Seguridad informática en medios extraíbles

Gabriel Guevara Gutiérrez
Adriana García Vargas

La seguridad de los datos, los propios y los de terceros, es una prioridad para las empresas que los administran. Prever su protección integral y rigurosa es una forma de evitar complicaciones que podrían convertirse en serios problemas legales.

En la práctica empresarial, compartir datos e información es esencial en todos los niveles de la organización: operativo, táctico y estratégico. Para ello, se ocupa, frecuentemente, medios físicos como las memorias Universal Serial Bus (USB), los discos duros externos, las tarjetas de memoria, entre otros. El uso de estos medios trae consigo riesgos de seguridad como el robo de datos, infecciones de archivos por *malware* o incurrir en infracciones por violación de derechos de autor. Por lo anterior, es importante identificar las causas de estos riesgos, así como las medidas para evitarlos o reducir su impacto.



Imagen de Jakub Zerdzicki en Pexels.

Riesgos en el empleo de medios extraíbles

La información es un activo intangible que aporta valor a cada uno de los procesos de la organización, principalmente, para la toma de decisiones. El extravío o pérdida de la información contenida en algún tipo de medio extraíble puede significar pérdida de dinero y tiempo o, en el peor de los casos, que la información disponible sea utilizada por un tercero para hacer aún más daño a la organización.

La información almacenada en los dispositivos extraíbles, de acuerdo con la actividad económica de la empresa, puede incluir datos confidenciales de clientes, estados financieros o planes estratégicos. Por ello, se debe tomar en cuenta que perder, por ejemplo, información de los clientes puede llevar a una empresa a enfrentar conflictos legales por incumplimiento de la regulación de protección de datos amparados en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, y hacerse acreedora a sanciones y multas.

Es común que el personal comparta sus archivos por medio de memorias USB o que las ocupen para transportar archivos de una computadora a otra. No es de extrañar que alguien vea la oportunidad de apropiarse de una USB que no es suya, simplemente porque el diseño le parece atractivo, en verdad la necesita o, en otros casos, las roban con fines ilícitos. Si un dispositivo cae en las manos equivocadas, los datos que contiene pueden ser utilizados de diversas maneras. Una vez que la información es

robada, la empresa podría enfrentar daños a su reputación, legales y financieros. Por ejemplo, si los estados financieros se ven comprometidos, las relaciones comerciales podrían afectarse.

En seguridad, un vector es una fuente de riesgo. En ese sentido, los medios extraíbles son un vector de la propagación de programas o códigos maliciosos (*malware*). El uso indiscriminado de cualquier medio extraíble lo hace la vía perfecta para diseminar *malware* entre computadoras que no tienen un antivirus con búsqueda activa en funcionamiento. El *malware* que puede ser distribuido por medios extraíbles es:

- Virus que están en los archivos y que pueden causar daños como la corrupción de archivos, es decir, la alteración o eliminación de los datos de un archivo informático que puede derivar en la pérdida de más datos o modificar el comportamiento de una computadora.
- *Gusanos* que, si bien no están en los archivos locales de los equipos, sí permiten controlar una computadora en forma remota sin que el usuario lo identifique.
- *Troyanos* que parecen ser un programa legítimo, pero realizan acciones maliciosas como robar información.
- *Rasomware* que cifra, es decir, hace ilegible los archivos de una computadora o una red de éstas. Es común que un externo a la organización exija algún pago para devolver la autonomía de los archivos.
- *Spyware* es un *software* que espía al usuario sin que se entere para acceder a contraseñas, al historial de navegación, entre otros datos.
- *Adware* es un tipo de *software* que muestra anuncios publicitarios que afectan el rendimiento de una computadora
- *Backdoors* es un *software* que permite al atacante entrar a la computadora de forma remota y secreta sin que se entere el usuario.

Hasta ahora, se habló de situaciones en las que un tercero roba un medio extraíble, pero ¿qué sucede cuando alguien del personal de una empresa sustrae medios extraíbles o copia los archivos contenidos en ellas? Principalmente, incurre en infracciones de derechos de autor. Si la información contenida en los archivos es de un tercero que la dejó en resguardo de la organización y se distribuye o se utiliza sin autorización, puede implicar demandas legales o sanciones administrativas.

Las amenazas anteriores son factores que afectan las operaciones diarias de la organización, por lo que es importante reconocerlas y, con ello, establecer un plan que evite o mitigue aquellas que tengan mayor impacto para nuestra organización, como:

- Pérdidas financieras. El proceso de recuperación o reelaboración de la información, así como la reparación de las computadoras afectadas implica un costo que, si bien es adecuado considerarlo en la reserva de contingencia, se debe tener cuidado de salvaguardar los medios extraíbles y su contenido para que el daño no sea mayor a lo esperado.
- Daños a la imagen y reputación de la empresa. Las violaciones de seguridad y la pérdida de datos sensibles pueden dañar gravemente la confianza que los clientes o socios de la empresa.
- Interrupción operativa. Un ataque de *malware* que produzca la pérdida de datos críticos puede paralizar temporalmente las operaciones de la empresa, que impacta en costos, productividad o imagen.

Como se aprecia, los medios extraíbles son portadores de varias *infecciones* que atacan a los equipos de cómputo y vulneran su sistema para extraer información relevante; de ahí que la principal recomendación para evitar una *infección* sea, en todo proceso, dónde se introducen estos dispositivos.



Imagen de cottonbro studio en Pexels.

A partir de prácticas de seguridad adecuadas, es posible utilizar dispositivos extraíbles sin poner en riesgo la información compartida

Buenas prácticas de seguridad

Para reducir riesgos, se recomienda implementar una serie de buenas prácticas en la gestión de medios extraíbles, como el cifrado de datos (Figura 1). Al cifrar la información almacenada, incluso si el dispositivo es robado o perdido, los datos no podrán ser leídos sin la clave de cifrado correspondiente. Hay herramientas de código abierto como VeraCrypt o soluciones comerciales como BitLocker de Microsoft o FileVault de Apple que permiten cifrar dispositivos de almacenamiento.

Otra buena práctica es el diseño de políticas de acceso a los espacios, a los equipos de cómputo y acerca de la introducción de equipo o dispositivos no autorizados a la organización. Debe estar claro para los responsables de la seguridad de la información que no todo el personal requiere el uso de dispositivos que contengan información confidencial. El uso de *software* de gestión de dispositivos es una medida que ayuda a las pequeñas y medianas empresas a monitorear y controlar qué dispositivos son conectados a las computadoras, y qué tipo de datos pueden ser transferidos.

Los antivirus son una herramienta que permite detectar *malware* en forma activa si se configura la opción de escaneo automático de dispositivos externos al momento de conectarlos. Esto significa que se debe emplear un antivirus confiable y mantenerlo actualizado.

Establecer políticas claras para el uso de medios extraíbles dentro de la empresa implica mencionar claramente las reglas sobre el tipo de información que se puede almacenar en ellos. También, se tiene que mencionar cómo deben protegerse y cómo se debe eliminar o reciclar de forma segura.

Realizar auditorías es una buena práctica que toda empresa debe incorporar para evitar riesgos en su información. La revisión sistemática para determinar el grado en que se cumplen los criterios o condiciones de los objetivos definidos ayuda a detectar vulnerabilidades en el uso de medios extraíbles. Con esto, podemos definir planes de acción para reducir o eliminar las brechas de seguridad.

Los medios extraíbles deben almacenarse en lugares seguros como cajones con cerradura o cajas de seguridad. Con esta medida, puede reducirse el riesgo de que se pierdan o sean robados. Otra medida, siempre que sea posible, es considerar el uso de soluciones de almacenamiento en la nube para la transferencia de datos. Si bien esto no elimina por completo los riesgos de seguridad, los servicios en la *nube* confiables suelen tener medidas de seguridad más robustas que los medios extraíbles físicos.

Por último, somos tan fuertes como nuestro eslabón más fuerte; la seguridad es un proceso que implica tratar diversas aristas de una organización. Uno de ellos son los medios extraíbles como las memorias USB o discos duros portátiles. La protección de los medios extraíbles es una responsabilidad para los emprendedores que requiere tomar acciones para evitar la pérdida de datos o el robo de dispositivos; gracias a ello se puede minimizar el impacto negativo en la imagen y las finanzas de la organización.

Referencias

Cámara de Diputados del H. Congreso de la Unión. Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP). https://www.diputados.gob.mx] (https://www.diputados.gob.mx

Mtro. Gabriel Guevara Gutiérrez
Jefe de la Licenciatura en Informática
Facultad de Contaduría y Administración, UNAM
gguevara@fca.unam.mx

Dra. Adriana García Vargas
Centro de Informática
Facultad de Contaduría y Administración, UNAM
agarcia@fca.unam.mx