aws partner network | competency

Competencia en venta minorista de AWS

Lista de verificación de validación para socios tecnológicos

Diciembre de 2019
Versión 1.0

Índice

Introducción

El objetivo del programa de competencias de AWS es identificar a los socios de la red de socios de AWS ("socios de APN") que demuestren un dominio técnico y el logro comprobado de resultados satisfactorios por parte de los clientes en ámbitos de soluciones especializadas. La lista de verificación de validación para socios con competencias ("Lista de verificación") está destinada a los socios de APN que estén interesados en obtener una competencia de AWS. La lista de verificación incluye los criterios necesarios para lograr la designación según el programa de competencias de AWS. Los socios de APN se someten a una auditoría de sus capacidades al momento de solicitar la competencia específica. Para realizar la auditoría, AWS recurre a compañías externas y a expertos internos. AWS se reserva el derecho de modificar este documento en cualquier momento.

Expectativas de las partes

Los socios de APN deben leer este documento detalladamente antes de enviar una solicitud al programa de competencias de AWS, aunque se cumplan todos los requisitos. Si las secciones de este documento no son claras y requieren una explicación más detallada, comuníquese en primera instancia con su representante de desarrollo para socios ("PDR") o su director de desarrollo para socios ("PDM") de AWS. El PDR o PDM se comunicará con la oficina del programa si fuera necesario.

Cuando estén listos para presentar una solicitud para el programa, los socios de APN deben completar la columna Autoevaluación del socio de la lista de verificación incluida más adelante en este documento.

Para presentar su solicitud:

1. Inicie sesión en la Central de socios de APN (https://partnercentral.awspartner.com/) como director de Alliance.
2. Seleccione "View My APN Account" (Ver mi cuenta de APN) en el sector izquierdo de la página
3. Desplácese hasta la sección "Program Details" (Detalles del programa).
4. Seleccione la opción "Update" (Actualizar) ubicada junto a la competencia de AWS para la cual desea enviar una solicitud.
5. Complete la solicitud para el programa y haga clic en "Submit" (Enviar).
6. Envíe la autoevaluación completada al email competency-checklist@amazon.com.
    - La autoevaluación debe incluir:
        - La categoría de la solución (interacción con los clientes, comercialización y planificación corporativas, cadena de suministro y distribución, almacén físico, digital y virtual, ciencia de datos de venta minorista avanzada y aplicaciones empresariales para venta minorista clave)
        - El tipo de implementación (SaaS o implementado por el cliente en AWS)
        - Documentación de los casos prácticos de AWS (ver definiciones a continuación)

Si tiene alguna pregunta sobre las instrucciones anteriores, comuníquese con su PDR o PDM.
AWS revisará e intentará disipar sus dudas dentro de los cinco días hábiles para comenzar la programación de la auditoría o para solicitar información adicional.

Con el fin de prepararse para la auditoría, los socios de APN deben leer la lista de verificación, completar la autoevaluación con esta lista y reunir y organizar evidencia objetiva para compartir con el auditor el día que se realice la auditoría.

AWS recomienda que los socios de APN cuenten con personas que puedan hablar detalladamente sobre los requisitos durante la auditoría. La práctica recomendada es que el socio de APN ponga a disposición el personal que se detalla a continuación para la auditoría: uno o más arquitectos o ingenieros certificados en AWS que tengan un nivel de conocimiento técnico alto, un gerente de operaciones responsable de las operaciones y los elementos de soporte y un ejecutivo de desarrollo comercial para dirigir la presentación general. Antes de programar una auditoría, los socios de APN deben asegurarse de contar con los consentimientos necesarios para compartir con el auditor (AWS o un tercero) toda la información incluida en la prueba objetiva o cualquier demostración.

Programa de competencia en venta minorista de AWS

Los socios con competencia en venta minorista de AWS proveen soluciones destinadas al sector de venta minorista para las áreas de interacción con los clientes, comercialización y planificación corporativas, cadena de suministro y distribución en venta minorista, almacén físico, digital y virtual, ciencia de datos de venta minorista avanzada y aplicaciones empresariales para venta minorista clave.

Categorías de la competencia en venta minorista

Los socios de APN deben identificar también la categoría de segmento a la que pertenece su solución:

- **Interacción con los clientes:** soluciones de fidelidad, administración de canales de redes sociales, administración de la relación con los clientes (CRM), centro de contacto, publicidad (correo postal y digital), SEO e interacción con la audiencia que permiten a los líderes del área de marketing del sector de la venta minorista atraer y retener clientes de manera proactiva con anterioridad y posterioridad a una compra.

- **Comercialización y planificación corporativas:** soluciones de comercialización, reabastecimiento, planificación de surtido de productos, planograma o planificación del espacio, promoción y optimización de precios, administración de categorías e interacción con proveedores que utilizan los equipos de comercialización y planificación corporativas.

- **Cadena de suministro y distribución:** soluciones de cadena de suministro y distribución que abarcan sistemas de administración de almacenes (WMS), planificación de recursos empresariales (ERP), automatización de almacenes, importación y exportación, transporte y logística.

- **Almacén físico, digital y virtual:** soluciones que transforman la experiencia de compra online o sin conexión y que abarcan puntos de venta, sistemas de administración de pedidos (OMS), comercio unificado, E-Commerce, entrega a domicilio, experiencia de tienda ilimitada (sin complicaciones), innovaciones digitales (realidad aumentada y virtual, ESL, IoT, avisos, voz, reconocimiento, puestos de autoservicio digitales, espejos inteligentes, pantallas interactivas), administración de recursos digitales (DAM) y pagos.

- **Ciencia de datos de venta minorista avanzada:** lago de datos para venta minorista, soluciones de inteligencia artificial o aprendizaje automático y análisis que mejoran la eficiencia operativa, la obtención de información sobre los clientes y la interacción con ellos.

- **Aplicaciones empresariales para venta minorista clave:** soluciones empresariales para venta minorista clave destinadas a ejecutivos de primera línea, finanzas, compras, recursos humanos, gestión de empleados, departamento legal y TI.

Los socios de APN también deben identificar a qué categoría de entrega corresponde su solución:

1. **SaaS:** se atienden varios clientes desde una infraestructura de AWS compartida. El socio de APN administra todas las cuentas de AWS.

2. **Implementación a cargo del cliente:** se implementan en un entorno de AWS del cliente. El cliente administra todas las cuentas de AWS.

Requisitos previos del programa de competencia en venta minorista de AWS

El gerente del programa de competencias de AWS validará los siguientes ítems. Se debe completar la información faltante antes de programar la revisión de validación de la tecnología.

1.0 Membresía del programa de APN		Cumple S/N
1.1 Nivel de socio tecnológico	El socio de APN debe leer las definiciones y las directrices del programa antes de enviar una solicitud de inscripción al programa de competencia en venta minorista. Haga clic aquí para leer los detalles del programa.	
1.2 Nivel de socio tecnológico	El socio de APN debe ser un socio tecnológico de APN de nivel avanzado antes de solicitar su inscripción al programa de competencia en venta minorista de AWS.	
1.3 Categoría de la solución	El socio de APN deberá identificar la categoría de segmento de su solución: ☐ **Interacción con los clientes** ☐ **Comercialización y planificación corporativas** ☐ **Cadena de suministro y distribución** ☐ **Almacén físico, digital y virtual** ☐ **Ciencia de datos de venta minorista avanzada** ☐ **Aplicaciones empresariales para venta minorista clave** El socio de APN deberá identificar la categoría de entrega de su solución: ☐ **SaaS** ☐ **Implementación a cargo del cliente**	
1.4 Captación de clientes	El socio de AWS deberá describir la cantidad total de clientes que utilizan su solución.	
2.0 Casos prácticos		**Cumple S/N**
2.1 Casos prácticos específicos de venta minorista	El socio de APN debe tener 4 casos prácticos específicos de una solución en revisión para el sector de venta minorista. Cada uno de los 4 casos prácticos debe identificarse con un ejemplo en el cual la solución del socio de APN se utilice en una de las seis categorías de segmento (interacción con los clientes, comercialización y planificación corporativas, cadena de suministro y distribución, almacén físico, digital y virtual, ciencia de datos de venta minorista avanzada y aplicaciones empresariales para venta minorista clave). Los socios de APN que ya cuenten con competencias en aprendizaje automático, migraciones, IoT, datos y análisis o experiencia de cliente digital (DCX) de AWS pueden reutilizar hasta 4 casos prácticos de clientes para proyectos entregados con soluciones personalizadas destinadas a desafíos específicos de la industria y con un ejercicio de actividades que ofrece conocimientos del ámbito de la industria de la venta minorista. Por cada caso práctico, el socio de APN debe proporcionar la siguiente información: ▪ Nombre del cliente ▪ Sitio web del cliente ▪ Desafío del cliente ▪ Cómo se implementó la solución para realizar el desafío ▪ Aplicaciones o soluciones de terceros utilizadas ▪ Fecha en que la referencia entró en producción ▪ Resultados ▪ Diagramas de arquitectura específicos, guías de implementación y demás materiales según el tipo de solución, como se describe en la próxima sección. Se requerirá esta información como parte del proceso de solicitud del programa en la central de socios de APN. La información que se brinde como parte de este caso práctico puede ser privada y no se hará pública. Los 4 casos prácticos presentados se examinarán en la revisión de documentación de la validación técnica. El caso práctico se descartará si el socio de APN no puede presentar la documentación necesaria para acceder a la referencia en cada uno de los puntos de la lista de verificación, o si no se cumple alguno de los puntos de la lista de verificación.	

	Los casos prácticos deben describir implementaciones realizadas dentro de los 18 meses anteriores y deben ser de proyectos que estén en producción con clientes, no en una etapa de prueba de concepto o piloto.	
2.2 Casos prácticos de acceso público	AWS utiliza casos prácticos disponibles al público previa aprobación en la competencia para demostrar el éxito, mediante indicadores clave de rendimiento medibles, que tuvo el socio de APN gracias a la solución y para brindar a los clientes la confianza de que el socio de APN tiene la experiencia y el conocimiento necesarios para desarrollar y crear soluciones que cumplirán sus objetivos. El socio de APN debe publicar 2 de las 4 implementaciones de clientes asociadas con los casos prácticos como casos prácticos disponibles públicamente. Estos casos prácticos disponibles públicamente pueden tener formato de casos formales, documentos técnicos o publicaciones de blog.	
	Los casos prácticos disponibles públicamente se deben poder encontrar fácilmente en el sitio web del socio de APN. Es decir, se debe poder acceder al caso práctico desde la página de inicio del socio y el socio de APN debe proporcionar los enlaces a dichos casos prácticos disponibles al público en su solicitud de inscripción.	
	Los casos prácticos disponibles públicamente deben incluir lo siguiente: ▪ Referencias del nombre del cliente, nombre del socio de APN y AWS ▪ Desafío del cliente ▪ Cómo se implementó la solución para realizar el desafío ▪ Cómo se utilizaron los servicios de AWS como parte de la solución ▪ Logros y resultados	
3.0 Liderazgo sólido y presencia web de venta minorista en AWS		**Cumple S/N**
3.1 Página de destino de AWS del socio de APN	La presencia en Internet de un socio de APN específica para las soluciones de venta minorista en AWS otorga a los clientes confianza sobre las capacidades y la experiencia en este sector del socio de APN. El socio de APN debe tener una página de destino de AWS que describa su solución de venta minorista en AWS, que direccione a casos prácticos públicos, que detalle las asociaciones tecnológicas y que provea cualquier otra información relevante que respalde la experiencia relacionada con la venta minorista del socio de APN y que destaque el trabajo conjunto con AWS. Esta página de venta minorista específica de AWS debe ser accesible desde la página de inicio del socio de APN. La página de inicio no se aceptará como página de destino de AWS a menos que el socio de APN sea una compañía tecnológica dedicada exclusivamente al sector de venta minorista y que la página de inicio refleje la concentración del socio de APN en este sector.	
3.2 Liderazgo sólido en venta minorista	Los socios con competencia en venta minorista de AWS son reconocidos por tener un gran dominio del sector y haber desarrollado soluciones innovadoras gracias a los servicios de AWS. El socio de APN debe tener material disponible públicamente (por ejemplo, publicaciones en blogs, artículos de prensa, videos, etc.) que demuestren la especialización y la experiencia del socio de APN en la venta minorista. Deben incluirse enlaces a ejemplos de publicaciones de los últimos 12 meses.	
4.0 Requisitos del negocio		
4.1 Conjuntos de herramientas listas para usar	El socio cuenta con documentación y conjuntos de herramientas del vendedor listas para usar, que incluye una propuesta clara de valor del producto que se puede articular para la organización de ventas de AWS con toda la información relevante necesaria para determinar si es compatible con la oportunidad de un cliente (por ejemplo, material de apoyo a ventas, presentación y casos prácticos del cliente). La evidencia debe presentarse en forma de material de apoyo a ventas, una presentación, un localizador y una lista de verificación de caso práctico.	
4.2 Soporte del producto/ Servicio de asistencia	El socio ofrece soporte para el producto a los clientes a través de chat web, teléfono o correo electrónico.	

	La evidencia debe presentarse como una descripción del soporte ofrecido a los clientes para su producto o solución.	
4.3 El producto aparece en AWS Marketplace.	El socio de APN pone la solución a disposición en AWS Marketplace. □ Sí □ No Si la respuesta es "sí", el socio de APN debe proporcionar un enlace al listado en AWS Marketplace. Si la respuesta es "no", no se necesita más información.	
4.4 Compensación de ventas para las ofertas conjuntas con AWS	El socio de APN cuenta con planes de compensación de ventas para sus vendedores en relación con las oportunidades conjuntas con AWS. □ Sí □ No □ Explicación: _____ La evidencia se debe presentar en forma de descripción breve del plan de compensación para los vendedores del socio de APN.	
4.5 Ganancias conjuntas de AWS y el socio de APN	El socio de APN documenta y publica las ganancias conjuntas. La evidencia se presenta como una descripción verbal del proceso.	
5.0 Autoevaluación del socio de APN		**Cumple S/N**
5.1 Autoevaluación de la lista de verificación para validación del programa de socios de competencias de AWS	El socio de APN debe conducir una autoevaluación de su cumplimiento de los requisitos de la lista de verificación para validación del socio tecnológico de venta minorista de AWS. ▪ El socio de APN debe completar todas las secciones de la lista de verificación. ▪ La autoevaluación completada se debe enviar por email a **competency-checklist@amazon.com** con el siguiente texto estándar en el asunto: "[Nombre del socio de APN], Autoevaluación para socio tecnológico con competencia en venta minorista completada". ▪ Se recomienda que el socio de APN haga que su arquitecto de soluciones del socio, representante de desarrollo para socios (PDR) o director de desarrollo para socios (PDM) revise la autoevaluación completada antes de enviarla a AWS. El objetivo es garantizar que el equipo de AWS del socio de APN se comprometa y trabaje para realizar sugerencias antes de la revisión y para ayudar a garantizar una experiencia de revisión productiva.	

Lista de verificación de validación de socios tecnológicos con competencia en venta minorista

Los auditores externos o arquitectos de soluciones de socios de AWS validarán los siguientes elementos. Se debe completar la información que falte antes de programar la revisión de la validación de tecnología.

Validación técnica		Aplica a: SaaS	Aplica a: Implementado por el cliente en AWS	Cumple S/N
Diagrama de la arquitectura	En función de la categoría de implementación, deben presentarse uno o más diagramas de la arquitectura. Cada diagrama de la arquitectura debe mostrar lo siguiente: ☐ Los elementos más importantes de la arquitectura y cómo se combinan para ofrecer la solución del socio a los clientes. ☐ Todos los servicios de AWS utilizados, con los íconos del servicio de AWS correspondientes. ☐ Cómo se implementan los servicios de AWS, incluidas la Amazon Virtual Private Cloud (VPC), las zonas de disponibilidad, las subredes y las conexiones a sistemas externos a AWS. ☐ Elementos implementados fuera de AWS, por ejemplo, componentes locales o dispositivos de hardware.	Sí, uno para toda la solución y uno para cada caso práctico.	Sí, uno para cada caso práctico.	
Guías de implementación	La guía de implementación debe proporcionar las prácticas recomendadas para implementar la solución de socio en AWS e incluir todas las secciones descritas en "Requisitos de referencia para las guías de implementación".	No	Sí, una para la solución.	
Lista de verificación de validación completada	Para cada uno de los 4 casos prácticos proporcionados para la solución de socio, el socio de APN debe proporcionar una versión completada de la siguiente lista de verificación en la que se indique qué elementos de la lista se cumplen.	Sí	Sí	
1.0 Seguridad **El pilar de seguridad se centra en la protección de la información y de los sistemas. Los temas principales incluyen la confidencialidad e integridad de los datos, la identificación y administración de los permisos mediante la administración de privilegios, la protección de los sistemas y el establecimiento de controles para detectar eventos de seguridad.**				
1.1 El usuario raíz de la cuenta de AWS no se usa para actividades de rutina	El usuario raíz de la cuenta de AWS no se debe usar para actividades de rutina. Tras crear su cuenta de AWS, debe crear cuentas de usuario de AWS Identity and Access Management (IAM) inmediatamente y usarlas para todas las actividades de rutina. Una vez que haya creado sus cuentas de usuario de IAM, debería almacenar de manera segura las credenciales de la cuenta raíz de AWS y usarlas solamente para realizar las pocas tareas de administración de cuentas y servicios que requiera el usuario raíz de la cuenta de AWS. Para obtener más información sobre cómo configurar cuentas de usuario de IAM y grupos para uso diario, consulte Creación del primer grupo y usuario administrador de IAM.	Sí	No	
1.2 Se habilitó Multi-Factor Authentication (MFA) en el usuario raíz de la cuenta de AWS	Se debe habilitar Multi-Factor Authentication (MFA) para su usuario raíz de la cuenta de AWS. Dado que el usuario raíz de su cuenta de AWS puede ejecutar operaciones sensibles en su cuenta de AWS, agregar una capa adicional de autenticación ayuda a optimizar la protección de su cuenta. Hay diferentes tipos de MFA disponibles, incluidas la MFA virtual y la MFA de hardware.	Sí	No	
1.3 Cuentas de usuario de IAM usadas para todas las actividades de rutina	El usuario raíz de la cuenta de AWS no se debe usar para ninguna tarea en la que no sea obligatorio. Cree un usuario de IAM nuevo para cada persona que requiera acceso de administrador. Luego, convierta esos usuarios en administradores colocándolos en un grupo de administradores al que le asignará la política gestionada de acceso de administrador. Una vez hecho esto, los usuarios en el grupo de	Sí	No	

	administradores podrán configurar los grupos, usuarios, etc. De la cuenta de AWS. Toda interacción futura debe realizarse a través de los usuarios de la cuenta de AWS y sus propias claves en vez de la del usuario raíz. No obstante, para realizar algunas tareas administrativas de la cuenta y el servicio, debe iniciar sesión con las credenciales del usuario raíz.			
1.4 La autenticación multifactor (MFA) está habilitada para todos los usuarios interactivos de IAM	Debe habilitar MFA para todos los usuarios interactivos de IAM. Con MFA, los usuarios tienen un dispositivo que genera un código de autenticación único (contraseña que se usa una sola vez u OTP). Los usuarios deben proporcionar sus credenciales normales (nombre de usuario y contraseña) y la OTP. El dispositivo MFA puede ser una pieza de hardware especial o puede ser un dispositivo virtual (por ejemplo, puede funcionar en una aplicación en un smartphone).	Sí	No	
1.5 Las credenciales de IAM se rotan con frecuencia	Debe cambiar sus contraseñas y las claves de acceso regularmente y asegurarse de que todos los usuarios de IAM de su cuenta también lo hagan. Así, si una contraseña o una clave de acceso se ve comprometida y usted no lo sabe, limita el tiempo que las credenciales se pueden usar para acceder a sus recursos. Puede aplicar una política de contraseña en su cuenta para pedirles a todos sus usuarios de IAM que roten sus contraseñas y puede elegir con qué frecuencia deben hacerlo. Si desea obtener más información sobre la rotación de las claves de acceso de los usuarios de IAM, consulte Rotación de las claves de acceso.	Sí	No	
1.6 Existe una política de contraseña segura para los usuarios de IAM.	Debe configurar una política de contraseña segura para sus usuarios de IAM. Si permite que usuarios cambien sus propias contraseñas, pídales que creen contraseñas seguras y que las cambien de manera periódica. En la página Configuración de la cuenta de la consola de IAM, puede crear una política de contraseña para su cuenta. Puede usar una política de contraseña para definir los requisitos de la contraseña, como una extensión mínima, si debe contener caracteres alfanuméricos, con qué frecuencia debe modificarse, etc. Si desea obtener más información, consulte Establecer una política de contraseña para la cuenta de usuarios de IAM.	Sí	No	
1.7 Las credenciales de IAM no se comparten entre varios usuarios.	Debe crear una cuenta de usuario de IAM individual para cualquier persona que necesite acceso a su cuenta de AWS. Cree un usuario de IAM también para usted, asigne a ese usuario privilegios de administrador y úselo para hacer todo su trabajo. Si crea usuarios de IAM individuales para quienes necesiten acceder a su cuenta, puede darle a cada usuario de IAM un conjunto de credenciales de seguridad único. También puede otorgar permisos diferentes a cada usuario de IAM. Si es necesario, puede modificar o anular los permisos de un usuario de IAM en cualquier momento. (Si comparte las credenciales de su usuario raíz, será difícil anularas y es imposible restringir sus permisos).	Sí	No	
1.8 Las políticas de IAM se centran en dar la menor cantidad de privilegios posible.	Debe seguir la recomendación de seguridad estándar de otorgar la menor cantidad de privilegios posible. Esto significa otorgar solamente los permisos necesarios para realizar una tarea. Determine qué deben hacer los usuarios y luego cree políticas para ellos que les permitan realizar únicamente esas tareas. Comience con un grupo de permisos mínimos y vaya otorgando más permisos a medida que sea necesario. De esta manera, es más seguro que comenzar con permisos más flexibles y luego ir restringiéndolos. Definir el grupo adecuado de permisos implica investigar un poco. Determine qué se requiere para la tarea específica, qué acciones admite un servicio en particular y qué permisos son necesarios para poder realizar dichas acciones.	Sí	No	
1.9 No se usan credenciales preprogramadas	Debe seguir las prácticas recomendadas para administrar las claves de acceso de AWS y evitar el uso de credenciales preprogramadas. Cuando accede a AWS programáticamente, usa una clave de acceso para verificar su identidad y la de sus	Sí	Sí	

(por ejemplo, claves de acceso).	aplicaciones. Cualquiera que tenga su clave de acceso tiene el mismo nivel de acceso a sus recursos de AWS que usted. Por este motivo, AWS se esfuerza por proteger sus claves de acceso y, para mantener nuestro modelo de responsabilidad compartida, usted también debería hacerlo.			
1.10 Todas las credenciales se cifran en reposo.	El requisito básico es garantizar el cifrado de cualquier credencial en reposo.	Sí	Sí	
1.11 Solamente los usuarios interactivos usan las claves de acceso de AWS.	No se debería usar ninguna clave de acceso de AWS, excepto en los siguientes casos: 1. Individuos que acceden a los servicios de AWS y que las almacenan de manera segura en un dispositivo que controla dicha persona. 2. Las usa un servicio para acceder a los servicios de AWS, pero solo en casos en los que: a) no es posible usar un rol de instancia de Amazon EC2, un rol de tarea de Amazon Elastic Container Service (Amazon ECS) o un mecanismo similar, b) las claves de acceso de AWS se rotan al menos una vez por semana, y c) la política de IAM tiene poco alcance de manera que: i) solo permite el acceso a objetivos y métodos específicos, y ii) restringe el acceso a las subredes a partir de las cuales se accede a los recursos.	Sí	Sí	
1.12 AWS CloudTrail está habilitado para todas las cuentas de AWS en todas las regiones.	AWS CloudTrail debe estar habilitado en todas las cuentas de AWS y en todas las regiones. La visibilidad de la actividad de su cuenta de AWS es un aspecto fundamental de las prácticas recomendadas de seguridad y operaciones. Puede usar AWS CloudTrail para ver, buscar, descargar, archivar, analizar y responder a la actividad de la cuenta en toda su infraestructura de AWS. Puede identificar quién o qué realizó una acción, qué recursos se utilizaron, cuándo ocurrió el evento y otros detalles para ayudarlo a analizar y responder a la actividad en su cuenta de AWS.	Sí	No	
1.13 Los registros de CloudTrail se almacenan en un bucket de S3 que pertenece a otra cuenta de AWS.	Los registros de AWS CloudTrail deben colocarse en un bucket que sea propiedad de otra cuenta de AWS configurada para el acceso extremadamente limitado, como auditoría y recuperación únicamente.	Sí	No	
1.14 El bucket de registro de S3 CloudTrail tiene las funciones control de versiones o eliminación MFA habilitadas.	El contenido del bucket del registro de AWS CloudTrail debe estar protegido con el control de versiones o la eliminación MFA.	Sí	No	
1.15 Los grupos de seguridad de Amazon EC2 tienen poco alcance.	Todos los grupos de seguridad de Amazon EC2 deben tener el acceso restringido en la mayor medida posible. Esto incluye al menos 1. Implementar grupos de seguridad para restringir el tráfico entre Internet y Amazon VPC, 2. Implementar grupos de seguridad para restringir el tráfico dentro de Amazon VPC, y 3. En todos los casos, permitir solamente la configuración que tenga la mayor restricción posible.	Sí	Sí	
1.16 Los buckets de Amazon S3 en su cuenta tienen los niveles adecuados de acceso.	Debe asegurarse de que cada bucket de Amazon S3 tenga los controles de acceso adecuados. Al usar AWS, la práctica recomendada es restringir el acceso a sus recursos exclusivamente a la gente que lo necesita (principio de privilegios mínimos).	Sí	Sí	
1.17 Los buckets de Amazon S3 están configurados perfectamente	Debe asegurarse de que los buckets que evitan el acceso público estén configurados adecuadamente para evitar el acceso público. De manera predeterminada, los buckets de Amazon S3 son privados y solo pueden acceder a ellos los usuarios que tienen el acceso habilitado. La mayoría de los casos de uso no requieren acceso público para leer archivos de sus buckets de Amazon S3,	Sí	Sí	

para evitar el acceso público.	a menos que esté usando Amazon S3 para alojar recursos públicos (por ejemplo, para alojar imágenes que se usan en un sitio web público). La práctica recomendada es nunca dar acceso abierto al público.			
1.18 Existe un mecanismo de monitoreo para detectar si los objetos o buckets de S3 se vuelven públicos.	Debe tener un sistema de monitorización o alerta en funcionamiento para detectar si los buckets de Amazon S3 se vuelven públicos. Una opción es usar AWS Trusted Advisor. AWS Trusted Advisor verifica los buckets en Amazon S3 que tienen permisos de acceso abierto. Los permisos del bucket que otorgan acceso a la Lista a todos pueden generar más cambios de lo esperado si usuarios no deseados colocan objetos en el bucket con una frecuencia alta. Los permisos del bucket que otorgan acceso de carga o eliminación a todos crean posibles vulnerabilidades de seguridad, ya que permiten que cualquiera agregue, modifique o elimine elementos en un bucket. Trusted Advisor examina los permisos explícitos del bucket y las políticas del bucket asociadas que podrían anular los permisos del bucket.	Sí	No	
1.19 Existe un mecanismo de monitorización para detectar cambios introducidos en las instancias Amazon EC2 y en los contenedores.	Cualquier cambio que ocurra en sus instancias Amazon S3 o contenedores puede indicar una actividad no autorizada y, como mínimo, se debe registrar en una ubicación duradera para poder investigarse. El mecanismo utilizado para este fin debe al menos: 1. Detectar cualquier cambio en el sistema operativo o en los archivos de la aplicación en las instancias Amazon S3 o los contenedores usados en la solución. 2. Almacenar datos que registren estos cambios en una ubicación duradera, externa a la instancia Amazon S3 o al contenedor. Algunos ejemplos de mecanismos adecuados incluyen: a. La implementación de la verificación de integridad de los archivos a través de una administración de configuración programada (por ejemplo, Chef, Puppet, etc.) o una herramienta especializada (por ejemplo, OSSEC, Tripwire o similar), o b. Ampliar las herramientas de administración de la configuración para validar la configuración del host de Amazon S3 y crear alertas para actualizaciones en los archivos de configuración principal o los paquetes con eventos push (logueados no op) configurados para garantizar que el servicio siga funcionando en todos los hosts dentro del alcance durante el tiempo de ejecución, o c. Implementar un sistema de detección de intrusos en el host, como una solución de código abierto como OSSEC con ElasticSearch y Kibana o usar la solución de un socio. Tenga en cuenta que el siguiente mecanismo no cumple con este requisito: a. Instancias Amazon S3 o contenedores con ciclos frecuentes.	Sí	No	
1.20 Se clasifican todos los datos.	Se consideran y clasifican todos los datos procesados y almacenados del cliente en la carga de trabajo para determinar su sensibilidad y los métodos adecuados que se deben usar al manipularlos.	Sí	Sí	
1.21 Toda la información confidencial está cifrada.	Todos los datos del cliente considerados confidenciales se cifran en tránsito y en reposo.	Sí	Sí	
1.22 Las claves criptográficas se administran de manera segura.	Todas las claves criptográficas se cifran en reposo y en tránsito. El acceso para usar las claves se controla mediante una solución de AWS, como AWS Key Management Service (KMS) o una solución de socio, como HashiCorp Vault.	Sí	Sí	
1.23 Todos los datos en tránsito están cifrados.	Todos los datos en tránsito en el límite de Amazon Virtual Private Cloud están cifrados.	Sí	Sí	
1.24 Existe y se ensaya un proceso de respuesta ante incidentes de seguridad.	Se debe definir un proceso de respuesta ante incidentes de seguridad para manejar incidentes, como riesgos en la cuenta de AWS. Este proceso se debe probar a través de la implementación de procedimientos para ensayar el proceso de respuesta ante incidencias, por ejemplo, realizando un ejercicio lúdico de seguridad. Se debe realizar un ensayo dentro de los últimos 12	Sí	No	

	meses para confirmar que: a. Las personas adecuadas tengan acceso al entorno. b. Las herramientas adecuadas estén disponibles. c. Las personas adecuadas sepan qué hacer para responder ante las diferentes incidencias de seguridad descritas en el plan.			
1.25 Estándares de seguridad de datos (DSS) de la industria de tarjetas de pago (PCI) – Certificación o SAQ	En las aplicaciones de E-Commerce, comercio unificado y punto de venta, donde existen datos de titulares de tarjetas, se define un proceso para realizar una evaluación anual del alcance de los estándares de seguridad de datos (DSS) de la industria de tarjetas de pago (PCI) para la carga de trabajo. En función de la evaluación del alcance, se realiza un cuestionario de evaluación o una certificación de PCI DSS, según sea necesario. La evidencia se debe presentar en forma de un informe de conformidad para la certificación de PCI DSS o un cuestionario de autoevaluación completado (SAQ).	Sí	Sí	
1.26 Cifrado integral de los datos de PCI	En las aplicaciones de E-Commerce, comercio unificado y punto de venta, donde existen datos de titulares de tarjetas, los datos se cifran en tránsito inclusive dentro de una Amazon VPC.	Sí	Sí	
1.27 Protección vigente contra ataques de denegación de servicio distribuido (DDoS)	Provee infraestructura y servicios que reducen la denegación de servicio distribuido (DDoS) en todos los niveles del modelo interconexión de sistema abierto (OSI).	Sí	No	
1.28 Mecanismos vigentes para reducir los 10 ataques principales del Proyecto de Seguridad de Aplicaciones en la Web Abierta (OWASP)	Provee infraestructura y servicios que reducen las vulnerabilidades identificadas por el Proyecto de Seguridad de Aplicaciones en la Web Abierta (OWASP).	Sí	No	
2.0 Fiabilidad El pilar de fiabilidad se centra en la capacidad de prevenir y recuperarse rápidamente de fallas para cumplir con la demanda de la empresa y del cliente. Los temas principales incluyen elementos básicos sobre configuración, requisitos comunes a todos los proyectos, planificación de recuperación y cómo manejamos los cambios.				
2.1 La conectividad a la red está altamente disponible	La conectividad a la red de la solución debe tener disponibilidad alta. Si usa una VPN o AWS Direct Connect para conectarse a las redes del cliente, la solución debe admitir conexiones redundantes, incluso si los clientes no siempre implementan esto.	Sí	Sí	
2.2 Los mecanismos de escalado de la infraestructura coinciden con los requisitos del negocio	Los mecanismos de escalado de la infraestructura deben coincidir con los requisitos del negocio, ya sea a través de: 1. La implementación de mecanismos de escalado automático en cada capa de la arquitectura, 2. La confirmación de que los requisitos actuales del negocio, incluidos los requisitos de costos y el crecimiento del usuario anticipado, no requieren mecanismos de escalado automático Y los procedimientos de escalado manual se documenten completamente y se prueben frecuentemente.	Sí	Sí	
2.3 Los registros de la aplicación y AWS se administran centralmente	Toda la información de registro de la aplicación, y de la infraestructura de AWS, debe consolidarse en un solo sistema.	Sí	No	
2.4 Las alarmas y el monitoreo de AWS y la aplicación se administran centralmente	La infraestructura de AWS y la aplicación se deben monitorear centralmente, con alarmas generadas y enviadas al personal de operaciones correspondiente.	Sí	No	
2.5 El aprovisionamiento y la administración de la infraestructura están automatizados.	La solución debe usar una herramienta automatizada, como AWS CloudFormation o Terraform, para aprovisionar y administrar la infraestructura de AWS. No se debe usar la consola de AWS para realizar cambios de rutina en la infraestructura de AWS de producción.	Sí	Sí	

2.6 Se realizan copias de seguridad de datos con frecuencia	Debe realizar copias de seguridad con frecuencia a un servicio de almacenamiento duradero. Las copias de seguridad le aseguran la posibilidad de recuperarse de situaciones de errores administrativos, lógicos o físicos. Amazon S3 y Amazon Glacier son los servicios ideales para las copias de seguridad y el archivado. Ambas son plataformas de almacenamiento duraderas y de bajo costo. Ambas ofrecen una capacidad ilimitada y no requieren de la administración de volúmenes o medios a medida que crecen los conjuntos de datos de copias de seguridad. El modelo de pago por uso y el bajo costo de GB por mes hacen que estos servicios sean la solución adecuada para la protección de datos.	Sí	Sí	
2.7 Los mecanismos de recuperación se prueban regularmente y después de cambios estructurales importantes	Debe probar los procedimientos y mecanismos de recuperación, ambos de manera periódica y después de realizar cambios importantes en su entorno de la nube. AWS proporciona recursos sustanciales para ayudarlo a realizar una copia de seguridad y una restauración de sus datos.	Sí	No	
2.8 La solución resiste la interrupción de la zona de disponibilidad	La solución debe seguir funcionando en caso de que todos los servicios de una única zona de disponibilidad hayan sido interrumpidos.	Sí	Sí	
2.9 La resistencia de la solución fue probada	La resistencia de la infraestructura a la interrupción de una única zona de disponibilidad se probó en producción, por ejemplo, a través de un ejercicio lúdico, dentro de los 12 meses.	Sí	No	
2.10 Se definió un plan de recuperación de desastres (DR)	Un plan de recuperación de desastres bien trazado incluye un objetivo de punto de recuperación (RPO) y un objetivo de tiempo de recuperación (RTO). Debe definir un RPO y un RTO para todos los servicios, que deben coincidir con el SLA que les ofrece a sus clientes.	Sí	Sí	
2.11 El objetivo de horario de recuperación (RTO) es menos de 24 horas	El requisito básico del RTO es que sea menos de 24 horas para los servicios centrales.	Sí	No	
2.12 El plan de recuperación de desastres (DR) se prueba pertinentemente	Su plan de DR se debe probar con el objetivo de punto de recuperación (RPO) y el objetivo de horario de recuperación (RTO), ambos de manera periódica y después de actualizaciones importantes. Se debe realizar al menos una prueba antes de la aprobación de la aplicación de la capa avanzada de APN de AWS.	Sí	No	
2.13 El plan de recuperación de desastres (DR) incluye recuperación en otra región	Su plan de DR debe incluir una estrategia para ejecutar una recuperación en otra región de AWS y su prueba de recuperación periódica debe comprobarlo. Debe haber completado al menos una prueba del plan de recuperación de desastres, incluida la recuperación en otra región de AWS, dentro de los 12 meses anteriores. Nota: Si bien los procesos de restauración de datos en entornos de prueba o de exportación de datos para usuarios son formas útiles para verificar las copias de seguridad, estos procesos no cumplen con el requisito de realizar una prueba de restauración completa en otra región de AWS.	Sí	No	
3.0 Excelencia operativa El pilar de excelencia operativa se centra en los sistemas de ejecución y monitoreo para proporcionar valor al negocio y mejorar constantemente los procesos y procedimientos. Los temas principales incluyen la administración y automatización de cambios, la respuesta a los eventos y la definición de estándares para administrar exitosamente las operaciones diarias.				
3.1 La implementación de cambios de código está automatizada.	La solución debe usar un método automatizado de implementación de código en la infraestructura de AWS. No se deben usar las sesiones interactivas de Secure Shell (SSH) o protocolo de escritorio remoto (RDP) para implementar actualizaciones en la infraestructura de AWS.	Sí	No	

3.2 Existen guías y procesos de escalamiento	Se deben desarrollar guías para definir los procedimientos estándar utilizados en respuesta a los diferentes eventos de AWS y de la aplicación. Se debe definir un proceso de escalamiento para tratar las alertas y alarmas generadas por el<sistema, y para responder ante las incidencias informadas por el cliente. El proceso de escalamiento debe incluir también el escalamiento a AWS Support cuando corresponda.	Sí	No	
3.3 El soporte de empresas de AWS está habilitado para la cuenta de AWS	Debe habilitarse el soporte de empresas. El soporte de empresas (o un nivel superior) es un requisito de la red de socios de APN para los socios tecnológicos de capa Advanced. Para calificar para la capa Advanced, debe habilitar el soporte de empresas en al menos una de sus cuentas de AWS.	Sí	No	
4.0 Eficiencia del desempeño El pilar de eficiencia del rendimiento se centra en usar los recursos informáticos y de TI de manera eficiente. Los temas principales incluyen la selección de los tipos y tamaños de recursos adecuados en función de los requisitos de las cargas de trabajo, la monitorización del rendimiento y la toma de decisiones informadas para mantener la eficiencia a medida que cambian las necesidades del negocio.				
4.1 La prueba de rendimiento queda habilitada después de las implementaciones.	Defina valores de rendimiento medibles y cuente con pruebas de rendimiento para controlar el cumplimiento de dichos valores antes de que se realice el lanzamiento en producción.	Sí	Sí	
4.2 Monitorización de umbrales existentes	Monitorice el rendimiento de las aplicaciones y cuente con mecanismos para activar alarmas cuando se exceden umbrales definidos.	Sí	Sí	

Recursos de AWS:

Título	Descripción
Cómo crear una página de inicio para el ejercicio de actividades	Se proporciona orientación sobre cómo crear una página de ejercicio de actividades o soluciones que cumpla con los requisitos previos del programa.
Cómo redactar un caso práctico público	Se proporciona orientación sobre cómo crear un caso práctico de cliente público que cumpla con los requisitos previos del programa.
Cómo crear un diagrama de arquitectura	Se proporciona orientación sobre cómo crear un diagrama de arquitectura que cumpla con los requisitos previos del programa.
Documento de preparación del socio	Se proporciona una guía y ejemplos de prácticas recomendadas de los requisitos previos del programa.
Sitio web de buena arquitectura de AWS	Se abordan prácticas recomendadas relacionadas con una buena arqutiectura.