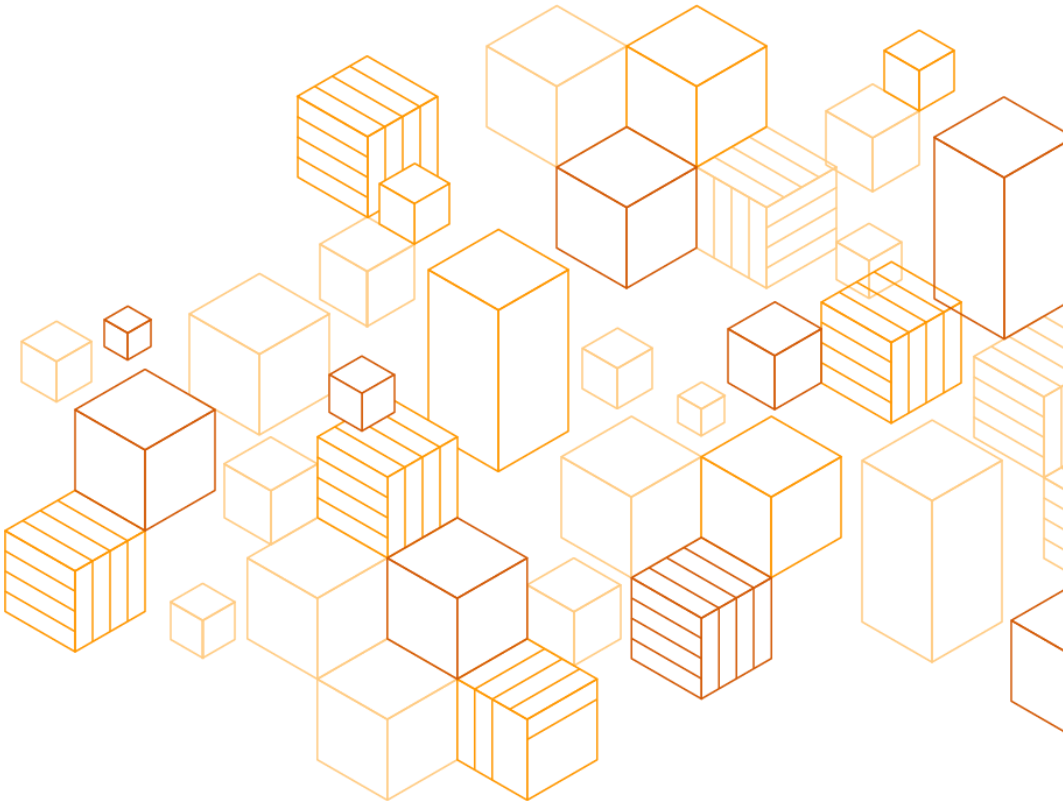
Guía del usuario de AWS acerca de las normas aplicables a las instituciones de crédito en México

Normas generales de la Comisión Nacional Bancaria y de Valores (CNBV) aplicables a las instituciones de crédito

18 de diciembre de 2021



Avisos

Los clientes son responsables de hacer su propia evaluación independiente de la información en este documento. Este documento: (a) solo tiene fines informativos, (b) representa las prácticas y las ofertas de productos de AWS actuales, las cuales están sujetas a cambios sin aviso previo, y (c) no crea compromisos ni promesas de parte de AWS y sus empresas afiliadas, proveedores o licenciantes. Los servicios o los productos de AWS se ofrecen “como son”, sin garantías, declaraciones ni condiciones de ningún tipo, ya sean expresas o implícitas. Las responsabilidades y obligaciones de AWS frente a sus clientes se rigen por los acuerdos celebrados con AWS, y este documento no forma parte de ningún acuerdo entre AWS y sus clientes, ni lo modifica.

Contenido

Acerca de esta guía

En este documento, se proporciona información para ayudar a las instituciones de crédito[1] en México reguladas por la Comisión Nacional Bancaria y de Valores (CNBV) en su proceso de adopción y uso de la nube de Amazon Web Services (AWS).

En esta guía:

- Se describen los roles respectivos que representan el cliente y AWS en la administración y la seguridad del entorno de la nube.
- Se describen los sistemas de seguridad de AWS y el modelo de responsabilidad compartida.
- Se proporciona información general sobre los requisitos regulatorios establecidos en la Circular Única de Bancos ("CUB") aplicable a las instituciones de crédito.
- Se proporcionan recursos adicionales para ayudar a las instituciones de crédito a diseñar y crear sus entornos de AWS para que cumplan sus objetivos de regulación y de seguridad.

[1] Salvo que se indique lo contrario, todas las referencias que se hagan a "Instituciones de crédito" se remiten a las "Instituciones de Crédito" definidas en la Circular Única de Bancos y en el Artículo 2 de la Ley de Instituciones de Crédito.

Información general

AWS proporciona servicios de infraestructura en la nube globales seguros y resistentes a instituciones de servicios financieros, como mercados de banca, pagos globales, capitales y seguros. Las instituciones financieras (IF) de todo el mundo utilizan los servicios de AWS para modernizar y automatizar sus aplicaciones principales, como banca móvil, presentación de informes reglamentarios y análisis de mercado. Gracias a la innovación continua, AWS puede ofrecer a las IF de todo el mundo sistemas de seguridad sólidos, la mayor variedad de servicios en el sector, una importante experiencia en la industria y una red de socios en crecimiento. AWS potencia a las IF para que modernicen su infraestructura de tecnología a fin de satisfacer las conductas y expectativas de los clientes, que cambian rápido, y de impulsar el crecimiento de la empresa. AWS ofrece servicios de tecnología de la información ("TI") en diferentes categorías que abarcan desde la informática, el almacenamiento, las bases de datos y las redes, hasta la inteligencia artificial y el aprendizaje automático.

La CNBV es el principal organismo regulatorio de México a cargo de regular y supervisar el uso de los servicios de nube en las instituciones de crédito. La CNBV tiene autoridad normativa sobre una gran variedad de IF en México, como agentes de bolsa y casas de cambio, cooperativas de crédito, instituciones de tecnología financiera ("*fintechs*"), empresas financieras rurales y comunitarias, depósitos, empresas de cambio de divisas, entre otras. Los requisitos regulatorios específicos que se aplican a las IF, inclusive aquellos relacionados con la subcontratación de servicios de tecnología, varían según la clasificación de la IF y la regulación y la autoridad regulatoria aplicables. Este documento se centra en las instituciones de crédito.

En diciembre de 2005, la CNBV emitió la CUB para recopilar las normas aplicables a las instituciones de crédito que regula dicha comisión. En la CUB, se detallan los requisitos técnicos, operativos y contractuales específicos que deben cumplir las instituciones de crédito reguladas cuando subcontratan servicios de tecnología de la información ("TI") con *cloud service providers* (CSP, proveedores de servicio de nube).

Este documento es un recurso para ayudar a las instituciones de crédito a comprender los requisitos técnicos y operativos a los que puedan estar sujetas de conformidad con la CUB cuando usan AWS. En este documento también se describe el marco de conformidad de AWS y las medidas de seguridad y herramientas avanzadas que podrían resultarles útiles a las instituciones de crédito para evaluar y demostrar su conformidad con los requisitos regulatorios aplicables en virtud de la CUB.

La guía no incluye un análisis completo de la CUB. Sin embargo, en las secciones descritas a continuación se tratan las consideraciones principales que suelen surgir en nuestras interacciones con las instituciones de crédito en México y se proporciona información que estas instituciones pueden usar para ayudarlas a comprender sus responsabilidades y las de AWS según la CUB.

- **Seguridad y responsabilidad compartida**: es importante que las instituciones de crédito comprendan el Modelo de responsabilidad compartida de AWS antes de evaluar los requisitos operativos y técnicos específicos establecidos en la CUB. El modelo de responsabilidad compartida de AWS es fundamental para comprender los roles respectivos del cliente y de AWS con respecto a la seguridad y el acceso a la información.
- **Programas de conformidad de AWS:** AWS obtuvo certificaciones y declaraciones de terceros en una gran variedad de cargas de trabajo específicas del sector. AWS también desarrolló programas de conformidad para poner estos recursos a disposición de los clientes. Los clientes pueden aprovechar los programas de conformidad de AWS para ayudar a satisfacer sus requisitos regulatorios.
- **Infraestructura de nube global de AWS**: la infraestructura de nube global de AWS comprende las zonas de disponibilidad y las regiones de AWS. La infraestructura de nube global de AWS ofrece a sus clientes una forma más sencilla y eficiente de diseñar y utilizar aplicaciones y bases de datos, lo que aumenta su nivel de disponibilidad, tolerancia a errores y escalabilidad, en comparación con los entornos en las instalaciones. Con la infraestructura de nube global de AWS, los clientes pueden diseñar un entorno de AWS coherente con sus necesidades regulatorias y comerciales, incluidos los requisitos aplicables según la CUB.
- **Consideraciones sobre la Circular Única de Bancos (CUB):** en esta sección, se detallan las consideraciones frecuentes sobre las instituciones de crédito que utilizan AWS en cuanto a algunos de los requisitos operativos y técnicos claves según la CUB. Además, se describe cómo las instituciones de crédito pueden aprovechar los servicios de AWS y sus herramientas para ayudarlas a cumplir con los requisitos regulatorios. En el Anexo Consideraciones de AWS sobre los requisitos de seguridad y operación de la CUB, se incluye una lista de los requisitos y las consideraciones correspondientes.

Seguridad y modelo de responsabilidad compartida de AWS

Es importante que las instituciones de crédito comprendan el Modelo de responsabilidad compartida de AWS antes de explorar sus requisitos técnicos y operativos según la CUB. La seguridad en la nube es una responsabilidad compartida. AWS administra la seguridad *de* la nube mediante la garantía de que su infraestructura de nube cumple con los requisitos regulatorios regionales y globales y con las prácticas recomendadas, pero la seguridad *en* la nube es responsabilidad del cliente. Es decir, nuestros clientes conservan el control de los programas de seguridad que eligen implementar para proteger su contenido, sus aplicaciones, sus sistemas y sus redes, como lo harían con las aplicaciones en un centro de datos propio.

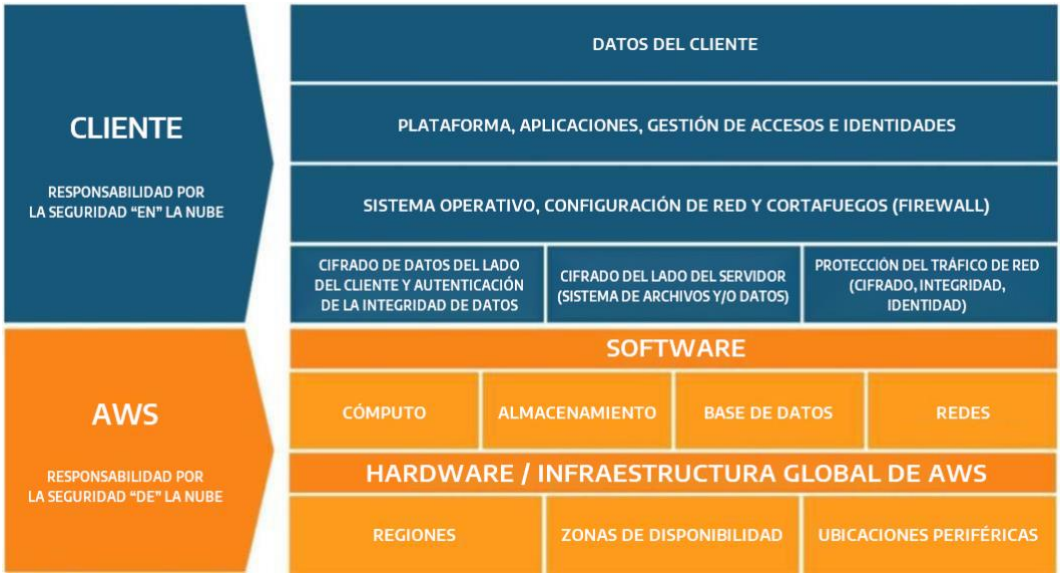


Figura 1: Modelo de responsabilidad compartida

El Modelo de responsabilidad compartida es fundamental para comprender los roles respectivos del cliente y de AWS con respecto a la seguridad de la nube. AWS opera, administra y controla los componentes de TI desde el sistema operativo anfitrión y la capa de virtualización hasta la seguridad física de las instalaciones en las que funciona el servicio.

Seguridad en la nube

Los clientes son responsables de la seguridad en la nube. Los clientes de AWS son responsables de administrar el sistema operativo huésped (incluida la instalación de actualizaciones y parches de seguridad) y otro software de la aplicación asociado, además de otros controles de seguridad de la red que correspondan.

Los clientes deben examinar con cuidado los servicios que eligen, ya que sus responsabilidades varían en función de los servicios utilizados, la integración de los servicios en los entornos de TI y las leyes y normas correspondientes. Es importante señalar que cuando se usan los servicios de AWS, los clientes conservan el control sobre su contenido y son responsables de administrar los requisitos de seguridad del contenido crítico, que comprende lo siguiente:

- El contenido que eligen almacenar en AWS.
- Los servicios de AWS que usan con el contenido.
- El país donde almacenan su contenido.
- El formato y la estructura del contenido y si se encuentra enmascarado, anonimizado o cifrado.
- Cómo cifran los datos y dónde almacenan las claves.

- Quién tiene acceso al contenido y cómo se otorgan, administran y revocan los derechos de acceso.

Como los clientes, en lugar de AWS, controlan estos factores importantes, son ellos quienes retienen la responsabilidad por sus elecciones. Los servicios en la nube de AWS que selecciona un cliente determinan su responsabilidad. A su vez, esta selección determina la cantidad de trabajo de configuración que el cliente debe realizar como parte de sus responsabilidades de seguridad. Por ejemplo, un servicio como Amazon Elastic Compute Cloud (Amazon EC2) se clasifica como *Infrastructure as a Service* (IaaS, infraestructura como servicio) y, como tal, necesita que el cliente realice todas las tareas de administración y configuración de seguridad necesarias. Los clientes que implementan una instancia de Amazon EC2 se encargan de administrar el sistema operativo huésped (incluidas las actualizaciones y los parches de seguridad), el software de aplicación o los servicios que instala el cliente en las instancias y la configuración del firewall que proporciona AWS (denominado grupo de seguridad) en cada instancia.

Para los servicios abstractos, como Amazon Simple Storage Service (Amazon S3) y Amazon DynamoDB, AWS opera la capa de infraestructura, el sistema operativo y las plataformas, y el cliente accede a los puntos de enlace para almacenar y recuperar datos. Los clientes son responsables de administrar sus datos (inclusive las opciones de cifrado), de clasificar sus activos y de usar las herramientas de Identity and Access Management (IAM) para otorgar los permisos apropiados.

Seguridad de la nube

Los servicios y la infraestructura de AWS están aprobados para operar según varios estándares de conformidad y certificaciones del sector en distintas regiones e industrias. Los clientes pueden usar las certificaciones de conformidad de AWS para validar la implementación y la eficacia de los controles de seguridad de AWS, inclusive las prácticas recomendadas y las certificaciones de seguridad reconocidas en el ámbito internacional. Para obtener más información, descargue nuestro documento técnico AWS y la ciberseguridad en el sector de servicios financieros.

El programa de conformidad de AWS se basa en los siguientes principios:

- **Validación** que los servicios de AWS y sus instalaciones en todo el mundo mantienen un entorno de control omnipresente que opera con eficacia. El entorno de control de AWS abarca a las personas, los procesos y la tecnología necesarios para establecer y mantener un entorno que admite la eficacia operativa del marco de control de AWS. En su marco de control, AWS integró controles específicos de la nube aplicables, que identificaron las principales entidades de la industria de la informática en la nube. AWS monitorea estos grupos del sector para identificar las prácticas principales que los clientes pueden implementar y para dar una mejor asistencia a los clientes en la administración de su entorno de control.

- **Demostración** de la postura de conformidad de AWS para ayudar a los clientes a verificar la conformidad con los requisitos del sector y del gobierno. AWS se comunica con los organismos de certificación externa y con los auditores independientes para proporcionar al cliente información sobre las políticas, los procesos y los controles que establece y ejecuta AWS. Los clientes pueden utilizar esta información para ejecutar sus procedimientos de verificación y evaluación de control, según sea necesario en virtud del estándar de conformidad aplicable.
- **Monitoreo**, mediante controles de seguridad aplicables, de que AWS mantiene la conformidad con los estándares y las prácticas recomendadas globales.

Programas de conformidad de AWS

Certificaciones y declaraciones de terceros

AWS obtuvo certificaciones y declaraciones de terceros independientes en una gran variedad de cargas de trabajo específicas del sector. Sin embargo, las siguientes normas son especialmente importantes para los bancos y las instituciones de crédito:

ISO 27001 es un estándar de administración de seguridad que especifica las prácticas recomendadas de administración de seguridad y los controles de seguridad integrales de conformidad con la guía de prácticas recomendadas ISO 27002. Esta certificación se basa en el desarrollo y la implementación de un programa de seguridad riguroso, que incluye el desarrollo y la implementación de un sistema de administración de seguridad de información, que define cómo AWS administra la seguridad de una forma holística e integral. Para obtener más información o descargar la certificación ISO 27001 de AWS, visite el sitio web Conformidad con ISO 27001.

ISO 27017 proporciona una guía sobre los aspectos de seguridad de la información en la nube y recomienda la implementación de controles de seguridad específicos de la nube que complementan las recomendaciones de los estándares ISO 27002 e ISO 27001. Este código de prácticas proporciona información adicional sobre la guía de implementación de controles de seguridad específicos para los CSP. Para obtener más información o descargar la certificación ISO 27017 de AWS, visite el sitio web Conformidad con ISO 27017.

ISO 27018 es un código de prácticas que se centra en la protección de los datos personales en la nube. Se basa en el estándar de seguridad de la información ISO 27002 y proporciona una guía de implementación sobre los controles ISO 27002 aplicables a la información de identificación personal (PII) en la nube pública. Además, ofrece un conjunto de controles adicionales y una guía asociada con el objetivo de abordar los requisitos de protección de la PII en la nube pública que no están cubiertos en el conjunto de controles ISO 27002 actual. Para obtener más información o descargar la certificación ISO 27018 de AWS, visite el sitio web Conformidad con ISO 27018.

ISO 9001 describe un enfoque orientado al proceso para documentar y revisar la estructura, las responsabilidades y los procedimientos necesarios para lograr una administración de calidad eficaz dentro de la organización. La clave para la certificación continua según este estándar es establecer, mantener y mejorar la estructura, las responsabilidades, los procedimientos, los procesos y los recursos de la organización de forma tal que los productos y servicios de AWS satisfagan de manera constante los requisitos de calidad de ISO 9001. Para obtener más información o descargar la certificación ISO 9001 de AWS, visite el sitio web Conformidad con ISO 9001.

PCI DSS Nivel 1: la norma de seguridad de datos del sector de pagos con tarjeta (también conocida como PCI DSS) es un estándar privado de seguridad de la información administrado por el Consejo de estándares de seguridad de la industria de pagos con tarjeta. La PCI DSS se aplica a todas las entidades que almacenan, procesan o transmiten c*ardholder data* (CHD, datos de titulares de tarjetas) o *sensitive authentication data* (SAD, datos de autenticación confidencial), entre los que se incluyen comercios, procesadores, cobradores, emisores y proveedores de servicios. La PCI DSS es definida por las empresas de tarjetas de crédito y administrada por el Consejo de estándares de seguridad de la industria de pagos con tarjeta. Para obtener más información o solicitar la declaración de conformidad con PCI DSS y el resumen de responsabilidad, consulte el sitio web Conformidad con PCI DSS.

SOC: los informes de los *System and Organization Controls* (SOC, controles de organizaciones y sistemas) son documentos de evaluación de terceros independientes, que demuestran cómo AWS alcanza los objetivos y controles de conformidad claves. El objetivo de estos informes es ayudar a los clientes y a sus auditores a comprender los controles de AWS establecidos para respaldar la conformidad y las operaciones. Para obtener más información, consulte el sitio web Conformidad con los SOC. Hay tres tipos de informes SOC de AWS:

- **SOC 1:** ofrece información sobre el entorno de control de AWS que podría ser relevante para los *internal controls over financial reporting* (ICOFR, controles internos sobre los informes financieros) de un cliente, además de información para la evaluación y opinión acerca de la eficacia de dichos controles.
- **SOC 2:** ofrece a los clientes y a los usuarios de sus servicios que tienen una necesidad comercial una evaluación independiente del entorno de control de AWS pertinente para la seguridad, la disponibilidad y la confidencialidad del sistema.
- **SOC 3:** ofrece a los clientes y a los usuarios de sus servicios que tienen una necesidad comercial una evaluación independiente del entorno de control de AWS pertinente para la seguridad, la disponibilidad y la confidencialidad del sistema sin divulgar información interna de AWS.

Para obtener más información sobre otras certificaciones y declaraciones de AWS, consulte el sitio web Programas de conformidad de AWS. Para obtener información acerca de los controles de seguridad generales y específicos al servicio de AWS, consulte las Prácticas recomendadas para la seguridad, la identidad y la conformidad.

AWS Artifact

Los clientes pueden revisar y descargar informes y detalles acerca de más de 2.600 controles de seguridad mediante AWS Artifact, el portal de informes de conformidad automatizado disponible en la consola de administración de AWS. El portal AWS Artifact proporciona acceso a documentos de conformidad y seguridad de AWS, incluso informes SOC, informes de PCI y certificaciones de organismos de acreditación en distintas áreas geográficas y de conformidad.

Infraestructura global de AWS

La Infraestructura de nube global de AWS comprende las zonas de disponibilidad y las regiones de AWS. Una región es una ubicación física en el mundo, que incluye varias zonas de disponibilidad. Las zonas de disponibilidad consisten en uno o más centros de datos, cada uno con conexiones eléctricas, de redes y conectividad redundantes, alojados en instalaciones separadas. Estas zonas de disponibilidad ofrecen al cliente la capacidad de operar aplicaciones y bases de datos con disponibilidad mucho más alta, tolerantes a los errores y escalables de lo que sería posible desde un entorno tradicional en las instalaciones de los clientes. Para obtener más información sobre estos temas, los clientes pueden descargar nuestro documento técnico Abordaje de Amazon Web Services a la resiliencia operativa en el sector financiero y en otros.

Los clientes de AWS eligen la región de AWS donde se ubican su contenido y servidores. Esto permite que los clientes establezcan entornos que cumplen con los requisitos geográficos o regulatorios específicos. Además, permite que los clientes que tienen como objetivos la continuidad del negocio y la recuperación de desastres establezcan entornos principales y de respaldo en una o más ubicaciones que elijan. Si desea obtener más información sobre nuestras recomendaciones para la recuperación de desastres, consulte Recuperación de desastres de cargas de trabajo en AWS: Recuperación en la nube.

Consideraciones sobre la Circular Única de Bancos

Subcontratación de instituciones financieras

La CNBV permite que las instituciones de crédito subcontraten tecnología de la información (TI) a través de *Cloud Services Providers* (CSP, proveedores de servicios de nube) que operan en México o en el exterior. La CUB impone requisitos específicos a las instituciones de crédito que deciden subcontratar sus servicios de TI con CSP que no se encuentran en México.

De conformidad con la CUB, las instituciones de crédito deben obtener la autorización de la CNBV para subcontratar servicios TI con CSP que operan en el exterior y deben cumplir con ciertos requisitos operativos y técnicos.

A. Requisito de autorización

Los requisitos generales que deben cumplir las instituciones de crédito para subcontratar sus servicios de TI con CSP se encuentran en los Artículos 318[2] y 328 de la CUB. Según el Artículo 328, los bancos y las instituciones de crédito deben solicitarle a la CNBV autorización con al menos veinte (20) días de anticipación a la contratación de los servicios de un CSP de otro país.[3] Entre otros requisitos, la autorización debe incluir documentos que demuestren la conformidad con ciertos requisitos contractuales y técnicos. La CNBV debe responder a la institución de crédito correspondiente dentro de los veinte (20) días hábiles posteriores al envío de la solicitud, como se estipula en los Artículos 328 y 326.[4] De conformidad con la CUB, se considera que la solicitud está aprobada de forma predeterminada si la institución de crédito no recibe una respuesta por escrito de la CNBV dentro de los veinte (20) días hábiles estipulados anteriormente.

Para obtener más información sobre estos requisitos, consulte Consideraciones de AWS sobre los requisitos de seguridad y operación de la CUB. Como parte de los requisitos para la autorización establecidos antes, las instituciones de crédito deben cumplir los requisitos contractuales descritos en el Artículo 318. Las instituciones de crédito que son clientes de AWS tienen la opción de celebrar un acuerdo empresarial con AWS.

El acuerdo empresarial de AWS ofrece a los clientes la opción de personalizar sus acuerdos parar satisfacer mejor sus necesidades, incluidos los requisitos regulatorios que generalmente se aplican a las IF. Mediante este tipo de acuerdos, AWS puede ofrecerles a las instituciones de crédito reguladas por la CNBV un marco contractual que las ayuda a satisfacer los requisitos contractuales aplicables de conformidad con la CUB, inclusive términos específicos vinculados con los derechos de acceso e inspección de la CNBV. Para obtener más información sobre los acuerdos empresariales de AWS, contacte a su representante de AWS. Si no tiene un representante de AWS, contáctenos.

---

[2] A menos que se indique lo contrario, todas las referencias a los “Artículos” que se hacen en este documento remiten a la CUB vigente a la fecha de publicación de este documento.

[3] La CNBV publicó una guía que las instituciones de crédito pueden seguir para pedirle su autorización. Consulte Guía Para La Autorización De Contratación Con Terceros De Servicios o Comisiones.

[4] Las instituciones de crédito deben saber que el proceso de autorización puede ser más largo. El período de respuesta de veinte (20) días de la CNBV se extiende de forma indefinida si la CNBV responde con preguntas o solicitudes adicionales.

B. Privacidad de los datos

Las instituciones de crédito también deben evaluar y considerar la aplicación de las leyes de privacidad de datos vigentes en México. Aunque la CUB no especifica requisitos adicionales sobre la privacidad de datos que se apliquen a la subcontratación de servicios de TI con CSP de otros países, en el Artículo 328 se establece que las instituciones de crédito deben celebrar contratos con CSP que residan en una jurisdicción cuyas leyes protegen los datos personales.[5]

C. Conformidad posterior a la aprobación

Después de que la institución de crédito obtiene la aprobación de la CNBV para subcontratar los servicios de TI con un CSP, debe garantizar la conformidad constante con los requisitos técnicos y operativos descritos en la CUB, incluso los del Artículo 316 Bis 11, los requisitos de seguridad y procesamiento de información del Artículo 316 Bis 10 y los requisitos de control de acceso del Artículo 316 Bis 11. Para obtener más información, consulte el anexo a continuación: Consideraciones de AWS sobre los requisitos de seguridad y operación de la CUB.

Planes de AWS Support

Los planes de AWS Support están diseñados para brindarles a los clientes la combinación adecuada de herramientas y acceso al conocimiento para que puedan tener éxito con AWS; mientras optimizan el rendimiento, administran el riesgo y mantienen los costos bajo control.

AWS Basic Support está incluido para todos los clientes de AWS e incluye los siguientes servicios:

- Comunidades y servicio al cliente: acceso las 24 horas del día, los 7 días de la semana, al servicio al cliente, la documentación, los documentos técnicos y los foros de soporte.
- AWS Trusted Advisor: acceso a las siete comprobaciones principales de Trusted Advisor y a la orientación para aprovisionar sus recursos siguiendo las prácticas recomendadas a fin de aumentar el rendimiento y mejorar la seguridad.
- AWS Personal Health Dashboard: ofrece una vista personalizada del estado de los servicios de AWS y envía alertas cuando sus recursos se ven afectados.

[5] El documento técnico de AWS, Cómo usar AWS en el contexto de las consideraciones frecuentes de privacidad y protección de datos, proporciona información útil a los clientes que usan los servicios en la nube de AWS para almacenar o procesar datos personales.

Introducción

El camino hacia la adopción de la nube es único en cada organización; por lo tanto, es necesario que comprenda el estado actual de su organización, el estado objetivo deseado y la transición requerida para llegar al objetivo y adoptar la nube de manera satisfactoria. Esta información es útil para establecer sus objetivos y crear flujos de trabajo que permitirán que su personal prospere en la nube.

En el caso de las instituciones de crédito en México, los pasos suelen ser los siguientes:

- Contactar a su representante de AWS para conocer de qué manera los equipos de la Red de socios de AWS, de AWS Solution Architects y de servicios profesionales, así como los instructores de formación, pueden ayudar en su camino a la adopción de la nube. Si no tiene un representante de AWS, contáctenos.
- Obtenga y revise una copia de los últimos informes SOC 1 y 2 de AWS, la declaración de conformidad con PCI-DSS y el resumen de responsabilidad y la certificación ISO 27001 en AWS Artifact (accesible a través de la consola de administración de AWS).
- Considere la relevancia y la aplicación de los documentos técnicos de seguridad de AWS, AWS Well-Architected Framework y los estándares de referencia de AWS Foundations según CIS, según corresponda para su traspaso a la nube y casos de uso. Estas prácticas recomendadas aceptadas en el sector, que publica el Center for Internet Security, abarcan más contenido que las guías de alto nivel de seguridad ya disponibles y ofrecen a los usuarios de AWS recomendaciones de implementación y evaluación claras y detalladas paso a paso.
- Explore en más detalle otras prácticas de administración del riesgo y de dirección según sea necesario, en vista de su evaluación de riesgo y diligencia debida, mediante el uso de las herramientas y los recursos a los que se hace referencia en esta guía y en la sección Recursos adicionales a continuación.
- Comuníquese con su representante de AWS para obtener información adicional sobre el acuerdo empresarial de AWS y determinar el nivel de soporte que coincide con sus necesidades.

Además de ayudar a los clientes a maximizar el uso de la tecnología proporcionada por AWS, el equipo técnico de AWS puede respaldar a nuestros clientes en sus esfuerzos por implementar la arquitectura, los productos y los servicios de conformidad con los requisitos técnicos y operativos aplicables según la CUB.

Recursos adicionales

A continuación, se exponen recursos adicionales para ayudar a las instituciones de crédito a pensar en la seguridad, la conformidad y el diseño de un entorno seguro y resistente en AWS.

- Guía de referencia rápida sobre la conformidad de AWS: AWS tiene varias características que le ayudan a cumplir sus objetivos de conformidad para las cargas de trabajo reguladas en la nube de AWS. Estas características le permiten alcanzar un nivel más alto de seguridad conforme a la escala. La conformidad basada en la nube ofrece un menor costo de entrada, operaciones más sencillas y agilidad mejorada porque proporciona mayor supervisión, control de seguridad y automatización central.
- La Arquitectura de referencia de seguridad de AWS (AWS SRA) es un conjunto integral de guías para implementar los servicios de seguridad de AWS en un entorno de varias cuentas de usuario AWS. Puede utilizarse para ayudar a diseñar, implementar y administrar los servicios de seguridad de AWS para que se ajusten a las prácticas recomendadas de AWS. Las recomendaciones se basan en una arquitectura que incluye los servicios de seguridad de AWS: cómo pueden ayudar a alcanzar objetivos de seguridad, cuál es el mejor lugar para implementarlos y administrarlos en sus cuentas de AWS y cómo interactúan con otros servicios de seguridad. Estas guías generales sobre la arquitectura complementan las recomendaciones específicas y detalladas del servicio, como las que se encuentran en el sitio web de AWS Security.
- AWS Well-Architected Framework: este servicio se desarrolló para ayudar a los arquitectos de la nube a crear la infraestructura más segura, eficiente, resiliente y de alto rendimiento posible para sus aplicaciones. Este servicio proporciona un enfoque coherente para que clientes y socios evalúen las arquitecturas y ofrece una guía para implementar diseños que escalen junto con las necesidades de la aplicación con el tiempo. AWS Well-Architected Framework se basa en cinco pilares: excelencia operativa, seguridad, fiabilidad, eficacia de rendimiento y optimización de costos.
- AWS elaboró documentos técnicos acerca de cada uno de estos pilares de Well-Architected Framework: Pilar de excelencia operativa de AWS; Pilar de seguridad de AWS; Pilar de fiabilidad de AWS; Pilar de eficacia de rendimiento de AWS y Pilar de optimización de costos de AWS.
- Principios regulatorios de los servicios financieros globales: AWS identificó cinco principios comunes relacionados con la regulación de los servicios financieros que los clientes deben tener en cuenta cuando utilizan los servicios en la nube de AWS y, específicamente, cuando aplican el Modelo de responsabilidad compartida a sus requisitos normativos. Los clientes pueden acceder a los documentos técnicos sobre estos principios en AWS Artifact.

- NIST Cybersecurity Framework (CSF). El documento técnico de AWS NIST Cybersecurity demuestra cómo las organizaciones del sector comercial y público pueden evaluar el entorno de AWS según NIST CSF y mejorar las medidas de seguridad que implementan y operan (por ejemplo, seguridad en la nube). El documento técnico también proporciona una carta para auditores que certifica la conformidad de la oferta de la nube de AWS con las prácticas de administración del riesgo de NIST CSF (es decir, seguridad de la nube). Las instituciones de crédito pueden aprovechar los recursos de NIST CSF y AWS para mejorar sus marcos de administración de riesgos.

Para obtener ayuda adicional, acceda a los documentos técnicos sobre seguridad, identidad y conformidad.

Revisiones del documento

Fecha	Descripción
18 de diciembre de 2021	Primera publicación.

Anexo: Consideraciones de AWS sobre los requisitos de seguridad y operación de la CUB.

En las siguientes secciones, se enumeran los requisitos técnicos y operativos clave identificados en la CUB junto con las consideraciones de AWS para ayudar a las instituciones de crédito clientes a comprender cada requisito en el uso de AWS, y una descripción de las prácticas recomendadas de AWS Well-Architected Framework, que las instituciones de crédito pueden usar para respaldar sus medidas de conformidad.

AWS Well-Architected Framework se desarrolló para que los arquitectos de la nube puedan crear una infraestructura segura, resiliente, eficiente y de alto rendimiento en sus aplicaciones. Basado en cinco pilares (excelencia operativa, seguridad, fiabilidad, eficiencia del rendimiento y optimización de costos), Well-Architected Framework proporciona un enfoque coherente para que los clientes evalúen arquitecturas e implementen diseños que escalarán con el tiempo.

Las tablas en las siguientes secciones están organizadas en las siguientes columnas:

- **Resumen de requisitos**: en esta columna, se resumen los requisitos de la CUB.
- **Consideraciones**: en esta columna, se explican las consideraciones para abordar los requisitos definidos en la CUB. Puede referirse a la seguridad y la conformidad de la nube, y a cómo AWS implementa y administra los controles o los servicios de AWS que las instituciones de crédito pueden usar para abordar estos requisitos.
- **Consideraciones de implementación**: en esta columna, se enumeran las prácticas recomendadas para la seguridad en la nube del AWS Well-Architected Framework que las instituciones de crédito pueden implementar como punto de partida para respaldar sus esfuerzos de conformidad. Los detalles sobre cada práctica recomendada y los servicios de AWS asociados que los clientes pueden aprovechar se encuentran en AWS Well-Architected Framework.

Las siguientes tablas proporcionan consideraciones adicionales sobre cómo los clientes pueden respaldar sus esfuerzos de conformidad para los requisitos aplicables según la CUB. Estas tablas contienen solo una muestra no exhaustiva de las consideraciones. **No es un consejo legal ni de conformidad.** Los clientes deberían consultar con sus propios equipos de asesoría legal y de conformidad.

Sección Tercera – De la contratación con terceros de servicios o comisiones que tengan por objeto la realización de procesos operativos o administración de bases de datos y sistemas informáticos.

Resumen de los requisitos	Consideraciones	Consideraciones de implementación (Prácticas de Well-Architected)
Artículo 326 Las Instituciones en la contratación de terceros para la realización de un proceso operativo o para la administración de bases de datos y sistemas informáticos, deberán dar aviso a la Comisión, previamente a la contratación con terceros. El aviso a que se refiere este artículo, deberá precisar el proceso operativo o de administración de bases de datos y sistemas informáticos objeto de los servicios o comisiones de que se trata y entregarse ala Comisión con una anticipación de por lo menos veinte (20) días hábiles a la fecha en que pretendan contratar dichos servicios o comisiones.	**Responsabilidad de los clientes** Las Instituciones de crédito deben notificar a la CNBV cuando subcontratan servicios de tecnología de la información con un CSP. Sin embargo, como parte de esta notificación, el Artículo 328 también requiere que las instituciones de crédito obtengan autorización de la CNBV antes de utilizar los servicios de un CSP extranjero como AWS. El Artículo 328 se explica en detalle en las siguientes secciones.	No aplicable.

Resumen de los requisitos	Consideraciones	Consideraciones de implementación (Prácticas de Well-Architected)
Artículo 327. El aviso a que se refiere el Artículo 326, deberá ser suscrito por el director general de la Institución y reunir los requisitos siguientes: **I.** Contener el informe a que se refiere la fracción II del Artículo 318. En caso que los servicios a contratar se refieran a la utilización de infraestructura tecnológica o de telecomunicaciones, el aviso deberá contener adicionalmente un informe técnico que especifique el tipo de operaciones o servicios bancarios que habrán de realizarse utilizando la base tecnológica que le sea proveída por terceros o comisionistas, así como la forma en que se dará cumplimiento a los lineamientos mínimos de operación y seguridad, que se señalan en el Anexo 52 de las presentes disposiciones . **II.** Acompañar el proyecto de contrato de prestación de servicios.	**Responsabilidad de los clientes** Las instituciones de crédito en México deben entregar a la CNBV un informe técnico que especifique el tipo de operaciones o servicios bancarios que realizará el CSP correspondiente. Asimismo, las instituciones de crédito deben demostrar en el informe mencionado la forma en que cumplirán con las guías mínimas de operación y de seguridad establecidas en el Anexo 52.	No aplicable.

Resumen de los requisitos	Consideraciones	Consideraciones de implementación (Prácticas de Well-Architected)
Artículo 328. Las Instituciones requerirán de la autorización de la Comisión, para la contratación con terceros de la prestación de servicios, para la realización de un proceso operativo o para la administración de bases de datos, que se proporcionen o ejecuten parcial o totalmente fuera de territorio nacional o por residentes en el extranjero. Las Instituciones deberán solicitar la autorización a la vicepresidencia de la Comisión encargada de su supervisión, con cuando menos veinte (20) días hábiles de anticipación a la fecha en que pretendan contratar los servicios.	**Responsabilidad de los clientes** Las instituciones de crédito en México deben obtener la autorización de la CNBV antes de subcontratar servicios de tecnología de la información con los CSP que operan fuera de México, como AWS. La CNBV requiere que las instituciones de crédito soliciten autorización al menos veinte (20) días antes de contratar al CSP correspondiente. La solicitud de autorización debe contener la documentación adecuada descrita en los Artículos 328 y 318 (explicados a continuación).	No aplicable.
Artículo 328 – I. Debe proveerse documentación para probar que los terceros con los que se contrate residen en países cuyas leyes proporcionan protección a los datos de las personas, resguardando su debida confidencialidad, o bien, los países de residencia mantengan suscritos con México acuerdos internacionales en dicha materia.	**Responsabilidad de los clientes** El cliente de AWS puede elegir la región o las regiones de AWS en las que se ubicará su contenido y puede optar por implementar sus servicios de AWS exclusivamente en una única región si lo prefiere. Los servicios de AWS están estructurados para que el cliente mantenga un control efectivo de su contenido, independientemente de la región que utilice para su contenido. Esto permite que los clientes establezcan entornos que cumplen con los requisitos geográficos o regulatorios específicos.	No aplicable.

Resumen de los requisitos	Consideraciones	Consideraciones de implementación (Prácticas de Well-Architected)
Artículo 328 – II. Las Instituciones deben mantener en sus oficinas principales ubicadas en los Estados Unidos Mexicanos, al menos la documentación e información relativa a las evaluaciones, resultados de auditorías y reportes de desempeño. Asimismo, cuando la Comisión lo requiera deberán proporcionar tal documentación en idioma español.	**Responsabilidad de los clientes** Los clientes de AWS pueden utilizar AWS Artifact, el portal de informes de conformidad automatizado disponible en la Consola de administración de AWS para revisar y descargar informes y detalles sobre más de 2.600 controles de seguridad. El portal de AWS Artifact proporciona acceso bajo demanda a los documentos de seguridad y conformidad de AWS, incluidos los informes SOC, los informes de *Payment Card Industry* (PCI, sector de pagos con tarjeta) y las certificaciones de los organismos de acreditación. Es posible que se apliquen restricciones a la traducción de informes y otra documentación disponible a través de AWS Artifact. Además, el AWS Personal Health Dashboard ofrece a los clientes una vista personalizada del rendimiento y la disponibilidad de los servicios. En el panel, se muestra información pertinente y oportuna para ayudar a los clientes a administrar los eventos en curso y proporciona una notificación proactiva que ayuda a planificar las actividades programadas.	No aplicable.

Resumen de los requisitos	Consideraciones	Consideraciones de implementación (Prácticas de Well-Architected)
Artículo 328 – III. Contar con la aprobación del Consejo o, en su caso, del Comité de Auditoría o del comité de riesgos, haciendo constar en el acuerdo respectivo los aspectos siguientes: **a**) Que al contratar los servicios no se pone en riesgo el adecuado cumplimiento de las disposiciones aplicables a la Institución. **b**) Que las prácticas de negocio del tercero o comisionista son consistentes con las de operación de la Institución. **c**) Que no habría impacto en la estabilidad financiera o continuidad operativa de la Institución, con motivo de la distancia geográfica y, en su caso, del lenguaje que se utilizará en la prestación del servicio. **d**) Las medidas que implementarán en los supuestos previstos por la fracción VII del Artículo 318 de las presentes disposiciones.	**Responsabilidad de los clientes** Los clientes de AWS son responsables de definir su modelo de proceso operativo para administrar sistemas, bases de datos y servicios, así como el proceso de evaluación de riesgos que utilizan. Los clientes de AWS, siguen siendo propietarios de su contenido y seleccionan qué servicios de AWS pueden procesar, almacenar y alojar su contenido. AWS no accede a su contenido ni lo utiliza para ningún propósito sin su consentimiento. AWS nunca utiliza el contenido del cliente ni deriva información de éste para fines de marketing o publicidad. Los requisitos descritos en el Artículo 326 se analizaron en las secciones anteriores de este documento.	No aplicable.

Resumen de los requisitos	Consideraciones	Consideraciones de implementación (Prácticas de Well-Architected)
Para la solicitud de autorización para la contratación de los servicios o comisiones a que se refiere el presente artículo, resultará aplicable lo dispuesto por los Artículos 326, penúltimo y último párrafos y 327 anteriores. Asimismo, la Comisión tendrá la facultad de requerirle a la Institución el proyecto del contrato y, en su caso, el contrato celebrado, con su traducción al idioma español		No aplicable.

Capítulo XI – De la contratación con terceros de servicios o comisiones. Sección primera – Disposiciones generales.

Artículo 318: Las instituciones de crédito, con excepción de aquellas en las secciones I a IX del artículo 317, deben cumplir con los siguientes requerimientos para contratar cualquiera de los servicios referidos en este capítulo.

Resumen de los requisitos	Consideraciones	Consideraciones de implementación (Prácticas de Well-Architected)
I. No aplicable.	No aplicable.	No aplicable.
II. Contar con un informe que especifique los procesos operativos o de administración de bases de datos y sistemas informáticos de la Institución que sean objeto de los servicios a contratar, así como las políticas y criterios para seleccionar al tercero, los cuales estarán orientados a evaluar la experiencia, capacidad técnica y recursos humanos del tercero con quien se contrate para prestar el servicio con niveles adecuados de desempeño, confiabilidad y seguridad, así como los efectos que pudieran producirse en una o más operaciones que realice la Institución.	**Responsabilidad de los clientes** Los clientes de AWS son responsables de definir su modelo de proceso operativo para administrar sistemas, bases de datos y servicios, así como el proceso de evaluación de riesgos que utilizan. A fin de que los clientes de AWS puedan aprovechar al máximo el marco de control de seguridad, AWS desarrolló un programa para garantizar la seguridad que utiliza prácticas recomendadas para la privacidad global y la protección de datos. Los programas de conformidad de AWS ayudan a los clientes a comprender los robustos controles establecidos en AWS para mantener la seguridad y la conformidad en la nube. AWS proporciona un enfoque consistente para que sus clientes evalúen sus arquitecturas y ofrece recomendaciones para ayudarlos a implementar sus diseños.	No aplicable.

Resumen de los requisitos	Consideraciones	Consideraciones de implementación (Prácticas de Well-Architected)
III. Incluir en el contrato de servicio con el tercero, la aceptación de los siguientes términos, entre otros: obligaciones de confidencialidad, reportar cambios al propósito de negocio, aceptación de revisiones de la CNBV.	**Responsabilidad compartida** Mediante un acuerdo empresarial de AWS, se ofrece a las instituciones de crédito reguladas por la CNBV un marco contractual que las ayuda a satisfacer los requisitos contractuales aplicables de conformidad con la CUB, inclusive términos específicos vinculados con los derechos de acceso e inspección de la CNBV. Para obtener más información sobre los acuerdos empresariales de AWS, contacte a su representante de AWS.	No aplicable.
IV. Establecer lineamientos y mecanismos tendientes a la no afectación y adecuada prestación de los servicios de la Institución al público, su estabilidad financiera o continuidad operativa después de haber finalizado el contrato con el prestador de servicios o comisionista, considerando aquellos necesarios para verificar que éste no conserve información alguna de la Institución o de sus clientes.	**Responsabilidad de los clientes** Los clientes retienen la propiedad y el control de su contenido y de su ciclo de vida cuando utilizan los servicios de AWS, y no ceden la propiedad, ni el control de su contenido a AWS. Los clientes de AWS tienen control completo sobre que servicios utilizan y a quién le dan permiso de acceder a su contenido y servicios, incluyendo qué credenciales serán requeridas. Los clientes controlan cómo configuraran sus ambientes y protegen su contenido, incluyendo si cifran su contenido (en reposo y en tránsito), y qué otras funciones y herramientas de seguridad utilizan y cómo las usan. Los servicios de AWS permiten a los clientes exportar su contendido, utilizando la AWS Management Console, APIs y otros métodos. Por ejemplo, AWS Snowball proporciona dispositivos diseñados para transferir grandes cantidades de datos hacia y fuera de la nube de AWS. Para más información sobre migración de datos hacia y fuera de AWS, ver Migration & Transfer on AWS. Los servicios de AWS dan a los clientes el control para borrar su contenido, como se describe en la Documentación de AWS.	No aplicable.

Resumen de los requisitos	Consideraciones	Consideraciones de implementación (Prácticas de Well-Architected)
V. Dar cumplimiento a los lineamientos mínimos de operación y seguridad que se señalan en los Anexos 52 y 58.	**Responsabilidad compartida** Los clientes de AWS son responsables de definir su modelo de gobernanza, gestión de riesgos y operación, y pueden hacerlo basados en los servicios y productos de AWS que utilizan. AWS apoya a los clientes para construir su arquitectura basadas en requerimientos regulatorios y del cliente. Como se explica en la sección “Seguridad y modelo de responsabilidad compartida”, la seguridad en la nube es una responsabilidad compartida. AWS maneja la seguridad de la nube, asegurando que la infraestructura de AWS cumpla con los requerimientos regulatorios globales y con las mejores prácticas Sin embargo, la seguridad en la nube es responsabilidad del cliente. Esto significa que los clientes son responsables de los programas de seguridad para proteger su contenido, plataforma, aplicaciones, sistemas, y redes en la misma forma que lo hacen en su centro de datos. Las auditorías internas y externas de AWS se planifican y realizan de acuerdo con un programa de auditoría documentado para revisar el rendimiento continuo de AWS en comparación con criterios basados en estándares y para identificar oportunidades de mejora general. Los criterios basados en estándares incluyen, entre otros, la ISO/IEC 27001, AT 801 (anteriormente Declaración de Estándares para Compromisos de Atestación [SSAE] 16) del Instituto Norteamericano de Contadores Públicos Certificados (AICPA) y los Estándares Internacionales para Compromisos de Aseguramiento de Normas profesionales n.° 3402 (ISAE 3402). AWS apoya a los clientes de AWS en el proceso de autorización con la CNBV con soporte técnico, información y documentación de los Programas de Cumplimiento de AWS. El Anexo 52 se explica a detalle en páginas subsiguientes.	OPS 4 Diseñar para la información de la carga de trabajo OPS 7 Disposición operativa OPS 8 Estado de la carga de trabajo OPS 10 Respuesta a eventos SEC 1 Operaciones seguras SEC 4 Eventos de seguridad SEC 7 Clasificación de los datos SEC 8 Protección de datos en reposo SEC 9 Protección de datos en tránsito SEC 10 Respuesta ante incidentes REL 4 Diseño de interacciones para evitar errores REL 5 Diseño de interacciones para mitigar errores REL 6 Monitoreo de los recursos REL 9 Copia de seguridad de datos REL 10 Aislamiento de errores REL 11 Implementación de resiliencia REL 12 Pruebas de fiabilidad REL 13 Recuperación de desastres PERF 7 Monitoreo del rendimiento

Resumen de los requisitos	Consideraciones	Consideraciones de implementación (Prácticas de Well-Architected)
VI. Verificar que los terceros no se encuentren dentro de las listas oficiales que emitan autoridades mexicanas, organismos internacionales, agrupaciones intergubernamentales o autoridades de otros países, de personas vinculadas o probablemente vinculadas con operaciones con recursos de procedencia ilícita, el terrorismo o su financiamiento, o con otras actividades ilegales. Adicionalmente, la Institución deberá manifestar que conoce el negocio al que se dedica el tercero.	**Responsabilidad de los clientes** Los clientes deben documentar que han confirmado que AWS no forma parte de las listas indicadas en la regulación al momento de contratar los servicios. El sitio de la CNBV contiene información adicional.	No aplicable.

VII. Contar con la previa aprobación del Consejo o de Comité de Riesgos de la Institución de la evaluación del impacto que las contrataciones a que se refiere el presente Capítulo XI pudieran tener cualitativa o cuantitativamente en las operaciones que realice la Institución, conforme a su objeto, tomando en cuenta para ello, lo siguiente: **a)** La capacidad de la Institución para, en caso de contingencia, mantener la continuidad operativa y la realización de operaciones y servicios con sus clientes. **b)** La complejidad y tiempo requerido para encontrar un tercero que, en su caso, sustituya al originalmente contratado. **c)** La capacidad de la Institución para mantener controles internos apropiados y registros contables, así como para cumplir con los requerimientos regulatorios en caso de suspensión del servicio por parte del tercero o comisionista. **d)** El impacto que la suspensión del servicio tendría en las finanzas, reputación y operaciones de la Institución. **e)** La vulnerabilidad de la información relativa a los clientes.	**Responsabilidad de los clientes** Los clientes de AWS pueden aprovechar las características de la infraestructura de AWS y los servicios de AWS para cumplir con una amplia gama de objetivos de resiliencia. El uso de varias zonas de disponibilidad, incluso dentro de una sola región, puede mejorar la resiliencia en comparación con un entorno en las instalaciones. El uso de varias regiones aumenta aún más la resiliencia. Las zonas de disponibilidad están diseñadas para mitigar el riesgo de desastres naturales y otras interrupciones que puedan ocurrir. Las zonas de disponibilidad están físicamente separadas dentro de una región metropolitana y se encuentran en diferentes llanuras aluviales. Cada zona de disponibilidad también está diseñada como una zona de error independiente y los procesos automatizados alejan el tráfico de clientes del área afectada en caso de error. Los clientes pueden lograr objetivos de puntos de recuperación y tiempos de recuperación extremadamente altos mediante el uso de múltiples zonas de disponibilidad y replicación de datos. Las arquitecturas más resistentes utilizan varias regiones de AWS. Las regiones de AWS proporcionan una mayor separación geográfica que el uso de una sola región. Las regiones de AWS están diseñadas para ser autónomas y se implementan copias dedicadas de los servicios en cada región. Los clientes de AWS pueden usar varias regiones para operar cargas de trabajo que requieren alta disponibilidad y mitigar los riesgos de interrupciones físicas a gran escala. Los servicios de AWS permiten que los clientes exporten contenido bajo demanda, mediante la consola de administración de AWS, las API y otros métodos de entrada. Por ejemplo, AWS Snowball proporciona dispositivos diseñados para ser seguros durante la transferencia de entrada y salida a la nube de AWS de grandes cantidades de datos. Para obtener más información sobre la migración de datos dentro de AWS y fuera de éste, consulte: Migración y transferencia en AWS. Los clientes conservan la propiedad y el control de su contenido cuando utilizan los servicios de AWS y no los ceden a AWS. Los clientes tienen control total sobre qué servicios utilizan y a quién autorizan para acceder a su contenido y servicios, incluidas las credenciales que requerirán. Los clientes controlan cómo configuran sus entornos y protegen su contenido, incluso si cifran su contenido (en reposo y en tránsito) y qué otras características y herramientas de seguridad utilizan y cómo las usan. AWS no cambia los valores de configuración del cliente, ya que es el cliente quien los determina y controla. Los clientes de AWS tienen total libertad para diseñar su arquitectura de seguridad que satisfaga sus necesidades de conformidad. Ésta es una diferencia clave con las soluciones de alojamiento tradicionales en las que el proveedor impone la arquitectura. AWS proporciona formas de categorizar los datos de la organización en función de los niveles de confidencialidad. Mediante el uso de etiquetas de recursos, políticas AWS IAM, AWS KMS y AWS CloudHSM, los clientes pueden definir e implementar las políticas para la clasificación de datos.	No aplicable.

Resumen de los requisitos	Consideraciones	Consideraciones de implementación (Prácticas de Well-Architected)
Art. 318 Bis Los requerimientos de información y, en su caso, las observaciones o medidas correctivas que deriven de la supervisión que realice la Comisión se realizarán directamente a la Institución. Asimismo, la Comisión podrá, en todo momento, ordenar la realización de las visitas y auditorías señaladas en el Artículo 318, fracción III, inciso a. **Art. 318 Bis I** La Institución deberá practicar, por lo menos, una vez cada dos años, auditorías que tengan por objeto verificar el grado de cumplimiento del presente Capítulo XI, así como lo establecido en los Anexos 52 y 58 de las presentes disposiciones de la prestación de servicios para la realización de procesos operativos, la administración de bases de datos o de sistemas informáticos, así como de la infraestructura, controles y operación del centro de cómputo del proveedor de servicio.	**Responsabilidad compartida** A través del AWS Enterprise Agreement, AWS ofrece a las instituciones de crédito reguladas por la CNBV un marco contractual que les puede ayudar a satisfacer los requerimientos contractuales aplicables bajo la CUB, incluyendo términos para atender los requerimientos de acceso e inspección de la CNBV. Para más información sobre los AWS Enterprise Agreements, favor de contactar a su representante de cuenta de AWS. Los clientes pueden validar los controles de seguridad implementados dentro del entorno de AWS a través de certificaciones e informes de AWS, como los informes de AWS Service Organization Control (SOC) 1, 2 y 3, las certificaciones ISO 27001, 27017 y 27018 y los informes de conformidad con PCI DSS. Estos informes y certificaciones son elaborados por auditores independientes y dan fe del diseño y la eficacia operativa de los controles de seguridad de AWS. Los clientes pueden revisar y descargar informes y detalles sobre más de 2.600 controles de seguridad mediante AWS Artifact, el portal de informes de conformidad automatizado disponible en la consola de administración de AWS. El portal de AWS Artifact proporciona acceso bajo demanda a los documentos de seguridad y conformidad de AWS, incluidos los informes SOC, los informes de PCI y las certificaciones de los organismos de acreditación en distintas regiones geográficas y verticales de conformidad. Hay cuatro informes SOC de AWS disponibles para los clientes de AWS desde AWS Artifact: • Informe SOC 1 de AWS • Informe de seguridad, disponibilidad y confidencialidad SOC 2 de AWS • Informe tipo I de privacidad SOC 2 de AWS • Informe de seguridad, disponibilidad y confidencialidad SOC 3 de AWS, disponible públicamente como documento técnico. Las auditorías internas y externas de AWS se planifican y realizan de acuerdo con el programa de auditoría documentado para revisar el rendimiento continuo de AWS en comparación con los criterios basados en estándares y para identificar oportunidades de mejora general. Los criterios basados en estándares incluyen, entre otros, la ISO/IEC 27001, AT 801 (anteriormente Declaración de Estándares para Compromisos de Atestación [SSAE] 16) del Instituto Norteamericano de Contadores Públicos Certificados (AICPA) y los Estándares Internacionales para Compromisos de Aseguramiento de Normas profesionales n.° 3402 (ISAE 3402).	No aplicable.

Anexo 52 - Lineamientos mínimos de operación y seguridad para la contratación de servicios de apoyo tecnológico.

Resumen de los requisitos	Consideraciones	Consideraciones de implementación (Prácticas de Well Architected)
I. Aspectos Operativos **a.** Esquemas de redundancia en las telecomunicaciones que minimicen el riesgo de interrupción. **b.** Estrategia de continuidad para procesar y operar sistemas en caso de contingencia. **c.** Mecanismos para establecer y vigilar la calidad en los servicios, así como tiempos de respuesta de aplicaciones. **d.** Esquema de soporte técnico. **e.** Mecanismos que permitirán a la Institución mantener bajo su resguardo en territorio nacional, los registros detallados de todas las Operaciones que se realicen, así como de sus registros contables de forma que se asegure la continuidad operativa en todo momento. **II. Aspectos de seguridad** **a.** Medidas para asegurar la transmisión de la Información Sensible del Usuario en forma cifrada. **b.** Establecimiento de funciones del oficial en jefe de seguridad de la información. **c.** Esquema mediante el cual se mantendrá la bitácora de acceso a la información por el personal.	**Responsabilidad de los clientes** Los clientes definen su modelo de administración, evaluación del riesgo y operación y pueden hacerlo con base en los servicios y productos de AWS que utilizan. Como se explica en la sección "Seguridad y responsabilidad compartida", la seguridad en la nube es una responsabilidad compartida. AWS administra la seguridad de la nube, mediante la garantía de que su infraestructura cumple con los requisitos normativos globales y con las prácticas recomendadas. Sin embargo, la seguridad en la nube es responsabilidad del cliente. Esto significa que los clientes son responsables de los programas de seguridad que implementan para proteger su contenido, plataforma, aplicaciones, sistemas y redes de la misma manera que lo hacen en un centro de datos local. Las auditorías internas y externas de AWS se planifican y realizan de acuerdo con el programa de auditoría documentado para revisar el rendimiento continuo de AWS en comparación con los criterios basados en estándares y para identificar oportunidades de mejora general. Los criterios basados en estándares incluyen, entre otros, la ISO/IEC 27001, AT 801 (anteriormente Declaración de Estándares para Compromisos de Atestación [SSAE] 16) del Instituto Norteamericano de Contadores Públicos Certificados (AICPA) y los Estándares Internacionales para Compromisos de Aseguramiento de Normas profesionales n.° 3402 (ISAE 3402). AWS respalda el proceso de autorización de los clientes de AWS con la CNBV, mediante la prestación de soporte técnico, información y documentación para los programas de conformidad de AWS. También hay información adicional disponible en la: Guía para la autorización de contratación con terceros de servicios o comisiones en el portal web del gobierno mexicano. Los clientes pueden definir la arquitectura de sus cargas de trabajo para cumplir con requerimientos geográficos o regulatorios. Los clientes pueden trabajar con su representante de cuenta de AWS y el arquitecto de AWS para obtener guía adicional de los servicios de AWS que pueden emplearse para dar cumplimiento al Anexo 52.	OPS 4 Diseñar para la información de la carga de trabajo OPS 7 Disposición operativa OPS 8 Estado de la carga de trabajo OPS 10 Respuesta a eventos SEC 1 Operaciones seguras SEC 4 Eventos de seguridad SEC 7 Clasificación de los datos SEC 8 Protección de datos en reposo SEC 9 Protección de datos en tránsito SEC 10 Respuesta ante incidentes REL 4 Diseño de interacciones para evitar errores REL 5 Diseño de interacciones para mitigar errores REL 6 Monitoreo de los recursos REL 9 Copia de seguridad de datos REL 10 Aislamiento de errores REL 11 Implementación de resiliencia REL 12 Pruebas de fiabilidad REL 13 Recuperación de desastres PERF 7 Monitoreo del rendimiento

III. Auditoría y Supervisión	
a. Políticas y procedimientos relativos a la realización de auditorías internas o externas.	
b. Mecanismos de acceso al ambiente tecnológico, incluyendo información, bases de datos y configuraciones de seguridad, desde las instalaciones de la Institución en territorio nacional.	

Sección Quinta – Otras disposiciones - Capítulo X - Uso de los servicios electrónicos del banco.

Sección Cuarta – Seguridad, Confidencialidad e Integridad de la Información Transmitida, Almacenada o Procesada Vía Medios Electrónicos.

Resumen de los requisitos	Consideraciones	Consideraciones de implementación (Prácticas de Well-Architected)
Artículo 316 Bis 10. Las Instituciones que utilicen Medios Electrónicos para la celebración de operaciones y prestación de servicios, deberán implementar medidas o mecanismos de seguridad en la transmisión, almacenamiento y procesamiento de la información: **I.** Cifrar los mensajes o utilizar medios de comunicación cifrada, en la transmisión de la Información Sensible del Usuario. **II.** Las Instituciones deberán cifrar Factores de Autenticación. **III.** En ningún caso, las Instituciones podrán transmitir las Contraseñas y Números de Identificación Personal (NIP) que no cuenten con mecanismos de cifrado. **IV.** Las Instituciones deberán asegurarse de que las llaves criptográficas y el proceso de cifrado y descifrado se encuentren instalados en dispositivos de alta seguridad, tales como los denominados HSM (Hardware Security Module). **V.** Tratándose del servicio de Banca Electrónica en el que se utilicen	**Responsabilidad de los clientes** Los clientes controlan cómo configuran sus entornos y protegen su contenido, incluso si cifran su contenido (en reposo y en tránsito) y qué otras características y herramientas de seguridad utilizan y cómo las usan. AWS protege la confidencialidad y la integridad de los datos transmitidos mediante la comparación de un *hash* criptográfico de los datos transmitidos, lo que ayuda a garantizar que el mensaje no se corrompa ni altere en el tránsito. Los datos corrompidos o alterados en el tránsito se rechazan inmediatamente. AWS proporciona varios métodos para que los clientes manejen sus datos de forma segura. AWS CloudHSM es un servicio para crear y administrar módulos de seguridad de hardware basados en la nube. Un *hardware security module* (HSM, módulo de seguridad de hardware) es un dispositivo de seguridad especializado que genera y almacena claves criptográficas. Si necesita proteger sus claves de cifrado en un servicio con el respaldo de HSM validados por FIPS, pero no necesita administrar el HSM, considere AWS Key Management Service. Para obtener la declaración de conformidad con PCI DSS y el resumen de responsabilidad, consulte el sitio web Conformidad con PCI DSS. Para obtener más información, visite la Guía del usuario de S3: Protección de datos mediante cifrado del lado del servidor.	SEC 7 Clasificación de los datos SEC 8 Protección de datos en reposo SEC 9 Protección de datos en tránsito PERF 5 Selección de red

Resumen de los requisitos	Consideraciones	Consideraciones de implementación (Prácticas de Well-Architected)
tarjetas de débito y de crédito, con las certificaciones que se indican a continuación. **a)** Certificaciones de normas de seguridad de la industria de tarjetas, incluyendo entre otras: la norma de seguridad de datos (PCI-DSS), la norma de seguridad de datos para las aplicaciones de pago (PA-DSS) y los requisitos de seguridad y transacciones con NIP (PTS) o sus equivalentes. **b)** Certificación conforme al estándar de interoperabilidad de tarjetas de débito y de crédito conocido como EMV, niveles 1 (interfases, físico, eléctrico y de transporte) y 2 (selección de aplicaciones de pago y procesamiento de transacciones).		
Artículo 316 Bis 11. Las Instituciones deberán contar con controles para el acceso a las bases de datos y archivos: **I.** El acceso a las bases de datos y archivos estará permitido exclusivamente a las personas expresamente autorizadas por la Institución en función de las actividades que realiza. **II.** Los accesos que se realicen en forma remota, deberán utilizar mecanismos de cifrado.	**Responsabilidad compartida** Los clientes conservan la propiedad y el control de su contenido cuando utilizan los servicios de AWS y no los ceden a AWS. En AWS, la administración de privilegios está respaldada principalmente por el servicio AWS Identity and Access Management (IAM), que le permite controlar el acceso programático y de los usuarios a los servicios y recursos de AWS. Puede aplicar políticas detalladas, que asignen permisos a un usuario, grupo, rol o recurso. También tiene la capacidad de exigir prácticas de contraseña seguras, como el nivel de complejidad, evitar la reutilización y aplicar la autenticación multifactor (MFA). Puede usar la federación con su servicio de directorio existente. Para las cargas de trabajo que requieren que los sistemas tengan acceso a AWS, IAM permite el acceso seguro a través de roles, perfiles de instancia, identidad federada y credenciales temporales.	SEC 2 Autenticación SEC 3 Control de acceso y autorización

Resumen de los requisitos	Consideraciones	Consideraciones de implementación (Prácticas de Well-Architected)
III. Contar con procedimientos seguros de destrucción de los medios de almacenamiento. **IV.** Desarrollar políticas del uso y almacenamiento de información, estando obligadas a verificar el cumplimiento de sus políticas por parte de sus proveedores.	AWS no conoce el tipo de contenido que el cliente elige almacenar en AWS, y el cliente retiene el control total de cómo elige clasificar su contenido y dónde se almacena, usa y protege contra la divulgación. AWS proporciona un conjunto avanzado de características de acceso, cifrado y registro, como AWS CloudTrail, para ayudar a las IF a lograr estos objetivos de manera eficaz. No accedemos al contenido de los clientes ni lo utilizamos para ningún otro propósito que no sea el requerido por la ley o para mantener los servicios de AWS y proporcionárselos a nuestros clientes y sus usuarios finales. AWS permite a los clientes abrir una sesión segura y cifrada en los servidores de AWS mediante HTTPS (Transport Layer Security, "TLS"). Además, AWS ofrece a los clientes la capacidad de agregar una capa adicional de seguridad a los datos en reposo en la nube, dado que proporciona características de cifrado escalables y eficientes. Es responsabilidad del cliente de AWS habilitar estas características para sus sistemas. Para garantizar que los procedimientos de mantenimiento e inventario de administración de activos se ejecuten correctamente, a los activos de AWS se les asigna un propietario y se les realiza un seguimiento y monitoreo con herramientas de administración de inventarios patentadas por AWS. Los servicios de AWS son independientes del contenido, ya que ofrecen el mismo alto nivel de seguridad a todos los clientes, sin importar el tipo de contenido que se almacene. En AWS estamos atentos a la seguridad de nuestros clientes e implementamos sofisticadas medidas técnicas y físicas contra el acceso no autorizado. AWS rastrea, documenta y verifica las acciones de eliminación y desinfección de medios de almacenamiento. Toda la eliminación de medios de almacenamiento está a cargo del personal designado de AWS. AWS clasifica los dispositivos de almacenamiento utilizados para almacenar datos de clientes como críticos y los trata en consecuencia, como de alto impacto, a lo largo de su ciclo de vida. Contamos con estándares exigentes sobre cómo instalar, reparar y, finalmente, destruir los dispositivos cuando ya no son útiles. Cuando un dispositivo de almacenamiento llega al final de su ciclo de vida útil, AWS da de baja los medios mediante técnicas detalladas en NIST 800-88. Los medios que almacenaron datos del cliente se retienen bajo el control de AWS hasta que se hayan retirado de servicio de forma segura. AWS está sujeto a evaluaciones de auditores externos en relación con más de 2.600 requisitos durante todo el año. Cuando los auditores terceros inspeccionan nuestros centros de datos, hacen un análisis profundo para confirmar que seguimos las reglas	

Resumen de los requisitos	Consideraciones	Consideraciones de implementación (Prácticas de Well-Architected)
	establecidas necesarias para obtener nuestras certificaciones de seguridad, que incluyen el retiro de servicio de los medios de almacenamiento. Para obtener más información sobre estos controles, consulte: Controles del centro de datos de AWS.	

Sección Quinta – Del monitoreo, control y continuidad de las operaciones y servicios de Banca Electrónica.

Resumen de los requisitos	Consideraciones	Consideraciones de implementación (Prácticas de Well-Architected)
Artículo 316 Bis 13. Las Instituciones deberán mantener mecanismos de control para la detección y prevención de eventos que se aparten de los parámetros de uso habitual de sus Usuarios. Para tales efectos, las Instituciones podrán: **I.** Solicitar a sus Usuarios la información que estimen necesaria para definir el uso habitual. **II.** Aplicar, bajo su responsabilidad, medidas de prevención en el evento que cuenten con elementos que hagan presumir que el Identificador de Usuario o los Factores de Autenticación no están siendo utilizados por el propio Usuario.	**Responsabilidad compartida** Los clientes son responsables de definir su modelo operativo en función de los servicios de AWS que eligen utilizar. Los cambios en sus entornos se pueden detectar y rastrear mediante servicios de AWS como AWS Config para evaluar y auditar las configuraciones de los recursos de AWS. Los clientes de AWS pueden configurar el registro en toda la carga de trabajo, incluidos los registros de aplicaciones, los registros de recursos y los registros de servicios de AWS. Por ejemplo, asegúrese que AWS CloudTrail, Amazon CloudWatch Logs, Amazon GuardDuty y AWS Security Hub están habilitados para todas las cuentas de su organización. Los clientes de AWS pueden utilizar la automatización para investigar y corregir eventos a fin de reducir el esfuerzo humano y los errores, lo que puede permitirles escalar las capacidades de investigación. Las revisiones periódicas lo ayudarán a ajustar las herramientas de automatización y a iterar de forma continua. Por ejemplo, automatice las respuestas a los eventos mediante la automatización del primer paso de la investigación, luego, repita para eliminar gradualmente el esfuerzo humano con Amazon GuardDuty, un servicio de monitoreo de seguridad continuo que lo ayuda a identificar actividades inesperadas y potencialmente no autorizadas o maliciosas en su entorno de AWS. Los clientes de AWS son responsables de todo el análisis, las pruebas de penetración, el monitoreo de la integridad de los archivos y la detección de intrusiones para sus instancias y aplicaciones de Amazon EC2 y Amazon ECS. Los análisis deben incluir las direcciones IP del cliente, no los puntos de enlace de AWS. Los puntos de enlace de AWS se prueban como parte de los análisis de vulnerabilidades de conformidad de AWS. AWS utiliza una amplia variedad de sistemas de monitoreo automatizados diseñados para detectar actividades y condiciones inusuales o no autorizadas en los puntos de comunicación de entrada y salida. Estas herramientas monitorean el uso de los servidores y la red, las actividades de escaneo de puertos, el uso de las aplicaciones y los intentos de intrusión no autorizados. Las herramientas permiten establecer umbrales de métricas de rendimiento personalizadas para actividades inusuales y las alarmas se configuran para notificar automáticamente al personal de operaciones y administración cuando se cruzan los umbrales de alerta temprana en métricas operativas clave. Las respuestas se realizan de acuerdo con los procesos y procedimientos de respuesta a incidentes. AWS Security realiza exploraciones periódicas de vulnerabilidades en la infraestructura subyacente, la aplicación web y las bases de datos en el entorno de AWS con una variedad	SEC 4 Eventos de seguridad SEC 5 Protección de la red SEC 6 Protección informática REL 6 Monitoreo de los recursos OPS 8 Estado de la carga de trabajo OPS 9 Estado de las operaciones

Resumen de los requisitos	Consideraciones	Consideraciones de implementación (Prácticas de Well-Architected)
	de herramientas. Las evaluaciones de vulnerabilidad externas las realiza un proveedor tercero aprobado por AWS una vez por trimestre como mínimo, y los problemas identificados se investigan y se rastrean hasta su resolución. Las vulnerabilidades identificadas se monitorean y evalúan y se diseñan, implementan y ejecutan contramedidas para compensar las vulnerabilidades conocidas y las recién identificadas. Los equipos de AWS Security también se suscriben a fuentes de noticias para detectar errores aplicables de proveedores y monitorean de manera proactiva los sitios web de los proveedores y otros medios relevantes en busca de nuevos parches. Los clientes de AWS también tienen la capacidad de informar sobre problemas a AWS a través del sitio web de Informe de vulnerabilidades de AWS.	
Artículo 316 Bis 14. Mantener en bases de datos todas las operaciones efectuadas a través del servicio de Banca Electrónica que no sean reconocidas por sus Usuarios. La información anterior deberá mantenerse en la Institución durante un periodo no menor a cinco años contado a partir de su registro.	**Responsabilidad de los clientes** Los clientes conservan la propiedad y el control de su contenido y ciclo de vida cuando utilizan los servicios de AWS y no los ceden a AWS. Los clientes de AWS tienen control total sobre qué servicios utilizan y a quién autorizan para acceder a su contenido y servicios, incluidas las credenciales necesarias. Los clientes controlan cómo configuran sus entornos y protegen su contenido, incluso si cifran su contenido (en reposo y en tránsito) y qué otras características y herramientas de seguridad utilizan y cómo las usan.	REL 6 Monitoreo de los recursos REL 9 Copia de seguridad de datos SEC 10 Respuesta ante incidentes OPS 4 Diseñar para la información de la carga de trabajo
Artículo 316 Bis 19 Las Instituciones deberán procurar la operación continua de la infraestructura de cómputo y de telecomunicaciones, así como dar pronta solución, para restaurar el servicio de Banca Electrónica, en caso de presentarse algún incidente. Las incidencias deberán informarse a los Comités de Auditoría y de Riesgos de la Institución.	**Responsabilidad de los clientes** Los clientes de AWS pueden aprovechar las características de la infraestructura de AWS y los servicios de AWS para cumplir con una amplia gama de objetivos de resiliencia. Los clientes pueden optar por utilizar varias regiones para operar cargas de trabajo que requieren alta disponibilidad. También pueden mitigar los riesgos de interrupciones físicas a gran escala mediante el uso de varias regiones. Las regiones de AWS están diseñadas para ser autónomas y se implementan copias dedicadas de los servicios en cada región. Las arquitecturas más resistentes utilizan varias regiones de AWS. El uso de varias zonas de disponibilidad, incluso dentro de una sola región, puede mejorar la resiliencia en comparación con un entorno en las instalaciones. Las zonas de disponibilidad están diseñadas para mitigar el riesgo de desastres naturales y otras interrupciones que puedan ocurrir. Las zonas de disponibilidad están físicamente separadas dentro de una región metropolitana y se encuentran en diferentes llanuras aluviales. Cada zona de disponibilidad también está diseñada como una zona de error independiente y los procesos automatizados alejan el tráfico de clientes del área afectada en caso de error.	OPS 1 Prioridades en las operaciones OPS 4 Diseñar para la información de la carga de trabajo OPS 8 Estado de la carga de trabajo OPS 9 Estado de las operaciones REL 6 Monitoreo de los recursos REL 9 Copia de seguridad de datos REL 10 Aislamiento de errores REL 11 Implementación de resiliencia REL 12 Pruebas de fiabilidad REL 13 Recuperación de desastres PERF 7 Monitoreo del rendimiento

Resumen de los requisitos	Consideraciones	Consideraciones de implementación (Prácticas de Well-Architected)
	Los clientes pueden lograr objetivos de puntos de recuperación y tiempos de recuperación extremadamente altos mediante el uso de múltiples zonas de disponibilidad y replicación de datos. Para obtener más información sobre estos temas, los clientes pueden descargar Abordaje de Amazon Web Services a la resiliencia operativa en el sector financiero y en otros y Recuperación de desastres de cargas de trabajo en AWS: recuperación en la nube.	
Artículo 316 Bis 21 Las Instituciones deberán implementar las acciones correctivas que la Comisión les requiera, como resultado de la identificación de riesgos asociados con el uso de los servicios de Banca Electrónica.	**Responsabilidad compartida** Los clientes son responsables de definir su modelo operativo en función de los servicios de AWS. En el lado de AWS del Modelo de responsabilidad compartida, AWS realiza un proceso continuo de evaluación de riesgos para identificar, evaluar y mitigar los riesgos en toda la empresa. El proceso implica desarrollar e implementar planes de tratamiento de riesgos para mitigar los riesgos según sea necesario. El equipo de administración de riesgos de AWS monitorea y escala los riesgos de manera continua, realizando evaluaciones de riesgos en los controles recién implementados al menos cada seis meses. AWS revisa y corrige los problemas con regularidad para abordar los problemas. Se identifica la siguiente información para cualquier problema que afecte el entorno de control de AWS: • Detalles del problema identificado • Causa • Controles compensatorios • Severidad • Propietario • Camino hacia adelante a corto plazo • Camino hacia adelante a largo plazo Dependiendo de la naturaleza y gravedad de los problemas, los registros de las acciones correctivas implementadas pueden revisarse durante una reunión del equipo de liderazgo de AWS programada regularmente.	OPS 4 Diseñar para la información de la carga de trabajo OPS 8 Estado de la carga de trabajo OPS 9 Estado de las operaciones OPS 10 Respuesta a eventos OPS 11 Progreso de las operaciones SEC 4 Eventos de seguridad SEC 10 Respuesta ante incidentes PERF 7 Monitoreo del rendimiento

Resumen de los requisitos	Consideraciones	Consideraciones de implementación (Prácticas de Well-Architected)
Artículo 316 Bis 22 En caso de catástrofes naturales u otras situaciones que afecten las operaciones y servicios bancarios, la Comisión podrá autorizar a las Instituciones a prestar servicios de Banca Electrónica en términos distintos.	**Responsabilidad de los clientes** Los clientes de AWS pueden aprovechar las características de la infraestructura de AWS y los servicios de AWS para cumplir con una amplia gama de objetivos de resiliencia. El uso de varias zonas de disponibilidad, incluso dentro de una sola región, puede mejorar la resiliencia en comparación con un entorno en las instalaciones. El uso de varias regiones aumenta aún más la resiliencia. Las zonas de disponibilidad están diseñadas para mitigar el riesgo de desastres naturales y otras interrupciones que puedan ocurrir. Las zonas de disponibilidad están físicamente separadas dentro de una región metropolitana y se encuentran en diferentes llanuras aluviales. Cada zona de disponibilidad también está diseñada como una zona de error independiente y los procesos automatizados alejan el tráfico de clientes del área afectada en caso de error. Los clientes pueden lograr objetivos de puntos de recuperación y tiempos de recuperación extremadamente altos mediante el uso de múltiples zonas de disponibilidad y replicación de datos. Las arquitecturas más resistentes utilizan varias regiones de AWS. Las regiones de AWS proporcionan una mayor separación geográfica que el uso de una sola región. Las regiones de AWS están diseñadas para ser autónomas y se implementan copias dedicadas de los servicios en cada región. Los clientes de AWS pueden utilizar varias regiones para operar cargas de trabajo que requieren alta disponibilidad. También pueden mitigar los riesgos de interrupciones físicas a gran escala mediante el uso de varias regiones. Los servicios de AWS permiten que los clientes exporten contenido bajo demanda, mediante la consola de administración de AWS, las APIs y otros métodos de entrada. Por ejemplo, AWS Snowball proporciona dispositivos diseñados para ser seguros durante la transferencia de entrada y salida a la nube de AWS de grandes cantidades de datos. Para obtener más información sobre la migración de datos dentro de la nube de AWS y fuera de ésta, consulte: Migración y transferencia en AWS.	No aplicable.

Título Segundo - Disposiciones Prudenciales - Capítulo VI – Controles Internos.

Sección Sexta – De la Dirección General.

Requisito	Consideraciones	Consideraciones de implementación (Prácticas de Well-Architected)
Artículos 164. IV, f, and 164 Bis. Implementar, los mecanismos necesarios para dar cumplimiento a lo autorizado al amparo del Artículo 46 Bis de la Ley, sin poner en riesgo el valor económico de la Institución, la confidencialidad de la información y la continuidad de sus operaciones. La Dirección General deberá elaborar el Plan de Continuidad de Negocio. **I.** La implementación, continua actualización y difusión del plan al interior de la Institución. **II.** Diseñar y llevar a cabo una política de comunicación respecto de la verificación de Contingencias Operativas, la cual deberá ser parte del Plan de Continuidad de Negocio. Dicha política deberá prever la comunicación oportuna. **III.** Hacer del conocimiento de la Comisión las Contingencias Operativa.	**Responsabilidad compartida** Los clientes son responsables de implementar adecuadamente la planificación de contingencias, la formación y las pruebas para sus sistemas alojados en AWS. AWS brinda a los clientes la capacidad de implementar un plan de continuidad sólido, que incluye la utilización de copias de seguridad frecuentes de instancias de servidor, replicación de redundancia de datos y la flexibilidad para colocar instancias y almacenar datos dentro de múltiples regiones geográficas, así como en varias zonas de disponibilidad dentro de cada región. En caso de un error, los procesos automatizados alejan el tráfico de datos del cliente del área afectada. Cada zona de disponibilidad está diseñada como una zona con independencia ante los errores. Esto significa que las zonas de disponibilidad suelen estar físicamente separadas dentro de una región metropolitana y se encuentran en diferentes llanuras aluviales. Los clientes también pueden utilizar AWS para permitir una recuperación de desastres más rápida de sus sistemas de TI críticos sin incurrir en el gasto de infraestructura de un segundo sitio físico. La nube de AWS es compatible con muchas arquitecturas populares de *Disaster Recovery* (recuperación de desastres, DR), desde entornos de “luz piloto” que están listos para escalar en cualquier momento hasta entornos de “espera activa”, que permiten una conmutación por error rápida. La infraestructura de AWS tiene un alto nivel de disponibilidad y ofrece a los clientes las características necesarias para implementar una arquitectura de TI resiliente. Los sistemas de AWS se han diseñado para tolerar errores en el sistema o el hardware con un nivel de impacto mínimo sobre el cliente. Además de contar con una fuente de alimentación ininterrumpida (UPS) e instalaciones de generación de energía de respaldo en el sitio, las zonas de disponibilidad de AWS se alimentan a través de diferentes redes correspondientes a servicios independientes para reducir aún más la posibilidad de errores en componentes individuales. Todas las zonas de disponibilidad están conectadas de forma redundante a varios proveedores de tránsito de datos de nivel 1.	No aplicable.

Además, el plan de continuidad empresarial de AWS detalla el proceso que sigue AWS en caso de una interrupción, desde la detección hasta la desactivación. Este plan está diseñado para recuperar y reconstituir AWS mediante un enfoque de tres fases: fase de activación y notificación, fase de recuperación y fase de reconstitución.

Este enfoque ayuda a AWS a realizar los esfuerzos de recuperación y reconstitución del sistema en una secuencia metódica, con el objetivo de maximizar la efectividad de los esfuerzos de recuperación y reconstitución y minimizar el tiempo de interrupción del sistema debido a errores y omisiones.

AWS prueba el plan de continuidad empresarial y sus procedimientos asociados al menos una vez al año para garantizar su eficacia y la preparación de la organización para ejecutarlo.

Además, como parte del modelo de responsabilidad de seguridad compartida, tanto los clientes de AWS como AWS deben monitorear los eventos de seguridad.

Los clientes de AWS pueden usar herramientas como AWS CloudTrail, Amazon CloudWatch, AWS Config, Amazon GuardDuty, Security Hub y AWS Config Rules para rastrear, monitorear, analizar y auditar eventos. Si estas herramientas identifican un evento que se analiza y se determina que es un incidente, ese “evento de calificación” generará un incidente y activará el proceso de administración de incidentes y las acciones de respuesta apropiadas necesarias para mitigarlo.

AWS ha implementado una política y un programa de respuesta a incidentes documentados y formales, que se pueden revisar en el informe SOC 2. Los clientes también pueden ver todas las notificaciones de seguridad a través del AWS Personal Health Dashboard.

AWS configura el monitoreo y las alarmas para identificar y notificar al personal operativo y de administración sobre incidentes cuando se cruzan los umbrales de alerta temprana en métricas operativas clave.

AWS requiere que el equipo de seguridad o de servicio afectado realice una evaluación luego del incidente para determinar su causa, así como para documentar las lecciones aprendidas.

Para obtener más información sobre estos temas, los clientes pueden descargar Abordaje de Amazon Web Services a la resiliencia operativa en el sector financiero y en otros y Recuperación de desastres de cargas de trabajo en AWS: recuperación en la nube.

ANEXO 67 – Requerimientos mínimos del Plan de Continuidad de Negocio.

Requisito	Consideraciones	Consideraciones de implementación (Prácticas de Well-Architected)
Las Instituciones, previo al desarrollo del Plan de Continuidad de Negocio deberán llevar a cabo un análisis de impacto al negocio: **a)** Identifique los procesos críticos que se consideran indispensables para la continuidad de las operaciones. **b)** Determine los recursos mínimos necesarios para mantener y restablecer los servicios. **c)** Elabore escenarios relevantes relativos a la verificación de posibles Contingencias Operativas, tales como: i. Desastres naturales y ambientales. ii. Enfermedades infecciosas. iii. Ataques cibernéticos o a la actividad informática. iv. Sabotajes. v. Terrorismo. vi. Interrupciones en el suministro de energía. vii. Fallas o indisponibilidad en la infraestructura tecnológica (telecomunicaciones, procesamiento de información y redes). viii. Indisponibilidad de recursos humanos, materiales o técnicos.	**Responsabilidad compartida** Los clientes son responsables de implementar adecuadamente la planificación de contingencias, la formación y las pruebas para sus sistemas alojados en AWS. AWS brinda a los clientes la capacidad de implementar un plan de continuidad sólido, que incluye la utilización de copias de seguridad frecuentes de instancias de servidor, replicación de redundancia de datos y la flexibilidad para colocar instancias y almacenar datos dentro de múltiples regiones geográficas, así como en varias zonas de disponibilidad dentro de cada región. En caso de un error, los procesos automatizados alejan el tráfico de datos del cliente del área afectada. Cada zona de disponibilidad está diseñada como una zona con independencia ante los errores. Esto significa que las zonas de disponibilidad suelen estar físicamente separadas dentro de una región metropolitana y se encuentran en diferentes llanuras aluviales. Los clientes también pueden utilizar AWS para permitir una recuperación de desastres más rápida de sus sistemas de TI críticos sin incurrir en el gasto de infraestructura de un segundo sitio físico. La nube de AWS es compatible con muchas arquitecturas populares de *Disaster Recovery* (recuperación de desastres, DR), desde entornos de “luz piloto” que están listos para escalar en cualquier momento hasta entornos de “espera activa”, que permiten una conmutación por error rápida. La infraestructura de AWS tiene un alto nivel de disponibilidad y ofrece a los clientes las características necesarias para implementar una arquitectura de TI resiliente. Los sistemas de AWS se han diseñado para tolerar errores en el sistema o el hardware con un nivel de impacto mínimo sobre el cliente. Además de contar con una fuente de alimentación ininterrumpida (UPS) e instalaciones de generación de energía de respaldo en el sitio, las zonas de disponibilidad de AWS se alimentan a través de diferentes redes correspondientes a servicios independientes para reducir aún más la posibilidad de errores en componentes individuales. Todas las zonas de disponibilidad están conectadas de forma redundante a varios proveedores de tránsito de datos de nivel 1. Además, el plan de continuidad empresarial de AWS detalla el proceso que sigue AWS en caso de una interrupción, desde la detección hasta la desactivación. Este plan está	OPS 1 Prioridades en las operaciones OPS 2 Modelo operativo REL 10 Aislamiento de errores REL 13 Recuperación de desastres

Requisito	Consideraciones	Consideraciones de implementación (Prácticas de Well-Architected)
ix. Interrupciones ocurridas en servicios prestados por terceros. **d)** Estime los impactos cuantitativos y cualitativos de las Contingencias Operativas. **e)** Defina la prioridad de recuperación. **f)** Determine el tiempo objetivo de recuperación. **g)** Establezca el punto objetivo de recuperación. **h)** Identifique y evalúe los riesgos relacionados con los procesos operativos y servicios. **i)** Determine los riesgos derivados de la ubicación geográfica de los centros principales de procesamiento de datos.	diseñado para recuperar y reconstituir AWS mediante un enfoque de tres fases: fase de activación y notificación, fase de recuperación y fase de reconstitución. Este enfoque ayuda a AWS a realizar los esfuerzos de recuperación y reconstitución del sistema en una secuencia metódica, con el objetivo de maximizar la efectividad de los esfuerzos de recuperación y reconstitución y minimizar el tiempo de interrupción del sistema debido a errores y omisiones. AWS prueba el plan de continuidad empresarial y sus procedimientos asociados al menos una vez al año para garantizar su eficacia y la preparación de la organización para ejecutarlo. Además, como parte del modelo de responsabilidad de seguridad compartida, tanto los clientes de AWS como AWS deben monitorear los eventos de seguridad. Los clientes de AWS pueden usar herramientas como AWS CloudTrail, Amazon CloudWatch, AWS Config, Amazon GuardDuty, Security Hub y AWS Config Rules para rastrear, monitorear, analizar y auditar eventos. Si estas herramientas identifican un evento que se analiza y se determina que es un incidente, ese "evento de calificación" generará un incidente y activará el proceso de administración de incidentes y las acciones de respuesta apropiadas necesarias para mitigarlo. AWS ha implementado una política y un programa de respuesta a incidentes documentados y formales, que se pueden revisar en el informe SOC 2. Los clientes también pueden ver todas las notificaciones de seguridad a través del AWS Personal Health Dashboard. AWS configura el monitoreo y las alarmas para identificar y notificar al personal operativo y de administración sobre incidentes cuando se cruzan los umbrales de alerta temprana en métricas operativas clave. AWS requiere que el equipo de seguridad o de servicio afectado realice una evaluación luego del incidente para determinar su causa, así como para documentar las lecciones aprendidas. Para obtener más información sobre estos temas, los clientes pueden descargar Abordaje de Amazon Web Services a la resiliencia operativa en el sector financiero y en otros y Recuperación de desastres de cargas de trabajo en AWS: recuperación en la nube.	
II. En el desarrollo del Plan de Continuidad de Negocio, las	**Responsabilidad compartida** Los clientes son responsables de implementar adecuadamente la planificación de contingencias, la formación y las pruebas para sus sistemas alojados en AWS.	REL 11 Implementación de resiliencia REL 12 Pruebas de fiabilidad OPS 11 Progreso de las operaciones

Requisito	Consideraciones	Consideraciones de implementación (Prácticas de Well-Architected)
Instituciones deberán incorporar las siguientes estrategias: **a) De prevención** **i.** Reducir la vulnerabilidad de los procesos y servicios de la institución. **ii.** Disposición de los recursos humanos, financieros, materiales, técnicos y de infraestructura tecnológica. **iii** El establecimiento de un programa de pruebas del funcionamiento y suficiencia del Plan de Continuidad de Negocios. **iv.** El programa de capacitación a que hace referencia la fracción I del Artículo 164. **v.** La política de comunicación a que hace referencia la fracción II del Artículo 164 bis. **vi.** Procedimientos de registro, atención, seguimiento y difusión al personal relevante de los hallazgos, incidencias u observaciones resultantes de las pruebas efectuadas al Plan de Continuidad de Negocios **b) De contingencia:** **i.** Identificar oportunamente la naturaleza de las Contingencias Operativas que afecten los procesos críticos de la Institución.	AWS brinda a los clientes la capacidad de implementar un plan de continuidad robusto, que incluye la utilización de copias de seguridad frecuentes de instancias de servidor, replicación de redundancia de datos y la flexibilidad para colocar instancias y almacenar datos dentro de múltiples regiones geográficas, así como en varias zonas de disponibilidad dentro de cada región. En caso de un error, los procesos automatizados alejan el tráfico de datos del cliente del área afectada. Cada zona de disponibilidad está diseñada como una zona con independencia ante los errores. Esto significa que las zonas de disponibilidad suelen estar físicamente separadas dentro de una región metropolitana y se encuentran en diferentes llanuras aluviales. Los clientes también pueden utilizar AWS para permitir una recuperación de desastres más rápida de sus sistemas de TI críticos sin incurrir en el gasto de infraestructura de un segundo sitio físico. La nube de AWS es compatible con muchas arquitecturas populares de *Disaster Recovery* (recuperación de desastres, DR), desde entornos de “luz piloto” que están listos para escalar en cualquier momento hasta entornos de “espera activa”, que permiten una conmutación por error rápida. La infraestructura de AWS tiene un alto nivel de disponibilidad y ofrece a los clientes las características necesarias para implementar una arquitectura de TI resiliente. Los sistemas de AWS se han diseñado para tolerar errores en el sistema o el hardware con un nivel de impacto mínimo sobre el cliente. Además de contar con una fuente de alimentación ininterrumpida (UPS) e instalaciones de generación de energía de respaldo en el sitio, las zonas de disponibilidad de AWS se alimentan a través de diferentes redes correspondientes a servicios independientes para reducir aun más la posibilidad de errores en componentes individuales. Todas las zonas de disponibilidad están conectadas de forma redundante a varios proveedores de tránsito de nivel 1. Además, el plan de continuidad empresarial de AWS detalla el proceso que sigue AWS en caso de una interrupción, desde la detección hasta la desactivación. Este plan está diseñado para recuperar y reconstituir AWS mediante un enfoque de tres fases: fase de activación y notificación, fase de recuperación y fase de reconstitución. Este enfoque ayuda a AWS a realizar los esfuerzos de recuperación y reconstitución del sistema en una secuencia metódica, con el objetivo de maximizar la efectividad de los esfuerzos de recuperación y reconstitución y minimizar el tiempo de interrupción del sistema debido a errores y omisiones.	

Requisito	Consideraciones	Consideraciones de implementación (Prácticas de Well-Architected)
ii. Contener los efectos de Contingencias Operativas sobre los procesos críticos. **c) Restauración**. **d) Evaluación**.	AWS prueba el plan de continuidad empresarial y sus procedimientos asociados al menos una vez al año para garantizar su eficacia y la preparación de la organización para ejecutarlo. Además, como parte del modelo de responsabilidad de seguridad compartida, tanto los clientes de AWS como AWS deben monitorear los eventos de seguridad. Los clientes de AWS pueden usar herramientas como AWS CloudTrail, Amazon Cloud Watch, AWS Config, Amazon GuardDuty, Security Hub y AWS Config Rules para rastrear, monitorear, analizar y auditar eventos. Si estas herramientas identifican un evento que se analiza y se determina que es un incidente, ese "evento de calificación" generará un incidente y activará el proceso de administración de incidentes y las acciones de respuesta apropiadas necesarias para mitigarlo. AWS ha implementado una política y un programa de respuesta a incidentes documentados y formales, que se pueden revisar en el informe SOC 2. Los clientes también pueden ver todas las notificaciones de seguridad a través de AWS Personal Health Dashboard. AWS configura el monitoreo y las alarmas para identificar y notificar al personal operativo y de administración sobre incidentes cuando se cruzan los umbrales de alerta temprana en métricas operativas clave. AWS requiere que el equipo de seguridad o de servicio afectado realice una evaluación luego del incidente para determinar su causa, así como para documentar las lecciones aprendidas. Para obtener más información sobre estos temas, los clientes pueden descargar Abordaje de Amazon Web Services a la resiliencia operativa en el sector financiero y en otros y Recuperación de desastres de cargas de trabajo en AWS: recuperación en la nube.	
Las instituciones, al definir las diferentes acciones y procedimientos a que hace referencia la presente fracción, deberán en todo momento determinar de manera clara el personal responsable, así como prever lo relativo a su suplencia o sustitución.	**Responsabilidad de los clientes** Los clientes de AWS tienen la responsabilidad de definir los roles y las responsabilidades de sus procesos.	No aplicable.

Sección Octava Bis – De la seguridad de la información.

Resumen de los requisitos	Consideraciones	Consideraciones de implementación (Prácticas de Well-Architected)
Las Instituciones de Crédito deben proteger la integridad y disponibilidad de la infraestructura tecnológica y la confidencialidad de los datos.	**Responsabilidad compartida** Lea nuestra respuesta al Artículo 168 Bis 11 más abajo.	No aplicable.
Artículo 168 Bis 11. El director general de la Institución será responsable de la implementación del Sistema de Control Interno en materia de seguridad de la información que procure su confidencialidad, integridad y disponibilidad.	**Responsabilidad compartida** Los clientes pueden validar los controles de seguridad implementados dentro del entorno de AWS a través de certificaciones e informes de AWS, como los informes de AWS Service Organization Control (SOC) 1, 2 y 3, las certificaciones ISO 27001, 27017 y 27018 y los informes de conformidad con PCI DSS. Estos informes y certificaciones son elaborados por auditores terceros independientes y dan fe del diseño y la eficacia operativa de los controles de seguridad de AWS. Los clientes pueden revisar y descargar informes y detalles sobre más de 2600 controles de seguridad mediante AWS Artifact, el portal de informes de conformidad automatizado disponible en la consola de administración de AWS. El portal de AWS Artifact proporciona acceso bajo demanda a los documentos de seguridad y conformidad de AWS, incluidos los informes SOC, los informes de PCI y las certificaciones de los organismos de acreditación en distintas regiones geográficas y verticales de conformidad. Hay cuatro informes SOC de AWS disponibles para los clientes de AWS desde AWS Artifact: • Informe SOC 1 de AWS • Informe de seguridad, disponibilidad y confidencialidad SOC 2 de AWS • Informe tipo I de privacidad SOC 2 de AWS • Informe de seguridad, disponibilidad y confidencialidad SOC 3 de AWS, disponible públicamente como documento técnico. Las auditorías internas y externas de AWS se planifican y realizan de acuerdo con el programa de auditoría documentado para revisar el rendimiento continuo de AWS en comparación con los criterios basados en estándares y para identificar oportunidades de mejora general. Los criterios basados en estándares incluyen, entre otros, la ISO/IEC 27001, AT 801 (anteriormente Declaración de Estándares para Compromisos de	No aplicable.

Resumen de los requisitos	Consideraciones	Consideraciones de implementación (Prácticas de Well-Architected)
	Atestación [SSAE] 16) del Instituto Norteamericano de Contadores Públicos Certificados (AICPA) y los Estándares Internacionales para Compromisos de Aseguramiento de Normas profesionales n.° 3402 (ISAE 3402).	
Art. 168 Bis 16. **I.** Prever lo necesario para hacer del conocimiento de la Comisión de forma inmediata los Incidentes de Seguridad de la Información. **II.** Llevar a cabo una investigación inmediata sobre las causas que generaron el Incidente de Seguridad de la Información, establecer un plan de trabajo, y enviarse a la Comisión en un plazo no mayor a 15 días hábiles.	**Responsabilidad de los clientes** Los clientes de AWS son responsables de cumplir con estos requisitos de la CNBV con respecto a los incidentes de seguridad de la información.	No aplicable.
Artículo 168 Bis 17. Las Instituciones deberán llevar un registro en bases de datos, de los incidentes, fallas o vulnerabilidades detectadas en la Infraestructura Tecnológica. La información deberá conservarse por, al menos, 10 años.	**Responsabilidad de los clientes** Los clientes de AWS son responsables de cumplir con estos requisitos de la CNBV con respecto a los incidentes de seguridad de la información.	No aplicable.