Requisitos de seguridad de Experian

Los requisitos de seguridad incluidos en este documento representan los requisitos mínimos de seguridad aceptables para Experian y tienen por objeto garantizar que un Tercero (es decir, un Proveedor, Revendedor (Reseller), Prestador de Servicios o cualquier otra organización que colabore con Experian) disponga de los controles adecuados para proteger la información y sus sistemas, incluida cualquier información que reciba, procese, transfiera, transmita, almacene, entregue y/o acceda de otra manera en nombre de Experian.

DEFINICIONES

"Información de Experian" significa la información altamente sensible de Experian, incluyendo, a modo de ejemplo y sin limitación, datos, bases de datos, software de aplicación, documentación de software, documentos de procesos de apoyo, documentación de procesos y procedimientos de operación, planes de prueba, casos de prueba, escenarios de prueba, informes de incidentes cibernéticos, información de consumidores, registros financieros, registros de empleados e información sobre posibles adquisiciones, y cualquier otra información que sea de naturaleza similar o que se haya acordado mutuamente por escrito, cuya divulgación, alteración o destrucción causaría un daño grave a la reputación, valoración y/o proporcionaría una desventaja competitiva a Experian.

"Recurso" se refiere a todos los dispositivos de Terceros, incluidos, entre otros, ordenadores portátiles, PC, enrutadores (routers), servidores y otros sistemas informáticos que almacenan, procesan, transfieren, transmiten, entregan o acceden a la Información de Experian.

REQUISITOS DE SEGURIDAD

1. **Políticas y gobernanza de seguridad de la información**

El Tercero debe tener políticas y procedimientos de seguridad de la información que sean consistentes con las prácticas descritas en una norma estándar de la industria, como la norma ISO 27002 y/o el presente documento de requisitos de seguridad, el cual está alineado con la política de seguridad de la información de Experian.

2. **Gestión de vulnerabilidades**

Los cortafuegos (Firewalls), enrutadores (routers), servidores, PCs y todos los demás recursos administrados por el Tercero (incluyendo la infraestructura física, local o alojada en la nube) se mantendrán actualizados con parches adecuados específicos al sistema de seguridad. El Tercero realizará pruebas periódicas de penetración para evaluar aún más la seguridad de los sistemas y recursos. El Tercero utilizará servicios y procedimientos de detección/escaneo de malware informático de punto final.

3. **Registro y seguimiento**

Habrá suficientes mecanismos de registro para identificar los incidentes de seguridad, establecer la responsabilidad individual y reconstruir los eventos. Los registros de auditoría se conservarán en un estado protegido (es decir, cifrados o bloqueados) con un proceso de revisión periódica.

4. **Seguridad de la red**

El Tercero utilizará medidas de seguridad, incluyendo software antivirus, para proteger los sistemas de comunicaciones y los dispositivos de red para reducir el riesgo de infiltración, piratería, penetración del acceso o exposición a un tercero no autorizado.

5. **Seguridad de datos**

El Tercero utilizará medidas para proteger la información suministrada por Experian, incluyendo encriptación de la información, con el fin de reducir el riesgo de divulgación de los datos almacenados y/o en tránsito a terceros no autorizados.

6. **Autorización de conexión de acceso remoto**

Todas las conexiones de acceso remoto a redes internas y/o sistemas informáticos del Tercero requerirán autorización con control de acceso en el punto de entrada mediante autenticación multifactorial. Dicho acceso utilizará canales seguros, como una red privada virtual (VPN).

7. **Respuesta a incidentes**

Se establecerán procesos y procedimientos para responder a violaciones de seguridad, eventos e incidentes inusuales o sospechosos. Ante sospecha o confirmación de violaciones de seguridad que

puedan afectar a la información de Experian, el Tercero deberá informar a Experian dentro de las veinticuatro (24) horas posteriores a la confirmación del Tercero de dicha violación o incidente.

8. **Identificación, autenticación y autorización**

Cada usuario de cualquier recurso tendrá una identificación de usuario asignada de forma única/exclusiva para permitir la autenticación y la responsabilidad individual. El acceso a las cuentas privilegiadas estará restringido a aquellas personas que administran el recurso, y se mantendrá la responsabilidad individual. Todas las contraseñas predeterminadas/por defecto (como las de proveedores de hardware o software) se cambiarán inmediatamente después de su recepción.

9. **Cuentas y contraseñas de usuario**

Todas las contraseñas permanecerán confidenciales, y se utilizarán contraseñas "seguras" que caduquen/expiren después de un máximo de 90 días calendario/naturales. Las cuentas se bloquearán automáticamente después de cinco (5) intentos de inicio de sesión fallidos consecutivos.

10. **Capacitación y sensibilización**

El Tercero requerirá que todo su personal participe en sesiones de capacitación y concientización/sensibilización sobre seguridad de la información al menos una vez al año, y establecerá pruebas de aprendizaje para todo su personal.

11. **Derecho de auditoría de Experian**

El Tercero estará sujeto a evaluaciones remotas y/o in situ por parte de Experian con el fin de evaluar sus controles de seguridad de la información y el cumplimiento de estos Requisitos de seguridad.