

# GUÍA PARA EL CISO: PROTECCIÓN DE CONEXIONES CON TERCEROS

## IDENTIFICACIÓN DE RIESGOS A TRAVÉS DE TERCEROS

- Cree y mantenga una lista actualizada de todas las relaciones con los proveedores y los activos y datos expuestos en cada uno de ellos.
- Revise los datos a los que tiene acceso cada proveedor o tercero. Asegúrese de que este nivel de acceso respeta el principio de “mínimo privilegio”.
- Clasifique sus relaciones con proveedores y terceros (bajo, medio, alto) basándose en el impacto que tendría un incumplimiento de sus sistemas en su organización.
- Comenzando con los proveedores de mayor riesgo, evalúe las capacidades de ciberseguridad de cada proveedor. El cumplimiento de los estándares relevantes es un buen punto de partida. Desarrolle un plan para una evaluación regular de la seguridad. Es posible que quiera llevar a cabo ocasionalmente evaluaciones in situ de proveedores con el mayor riesgo o acceso a los datos del cliente.

## GESTIÓN DE SEGURIDAD DE TERCEROS

- Realice una diligencia debida exhaustiva. Establezca expectativas de ciberseguridad en las solicitudes de su organización de propuestas, contratos, continuidad del negocio, respuesta a incidentes y acuerdos de nivel de servicio con proveedores. Acuerde responsabilidades y obligaciones en caso de producirse un incidente cibernético.
  - Pregunte sobre las prácticas de ciberseguridad de otros terceros, como organizaciones financieras con las que usted haga transacciones o comparta datos. Todos los requisitos de ciberseguridad a los que debe adherirse su organización también deben ser seguidos por sus proveedores y cualquier otra organización con la que comparta los datos o exponga los activos a los mismos.
- Utilice medidas establecidas y acordadas para supervisar el cumplimiento de sus proveedores con los estándares de ciberseguridad.
- Consulte con sus proveedores que manejan datos confidenciales para ver si ofrecen autenticación de dos factores, cifrado u otras medidas de seguridad para cualquier cuenta que tenga con ellos.
- Asegúrese de que todo el software y hardware de terceros que instale tenga un control de seguridad para que los procesos de arranque se fijen mediante códigos de autenticación y no se ejecuten si no se reconocen los códigos.
- Si encuentra productos de proveedores que sean falsificados o que no cumplan las especificaciones, trabaje para negociar una resolución o una estrategia de salida.
- Evalúe anualmente los contratos de proveedores y asegúrese de que sigan cumpliendo con su dirección estratégica y con los requisitos de seguridad de los datos normativos. Tras la finalización del contrato, incluya las estipulaciones sobre la obtención de sus activos o datos y verifique que los activos o datos se eliminen por completo por parte del proveedor, y desactive cualquier acceso a sus sistemas o servidores.

## USO COMPARTIDO DE INFORMACIÓN

- Asegúrese de disponer de canales de comunicación y puntos de contacto claros para comunicarse sobre cuestiones de seguridad con los proveedores y los homólogos de su organización.
- Participe en el intercambio oportuno de información fiable y procesable sobre ciberseguridad con partes interesadas internas y externas (incluidas entidades y autoridades públicas dentro y fuera del sector financiero).
- Realice un seguimiento de las actualizaciones relevantes sobre lo que otras organizaciones están experimentando con sus terceros en términos de amenazas, vulnerabilidades, incidentes y respuestas para mejorar las defensas de su organización, aumentar la concienciación situacional y ampliar el aprendizaje. Formar parte de organizaciones de intercambio de información, como, por ejemplo, el FS-ISAC, le facilitará estar al día.

## Cómo elegir proveedores teniendo en mente la ciberseguridad

Haga las siguientes preguntas a los posibles proveedores para evaluar su preparación y concienciación cibernéticas y, en consecuencia, el impacto que tendría en el perfil de riesgo de su organización:

1. **¿Qué experiencia tienen?** Conozca el historial del proveedor prestando servicios a clientes. ¿Han prestado servicios a clientes similares a su organización?
2. **¿Han documentado su cumplimiento con los estándares de ciberseguridad conocidos,** como el marco NIST o la norma ISO 27001, o pueden proporcionar un informe SOC2?
3. **¿A cuáles de sus datos o activos tendrán que acceder para prestar sus servicios?** ¿Están solicitando un acceso aparentemente innecesario?
4. **¿Cómo planean proteger los activos y los datos de su organización que están en su posesión?**
5. **¿Cómo gestionan su propio riesgo cibernético de terceros?** ¿Pueden proporcionar información sobre su cadena de suministros?
6. **¿Cuál es su plan de recuperación ante desastres y continuidad empresarial** en caso de producirse un incidente que afecte a los activos o datos de su organización?
7. **¿Cómo mantendrán actualizada su organización?** ¿Cuál es su plan para comunicar tendencias, amenazas y cambios dentro de su organización?