

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 antispymware](#) 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).