Publicado en México el 27/02/2023

# [Lecciones tecnológicas que ha dejado la pandemia en México](http://www.notasdeprensa.es)

## DigiCert y Certsuperior hacen una reflexión sobre las lecciones aprendidas durante la pandemia en ciberseguridad en México

 Hace ya más de 2 años que el mundo convive con un virus que ha cambiado la historia de la humanidad y, en consecuencia, de la tecnología. México ha sido una de las naciones que más ha tenido una tendencia al incremento en ciberataques, lo cual indica la necesidad de impulsar estrategias de ciberseguridad y generar estrategias y/o políticas empresariales para prevenir ser vulnerados. Según recientes datos de IDC México tiene el primer lugar con 85 mil millones de intentos de ciberataque en el primer semestre de 2022, lo que representa un aumento del 40% en cifras anuales. Datos generados por un estudio publicado por la Asociación Mexicana de Ciberseguridad IMECI, mientras que de acuerdo con el estudio realizado por IDC: Worldwide Security Governance 2022, los ingresos mundiales en seguridad para gobierno, riesgo y cumplimiento se incrementarán en un 35% para el año 2026 comparado con 2021. De lo anterior, América Latina crecerá un 66% en cuanto a ingresos de seguridad en 2026 tomando como base los $95M USD de ingresos de 2021. Ante este panorama DigiCert y Certsuperior hacen una reflexión sobre las lecciones aprendidas durante la pandemia  en la ciberseguridad: 1. La ciberseguridad es más importante que nuncaLos ataques exitosos en todo el mundo ya han generado pérdidas globales estimadas entre 1 billón de dólares estadounidenses en 2020 y 6 billones de dólares estadounidenses en 2021, informa el Unión Internacional de Telecomunicaciones. La necesidad de un ciberespacio seguro ha cobrado mucha importancia dada la creciente dependencia que las personas y empresas tienen de Internet. Instituciones que ya han sido víctimas de delincuentes y aquellas que temen sumar a esta estadística buscan estar prevenidas, adquiriendo más servicios de seguridad y compartiendo información. 2. La seguridad del trabajo remoto es esencialMillones de personas en todo el mundo han comenzado a trabajar desde casa en lugar de ir a las oficinas y otros lugares de trabajo durante la pandemia. La pandemia ha demostrado que este tipo de trabajo no reduce la productividad y ha provocado que muchas empresas abandonen su resistencia a adoptarlo. Si bien trabajar desde casa tiene sus méritos, como costos más bajos para las empresas, este ascenso meteórico ha generado algunos problemas de seguridad de TI preocupantes, y las empresas han aprendido hasta ahora: Transición a la nube. Desde la pandemia, se prefieren las soluciones de acceso remoto y las organizaciones están trasladando gradualmente los procesos comerciales críticos a la nube. Sin embargo, aumentar la confianza en la nube y desarrollar la agilidad de la nube podría crear más vulnerabilidades si no se asegura adecuadamente. Microsoft descubrió que el 39% de las empresas priorizan las inversiones en seguridad en la nube sobre la seguridad de los datos y la información o incluso la seguridad de la red. PKI puede ayudar a proteger la nube y proporcionar autenticación sólida e integridad operativa a escala.   Phishing por correo electrónico. El phishing por correo electrónico durante la pandemia se disparó. Hay una mayor prioridad para capacitar a los trabajadores y prepararlos para reconocer y saber cómo lidiar con las amenazas desde la pandemia y desarrollar las mejores prácticas para el acceso seguro al correo electrónico.   Varios dispositivos remotos. Los dispositivos móviles necesitan su propia protección de seguridad única. Pero al 52 % de las organizaciones les resulta difícil proteger los dispositivos móviles de los problemas de ciberseguridad. Un primer paso crítico para resolver esto es implementar un política de gestión de dispositivos móviles (MDM).   No hay ciberseguridad en la oficina. La empresa es más vulnerable cuando su personal no puede utilizar las medidas de seguridad informática de la oficina, como los cortafuegos. Afortunadamente, con herramientas como Enterprise PKI Manager de DigiCert, puede aumentar la seguridad y proporcionar a los trabajadores remotos acceso VPN seguro.   Protección de contraseña. Los empleados deben recibir capacitación sobre las mejores prácticas de política de contraseñas, y su organización debe implementar la autenticación de múltiples factores. Además, con el personal que trabaja desde casa, pueden verse tentados a compartir contraseñas de trabajo con amigos o familiares para ayudarlos con ciertas tareas laborales. Obviamente, este es un problema de seguridad y debe abordarse con la capacitación adecuada para todo el personal. 3. Los ataques de ingeniería social ahora son mas complejosLa ingeniería social es un vector de ataque principal para los piratas informáticos. Los actores de amenazas aprovecharon mucho las pruebas gratuitas de COVID-19 en los últimos dos años. Los estafadores han utilizado la ingeniería social para engañar a los usuarios para que proporcionen una dirección postal, un número de teléfono y un número de tarjeta de crédito con la promesa de cobrar 25 centavos para verificar su información y calificar para una oferta de prueba gratuita de COVID-19. Ofreciendo tecnologías de vanguardia falsas y "aprobadas por el gobierno" para luchar contra el COVID y tomar la temperatura de los usuarios engañados cercanos para que descarguen aplicaciones maliciosas en sus dispositivos inteligentes que amenazan a los actores explotados para actividades nefastas. Por este motivo, es importante que los usuarios sean conscientes y no hagan clic en los enlaces de las redes sociales y estén atentos a los correos electrónicos fraudulentos que solicitan hacer clic en los enlaces o revelar datos personales. Siempre es importante verificar la legitimidad del sitio en cuestión, ya sea mirando más allá del candado y revisando sus Certificados TLS/SSL. A medida que las organizaciones trabajaban para mantener las luces encendidas y examinar el resultado final, hubo un impulso resultante para la eficiencia en las tecnologías de seguridad. También se hizo hincapié en las tecnologías que permitían a las organizaciones hacer más con menos, conla automatización juega un papel importante en términos de innovación en seguridad. Asimismo, también tiene otros beneficios como la reducción de costos, aumento de la productividad, confiabilidad y óptimo desempeño en los procesos. "La pandemia dejo claro que es importante ser conscientes de los riesgos asociados al uso de la tecnología dentro y fuera del lugar de trabajo. Las estafas como el phishing, los ataques de malware y las violaciones de datos comienzan en el punto más débil. Al tomar medidas para aumentar su conocimiento sobre ciberseguridad y practicar hábitos seguros de navegación en Internet, ayuda a protegerse a sí mismo y a su organización de posibles amenazas". concluye Roger Werner, Director General de CertSuperior, socio de DigiCert en México.

**Datos de contacto:**

DigiCert Latam

3125893314

Nota de prensa publicada en: [https://www.mexicopress.com.mx/lecciones-tecnologicas-que-ha-dejado-la](http://www.notasdeprensa.es/educalivecom-disfruta-de-cursos-presenciales-y-clases-particulares-a-traves-de-internet)

Categorías: Hardware Software Ciberseguridad Dispositivos móviles Innovación Tecnológica



[**http://www.mexicopress.com.mx**](http://www.notasdeprensa.es)