THOMSON REUTERS
CHECKPOINT

La importancia de la ciberseguridad en tiempos de pandemia

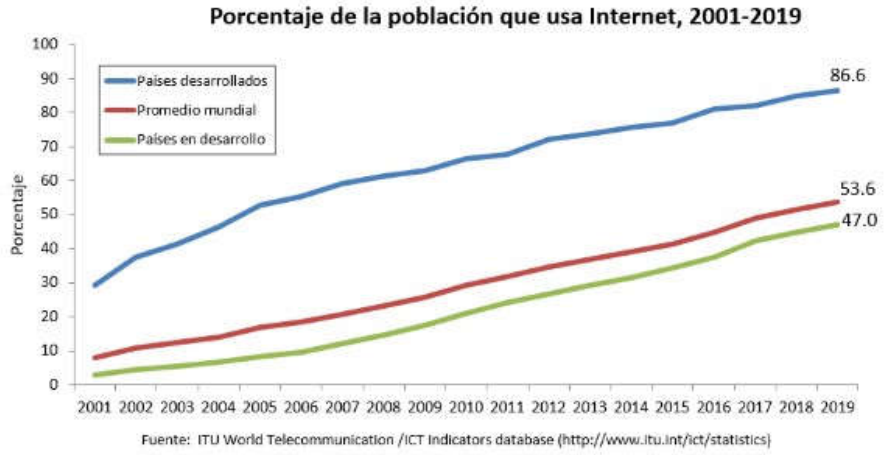
Nicolao, Ricardo Gabriel

Abstract: En la actualidad, el mundo está atravesando una pandemia sin precedentes, forzando a las organizaciones a una aceleración de la transformación digital y a una profundización del denominado home office, por lo que la ciberseguridad está en el centro de la escena más que en ningún otro momento de la historia.

I. Introducción

Desde que fueron creadas, las Tecnologías de la Información y la Comunicación (TIC) no han parado de crecer, produciendo una profunda y positiva transformación en la sociedad.

De acuerdo con estudios de la Unión Internacional de Telecomunicaciones (ITU, por sus siglas en inglés), organismo dependiente de la Organización de las Naciones Unidas, el 8,0% de la población mundial usaba Internet en 2001. En la actualidad, los habitantes del mundo que utilizan la red de redes ya superan el 53,6%, según puede verse en el siguiente gráfico.



Aspectos como la globalización y el abaratamiento de la tecnología, generaron una marcada masificación del uso de computadoras personales, junto con un crecimiento exponencial de la generación de información. Pero toda esa evolución también trajo dificultades, tales como sobrecarga de datos, capacitación del personal, reformas legales y, especialmente, vulnerabilidades en la seguridad de la información.

Actualmente, el mundo está atravesando una pandemia sin precedentes, forzando a las organizaciones a una aceleración de la transformación digital y a una profundización del denominado Home Office, Work From Home, Teletrabajo o, simplemente, trabajar desde casa. Esto hace que la ciberseguridad esté en el centro de la escena más que en ningún otro momento de la historia.

II. Qué es la ciberseguridad

De acuerdo con la Asociación de Auditoría y Control de Sistemas de Información (ISACA, por sus siglas en inglés), se puede definir a la ciberseguridad como "la protección de los activos de información, abordando las amenazas a la información procesada, almacenada y transportada por sistemas de información interconectados" (1). En otras palabras, se trata de proteger el ciberespacio, es decir, al ámbito de información que se encuentra implementado dentro de dispositivos informáticos (2) y/o redes digitales, de los ciberataques, asegurando la gestión de la información en cuanto a confidencialidad, integridad y disponibilidad.

¿Quiénes realizan los ciberataques? Los denominados hackers, es decir, personas con malas intenciones (3) expertas en el manejo de dispositivos informáticos que tienen diversos fines, entre los cuales se encuentran:

- Fama: se trata de personas que se esmeran por tener reconocimiento y popularidad.

- Publicidad: también llamado spyware, que consiste en instalar un programa que recopila y envía información del usuario a una entidad externa sin su consentimiento para utilizarlos con objetivos publicitarios, entre otros.

- Zombies: denominados botnets o robots informáticos, que son programados para ejecutarse de forma autónoma y remota para, por ejemplo, ralentizar el dispositivo.

- Robar información (keylogger): programas que registran las teclas pausadas, incluyendo contraseñas, datos de inicio de sesión e información confidencial.

- Secuestrar información (ransomware): programa con capacidad para bloquear un dispositivo completo o encriptar archivos, impidiendo su acceso.

En todos los casos existen tres condiciones fundamentales:

1) El desarrollo de un programa malicioso, llamado malware.

2) La decisión de utilizar el malware en un dispositivo informático o red digital (4).

3) La presencia de una vulnerabilidad de seguridad en el dispositivo o red.

En el presente trabajo, el objetivo se focalizará en el tercer punto.

III. Motivos

Existe una gran cantidad de motivos (y cada vez son más) que propician la realización de un ciberataque y/o la necesidad de una política de ciberseguridad:

- Relegación de la inversión en seguridad informática: si bien en los últimos años aumentó su relevancia, tradicionalmente la seguridad informática no era un factor preponderante en las organizaciones, las cuales destinaban sus inversiones en otros temas que consideraban más prioritarios.

- Gran cantidad de proveedores distintos: la creciente complejidad de las organizaciones (5) generó necesidades que fueron cubriéndose gradualmente, aunque no siempre con una adecuada planificación. Por este motivo, actualmente suelen coexistir softwares de distintos proveedores, dificultando la tarea de mantener bajo control no solo la seguridad informática de cada uno de ellos por separado, sino también sus interfaces, de corresponder.

- Multiconectividad de redes: en una organización coexisten diferentes tipos de redes (LAN, VLAN, WAN, VPN, WIFI, Internet, nube, etc.). Esto genera que para cada una de las redes se deban tomar distintas medidas de seguridad, aumentando el riesgo de vulnerabilidades.

- Multiconectividad de dispositivos: en la actualidad ya no se utiliza solo la computadora para trabajar. Es común ver los e-mails desde un teléfono celular, realizar una llamada usando la webcam, grabar información en un pendrive o leer un informe en una tablet. Al igual que el punto anterior, cuantos más dispositivos se utilicen, mayor será el riesgo a considerar. Adicionalmente, el surgimiento de la IoT o "Internet de las cosas" acentuará este punto.

- Ningún sistema es 100% confiable: esto se debe a que son desarrollados por seres humanos, y debido a que los seres humanos no son infalibles, es de esperar que los sistemas creados por seres humanos tampoco lo sean, requiriendo de medidas de monitoreo periódicas y de una política de seguridad informática.

- Importantes intereses económicos: en los últimos años han surgido grandes ejemplos de ciberataques que pusieron en jaque a empresas de primera línea mundial. El último gran malware mundialmente conocido fue Wannacry en 2017, siendo un ransomware que generó pérdidas multimillonarias. El beneficio obtenido es un aliciente más al momento de considerar el riesgo asociado.

- Propagación de criptomonedas: la relación que tienen las criptomonedas con los ciberataques es simple: al tratarse de acciones ilegales, los hackers necesitan obtener ingresos fuera del circuito bancario tradicional. De tal manera, la popularización de las criptomonedas contribuye a la probabilidad de recibir un ciberataque.

- La reglamentación siempre "corre de atrás": en algunas ocasiones, las sanciones impuestas por los gobiernos de cada país llegan cuando el daño ya está hecho; en otras, se dificulta jurídicamente por tratarse de un delito trasnacional. Esto deja a las organizaciones en una situación de vulnerabilidad, dependiendo de su personal para enfrentar los posibles ciberataques.

- Competencias del personal: ya sea por la falta de nivel técnico de los encargados en llevar a cabo las políticas de ciberseguridad o porque la complejidad actual requiere de una evidente inversión en equipos interdisciplinarios, muchas organizaciones se encuentran expuestas ante potenciales ciberdelincuentes.

- La importancia de la información: en la actualidad, el impacto de perder información es significativamente mayor que en el pasado, debido a la automatización de los procesos y la

sistematización del conocimiento adquirido. Pensar en trabajar un día sin poder acceder a la información almacenada es casi una utopía.

- Trilogía costo, tiempo y calidad: son las tres principales variables presentes en todo proyecto de software. La cada vez mayor presión que ejercen las organizaciones sobre la reducción de tiempos y/o costos genera ocasionalmente disminuciones en la calidad, necesitando un esfuerzo adicional por cubrir esa dificultad, o bien la atención suficiente para descargar actualizaciones de software.

- "Mientras todo funcione bien...": el principio de la inercia es una tentación para no darle la suficiente importancia a la seguridad informática hasta que es demasiado tarde. Es quizás uno de los principales motivos por el cual un ciberataque genera tanto daño en muchas organizaciones. En consecuencia, resulta ineludible desterrarlo como tal y tomar cartas en el asunto.

Si bien la necesidad de optimizar la ciberseguridad es atemporal, ocasionalmente aparecen momentos en los cuales la probabilidad de sufrir daños se incrementa. El escenario actual describe uno de esos momentos, requiriendo de una mayor atención.

Haciendo una analogía, el ciclo de vida del COVID-19 no es muy distinto al del malware: inicia en un lugar específico, se expande por todo el mundo e infecta aprovechando vulnerabilidades. Entonces, el desafío consiste en generar los anticuerpos necesarios para que el daño sea el menor posible.

IV. Empezar por las personas

Si en un día normal de trabajo las personas son un factor fundamental para mantener a salvo la información de una gran organización o de una simple computadora personal, en tiempos de pandemia su importancia es aún más preponderante, ya sea por las dificultades para trasladarse a una oficina, la utilización de un dispositivo tanto para fines laborales como personales, o el mayor nivel de actividad de ciberdelincuentes, conocedores de que es una situación propicia para actuar.

Incluso con los controles tecnológicos más estrictos, las personas deben ser criteriosas. El trabajo desde la casa puede generar cambios en el comportamiento, en especial si es la primera vez que se mezcla un lugar de descanso con uno laboral. Más aún si se acentúa por mayores niveles de estrés, producto de la incertidumbre por la pandemia que estamos atravesando. Por ejemplo, siempre existe la posibilidad de leer un e-mail personal y hacer un click en un enlace que lleve a un sitio malicioso.

Ninguna inversión en tecnología será suficiente sin la colaboración de las personas. Por eso, la clave es convertir a cada persona en un "firewall humano", respecto del cual:

- Aumente la conciencia de la ciberseguridad, difundiendo o incentivando la lectura de artículos relacionados con la temática.

- Reciba comunicaciones simples pero eficaces para comprender los riesgos (no ahogar con mensajes inútiles).

- No descuide la seguridad física, en especial si poseen información sensible (dejar la computadora con la pantalla bloqueada, cerrar sesión en caso de no usarla, etc.).

- Se concentre en qué debe hacer en lugar de qué no debe hacer (las acciones punitivas no generan motivación).

- Se diferencien los usuarios de alto riesgo de los que no lo son (p. ej., los que utilizan información confidencial).

V. Continuar por los procesos

Indudablemente los procesos de una organización se ven afectados en tiempos de pandemia, por causas como una menor interacción física entre las personas, información que debe ser compartida por vía remota, documentación física que se dificulta firmar, entre otras.

Nuevamente, si la pandemia provoca un trabajo desde la casa sin antecedentes, puede ocurrir, p. ej., que una mala configuración del VPN impida realizar las tareas con normalidad, o compartir información confidencial por vías no seguras. En esos casos se debe prestar atención a:

- Evaluar el impacto en los controles internos (reestimación de riesgos de auditoría de sistemas, identificación de nuevos controles clave, etc.). Puede ocurrir que se deban diseñar controles compensatorios, como, p. ej., la revisión de registros en fechas u horarios inusuales.

- Ampliar la política de seguridad informática debido, por un lado, al mayor riesgo de que haya vulnerabilidades, y por otro, a la proliferación de ciberataques.

- Tener el soporte adecuado en cuanto a mesas de ayuda de sistemas, o bien tenerlo organizado (p. ej., estableciendo referentes por grupos).

- Extender los controles a procesos externos a la organización (principalmente incluir evaluaciones a proveedores y clientes, ya que también pueden manejar información sensible).

- Testear aspectos como la recuperación ante desastres (p. ej., una caída del servidor), validación de conexiones remotas, planes de respuesta ante incidentes, etcétera.

- Saber qué hacer cuando ocurre un incidente en un dispositivo remoto (es decir, tener un protocolo bien establecido).

- Actividades que impliquen distribución y destrucción de documentos físicos (redactar normas, listar los documentos distribuidos con información sensible, monitorearlos periódicamente, asegurarse que su destrucción sea completa).

VI. Lograr una buena autenticación

La autenticación es el proceso de confirmar que algo es lo que dice ser. En informática se utiliza para evitar accesos indebidos al sistema, previa identificación por parte del usuario, por parte de personas no autorizadas.

Como se puede apreciar, la autenticación está directamente relacionada con la ciberseguridad. En conexiones remotas, la autenticación tiene una importancia aún mayor que dentro de una oficina. Más aún si la práctica de esta modalidad tiene escasos o nulos antecedentes.

Existen básicamente cuatro maneras de autenticación, que se detallan a continuación:

Lo que uno sabe	**El ejemplo más conocido es la contraseña. Previa identificación del usuario, el sistema pide que escriba la contraseña y luego verifica que haya una asociación. De no existir tal asociación, el sistema rechaza el acceso. También hay alternativas para reforzar la autenticación, como por ejemplo haciendo caducar la contraseña cada determinado tiempo.**
Lo que uno tiene	Una tarjeta con chip, una tarjeta con coordenadas, un token, son todos ejemplos aplicables. Al igual que en el punto anterior, puede ser cambiado periódicamente.
Lo que uno es	En este caso se hace referencia a la autenticación biométrica, que puede darse por la huella digital, el reconocimiento del iris, reconocimiento facial, etc. En un comienzo se pensaba que era un método infalible. Sin embargo, en la actualidad eso está en discusión.
Lo que uno sabe hacer	Entre los más difundidos, es el método más reciente de autenticación. Incluye a los movimientos del mouse, hábitos de navegación y escritura a mano.

Para evitar accesos indebidos, lo recomendable es utilizar al menos dos de las formas descriptas en simultáneo, aunque esto generalmente no ocurre. Es decisión de cada organización elegir el nivel de autenticación que requerirá en cada caso, asumiendo los riesgos asociados.

Vale aclarar que se están comenzado a implementar otras alternativas. Tal es el caso de la ubicación geográfica, aprovechando la tecnología GPS, mediante la cual se podrá distinguir entre un usuario habilitado y un ciberdelincuente ubicado en cualquier otra parte del mundo.

VII. No olvidarse de las buenas prácticas

Las buenas prácticas siempre son bienvenidas, y deben serlo más en los tiempos actuales. La ciberseguridad no se encuentra ajeno a ello, y por tal motivo resulta necesario mencionar qué medidas contribuyen a un mejor ambiente de seguridad informática, a fin de minimizar riesgos.

Ejemplos de buenas prácticas son:

- Tener cuidado con lo que se descarga: tratándose de una acción conjunta a realizar entre el usuario, quien debe usar el dispositivo informático con responsabilidad, y el soporte tecnológico, que debe tomar medidas de restricción de acceso a sitios web de dudosa legitimidad.

- Tener softwares y elementos de protección: incluyendo antivirus, firewalls, proxys, contraseñas adecuadas, cifrados de información, etcétera.

- Mantener los softwares actualizados: particularmente este es un punto tan indiscutible como frecuentemente no cumplido. Es imprescindible instalar las actualizaciones en el momento que se publican y, de ser posible, tener programas de detección de las actualizaciones que vayan surgiendo.

- Hacer backup: la diferencia entre hacer un backup y no hacerlo equivale a perder toda la información almacenada o poder recuperarla. A veces no basta con tener un solo backup, y existen varias alternativas (completo, diferencial, incremental, espejo). La naturaleza y la frecuencia del backup dependerá del tipo de organización y de sus procesos. Es fundamental que el backup esté físicamente en un lugar distinto al de la información (p. ej., en el servidor ubicado en las oficinas de una empresa, en una nube, etc.).

- Incluir conceptos de seguridad física: en adición a lo mencionado con anterioridad, se incluye la prevención ante desastres naturales (inundaciones, incendios), y las alteraciones del entorno (cortocircuitos, humedad).

- Establecer la seguridad lógica por capas: relacionado con las redes, cuantas más capas haya, más difícil será acceder al dispositivo del usuario. P. ej., mediante la utilización de protocolos de red, switches, routers y firewalls, en sus distintas clases, o incluso utilizando la encriptación de mensajes (respecto de la cual hay varios métodos).

- Revisar redes, sistemas y plataformas periódicamente: debe establecerse un procedimiento de rutina periódico para asegurarse de que todo funcione correctamente.

- Establecer un reporte obligatorio de incidentes: si bien se mencionó anteriormente un protocolo para incidentes en dispositivos con conexión remota, no todas las organizaciones poseen actualmente un reporte.

VIII. Otras consideraciones

- Garantizar capacidad de trasmisión y almacenamiento: en las circunstancias presentes donde el trabajo desde casa es mayor al habitual, las organizaciones deben realizar un esfuerzo para garantizar que la capacidad de transmisión de datos sea suficiente, al igual que la capacidad de almacenamiento en red. En caso contrario, se corre el riesgo de tener pérdidas de conexión o del trabajo realizado por acceso remoto, entre otros ejemplos.

- Los servicios remotos también tienen riesgos: los servicios en la nube (como IaaS, SaaS, PaaS), las plataformas de comunicación (como Skype, Hangouts, Zoom), las plataformas de almacenamiento en la nube (como Google Drive, Onedrive, Dropbox) y cualquier otro servicio remoto están expuestos a riesgos. Una plataforma de almacenamiento en la nube puede no tener ningún tipo de responsabilidad en caso de pérdida de información. Una plataforma de comunicación puede permitir el acceso a usuarios no autorizados. Por tal motivo, también en estos casos es necesario analizar los riesgos y tomar medidas, de corresponder.

- No descuidar la gestión integral del riesgo: si bien es muy importante prevenir el impacto de los cambios en la modalidad de trabajo que está generando la pandemia respecto a la seguridad de los sistemas informáticos, pueden ocurrir problemas en otros ámbitos, como por ejemplo cuestiones relacionadas con fraude, accidentes de trabajo, etcétera.

- Cada organización tiene sus propias particularidades: es posible que ningún artículo pueda prever la totalidad de los elementos a tener en cuenta, debido a que la ciberseguridad se encuentra en evolución permanente. Sin embargo, sí es posible trabajar en una cultura organizacional que acompañe el concepto de "qué podría fallar", a fin de evitar que ocurra.

IX. Conclusiones

La innovación tecnológica ha permitido a la sociedad mayor desarrollo y bienestar. Sin embargo, en él, debe se encuentran cuestiones tan importantes como la ciberseguridad, cuyas deficiencias generaron varios dolores de cabezas a organizaciones en el mundo entero.

La ciberseguridad en tiempos de pandemia ha recobrado valor como práctica que debe ser habitual en las organizaciones, incluyendo a las personas físicas, y bajo la amenaza de sufrir serios problemas, tanto en los grandes flujos de información presentes en los procesos informáticos como en la información almacenada en los diferentes dispositivos.

Si bien en la actualidad es imposible obtener una seguridad absoluta de los procesos informáticos y nadie está exento de sufrir vulnerabilidades, es posible tomar medidas preventivas que reduzcan tanto la probabilidad como el impacto de recibir un ciberataque.

Aún hoy no todos consideran a la ciberseguridad como un factor crítico. Sin embargo, la evolución constante de la tecnología genera cada vez más la necesidad de tomar las erogaciones en ciberseguridad

como una inversión en lugar de un gasto.

(1) ISACA®, "Glossary of Terms - Spanish", 2015, 3ª ed.

(2) Principalmente computadoras, pero también aplica a teléfonos celulares, tablets, etcétera.

(3) No todos los hackers tienen malas intenciones: la clasificación general se compone de los "White Hat" (Sombrero Blanco), que trabajan con ética en pos de la protección de los sistemas, los "Black Hat" (Sombrero Negro), cuyo rol es hacer daño, y los "Grey Hat" (Sombrero Gris), que usualmente demuestran sus conocimientos informáticos a organizaciones para que luego los contraten.

(4) P. ej., el sistema de almacenamiento en la nube o cloud computing.

(5) El concepto de organizaciones se utiliza en forma genérica, aplicando tanto a empresas multinacionales como a personas físicas.