.8 Registros y logs

Para cada sistema GxP, las organizaciones de ciencias de la salud deben identificar los registros que se deben conservar y los logs necesarios como prueba de GxP, y mantener la integridad y disponibilidad de los registros durante el período de retención. Cuando se usan productos de AWS en sistemas GxP, los registros que deben conservarse son principalmente los datos del cliente en el sistema GxP, el código de software y los registros de SDLC del sistema GxP, y los logs y pistas de auditoría generados por el sistema disponibles en la cuenta de AWS del cliente. Debido a los elevados niveles de automatización posibles con los productos de AWS y a las metodologías de SDLC modernas, muchos de estos registros que anteriormente se creaban por medio de procesos manuales, como protocolos de instalación impresos, ahora se generan a través de comandos ejecutados mediante programación. Esta forma más fiable de generar registros reduce la variabilidad y mejora manifiestamente la integridad de los datos, tanto desde el punto de vista de los datos de GxP como desde la perspectiva del SDLC.

Como los tipos de registros y formatos asociados con los procesos de TI automatizados son bastante diferentes de los registros generados manualmente, los clientes de sistemas GxP deben asegurarse de identificar los tipos de registros y formatos que necesitan conservar y desarrollar sus directrices de mantenimiento de registros correctamente. Los productos de AWS usados en aplicaciones y dispositivos médicos GxP también deben evaluarse para identificar el impacto del mantenimiento de registros en el archivo de historial de diseño (DHF) y en el registro maestro de dispositivos (DMR). En muchos casos, los registros que se generan automáticamente mediante programación por medio de los productos de AWS, como pistas de auditoría y alarmas, se pueden transferir en su totalidad y mantener en la cuenta de AWS del cliente o transferirse a otra ubicación.

Los clientes deberían actualizar los siguientes documentos para respaldar el uso de productos de AWS en sistemas GxP:

- Calendario de retención de registros
- Directrices de tipo y formato de registros
- Procedimientos de mantenimiento de registros
- Logs de CloudTrail
- Alarmas de CloudWatch
- Políticas de retención y reglas de ciclo de vida de S3 y Glacier
- Casos de soporte técnico de AWS

3.2 Ciclo de vida de desarrollo del sistema

Además de evaluar los requisitos del sistema de la organización, cada sistema GxP debe tener determinadas características y un proceso de SDLC controlado para su distribución. Las características y los controles de SDLC específicos que se aplican a cada sistema dependen de una serie de factores y se basan en normativas como 21 CFR Partes 11 y 820 en Estados Unidos, Anexo 11 y 93/42/EEC en la Unión Europea y sus equivalentes internacionales. El propósito general de estos marcos reglamentarios es garantizar que el sistema GxP cumple la función prevista y que los datos son exactos y fiables, ya que podrían usarse para la prestación de servicios médicos o para tomar decisiones sobre la seguridad y eficacia de productos medicinales, como alimentos, medicinas y dispositivos médicos para seres humanos, así como alimentos y medicinas para animales.

Controles de SDLC para sistemas GxP:

- Controlar el diseño y desarrollo para garantizar que se satisfacen los requisitos especificados
- Validar las aplicaciones de software y evaluar la infraestructura para garantizar su exactitud, fiabilidad y desempeño previsto continuado
- Control de cambios e historial de cambios de los sistemas que operan en un entorno de producción, incluida la documentación de los usuarios del sistema
- Monitorear el sistema en el entorno de producción para detectar y responder a la falta de conformidad (por ejemplo, errores)
- Documentar y procesar las reclamaciones relacionadas con el sistema y los casos de soporte técnico de los usuarios
- Conservación de los registros de SDLC y los datos de GxP durante todo el ciclo de vida del sistema, incluida la obsolescencia

Características necesarias en sistemas GxP:

- Capacidad de generar copias exactas y completas de datos de GxP en formatos legibles para los humanos y para las máquinas
- Validación de la entrada de datos y comprobaciones de la integridad de los datos
- Controles de acceso de los usuarios y comprobaciones de autorización de las acciones de los usuarios
- Pistas de auditoría seguras, generadas por el equipo y con marca de tiempo de las acciones de los usuarios y los cambios en los datos
- Comprobaciones que impongan la secuenciación permitida de los pasos (es decir, aplicación del flujo de trabajo)
- Cifrado de los datos en tránsito y en reposo
- Manifiestos de firmas electrónicas de las acciones en los datos autorizadas para los usuarios

Satisfacer estos requisitos con el modelo de infraestructura de TI tradicional es complicado porque el SDLC de las aplicaciones basadas en software y el SDLC de la infraestructura basada en hardware son bastante diferentes, y la naturaleza de los componentes de infraestructura física creados por los distintos fabricantes requiere una serie de controles de procedimiento manuales para garantizar que las configuraciones se mantienen y que se puede realizar un seguimiento de los cambios en toda la infraestructura. Con los productos de AWS, las empresas reemplazan su infraestructura física por un conjunto armonizado de productos de infraestructura virtualizados, que les permite crear y administrar toda la infraestructura como código de software. Los clientes no solo pueden usar productos de AWS como Amazon EC2 para lanzar servidores virtuales idénticos a partir de imágenes con control de versiones; toda la infraestructura, incluido el almacenamiento, la base de datos y la red, se puede desarrollar, realizar un control de sus versiones e implementar mediante plantillas de configuración basadas en software. Este enfoque de infraestructura como código ofrece un nivel sin precedentes de control, uniformidad y automatización durante el SDLC de todo el sistema, incluida la aplicación y la infraestructura. También implica que la sincronización de entornos de desarrollo, pruebas y producción requiere mucho menos esfuerzo que los modelos tradicionales de TI.

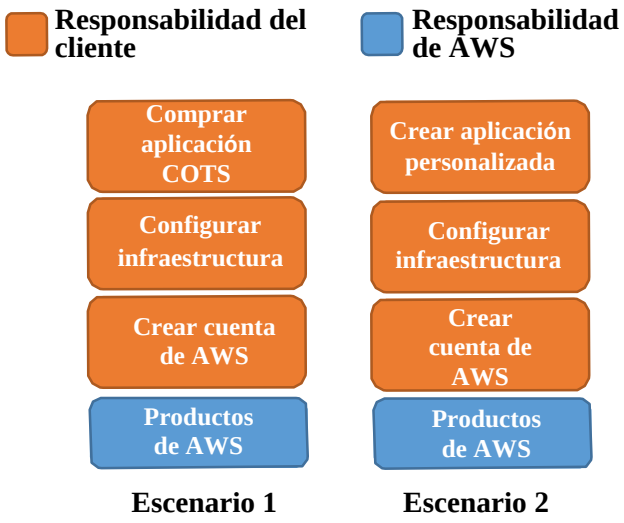
Aunque los productos de AWS suelen estar asociados a metodologías de SDLC como DevOps, los SDLC como Waterfall y el modelo V también se admiten en su totalidad. En esta sección se usará un ejemplo de SDLC general de tres fases para explicar algunas de las consideraciones para los clientes que usan productos de AWS en sistemas GxP.

3.2.1 Desarrollar

Los sistemas GxP deben desarrollarse siguiendo procedimientos documentados que garanticen que los sistemas satisfacen los requisitos especificados. Los clientes que usen productos de AWS en sistemas GxP son responsables de todas las actividades de desarrollo del sistema GxP, incluida la planificación, codificación, creación, configuración, comprobación, validación e implementación de las aplicaciones, así como el diseño, aprovisionamiento, configuración, organización, implementación, calificación y funcionamiento de la infraestructura definida por software. AWS no diseña ni desarrolla sistemas GxP en nombre de los clientes, pero los productos de AWS cuentan con extensa documentación para los usuarios y documentos técnicos que los ingenieros del sistema GxP pueden usar como referencia para el diseño del sistema y las actividades de desarrollo.

Los requisitos de especificación del diseño de sistemas GxP deben incluir también requisitos de ciberseguridad, y AWS recomienda que los clientes desarrollen un plan de seguridad del sistema GxP que siga un estándar de planificación de la seguridad reconocido como NIST Special Publication 800- 13 y cualquier documento de directrices normativas como Content of Premarket Submissions for Management of Cybersecurity in Medical Devices de la FDA.

Aunque los clientes pueden crear muchos tipos de sistemas con los productos de AWS, hay dos escenarios de desarrollo básicos: 1) comprar una aplicación COTS o 2) crear una aplicación personalizada.



Al evaluar los paquetes de software COTS para su uso con productos de AWS, los clientes de sistemas GxP deben incluir en su evaluación a los socios tecnológicos de la red de socios de AWS (APN) y AWS Marketplace. Los socios tecnológicos de AWS ofrecen soluciones de software que están alojadas o integradas en plataforma de AWS, y AWS Marketplace es una tienda online donde los clientes pueden comprar e implementar software compatible con AWS directamente en su cuenta de AWS.

- Socios tecnológicos de APN https://aws.amazon.com/partners/technology/
- AWS Marketplace https://aws.amazon.com/marketplace/

Los productos de AWS se pueden usar también con aplicaciones de software comerciales ajenas a la red de APN o a AWS Marketplace, pero los clientes tendrán que examinar los contratos de licencia de la aplicación y realizar una evaluación del producto (véase la página 15 anterior) para determinar la compatibilidad de la aplicación con los productos de AWS. Para esta actividad también se puede contar con los socios de consultoría de APN: https://aws.amazon.com/partners/consulting/.

Aunque las organizaciones de ciencias de la salud suelen preferir comprar las aplicaciones de software en lugar de crearlas, uno de los beneficios importantes de combinar productos de AWS con tecnologías de SDLC modernas es la capacidad de distribuir soluciones de software personalizadas de manera rápida, repetida y fiable. Muchas de las razones por las que las organizaciones han rehusado crear su propio software en el pasado, como la creación manual de paquetes de software a partir de código fuente o la realización manual de pruebas de regresión, han desaparecido ahora que las herramientas totalmente automatizadas han reducido o eliminado los retrasos y los errores causados por las actividades manuales de desarrollo.
Los productos de AWS como AWS OpsWorks, AWS CodeCommit y AWS CodePipeline proporcionan a los ingenieros de sistemas herramientas flexibles y configurables que les ayudan a satisfacer los requisitos específicos de su organización y, al mismo tiempo, simplifican los controles de SDLC de sus actividades de desarrollo de software.

Una vez que el cliente haya desarrollado y esté listo para implementar su sistema GxP en un entorno de validación, producción o de otro tipo, los productos de AWS como Amazon Machine Images (AMI), AWS CloudFormation, AWS CodeDeploy y AWS Elastic Beanstalk permiten realizar una implementación coherente y controlada de forma sencilla y repetible. Estas herramientas permiten también crear copias con control de versiones de todo el entorno del sistema, desde la pila de red, la base de datos y los volúmenes de almacenamiento hasta las instancias de computación. Estas copias con control de versiones se pueden conservar para el archivado y la administración de cambios o para aprovisionar entornos de desarrollo y pruebas para el desarrollo continuo o la solución de problemas.

Este nuevo modelo de implementación continua es una de las razones por las que muchos clientes de muchos sectores usan productos de AWS para la innovación en su empresa. Para aprovechar estos beneficios en sus sistemas GxP, puede ser conveniente que los clientes revisen y actualicen sus metodologías y procedimientos de desarrollo.

Los clientes deberían actualizar la siguiente documentación para respaldar el uso de productos de AWS en sistemas GxP:

- Procedimiento de SDLC
- Diseño del sistema y plan de desarrollo
- Procedimiento de evaluación de riesgos
- Procedimiento operativo estándar de inspección del código
- Casos de uso y casos de usuarios u otras especificaciones de requisitos
- Criterios de SLA del usuario final, incluido soporte técnico para el usuario final
- Especificaciones de arquitectura de software
- Requisitos funcionales de la aplicación
- Análisis de riesgos preliminares para las aplicaciones médicas o móviles de GxP
- Logs de AWS CloudTrail y Config
- Código fuente de la aplicación
- AMI de EC2 y plantillas de CloudFormation
- Procedimiento operativo estándar de implementación de código

3.2.2 Validar

Las aplicaciones GxP deben validarse para garantizar que las especificaciones de software satisfacen los requisitos de los usuarios y la infraestructura de software en la que se ejecuta la aplicación debe evaluarse para garantizar que satisface los requisitos del sistema de la aplicación. Como los productos de AWS se proporcionan en su totalidad como productos de autoservicio, los clientes que usen productos de AWS en sistemas GxP son responsables de todas las actividades de validación del software y evaluación de la infraestructura dentro de su cuenta de AWS. Puesto que AWS no desarrolla ni administra aplicaciones en nombre de los clientes, ni tampoco aprovisiona o configura la infraestructura específica de los clientes, AWS no puede realizar actividades de validación o evaluación de GxP en nombre de los clientes. AWS es responsable de garantizar que los productos de AWS cumplen las especificaciones del producto, los SLA y los estándares de TI comerciales, y los clientes del sistema GxP son responsables de validar el sistema que crean con productos de AWS.

La instalación, creación de instancias e implementación de aplicaciones e infraestructura son sustancialmente diferentes con los productos de AWS que con la infraestructura física y los medios de instalación tradicionales. En la época del hardware de infraestructura físico, las actividades de instalación se realizaban sobre todo manualmente siguiendo un protocolo. Normalmente, se desarrollaban y aprobaban protocolos para cada componente del sistema, que después ejecutaba un operador con la supervisión de un verificador para garantizar que cada paso se había realizado correctamente.
Una vez completado, el protocolo debía ser revisado y aprobado por un representante de control de calidad. Conforme se desarrollaron los SDLC de TI y se popularizó el uso de la virtualización de servidores, las actividades de validación dejaron de basarse en los protocolos para controlarse mediante procedimientos, si bien estas actividades seguían siendo prácticamente manuales. Algunas organizaciones creaban una "imagen maestra" validada mediante un protocolo que usaban después para crear un servidor virtual siguiendo un procedimiento.

En la era de la cloud donde la infraestructura se define por software, los ingenieros de sistemas GxP tienen la capacidad de controlar las versiones de toda la pila del sistema y automatizar la implementación mediante plantillas de infraestructura con control de versiones. Una de las prácticas habituales entre los clientes de AWS es crear plantillas del sistema validadas y usarlas en combinación con herramientas de implementación automatizadas para aprovisionar los distintos recursos y todos los entornos de desarrollo, pruebas y validación. La tecnología de API de servicios web incorporada en todos los productos de AWS permite también que se utilicen herramientas de verificación de API de terceros como RunScope y SoapUI como un medio de validar el comportamiento previsto del sistema en muchos más casos de lo que antes era posible con la validación manual periódica.

Debido a este cambio de paradigma de actividades manuales puntuales a actividades automáticas continuas, las prácticas de control y validación de cambios de GxP que muchas organizaciones de ciencias de la salud siguen para su infraestructura de hardware tradicional debe ser revisadas y actualizadas para abordar el modelo de infraestructura automatizada cuando usen productos comerciales de la cloud de AWS como componentes de sistemas GxP.

Los clientes deberían actualizar la siguiente documentación para respaldar el uso de productos de AWS en sistemas GxP:

- Procedimiento de SDLC
- Procedimiento de validación
- Procedimiento de validación de TI
- Procedimiento de implementación automatizada
- Logs de AWS CloudTrail y Config
- Código fuente de la aplicación
- AMI de EC2 y plantillas de CloudFormation

3.2.3 Operar

Desarrollar, dirigir, controlar y monitorear sistemas GxP en operaciones de producción es importante para garantizar que siguen cumpliendo las especificaciones. Cuando se producen problemas o desviaciones del sistema, las organizaciones con sistemas GxP también deben mantener un proceso para responder, corregir y evitar esos problemas. Aunque se pueden usar productos de AWS para estas actividades, AWS no realiza operaciones ni actividades de monitorización de sistemas GxP en nombre de los clientes.

Principio del sistema GxP	Resumen del requisito	Consideraciones
Control de cambios	Los cambios en los sistemas GxP en producción deben verificarse o validarse para garantizar que el sistema satisface los requisitos definidos por el usuario.	Cliente: es el cliente quien define los requisitos de los usuarios del sistema y configura y valida los productos de AWS para satisfacer estos requisitos. Los clientes son responsables de verificar y validar los cambios que implementen en los requisitos del usuario y las configuraciones del producto. AWS: AWS no tiene control sobre los requisitos del cliente ni las configuraciones del producto. Por tanto, AWS no puede verificar ni validar los cambios en el sistema GxP en nombre de los clientes. AWS no verifica los cambios en los productos de AWS para garantizar que se satisfacen las especificaciones y los SLA del producto

Principio del sistema GxP	Resumen del requisito	Consideraciones
Acuerdo de nivel de servicios	Deben existir contratos formales entre los usuarios del sistema GxP y las otras partes, incluidos los departamentos de TI, que mantienen el sistema GxP.	Cliente: el cliente define el acuerdo de nivel de servicios del sistema GxP y debe configurar y usar los productos de AWS para cumplir el SLA. AWS: los SLA de los productos de AWS son diferentes de los SLA del sistema GxP, y AWS no tiene control ni visibilidad sobre los SLA que el cliente establece para el sistema. Consulte el apéndice 4.3: Responsabilidades compartidas en los contratos de AWS
Soporte técnico para el usuario final	Los propietarios de sistemas GxP deben establecer procedimientos para proporcionar soporte técnico a los usuarios finales.	Cliente: los clientes son responsables de proporcionar soporte técnico a los usuarios finales del sistema GxP. AWS: AWS no proporciona soporte técnico ni servicios a los usuarios finales del sistema GxP.
Backup y recuperación	Deben realizarse backups periódicos de los datos de GxP y debe incluirse la verificación de la integridad y capacidad de recuperación de los datos.	Cliente: el cliente es responsable de configurar y usar los productos de AWS para mantener un nivel de seguridad, protección y backup adecuado de los datos. AWS: AWS no tiene control alguno sobre la configuración del cliente de los productos ni visibilidad sobre el contenido del cliente (es decir, los datos). Por consiguiente, AWS no realiza backups del contenido en nombre de los clientes.
Respuesta a incidentes	Los incidentes del sistema GxP deben registrarse, evaluarse y documentarse.	Cliente: el cliente es responsable de recibir los informes de incidentes de los usuarios finales y administradores del sistema, y de acceder a estos informes y documentarlos. Si un incidente requiere soporte técnico de AWS, el cliente puede tramitar un caso de soporte técnico mediante un método acorde con su contrato de soporte técnico.

Principio del sistema GxP	Resumen del requisito	Consideraciones
		AWS: AWS no tiene visibilidad sobre los incidentes del sistema GxP, pero los casos de soporte técnico del cliente enviados a AWS relativos a un problema con los productos de AWS se evaluarán e investigarán de acuerdo con el contrato de nivel de soporte técnico del cliente. Los casos de soporte técnico de los clientes están documentados y disponibles para los clientes online.
Acciones correctivas y preventivas	Los sistemas GxP deben tener procedimientos para corregir y prevenir las discrepancias del sistema.	Cliente: el cliente controla la identificación y seguimiento de las discrepancias del sistema GxP y es responsable de implementar las medidas de corrección y prevención necesarias. AWS: AWS no tiene visibilidad sobre las operaciones del sistema y sus discrepancias, y no puede implementar medidas correctivas y preventivas para el sistema. AWS mantiene un programa de mejora continua de los productos de AWS y este programa se inscribe en el ámbito de las certificaciones de calidad y seguridad.

La tecnología de servicios web combinada con las prácticas modernas de implementación automatizada permite aumentar la velocidad y robustez de los sistemas sometidos a desarrollo continuo, ya que los distintos componentes del sistema se pueden actualizar con tiempos de inactividad mínimos o, a menudo, inexistentes y sin que se deshagan las dependencias. Siempre que la especificación de la interfaz API no cambie, el cliente puede interactuar con el sistema y tener la seguridad (aunque deberá verificarlo) de que las características que usa estarán disponibles. Los clientes que usan productos de AWS se benefician de las API de los servicios Web, si bien deben diseñar sus sistemas para que sean resistentes frente a las interrupciones de las API. Los sistemas basados en API se pueden integrar también con sistemas de control de cambios como Remedy, ServiceNow, Sparta Systems y otros sistemas de control de administración de cambios, con el fin de integrar totalmente el desarrollo de software y el proceso de implementación con los controles de calidad de GxP.

Para que los clientes de GxP puedan disfrutar de estos beneficios, deben revisar y, si es necesario, actualizar sus documentos y registros de operaciones para adecuarlos a los productos de AWS.

Los clientes deberían actualizar la siguiente documentación para respaldar el uso de productos de AWS en sistemas GxP:

- Procedimiento de control de cambios
- Procedimiento de administración de la configuración
- Procedimiento de lanzamiento a producción
- Procedimientos de monitorización
- Logs de AWS CloudTrail y Config
- Código fuente de la aplicación
- AMI de EC2 y plantillas de CloudFormation
- Casos de soporte técnico de los clientes

3.3 Cuestiones legales

En los sectores regulados por GxP, los profesionales de asuntos jurídicos usan los datos de los sistemas GxP para presentar declaraciones y documentos de registro a las autoridades sanitarias y los comités de ética. También desarrollan y mantienen procedimientos para las inspecciones de los organismos reguladores y para estar al día con la legislación en continuo cambio en las regiones en las que la organización desea distribuir sus productos GxP. Cuando un cliente de GxP usa productos de AWS en sus sistemas GxP, su equipo de TI, de calidad y jurídico debe determinar de qué forma estos productos podrían afectar a sus prácticas reguladoras, incluido lo siguiente:

- Presentaciones a los organismos reguladores
- Inspecciones de las autoridades sanitarias
- Revisión de los requisitos del consejo y el comité de ética

3.3.1 Presentaciones

Usar sistemas GxP para las presentaciones a los organismos reguladores no es nuevo, y ya hay aplicaciones de software basadas en la cloud para generar, controlar y enviar estas presentaciones. De hecho, la FDA usa productos de AWS para publicar datos de las presentaciones reglamentarias mediante la plataforma openFDA.gov. Lo que es nuevo y debe ser examinado por los clientes de GxP es si su sistema GxP se debe incluir o no en el contenido de la presentación a las autoridades y, en tal caso, cómo el equipo jurídico del cliente debe abordar el uso de productos de AWS.

Por ejemplo, una aplicación de software de un dispositivo médico, como un sistema de archivado y comunicación de imágenes (PACS), puede requerir la presentación del modelo 510k para su aprobación por la FDA. Si la aplicación PACS se ha diseñado para ejecutarse en un servidor x86 común compatible con el producto Amazon EC2 de AWS, el modelo 510k de la aplicación podría no mencionar explícitamente los productos de AWS, sino simplemente indicar que “la aplicación de software es una aplicación PACS usada con servidores de propósito general”.

La decisión de incluir los productos de AWS en las presentaciones a los organismos reguladores es responsabilidad de los clientes de GxP, y AWS recomienda a los clientes de GxP que consulten a un profesional cualificado en asuntos legales todas las cuestiones relativas a estas presentaciones.

3.3.2 Inspecciones

Las autoridades sanitarias pueden realizar inspecciones de las organizaciones de ciencias de la salud y sus sistemas GxP en cualquier momento. Aunque los productos de TI COTS cuentan con un largo historial de uso en sistemas GxP sometidos a inspecciones reglamentarias, el uso de proveedores de productos COTS en la cloud como AWS en sistemas GxP es relativamente nuevo y el personal de campo de inspecciones reglamentarias posiblemente no esté familiarizado con los productos de AWS o con su uso. Para garantizar un resultado satisfactorio de la inspección de sistemas GxP que usan productos de AWS, AWS recomienda que los clientes de GxP establezcan y mantengan un plan de preparación de las inspecciones que incluya los siguientes elementos:

- Identificación de las personas clave de la organización del cliente familiarizadas con la configuración y uso de productos AWS en sistemas GxP
- Procedimientos que garanticen que esas personas clave son avisadas y están disponibles si se produce una inspección de la FDA
- Una presentación general de cada sistema GxP que describa brevemente y con exactitud los elementos clave del sistema para el inspector de la FDA o autoridad sanitaria. Los clientes deberían incluir los siguientes elementos en los materiales de presentación:
    - Identificación del sistema, incluido el nombre del sistema, la versión (si procede) y el tipo de sistema
    - Descripción del sistema que incluya información general sobre las actividades clave de GxP y puestos que utilicen el sistema; deben identificarse también las interfaces con otros sistemas
    - Diagrama de red o arquitectura con todas las responsabilidades relacionadas
    - Operaciones del sistema, incluidas las ubicaciones físicas donde se accede al sistema, el número de usuarios finales, las interfaces y los productos
    - Lista de procedimientos operativos estándar de la aplicación, incluidos los procedimientos de todas las unidades de negocio, técnicos y corporativos
    - Resumen de las responsabilidades con los nombres de las unidades de negocio de los usuarios finales, la responsabilidad técnica y administrativa, las operaciones de seguridad, etc.

En el caso de una investigación relacionada con el sistema que requiera soporte técnico para solucionar problemas del producto por parte de AWS, el nivel de soporte técnico de AWS seleccionado por el cliente determinará el canal para enviar las solicitudes de soporte técnico y el tiempo de respuesta esperado de AWS.

Los clientes deberían actualizar la siguiente documentación para respaldar el uso de productos de AWS en sistemas GxP:

- Plan de preparativos de la inspección
- Presentación general del sistema GxP
- Índice de documentación del sistema

3.3.3 Controles de privacidad de los datos personales de las personas que participan en investigaciones

Los sistemas GxP usados en investigaciones clínicas puede requerir también controles de privacidad de datos personales para proteger la confidencialidad de las personas cuya información de identificación personal (PII) e información médica protegida (PHI) almacene, procese o transmita el sistema. Estos son algunos ejemplos:

- Herramientas de contratación de la investigación
- Sistema de captura de datos electrónicos (EC)
- Almacenamiento y archivado de datos
- Aplicaciones de dispositivos médicos de diagnóstico
- Aplicaciones de dispositivos médicos móviles

Los comités institucionales de revisión (IRB), los comités de ética independientes (IEC) o los comités de acceso a los datos (DAC) pueden pedir a los patrocinadores e investigadores que realizan estudios de investigación con humanos que usan sistemas GxP con productos de AWS que proporcionen información sobre cómo el sistema protege la información personal de los participantes en el estudio, incluidas todas las revisiones de seguridad del sistema y controles de operaciones de seguridad realizados, como la descripción de los procedimientos para revocar el acceso al sistema cuando ya no es necesario. Los clientes que usan productos de AWS en sistemas GxP que contienen PII deben asegurarse de conocer los requisitos de ubicación de los datos y, si es necesario, describir los controles de seguridad y ubicación de los datos implementados en los productos de AWS en los que se ejecuta el sistema.
Se puede encontrar información adicional sobre los controles de ubicación de los datos en los productos de AWS online: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-regions-availability-zones.html.

Los clientes deberían actualizar la siguiente documentación para respaldar el uso de productos de AWS en sistemas GxP:

- Política de protección de PII
- Plan de control de ubicación de los datos
- Plan de seguridad del sistema para sistemas GxP

4 CONCLUSIÓN

Aunque la distribución de productos de AWS se realiza a través de Internet en lugar de físicamente, los clientes de sistemas GxP siguen siendo responsables del uso de los productos, incluidas las aplicaciones e infraestructura que desarrollen, la validación y el uso de productos de AWS. Mediante las recomendaciones que se indican en este documento, las empresas de GxP pueden evaluar sus sistemas de calidad, controles de SDLC y planes de asuntos legales para demostrar el control eficaz de los sistemas GxP que incorporan productos de AWS como un componente.

5 REVISIONES DEL DOCUMENTO

En la tabla siguiente se muestra el historial completo de revisiones de este documento técnico.

Fecha	Descripción
Enero de 2016	Versión inicial

6 APÉNDICES

6.1 Recursos de privacidad de los datos

En AWS, la protección de los datos es siempre una prioridad. Aunque los clientes conservan la propiedad y el control de sus datos cuando usan productos de AWS, AWS se esfuerza por proporcionar garantías de seguridad y transparencia a los clientes. En este apéndice se indican algunos de los recursos principales de privacidad de los datos que AWS pone a disposición de los clientes.

- Preguntas más frecuentes sobre la privacidad de los datos https://aws.amazon.com/compliance/data-privacy-faq/
- Informe de solicitud de información semestral corporativo de Amazon http://d0.awsstatic.com/certifications/Information_Request_Report.pdf
- Lista de acceso de terceros de AWS http://aws.amazon.com/compliance/third-party-access/
- LEY SAFE HARBOR DE EE. UU/UNIÓN EUROPEA https://safeharbor.export.gov/companyinfo.aspx?id=27379
- Preguntas más frecuentes y cláusulas del modelo de la Directiva de la Unión Europea 95/46/EC https://aws.amazon.com/compliance/eu-data-protection/
- http://www.cnpd.public.lu/en/actualites/international/2015/03/AWS/index.html
- Base de datos de EE. UU. de genotipos y fenotipos https://d0.awsstatic.com/whitepapers/compliance/AWS_dBGaP_Genomics_on_AWS_Best_Practices.pdf
- Preguntas más frecuentes sobre socios comerciales conformes a la ley HIPAA de EE. UU. https://aws.amazon.com/compliance/hipaa-compliance/

6.2 21 CFR Parte 11 anotada

En este apéndice se indican algunas de las formas en las que los clientes pueden usar productos de AWS para satisfacer los requisitos de registro electrónico y firma electrónica de las normativas 21 CFR Parte 11.

- **Controles de acceso:** los clientes pueden restringir los sistemas GxP y el acceso a los datos a usuarios autorizados. Los clientes pueden usar productos de AWS como Amazon Identity and Access Management (IAM) y AWS Directory Service para implementar controles de acceso. Los clientes de AWS también pueden configurar los controles de acceso de su cuenta para trabajar con directorios locales existentes como Microsoft Active Directory con el fin de crear un entorno de control de acceso sencillo para las implementaciones de la cloud híbrida.
- **Validación del sistema GxP:** las aplicaciones se pueden implementar y validar en AWS. Los clientes pueden validar sus sistemas GxP de acuerdo con las políticas y procedimientos de su organización.
- **Capacidad de recuperación de los datos:** los clientes de AWS pueden generar y recuperar copias completas y exactas de los registros de su cuenta de AWS en cualquier momento durante todo el período de retención de registros. Como los clientes de AWS conservan el acceso administrativo raíz a su cuenta de AWS, sistemas y datos, pueden recuperar sus datos o pistas de auditoría de forma independiente en cualquier momento, siempre que el cliente habilite los productos y características de pista de auditoría de AWS.
- **Pistas de auditoría:** se pueden generar, monitorear, descargar y conservar pistas de auditoría seguras, generadas por el equipo y con marca de tiempo de acuerdo con las políticas definidas por el cliente. Los productos de AWS como AWS CloudTrail y Amazon CloudWatch permiten a los clientes desarrollar y usar sistemas de registro para satisfacer los mayores niveles de auditoría de datos y del sistema, desde el nivel de objeto de archivo individual hasta el nivel de aplicación.
- **Aplicación de flujos de trabajo:** las comprobaciones operativas del sistema de las actividades del flujo de trabajo de GxP las controlan en su totalidad los clientes de AWS, incluidos los procesos de SDLC que mantienen para dicho sistema.
- **Autorización de usuarios:** los clientes de AWS pueden implementar comprobaciones de autorización para garantizar que solo las personas autorizadas puedan usar el sistema o actuar con los datos. Para ello, se pueden usar roles de nivel de infraestructura y grupos de permisos en la cuenta de AWS y en las aplicaciones. Productos como Amazon IAM permiten a los clientes definir los roles, los niveles de seguridad y las políticas de transacciones que necesitan para las cuentas de usuario de la infraestructura y para las cuentas de servicio entre máquinas.

- **Verificación de la entrada y salida de datos:** las comprobaciones de entrada de datos y los controles de aceptación dependen en gran medida de las personas, los procesos y las tecnologías que crean y actualizan los datos de GxP. Si los datos de GxP se introducen manualmente en una aplicación web o móvil, los clientes de AWS pueden implementar una combinación de procesos manuales para entrenar y verificar a sus usuarios antes de proporcionarles acceso a la aplicación. Una vez otorgado el acceso, los controles de nivel de aplicación pueden imponer automáticamente las comprobaciones de entrada de datos necesarias. Los productos de AWS de la cuenta del cliente se pueden usar para supervisar y controlar la conectividad de los recursos en red como estaciones de trabajo y dispositivos móviles. Si los datos de GxP se generan automáticamente desde instrumentos locales, sensores de dispositivos o procesos computacionales de la aplicación, la puesta en cola y el transporte de los datos desde el entorno local del cliente a su cuenta de AWS se puede realizar y controlar mediante una serie de productos de AWS como Amazon Simple Queue Service (SQS) y Amazon Kinesis, y herramientas de administración de identidad y acceso que permitan controles de acceso de nivel de usuario y servicio.

- **Capacitación del personal:** los clientes de AWS desarrollan, mantienen y usan los datos y sistemas GxP en su cuenta de AWS, lo que significa que pueden seguir las políticas y procedimientos existentes para determinar si el personal tiene los conocimientos, la capacitación y la experiencia necesarios para realizar sus tareas de GxP asignadas. AWS ofrece extensa documentación técnica y programas de capacitación de los clientes para ayudar al personal de ingeniería de TI a lograr sus objetivos de aprendizaje de AWS, y el amplio ecosistema de socios de AWS incluye integradores de sistemas de otras empresas y socios de consultoría con competencias en asistencia sanitaria y ciencias de la salud.

- **Documentación del sistema:** los clientes pueden conseguir que se haga un uso de los controles apropiados en toda la documentación del sistema mediante los procedimientos y sistemas de documentación existentes. Se puede hacer referencia a la documentación técnica de AWS usando las direcciones URL correspondientes y cualquier información específica de la versión que requiera el cliente. Asimismo, como la infraestructura virtual de cada cliente en AWS es por naturaleza una estructura definida por software, los clientes pueden aplicar el control de versiones y archivar el conjunto completo de código y plantillas que usan para definir los recursos de AWS en su cuenta (véase Infraestructura validada).
- **Controles de seguridad:** los clientes pueden implementar medidas adicionales como el cifrado de datos en reposo y en tránsito mediante sus soluciones de cifrado cliente existentes o a través de la amplia gama de productos de seguridad de AWS, como Amazon Key Management Service (KMS), además de las características de cifrado en el servidor, cifrado de datos transparente (TDS) y Capa de conexión segura (SSL) en productos como Amazon Simple Storage Service (S3), Amazon Relational Database Service (RDS) y Amazon Elastic Load Balancer (ELB). Amazon Virtual Private Cloud (VPC) es un producto que permite a los clientes controlar su entorno de red virtual y crear conexiones de red privada virtual (VPN) por hardware cifradas entre su centro de datos local y su Amazon VPC, lo que les permite usar la cloud como una extensión de sus redes existentes.
- **Firmas electrónicas:** los requisitos de manifiestos de firma electrónica, vinculación de firma y registro y componentes y controles de firma electrónica se satisfacen normalmente como parte de las aplicaciones validadas que los clientes usan para generar y mantener su datos del sistema GxP. Los clientes deben evaluar la idoneidad de sus aplicaciones de firma electrónica existentes con la red virtual de su cuenta de AWS o pueden abordar los requisitos de firma electrónica como parte de las aplicaciones personalizadas nativas en la cloud que desarrollen. Cuando se usan productos de AWS para abordar requisitos como los controles de contraseñas, las características listas para usar como las políticas de contraseñas de Amazon IAM pueden permitir a los clientes crear sus propias políticas de complejidad y antigüedad de las contraseñas de acuerdo con sus requisitos específicos.
- **Conservación de los datos:** los procedimientos y las políticas para los requisitos de ciclo de vida y conservación de los datos de GxP de cada cliente varían considerablemente en función de los requisitos particulares y de la organización del cliente que se apliquen. Cuando diseñen y desarrollen soluciones de administración de datos de GxP en su cuenta de AWS, los clientes deben encargarse de especificar sus requisitos de confidencialidad, integridad y disponibilidad, incluidas todas las políticas de conservación de registros de los datos sin procesar, datos derivados y metadatos.

6.3 Responsabilidades compartidas en los contratos de AWS

Esta tabla pretende ofrecer un resumen útil de las responsabilidades encontradas en los contratos estándar de AWS, pero no tiene carácter oficial. Las responsabilidades indicadas en esta sección son solo para los distintos productos de AWS y no incluyen las responsabilidades de SLA entre los clientes de AWS y sus usuarios finales.

Tema	**Responsabilidades**	**Cliente**	**AWS**
Contactos	Mantener una dirección de correo electrónico válida asociada a la cuenta de AWS (contrato del cliente 1.2)	x	
Cambios	Notificar a los clientes los cambios importantes o la retirada de un producto de AWS (contrato del cliente 2.1)		x
Cambios	Admitir versiones anteriores de las API de productos de AWS durante 12 meses (contrato del cliente 2.2)		x
Cambios	Realizar actualizaciones de seguridad según sea necesario para garantizar la confidencialidad, integridad y disponibilidad de los productos de AWS https://aws.amazon.com/security/security-bulletins/		x
Contenido	Desarrollo, contenido, mantenimiento y uso de contenido (por ejemplo, registros y aplicaciones GxP) (contrato del cliente 4.1)	X	
Contenido	Seguridad, protección y backup del contenido (contrato del cliente 4.2)	x	
Soporte	Proporcionar soporte a los usuarios finales de sistema GxP (contrato del	x	
Soporte	Soporte técnico básico para el cliente (https://aws.amazon.com/premiumsupport/)		x
Privacidad	Control de las regiones geográficas donde residen los datos	x	