Ley de Protección de los Datos Personales de Argentina Disposición N° 11/2006 Manual de trabajo

Mayo 2018

aws

[Manual de trabajo]

Avisos

Este documento se suministra únicamente con fines informativos. Representa la oferta actual de productos y prácticas de AWS en el momento de publicación de este documento. Dichas prácticas y productos pueden modificarse sin previo aviso. Los clientes son responsables de realizar sus propias evaluaciones independientes de la información contenida en este documento y de cualquier uso de los productos o servicios de AWS, cada uno de los cuales se ofrece "tal cual", sin garantía de ningún tipo, ya sea explícita o implícita. Este documento no genera ninguna garantía, declaración, compromiso contractual, condición ni certeza por parte de AWS, sus filiales, proveedores o licenciantes. Las responsabilidades y obligaciones de AWS para con sus clientes están sujetas a los acuerdos de AWS. Este documento no forma parte de ningún acuerdo entre AWS y sus clientes ni modifica acuerdo alguno.

Contents

Introducción

Este documento provee información para asistir a los clientes que deseen utilizar AWS para almacenar o tratar contenido que contenga datos personales, en el contexto de la Ley de Protección de los Datos Personales de Argentina, N° 25.326, incluyendo el Decreto Reglamentario N° 1558/2001 y normas complementarias (en adelante "LPDP"), que es aplicable a la protección de los datos personales en Argentina y a la transferencia internacional de datos personales para su procesamiento.

La Disposición N° 11/2006 de la Dirección Nacional de Protección de Datos Personales, bajo la LPDP, describe tres niveles diferentes de medidas de seguridad técnica y organizacional (básico, medio y crítico) a ser considerados, dependiendo de las actividades que usted realiza o la naturaleza de los datos personales que usted procesa.

Este manual ayudará a los clientes a implementar los controles que se listan en el Anexo I de la Disposición N° 11/2006.

Enfoque

Este manual reúne las preguntas más frecuentes de los clientes de AWS al momento de considerar los requerimientos sobre privacidad y de protección de datos personales que sean relevantes para el uso de los servicios de AWS para almacenar o tratar contenido que contenga datos personales. También habrá otras consideraciones relevantes que los clientes deberán tener en cuenta, por ejemplo, un cliente puede tener que cumplir con requerimientos específicos de una determinada industria, con las leyes de las jurisdicciones donde el cliente desarrolla sus actividades, o con los compromisos contractuales que asuma con terceras partes.

Este documento es provisto sólo a fines informativos. No es una opinión legal ni debe ser considerado como tal. Dado que los requerimientos de cada cliente son distintos, AWS les aconseja enfáticamente que obtengan asesoramiento adecuado en lo que concierne a la implementación de requisitos legales vinculados a la privacidad y la protección de datos personales, así como a las leyes aplicables y los demás requerimientos relevantes para su negocio.

Para mayor información, por favor visite: https://aws.amazon.com/compliance/argentina-data-privacy/.

Consideraciones relevantes para la protección de la privacidad y los datos personales

Al momento de utilizar los servicios de AWS, cada cliente de AWS mantiene la propiedad y el control de su contenido, incluyendo el control sobre:

- El contenido que decidan almacenar o tratar usando los servicios de AWS
- Qué servicios de AWS utilizan para administrar su contenido
- La(s) Región(es) donde almacenan su contenido
- El formato, la estructura y la seguridad de su contenido, incluyendo si se encuentra oculto, anonimizado o encriptado
- Quién tiene acceso a sus cuentas y contenidos de AWS y cómo se otorgan, gestionan y revocan esos accesos

Dado que los clientes de AWS conservan la propiedad y el control sobre su contenido dentro del entorno de AWS, también conservan responsabilidades en relación con la seguridad de ese contenido como parte del modelo de "responsabilidad compartida" de AWS. Este modelo de responsabilidad compartida es fundamental para entender los respectivos roles de AWS y de los clientes en el contexto de los requerimientos de privacidad y de protección de datos que pueden aplicar a contenidos que los clientes deciden almacenar o tratar usando los servicios de AWS.

Para acceder a información complementaria sobre cómo operan los servicios de AWS, incluyendo cómo los clientes pueden abordar temas de seguridad y encriptar su contenido, las ubicaciones geográficas donde

los clientes pueden elegir almacenar su contenido y otras consideraciones relevantes, por favor acceda al documento técnico Utilizando AWS y consideraciones comunes de privacidad y protección de datos personales.

El enfoque de responsabilidad compartida de AWS para manejar la seguridad en la nube

La migración de infraestructura de TI a AWS crea un modelo de responsabilidad compartida entre el cliente y AWS, ya que ambos tienen roles importantes en la operación y la gestión de la seguridad. AWS opera, administra y controla los componentes desde el sistema operativo central (host) y la capa de virtualización hacia la seguridad física de las instalaciones en las que AWS opera sus servicios. El cliente es responsable de gestionar el sistema operativo huésped (incluyendo actualizaciones y parches de seguridad para el sistema operativo huésped) y el software de aplicación asociado, así como las configuraciones de las funciones del firewall de seguridad que provee AWS y otras medidas de seguridad relacionadas. El cliente generalmente se conectará con el entorno de AWS a través de servicios que el cliente adquiere de terceras partes (por ejemplo, de su proveedor de internet). AWS no provee de estas conexiones, y es por ello que son parte del área de responsabilidad del cliente. Los clientes deberían considerar la seguridad de estas conexiones y las responsabilidades de seguridad de esas terceras partes en relación a sus sistemas.

Los roles respectivos del cliente y de AWS en el marco del modelo de responsabilidad compartida se muestran en la Figura 1.

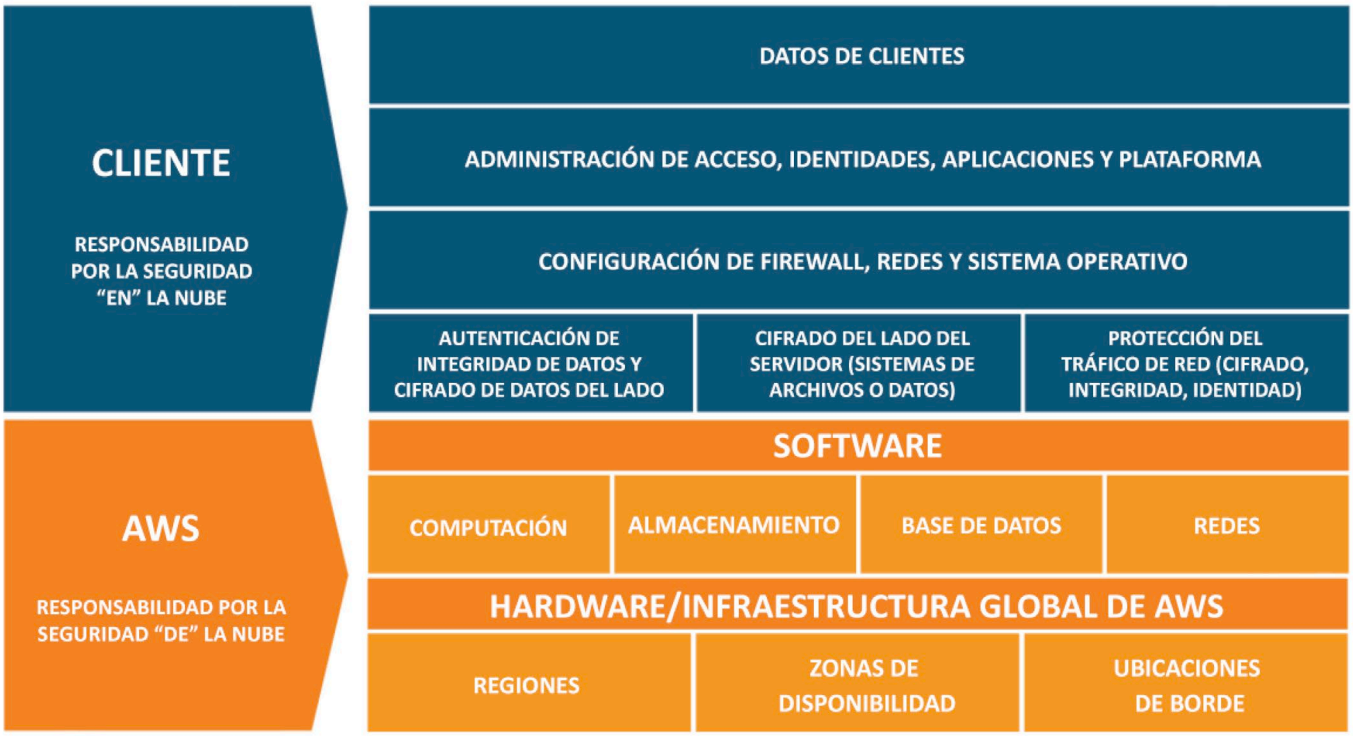

Figura 1- Modelo de responsabilidad compartida

¿Cuál es el impacto del modelo de responsabilidad compartida para la seguridad del contenido del cliente?

Cuando evalúan la seguridad de una solución en la nube, es importante que los clientes entiendan y distingan entre:

- Medidas de seguridad que el proveedor de servicios de nube (AWS) implementa y opera - "seguridad de la nube"
- Medidas de seguridad que el cliente implementa y opera, en relación a la seguridad del contenido del cliente y las aplicaciones que usan los servicios de AWS - "seguridad en la nube".

Mientras que AWS gestiona la seguridad de la nube, la seguridad en la nube es responsabilidad del cliente, ya que los clientes retienen el control para decidir qué seguridad deciden implementar para proteger su propio contenido, plataforma, aplicaciones, sistemas y redes - de la misma manera que lo harían para aplicaciones en un centro de datos en sus propias instalaciones (on-site).

Para una explicación más detallada del modelo de responsabilidad compartida de AWS, por favor acceda a: https://aws.amazon.com/es/compliance/shared-responsibility-model/.

Programas de garantía de seguridad de AWS

En la gestión de la seguridad de la nube, AWS implementa y mantiene medidas de seguridad técnicas y organizativas aplicables a los servicios de infraestructura en la nube de AWS bajo marcos de seguridad y certificaciones de seguridad reconocidos mundialmente, que incluyen ISO 27001, ISO 27017, ISO 27018, PCI DSS Level 1 y SOC 1, 2 y 3. Estas medidas de seguridad técnicas y organizativas son validadas por asesores externos independientes, y están diseñadas para evitar el acceso no autorizado o la divulgación del contenido del cliente.

Por ejemplo, ISO 27018 es el primer código internacional de prácticas que se centra en la protección de datos personales en la nube. Se basa en la norma de seguridad de la información ISO 27002 y proporciona una guía de implementación sobre los controles ISO 27002 aplicables a la Información de Identificación Personal (PII) procesada por los proveedores de servicios en la nube pública. Esto demuestra a los clientes que AWS tiene un sistema de controles orientado específicamente a la protección de la privacidad de su contenido.

Visite nuestro sitio web para obtener información adicional sobre la seguridad de la nube de AWS y todos los Programas de Conformidad (Compliance) de AWS, donde también puede realizar un Recorrido Digital por un Centro de Datos de AWS. Para acceder a una lista completa de todas las medidas de seguridad implementadas en la infraestructura de la nube, las plataformas y los servicios de AWS, por favor lea nuestro documento técnico Descripción General de los Procesos de Seguridad.

Ley de Protección de los Datos Personales de Argentina - Disposición N° 11/2006

El Anexo I de la Disposición N° 11/2006 aprueba las medidas de seguridad aplicables al tratamiento y la conservación de los datos personales contenidos en archivos, registros y bases de datos públicos no estatales y privados. http://www.jus.gob.ar/media/33445/disp_2006_11.pdf

Esta sección del documento provee información acerca de cada control listado en la Disposición N° 11/2006, quién tiene responsabilidad por controles de *compliance* dentro del Esquema de Responsabilidad Compartida de AWS y, en los casos en los que AWS comparte responsabilidad, cómo los clientes pueden usar los recursos de compliance de la nube para demostrar su cumplimiento con controles específicos.

N°	Requerimientos	Responsabilidad	Consideraciones
Medidas de Seguridad de Nivel Básico Los archivos, registros, bases y bancos de datos que contengan datos de carácter personal deberán adoptar las medidas de seguridad calificadas como de Nivel Básico que a continuación se detallan: Disponer del Documento de Seguridad de Datos Personales en el que se especifiquen, entre otros, los procedimientos y las medidas de seguridad a observar sobre los archivos, registros, bases y bancos que contengan datos de carácter personal. Deberá mantenerse en todo momento actualizado y ser revisado cuando se produzcan cambios en el sistema de información. Deberá contener:			
1	Funciones y obligaciones del personal.	Cliente	Los clientes que no tienen experiencia en temas relacionados a la nube informática pueden revisar un resumen del Marco de Adopción de la Nube de AWS, el cual ayuda a las organizaciones a desarrollar planes eficientes y efectivos para su migración a la nube. Para mayor información consulte el sitio web https://aws.amazon.com/es/professional-services/CAF/. Los clientes nuevos también pueden leer más sobre los procesos de seguridad en Introducción a los Procesos de Seguridad que refiere, pero no se limita, al Modelo de Responsabilidad Compartida, Seguridad Física y Ambiental, Continuidad del Negocio, Principios de Diseño y Funcionalidades de Seguridad.
2	Descripción de los archivos con datos de carácter personal y los sistemas de información que los tratan.	Cliente	Los clientes retienen el control de sus datos y son responsables por ellos, así como de los controles y los procedimientos de seguridad.

N°	Requerimientos	Responsabilidad	Consideraciones
3	Descripción de las rutinas de control de datos de los programas de ingreso de datos y las acciones a seguir ante los errores detectados a los efectos de su corrección. Todos los programas de ingreso de datos, cualquiera sea su modo de procesamiento (batch, interactivo, etc.) deben incluir en su diseño rutinas de control que minimicen la posibilidad de incorporar al sistema de información datos ilógicos, incorrectos o faltantes.	Cliente	Los clientes retienen el control de sus datos y son responsables por ellos, así como de los controles y procedimientos de seguridad.
4	Registro de incidentes de seguridad. Notificación, gestión y respuesta ante los incidentes de seguridad.	Compartida	Los clientes pueden mantener una variedad de registros (logs) y notificaciones automatizadas. AWS ofrece servicios como Amazon CloudWatch para monitorear los recursos de la nube de AWS y las aplicaciones que usted ejecuta en los servicios de AWS. Los clientes pueden usar Amazon CloudWatch para recopilar y realizar el seguimiento de métricas y logs, establecer alarmas, enviar notificaciones y reaccionar automáticamente ante cambios en sus recursos de AWS. Con AWS CloudTrail, usted puede iniciar sesión y acceder, monitorear constantemente, y conservar eventos relacionados con llamadas de la interfaz de programación de aplicaciones (API) a lo largo de su infraestructura de AWS. Para mayor información sobre acceso y monitoreo, visite https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Best_Practices.pdf. AWS ha implementado una política y un programa de respuesta formal y documentada de los incidentes, desarrollados en línea con los estándares ISO 27001. Los usos del sistema son apropiadamente restringidos y monitoreados. Los reportes SOC de AWS proveen detalles adicionales sobre los controles implementados para restringir el acceso al sistema. Para obtener más información, por favor referirse a la sección de Respuesta de Incidentes en el documento técnico AWS: Resumen de los Procesos de Seguridad https://d1.awsstatic.com/whitepapers/Backup_and_Recovery_Approaches_Using_AWS.pdf.

N°	Requerimientos	Responsabilidad	Consideraciones
5	Procedimientos para efectuar las copias de respaldo y de recuperación de datos.	Cliente	AWS le permite a sus clientes desarrollar sus propias copias de seguridad usando servicios tales como el Servicio de Amazon de Almacenamiento Simple o Amazon Glacier, diseñados para rendir con una durabilidad del 99,999999999%. Para acceder a información adicional por favor vea el documento técnico relativo a Enfoques sobre Back-up y Recuperación usando AWS https://aws.amazon.com/es/whitepapers/backup-and-recovery-using-aws/.
6	Relación actualizada entre Sistemas de Información y usuarios de datos con autorización para su uso.	Cliente	Bajo el Modelo de Responsabilidad Compartida, el control de acceso a los datos es una responsabilidad del cliente. Sin perjuicio de ello, el servicio de Administración de Acceso e Identidad (IAM) de AWS ofrece una manera fácil de listar usuarios, grupos, roles y políticas que permiten el acceso a datos directamente desde la consola de administración de AWS. La Administración de Seguridad y Usuarios utilizando IAM está detalladamente explicada en el documento técnico sobre las Buenas Prácticas de Seguridad de AWS (https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Best_Practices.pdf), en la sección denominada Administrar Cuentas de AWS, Usuarios de IAM, Grupos y Funciones.
7	Procedimientos de identificación y autenticación de los usuarios de datos autorizados para utilizar determinados sistemas de información. La relación entre el usuario autorizado y el/los sistemas de información a los que puede acceder debe mantenerse actualizada. En el caso en que el mecanismo de autenticación utilice contraseña, la misma será asignada por el responsable de seguridad de acuerdo a un procedimiento que garantice su confidencialidad. Este procedimiento deberá prever el cambio periódico de la contraseña (lapso máximo de vigencia) las que deberán estar almacenadas en forma ininteligible.	Cliente	AWS brinda a los clientes la posibilidad de configurar y usar adecuadamente los servicios ofrecidos por AWS con el fin de mantener su contenido adecuadamente protegido, seguro y respaldado. Los clientes pueden utilizar los APIs de AWS para configurar permisos de control de acceso para cualquier servicio que desarrollen o desplieguen en un ambiente de AWS. IAM permite a los clientes controlar de forma segura el acceso para sus usuarios a los servicios y recursos de AWS. Información adicional sobre IAM puede obtenerse en el sitio web https://aws.amazon.com/iam/. Se pueden encontrar estrategias para administrar usuarios, grupos, roles y otorgar acceso al contenido de los clientes dentro del documento técnico sobre las Buenas Prácticas de Seguridad de AWS (https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Best_Practices.pdf), bajo la sección denominada Administrar Cuentas de AWS, Usuarios de IAM, Grupos y Funciones.

N°	Requerimientos	Responsabilidad	Consideraciones
8	Control de acceso de usuarios a datos y recursos necesarios para la realización de sus tareas para lo cual deben estar autorizados.	Compartida	Los clientes mantienen todo el control y la responsabilidad de configurar el acceso a su información. AWS utiliza el principio de mínimo privilegio, permitiendo a los usuarios únicamente el acceso necesario para cumplir con su puesto de trabajo. Las cuentas de nuevos usuarios se crean con acceso mínimo. El acceso del usuario a los sistemas de AWS (por ejemplo, red, aplicaciones, herramientas, etc.) requiere aprobación documentada por parte de personal autorizado (por ejemplo, gerente del usuario y/o dueño del sistema) y validación del usuario activo en el sistema de recursos humanos. Los Sistemas de Administración de Seguridad de la Información (ISMS) deberán ser determinados y utilizados. Más información para diseñar su ISMS para proteger sus activos en AWS puede encontrarse en el documento técnico sobre las Buenas Prácticas de Seguridad de AWS (https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Best_Practices.pdf, bajo la sección con el mismo nombre.
9	Adoptar medidas de prevención a efectos de impedir amenazas de software malicioso (virus, troyanos, etc.) que puedan afectar archivos con datos de carácter personal. Entre otras: 1) Instalar y actualizar, con la periodicidad pertinente, software de detección y reparación de virus, ejecutándolo rutinariamente; 2) Verificar, antes de su uso, la inexistencia de virus en archivos recibidos a través de la web, correo electrónico y otros cuyos orígenes sean inciertos.	Cliente	Los clientes retienen el control de sus datos y son responsables por ellos, así como de los controles y procedimientos de seguridad.

N°	Requerimientos	Responsabilidad	Consideraciones
10	Procedimiento que garantice una adecuada Gestión de los Soportes que contengan datos de carácter personal (identificación del tipo de información que contienen, almacenamiento en lugares de acceso restringidos, inventarios, autorización para su salida fuera del local en que están ubicados, destrucción de la información en desuso, etc.). Nota: Cuando los archivos, registros, bases y bancos contengan una serie de datos personales con los cuales, a través de un determinado tratamiento, se permita establecer el perfil de personalidad o determinadas conductas de la persona, se deberán garantizar las medidas de seguridad del presente nivel más las establecidas en los puntos 2, 3, 4 y 5 del siguiente.	Compartida	AWS ha establecido procedimientos y mecanismos para restringir apropiadamente el acceso no autorizado, tanto interno como externo, a los datos, y el acceso a datos de los clientes se encuentra apropiadamente separado de otros clientes. Todo el contenido y los datos son clasificados de acuerdo a los requerimientos de la Política de Clasificación de Datos de Amazon. Los datos clasificados como Críticos son los datos más sensibles de AWS. Todos los datos son manejados de acuerdo con la Política de Manejo y Retención de Datos. AWS clasifica todo el material ingresado a las instalaciones de AWS como Crítico y lo trata consecuentemente como de alto impacto durante todo su ciclo de vida. AWS clasifica todo el contenido y activos asociados de los clientes como Crítico. La información de los clientes no es utilizada en la prueba y desarrollo de ambientes. Información adicional acerca de estos procedimientos y mecanismos puede encontrarse en el Resumen de Procesos de Seguridad de AWS https://d1.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf.
Medidas de Seguridad de Nivel Medio Los archivos, registros, bases y bancos de datos de las empresas privadas que desarrollen actividades de prestación de servicios públicos, así como los archivos, registros, bases y bancos de datos pertenecientes a entidades que cumplan una función pública y/o privada que, más allá de lo dispuesto por el artículo 10 de la Ley N° 25.326, deban guardar secreto de la información personal por expresa disposición legal (v.g.: secreto bancario), además de las medidas de seguridad de nivel Básico, deberán adoptar las que a continuación se detallan:			
1	El Instructivo de seguridad deberá identificar al Responsable (u órgano específico) de Seguridad.	Cliente	Los clientes retienen el control de sus datos y son responsables por ellos, así como de los controles y procedimientos de seguridad. Los clientes que no tienen experiencia en temas relacionados a la nube informática pueden revisar un resumen del Marco de Adopción de la Nube de AWS, el cual ayuda a las organizaciones a desarrollar planes efectivos y eficientes para su migración a la nube. Se puede acceder a información adicional en el sitio web: https://aws.amazon.com/professional-services/CAF/.

N°	Requerimientos	Responsabilidad	Consideraciones
2	Realización de auditorías (internas o externas) que verifiquen el cumplimiento de los procedimientos e instrucciones vigentes en materia de seguridad para datos personales. Los informes de auditoría pertinentes, serán presentados al Responsable del Archivo a efectos de que se adopten las medidas correctivas que correspondan. La Dirección Nacional de Protección de Datos Personales, en las inspecciones que realice, deberá considerar obligatoriamente, con carácter no vinculante, los resultados de las auditorías referidas precedentemente, siempre que las mismas hayan sido realizadas dentro de un período máximo de un año.	Compartida	AAWS ha establecido un programa formal de auditorías que incluye una continua evaluación independiente, interna y externa para validar la implementación y la operación efectiva del control de ambiente de AWS. Las auditorías internas y externas son planeadas y ejecutadas de conformidad con el programa documentado de auditorías a fin de revisar el continuo funcionamiento de AWS frente al criterio estándar e identificar las oportunidades generales de mejora. El criterio estándar incluye, pero no se limita, a los estándares profesionales de ISO/IEC 27001, Programa Federal de Administración de Riesgo y Autorización (Federal Risk and Authorization Management Program, o FedRAMP), Instituto Americano de Contadores Públicos Certificados (American Institute of Certified Public Accountants, o AICPA), AT 801 (anteriormente la Declaración de Estándares para Compromisos de Certificación (Statement on Standards for Attestation Engagements - SSAE 16)) y los Estándares Internacionales para Compromisos de Garantías N° 3402 (International Standards for Assurance Engagements No.3402 (ISAE 3402)). Los informes de compliance basados en estas evaluaciones están a disposición de los clientes para permitirles evaluar a AWS. Los Informes de Compliance de AWS identifican el alcance de los servicios de AWS y las regiones evaluadas, así como también la certificación de compliance del evaluador. La evaluación de un proveedor o distribuidor puede aprovechar estos informes y certificaciones. Para más información sobre los informes de compliance de AWS, visite el sitio web https://aws.amazon.com/compliance/.
3	Se limitará la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.	Cliente	Los clientes mantienen el control y la responsabilidad sobre sus datos y activos asociados. El cliente puede determinar su Política de Contraseñas en el ambiente AWS: Establecer una Política de Contraseña para cuentas de usuarios IAM http://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_passwords_account-policy.html.

N°	Requerimientos	Responsabilidad	Consideraciones
4	Se establecerá un control de acceso físico a los locales donde se encuentren situados los sistemas de información con datos de carácter personal.	Compartida	El acceso físico a todos los centros de datos de AWS que alojan componentes de infraestructura de IT está restringido a empleados autorizados del centro de datos, proveedores y contratistas que requieran acceso para realizar sus trabajos. El acceso a instalaciones está permitido únicamente en puntos controlados que exigen autentificaciones múltiples para prevenir el acceso no autorizado y asegurar que únicamente individuos autorizados ingresen al centro de datos de AWS. Trimestralmente el respectivo Administrador de Acceso al Área (*Area Access Managers* (AAM)) revisa las listas de acceso y credenciales de autorización de personal con acceso a los sistemas centrales o dispositivos de dichos sistemas de los centros de datos. Todas las entradas a los centros de datos de AWS, incluyendo la entrada principal, el muelle de carga y las puertas o ventanas de los techos, son aseguradas con dispositivos de detección de intrusión que hacen sonar alarmas si la puerta es forzada o mantenida abierta. Guardias de seguridad entrenados son apostados en la entrada del edificio 24x7x365. En caso de que una puerta o jaula dentro del centro de datos tenga un lector de credenciales o panel de PIN funcionando mal y no pueda ser asegurado electrónicamente, un guardia de seguridad es apostado en esa puerta hasta que sea reparado. Conozca más sobre cómo aseguramos los centros de datos de AWS a través del diseño tomando un tour virtual en https://aws.amazon.com/compliance/data-center/. Se puede encontrar información adicional sobre la seguridad física y del medioambiente en el Resumen de Procesos de Seguridad de AWS (https://d1.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf) bajo la sección con el mismo nombre.

N°	Requerimientos	Responsabilidad	Consideraciones
5	Gestión de Soportes e información contenida en ellos. 5.1 Se dispondrá de un registro de entradas y salidas de los soportes informáticos de manera de identificar, día y hora de entrada y salida del soporte, receptor, emisor, forma de envío, etc. 5.2 Se adoptarán las medidas necesarias para impedir cualquier recuperación de la información con posterioridad a que un soporte vaya a ser desechado o reutilizado, o que la información deba ser destruida, por la causa que correspondiere. Asimismo se deberán adoptar similares medidas cuando los soportes, o la información (ej.: cuando se hacen copias de respaldo a través de una red de transmisión de datos, la información sale de un soporte local y viaja hasta otro remoto vía dicha red), vaya a salir fuera de los locales en que se encuentren ubicados. Deberá disponerse de un procedimiento de recuperación de la información de respaldo y de tratamiento de la misma en caso de contingencias que pongan no operativo el/los equipos de procesamiento habituales.	Compartida	AWS ha sido validado y certificado por un auditor independiente para confirmar su armonización con el estándar de certificación ISO 27001. Cuando un dispositivo de almacenamiento ha llegado al final de su vida útil, los procedimientos de AWS incluyen un proceso de desmantelamiento que está diseñado para evitar que los datos del cliente queden expuestos a personas no autorizadas. AWS utiliza las técnicas detalladas en NIST 800-88 (“Directrices para el saneamiento de la información tecnológica”) como parte del proceso de desmantelamiento. Para obtener más detalles lea el documento técnico AWS Cloud Security - disponible en http://aws.amazon.com/security. Desde la perspectiva del cliente, tal como se establece en el Modelo de Responsabilidad Compartida, los clientes son responsables de asegurar la protección de sus datos y de hacer copias a través de su propio software o utilizando uno o más de los servicios ofrecidos por AWS. Para obtener información adicional, por favor acceda al documento técnico relativo a Enfoques sobre Backup y Recuperación usando AWS https://aws.amazon.com/es/whitepapers/backup-and-recovery-using-aws/. Los clientes también son responsables de administrar el ciclo de vida de sus datos, y purgar y auditar cuando sea necesario.

N°	Requerimientos	Responsabilidad	Consideraciones
6	Los registros de incidentes de seguridad, en el caso de tener que recuperar datos, deberán identificar la persona que recuperó y/o modificó dichos datos. Será necesaria la autorización en forma fehaciente del responsable del archivo informatizado.	Compartida	AWS ha implementado una política y un programa de respuesta formal y documentada de los incidentes, desarrollados en línea con los estándares ISO 27001. Los usos del sistema son apropiadamente restringidos y monitoreados. Los reportes SOC de AWS proporcionan detalles adicionales sobre los controles implementados para restringir el acceso al sistema. AWS ofrece servicios como Amazon CloudWatch para monitorear los recursos de la nube de AWS y las aplicaciones que usted ejecuta en los servicios de AWS. Los clientes pueden usar Amazon CloudWatch para recopilar y realizar el seguimiento de métricas y *logs*, establecer alarmas, enviar notificaciones y reaccionar automáticamente ante cambios en sus recursos de AWS. Con AWS CloudTrail, usted puede iniciar sesión y acceder, monitorear constantemente, y conservar eventos relacionados con llamadas API a lo largo de su infraestructura de AWS. Para mayor información sobre acceso y monitoreo, visite https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Best_Practices.pdf.
7	Las pruebas de funcionamiento de los sistemas de información, realizadas con anterioridad a su puesta operativa no se realizarán con datos/archivos reales, a menos que se aseguren los niveles de seguridad correspondientes al tipo de datos informatizados tratados.	Cliente	Los clientes retienen el control de sus datos y son responsables por ellos, así como de los controles y procedimientos de seguridad.

Medidas de Seguridad de Nivel Crítico

Los archivos, registros, bases y bancos de datos que contengan datos personales, definidos como “datos sensibles,” con la excepción que se señalará más abajo, además de las medidas de seguridad de nivel Básico y Medio, deberán adoptar las que a continuación se detallan:

Nota: Quedan exceptuados de aplicar las medidas de seguridad de nivel crítico, los archivos, registros, bases y bancos de datos que deban efectuar el tratamiento de datos sensibles para fines administrativos o por obligación legal. No obstante, ello no excluye que igualmente deban contar con aquellas medidas de resguardo que sean necesarias y adecuadas al tipo de dato.

N°	Requerimientos	Responsabilidad	Consideraciones
1	Distribución de soportes: cuando se distribuyan soportes que contengan archivos con datos de carácter personal —incluidas las copias de respaldo—, se deberán cifrar dichos datos (o utilizar cualquier otro mecanismo) a fin de garantizar que no puedan ser leídos o manipulados durante su transporte.	Cliente	AWS le ofrece la posibilidad de agregar una capa adicional de seguridad a sus datos en reposo en la nube, proporcionando funciones de cifrado escalables y eficientes. Esto incluye: • Capacidades de encriptación de datos disponibles en los servicios de bases de datos y almacenamiento de AWS, como EBS, S3, Glacier, Oracle RDS, SQL Server RDS y Redshift. • Opciones flexibles de administración de claves, incluido AWS Key Management Service, que le permite al cliente elegir si AWS administrará las claves de cifrado o el cliente mantiene un control total sobre las claves. • Almacenamiento de claves criptográficas basadas en *hardware* utilizando AWS CloudHSM, lo cual le permite al cliente cumplir con los requisitos de *compliance*. Además, AWS le proporciona APIs para que pueda integrar el cifrado y la protección de datos con cualquiera de los servicios que desarrolle o implemente en un entorno de AWS.
2	Registro de accesos: se deberá disponer de un registro de accesos con información que identifique al usuario que accedió, cuando lo hizo (fecha y hora), tipo de acceso y si ha sido autorizado o denegado. En el caso que el acceso haya sido autorizado se deberá identificar el dato accedido y el tratamiento que se le dio al mismo (baja, rectificación, etc.). Este registro de accesos deberá ser analizado periódicamente por el responsable de seguridad y deberá ser conservado como minino por el término de un TRES (3) años.	Cliente	Los clientes retienen el control de sus datos y son responsables por ellos, así como de los controles y procedimientos de seguridad. Los clientes retienen el control de sus propios sistemas operativos huéspedes, software y aplicaciones, y son responsables de desarrollar un monitoreo lógico de las condiciones de estos sistemas. En línea con los estándares ISO 27001, los sistemas de información AWS utilizan relojes internos del sistema sincronizados a través de NTP (Protocolo de tiempo de red). AWS CloudTrail proporciona una solución simple para registrar la actividad del usuario que ayuda a aliviar la carga de implementar un sistema de registro complejo. Para obtener más información, visite https://aws.amazon.com/es/cloudtrail/. AWS Cloudwatch proporciona un monitoreo de los recursos de la nube de AWS y las aplicaciones que los clientes ejecutan en AWS. Para obtener más información, visite https://aws.amazon.com/es/cloudwatch/. AWS proporciona a los clientes la capacidad de eliminar sus datos. Sin embargo, los clientes de AWS retienen el control y la propiedad de sus datos, por lo que es responsabilidad del cliente administrar la retención de datos según sus propios requisitos.

N°	Requerimientos	Responsabilidad	Consideraciones
3	Copias de respaldo: además de las que se mantengan en la localización donde residan los datos deberán implementarse copias de resguardo externas, situadas fuera de la localización, en caja ignífuga y a prueba de gases o bien en una caja de seguridad bancaria, cualquiera de ellas situadas a prudencial distancia de la aludida localización. Deberá disponerse de un procedimiento de recuperación de esa información y de tratamiento de la misma en caso de contingencias que pongan no operativo el/los equipos de procesamiento habituales.	Cliente	Cada cliente tiene la responsabilidad de habilitar o diseñar el sistema adecuado para que sus recursos cumplan con este requisito (se trate de una zona de disponibilidad múltiple o de varias regiones). Los clientes pueden optar por hacer una copia de seguridad de sus datos en una Región determinada, en todas las Regiones o cualquier combinación de Regiones, incluidas las regiones de Brasil y los Estados Unidos. Visite la página web de AWS Global Infrastructure para obtener una lista completa de las regiones de AWS.
4.	Transmisión de datos: los datos de carácter personal que se transmitan a través de redes de comunicación[1], deberán serlo cifrados o utilizando cualquier otro mecanismo que impida su lectura y/o tratamiento por parte de personas no autorizadas. [1] Se trata de comunicaciones que salgan fuera de la red de la organización.	Cliente	AWS le ofrece la posibilidad de agregar una capa adicional de seguridad a sus datos en reposo en la nube, proporcionando funciones de cifrado escalables y eficientes. Esto incluye: • Capacidades de encriptación de datos disponibles en los servicios de bases de datos y almacenamiento de AWS, como EBS, S3, Glacier, Oracle RDS, SQL Server RDS y Redshift. • Opciones flexibles de administración de claves, incluido AWS Key Management Service, que le permite al cliente elegir si AWS administrará las claves de cifrado o el cliente mantiene un control total sobre las claves. • Almacenamiento de claves criptográficas basadas en *hardware* utilizando AWS CloudHSM, lo cual le permite al cliente cumplir con los requisitos de *compliance*. Además, AWS le proporciona APIs para que pueda integrar el cifrado y la protección de datos con cualquiera de los servicios que desarrolle o implemente en un entorno de AWS.

Observaciones Finales

Para AWS, la seguridad es siempre nuestra prioridad principal. Prestamos servicios a más de un millón de clientes activos, que incluyen empresas, instituciones educativas y agencias gubernamentales en más de 190 países. Nuestros clientes incluyen proveedores de servicios financieros y proveedores de atención médica que nos confían su información más sensible.

Los servicios de AWS están diseñados para brindar a los clientes flexibilidad sobre cómo configuran e implementan sus soluciones, así como el control de su contenido, incluyendo dónde se almacena, cómo se almacena y quién tiene acceso al mismo. Los clientes de AWS pueden desarrollar sus propias aplicaciones seguras y almacenar su contenido de manera segura en AWS.

Para ayudar a los clientes a entender mejor cómo pueden abordar sus requisitos de privacidad y protección de datos, les recomendamos que lean los documentos técnicos sobre riesgos, compliance y seguridad, buenas prácticas, listas de control y directrices publicados en el sitio web de AWS. Este material se puede encontrar en http://aws.amazon.com/compliance y http://aws.amazon.com/security.