

CIBERSEGURIDAD PARA ORGANIZACIONES FINANCIERAS MÁS PEQUEÑAS

LISTA DE COMPROBACIÓN DE LA JUNTA DIRECTIVA: LIDERAZGO DE CIBERSEGURIDAD

FUNDAMENTOS DE LA GOBERNANZA DEL RIESGO CIBERNÉTICO

- Como grupo, evalúe periódicamente si la junta directiva puede responder afirmativamente a las siguientes preguntas:
 - ¿Su organización ha cumplido los requisitos legales y reglamentarios pertinentes, como el RGPD?
 - ¿Su organización ha cuantificado sus exposiciones cibernéticas y probado su resiliencia financiera?
 - ¿Su organización ha implementado un plan de mejora para garantizar que las exposiciones están dentro de su predisposición al riesgo acordado?
 - ¿La junta directiva regularmente discute información concisa, clara y práctica sobre la resiliencia cibernética de la organización proporcionada por la dirección?
 - ¿Su organización tiene planes de respuesta a incidentes que se han probado recientemente, incluido a nivel directivo?
 - ¿Están las funciones de personas clave responsables de gestionar el riesgo cibernético claras y en sintonía con las tres líneas de defensa?
 - ¿Ha obtenido validación y garantía independientes de la postura de riesgo cibernético de su organización, como por ejemplo a través de una prueba, certificación o seguro?
- Si no puede responder de forma afirmativa a una o más de las anteriores preguntas, trabaje con su CEO (Chief Executive Officer [Director ejecutivo]), CISO (Chief Information Security Officer [Director de seguridad de la información]), personal de la organización pertinente o recursos externos para corregir el problema.

SUPERVISIÓN

- Asegúrese de que la junta directiva es consciente de su papel como titular de la responsabilidad final en cuanto al riesgo cibernético y la resiliencia de su organización.
 - Delegue la supervisión a un comité de junta directiva específico si se considera necesario.
- Asigne un directivo corporativo, normalmente el CISO, para que sea el responsable de informar sobre la capacidad de su organización de gestionar la resiliencia cibernética y el progreso en la implementación de objetivos de resiliencia cibernética.
 - Asegúrese de que este directivo tiene acceso regular a la junta directiva, autoridad suficiente, dominio de la materia, experiencia y recursos para cumplir estas obligaciones.
- Defina anualmente la tolerancia al riesgo de su organización; garantice la coherencia con su estrategia corporativa y su predisposición al riesgo.
- Asegúrese de que se realiza anualmente una revisión formal e independiente de la resiliencia cibernética de su organización.
- Integre la evaluación de riesgos y resiliencia cibernética en la estrategia empresarial general de su organización, gestión de riesgos, presupuestos y asignación de recursos.
- Supervise la creación, implementación, pruebas y mejora continua de los planes de resiliencia cibernética, asegurándose de que se alineen en toda su organización y de que su CISO u otro directivo responsable informe regularmente sobre ellos a la junta directiva.
- Revise periódicamente su rendimiento en cuanto a lo anterior y considere asesoramiento independiente para la mejora continua.

CÓMO MANTENERSE INFORMADO

- Cuando una persona se incorpore a la junta directiva, garantice que tenga habilidades y conocimientos actualizados para comprender y gestionar los riesgos planteados por amenazas cibernéticas.
- Solicite asesoramiento habitual de la gerencia sobre la exposición al riesgo actual y futuro de su organización, los requisitos normativos pertinentes y los índices de referencia de la industria y la sociedad para la predisposición al riesgo. Planee participar en:
 - Sesiones informativas periódicas sobre los deberes creados por nuevas normativas y leyes.
 - La planificación conjunta de la junta directiva y el comité ejecutivo y visitas a compañeros y líderes de mejores prácticas y ciberseguridad.
 - Sesiones informativas sobre seguridad en el entorno de amenazas.
 - Intercambios a nivel de junta directiva de información sobre gobernanza e informes.
- Deje claro a la gerencia que son responsables de informar de una evaluación cuantificada y comprensible de los riesgos cibernéticos, amenazas y eventos como un elemento de la orden del día permanente durante las reuniones de la junta directiva.
- Compruebe periódicamente con la dirección y otros miembros del personal relevantes los desarrollos relacionados con los retos sistémicos continuos, como las vulnerabilidades de la cadena de suministro, las dependencias comunes y la brecha en el intercambio de información entre juntas directivas sobre la gobernanza del riesgo cibernético.

EXPLICACIÓN DEL CONTEXTO

- Asegúrese de que el personal de todos los niveles reconoce que cada uno tiene responsabilidades importantes para garantizar la resiliencia cibernética de su organización.
- Supervise el papel de la gerencia en la promoción y el mantenimiento de la cultura del riesgo de su organización. Evalúe periódicamente la eficacia de la cultura del riesgo de su organización, teniendo en cuenta el impacto de la cultura en la seguridad y la solidez, y haga cambios cuando sea necesario.
- Deje claro que espera que todo el personal actúe con integridad y que informe rápidamente de los casos de incumplimiento observados dentro o fuera de su organización.

CIBERSEGURIDAD PARA ORGANIZACIONES FINANCIERAS MÁS PEQUEÑAS

LISTA DE COMPROBACIÓN DEL CEO: LIDERAZGO DE CIBERSEGURIDAD

GOBERNANZA

- Nombre a un CISO (Chief Information Security Officer [Director de seguridad de la información]) si no existe ninguno.
- Establezca y mantenga una política de ciberseguridad en toda la organización que esté basada en el riesgo y sobre las que informan las normas y directrices internacionales, nacionales y del sector.
- Defina las funciones y responsabilidades para todo el personal involucrado en la ciberseguridad. Trabaje con el CISO para identificar las funciones de ciberseguridad y los derechos de acceso adecuados para todos los niveles de personal.
- Establezca o identifique canales de comunicación claros entre cualquier unidad o personal independiente que trate con distintos aspectos de la ciberseguridad.
- Garantice que el CISO tenga una línea de comunicación clara y directa para comunicar las amenazas de forma oportuna con usted y con la junta directiva.
- Mantenga una invitación periódica para que su CISO u otro personal técnico informe a la alta gerencia.
- Compruebe que las políticas, normas y mecanismos de ciberseguridad son uniformes en toda la organización.

EVALUACIÓN Y GESTIÓN DE RIESGOS

- Realice una evaluación de riesgos de ciberseguridad en colaboración con su CISO u otro personal técnico, que debe incluir:
 - Describir los activos de su organización y sus diversos niveles de dependencia tecnológica.
 - Evaluar la madurez de su organización y los riesgos inherentes asociados a las dependencias tecnológicas de sus activos.
 - Determinar el estado de madurez deseado de su organización.
 - Comprender dónde se encuentran las amenazas de ciberseguridad en la lista de prioridades de riesgo de su organización.
 - Identificar brechas entre su estado actual de ciberseguridad y el estado objetivo deseado.
 - Implementar planes para alcanzar y mantener la madurez.
 - Reevaluar continuamente la madurez, los riesgos y los objetivos de la ciberseguridad de su organización.
 - Considerar tomar medidas de protección, como adquirir un seguro cibernético.
- Analice y presente los resultados a las partes interesadas clave y a la junta directiva.
- Planee supervisar los pasos para aumentar la preparación cibernética y controlar el progreso.

CULTURA ORGANIZATIVA

- Discuta con regularidad el riesgo cibernético y la seguridad en el nivel de liderazgo.
- Asegúrese de que la formación sobre ciberseguridad forma parte de la incorporación de todos los empleados y de que todos los empleados firmen documentos que acepten adherirse a las políticas de ciberseguridad de la organización.
- Establezca formación de ciberseguridad recurrente para todo el personal.
- Asegúrese de que la ciberseguridad siempre se tenga en cuenta cuando su organización evalúe los posibles proveedores y comparta datos con terceros.
- Instituya una revisión anual de las políticas de ciberseguridad de la organización.
- Fomente el intercambio voluntario de información sobre amenazas e incidentes de ciberseguridad entre el personal técnico.

CIBERSEGURIDAD PARA ORGANIZACIONES FINANCIERAS MÁS PEQUEÑAS

LISTA DE COMPROBACIÓN DEL CISO: PROTEGER SU ORGANIZACIÓN

DESARROLLO DE UN PROGRAMA DE SEGURIDAD DE LA INFORMACIÓN BASADO EN RIESGOS

- Enumere todos los tipos de información que almacena o utiliza su empresa (p. ej., nombres de clientes y correo electrónico).
- Pregunte y registre las respuestas para cada tipo de información:
 - ¿Qué ocurriría si esta información se hiciera pública?
 - ¿Qué ocurriría con mi negocio si esta información fuera incorrecta?
 - ¿Qué ocurriría con mi negocio si mis clientes o yo no pudiéramos acceder a esta información?
- [Registre qué tecnología](#) entra en contacto con la información que ha identificado. Esto puede incluir hardware (p. ej., ordenadores) y aplicaciones de software (p. ej., correo electrónico del navegador).
 - Si procede, incluya tecnologías ajenas a su negocio (p. ej., “la nube”) y cualquier tecnología de protección que tenga instalada, como cortafuegos.
 - Incluya la marca, el modelo, los números de serie y otros identificadores.
 - Realice un seguimiento de dónde se encuentra cada producto. Para el software, identifique las máquinas en las que se ha cargado el software.
- Revise periódicamente la información de su CERT (Computer Emergency Response Team [Centro criptológico nacional Computer Emergency Response Team]) nacional, FS-ISAC (Financial Services - Information Sharing and Analysis Center [Centro de Análisis e Intercambio de Información de Servicios Financieros]), su filial local de InfraGard y otras personas sobre las amenazas y vulnerabilidades que el sector financiero puede afrontar y estime la probabilidad de que se vea afectado.
- Realice una exploración o análisis de vulnerabilidad al menos una vez al año.
- Cree una política de ciberseguridad para su organización.
- Forme a todos los empleados sobre los detalles de la política y haga que firmen documentos en los que reconozcan su papel en el mantenimiento continuo de la ciberseguridad de su organización mediante la adhesión a la política.

PREVENCIÓN DE DAÑOS POR MALWARE

- Active su cortafuegos y establezca listas de control de acceso (ACL, por sus siglas en inglés). Restrinja el acceso mediante una configuración de lista blanca.
- [Utilice software antivirus y antispyware](#) en todos los ordenadores y portátiles.
- [Aplique las últimas actualizaciones de software](#) proporcionadas por fabricantes y proveedores. Active la ‘Actualización automática’ cuando esté disponible.
- Restrinja la instalación de nuevos programas al personal de TI con derechos de administración.
- Mantenga y supervise los registros de actividad generados por hardware o software de protección/detección. Proteja los registros con protección y cifrado con contraseña.
- Mantenga sincronizados todos los relojes del host.
- Controle el acceso a medios extraíbles, como tarjetas SD y memorias USB. Anime al personal a transferir archivos por correo electrónico o almacenamiento en la nube. Eduque al personal sobre los riesgos de [utilizar los USB](#) de fuentes externas o entregar sus USB a otros.
- [Configure la seguridad de correo electrónico y filtros de correo no deseado](#) en los servicios de correo electrónico.
- Proteja todas las páginas de sus [sitios web orientados al público](#) con [cifrado](#) y otras herramientas disponibles.

- Considere la contratación de un servicio de pruebas de penetración para evaluar la seguridad de los activos y sistemas de su organización.

FORMACIÓN PARA EMPLEADOS

- Planee impartir cursos obligatorios de formación sobre ciberseguridad durante la incorporación de nuevos empleados y a intervalos regulares para todos los empleados actuales, al menos una vez al año. Exija a los empleados que:
 - [Utilicen contraseñas seguras](#) en todos los dispositivos y cuentas profesionales, y anímelos para que hagan lo mismo para dispositivos personales y utilicen un gestor de contraseñas.
 - Mantengan todos los sistemas operativos, software y aplicaciones [actualizados](#) en todos los dispositivos.
 - [Usen autenticación de dos factores](#) en todas las cuentas.
 - Mantengan los detalles de la cuenta y las tarjetas de acceso de forma segura y bloqueen los dispositivos cuando no estén supervisados.
 - Se abstengan de compartir detalles de cuentas u otros datos confidenciales mediante correo electrónico no cifrado u otras comunicaciones abiertas.
 - [Eviten abrir de inmediato archivos adjuntos](#) o hacer clic en enlaces en correos electrónicos no solicitados o sospechosos.
 - Verifiquen la validez de un correo electrónico de aspecto sospechoso o un mensaje emergente antes de proporcionar información personal, y presten mucha atención a la dirección de correo electrónico.
 - Informen de cualquier posible incidente de seguridad interno o externo, amenazas o manipulación indebida de datos o dispositivos al personal técnico de su organización o a la gerencia superior.
- Compruebe periódicamente la concienciación de los empleados mediante problemas simulados, como el envío de correos electrónicos de tipo phishing desde cuentas falsificadas. Evalúe los fallos de los empleados y utilícelos como oportunidades de aprendizaje y mejora.

PROTECCIÓN DE SUS DATOS

- [Realice copias de seguridad periódicas](#) de sus datos importantes (p. ej., documentos, correos electrónicos y calendarios) y compruebe que pueden restaurarse. Considere la posibilidad de hacer copias de seguridad en la nube.
- Asegúrese de que el dispositivo que contiene su copia de seguridad no esté permanentemente conectado al dispositivo que contenga la copia original, ni físicamente ni a través de una red local.
- Instale protectores contra sobrecargas de tensión, utilice generadores y asegúrese de que todos sus ordenadores y dispositivos de red críticos estén conectados a fuentes de alimentación ininterrumpidas.
- Utilice una solución de gestión de dispositivos móviles (MDM, por sus siglas en inglés).

MANTENIMIENTO DE DISPOSITIVOS SEGUROS

- Active la protección por contraseña o PIN para dispositivos móviles. Configure los dispositivos para que cuando se pierdan o se roben puedan ser rastreados, borrados o bloqueados a distancia.
- Mantenga sus dispositivos (y todas las aplicaciones instaladas) [actualizadas](#), utilizando la opción de actualización automática, si está disponible.
- Al enviar datos confidenciales, no se conecte a puntos de acceso Wi-Fi públicos: utilice conexiones celulares (lo que incluye conexión y dongles inalámbricos) o una VPN.
- Sustituya los dispositivos que ya no sean compatibles con los fabricantes con alternativas actualizadas.
- Establezca procedimientos de notificación de equipos perdidos o robados.

USO DE CONTRASEÑAS

- Asegúrese de que todos los ordenadores utilizan productos de cifrado que requieran una contraseña para arrancar. Active la protección por contraseña o PIN para dispositivos móviles.
- [Utilice contraseñas seguras](#), evitando contraseñas predecibles (como passw0rd) e identificadores personales (como nombres de familiares y mascotas). Indique a todos los empleados que hagan lo mismo.
- [Utilice la autenticación de dos factores](#) (2FA, por sus siglas en inglés) siempre que sea posible.
- Cambie las contraseñas predeterminadas emitidas por el fabricante en todos los dispositivos, incluidos los dispositivos de red e IoT, antes de distribuirlos al personal.
- Asegúrese de que el personal puede restablecer sus propias contraseñas fácilmente. También puede solicitar que el personal cambie su contraseña a intervalos regulares (por ejemplo, trimestral, semestral o anualmente).
- Considere utilizar un [gestor de contraseñas](#). Si utiliza uno, asegúrese de que la contraseña “maestra” (que proporciona acceso a todas las demás contraseñas) sea segura.

CONTROL DE PERMISOS

- Asegúrese de que todo el personal tenga cuentas identificables únicas que se autentican cada vez que acceden a sus sistemas.
- Proporcione únicamente privilegios administrativos al personal de TI y personal clave de confianza y revoque los privilegios de administrador en estaciones de trabajo para usuarios estándar.
- Facilite a los empleados únicamente acceso a los sistemas de datos específicos que necesiten para sus trabajos y asegúrese de que no pueden instalar ningún software sin permiso.
- Cree cuentas de usuario para cada empleado en los ordenadores de su organización.

PROTECCIÓN DE LA WI-FI

- Asegúrese de que su Wi-Fi en el lugar de trabajo sea segura y esté cifrada con WPA2. Los routers con frecuencia vienen con el cifrado desactivado, así que tiene que asegurarse de que lo activa. Proteja con contraseña el acceso al router y asegúrese de que la contraseña se actualice desde el valor predeterminado. Desactive todas las funciones de “gestión remota”.
- Configure el punto de acceso inalámbrico o el router para que no transmita el nombre de red, conocido como identificador del conjunto de servicios (SSID).
- Limite el acceso a su red Wi-Fi permitiendo solo dispositivos con determinadas direcciones de control de acceso a los medios. Si los clientes necesitan Wi-Fi, configure una red pública independiente.
- Habilite el Protocolo de configuración dinámica de host (DHCP) en sus dispositivos de red para permitir un seguimiento sencillo de todos los dispositivos que han estado en su red.
- Cierre sesión como administrador después de configurar el router.
- Mantenga actualizado el software del router. Manténgase informado de las actualizaciones registrando su router con el fabricante e inscribiéndose para obtener actualizaciones.

CÓMO EVITAR ATAQUES DE PHISHING

- Asegúrese de que el personal no navegue por la web ni revise los correos electrónicos en servidores o desde una cuenta con privilegios de Administrador.
- Configure filtros web y de correo electrónico. Considere la posibilidad de impedir que los empleados visiten sitios web comúnmente asociados a amenazas de ciberseguridad.
- Enseñe a los empleados a detectar [señales obvias de phishing](#), como mala ortografía y gramática, o versiones de baja calidad de logotipos reconocibles. ¿Parece legítima la dirección de correo electrónico del remitente?
- Escanee en busca de malware y cambie las contraseñas lo antes posible si sospecha que se ha producido un ataque. No castigue al personal si se convierte en víctima de un ataque de phishing (disuadirá a las personas de informar en el futuro).

ASESORAMIENTO A CLIENTES Y EMPLEADOS SOBRE LA PROTECCIÓN DE DATOS A NIVEL INDIVIDUAL

- Proporcione a los empleados y a los clientes las siguientes directrices personales a seguir para proteger mejor sus datos:
 - [Utilice contraseñas seguras](#) en todos los dispositivos personales y profesionales, y considere utilizar un gestor de contraseñas.
 - Mantenga [actualizados](#) los sistemas operativos, otro software y aplicaciones en sus ordenadores y dispositivos móviles.
 - [Instale](#) software antivirus, antimalware y antiransomware que prevenga, detecte y elimine programas malintencionados.
 - Utilice un programa cortafuegos para evitar el acceso no autorizado a su ordenador.
 - Utilice únicamente productos de seguridad de empresas fiables. Lea las revisiones de las publicaciones de ordenadores y consumidores, y considere la posibilidad de consultar al fabricante de su ordenador o sistema operativo.
 - Tenga cuidado con la información confidencial. No envíe contraseñas de cuentas bancarias ni otros datos de cuentas financieras confidenciales a través de correo electrónico sin cifrar.
 - Sea inteligente sobre dónde y cómo se [conecta a Internet](#) para acciones bancarias u otras comunicaciones relacionadas con información personal confidencial.
 - No abra de inmediato archivos adjuntos de correo electrónico ni haga clic en enlaces en correos electrónicos no solicitados o sospechosos. Pare. Piense. Haga clic.
 - Sospeche si alguien se pone en contacto con usted inesperadamente en línea o por teléfono y le pide su información personal. Incluso cuando se comunique con direcciones conocidas, minimice el intercambio de información personal por correo electrónico.
 - Recuerde que ninguna institución financiera le enviará un correo electrónico o le llamará y solicitará información confidencial que ya tenga sobre usted.
 - Suponga que una solicitud de información de un banco donde nunca ha abierto una cuenta es una estafa.
 - [Verifique](#) la validez de un correo electrónico de aspecto sospechoso o un mensaje emergente antes de proporcionar información personal. Preste mucha atención a la dirección de correo electrónico.

ADMINISTRACIÓN DE CUENTAS

- [Exija que los clientes utilicen nombres de usuario y contraseñas seguros](#) para iniciar sesión en sus servicios. Aconséjeles que no utilicen la misma contraseña que para otras cuentas.
- Utilice verificación instantánea, verificación en tiempo real, verificación de depósito de prueba, verificación de identidad o preguntas de autenticación para validar clientes reales y reducir la oportunidad de fraude.
- Ofrezca, si no puede exigirlo, la autenticación de dos factores para que los clientes la utilicen al iniciar sesión en sus servicios.
- Compruebe periódicamente las cuentas de usuario para detectar signos de fraude.

PROTECCIÓN DE DATOS

- Considere qué datos de clientes su organización debe recopilar para prestar sus servicios y tenga cuidado para evitar recopilar datos de clientes que vayan más allá de eso.
- Establezca y distribuya políticas de retención de datos. Elimine los datos del cliente cuando ya no sean necesarios.
- Cifre los datos del cliente en tránsito y en reposo.
- Ponga en marcha políticas de seguridad de datos para aclarar qué métodos de transferencia de datos están aprobados y cuáles restringidos, y que especifiquen qué es aceptable para todos los empleados cuando se trata con datos de clientes. Garantice que estas políticas se documenten, se comuniquen, se apliquen a todos los empleados y se revisen y actualicen periódicamente.

PROTECCIÓN DE APLICACIONES WEB PÚBLICAS

- Implemente HTTPS en las aplicaciones web orientadas al público de su organización y redirija todo el tráfico HTTP a HTTPS.
- Utilice una política de seguridad de contenido en su(s) sitio(s) web.
- Habilite la colocación de claves públicas de su sitio web.
- Asegúrese de que sus aplicaciones web orientadas al público nunca utilicen cookies para almacenar información de clientes muy confidencial o crítica (como contraseñas) y de que tengan fechas de caducidad conservadoras para las cookies (el menor tiempo posible).
- Considere cifrar la información almacenada en las cookies que utilice.
- Considere contratar un servicio de pruebas de penetración para evaluar la seguridad de sus aplicaciones web orientadas al público al menos una vez al año.

FORMACIÓN PARA EMPLEADOS

- Enseñe a sus empleados la responsabilidad y las estrategias para minimizar los errores humanos que podrían exponer los datos del cliente. Esto significa aconsejarles:
 - Minimizar el acceso y la transmisión de los datos del cliente a solo lo necesario para realizar sus funciones laborales.
 - Mantener prácticas de seguridad sólidas en todos los dispositivos y cuentas que tratan con los datos de los clientes utilizando contraseñas seguras, habilitando autenticación de dos factores, manteniendo actualizado el software y no haciendo clic en enlaces sospechosos.
 - Informar de cualquier posible incidente de seguridad interno o externo, amenazas o manipulación indebida de datos del cliente al personal técnico de su organización o a la gerencia superior.
- Asegúrese de que sus empleados comprenden y han firmado documentos para cumplir con las políticas de seguridad y protección de datos de su organización.

NOTIFICACIÓN A LOS CLIENTES

- Comprenda el entorno normativo de su organización cuando se trata de gestionar la vulneración de datos de los clientes para asegurarse de que está preparado para cumplir con los incidentes.
- Cuando su organización tenga conocimiento de un incidente de acceso no autorizado a información confidencial del cliente, investigue con prontitud la probabilidad de que la información se haya utilizado o se utilice de forma incorrecta. Siga las prácticas recomendadas de notificación y notifique al cliente o clientes afectados lo antes posible con:
 - Una descripción general del incidente y la información a la que se ha tenido acceso.

- Un número de teléfono para obtener más información y asistencia.
- Un recordatorio de “permanecer alerta” durante los próximos 12 a 24 meses.
- Una recomendación de que los incidentes de sospecha de robo de identidad se notifiquen de inmediato.
- Una descripción general de los pasos adoptados por la institución financiera para proteger la información contra un mayor acceso o uso no autorizado.
- Información de contacto para agencias de informes crediticios.
- Cualquier otra información exigida por las normativas con las que su organización debe cumplir.

CIBERSEGURIDAD PARA ORGANIZACIONES FINANCIERAS 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 los activos o datos de 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 uno de ellos.
- 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.
- 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.

CIBERSEGURIDAD PARA ORGANIZACIONES FINANCIERAS MÁS PEQUEÑAS

LISTA DE COMPROBACIÓN DE RESPUESTA A INCIDENTES

PREPARACIÓN

- Trabaje con el equipo directivo sénior de su organización y con otro personal relevante para desarrollar un plan de respuesta a incidentes y continuidad del negocio basado en los riesgos más urgentes que se han identificado en la evaluación de riesgos cibernéticos de su organización.
- Desarrolle escenarios de amenazas para los tipos de incidentes relacionados con los riesgos cibernéticos de mayor prioridad de su organización. Céntrese en el fomento de la capacidad para responder a esos escenarios.
- Identifique, registre y ponga a disposición dentro de su organización una lista de puntos de contacto para la respuesta a incidentes.
- Identifique y registre la información de contacto de las agencias y funcionarios de cumplimiento de la ley locales y federales pertinentes.
- Establezca disposiciones que especifiquen qué tipos de incidentes deben notificarse, cuándo deben notificarse y a quién.
- Establezca directrices escritas que describan la rapidez con la que el personal debe responder a un incidente y qué acciones deben realizarse, basándose en factores relevantes como el impacto funcional y de información del incidente, y la probable recuperación del incidente.
- Informe a todos los empleados de que deben ponerse en contacto con su equipo técnico (con mayor frecuencia, será el personal de TI, el CISO/CIO u otro gerente comparable) cuando ocurra un incidente.
- Implemente soluciones para supervisar las acciones de los empleados y permitir la identificación de amenazas e incidentes.
- Incluya planes de continuidad del negocio para coordinar cómo funcionará su organización con los proveedores y los clientes principales durante una emergencia empresarial, que incluye cómo realizaría operaciones comerciales manuales o alternativas, si fuera necesario.
- Incluya procedimientos escritos para apagar y reiniciar el sistema de emergencia.
- Desarrolle y pruebe métodos para recuperar y restaurar datos de una copia de seguridad; compruebe periódicamente los datos de una copia de seguridad para verificar su validez.
- Tenga establecidos acuerdos y procedimientos para llevar a cabo operaciones comerciales en instalaciones/centros alternativos.
Tenga un canal de difusión claro para todos los clientes.
- Desarrolle y pruebe métodos para recuperar y restaurar datos de una copia de seguridad; compruebe periódicamente los datos de una copia de seguridad para verificar su validez.
- Tenga establecidos acuerdos y procedimientos para llevar a cabo operaciones comerciales en instalaciones/centros alternativos.
- Tenga un canal de difusión claro para todos los clientes.

EJERCICIOS

- Organice pequeños ejercicios de simulación con todo el personal o representantes de todos los niveles de personal, incluidos ejecutivos de la organización, personal de RR. PP./comunicaciones y equipos legales y de cumplimiento.
- Identifique, e idealmente participe, en ejercicios de simulación de todo el sector relevantes para su organización.
- Establezca el proceso para garantizar que las lecciones aprendidas de los ejercicios se incorporan y abordan en la estrategia de ciberseguridad de su empresa.

RESPUESTA

- Implemente acciones del plan de respuesta a incidentes para minimizar el impacto en las operaciones empresariales.
- Identifique los sistemas afectados/comprometidos y evalúe los daños.
- Reduzca los daños eliminando (desconectando) los activos afectados.
- Comience a registrar toda la información tan pronto como el equipo sospeche que se ha producido un incidente. Intente conservar pruebas del incidente al desconectar/segregar el activo identificado afectado; por ejemplo, recopilando los registros de configuración del sistema, red y detección de intrusión de los activos afectados.
- Notifique a las partes internas, proveedores externos y autoridades pertinentes, y solicite ayuda si es necesario.
- Inicie las actividades de notificación y asistencia al cliente de acuerdo con las leyes, las normativas y las directrices entre agencias.
- Utilice plataformas de intercambio de amenazas como FS-ISAC o MISP (Malware Information Sharing Platform [Plataforma de intercambio de información sobre malware]) para notificar a la industria sobre la amenaza.
- Documente todos los pasos que se llevaron a cabo durante el incidente para revisarlos más tarde.

RECUPERACIÓN

- Restablezca los activos recuperados a “puntos de recuperación” periódicos si están disponibles y utilice datos de una copia de seguridad para restaurar los sistemas al último estado “bueno” conocido.
- Cree copias de seguridad “limpias” actualizadas de activos restaurados y garantice que todas las copias de seguridad de los activos críticos se almacenen en una ubicación protegida a nivel físico y medioambiental.
- Compruebe y verifique que los sistemas infectados estén completamente restaurados. Confirme que los sistemas afectados funcionan con normalidad.

REVISIÓN

- Lleve a cabo una conversación de “lecciones aprendidas” después de que se produzca el incidente: reúnanse con el personal sénior, asesores de confianza y proveedores de asistencia informática para revisar posibles vulnerabilidades o recomendar nuevos pasos a implementar.
- Si es posible, identifique las vulnerabilidades (ya sea en software, hardware, operaciones empresariales o comportamiento del personal) que causaron el incidente y desarrolle un plan para mitigarlos.
- Confirme que los sistemas afectados funcionan con normalidad.
- Desarrolle un plan de supervisión para detectar incidentes similares o adicionales relacionados con los problemas identificados.
- Comparta lecciones aprendidas e información sobre el incidente en plataformas de intercambio de amenazas como FS-ISAC.
- Integre las lecciones aprendidas en los protocolos de respuesta a incidentes de su organización.