Programa de Suscripciones a la Nube

Anexo de medidas de seguridad de la información

El Proveedor ha implementado y mantendrá las siguientes medidas de seguridad. Estas medidas, junto con las medidas de seguridad descritas en la Especificación de la Suscripción aplicable, constituyen la única responsabilidad del Proveedor con respecto a la seguridad de la Oferta del Proveedor. A menos que se defina lo contrario en el presente documento, todos los términos en mayúscula que se utilizan en este documento tendrán el significado que se les ha adscrito en el Programa de Suscripciones a la Nube.

Descripción	Medidas
Programa de seguridad de la información	El Proveedor ha implementado y mantendrá un programa de seguridad de la información (incluyendo la adopción de políticas y normas internas) diseñado para: (a) identificar los riesgos de seguridad razonablemente previsibles para las partes de los centros de datos, servidores, equipos de red, cortafuegos y sistemas de software host que estén bajo el control del Proveedor y se utilizan para prestar la Oferta del Proveedor ("**Red del Proveedor**"), y (b) mitigar los riesgos de seguridad identificados, cuando lo considere adecuada, incluso mediante evaluaciones y pruebas de riesgo periódicas. El Proveedor ha designado a uno o más responsables de seguridad para coordinar, supervisar y hacer cumplir el programa de seguridad de la información. El Proveedor mantendrá un programa de gestión de amenazas y vulnerabilidades que supervise las vulnerabilidades de la Red del Proveedor de forma continua. Las vulnerabilidades se identifican mediante una serie de fuentes/métodos que pueden incluir proveedores, investigadores de seguridad, análisis de vulnerabilidades, actividades del red team, pruebas de penetración y reportes de empleados. Las vulnerabilidades de terceras partes que hayan sido dadas a conocer públicamente son revisadas para determinar la aplicabilidad de las mismas al entorno del Proveedor. Los análisis y las evaluaciones de vulnerabilidades se realizan de forma rutinaria y periódica en la infraestructura de aplicaciones del Proveedor. Estos procesos se han concebido para permitir la identificación proactiva y la corrección de vulnerabilidades, así como para respaldar el cumplimiento de los requisitos corporativos y normativos del Proveedor.
Ciclo de vida de desarrollo seguro y respuesta a vulnerabilidades	El Proveedor ha implementado y mantiene un programa de ciclo de vida de desarrollo seguro para definir los pasos que se deben seguir para asegurar que sus ofertas se han diseñado, desarrollado y empaquetado adecuadamente bajo la estructura de un programa de gobernanza formal. Este programa, junto con el programa de seguridad de la información del Proveedor, ayuda a abordar la seguridad en todo el ciclo de vida de desarrollo y mantenimiento de la Oferta del Proveedor. El Proveedor utiliza un proceso riguroso para evaluar y mejorar continuamente sus prácticas de desarrollo seguro y respuesta a vulnerabilidades, y el Proveedor las compara periódicamente con las prácticas estándar del sector.

	Tras investigar y validar una vulnerabilidad notificada en la Oferta del Proveedor, el Proveedor intentará identificar, desarrollar y habilitar una solución adecuada de acuerdo con la política de respuesta ante vulnerabilidades publicada por el Proveedor, que actualmente se encuentra en: Política de respuesta a vulnerabilidades del Proveedor | Proveedor EE. UU. El Proveedor comunica las soluciones a sus Clientes a través de avisos de seguridad cuando procede. El Proveedor hace todo lo posible por proporcionar soluciones en un plazo comercialmente razonable. Los plazos de respuesta dependerán de muchos factores, como la gravedad de la vulnerabilidad, la complejidad de la solución o el componente afectado.
Administración de activos	El Proveedor rastrea los activos físicos y lógicos de la Red del Proveedor. Entre los ejemplos de los activos que el Proveedor puede rastrear, y los controles que puede aplicar, se incluyen: (a) Activos de software, como aplicaciones y programas de software del sistema. (b) Activos físicos, como servidores, equipos portátiles o de escritorio, cintas de archivado o copia de seguridad, impresoras y equipos de comunicaciones. (c) Activos de información, como bases de datos, planes de recuperación ante desastres, planes de continuidad empresarial, clasificación de datos o información archivada. El Proveedor clasifica los activos en función de la criticidad empresarial y/o la sensibilidad de la clasificación de datos. Dicha clasificación permite restringir y manejar adecuadamente el acceso a dicho activo.
Seguridad en Recursos Humanos	Como parte del proceso de contratación, los empleados del Proveedor deben firmar un acuerdo de confidencialidad en el momento de la contratación y someterse a un proceso de verificación sujeto a la legislación aplicable. Aunque el Proveedor se reserva el derecho de revisar sus políticas e implementar las medidas que considere necesarias para velar por la seguridad en cuanto a los recursos humanos, bajo la política actual y sujeto a la legislación local y disponibilidad, el Proveedor lleva a cabo una o más de las siguientes revisiones para contratar a un nuevo empleado: pruebas toxicológicas, verificación de la información relacionada con la seguridad social, búsqueda de antecedentes penales, verificación de educación y empleo, y verificación de elegibilidad laboral. El Proveedor intenta cumplir con los estándares actuales del sector para empresas similares del mismo sector del Proveedor, pero el Proveedor no puede adaptar la seguridad de su personal ni el proceso de selección para cumplir con las expectativas específicas de un Cliente en particular. Los terceros o contratistas externos son, o bien verificados por el Proveedor como condición del contrato respectivo, o bien verificados por el contratista siguiendo un proceso de verificación aprobado por el Proveedor. El Proveedor mantiene un proceso disciplinario para tomar medidas frente el personal que no cumpla con los requisitos de su programa de seguridad de la información, incluidos, entre otros, los establecidos para cumplir con sus compromisos y requisitos de seguridad, disponibilidad y confidencialidad.

	El Proveedor proporciona entrenamientos anuales de concienciación sobre seguridad a todo el personal aplicable y exige a los subcontratistas aplicables que impartan dicho entrenamiento a su personal.
Seguridad física	Existen controles basados en riesgos en las instalaciones que albergan componentes físicos de la Red del Proveedor (por ejemplo, centros de datos). Entre los controles de acceso pueden figurar guardias de seguridad, registros de seguridad, vigilancia, alarmas, acceso limitado a zonas seguras, protección de las vías de acceso, videovigilancia, tarjetas llave o autenticación de dos factores. Esta disposición se aplica a los Sitios de Colocación (Colocation Sites), gestionados por el Proveedor y a los centros de datos administrados por el proveedor que alojan servicios de nube pública.
Seguridad de la red	El personal del Proveedor podrá acceder electrónicamente a la Red del Proveedor según sea necesario para prestar la Oferta del Proveedor. El Proveedor mantendrá políticas y controles de acceso para gestionar el acceso permitido a la Red del Proveedor desde cada conexión, incluido el uso de cortafuegos y controles de autenticación. El Proveedor protege contra el uso malicioso de activos y software malicioso en la Red del Proveedor, a través de la implementación de controles basados en el riesgo. Esos controles pueden ser, entre otros: políticas de seguridad; controles de acceso restrictivos; entornos para desarrollo y pruebas separados; detección de malware en servidores, equipos de escritorio y equipos portátiles; análisis de archivos adjuntos de correo electrónico en busca de malware; análisis de cumplimiento normativo del sistema; monitorización para impedir intrusiones y respuesta a estas; registro de eventos sospechosos clave y envío de alertas al respecto; procedimientos de manejo de la información según el tipo de datos, aplicación de comercio electrónico y seguridad de la red; uso de activos externos y análisis del sistema y las aplicaciones en busca de vulnerabilidades. El Proveedor exige el cifrado de los datos en tránsito y en reposo cuando sea necesario y de conformidad con su programa de seguridad de la información. El Proveedor utiliza cifrado y protocolos adecuados (por ejemplo, TLS) cuando accede de forma remota al entorno de un cliente o al transmitir datos del cliente entre redes abiertas. El Proveedor almacena sus claves de cifrado, cuando no están en uso, en soluciones aprobadas diseñadas para proporcionar prácticas de gestión de claves aceptadas por el sector.
Controles de acceso	El Proveedor implementa controles de acceso adecuados diseñados para proteger contra el acceso no autorizado a la Red del Proveedor. Para reducir el riesgo de uso indebido, intencionado o no, el acceso a la Red del Proveedor se controla según los principios de “mínimo privilegio” y “necesidad de saber”. El Proveedor puede utilizar diversos controles de acceso, tales como revisiones de acceso, mantenimiento de cuentas de servicio y acceso privilegiado a las aplicaciones, configuraciones a nivel de sistema para el acceso y la generación de informes relacionados con el acceso.

	El Proveedor utiliza prácticas estándar del sector, incluida, cuando procede, la autenticación de dos factores, para identificar y autenticar a los usuarios de la Red del Proveedor. El Proveedor exige el uso de contraseñas seguras en toda la Red del Proveedor. El Proveedor (a) prohíbe a los usuarios de la Red del Proveedor compartir, escribir, enviar por correo electrónico, enviar por mensajería instantánea o almacenar contraseñas sin cifrar en cualquier sistema; y (b) bloquea las cuentas tras una serie de intentos fallidos de introducir la contraseña. Según corresponda, el Proveedor utiliza prácticas estándar del sector para mejorar los controles de acceso, incluyendo: (a) La desconexión automática de las sesiones de usuario en caso de inactividad. (b) El requisito de introducir la identificación y la contraseña para volver a acceder. (c) La protección contra el acceso externo mediante uno o varios firewalls aceptados por el sector cuya conexión a Internet, en su caso, esté salvaguardada por una conexión VPN. (d) El enmascaramiento de las contraseñas cuando se muestran o se introducen, según proceda. (e) Un cifrado de contraseñas adecuado y estándar del sector cuando se transmiten.
Administración de incidentes	El Proveedor utiliza un marco de respuesta a incidentes para preparar, responder, gestionar y minimizar los efectos de los eventos de seguridad. El marco incluye procedimientos que deben seguirse en caso de incidente de seguridad, entre ellos: (a) Un equipo interno de respuesta a incidentes con un jefe de respuesta. (b) Un equipo de investigación que realice un análisis de causa raíz e identifique a las partes afectadas. (c) Procesos internos de información y notificación. (d) Un proceso de documentación de las medidas de respuesta y los planes de corrección. (e) Una revisión de los acontecimientos tras el incidente.
Gestión de la continuidad empresarial	El Proveedor cuenta con planes de continuidad empresarial (“**BCP**”), por sus siglas en inglés) para recuperarse de una interrupción empresarial y reanudar las operaciones empresariales normales tan pronto como sea razonablemente posible. El Proveedor hará intentos razonables y oportunos, según las circunstancias, para ponerse en contacto con Usted en caso de una interrupción de la actividad empresarial que afecte materialmente a los clientes del Proveedor.