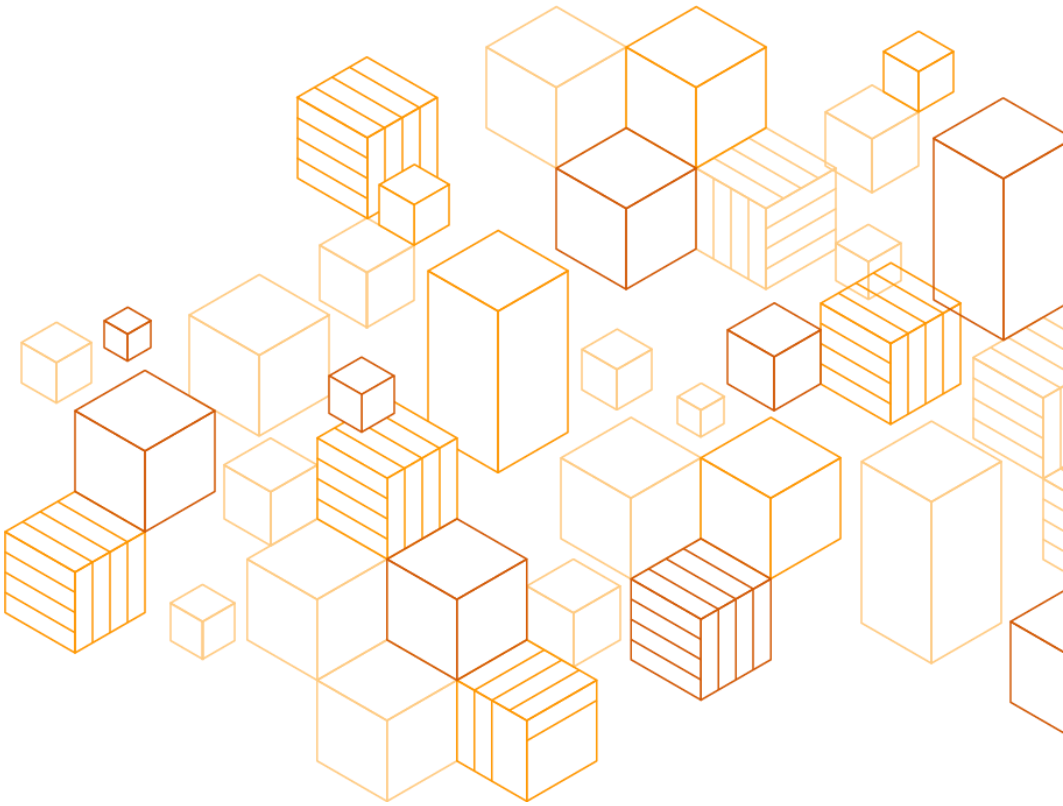
Guía de usuario de AWS para las regulaciones de servicios financieros en Argentina

Comunicaciones "A" *6.354 y 6.375*
del Banco Central de la República Argentina (BCRA)

Agosto de 2020



Notas

Los clientes son responsables de realizar su propia evaluación independiente de la información en este documento. Este documento: (a) es para propósitos informativos solamente, (b) representa la oferta actual de productos y prácticas de AWS, las cuales están sujetas a cambios sin previo aviso, y (c) no crea ningún compromiso ni aseguramiento de parte de AWS, sus afiliados, proveedores y licenciantes. Los productos o servicios de AWS se proveen “tal como son”, sin garantías, representaciones, ni condiciones de ningún tipo, ya sean explícitas o implícitas. Las responsabilidades y obligaciones de AWS respecto a sus clientes están controladas por acuerdos de AWS y este documento no forma parte, ni modifica, ningún acuerdo entre AWS y sus clientes.

Contenidos

Acerca De Esta Guía

Este documento provee información para apoyar a bancos e instituciones de servicios financieros en Argentina regulados por el Banco Central de la República Argentina (BCRA) a medida que adoptan y aceleran su uso de la nube de Amazon Web Services (AWS).

Esta guía:

- describe los respectivos roles que ejercen tanto el cliente como AWS al manejar y asegurar el entorno en la nube;
- presenta un panorama general de los requisitos regulatorios y la orientación del BCRA que las instituciones financieras pueden tener en cuenta al utilizar AWS;
- provee recursos adicionales que las instituciones financieras pueden usar para diseñar y construir sus entornos de AWS para asegurar y cumplir con las expectativas regulatorias incluidas dentro de las Normativas del BCRA.

Perspectiva General

AWS ofrece a las instituciones de servicios financieros, ya sean bancos, medios de pago, mercados de capitales o seguros, una infraestructura en la nube global resistente y segura. A su vez, ofrece los servicios que estas instituciones necesitan para diferenciarse hoy y adaptarse a las necesidades del mañana. Mediante la innovación continua, AWS cumple con estrictos requisitos de seguridad, ofreciendo una gama de servicios amplia y profunda, con una gran experiencia en la industria y una extensa red de socios. Construir sobre AWS les permite a las organizaciones modernizar su infraestructura, cumplir con los rápidos cambios de comportamiento y expectativas de los usuarios e impulsar el crecimiento empresarial. AWS ofrece servicios de TI en categorías que van desde la capacidad informática, almacenamiento, bases de datos y redes, hasta la inteligencia artificial y el aprendizaje automático. Alrededor del mundo, las instituciones financieras han utilizado los servicios de AWS para crear sus propias aplicaciones para banca móvil, presentación de informes reglamentarios y análisis de mercado.

El Banco Central de la República Argentina (BCRA) es la autoridad principal de supervisión financiera en Argentina, responsable de la regulación, inspección y supervisión de las instituciones financieras, incluidas las instituciones bancarias y de crédito y procesadores de pagos (en conjunto, instituciones financieras o entidades reguladas).

En noviembre de 2017, el BCRA emitió la Comunicación “A” 6354 (enmendada por la Comunicación “A” 6375) para actualizar las normas generales de tercerización que las instituciones financieras reguladas por el BCRA deben seguir cuando tercerizan servicios de tecnología de la información (TI) a un proveedor de tecnología externo, incluyendo la utilización de servicios en la nube (las “Normativas del BCRA”). Adicionalmente, el BCRA ha publicado directrices regulatorias a través de varias Interpretaciones Normativas públicas disponibles en su sitio web. Estas Interpretaciones Normativas han clarificado el alcance de las Normativas del BCRA con respecto a la tercerización de las instituciones financieras a los proveedores de servicios en la nube (CSPs por sus siglas en inglés).

Las Normativas del BCRA definen, entre otros aspectos, los requisitos técnicos y operativos mínimos que las instituciones financieras deben establecer para la gestión, la aplicación y el control de riesgos relacionados con tecnología de la información, sistemas de información y otros recursos cuando se tercerizan servicios de TI a un proveedor de servicios externo, incluyendo el uso de servicios en la nube.

Esta guía es un recurso para que las instituciones financieras puedan comprender esos requisitos técnicos y operativos incluidos en las Normativas del BCRA cuando hagan uso de los servicios de AWS. Asimismo, se describe el marco de cumplimiento de AWS y las herramientas avanzadas y medidas de seguridad que las instituciones financieras pueden utilizar para evaluar, cumplir y demostrar el cumplimiento de sus requisitos regulatorios que les sean aplicables según las Normativas del BCRA.

Un análisis completo de las Normativas del BCRA está por fuera del alcance de esta guía. Sin embargo, en las secciones que aparecen a continuación, se abordarán las consideraciones que surgen con mayor frecuencia en las interacciones con instituciones financieras en Argentina, y se proporcionará información que instituciones financieras pueden utilizar para comprender mejor sus responsabilidades y las de AWS en relación con las Normativas del BCRA:

- **Seguridad y responsabilidad compartida**: es importante que las instituciones financieras comprendan el Modelo de Responsabilidad Compartida de AWS antes de adentrarse en los requisitos técnicos y operativos específicos esbozados en las Normativas del BCRA. El Modelo de Responsabilidad compartida de AWS es fundamental para comprender las funciones respectivas del cliente y de AWS para la seguridad, e informa sobre las medidas que deben tomar las instituciones financieras para asegurarse que cumplen con las Normativas del BCRA.
- **Programas de cumplimiento de AWS:** AWS ha obtenido certificaciones y atestaciones de terceros para una variedad de tareas específicas de la industria. AWS también ha desarrollado programas de cumplimiento para poner estos recursos a disposición de sus clientes. El BCRA ha reconocido en varias Interpretaciones Normativas que las entidades reguladas pueden basarse en informes de auditoría, certificaciones y otros mecanismos de terceros para monitorear y auditar los servicios tercerizados a un CSP. Los clientes pueden aprovechar los programas de cumplimiento de AWS para ayudar a satisfacer sus requisitos regulatorios.
- **Infraestructura de nube global de AWS**: la Infraestructura de Nube Global de AWS comprende las regiones de AWS y sus zonas de disponibilidad. La Infraestructura de Nube Global de AWS ofrece a los clientes de AWS una forma más fácil y efectiva para diseñar y operar aplicaciones y bases de datos, haciéndolas más accesibles, tolerantes a fallos y escalables que los entornos locales (on-premises) tradicionales. Los clientes de AWS pueden utilizar la Infraestructura de Nube Global de AWS para diseñar un entorno en AWS congruente con su negocio y sus necesidades regulatorias, incluyendo cualquier requisito aplicable según las Normativas del BCRA.
- **Normativas del BCRA**: esta sección explica las consideraciones comunes para las instituciones financieras que utilizan AWS, ya que describe algunos de los requisitos técnicos y operativos clave según las Normativas del BCRA. Asimismo, describe la manera en que las instituciones financieras pueden aprovechar los servicios y herramientas de AWS para cumplir con sus requisitos regulatorios aplicables. El Apéndice: Consideraciones de AWS acerca de los requisitos técnico-operativos en las Normativas del BCRA proporciona una lista de los requisitos y las consideraciones respectivas.

Seguridad y Responsabilidad Compartida

Es importante que las instituciones financieras comprendan el Modelo de Responsabilidad Compartida de AWS antes de explorar los requisitos específicos según las Normativas del BCRA. La seguridad de la nube es una responsabilidad compartida. Si bien AWS gestiona la seguridad de la nube, al asegurarse de que la infraestructura de la nube de AWS cumpla con los requisitos regulatorios y las prácticas recomendadas a nivel mundial y regional, la seguridad en la nube es responsabilidad del cliente. Esto significa que los clientes conservan el control del programa de seguridad que deciden implementar para proteger su propio contenido, sus propias aplicaciones, sistemas y redes tal como lo harían con las aplicaciones en un centro de datos local (on-premises).

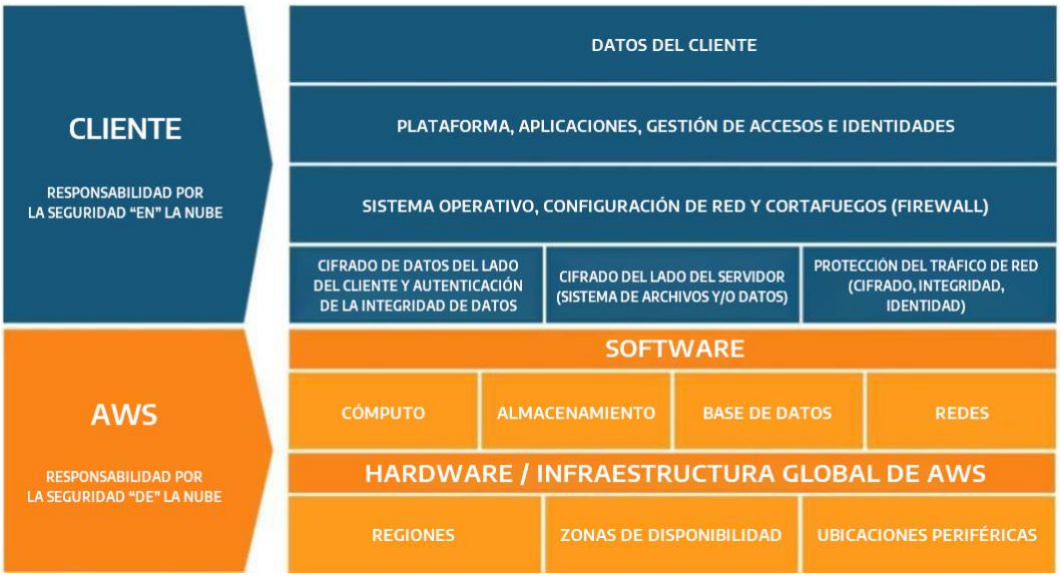


Figura 1: Modelo de Responsabilidad Compartida

El Modelo de Responsabilidad Compartida es fundamental para comprender los respectivos roles del cliente y de AWS en el contexto de los principios de la seguridad de la nube. AWS opera, administra y controla los componentes de TI desde el sistema operativo anfitrión (host) y la capa de virtualización hasta la seguridad física de las instalaciones en las que funcionan los servicios.

Seguridad en la nube

Los clientes son responsables de su seguridad en la nube. Los clientes de AWS son responsables de administrar el sistema operativo invitado (incluyendo la instalación de actualizaciones y parches de seguridad) y otro software de aplicación asociado, así como cualquier control de seguridad de la red aplicable. Los clientes deben pensar detenidamente en los servicios que eligen, ya que las responsabilidades varían en función de los servicios que utilicen, de la integración de estos en sus entornos de TI y de la legislación y las

regulaciones correspondientes. Es importante señalar que, al utilizar los servicios de AWS, los clientes mantienen el control sobre su contenido y son responsables de la gestión de los requisitos de seguridad del contenido crítico, incluyendo:

- El contenido que eligen almacenar en AWS.
- Los servicios de AWS que se utilizan con el contenido.
- El país donde se almacena su contenido.
- El formato y la estructura de su contenido y si está oculto, anonimizado o cifrado.
- La forma en que se codifican o cifran sus datos y dónde se almacenan las claves.
- La decisión de quién tiene acceso a su contenido y cómo se conceden, administran y revocan esos derechos de acceso.

Debido a que los clientes, en lugar de AWS, controlan estos factores importantes, los clientes mantienen la responsabilidad por sus elecciones. La responsabilidad del cliente se determinará por los servicios de la nube de AWS que el cliente elija. Esto determina la cantidad de trabajo de configuración que debe llevar a cabo el cliente como parte de sus responsabilidades de seguridad. Por ejemplo, un servicio como Amazon Elastic Compute Cloud (Amazon EC2) se clasifica como Infraestructura como un Servicio (IaaS por sus siglas en inglés) y, de tal forma, requiere que el cliente realice todas las tareas de configuración y gestión de seguridad necesarias. Los clientes que hacen uso una instancia de Amazon EC2 son responsables de la gestión del sistema operativo invitado (guest) (incluidas las actualizaciones y los parches de seguridad), de cualquier software o funcionalidades de aplicación instaladas por el cliente en las instancias, y de la configuración del cortafuego (firewall) proporcionado por AWS (llamado grupo de seguridad) en cada instancia. En el caso de 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 los clientes acceden a los puntos finales (end points) para almacenar y recuperar datos. Los clientes son responsables de la gestión de sus datos (incluidas las opciones de cifrado), de la clasificación de sus activos, y del uso de herramientas IAM (Identity and Access Management) para aplicar los permisos adecuados.

Seguridad de la Nube

La infraestructura y los servicios de AWS están aprobados para operar según varios estándares de cumplimiento y certificaciones de la industria en todas las geografías e industrias. Los clientes pueden utilizar las certificaciones de cumplimiento de AWS para validar la implementación y la eficacia de los controles de seguridad de AWS, incluidas certificaciones y prácticas recomendadas de seguridad reconocidas internacionalmente. Para más información, consulte nuestro documento técnico AWS y seguridad informática en el sector de servicios financieros.

El Programa de cumplimiento de AWS se basa en las siguientes acciones:

- **Validación** de que los servicios e instalaciones de AWS en todo el mundo mantengan un entorno de control ubicuo que funcione eficazmente. El entorno de control de AWS abarca las personas, los procesos y la tecnología necesarios para establecer y mantener un entorno que apoye la eficacia operativa del marco conceptual de control de AWS. AWS ha integrado controles aplicables específicos para la nube, identificados por los organismos principales de la industria de computación en la nube, en el marco conceptual de control de AWS. AWS monitorea estos grupos de la industria para identificar las principales prácticas que los clientes pueden implementar para que puedan mejorar la gestión de su entorno de control.
- **Demostración** de la postura de cumplimiento de AWS para ayudar a los clientes a verificar el cumplimiento de los requisitos de la industria y del gobierno. AWS colabora con organismos de certificación externos y auditores independientes para proporcionar a los clientes información sobre las políticas, procesos y controles establecidos y operados por AWS. Los clientes pueden utilizar esta información para llevar a cabo sus procedimientos de evaluación y verificación del control, así como se requiere según el estándar de cumplimiento correspondiente.
- **Monitoreo**, a través de los controles de seguridad correspondientes, AWS mantiene el cumplimiento de prácticas recomendadas y estándares mundiales.

Programas de Cumplimiento de AWS

Certificaciones y Atestaciones de Terceros

AWS ha obtenido certificaciones y atestaciones de terceros para una variedad de tareas específicas de diferentes industrias. Sin embargo, los siguiente son de particular importancia para las instituciones financieras:

ISO 27001 es un estándar de gestión de la seguridad informática que especifica las prácticas recomendadas y los controles de seguridad exhaustivos siguiendo la guía de prácticas recomendadas de la norma ISO 27002. La base de esta certificación es el desarrollo e implementación de un riguroso programa de seguridad, que incluye el desarrollo e implementación de un Sistema de Gestión de la Seguridad Informática, el cual define la manera en que AWS gestiona perpetuamente la seguridad de forma holística y exhaustiva. Para más información, o para descargar la certificación ISO 27001 de AWS, consulte la página web de Cumplimiento de ISO 27001.

ISO 27017 orienta sobre los aspectos de seguridad informática de la computación en la nube recomendando la implementación de controles de seguridad informática específicos de la nube que complementan la orientación de los estándares ISO 27002 e ISO 27001. Este código de práctica proporciona una orientación adicional para la aplicación de controles de seguridad informática específicos para los proveedores de servicios en la nube. Para más información, o para descargar la certificación ISO 27017 de AWS, consulte la página web de Cumplimiento de ISO 27017.

ISO 27018 es un código de práctica que se centra en la protección de datos personales en la nube. Se basa en el estándar ISO 27002 de seguridad informática y proporciona orientación para la aplicación de controles del estándar ISO 27002 correspondientes a la Información de Identificación Personal (PII por sus siglas en inglés) en la nube pública. También proporciona un conjunto de controles adicionales y orientación relacionada destinados a abordar los requisitos de protección de la PII en la nube pública que no se abordan en el actual conjunto de controles del estándar ISO 27002. Para más información, o para descargar la certificación ISO 27018 de AWS, consulte la página web de Cumplimiento de ISO 27018.

ISO 9001 es una norma que esboza un enfoque orientado a los procesos para documentar y revisar la estructura, las responsabilidades y los procedimientos necesarios para lograr una gestión eficaz de la calidad dentro de una organización. La clave de la certificación en curso según este estándar es establecer, mantener y mejorar la estructura organizacional, las responsabilidades, los procedimientos, los procesos y los recursos de manera que los productos y servicios de AWS satisfagan sistemáticamente los requisitos de calidad del estándar ISO 9001. Para más información, o para descargar la certificación ISO 9001 de AWS, consulte la página web del Cumplimiento de ISO 9001.

PCI DSS Level 1 - El estándar de Seguridad de Datos de la Industria de las Tarjetas de Pago (PCI DSS por sus siglas en inglés), es un estándar exclusivo de seguridad de la información administrado por el Consejo de Estándares de Seguridad de PCI. PCI DSS se aplica a todas las entidades que almacenan, procesan o transmiten datos de titulares de tarjeta (CHD) y/o datos de autenticación sensibles (SAD), incluidos comerciantes, procesadores de pago, adquirentes, emisores y proveedores de servicios. PCI DSS es requerida por las marcas de tarjetas y administrada por el Consejo de Estándares de Seguridad de la Industria de Tarjetas de Pago. Para obtener más información, o para solicitar el Resumen de la atestación de cumplimiento y responsabilidad de PCI DSS, consulte la página web de Cumplimiento de PCI DSS.

SOC - Los informes de los Controles del Sistema y Organización (SOC por sus siglas en inglés) son informes de análisis realizados por terceros independientes que demuestran cómo AWS cumple con los controles y objetivos de cumplimiento claves. El propósito de estos informes es ayudar a los clientes y a sus auditores a comprender los controles de AWS establecidos para apoyar las operaciones y el cumplimiento. Para más información, consulte la página de Cumplimiento de SOC. Hay tres tipos de informes SOC para AWS:

- **SOC 1:** ofrece información acerca del entorno de control de AWS que puede ser relevante para los controles internos sobre los informes financieros de un cliente, así como información para la evaluación y la opinión de la eficacia de los controles internos sobre los informes financieros (ICOFR).
- **SOC 2**: proporciona a los clientes y a los usuarios de sus servicios que tengan una necesidad comercial con una evaluación independiente del entorno de control de AWS relevante para la seguridad, disponibilidad y confidencialidad del sistema.
- **SOC 3**: proporciona a los clientes y a los usuarios de sus servicios que tengan una necesidad comercial una evaluación independiente del entorno de control de AWS relevante para la seguridad, disponibilidad y confidencialidad del sistema sin revelar la información interna de AWS.

Al vincular las características de los servicios centrados en la administración y control y favorables a la auditoría con esas certificaciones, atestaciones y estándares de auditoría, los encargados del cumplimiento de las normas de AWS se basan en programas tradicionales y ayudan a los clientes a establecerse y operar en un entorno de AWS.

Para obtener más información acerca de otras certificaciones y atestaciones de AWS, consulte la página web del Programa de cumplimiento de AWS. Se puede encontrar más información sobre los controles de seguridad generales de AWS y la seguridad específica de los servicios en el documento técnico Amazon Web Services: resumen de los procesos de seguridad.

AWS Artifact

Los clientes pueden revisar y descargar reportes y detalles acerca de más de 2,600 controles de seguridad utilizando AWS Artifact, el portal de reportes de cumplimiento disponible en la Consola de Gestión de AWS (AWS Management Console). El portal de AWS Artifact proporciona acceso bajo demanda a documentos de cumplimiento y seguridad de AWS, incluidos los informes de los controles del sistema y organización (SOC), informes de la industria de las tarjetas de pago (PCI) y certificaciones de organismos de acreditación de distintas regiones y tipos de conformidad.

Infraestructura de Nube Global de AWS

La Infraestructura de Nube Global de AWS comprende las regiones de AWS y zonas de disponibilidad. Una región es una ubicación física en el mundo, que se compone de múltiples zonas de disponibilidad. Las zonas de disponibilidad consisten en uno o más centros de datos, cada uno con energía, redes y conectividad redundantes, todos alojados en instalaciones separadas. Estas zonas de disponibilidad ofrecen a los clientes la posibilidad de operar aplicaciones y bases de datos de mayor disponibilidad, tolerancia a las fallas y adaptabilidad de lo que sería posible en un ambiente tradicional en las instalaciones. Los clientes pueden obtener más información acerca de estos temas al descargar nuestro documento técnico acerca de Amazon Web Services y su enfoque de la tolerancia a fallos operativos en el sector financiero y en otros campos. Los clientes de AWS eligen la región o regiones de AWS en las que sus contenidos y servidores están ubicados. Esto les permite a los clientes establecer entornos que cumplan con los requisitos regulatorios o geográficos específicos. Asimismo, esto permite que los clientes con objetivos de continuidad de negocio y recuperación ante desastres establezcan entornos primarios y de respaldo en un lugar o lugares de su elección. Se puede encontrar más información acerca de nuestras recomendaciones acerca de la recuperación ante desastres en Recuperación ante Desastres de AWS.

Normativas del BCRA

Tercerización de actividades por parte de las Instituciones Financieras

Las Normativas del BCRA les permiten a las instituciones financieras tercerizar, total o parcialmente, a un proveedor de servicios externo, un amplio conjunto de servicios de tecnología de la información, incluido el uso de servicios en la nube.

Sección 2 (Descentralización y tercerización de actividades) de las Normativas del BCRA define las consideraciones generales que las instituciones financieras deben tener en cuenta al tercerizar los servicios de TI a un proveedor de servicios externo, incluyendo los siguientes:

- Requisito de notificación previa de 60 días (consulte la sección de Notificaciones).
- Condiciones: incluidos, entre otros, los requisitos técnicos y operativos que las instituciones financieras necesitan implementar dependiendo de la naturaleza y el tipo de actividades tercerizadas.
- Requisitos de notificación: incluye una lista de información que las instituciones financieras necesitan presentar ante el regulador.
- Responsabilidades de las instituciones financieras: las instituciones financieras que deciden tercerizar servicios no están liberadas de su responsabilidad de cumplir con las regulaciones y leyes que les sean aplicables, así como las normas dictadas por el BCRA.

Notificación

Las Normativas del BCRA (Sección 2 - Descentralización y tercerización de actividades) no exigen que las instituciones financieras obtengan una aprobación formal del BCRA o de la Superintendencia de Entidades Financieras y Cambiarias (SEFyC) antes de descentralizar y/o tercerizar servicios de TI, sino que las instituciones financieras deben notificar dicha descentralización y/o tercerización a la SEFyC con al menos 60 días corridos antes del inicio de esas actividades[1].1

Facultades de supervisión y fiscalización del regulador

El BCRA ha publicado directrices regulatorias a través de varias Interpretaciones Normativas. Estas interpretaciones han clarificado el alcance de las Normativas del BCRA con respecto a las actividades tercerizadas a un CSP por las instituciones financieras. En junio de 2019, el BCRA publicó unas Interpretaciones Normativas que reconocen que la revisión de las certificaciones internacionales de seguridad de la información y de sistemas de terceros (como las certificaciones ISO) y los informes de auditores externos independientes (como los informes SOC) son generalmente suficientes para satisfacer las facultades de auditoría y acceso del BCRA y la SEFyC con respecto a los CSP que prestan servicios a las entidades reguladas. Esta clarificación resalta que dichas certificaciones, atestaciones e informes de auditoría de terceros son valiosos recursos de cumplimiento que benefician tanto a las instituciones financieras como al regulador para que puedan desempeñar sus funciones de supervisión respecto a las actividades tercerizadas. Para más información acerca de estas certificaciones e informes de auditoría de terceros, consulte la sección de Programas de Cumplimiento de AWS.

Las instituciones financieras que son clientes de AWS tienen la opción de firmar un Acuerdo Empresarial (Enterprise Agreement) con AWS. Los Acuerdos Empresariales ofrecen a los clientes la opción de adaptar los acuerdos a sus necesidades, incluidos los requisitos regulatorios. Mediante un Acuerdo Empresarial, AWS les ofrece a sus clientes regulados por el BCRA un marco contractual que les ayuda a satisfacer los requisitos contractuales aplicables según las Normativas del BCRA, incluyendo términos específicos que se refieren a los derechos de acceso e inspección del regulador, cuando lo exija la ley aplicable y bajo determinadas condiciones. Para más información acerca de los Acuerdos Empresariales de AWS, contacte a su representante de AWS.1 El BCRA clarificó este requisito de notificación en sus Interpretaciones Normativas.

Planes de Soporte

Los planes de soporte de AWS están diseñados para ofrecerle al cliente la combinación adecuada de herramientas y acceso a la experiencia, de modo que el cliente pueda tener éxito con AWS, a la vez que optimiza el rendimiento, gestiona el riesgo y mantiene los costos bajo control.

[1] El BCRA clarificó el requerimiento en sus Interpretaciones Normativas

El soporte básico de AWS está disponible para todos los clientes de AWS e incluye:

- Servicio al cliente y comunidades - acceso 24/7 a servicio al cliente, documentación, documentos técnicos, y foros de soporte.
- AWS Trusted Advisor - Acceso a las siete comprobaciones básicas y guía del Trusted Advisor para la provisión de sus recursos según las mejores prácticas para aumentar el rendimiento y mejorar la seguridad.
- AWS Personal Health Dashboard - Una vista personalizada de la salud de los servicios de AWS, y alertas cuando sus recursos se ven afectados.

Requisitos Técnicos y Operativos

La Sección 7 (Servicios de tecnología informática tercerizados) de las Normativas del BCRA describe las categorías amplias de actividades de TI que las instituciones financieras pueden tercerizar a proveedores de servicios. La Sección 7 detalla los requisitos generales y los "controles técnicos y operativos" específicos que las instituciones financieras pueden tener que implementar dependiendo, entre otras cosas, de la naturaleza y el tipo de las actividades tercerizadas.

Punto de Acceso Unificado

La sección 7.3.2.2 de las Normativas del BCRA define el Punto de Acceso Unificado (PAU) y requiere a las instituciones financieras implementar un entorno no operativo que les permita controlar y monitorear de forma activa, continua y permanente todas las actividades de TI tercerizadas, así como sus datos. El PAU debe estar emplazado en Argentina y gestionado por la institución financiera. Las instituciones financieras pueden aprovechar la Consola de Gestión de AWS (AWS Management Console) o la Interfaz de Línea de Comando de AWS (AWS CLI por sus siglas en inglés) para satisfacer el requisito del PAU. La Consola de Gestión de AWS provee una interfaz web simple para los servicios de AWS. La consola comprende y proporciona acceso a una colección amplia de consolas de servicio para la gestión de los servicios de AWS, y ofrece una interfaz de usuario incorporada para realizar tareas en AWS. El BCRA ha explicado con más detalle el alcance de este requisito del PAU en sus Interpretaciones Normativas.

Matriz de escenarios

La sección 7.5 de las Normativas del BCRA presenta una "matriz de escenarios" que describe cuatro escenarios distintos de servicios de tecnología informática (STI) tercerizados en función de la naturaleza y los tipos de datos que se manejan y la categoría de los servicios tercerizados implicados. El BCRA ha asignado ciertos requisitos técnicos y operativos mínimos a cada uno de esos escenarios.

Las instituciones financieras deben considerar la carga de trabajo que se está examinando, las categorías relevantes de datos y servicios que se han de tercerizar, y evaluar la materialidad o criticidad de la carga de trabajo a la luz de los escenarios detallados en las Normativas del BCRA y sus políticas de gestión de riesgos operativos. Dado que los requisitos de los clientes difieren, AWS recomienda a cada uno de ellos a obtener el asesoramiento adecuado sobre el cumplimiento de todos los requisitos regulatorios y legales que sean relevantes para su negocio, incluidos los requisitos técnicos y operativos mínimos contemplados en las Normativas del BCRA, y otras regulaciones y leyes locales.

La siguiente tabla resume la matriz de escenarios definida en las Normativas del BCRA:

		Requisitos Técnicos y Operativos Mínimos						
Escenario	**Situación**	**Seguridad Información**	**Concientización y Capacitación**	**Control de Acceso**	**Integridad y Registro**	**Monitoreo y Control**	**Gestión de Incidentes**	**Continuidad Operativa**
ESD001	Datos del cliente: uso/explotación, conservación y transporte, incluyendo transacciones financieras que incluyan datos del cliente.	RGS001 RGS002 RGS003 RGS004 RGS005 RGS006 RGS007	RCC001 RCC002 RCC005 RCC006 RCC007 RCC008 RCC010 RCC012 RCC013	RCA049 RCA050 RCA051 RCA052	RIR003 RIR010 RIR011 RIR020 RIR021 RIR022 RIR023 RIR024	RMC004 RMC006 RMC014 RMC015	RGI001 RGI002 RGI003 RGI005	RCO001 RCO002 RCO003 RCO004
ESD002	Datos contables-financieros: uso/explotación, conservación y transporte, incluyendo o no datos de clientes.	RGS001 RGS002 RGS003 RGS004 RGS005 RGS006 RGS007	RCC001 RCC002 RCC005 RCC006 RCC007 RCC008 RCC010 RCC012 RCC013	RCA049 RCA050 RCA051 RCA052	RIR003 RIR010 RIR011 RIR020 RIR021 RIR022 RIR023 RIR024	RMC004 RMC006 RMC014 RMC015	RGI001 RGI002 RGI003 RGI005	RCO001 RCO002 RCO003 RCO004
ESD003	Datos transaccionales financieros: uso/explotación, conservación y transporte que no incluya datos del cliente.	RGS001 RGS004 RGS005 RGS007	RCC001 RCC005 RCC006 RCC007 RCC010 RCC012 RCC013	RCA050 RCA051 RCA052	RIR003 RIR010 RIR011 RIR021 RIR022 RIR023	RMC004 RMC006 RMC014 RMC015	RGI001 RGI002 RGI003 RGI005	RCO001 RCO002 RCO003 RCO004
ESD004	Datos operativos: uso/explotación, conservación y transporte que no incluya información contable-financiera, del cliente o transaccional financiera.	RGS001 RGS004 RGS005 RGS007	RCC001 RCC005 RCC006 RCC007 RCC010 RCC012 RCC013	RCA050 RCA051 RCA052	RIR003 RIR010 RIR011 RIR021 RIR022 RIR023 RIR025	RMC003 RMC006 RMC014 RMC015	RGI001 RGI002 RGI003 RGI005	RCO001 RCO002 RCO003 RCO004

Para más información acerca de los requisitos técnicos y operativos descritos en las Normativas del BCRA, consulte el Apéndice: Consideraciones de AWS acerca de los Requisitos Técnico-Operativos en las Normativas del BCRA.

Próximos Pasos

Cada organización tiene su propio proceso de adaptación a la nube, por lo tanto, para ejecutar con éxito su adopción, es necesario comprender el estado actual de su organización, el escenario deseado, y la transición necesaria para alcanzar el objetivo. Saber esto le ayudará a establecer objetivos y crear flujos de trabajo que le permitan al personal desarrollarse en la nube.

Para las instituciones financieras en Argentina, típicamente se contemplan los siguientes próximos pasos:

- Contactar al representante de AWS para discutir cómo la red de socios de AWS, y los arquitectos de soluciones de AWS, los equipos de servicios profesionales y los instructores de formación pueden ayudarle en su proceso de adopción de la nube. Si no cuenta con un representante de AWS, por favor contáctenos.
- Obtener y revisar una copia de los últimos informes SOC 1 y SOC 2 de AWS, el resumen de la atestación de cumplimiento y responsabilidad del PCI-DSS y la certificación ISO 27001 a través del portal de AWS Artifact (accesible a través de la Consola de Gestión de AWS).
- Considerar la relevancia y aplicación de los documentos técnicos de seguridad de AWS según sea apropiado para su proceso en la nube y los casos de uso. Estas prácticas recomendadas proporcionan a los usuarios de AWS recomendaciones claras de aplicación y evaluación.
- Profundice sobre otras prácticas de gestión de riesgos y de gobierno, según sea necesario, a partir de su diligencia debida y la evaluación del riesgo, utilizando las herramientas y recursos a los que se hace referencia a lo largo de esta guía y en la sección de Recursos adicionales.
- Comuníquese con su representante de AWS para obtener información adicional acerca del Acuerdo Empresarial de AWS (Enterprise Agreement).

Asimismo, para ayudar a nuestros clientes a maximizar el uso de la tecnología proporcionada por AWS, el equipo técnico de AWS puede apoyar a nuestros clientes para que implementen la arquitectura, productos y servicios que les permitan cumplir con cualquier requisito técnico y operativo que les sea aplicable según las Normativas del BCRA.

Recursos Adicionales

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

- Guía de referencia rápida de cumplimiento de AWS: AWS tiene muchas características de cumplimiento que usted puede utilizar para las cargas de trabajo reguladas en la nube de AWS. Estas características le permiten alcanzar un mayor nivel de seguridad a gran escala. El cumplimiento basado en la nube ofrece un menor costo de introducción, operaciones más fáciles y una mayor agilidad, al proporcionar más supervisión, control de seguridad y automatización central.
- Marco de buena arquitectura de AWS: el marco de buena arquitectura ha sido desarrollado para ayudar a los arquitectos de la nube a construir la infraestructura más segura, de alto rendimiento, resistente y eficiente para sus aplicaciones. Este marco proporciona un enfoque coherente para que los clientes y socios evalúen las arquitecturas, y ofrece orientación para ayudar a implementar diseños que cumplan con las necesidades de aplicación a lo largo del tiempo. El marco de buena arquitectura consiste en cinco pilares: Excelencia Operativa, Seguridad, Fiabilidad, Eficiencia en el Rendimiento y Optimización de Costos.

  AWS ha publicado la siguiente lista de documentos técnicos que abordan cada pilar del Marco de buena arquitectura de AWS: Documento técnico sobre el pilar de excelencia operativa de AWS. Documento técnico sobre el pilar de seguridad de AWS. Documento técnico sobre el pilar de fiabilidad de AWS. Documento técnico sobre la eficiencia del rendimiento de AWS. Documento técnico sobre la optimización de costos de AWS.
- Principios reguladores de los servicios financieros mundiales: AWS ha identificado cinco principios comunes relacionados con la regulación de los servicios financieros que los clientes deben tener en cuenta al utilizar los servicios en la nube de AWS y, específicamente, al aplicar el modelo de responsabilidad compartida a sus requisitos regulatorios. Los clientes pueden acceder a un documento técnico sobre estos principios bajo un acuerdo de confidencialidad a través de AWS Artifact.
- Marco de seguridad cibernética del NIST (CSF): el documento técnico de AWS llamado Marco de seguridad cibernética del NIST (CSF): alineación con el CSF del NIST en la nube de AWS demuestra cómo las organizaciones del sector público y comercial pueden evaluar el entorno de AWS en relación con el CSF del NIST y mejorar las medidas de seguridad que implementan y operan (es decir, la seguridad de la nube). El documento técnico también proporciona una carta de un auditor externo que certifica la conformidad de la oferta de la nube de AWS con las prácticas de gestión de riesgos de la CSF del NIST (es decir, la seguridad de la nube). Las instituciones financieras pueden aprovechar los recursos de CSF del NIST y AWS para elevar sus marcos de gestión de riesgos.

Para obtener ayuda adicional, consulte los Documentos de seguridad, identidad y cumplimiento.

Revisiones de Documentos

Fecha	Descripción
Mayo de 2020	Primera publicación (idioma inglés)

Apéndice: Consideraciones de AWS acerca de los Requisitos Técnico-Operativos en las Normativas del BCRA

En las secciones siguientes se enumeran los requisitos técnicos y operativos identificados en las secciones 7.7.1 a 7.7.7 de las Normativas del BCRA junto con las consideraciones de AWS para ayudar a las instituciones financieras clientes a comprender cada requisito cuando utilizan AWS, y también se incluye una descripción de las prácticas recomendadas del Marco de buena arquitectura de AWS que las instituciones financieras pueden utilizar para apoyar sus esfuerzos de cumplimiento.

El Marco de buena arquitectura de AWS ha sido desarrollado para ayudar a los arquitectos de la nube a construir infraestructura segura, de alto rendimiento, resistente y eficiente para sus aplicaciones. Basado en cinco pilares: excelencia operativa, seguridad, fiabilidad, eficiencia de rendimiento y optimización de costos; el marco proporciona un enfoque consistente para que los clientes evalúen las arquitecturas e implementen diseños que se adapten a lo largo del tiempo.

Las tablas de las siguientes secciones están organizadas con las siguientes columnas:

- **Requisito:** en esta columna se enumeran los requisitos técnicos y operativos mínimos (por categoría) que pueden aplicarse a cada uno de los escenarios descritos en las Normativas del BCRA.
- **Consideraciones:** esta columna explica algunas consideraciones para abordar los requisitos definidos por el BCRA. Pueden referirse a la seguridad y el cumplimiento de la nube y a la forma en que AWS implementa y gestiona los controles, y/o a los servicios de AWS que las instituciones financieras pueden utilizar para abordar estos requisitos.
- **Consideraciones de Implementación:** esta columna enumera las mejores prácticas recomendadas para la seguridad en la nube del Marco de buena arquitectura de AWS, que las instituciones financieras pueden implementar como punto de partida para apoyar sus esfuerzos de cumplimiento. Los detalles de cada una de las prácticas recomendadas y los servicios asociados de AWS que los clientes pueden usar se encuentran en el Marco de buena arquitectura de AWS.

En las tablas siguientes se presentan consideraciones adicionales para apoyar a los clientes en sus esfuerzos de cumplimiento de sus requisitos aplicables bajo las Normativas del BCRA. Estas tablas contienen tan sólo algunas consideraciones y no proporcionan un abordaje exhaustivo. Esto no debe considerarse como un consejo legal ni de cumplimiento. Los clientes deben consultar con sus propios equipos legales y de cumplimiento.

De Gobierno de Seguridad de la Información (GS) - Sección 7.7.1

Estos requisitos técnicos y operativos están relacionados con la organización de los procesos de administración estratégica y operativa de la seguridad de la información, la estructura funcional y operativa y la determinación de las responsabilidades asociadas.

Requisito	Consideraciones	Consideraciones de Implementación (Prácticas de Buena Arquitectura)
RGS001: Las entidades/prestadores deberán establecer y notificar al BCRA el detalle completo, exhaustivo y actualizado de las responsabilidades compartidas y/o exclusivas sobre los roles y funciones para la administración y gestión operativa de seguridad de la información asociadas a servicios de tecnología informática (STI).	**Responsabilidad del cliente** Los clientes deben definir su modelo operativo basado en los servicios y productos de AWS que utilizan. Como se explica en la sección de Seguridad y Responsabilidad compartida, la seguridad en la nube es una responsabilidad compartida. AWS gestiona la seguridad de la nube asegurándose de que la infraestructura de AWS cumpla con los requisitos regulatorios mundiales, así como 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 quieren utilizar para proteger sus contenidos, aplicaciones, sistemas y redes, de la misma manera que lo hacen en un centro de datos local.	No aplica.

Requisito	Consideraciones	Consideraciones de Implementación (Prácticas de Buena Arquitectura)
RGS002: La entidad/prestador deberá establecer roles y funciones para el tratamiento de los datos del cliente, estableciendo las responsabilidades correspondientes según el nivel de participación y tarea que realice. Estas obligaciones deberán estar formalizadas en los acuerdos del STI.	**Responsabilidad compartida** AWS considera que la definición de roles y responsabilidades de las instituciones financieras sobre la manera en cómo procesarán los datos de sus clientes, es una tarea que le corresponde completar a las instituciones financieras. Al utilizar los servicios de AWS, los clientes mantienen el control sobre todo el ciclo de vida de sus contenidos en AWS, y son responsables de gestionar su contenido, de acuerdo con sus propias necesidades específicas, incluyendo la clasificación de los contenidos, el control de acceso, la retención y la eliminación. AWS trata todo el contenido del cliente y los activos asociados como información crítica. Los servicios de AWS no hacen diferenciación entre los contenidos, ya que ofrecen el nivel de seguridad más alto a todos los clientes, independientemente del tipo de contenido que se almacene. Somos muy cuidadosos con la seguridad de nuestros clientes y hemos implementado medidas técnicas y físicas sofisticadas diseñadas para prevenir el acceso no autorizado. AWS no tiene una visibilidad significativa en cuanto al tipo de contenido que el cliente elige almacenar en AWS y, de igual forma, el cliente conserva el control completo de cómo desea clasificar su contenido y dónde almacenarlo, utilizarlo y protegerlo de la divulgación. En sus acuerdos con los clientes, AWS asume compromisos específicos de seguridad y privacidad que se aplican ampliamente al contenido del cliente en cada una de las regiones que el cliente elige para almacenar sus datos. Consulte las secciones 3 y 4 del Acuerdo de cliente de AWS (AWS Customer Agreement). Los clientes de AWS también tienen la opción de firmar un Acuerdo Empresarial con AWS (Enterprise Agreement). Los Acuerdos Empresariales les ofrecen a los clientes la opción de adaptar los acuerdos a sus necesidades, incluidos los requisitos regulatorios. Para más información acerca de los Acuerdos Empresariales de AWS, contacte a su representante de AWS.	SEC-2 Control de acceso humano SEC-7 Clasificación de datos

Requisito	Consideraciones	Consideraciones de Implementación (Prácticas de Buena Arquitectura)
RGS003: La entidad y el prestador del STI tercerizado deberán cumplir con las leyes y regulaciones nacionales relacionadas con la protección de datos personales (Ley 25.326) cuando el servicio involucra la recolección y uso de datos personales, lo que deberá reflejarse en los acuerdos del STI.	**Responsabilidad compartida** Tal como se explicó en la sección Seguridad y Responsabilidad Compartida, es importante señalar que, al utilizar los servicios de AWS, los clientes mantienen el control de sus datos y son responsables de la gestión de los requisitos de seguridad del contenido crítico. Esto les permite a los clientes controlar todo el ciclo de vida de su contenido en AWS y gestionar su contenido de acuerdo con sus propias necesidades, incluyendo clasificación de contenido, control de acceso, retención y eliminación. Para obtener más información acerca del Modelo de Responsabilidad compartida y sus implicaciones para el almacenamiento y procesamiento de datos personales utilizando AWS, consulte el documento técnico de AWS Utilizando AWS en el contexto de privacidad común y consideraciones de la protección de datos y nuestro sitio web de Privacidad de datos en Argentina, el cual incluye un resumen de la Ley de Protección de Datos Personales de Argentina N° 25.326 (LPDP) y preguntas frecuentes. En sus acuerdos con los clientes, AWS asume compromisos específicos de seguridad y privacidad que se aplican ampliamente al contenido del cliente en cada una de las regiones que el cliente elige para almacenar sus datos. Los compromisos que asume AWS son consistentes con los objetivos de la LPDP y la Disposición 60-E/2016 para proteger datos personales. AWS también ofrece un acuerdo de procesamiento internacional de datos (Data Processing Addendum, o DPA), también denominado acuerdo de transferencia de datos, que incluye compromisos contractuales específicos para abordar adecuadamente las funciones y obligaciones de cada parte con respecto a la privacidad y la seguridad de los datos personales. Para información adicional sobre los Acuerdos Empresariales de AWS o el DPA, por favor contacte a su representante de AWS.	No aplica.

Requisito	Consideraciones	Consideraciones de Implementación (Prácticas de Buena Arquitectura)
RGS004: La entidad y prestador deberán establecer y documentar los protocolos de intercambio de información entre los participantes del acuerdo de STI, incluyendo terceros subcontratados, así como las técnicas y medidas operativas (formatos, límites de tiempo, responsables, etc.) que garanticen información útil, oportuna y completa a las partes involucradas y al BCRA.	**Responsabilidad del cliente** Los clientes son responsables de definir los procesos internos utilizados para gestionar los STI tercerizados. Para apoyar a sus clientes, AWS desarrolla y mantiene procedimientos de asistencia al cliente que incluyen métricas para verificar el rendimiento. Cuando un cliente se pone en contacto con AWS para informar que los servicios de AWS no cumplen sus objetivos de calidad, sus problemas se investigan inmediatamente y, cuando es necesario, se toman medidas comercialmente razonables para resolverlos. El sistema de calidad de asistencia al cliente incluye, pero no se limita a, procedimientos de revisión y evaluación de las quejas de los clientes, la participación de los recursos y equipos internos necesarios de AWS y la comunicación de la disposición final del asunto al cliente. Los planes de asistencia de AWS están diseñados para ofrecerle al cliente la combinación adecuada de herramientas y acceso al conocimiento, de modo que el cliente pueda tener éxito con AWS, a la vez que optimiza el rendimiento, gestiona el riesgo y mantiene los costos bajo control. AWS mantiene procedimientos para notificar a los clientes de los problemas que afectan a los clientes utilizando el AWS Service Health Dashboard. El AWS Service Health Dashboard publica información actualizada cada minuto acerca de la disponibilidad del servicio. En este dashboard los clientes pueden suscribirse a un feed RSS para ser notificados acerca de interrupciones de cada servicio individual y un historial completo de salud de cada servicio. Además, el AWS Personal Health Dashboard les da a los clientes una vista personalizada del rendimiento y disponibilidad de los servicios. Muestra información relevante y oportuna para ayudar a los clientes a gestionar los eventos en curso, y proporciona una notificación proactiva para ayudar a los clientes a planificar las actividades programadas.	No aplica.

Requisito	Consideraciones	Consideraciones de Implementación (Prácticas de Buena Arquitectura)
RGS005: En el caso de prestador o subcontratistas participantes de un STI que procesen, almacenen o transporten datos o procesos de la entidad en locaciones en el exterior, la entidad, los prestadores y los terceros involucrados deberán proveer los mecanismos necesarios para verificar si las locaciones satisfacen las disposiciones legales, normativas y contractuales establecidas en el acuerdo de STI, incluyendo lo establecido en las normas sobre "Expansión de entidades financieras".	**Responsabilidad del cliente** Los clientes de AWS designan en qué región geográfica se ubicará su contenido. Con AWS, las instituciones financieras pueden: • Determinar dónde se almacenará su contenido, incluido el tipo de almacenamiento y la región geográfica de ese almacenamiento. • Replicar y respaldar su contenido en más de una región, y AWS no trasladará ni replicará al cliente fuera de la región(es) elegida(s) por las instituciones financieras, excepto en la medida en que se requiera legalmente y sea necesario para mantener los servicios de AWS y proporcionarlos a nuestros clientes y sus usuarios finales. Para obtener información actualizada sobre las regiones y zonas de disponibilidad de AWS, consulte el artículo sobre Infraestructura mundial. • Elegir el estado de seguridad de su contenido. Les ofrecemos a las instituciones financieras un cifrado fuerte para el contenido en tránsito o en reposo, y les ofrecemos a las instituciones financieras la opción de gestionar sus propias claves de cifrado. • Gestionar el acceso a su contenido y a los servicios y recursos de AWS a través de usuarios, grupos, permisos y credenciales que las instituciones financieras controlan.	No aplica.

Requisito	Consideraciones	Consideraciones de Implementación (Prácticas de Buena Arquitectura)
RGS006: El acuerdo de STI deberá incluir la obligación de no divulgación de datos personales y extender tal obligación a terceros subcontratados.	**Responsabilidad compartida** AWS les da a los clientes la propiedad y el control de su contenido a través de herramientas que les permiten a los clientes determinar dónde se almacenará su contenido, cómo se asegurará en tránsito o en reposo, y cómo se gestionará el acceso a su entorno de AWS. AWS ha implementado prácticas recomendadas mundiales de protección de datos y privacidad para ayudar a los clientes a establecer, operar y aprovechar nuestro entorno de control de seguridad. Estas protecciones de seguridad y procesos de control son validados independientemente por varias evaluaciones independientes de terceros. La auditoría de la norma ISO 27018 de AWS verifica la implementación de controles de seguridad centrados en la protección de los datos personales. Para obtener más información acerca del cumplimiento de la norma ISO 27108 de AWS, visite Cumplimiento de ISO/IEC 27018:2019. Si desea conocer más sobre la privacidad de datos en AWS, consulte las Preguntas frecuentes sobre la privacidad de datos. En sus acuerdos con los clientes, AWS asume compromisos específicos de seguridad y privacidad que se aplican ampliamente al contenido del cliente en cada una de las regiones que el cliente elige para almacenar sus datos. Por ejemplo, consulte las secciones 3 y 4 del Contrato de usuario de AWS. Los clientes de AWS también tienen la opción de firmar un Acuerdo Empresarial con AWS (Enterprise Agreement). Los Acuerdos Empresariales les ofrecen a los clientes la opción de adaptar los acuerdos a sus necesidades, incluidos los requisitos regulatorios. Para más información acerca de los Acuerdos Empresariales de AWS, contacte a su representante de AWS.	SEC-7 Clasificar datos SEC-8 Proteger datos en reposo

Requisito	Consideraciones	Consideraciones de Implementación (Prácticas de Buena Arquitectura)
RGS007: Las entidades/ prestadores deben documentar y asignar la propiedad de todos los activos de información en el STI, determinando el nivel de responsabilidad administrativa y operativa de cada parte en el ciclo de vida de la información.	**Responsabilidad compartida** Los clientes conservan la propiedad y el control de su contenido cuando utilizan los servicios de AWS, y no ceden esa propiedad y control de su contenido a AWS. AWS no tiene una visibilidad significativa en cuanto al tipo de contenido que el cliente elige almacenar en AWS y el cliente conserva el control completo de cómo elige clasificar su contenido, dónde almacenarlo, utilizarlo y protegerlo de divulgación. AWS proporciona un conjunto avanzado de funciones de acceso, cifrado y registro para ayudar a las instituciones financieras a hacer esto con eficacia (como AWS CloudTrail). No accedemos ni utilizamos el contenido de los clientes para ningún otro propósito que no sea el legalmente requerido y para mantener los servicios de AWS y proporcionarlos a nuestros clientes y sus usuarios finales. Con el fin de garantizar que el inventario de gestión de activos y los procedimientos de mantenimiento se ejecuten correctamente, a los activos de AWS se les asigna un propietario, se les hace un seguimiento y se monitorean con las herramientas de gestión de inventario propiedad de AWS. Los servicios de AWS no hacen diferenciación entre los contenidos, ya que ofrecen el nivel de seguridad más alto a todos los clientes, independientemente del tipo de contenido que se almacene. AWS está atento a la seguridad de los clientes, por lo que ha implementado sofisticadas medidas técnicas y físicas diseñadas para prevenir el acceso no autorizado. AWS rastrea, documenta y verifica acciones de saneamiento y eliminación de medios. Toda eliminación de medios es llevada a cabo por personal designado de AWS. Destrucción de datos: el contenido de las unidades de almacenamiento se trata al nivel más alto de clasificación (crítico) según la política de clasificación de datos de AWS. El contenido se destruye en los dispositivos de almacenamiento como parte del proceso de desmantelamiento de acuerdo con las normas de seguridad informática de AWS. Los servidores de AWS se borran o se sobrescriben de forma segura antes de su reutilización. Los medios de almacenamiento de AWS se borran o se desmagnetizan de manera segura y se destruyen físicamente antes de salir de las zonas de seguridad de AWS. Para validar los procesos y procedimientos de borrado seguro de AWS, los auditores externos revisan las directrices dentro de la política de protección de medios de AWS, examinan el equipo de desmagnetización y los contenedores de trituración seguros ubicados dentro de las instalaciones de AWS, examinan el historial de notificaciones que han documentado la destrucción de un disco duro en un centro de datos y el proceso de borrado y eliminación de un dispositivo del entorno.	SEC-7 Clasificar datos SEC-8 Protección de datos en reposo

De Concientización y Capacitación (CC). – Sección 7.7.2

Estos requisitos técnicos y operativos están relacionados con la adquisición y entrega de conocimiento en prácticas de seguridad, su difusión, entrenamiento y educación, para el desarrollo de tareas preventivas, detectivas y correctivas de los incidentes de seguridad en los STI tercerizados.

Requisito	Consideraciones	Consideraciones de Implementación (Prácticas de Buena Arquitectura)
RCC001: Los contenidos del programa de CC deben formularse y mantenerse actualizados en base a un análisis de las vulnerabilidades y los resultados de la Gestión de Incidentes, e incluir, pero no limitarse a incidentes: reportados, detectados y conocidos.	**Responsabilidad compartida** Los clientes son responsables de definir su propio programa interno de capacitación y concientización. Sin embargo, los clientes pueden aprovechar los servicios y recursos de capacitación de AWS para asegurarse de que su personal tenga la capacitación y los recursos adecuados para gestionar los servicios de AWS. La oferta de capacitaciones se puede encontrar en Capacitación y certificación. AWS ha implementado políticas y procedimientos formales y documentados de concientización de la seguridad informática y capacitación que abordan el propósito, el alcance, las funciones, las responsabilidades, el compromiso de la gestión, la coordinación entre las entidades organizativas y el cumplimiento. La política y los procedimientos de capacitación y concientización de la seguridad informática se revisan y actualizan por lo menos una vez al año, o antes, si es necesario debido a cambios en los sistemas de información. La política se difunde a través del portal de comunicación interna de Amazon a todos los empleados, proveedores y contratistas, antes de recibir acceso autorizado al sistema de información o de realizar tareas asignadas. AWS ha desarrollado, documentado y difundido capacitación de concientización de la seguridad informática basada en funciones, para los empleados responsables de diseñar, desarrollar, implementar, operar, mantener y monitorear los sistemas de gestión de la seguridad y la disponibilidad, y proporciona los recursos necesarios para que los empleados cumplan sus responsabilidades.	OPS-1 Determinación de prioridades SEC-4 Detección e investigación de eventos de seguridad SEC-10 Respuesta ante un incidente
RCC002: Los contenidos del programa de CC deben incluir: técnicas de detección y prevención de apropiación de datos personales y de las credenciales mediante ataques de tipo “ingeniería social”, “phishing”, “vishing” y otros de similares características.		OPS-1 Determinación de prioridades SEC-4 Detección e investigación de eventos de seguridad SEC-10 Respuesta ante un incidente
RCC005: Mantener informado al personal interno, personal responsable por la gestión del STI, personal de terceros involucrado en las tareas operativas y clientes sobre las vías de comunicación para la recepción de denuncias o problemas en el circuito asociado al escenario descrito.		OPS-10 Gestión de la carga de trabajo y los eventos de operaciones

Requisito	Consideraciones	Consideraciones de Implementación (Prácticas de Buena Arquitectura)
RCC006: Respecto de la audiencia del programa de CC, deben aplicarse los siguientes criterios: **a. Características y segmentación de la audiencia, de acuerdo con el nivel de intervención en el proceso y naturaleza de la función o rol que ocupa cada participante.** **b. Deben encontrarse alcanzados todos los participantes necesarios en el flujo completo de la actividad indicada en el escenario.** **c. Orientado pero no limitado a: personal interno, personal responsable por la gestión del STI, proveedores y clientes.**		No aplica.
RCC007: Con una periodicidad mínima anual, debe efectuarse un análisis del programa de CC ejecutado que mida la evolución de los incidentes, respecto de las actividades de CC realizadas incluyendo como mínimo: **a. Un reporte de la cantidad y segmentación de destinatarios y contenidos del programa de CC.** **b. Una comparación entre los contenidos cubiertos por el programa de CC y la cantidad y tipo de incidentes de seguridad reportados/detectados/conocidos.**		OPS–11 Evolución de las operaciones

Requisito	Consideraciones	Consideraciones de Implementación (Prácticas de Buena Arquitectura)
RCC008: Los contenidos del programa de CC deben incluir: medidas y técnicas para la protección de la privacidad de las credenciales.		SEC-1 Gestión de credenciales y autenticación SEC-2 Control de acceso humano SEC-3 Control del acceso programático
RCC010: Los contenidos del programa de CC deben incluir: recomendaciones específicas sobre las prácticas de seguridad en la plataforma de soporte de STI.		No aplica.
RCC012: Los contenidos del programa de CC deben incluir técnicas específicas para el desarrollo/ adquisición/fabricación, implementación, homologación y prueba de características de seguridad de los recursos informáticos del STI, asegurando que el personal involucrado interno/externo se encuentra debidamente capacitado para disminuir las fallas de implementación de las características de seguridad.		No aplica.
RCC013: Las entidades/prestadores deben contar con un mecanismo de comunicación de los contenidos de su programa de concientización y capacitación del STI que asegure: **a. Que los destinatarios se encuentran informados de forma continua.** **b. Que los destinatarios pueden efectuar consultas y evacuar dudas.**		OPS-1 Determinación de prioridades

De Control de Acceso (CA) - Sección 7.7.3

Estos requisitos técnicos y operativos se relacionan con la evaluación, desarrollo e implementación de medidas de seguridad para la protección de la identidad, mecanismos de autenticación, segregación de roles y funciones y demás características del acceso a los STI.

Requisito	Consideraciones	Consideraciones de Implementación (Prácticas de Buena Arquitectura)
RCA049: La entidad y prestador deberán garantizar que los datos personales no sean accedidos/procesados/ explotados por ellos o cualquiera de sus proveedores para fines diferentes de los establecidos en los acuerdos formales del STI, ni se realicen sin el formal y expreso consentimiento del responsable primario de los datos.	**Responsabilidad compartida** Los clientes de AWS conservan el control y la propiedad de sus datos y son responsables de gestionar los requisitos de seguridad del contenido crítico. Esto les permite a los clientes controlar todo el ciclo de vida de su contenido en AWS y gestionar su contenido de acuerdo con sus propias necesidades, incluyendo clasificación de contenido, control de acceso, retención y supresión. AWS les da a los clientes la propiedad y el control de su contenido mediante el diseño, a través de herramientas que les permiten determinar dónde se almacenará su contenido, cómo se asegurará en tránsito o en reposo, y cómo se gestionará el acceso a su entorno AWS. AWS ha implementado prácticas recomendadas mundiales de protección de datos y privacidad para ayudar a los clientes a establecer, operar y aprovechar nuestro entorno de control de seguridad. Estas protecciones de seguridad y procesos de control son validados independientemente por varias evaluaciones independientes de terceros. AWS ha establecido políticas y procedimientos formales para proporcionar a los empleados una base común de orientación y normas de seguridad informática. La política del Sistema de gestión de la seguridad informática de AWS establece directrices para proteger la confidencialidad, integridad y disponibilidad de los sistemas y contenido de los clientes. Mantener la confianza de los clientes es de suma importancia para AWS. Los empleados, proveedores y contratistas de AWS que necesiten una cuenta de usuario deben ser incorporados a través del sistema de gestión de recursos humanos de Amazon. Como parte del flujo de trabajo de incorporación, el gerente directo del empleado, proveedor o contratista solicita el establecimiento de una cuenta de usuario. No se permiten las cuentas grupales o compartidas dentro del perímetro de los sistemas que procesan o almacenan datos de clientes, a menos que se aprueben para fines comerciales específicos que se ajusten a determinados requisitos de cumplimiento. AWS lleva a cabo un proceso continuo de evaluación del riesgo, para identificar, evaluar y mitigar riesgos en toda la empresa. El proceso implica la elaboración e implementación de planes de tratamiento de riesgos, para mitigarlos según sea necesario. El equipo de gestión de riesgos de AWS monitorea y escala riesgos de forma continua, realizando evaluaciones de riesgo de controles recién implementados, al menos cada seis meses. El Informe SOC proporciona una evaluación independiente del entorno de control de AWS en relación con la seguridad, la disponibilidad y la confidencialidad del sistema. Se pueden encontrar más detalles sobre las medidas que AWS pone en práctica para mantener niveles de seguridad consistentemente altos, en el documento técnico Perspectiva general sobre procesos de seguridad, seguridad específica de servicios de AWS – página 20.	SEC-1 Gestión de credenciales y autenticación SEC-2 Control de acceso humano SEC-3 Control del acceso programático SEC-7 Clasificación de datos SEC-8 Protección de datos en reposo

RCA050: Las entidades/ prestadores deben garantizar el acceso irrestricto a la entidad y al BCRA, a toda documentación e información relativa al procesamiento, operaciones y procedimientos del STI cuando sea requerida.	**Responsabilidad compartida** Los clientes tienen pleno acceso de raíz o control administrativo sobre las cuentas, servicios y aplicaciones, y tienen una visibilidad completa de sus recursos, servicios y aplicaciones en la nube, para monitorear el uso y el registro, recopilar métricas, establecer alarmas y reaccionar automáticamente a los cambios. Los clientes de AWS también pueden proporcionar a los usuarios internos y a los reguladores un acceso lógico a su información y datos, si es necesario. Los clientes pueden validar los controles de seguridad en el entorno AWS a través de certificaciones e informes de AWS, incluyendo los informes SOC 1, 2 y 3, las certificaciones ISO 27001, 27017 y 27018, y los informes de cumplimiento del PCI DSS. Estos informes y certificaciones son elaborados por auditores independientes externos y dan fe del diseño y la eficacia operativa de los controles de seguridad de AWS. Los clientes pueden utilizar AWS Artifact, el portal de informes de cumplimiento automatizado disponible en la consola de gestión 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 documentos de cumplimiento y seguridad de AWS, incluidos informes de control de organizaciones de servicios (SOC), informes de la industria de las tarjetas de pago (PCI) y certificaciones de organismos de acreditación de distintas regiones y tipos de conformidad. Hay cinco informes SOC de AWS, todos 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 de seguridad, disponibilidad y confidencialidad SOC 2 de AWS (el alcance incluye sólo Amazon DocumentDB). • Informe tipo I de privacidad SOC 2 de AWS. • Informe de seguridad, disponibilidad y confidencialidad SOC 3 de AWS, disponible de manera pública como un documento técnico. Las auditorías internas y externas de AWS se planifican y realizan de acuerdo con la auditoría documentada y programada para examinar el rendimiento continuado de AWS en función de criterios basados en estándares, así como para identificar oportunidades de mejora general. Los criterios basados en estándares incluyen, pero no se limitan a, las normas profesionales ISO/IEC 27001, Programa Federal de Gestión de Riesgos y Autorizaciones (FedRAMP), el Instituto Americano de Contadores Públicos Certificados (AICPA): AT 801 (anteriormente Declaración de Estándares para los Compromisos de Atestación (SSAE) 16), y los Estándares Internacionales de Compromisos de Aseguramiento nº 3402 (ISAE 3402). Asimismo, el BCRA ha publicado directrices reglamentarias a través de Interpretaciones Normativas. Estas directrices han clarificado el alcance de las Normativas del BCRA con respecto a la tercerización a un CSP por las instituciones financieras. En junio de 2019, el BCRA publicó una interpretación normativa que reconoce que la revisión de las certificaciones internacionales de seguridad de la información y de sistemas de terceros (como las certificaciones ISO) y los informes de auditores externos independientes (como los informes SOC) son generalmente suficientes para satisfacer las facultades de acceso y auditoría del BCRA y la SEFyC con respecto a los CSP que prestan servicios a entidades reguladas. Esta clarificación resalta que dichas certificaciones, atestaciones e informes de auditoría de terceros son valiosos recursos de cumplimiento que benefician tanto a las instituciones financieras como al regulador para que puedan desempeñar sus funciones de supervisión respecto a las actividades tercerizadas. Para más información sobre estos informes de auditoría y certificaciones de terceros, consulte la página web del Programa de cumplimiento de AWS. Si desea saber más sobre el enfoque de AWS respecto al acceso a documentación e información, auditoría e inspección, y sobre cómo se pueden abordar estos requisitos en un Acuerdo Empresarial con AWS, póngase en contacto con su representante de AWS.	OPS-1 Determinación de prioridades SEC-1 Gestión de credenciales y autenticación

Requisito	Consideraciones	Consideraciones de Implementación (Prácticas de Buena Arquitectura)
RCA051: La entidad debe asegurar que el prestador del STI documente y respalde el nivel de controles implementados para la protección de los servicios provistos, por medio de mediciones independientes, auditorías externas y certificaciones de estándares internacionales.	**Responsabilidad compartida** AWS colabora con organismos de certificación externos y auditores independientes para proporcionar a los clientes información relevante sobre sus políticas, procesos y controles. Los clientes pueden aprovechar esta información para llevar a cabo sus procedimientos de evaluación y verificación de control, como exigen las Normativas del BCRA y otras leyes y regulaciones aplicables. Para más información sobre otras certificaciones y atestaciones de AWS, consulte la página web del Programa de cumplimiento de AWS. AWS ha establecido un programa de auditoría formal que incluye evaluaciones internas y externas continuas e independientes para validar la aplicación y la eficacia operativa del entorno de control de AWS. Las auditorías internas y externas se planifican y realizan de acuerdo con la auditoría documentada programada para examinar el rendimiento continuado de AWS en función de criterios basados en estándares y para identificar oportunidades de mejora general. Los criterios basados en estándares incluyen, pero no se limitan a, las normas profesionales ISO/IEC 27001, Programa Federal de Gestión de Riesgos y Autorizaciones (FedRAMP), el Instituto Americano de Contadores Públicos Certificados (AICPA): AT 801 (anteriormente Declaración de Estándares para los Compromisos de Atestación (SSAE) 16), y los Estándares Internacionales de Compromisos de Aseguramiento nº 3402 (ISAE 3402). Los clientes pueden utilizar AWS Artifact, el portal de informes de cumplimiento automatizado disponible en la consola de gestión 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 documentos de cumplimiento y seguridad de AWS, incluidos informes de control de organizaciones de servicios (SOC), informes de la industria de las tarjetas de pago (PCI) y certificaciones de organismos de acreditación de distintas regiones y tipos de conformidad.	OPS-1 Determinación de prioridades

Requisito	Consideraciones	Consideraciones de Implementación (Prácticas de Buena Arquitectura)
RCA052: Las entidades/ prestadores deben contar e implementar con una política homogénea de administración de credenciales, basada en la necesidad de uso/conocimiento, la separación de roles incompatibles y la prevención de colusiones, para el acceso a, pero sin limitarse a: • **Mecanismos de encripción de datos y canales de comunicación.** • **Usuarios privilegiados de la plataforma operativa/aplicativa.** • **Usuarios de emergencia/ contingencia.** • **Usuarios comunes.** **Asimismo, deberán asegurar un ciclo de vida de las credenciales, cuyos parámetros, reglas, algoritmos, piezas de software involucradas deberán ser actualizadas y debidamente comunicadas a las partes.**	**Responsabilidad del cliente** Los clientes conservan la propiedad y el control de su contenido cuando utilizan los servicios de AWS, y no ceden esa propiedad y control de su contenido a AWS. Los clientes tienen un control total sobre los servicios que utilizan y a quién facultan para acceder a su contenido y servicios, incluidas las credenciales necesarias. Los clientes controlan la forma en que configuran sus entornos y aseguran su contenido, incluyendo si cifran su contenido (en reposo y en tránsito). A su vez, eligen qué otras características y herramientas de seguridad utilizan y cómo las utilizan. AWS no cambia los ajustes de configuración del cliente, ya que estos ajustes son determinados y controlados por el cliente. Los clientes de AWS tienen la libertad de diseñar su arquitectura de seguridad para satisfacer sus necesidades de cumplimiento. Esta es una diferencia clave con respecto a las soluciones de alojamiento tradicionales en las que el proveedor decide la arquitectura. AWS proporciona formas de categorizar los datos de la organización en función de los niveles de sensibilidad. Mediante el uso de etiquetas de recursos, políticas IAM de AWS, KMS de AWS y CloudHSM de AWS, los clientes pueden definir e implementar políticas para la clasificación de datos.	SEC-2 Control de acceso humano SEC-3 Control del acceso programático SEC-7 Clasificación de datos SEC-8 Protección de datos en reposo SEC-9 Protección de datos en tránsito OPS-1 Determinación de prioridades

De Integridad y Registro (IR) - Sección 7.7.4

Estos requisitos técnicos y operativos están relacionados con la utilización de técnicas de control de la integridad y registro de los datos y las transacciones, así́ como el manejo de información sensible de los STI y las técnicas que brinden trazabilidad y permitan su verificación. Incluye, pero no se limita a transacciones, registros de auditoria y esquemas de validación.

Requisito	Consideraciones	Consideraciones de Implementación (Prácticas de Buena Arquitectura)
RIR003: Los registros colectados por los servicios provistos por el prestador, deben asegurar la trazabilidad de las acciones realizadas en la totalidad de las actividades, identificando quien (cuenta, origen, destino), qué (actividad, función, transacción), dónde (servicio, ubicación), cuando (tiempo), cómo (patrón, relación de eventos).	**Responsabilidad del cliente** AWS le ofrece a sus clientes herramientas para el gobierno y la trazabilidad de datos. Los clientes de AWS pueden usar herramientas como AWS CloudTrail, Amazon CloudWatch, AWS Config y AWS Config Rules para rastrear, monitorear, analizar y auditar eventos. AWS CloudTrail es un servicio que permite el gobierno, el cumplimiento, la auditoría operativa y la auditoría de riesgo de cuentas de AWS. Con AWS CloudTrail, los clientes pueden registrar, monitorear continuamente y conservar actividad de cuenta relacionada con acciones a través de la infraestructura de AWS. AWS CloudTrail proporciona un historial de eventos de la actividad de la cuenta de AWS, incluyendo acciones realizadas a través de la Consola de gestión de AWS, kits de desarrollo de software de AWS, herramientas de línea de comandos y otros servicios de AWS. Este historial de eventos simplifica el análisis de seguridad, el seguimiento de cambios en los recursos y la resolución de problemas. Amazon CloudWatch es un servicio que permite supervisar y gestionar recursos y ofrece una visibilidad completa de los recursos y aplicaciones de la nube para recopilar métricas, monitorear archivos de registro, establecer alarmas y reaccionar automáticamente a cambios. AWS Config es un servicio de gestión de la configuración de recursos que registra y evalúa configuraciones de sus recursos de AWS para permitir la auditoría de cumplimiento, el seguimiento de cambios en recursos y el análisis de seguridad.	OPS-4 Diseño de la carga de trabajo para entender su estado SEC-4 Detección e investigación de eventos de seguridad

RIR010: Los dispositivos/ equipamiento y/o piezas de software dispuestas por la entidad/prestador para el STI, deben asegurar que satisfacen un ciclo de vida y de desarrollo, basado en las siguientes etapas conceptuales: **a. Análisis de requerimientos.** **b. Adquisición/fabricación/ desarrollo.** **c. Prueba y homologación.** **d. Implementación.** **e. Operación y mantenimiento.** **f. Descarte y reemplazo.** **Asimismo, este ciclo, debe proveer los elementos de seguridad relacionados con, pero no limitados, a:** **g. Requisitos funcionales de seguridad.** **h. Tipos y características de validación de los datos de entrada.** **i. Granularidad de las funciones y los registros.** **j. Niveles de acceso.** **k. Control de cambios.** **l. l. Actualización y parches.**	**Responsabilidad compartida** Los clientes son responsables de gestionar todo el ciclo de vida de los dispositivos que poseen. AWS mantiene un enfoque sistemático de planificación y desarrollo de nuevos servicios para el entorno de AWS para garantizar que se cumplan los requisitos de calidad y seguridad con cada lanzamiento. La estrategia de AWS para el diseño y desarrollo de servicios consiste en definir claramente los servicios en términos de casos de uso por parte del cliente, rendimiento del servicio, requisitos de comercialización y distribución, producción y pruebas, y requisitos regulatorios y legales. El diseño de todos los servicios nuevos o cualquier cambio significativo de los servicios actuales sigue prácticas seguras de desarrollo de software y se controlan a través de un sistema de gestión de proyectos con participación multidisciplinaria. Los requisitos y especificaciones del servicio se establecen durante el desarrollo del mismo, teniendo en cuenta los requisitos regulatorios y legales, los compromisos contractuales del cliente y los requisitos para cumplir con la confidencialidad, integridad y disponibilidad del servicio. La revisión de los servicios se completan como parte del proceso de desarrollo. AWS rastrea, documenta y verifica acciones de saneamiento y eliminación de medios de almacenamiento. Toda eliminación de medios de almacenamiento es llevada a cabo por personal designado de AWS. Los dispositivos de almacenamiento utilizados para almacenar los datos de los clientes son clasificados por AWS como Críticos y tratados como tales, a lo largo de sus ciclos de vida. AWS tiene estándares exigentes sobre cómo instalar, mantener y eventualmente destruir los dispositivos cuando ya no son útiles. Cuando un dispositivo de almacenamiento ha llegado al final de su vida útil, AWS retira del servicio el dispositivo utilizando las técnicas detalladas en NIST 800-88. El dispositivo que almacenó los datos del cliente se mantiene bajo control de AWS hasta que se haya retirado de servicio de forma segura. Los hosts de AWS se borran o se sobrescriben de forma segura antes de su reutilización. Los dispositivos de almacenamiento de AWS se borran o se desmagnetizan de manera segura y se destruyen físicamente antes de salir de las zonas de seguridad de AWS. Para validar los procesos y procedimientos de borrado seguro de AWS, los auditores externos revisan las directrices dentro de la política de protección de medios de AWS, examinan el equipo de desmagnetización y los contenedores de trituración seguros ubicados dentro de las instalaciones de AWS, examinan el historial de notificaciones que han documentado la destrucción de un disco duro dentro de un centro de datos y el proceso de un dispositivo siendo borrando y removido del entorno.	REL-8 Implementación de cambios OPS-6 Mitigación de riesgos de implementación OPS-7 Apoyo a una carga de trabajo

Requisito	Consideraciones	Consideraciones de Implementación (Prácticas de Buena Arquitectura)
	• **Eliminación de datos para almacenamiento basado en dispositivos de bloque (EBS, RDS, unidades efímeras, etc.):** para asegurar que el contenido del cliente se borre correctamente, AWS elimina los medios de almacenamiento subyacentes al reabastecerse (re-provisioning) y no al desabastecerse (de-provisioning). Los procesos que borran el contenido al liberar un activo (volumen, objeto, etc.) son menos fiables que los procesos que sólo vuelven a proporcionar almacenamiento limpio a los clientes. Los servidores físicos pueden reiniciarse en cualquier momento por muchas razones (corte de energía, interrupción o fallo del proceso del sistema, etc.), lo que podría dejar un procedimiento de borrado en un estado incompleto. Los clientes no tienen acceso a dispositivos de bloque o a medios físicos que se utilizaron anteriormente para almacenar el contenido de otro cliente. Por ejemplo, en el caso de EBS, los clientes sólo ven su contenido o ceros (por ejemplo, un disco vacío) después de escribir un bloque o un bloque parcial. Borrar bloques en el momento en que se reabastece la capacidad de almacenamiento es suficiente para garantizar que el contenido anterior no pueda recuperarse desde un nuevo volumen u objeto. • **Eliminación de datos para servicios de dispositivos que no son de bloque:** para servicios como Amazon S3 o DynamoDB, los clientes nunca ven un dispositivo de bloque adjunto, sólo los objetos y el camino a ese objeto (por ejemplo, una tabla). Cuando un cliente elimina un activo en estos servicios, la eliminación del mapeo entre un identificador o clave de activos y el contenido subyacente comienza inmediatamente. Una vez eliminado el mapeo, el contenido ya no es accesible y no puede ser procesado por una aplicación.	

Requisito	Consideraciones	Consideraciones de Implementación (Prácticas de Buena Arquitectura)
RIR011: Las entidades/ prestadores deben ejecutar un proceso de homologación de dispositivos/equipamientos y/o piezas de software para interactuar con el STI, garantizando la verificación de todos los aspectos de diseño, funcionalidad, interoperabilidad y características de seguridad definidos en las etapas de adquisición/fabricación/ desarrollo e implementación.	**Responsabilidad compartida** Los clientes son responsables de gestionar todo el ciclo de vida de los dispositivos que poseen. AWS mantiene un enfoque sistemático de planificación y desarrollo de nuevos servicios para el entorno de AWS para garantizar que se cumplan los requisitos de calidad y seguridad con cada lanzamiento. La estrategia de AWS para el diseño y desarrollo de servicios consiste en definir claramente los servicios en términos de casos de uso por parte del cliente, rendimiento del servicio, requisitos de comercialización y distribución, producción y pruebas, y requisitos regulatorios y legales. El diseño de todos los servicios nuevos o cualquier cambio significativo de los servicios actuales sigue prácticas seguras de desarrollo de software y se controlan a través de un sistema de gestión de proyectos con participación multidisciplinaria. Los requisitos y especificaciones del servicio se establecen durante el desarrollo del mismo, teniendo en cuenta los requisitos regulatorios y legales, los compromisos contractuales del cliente y los requisitos para cumplir con la confidencialidad, integridad y disponibilidad del servicio. La revisión de los servicios se completan como parte del proceso de desarrollo.	OPS-1 Determinación de prioridades OPS-5 Reducción de defectos, facilitación de la corrección y mejora del flujo en la producción REL-8 Implementación de cambios OPS-6 Mitigación de riesgos de implementación OPS-7 Apoyo a una carga de trabajo

Requisito	Consideraciones	Consideraciones de Implementación (Prácticas de Buena Arquitectura)
RIR020: Las entidades/ prestadores deben contar con mecanismos preventivos y correctivos para la atención de reclamos por el acceso, modificación y eliminación de datos personales, ante requerimientos al amparo de la protección de derechos del cliente.	**Responsabilidad del cliente** Los clientes conservan la propiedad y el control de su contenido cuando utilizan los servicios de AWS. Tal como se explicó en la sección Seguridad y responsabilidad compartida, es importante señalar que, al utilizar los servicios de AWS, los clientes mantienen el control de sus datos y son responsables de la gestión de los requisitos de seguridad del contenido crítico. Esto permite que los usuarios puedan controlar todo el ciclo de vida de su contenido en AWS y gestionarlo de acuerdo con sus propias necesidades regulatorias, incluso para atender las solicitudes de acceso, modificación y eliminación de datos personales por parte de los interesados. Los clientes pueden utilizar los controles disponibles en los servicios de AWS, incluidos los controles de configuración de seguridad, para el tratamiento de datos personales. Para obtener más información acerca del Modelo de responsabilidad compartida y sus implicaciones para el almacenamiento y procesamiento de datos personales utilizando AWS, consulte el documento técnico de AWS Utilizando AWS en el contexto de privacidad común y Consideraciones de la protección de datos, el sitio web de Preguntas frecuentes sobre privacidad de datos y nuestro sitio de Privacidad de datos de Argentina, el cual incluye un resumen de la Ley de Protección de Datos Personales de Argentina n° 25.326 (LPDP) y preguntas frecuentes.	SEC-1 Gestión de credenciales y autenticación SEC-2 Control de acceso humano SEC-3 Control del acceso programático SEC-7 Clasificación de datos SEC-8 Protección de datos en reposo SEC-9 Protección de datos en tránsito

Requisito	Consideraciones	Consideraciones de Implementación (Prácticas de Buena Arquitectura)
RIR021: Las entidades/ prestadores deben garantizar y establecer los mecanismos de recupero de los activos de información ante rescisión/ terminación y/o interrupción indefinida de los servicios y/o relocalización, respetando las condiciones de seguridad de la información y continuidad de las operaciones.	**Responsabilidad del cliente** Los clientes de AWS pueden aprovechar las características de la infraestructura de AWS y los servicios de AWS para cumplir una amplia gama de objetivos de recuperación. El uso de múltiples zonas de disponibilidad, incluso dentro de una misma región, puede aumentar la capacidad de recuperación en comparación con un entorno local. Las zonas de disponibilidad están concebidas para mitigar el riesgo de desastres naturales y otras perturbaciones que puedan producirse. Las zonas de disponibilidad están físicamente separadas dentro de una región metropolitana y se encuentran en diferentes zonas de inundación (flood zones). Cada zona de disponibilidad está diseñada como una zona de fallo independiente y los procesos automatizados alejan el tráfico de clientes de la zona afectada en caso de fallo. Los clientes pueden alcanzar objetivos extremadamente altos de tiempo de recuperación y puntos de recuperación mediante el uso de múltiples zonas de disponibilidad y la replicación de datos. Los servicios de AWS permiten la exportación de contenido por parte de los clientes bajo demanda, utilizando la consola de gestión de AWS, las API y otros métodos de entrada. Por ejemplo, AWS Snowball proporciona dispositivos diseñados para ser seguros para transferir grandes cantidades de datos dentro y fuera de la nube de AWS. Para más información acerca de la migración de datos dentro y fuera de la nube de AWS, consulte Migración y transferencia en AWS	REL-9 Respaldo de datos REL-13 Plan de recuperación ante desastres

Requisito	Consideraciones	Consideraciones de Implementación (Prácticas de Buena Arquitectura)
RIR022: Los recursos e información que se utilicen en el STI deben estar inventariados con su correspondiente identificación del propietario e indicando los parámetros de eliminación segura y sus parámetros de validación en el ciclo de vida del dato.	**Responsabilidad del cliente** AWS considera que el inventario y la gestión del ciclo de vida de los datos de los clientes es una acción que deben completar las instituciones financieras. AWS ofrece Amazon Macie, un servicio de seguridad que utiliza el aprendizaje automático para ayudar a los clientes a descubrir, clasificar y proteger automáticamente los datos sensibles en AWS. Este servicio plenamente gestionado (fully managed) monitorea continuamente la actividad de acceso a los datos en busca de anomalías y genera alertas detalladas cuando detecta el riesgo de acceso no autorizado o de fugas de datos inadvertidas, como el acceso a datos confidenciales que se han hecho accesibles externamente por accidente. Amazon Macie está certificado según estándares reconocidos internacionalmente, como ISO 27017 para seguridad en la nube e ISO 27018 para privacidad en la nube. AWS proporciona formas de categorizar los datos de la organización en función de los niveles de sensibilidad. Mediante el uso de etiquetas de recursos, políticas IAM de AWS, KMS de AWS, los clientes pueden definir e implementar políticas para clasificación de datos.	SEC-7 Clasificación de datos
RIR023: Las entidades/ prestadores deben establecer un ciclo de vida de los datos de registro de las actividades, según lo establece el requisito RIR003, cumpliendo con los requerimientos legales y las previsiones de seguridad para su almacenamiento, inalterabilidad por el tiempo legal de conservación y su accesibilidad a los responsables del control para soporte de investigaciones forenses en casos de incidentes de seguridad y detección de brechas de seguridad.	**Responsabilidad del cliente** AWS ofrece a los clientes múltiples herramientas para el gobierno y trazabilidad de datos. Consulte nuestros comentarios en el requisito **RIR003**.	SEC-4 Detección e investigación de eventos de seguridad

RIR024: Las entidades/ prestadores, deben establecer una política de encripción de los datos estén en reposo, tránsito o en ambos estados, incluyendo la asignación de la responsabilidad para los controles definidos en cada estado del dato.	**Responsabilidad del cliente** Los clientes controlan la forma en que configuran sus entornos y aseguran su contenido, incluyendo si cifran su contenido (en reposo y en tránsito). A su vez, eligen qué otras características y herramientas de seguridad utilizan y cómo las utilizan. AWS está diseñado para proteger la confidencialidad e integridad de los datos transmitidos mediante la comparación de un hash criptográfico de datos transmitidos. Esto se hace para ayudar a asegurar que el mensaje no se corrompa o altere en tránsito. Los datos que han sido corrompidos o alterados en tránsito son rechazados inmediatamente. AWS proporciona varios métodos para que los clientes manejen sus datos de forma segura: • Tras la comunicación inicial con una imagen de máquina de Amazon (AMI por sus siglas en inglés) de Windows proporcionada por AWS, AWS permite una comunicación segura al configurar servicios de terminal en la instancia y generando un certificado de servidor X.509 autofirmado único y entregando la huella digital del certificado al usuario a través de un canal de confianza. • AWS permite además una comunicación segura con los AMI de Linux mediante la configuración de Secure Shell (SSH) en la instancia, generando una clave de host única y entregando la huella digital de la clave al usuario a través de un canal de confianza. Las claves maestras de los clientes (Customer Master Keys, o CMK por sus siglas en inglés) utilizadas para operaciones criptográficas en el Servicio de gestión de claves (AWS Key Management Service, o KMS por sus siglas en inglés) de AWS, incluidas las operaciones de los empleados de AWS, están aseguradas por controles tanto técnicos como operativos. Por su diseño, ningún empleado de AWS puede acceder al material físico de CMK durante su servicio, debido a técnicas que no permiten almacenar nunca claves maestras de texto plano en el disco persistente, que permiten el uso, pero no la persistencia de las mismas en la memoria volátil, y que limitan cuáles usuarios y sistemas pueden conectarse a los hosts del servicio. Además, se imponen controles de acceso multipartito para las operaciones en los dispositivos de seguridad reforzados por KMS que manejan CMK de texto plano en memoria. AWS les permite a los clientes abrir una sesión segura y encriptada a los servidores de AWS usando HTTPS (Transport Layer Security [TLS]). Además, AWS ofrece a los clientes la posibilidad de añadir una capa adicional de seguridad a los datos en reposo en la nube, proporcionando características de cifrado escalables y eficientes. Es responsabilidad del cliente de AWS habilitar estas características para sus sistemas. Estas características incluyen:	SEC-8 Protección de datos en reposo SEC-9 Protección de datos en tránsito

Requisito	Consideraciones	Consideraciones de Implementación (Prácticas de Buena Arquitectura)
	• Capacidades de cifrado de datos disponibles en los servicios de almacenamiento y bases de datos de AWS, como Amazon EBS, Amazon S3, Amazon Glacier, Amazon RDS para Oracle, Amazon RDS para SQL Server y Amazon Redshift. • Las opciones flexibles de administración de claves, incluyendo KMS, permiten a los clientes elegir entre permitir que AWS gestione las claves de cifrado o permitir que los clientes mantengan un control completo sobre sus claves. • Los clientes de AWS pueden emplear el cifrado del lado del servidor (SSE) con claves gestionadas por Amazon S3 (SSE-S3), SSE con claves gestionadas por AWS KMS (SSE-KMS), o SSE con claves proporcionadas por el cliente (SSE-C). Para obtener más información, consulte Protección de datos mediante el cifrado del lado del servidor.	

RIR025: Las entidades/ prestadores deben asegurar una separación lógica de los ambientes de procesamiento, almacenamiento, transporte y recuperación de datos de la entidad respecto del prestador, otras entidades y terceros. Asimismo, deben asegurar que los dispositivos/equipamientos y piezas de software que se empleen o accedan a los entornos de la entidad, deben restringirse a los necesarios y homologados según lo indicado en el requisito RIR011.	**Responsabilidad compartida** Los clientes son responsables de la separación de los entornos y los datos que crean en AWS. Los clientes deben gestionar el acceso a su contenido y recursos a través de usuarios, grupos, permisos y credenciales que los clientes controlan. El Manual de separación lógica ayudará a las instituciones financieras a comprender la separación lógica en la nube y demuestra sus ventajas sobre un modelo tradicional de separación física. Los entornos de los clientes están lógicamente segregados para evitar que los usuarios y clientes accedan a recursos no asignados a ellos. Los clientes mantienen un control total sobre quién tiene acceso a sus datos. Los servicios que proporcionan ambientes operativos virtualizados a los clientes (es decir, EC2) aseguran que los clientes estén separados unos de otros y evitan la ampliación de los privilegios de los usuarios y la revelación de información a través de los hipervisores y el aislamiento de la instancia. Las diferentes instancias que funcionan en la misma máquina física están aisladas unas de otras a través del hipervisor. Además, el cortafuegos (firewall) de Amazon EC2 reside dentro de la capa de hipervisor, entre la interfaz de la red física y la interfaz virtual de la instancia. Todos los paquetes deben pasar a través de esta capa; así, los vecinos de una instancia no tienen más acceso a esa instancia que cualquier otro host de Internet y pueden ser tratados como si estuvieran en hosts físicos separados. La memoria física de acceso aleatorio (RAM) se separa utilizando mecanismos similares. Las instancias del cliente no tienen acceso a los dispositivos de disco físico, sino que se les presentan discos virtualizados. La capa de virtualización de discos patentada de AWS borra automáticamente cada bloque de almacenamiento antes de ponerlo a disposición para su uso, lo que protege los datos de un cliente de ser expuestos involuntariamente a otro. Los clientes pueden proteger aún más sus datos utilizando los mecanismos tradicionales de cifrado de sistema de archivos o, en el caso de los volúmenes de Amazon Elastic Block Store (Amazon EBS), al habilitar el cifrado del disco gestionado por AWS. Un Host Dedicado (Dedicated Host) es también un servidor físico que está dedicado para el uso del cliente. Con un Host Dedicado, los clientes tienen visibilidad y control sobre cómo se colocan las instancias hipervisadas en el servidor. Las instancias bare metal son dispositivos de hardware no hipervisados. Utilizando la tecnología Nitro de AWS para la descarga de red y almacenamiento, así como el chip de seguridad Nitro para eliminar los riesgos asociados con el arrendamiento único en serie sobre bare metal, los clientes tienen acceso directo al hardware de Amazon EC2. Estas instancias bare metal son miembros de pleno derecho del servicio Amazon EC2 y tienen acceso a servicios como Amazon VPC y Amazon Elastic Block Store (EBS).	SEC-5 Protección de redes REL-2 Topología de red SEC-6 Protección de recursos de computación OPS-5 Reducción de defectos, facilitación de la corrección y mejora del flujo en la producción

De Monitoreo y Control (MC) - Sección 7.7.5

Estos requisitos definen la recolección, análisis y control de eventos ante fallas, indisponibilidad, intrusiones y otras situaciones que afecten los servicios ofrecidos por los prestadores de STI, y que puedan generar un daño eventual sobre la infraestructura y la información.

Requisito	Consideraciones	Consideraciones de Implementación (Prácticas de Buena Arquitectura)
RMC003: Las entidades/ prestadores deben realizar un seguimiento en los STI de los cambios de configuración de seguridad y verificar los niveles de actualización de: sistemas operativos, bases de datos, vínculos de comunicación, herramientas de prevención y detección de códigos maliciosos, equipamientos de seguridad de red, controladores de tráfico y cualquier otra herramienta de seguridad. Deben incluir, pero no limitarse a: **a) Seguimiento de privilegio y derechos de acceso;** **b) Procesos de copia, resguardo y recuperación de información;** **c) Disponibilidad de los dispositivos/equipamiento;** **d) Alarmas, alertas y problemas detectados por los sistemas de registro de eventos.**	**Responsabilidad compartida** Los clientes son responsables de definir su modelo operativo basado en los servicios de AWS que elijan utilizar. Los cambios en sus entornos pueden ser detectados y rastreados usando los servicios de AWS como AWS Config para valorar, auditar y evaluar las configuraciones de los recursos 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 entrantes a la red y salientes de la red. Estas herramientas monitorean el uso del servidor y de la red, las actividades de escaneo de puertos, el uso de aplicaciones y los intentos de intrusión no autorizados. Las herramientas tienen la capacidad de establecer umbrales personalizados de métricas de rendimiento para actividad inusual y las alarmas están configuradas para notificar automáticamente al personal de operaciones y de gestión cuando se cruzan los umbrales de alerta temprana en las métricas operativas clave. Las respuestas se realizan de acuerdo con los procesos y procedimientos de respuesta a incidentes. AWS Security realiza regularmente escaneos de vulnerabilidad en la infraestructura subyacente, la aplicación web y las bases de datos en el entorno de AWS utilizando una variedad de herramientas. Se llevan a cabo evaluaciones de vulnerabilidad externa por un proveedor externo aprobado por AWS al menos trimestralmente, y los problemas identificados son investigados y rastreados para su resolución. Se monitorean y evalúan las vulnerabilidades que se identifican, y se diseñan, implementan y operan contramedidas para compensar las vulnerabilidades conocidas y las recientemente identificadas. Los equipos de seguridad de AWS también se suscriben a boletines de noticias para defectos de los proveedores correspondientes y monitorean proactivamente los sitios web de los proveedores y otros medios relevantes para encontrar nuevos parches. Los clientes de AWS también tienen la posibilidad de informar de sus problemas a AWS a través del sitio web de Informes de vulnerabilidad de AWS. Los clientes de AWS son responsables de todos los escaneos, pruebas de penetración, monitoreo de la integridad de los archivos y detección de intrusos para sus instancias y aplicaciones de Amazon EC2 y Amazon ECS. Los escaneos deben incluir las direcciones IP del cliente y no los puntos finales (end points) de AWS. Los puntos finales de AWS se prueban como parte de los escaneos de vulnerabilidad de cumplimiento de AWS.	OPS-4 Diseño de la carga de trabajo para entender su estado SEC-1 Gestión de credenciales y autenticación SEC-4 Detección e investigación de eventos de seguridad REL-9 Respaldo de datos

Requisito	Consideraciones	Consideraciones de Implementación (Prácticas de Buena Arquitectura)
RMC004: Las entidades/prestadores deben disponer de mecanismos monitoreo transaccional en los STI que operen basados en características del perfil y patrón transaccional del cliente en alguno de los siguientes modelos de acción: **a) Preventivo. Detectando, disparando acciones de comunicación con el cliente por vías alternativas antes de confirmar operaciones.** **b) Reactivo. Detectando y disparando acciones de comunicación con el cliente en forma posterior a la confirmación de operaciones sospechosas.** **c) Asumido. Detectando y asumiendo la devolución de las sumas involucradas ante los reclamos del cliente por desconocimiento de transacciones efectuadas.**	**Responsabilidad compartida** Consulte nuestros comentarios en **RMC003**.	OPS-4 Diseño de la carga de trabajo para entender su estado SEC-4 Detección e investigación de eventos de seguridad
RMC006: A partir de los registros colectados por los recursos del STI asociados al escenario, las entidades/ prestadores deben realizar una clasificación y determinación de los eventos de seguridad, una definición de los límites y umbrales de compromiso, niveles de comportamiento normal/ inesperado y establecer las acciones de acuerdo con cada clasificación y límite determinados.	**Responsabilidad del cliente** Los clientes son responsables de definir su modelo operativo basado en los servicios de AWS que elijan utilizar. Los clientes de AWS pueden usar herramientas como AWS CloudTrail, Amazon CloudWatch y AWS Config para rastrear, monitorear, analizar y auditar eventos. Si estas herramientas identifican un evento que se analiza y se clasifica como un incidente, ese "evento calificado" planteará un incidente y desencadenará el proceso de gestión de incidente y las medidas de respuesta apropiadas necesarias para mitigarlo.	SEC-4 Detección e investigación de eventos de seguridad SEC-10 Respuesta ante un incidente
RMC014: Las entidades/prestadores deben determinar, documentar y procedimentar los recursos, dispositivos/equipamientos y piezas de software para monitorear las actividades de los STI.	**Responsabilidad del cliente** Los clientes son responsables de definir su modelo operativo basado en los servicios de AWS que elijan utilizar.	No aplica.

Requisito	Consideraciones	Consideraciones de Implementación (Prácticas de Buena Arquitectura)
RMC015: Las entidades/prestadores deben establecer formalmente y ejecutar periódicamente tareas de prueba y análisis de vulnerabilidades de los recursos asociados al STI en todos sus procesos críticos.	**Responsabilidad del cliente** Los clientes pueden usar los servicios de AWS para realizar pruebas de penetración y pruebas de eventos simulados. Para más información, consulte Pruebas de penetración.	SEC-5 Protección de redes SEC-6 Protección de recursos de computación

De Gestión de Incidentes (GI) - Sección 7.7.6

Estos requisitos técnicos y operativos definen el tratamiento de los eventos y consecuentes incidentes de seguridad en los STI, su detección, evaluación, contención y respuesta, así como las actividades de escalamiento y corrección del entorno técnico y operativo.

Requisito	Consideraciones	Consideraciones de Implementación (Prácticas de Buena Arquitectura)
RGI001: Las entidades/ prestadores deben realizar con una periodicidad mínima anual y con base en el análisis de riesgo de los activos informáticos asociados al escenario, un análisis de los incidentes ocurridos y un reporte que sirva para establecer medidas de protección, contenidos del programa de capacitación y concientización, modificaciones a la registración y control de eventos, y una redefinición de las alertas, límites y umbrales.	**Responsabilidad compartida** AWS considera que el desarrollo y la implementación de mecanismos y planes para detectar, responder y gestionar incidentes de seguridad informática es una responsabilidad compartida entre AWS y las instituciones financieras. Los planes de respuesta de seguridad informática de los clientes deben incluir mecanismos para gestionar todas las etapas pertinentes de un incidente, incluida la fase de escalación y la presentación de informes. Las instituciones financieras deben examinar y poner a prueba anualmente sus planes de respuesta en materia de seguridad informática para asegurarse de que siguen siendo eficaces y adecuados para su propósito. Los clientes de AWS pueden usar herramientas como AWS CloudTrail, Amazon CloudWatch, AWS Config, Amazon GuardDuty y Security Hub, para rastrear, monitorear, analizar y auditar eventos. Si estas herramientas identifican un evento que se analiza y se clasifica como un incidente, ese "evento calificado" planteará un incidente y desencadenará el proceso de gestión de incidente y las medidas de respuesta apropiadas necesarias para mitigarlo. En cuanto al proceso de gestión de incidentes de AWS, AWS ha implementado una política y un programa de respuesta a incidentes formales y documentados. La política aborda el propósito, el alcance, las funciones, las responsabilidades y el compromiso de gestión. Las pruebas de respuesta a incidentes se ejecutan anualmente como parte del plan de respuesta a incidentes. Las pruebas incluyen múltiples escenarios, posibles vectores de ataque, incluyen a integradores de sistemas en la presentación de informes y la coordinación (cuando corresponda), y diversas vías de presentación de informes/detección (es decir, presentación de informes/detección por parte del cliente, presentación de informes/detección por parte de AWS).	SEC-4 Detección e investigación de eventos de seguridad SEC-10 Respuesta ante un incidente

Requisito	Consideraciones	Consideraciones de Implementación (Prácticas de Buena Arquitectura)
RGI002: La identificación de incidentes debe estar basada al menos en alertas tempranas, estadísticas de tipo/frecuencia/patrón de incidentes y recomendaciones de seguridad informática.	**Responsabilidad compartida** Como parte del modelo de responsabilidad compartida en materia de seguridad, el monitoreo de eventos de seguridad debe ser realizado tanto por AWS como por la institución financiera. Los clientes de AWS pueden usar herramientas como AWS CloudTrail, Amazon CloudWatch, AWS Config, Amazon GuardDuty y Security Hub, para rastrear, monitorear, analizar y auditar eventos. Si estas herramientas identifican un evento que se analiza y se clasifica como un incidente, ese "evento calificado" planteará un incidente y desencadenará el proceso de gestión de incidente y las medidas de respuesta apropiadas necesarias para mitigarlo. AWS ha implementado una política y un programa formal y documentado de respuesta a incidentes, que puede ser revisado en el informe SOC 2. Los clientes también pueden ver todas las notificaciones de seguridad a través del AWS Service Health Dashboard o el AWS Personal Health Dashboard. El monitoreo y las alarmas están configuradas por AWS para identificar y notificar al personal operativo y de gestión sobre incidentes cuando se cruzan los umbrales de alerta temprana en las métricas operativas. AWS requiere que el equipo de seguridad y/o del servicio afectado realice un análisis post mortem para determinar la causa del incidente, así como para documentar las lecciones aprendidas.	OPS-10 Gestión de la carga de trabajo y eventos de las operaciones REL-6 Monitoreo de recursos REL-5 Resistencia a fallos de componentes PERF-7 Monitoreo de los recursos para asegurar que se están desempeñando como se espera
RGI003: La gestión de incidentes de seguridad puede ejecutarse en forma tercerizada, pero debe ser coordinada con personal de la entidad financiera.	**Responsabilidad compartida** AWS considera que el desarrollo y la implementación de mecanismos y planes para detectar, responder y gestionar incidentes de seguridad informática es una responsabilidad compartida entre AWS y las instituciones financieras. Consulte nuestros comentarios para los requisitos **RGI001/RGI002**.	SEC-10 Respuesta ante un incidente

RGI005: Los incidentes detectados deben recibir un tratamiento regular con un escalamiento definido formalmente.	**Responsabilidad compartida** AWS considera que el desarrollo y la implementación de mecanismos y planes para detectar, responder y gestionar incidentes de seguridad informática es una responsabilidad compartida entre AWS y las instituciones financieras. Los programas de acción para la seguridad informática de los clientes deben incluir mecanismos para gestionar todas las etapas pertinentes de un incidente, incluidas la fase de escalación y la presentación de informes. Los clientes de AWS pueden usar herramientas como AWS CloudTrail, Amazon CloudWatch, AWS Config, Amazon GuardDuty y Security Hub, para rastrear, monitorear, analizar y auditar eventos. Si estas herramientas identifican un evento que se analiza y se clasifica como un incidente, ese "evento calificado" planteará un incidente y desencadenará el proceso de gestión de incidente y las medidas de respuesta apropiadas necesarias para mitigarlo. En cuanto al proceso de gestión de incidentes de AWS, AWS ha implementado una política y un programa de respuesta a incidentes formales y documentados. La política aborda el propósito, el alcance, las funciones, las responsabilidades y el compromiso de gestión. AWS utiliza un enfoque de tres fases para gestionar incidentes: 1. **Fase de activación y notificación:** los incidentes para AWS comienzan con la detección de un evento. Los eventos se originan a partir de varias fuentes como: ○ Métricas y alarmas - AWS mantiene una capacidad excepcional de percepción situacional (situational awareness). La mayoría de los problemas se detectan rápidamente por medio del monitoreo y alarmas, 24/7 los 365 días del año, de dashboards de servicio y métricas en tiempo real. La mayoría de los incidentes se detectan de esta manera. AWS utiliza alarmas indicadoras tempranas para identificar de forma proactiva los problemas que pueden afectar en última instancia a los clientes. ○ Notificaciones de problemas enviadas por un empleado de AWS. ○ Llamadas a la línea de soporte técnico 24/7 los 365 días del año. Si el evento cumple con los criterios de incidente, el ingeniero de soporte de guardia correspondiente utiliza la herramienta de gestión de eventos para iniciar una intervención y contactar a los encargados de resolución del programa correspondiente (por ejemplo, el equipo de Seguridad). Los encargados de resolución realizarán un análisis del incidente para determinar si deben contactarse más encargados de resolución y para determinar la raíz del problema aproximada. 2. **Fase de recuperación -** Los encargados de resolución correspondientes realizarán una reparación de averías (break fix) para tratar el incidente. Después de realizar la solución de problemas, la reparación de averías	OPS-10 Gestión de la carga de trabajo y eventos de las operaciones SEC-4 Detección e investigación de eventos de seguridad SEC-10 Respuesta ante un incidente

(break fix) y los componentes afectados, el responsable de la llamada asignará la documentación de seguimiento y las acciones de seguimiento y pondrá fin al compromiso de la llamada.

3. **Fase de reconstitución** – El responsable de la llamada declarará la fase de recuperación completa después de que se hayan atendido las actividades de reparación pertinentes. El análisis post mortem y de la causa raíz del incidente se asignará al equipo correspondiente. Los resultados del estudio post mortem serán revisados por los directivos superiores correspondientes y las medidas, como los cambios de diseño, se plasmarán en un documento de Corrección de errores (Correction of Errors o sus siglas en inglés, COE) y se seguirán hasta su finalización.

Para asegurar la efectividad del plan de Gestión de incidentes de AWS, AWS lleva a cabo pruebas de respuesta a incidentes. Estas pruebas proporcionan una excelente cobertura para el descubrimiento de defectos y modos de fallo previamente desconocidos. Además, permiten a los equipos de seguridad y de servicios de AWS poner a prueba los sistemas para determinar el posible impacto en los clientes y preparar mejor al personal para manejar incidentes como la detección y el análisis, la contención, la erradicación
y recuperación y las actividades posteriores a los incidentes.

De Continuidad de las Operaciones (CO) - Sección 7.7.7

Estos requisitos están relacionados con los recursos y tareas estratégicas y operativas para prevenir, contener y recuperar los procesos críticos del negocio, los servicios financieros y la información crítica ante fallas que afecten la disponibilidad de los STI y la infraestructura informática que los soporta.

Requisito	Consideraciones	Consideraciones de Implementación (Prácticas de Buena Arquitectura)
RCO001: Se debe contar con la provisión de los recursos necesarios para la creación, mantenimiento, actualización y prueba de un plan de continuidad del procesamiento de datos. El mismo debe ser operable y funcional, en base a los requerimientos acordados en el STI, propios de la entidad y regulados por el BCRA.	**Responsabilidad compartida** Los clientes son responsables de implementar adecuadamente la planificación de contingencia, la capacitación y las pruebas de sus sistemas alojados en AWS. AWS les proporciona a los clientes la capacidad de implementar un sólido plan de continuidad, que incluye la utilización de frecuentes copias de seguridad de instancias del servidor, la replicación de redundancia de datos y la flexibilidad para colocar instancias y almacenar datos dentro de múltiples regiones geográficas, así como a través de múltiples zonas de disponibilidad dentro de cada región. En caso de fallo, los procesos automatizados alejan el tráfico de datos del cliente de la zona afectada. Cada zona de disponibilidad está diseñada como una zona de fallo independiente. Esto significa que las zonas de disponibilidad están típicamente separadas físicamente dentro de una región metropolitana y se encuentran en diferentes planos de influencia. Los clientes utilizan AWS para permitir una recuperación ante desastres más rápida de sus sistemas de TI críticos, sin incurrir en el gasto de infraestructura de un segundo sitio físico. La nube AWS es compatible con muchas arquitecturas populares de recuperación ante desastres (Disaster Recovery, o DR por sus siglas en inglés), desde los entornos de "luz piloto" que están listos para ampliarse en cualquier momento, hasta los entornos de "espera en caliente" que permiten una rápida conmutación por error. La infraestructura de AWS tiene un alto nivel de disponibilidad y les proporciona a los clientes las características necesarias para implementar una arquitectura de TI resistente. AWS ha diseñado sus sistemas para tolerar fallos del sistema o del hardware con un impacto mínimo para el cliente. Además del suministro de energía ininterrumpida discreta (UPS por sus siglas en inglés) y de las instalaciones de generación eléctrica de respaldo en el lugar, cada uno de ellos se alimenta a través de diferentes redes eléctricas proporcionadas por servicios independientes para reducir aún más los puntos de fallo únicos. Las zonas de disponibilidad están conectadas de forma reiterada a múltiples proveedores de conectividad de red de nivel 1. Además, el plan de continuidad de negocio de AWS detalla el proceso que AWS sigue en caso de una interrupción, desde la detección hasta la desactivación. Este plan está diseñado para recuperar y reconstituir AWS utilizando 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 eficacia de los esfuerzos de recuperación y reconstitución y minimizar el tiempo de interrupción del sistema debido a errores y omisiones. AWS pone a prueba el plan de continuidad del negocio y sus procedimientos asociados al menos una vez al año para asegurar la efectividad del plan y la preparación de la organización para ejecutar el plan.	REL-9 Respaldo de datos REL-5 Resistencia a fallos de los componentes REL-12 Prueba de tolerancia a fallos REL-13 Plan de recuperación ante desastres

RCO002: Las entidades/prestadores deben definir, acordar, documentar y poner en ejecución los métodos para determinar el impacto de un evento que interrumpa las actividades de la organización tanto de la entidad, el prestador o terceros subcontratados contemplando, pero no limitándose, a: **i) Identificación de recursos críticos, incluyendo usuarios operativos y de control;** **ii) Identificación de todas las dependencias, incluyendo procesos aplicaciones, pares, y terceros subcontratados;** **iii) Detección de las amenazas de los recursos críticos;** **iv) Determinación del impacto de las interrupciones planeadas o no, y su variación en el tiempo;** **v) Establecimiento de un periodo máximo tolerable de interrupción;** **vi) Establecimiento de periodos de recuperación parciales y totales;** **vii) Establecimiento del tiempo máximo tolerable de interrupción para la recuperación de recursos críticos;** **viii) Estimación de los recursos requeridos para la continuidad y eventual restauración de la operatoria y locaciones alternativas.** **Debe asimismo, darse participación activa a los responsables primarios de los procesos y recursos críticos, garantizando una cobertura completa de los asociados al STI.**	**Responsabilidad compartida** Consulte nuestros comentarios en **RCO001**.	OPS-4 Diseño de la carga de trabajo para entender su estado OPS-10 Gestión de la carga de trabajo y eventos de las operaciones REL-12 Prueba de tolerancia a fallos

Requisito	Consideraciones	Consideraciones de Implementación (Prácticas de Buena Arquitectura)
RCO003: El plan de continuidad de procesamiento de datos debe, considerar, pero no limitarse a la incorporación de los siguientes contenidos: **a) Procedimientos operativos manuales, logísticos y automatizados de emergencia según cada proceso/recurso identificado y acción determinada;** **b) Ubicación/locación, traslado y transporte de responsables, proveedores y servicios de emergencia y recursos físicos y lógicos;** **c) Procedimientos de recuperación/ restauración de los recursos comprometidos.**	**Responsabilidad compartida** Consulte nuestros comentarios en **RCO001**.	REL-9 Respaldo de datos REL-5 Resistencia a fallos de los componentes REL-12 Prueba de tolerancia a fallos REL-13 Plan de recuperación ante desastres
RCO004: El plan de continuidad de procesamiento de datos debe ser probado periódicamente, como mínimo una vez al año. Las pruebas deben ser consistentes y coherentes con los criterios del requisito RCO002. Las pruebas también deben garantizar que todos los responsables y participantes de los procesos de continuidad y recuperación se encuentren informados de manera regular, continua y formal.	**Responsabilidad compartida** Consulte nuestros comentarios en **RCO001**.	REL-12 Prueba de tolerancia a fallos REL-13 Plan de recuperación ante desastres