MEDIDAS TÉCNICAS Y ORGANIZATIVAS

A menos que se especifique lo contrario a continuación, cada uno de los términos definidos en la presente tendrá el significado asignado en el SDPA.

Las medidas técnicas y organizativas del Proveedor deberán incluir, entre otros, lo siguiente:

(i) **Organización de la seguridad de la información** – Creación, ejecución y mantenimiento de políticas de seguridad de la información y un programa de medidas técnicas y organizativas de seguridad adecuadas para proteger la Información del cliente, de conformidad con las Buenas prácticas del sector.

(ii) **Estándares básicos seguros** – Medidas para garantizar que se desarrollen, documenten y mantengan configuraciones seguras en los sistemas de información.

(iii) **Controles de acceso** – Acceso al sistema, acceso de usuarios y medidas de autenticación para evitar el acceso a la Información del cliente de cualquier manera o con cualquier finalidad no autorizadas por el Cliente; las medidas deben incluir, entre otros, la prevención de entradas no autorizadas, lecturas, copias, eliminaciones, modificaciones o revelación de Información del cliente.

(iv) **Seguridad del sistema** – Medidas para reforzar los sistemas de información y otros recursos de conformidad con las Buenas prácticas del sector.

(v) **Auditoría y supervisión –** Medidas para mantener un seguimiento automatizado de auditoría que documente los eventos de seguridad del sistema y cualquier evento de gestión de cambios que suponga el acceso, la modificación y/o la supresión de Información del cliente.

(vi) **Seguridad de la red** – Medidas para mantener un proceso formal de aprobación, comprobación y documentación de todas las conexiones de red, así como de los cambios en las configuraciones de los dispositivos de red.

(vii) **Protección de datos** – Medidas para prevenir el acceso no autorizado, la alteración o la retirada de Información del cliente que se almacena o se está transmitiendo.

(viii) **Concienciación sobre seguridad y formación** – Medidas para ofrecer periódicamente a los empleados formación anual de concienciación sobre seguridad que induzca a la reflexión y sea apropiada para informar sobre tendencias de seguridad, amenazas y mejores prácticas.

(ix) **Pruebas de seguridad –** Medidas para identificar periódicamente y corregir vulnerabilidades según la política del Proveedor, y realizar pruebas periódicas de seguridad en los sistemas y aplicaciones o cuando se produzcan cambios significativos. Estas medidas deben incluir, entre otros, (1) implicar a un tercero independiente para que lleve a cabo una auditoría de seguridad anual en todos los sistemas del Proveedor, (2) realizar pruebas periódicas de penetración y escaneados semanales de vulnerabilidad en todos los sistemas del Proveedor, (3) establecer y mantener un programa de gestión de parches que cumpla las Buenas prácticas del sector y vaya más allá, según el cual el Proveedor actualizará periódicamente el programa que tenga un impacto directo o

indirecto en la Información del cliente y/o los sistemas del Proveedor y (4) designará un enlace de seguridad para el Cliente que podrá abordar los incidentes de seguridad de la información, las pruebas de seguridad, los hallazgos sobre seguridad y otras preocupaciones sobre seguridad a intervalos regulares. Si se identifica cualquier deficiencia material como resultado de lo anterior o de la evaluación de seguridad del Cliente, el Proveedor corregirá la deficiencia material en el plazo de 30 días (cualquier hallazgo crítico que no se corrija en el plazo de 30 días deberá escalarse inmediatamente al Cliente y, a petición del Cliente, el Proveedor proporcionará una certificación escrita conforme se han llevado a cabo las pruebas de seguridad anteriores y una lista detallada de las vulnerabilidades pendientes y los planes para subsanarlas).

(x) **Controles de disponibilidad –** Medidas para desarrollar, operar, gestionar y revisar la continuidad del negocio y los planes de recuperación en caso de catástrofe, incluida la recuperación tecnológica.

(xi) **Corrección de problemas de seguridad del programa –** Si, como parte de los Servicios, el Proveedor ofrece SaaS o PaaS o cualquier servicio de programa alojado, y si el Proveedor o el Cliente descubren o sospechan que existen vulnerabilidades u otros problemas de seguridad en el programa, las medidas para proporcionar correcciones de errores, actualizaciones, parches, revisiones, reparaciones y nuevas versiones del programa (con documentación de cada actuación) incluidas en la aplicación al Cliente de conformidad con los plazos siguientes. El Proveedor proporcionará pruebas al Cliente que demuestren que todos los problemas de seguridad identificados se han corregido en su totalidad de conformidad con el plan definido de acciones correctivas.

Gravedad	Descripción	Aceptación	Actualizaciones	Resolución	Cierre
Emergencia	Problemas catastróficos sin una solución alternativa viable	1 hora laborable tras la detección de la vulnerabilidad o del problema de seguridad	Cada 3 horas laborables	1 día	7 días
Crítico	Problemas que suponen una amenaza seria para el usuario final y/o el Cliente	4 horas laborables tras la detección de la vulnerabilidad o del problema de seguridad	A diario	5 días	14 días
Importante	Problemas con una solución alternativa viable que se pueden mitigar con otros controles de seguridad existentes	2 días laborales tras la detección de la vulnerabilidad o del problema de seguridad	5 días	10 días	45 días
No crítico	Otros problemas o soluciones alternativas	5 días laborales tras la detección de la vulnerabilidad o del problema de seguridad	5 días	15 días	Siguiente versión