CIBERSEGURIDAD PARA ORGANIZACIONES MÁS PEQUEÑAS

LISTA DE COMPROBACIÓN DEL CISO: PROTECCIÓN DE CONEXIONES CON TERCEROS

CÓMO ELEGIR PROVEEDORES TENIENDO EN MENTE LA CIBERSEGURIDAD

Cada vez que evalúe a un proveedor potencial, consulte las siguientes preguntas:

- ☐ **¿Qué experiencia tienen prestando servicios a clientes similares a su organización?**
- ☐ **¿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?**
- ☐ **¿A cuáles de sus datos o activos tendrán que acceder para prestar sus servicios? ¿Están solicitando un acceso que parece innecesario?**
- ☐ **¿Cómo planean proteger los activos y los datos de su organización que están en su posesión?**
- ☐ **¿Cómo gestionan su propio riesgo cibernético de terceros? ¿Pueden proporcionar información sobre la seguridad de su cadena de suministro?**
- ☐ **¿Cuál es su plan de recuperación ante desastres y continuidad empresarial en caso de producirse un incidente que afecte a su organización?**
- ☐ **¿Cómo mantendrán actualizada su organización para comunicar tendencias, amenazas y cambios dentro de su organización?**

IDENTIFICACIÓN DE RIESGOS A TRAVÉS DE TERCEROS

Realice una evaluación de riesgos cibernéticos de terceros, incluidos los siguientes pasos:

- ☐ **Cree y mantenga una lista actualizada de todas las relaciones con los proveedores y los activos y datos expuestos en cada una de ellas.**
- ☐ **Revise los datos a los que tiene acceso cada proveedor o tercero, asegurándose de que cada nivel de acceso cumpla con el principio de "privilegio mínimo".**
- ☐ **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 y el cumplimiento de los estándares relevantes.**
- ☐ **Desarrolle un plan para realizar una evaluación regular de la seguridad, teniendo en cuenta que 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 organizaciones financieras y otras entidades con las que usted haga transacciones o comparta datos, teniendo en cuenta que sus proveedores y terceros también deben seguir los requisitos de ciberseguridad que su organización debe cumplir.**

- ☐ 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, convirtiéndose en parte de organizaciones de intercambio de información como FS-ISAC y buscando otras fuentes de información de amenazas.

CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE

CarnegieEndowment.org

THE WORLD BANK IBRD • IDA | WORLD BANK GROUP · SWIFT · SWIFT INSTITUTE · FS-ISAC · Standard Chartered · CYBER READINESS INSTITUTE · GLOBAL CYBER ALLIANCE · ICBA Independent Community Bankers of America®