GUÍA DE CIBERSEGURIDAD

PRÁCTICAS DE LOS EXPERTOS

Por · Claudia Cerezo

La ciberseguridad no puede reducirse a un proceso de uno, dos o tres pasos. Implica una combinación de mejores prácticas y técnicas defensivas de ciberseguridad. Esta guía, dictada por seis expertos, te ayudará a proteger tus datos y los de tus clientes, pero recuerda que la ciberseguridad es un proceso continuo.

La ciberseguridad nunca ha sido un tema que las empresas puedan ignorar. Desde el auge de las puntocom, durante la década de los 90, los ataques cibernéticos se han vuelto más avanzados, peligrosos y generalizados.

En 2020 y 2021, los ataques no solo crecieron en número, sino en impacto, pues los ciberdelincuentes se han aprovechado de la pandemia de muchas formas; desde correos electrónicos maliciosos con información sobre el coronavirus, hasta intentos de fraude y robo de datos cuando escaneamos códigos QR en restaurantes, museos, anuncios y otros lugares públicos. Además, con el aumento del trabajo remoto, los delincuentes tuvieron un acceso más fácil a equipos que no estaban tan protegidos.

Pensando en ayudar a las organizaciones a enfrentar estos retos, aquí presentamos una guía con algunas medidas de seguridad, recomendadas por expertos.

PABLO CUBELA
DIRECTOR DE TI EN BUPA MÉXICO

- No visitar sitios web ilegítimos ni dar clic a enlaces sospechosos. Tampoco abrir, descargar o instalar archivos de dudosa procedencia, para evitar ser víctimas del malware (archivos dañinos que pueden controlar la computadora de la empresa si son abiertos, o enviar archivos confidenciales al atacante) o del phishing (robo de dinero o identidad mediante sitios web o correos electrónicos que fingen ser sitios legítimos, haciendo que se revele información personal, como números de tarjeta de crédito, información bancaria o contraseñas). Como cada vez es más difícil distinguir entre correos electrónicos reales o falsos, es importante leer con atención la dirección del remitente y compararla con las direcciones oficiales, así como identificar errores tipográficos. Ante cualquier duda, reportarla de inmediato con el equipo de Tecnologías de la Información (TI) y eliminarlo de la bandeja de entrada.
- Usar contraseñas fuertes es indispensable. Siempre hay que combinar números, letras mayúsculas, minúsculas y símbolos, y no repetirlos. Tampoco se deben usar contraseñas similares a las de otras cuentas; de esta forma será más difícil conseguirlas.
- Evitar compartir datos personales es fundamental, sobre todo en las redes sociales y en cualquier página web que no sea confiable. Lo recomendable es solo compartir información cuando sea absolutamente indispensable. Además, hay que tener cuidado respecto de con quién se comparte la información en la red, ya sea a través de imágenes o texto.
- Desactivar la tecnología Bluetooth y los puertos USB, porque pueden servir de entrada a software malicioso y como medio para fugas de información.
- No utilizar puntos de acceso Wi-Fi públicos, ya que pueden ser una trampa; comúnmente tienen nombres de establecimientos u organizaciones cercanas para atraer más fácilmente a las víctimas.
- Realizar pruebas de penetración y cerrar de inmediato las brechas o vulnerabilidades identificadas por el equipo de seguridad.
- Implementar herramientas que ayuden a prevenir la fuga de información, identificar rápidamente la presencia de intrusos en la red corporativa, segmentar la red, verificar los accesos, y revisar la configuración y actualización de todos los sistemas constantemente.

JOSÉ JUAN MARROQUÍN
GERENTE DE CIBERSEGURIDAD & REDES ADMINISTRADAS EN ALESTRA

- Realizar inversiones acordes al presupuesto de la empresa para cuidarse de las amenazas informáticas.
- Construir una estrategia de ciberseguridad de mano de socios tecnológicos y consultores que ayuden en el desarrollo de planes y programas para fortalecer al negocio.
- Concientizar a los colaboradores sobre el valor de la información que manejan. Esta práctica debe ir desde el director general hasta la persona con menor responsabilidad. Toda la organización debe contar con una guía en la que se destaquen los puntos importantes a cuidar cuando se utilice información a través de los distintos equipos, incluidos los móviles. La cultura o concientización de los colaboradores en materia de ciberseguridad es indispensable para reducir la probabilidad de que, por desconocimiento u omisión, la organización sea víctima de un ciberataque.
- Instrumentar controles de hardware y software debidamente licenciado, actualizar los sistemas operativos de todos los dispositivos empresariales (las actualizaciones corrigen agujeros de seguridad), implementar antivirus de siguiente generación en todos los equipos personales y empresariales conectados a la red de la compañía, y sistemas de doble factor de autenticación (la doble identificación puede ser la contraseña habitual, más un código de seguridad que se le envía al usuario mediante otro medio para así confirmar que realmente es el propietario de la cuenta) y contar con un constante respaldo o copias de seguridad de la información en entornos físicos o virtuales.
- Implementar plataformas de seguridad de nueva generación, como un EDR (Endpoint Detection and Response) con inteligencia artificial y machine learning, para aprender de las nuevas amenazas y, de esta forma, contener ataques. También puede considerarse un sistema NDR (Network Detection and Response), el cual proporciona una visión completa de la posible superficie de ataque y las interacciones entre todos los dispositivos de la red.

JUAN CARLOS ZEVALLOS
CYBERSECURITY MANAGER EN IBM MÉXICO

- Sensibilizar a los usuarios; esa es la primera línea de defensa. De acuerdo con el Índice de Inteligencia de Amenazas de IBM X-Force 2022, más del 90% de los ciberataques son posibles, en mayor o menor medida, por errores humanos. Por ello, a pesar de los avances tecnológicos para minimizar las amenazas, la primera línea de defensa es la concientización de los usuarios y las buenas prácticas. Es importante trabajar en la falta de precaución de los colaboradores, la cual conlleva a acciones como la configuración inadecuada de gestión de identidades y accesos en entornos de nube, y a la fuga y pérdida involuntaria de datos.
- Redefinir la base sobre la que se construyen las alianzas. Para innovar mientras las empresas se mantienen seguras, los líderes deben verificar que los estándares de seguridad se extiendan desde sus programas internos hasta sus relaciones con proveedores y terceros. Asegurar la cadena de suministro requiere que los equipos de seguridad implementen los procedimientos adecuados en la gestión de riesgos de cada nuevo socio y tengan buena visibilidad de lo que sucede con los datos cuando se accede a ellos.
- Desconfiar. Al operar con la idea de que un entorno tecnológico ya está expuesto y que un adversario ha aprovechado esa exposición para comprometer una red, la empresa está más preparada para examinar sus relaciones de confianza. Si se trabaja con la gestión del riesgo en mente, esas relaciones de confianza podrán limitarse en diversos grados, ya sea con usuarios, clientes o aplicaciones internas y de terceros.
- Optar por nubes especializadas. Las industrias muy reguladas, como servicios financieros, enfrentan una presión cada vez mayor para transformarse digitalmente, mientras atienden los desafíos regulatorios, de cumplimiento y seguridad. Ante este panorama, los bancos, neobancos y fintechs podrían apoyarse en nubes y plataformas especializadas, con controles de seguridad específicos

de la industria incorporados, para soportar la innovación y la funcionalidad con estrictos protocolos de cumplimiento.

- Implementar capacidades de seguridad mejoradas dentro de la organización a través de sus ecosistemas, antes de que las organizaciones sigan ampliando sus operaciones en la nube. Esto requiere la colaboración de los participantes de la industria y proveedores de la nube. Además, los modelos aumentados de IA, cuando hay datos compartidos entre instituciones, refuerzan el sistema inmunológico de la industria, revelando patrones criminales antes que sean virales en ecosistemas extendidos.
- Automatizar la respuesta a incidentes, para externalizar a las máquinas tareas que podrían llevarle horas a un analista o equipo humano, y para identificar mecanismos que mejoren los flujos de trabajo.
- Instrumentar soluciones de detección y respuesta ampliada (XDR), para optimizar la detección, investigación, respuesta y búsqueda de amenazas en tiempo real. Cuando se combinan varias soluciones diferentes en una solución de detección y respuesta ampliada, las organizaciones tienen una ventaja significativa al momento de identificar y erradicar a los atacantes de una red antes de que puedan llegar a la fase final.

ROMAN BAUDRIT
VICEPRESIDENTE DE VENTAS PARA LATINOAMÉRICA DEL ÁREA DE PROTECCIÓN DE DATOS EN THALES CLOUD PROTECTION AND LICENSING

- Identificar cuáles son los datos más críticos para el negocio y dónde están almacenados. Si no se sabe dónde se encuentra la información que en caso de ser sustraída o secuestrada generaría daño a la empresa, entonces la estrategia de seguridad no tiene bases firmes. Revisar los procesos de negocio para poder seguir el rastro de los datos es lo que debe definir las prioridades de protección. Es recomendable utilizar herramientas de descubrimiento de datos para saber cuánta información se debe proteger, dónde se encuentra, quién la utiliza y cuál es la mejor manera de protegerla. La información es el instrumento de cambio en el mercado negro. Por ello, la estrategia de ciberseguridad tiene que estar centrada en los datos.
- Cifrar los datos. Si no cifras tus datos, alguien lo hará: un tercero cifrará los datos de tu empresa para coaccionarte y hacer que pagues por recuperarlos. Eso si tienes suerte. Las consecuencias de no pagar el rescate es que tus datos serán destruidos, vendidos o expuestos. Lamentablemente, incluso si pagas la recompensa, no tienes la certeza de que no te pedirán más dinero o de que, en efecto, te devolverán la información en su estado original. ¿No habría sido más fácil que hubieras cifrado tus datos antes que los atacantes? Información cifrada es información protegida.

- Implementar un modelo de confianza Zero Trust (confianza cero). ¿Sabías que toma minutos –por no decir segundos– romper una contraseña de seis dígitos, y algunas horas para credenciales complejas de ocho dígitos? ¿Sabías que muchas empresas siguen basando su seguridad en modelos de contraseñas de este tipo?

Cuando salimos en la noche de nuestra casa o empresa, vamos con cautela; incrementamos nuestro nivel de alerta, cerramos las puertas y ventanas de nuestro auto. ¿Por qué? Porque afuera nos sentimos inseguros o menos seguros. De la misma forma en que estamos expuestos a riegos físicos, las personas, sistemas e infraestructuras están expuestas a riesgos cibernéticos, a toda hora, todos los días.

En una estrategia Zero Trust, las personas deben justificar su derecho de acceso a los activos digitales de la empresa. De la misma forma en que existen áreas restringidas en las fábricas y oficinas, así debe haber restricciones en las plataformas tecnológicas. Zero Trust es limitar el acceso, pedir doble factor de autenticación (de la misma forma que en la entrada de los edificios se nos pide un código de acceso y un gafete) para que los usuarios ingresen a los sistemas, y proteger la información para que los daños sean mínimos en caso de que algún usuario ponga en riesgo los sistemas. No desconfiemos de las personas, pero aceptemos que los empleados no son expertos en ciberseguridad. Limitando y controlando el acceso a los datos los protegemos a ellos y a la empresa.

SOL GONZÁLEZ
INVESTIGADORA DE SEGURIDAD INFORMÁTICA EN ESET

- Instrumentar mejores prácticas de seguridad en la nube, para mitigar los riesgos, pues con el uso de software como servicio (SaaS) los datos se ponen en manos de un proveedor externo y fuera del control de TI. Estas son algunas de las mejores prácticas de seguridad en la nube:

1. Clasificar los datos corporativos que fluyen a través de la nube y establecer los controles adecuados.
2. Comprender el modelo de responsabilidad compartida, en el cual las organizaciones comparten la responsabilidad de la seguridad con sus proveedores de servicios en nube.
3. Usar cifrado sólido para los datos que residen en la nube, tanto en reposo (almacenados) como en tránsito (cuando recorren la red).
4. Establecer contraseñas seguras mediante el uso de un administrador de contraseñas
5. Robustecer los inicios de sesión mediante el doble factor de autenticación para todas las cuentas. De esta manera, no se dependerá de una sola contraseña, sino que se necesitará otro código de acceso que puede recibirse en el smartphone, por ejemplo.
6. Restringir el acceso a cuentas confidenciales a través de una política que tenga en cuenta el principio del menor privilegio; es decir, otorgar los permisos necesarios y suficientes a un usuario para desempeñar sus actividades por un tiempo limitado y con el mínimo de derechos necesarios para sus tareas.
7. Considerar la posibilidad de utilizar un agente de seguridad de acceso a la nube para coordinar la autenticación y el cifrado. Estos agentes son soluciones de software o hardware encargados de proteger los datos y la identidad, y prevenir amenazas en la nube.
8. Configurar las cuentas SaaS correctamente, según los riesgos (configuración de seguridad y privacidad).
9. Usar una herramienta de gestión de la postura de seguridad en la nube (CSPM) para verificar, de forma automática y continua, las configuraciones erróneas que pueden provocar filtraciones de datos.
10. Capacitar a los empleados en temas de seguridad, de manera regular (por ejemplo: cómo evitar el phishing).
11. Aplicar parches, basados en el riesgo, en todos los servidores y software en la nube.
12. Considerar el enfoque Zero Trust para reducir el impacto de las brechas en la nube.

ERIK MORENO
DIRECTOR DE CIBERSEGURIDAD EN MINSAIT

- Establecer una estrategia de ciberseguridad basada en riesgos y su impacto en el negocio y no en componentes tecnológicos. Muchas empresas desarrollan estrategias de protección basándose en las tecnologías o fabricantes de moda, sin definir cuáles son los activos críticos de información que deben proteger. Una vez identificados estos activos, los riesgos deben cuantificarse y valorizarse. Recuerda que la tecnología no es la directriz de la estrategia de ciberseguridad, sino un habilitador.
- Diseñar estrategias de seguridad de fronteras abiertas, que contemplen a clientes, proveedores, aplicaciones interconectadas, enlaces de comunicaciones, etcétera. Con el aumento del trabajo remoto, la ciberseguridad escapó del espacio físico empresarial tradicional y trascendió fronteras: ahora hay que proteger los equipos que están en los hogares de los colaboradores y contemplar, también, a los proveedores de servicio. Hoy, las amenazas ya no están enfocadas en atacar el núcleo de la organización de manera directa, sino a través de sus proveedores de servicio.
- Los delincuentes están aprovechando la falta de madurez, controles de seguridad y cumplimiento normativo de los pequeños proveedores de servicio, para vulnerarlos y a través de ellos llegar a las organizaciones.
- Considerar que las nuevas tecnologías (IA, ambientes de nube, virtualización de sistemas, etcétera) conllevan nuevos riesgos, y que la información de los clientes es uno de los activos más valiosos de cualquier organización.
- Contemplar las áreas operativas en la estrategia de seguridad, sobre todo en empresas industriales (manufactura, energía, alimentación, armadoras, etcétera), porque mucha de la información que proviene de las fábricas es crítica para la toma de decisiones. Al juntar el mundo de tecnología operativa con el mundo de tecnologías de la información se abre un nuevo panorama de riesgos.

La ciberseguridad no es un lujo; es una prioridad. Los ciberataques pueden ocurrir a cualquier empresa, de cualquier vertical y de cualquier tamaño. Pueden interrumpir cualquier proceso de negocio, pero normalmente pasan a segundo término. Tenemos guardias de seguridad para cuidar el edificio y al personal, pero no guardias para nuestros datos. Tenemos cajas fuertes para los documentos físicos, pero no para la información digital. Tenemos centros de monitoreo para nuestros pasillos, pero no para saber qué ocurre en los servidores donde reside información crucial.

Es imperativo estar preparado y armado. Las empresas deben dedicar tiempo y recursos a proteger sus computadoras, servidores, redes y software, y deben mantenerse al día con la tecnología emergente. Manejar los datos con cuidado hace que tu negocio sea más confiable y transparente, y que tus clientes sean más leales. **AN**