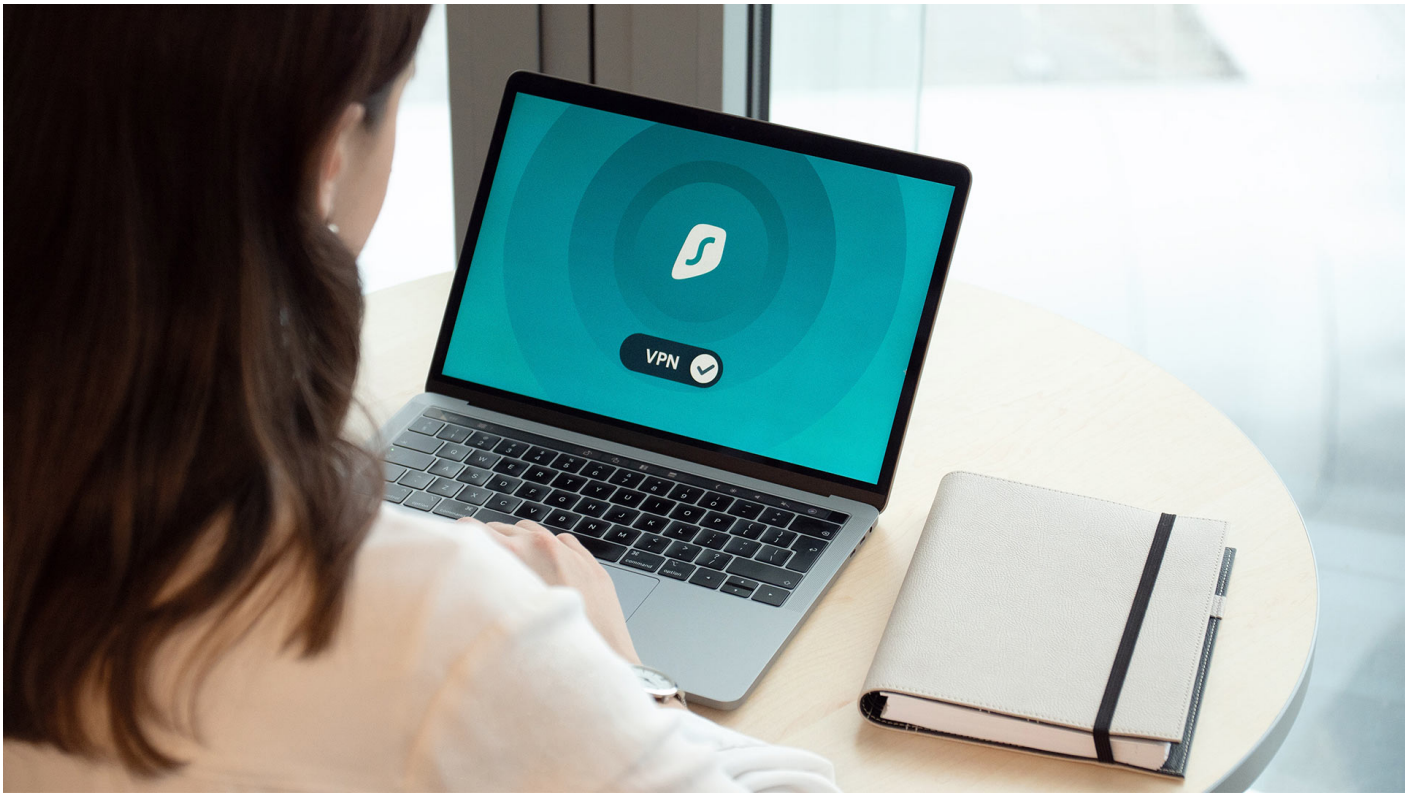
El ABC de la ciberseguridad para tu PyME



Félix Barrio, director del **Hub de Ciberseguridad del Tec de Monterrey,** compartió una serie de buenas prácticas que deben tomar en cuenta **pequeñas y medianas empresas** para estar convenientemente protegidos en una charla impartida a través de **ZEries.**

ZEries es un espacio virtual de charlas de expertos en temas de emprendimiento de la **Zona de Emprendimiento Innovador** del **Tecnológico de Monterrey.**

“Estamos haciendo desde el Hub de Ciberseguridad del Tec de Monterrey, una serie de webinars que intentan insistir en la importancia que tiene la ciberseguridad en la sociedad y las economías digitales,

“Nuestro objetivo es que los que asistan al webinar tengan una idea aproximada de elementos que deben exigir a sus proveedores, profesionales de tecnologías de la información, o bien para los que están intentando desarrollarse como expertos en ciberseguridad”, compartió.

Durante la charla el experto abordó las dimensiones del problema de la **ciberseguridad** y repasó cuales son las dimensiones de las **amenazas y riesgos.**

“En definitiva, el problema que tenemos a nivel profesional dentro de las organizaciones es que tenemos que aprender a generar soluciones para el riesgo tecnológico, con una visión de gestores”, enfatizó.

Según el experto, cada vez es más importante adquirir este tipo de capacitaciones para profesionales, porque **el 80% de los problemas que tiene en ciberseguridad una organización, habitualmente radican en usuarios,** personal de la propia organización.

“Puede ser por desconocimiento, mala fe, o por no disponer de las capacidades suficientes para estar protegido y eso evidentemente, nos alude a esa limitación que tenemos las organizaciones a menudo en nuestra gestión”, mencionó.

La pandemia de **COVID-19** ha generado la multiplicación de los hábitos de consumo del recurso del teletrabajo, el incremento del comercio electrónico, de las transacciones online, haciendo una dependencia de las empresas hacia la **ciberseguridad,** la cual, se va a multiplicar a partir de ahora, según el experto.

“Hay una mayor dependencia de la tecnología y consiguientemente, estamos asistiendo a un incremento de las amenazas cibernéticas, *y muchas están relacionadas a esta situación de crisis,*

"Hay un aumento en los ataques, en el volumen de lugares con software malicioso, sitios web que han aparecido en los últimos dos meses, problemas que se están multiplicando respecto a la situación anterior que teníamos”, destacó.

width="900" loading="lazy">

La **ciberseguridad** comprende la protección del ciberespacio en tres niveles, la defensa de la **infraestructura** tecnológica; los **servicios** que se prestan y la **información** que se encuentra en el mismo.

“Estos tres niveles son víctimas de ataque periódicamente y ***están detrás del dinero que es lo que está haciendo que nuestra economía sea cada vez menos tradicional y más digital,*** *y la mayoría de las vulnerabilidades están las pequeñas y medianas empresas”, puntualizó.*

Entonces… ¿Qué es lo que tenemos que hacer?

Implantar las medidas de seguridad que nos permitan **prevenir, detectar y responder** a cualquier tipo de riesgo o cualquier tipo de amenaza que se pueda dar dentro de nuestras organizaciones.

“Vamos a intentar establecer medidas que nos permitan reaccionar y reducir el impacto en caso de que recibamos un ataque, porque como hemos visto hasta ahora, ***no existe el 100% de la seguridad y si existe el 100% de riesgo de ser permanentemente infectados,*** *analizados, hay amenazas que están tratando de entrar en cualquier dispositivo o usuario que se conecta a la red”, detalló.*

Las familias de malware que aparecen cada año, van a seguir creciendo, dice el experto, ya que hay millones de nuevas formas de ataque, no solo en México, sino en cualquier parte del mundo.

“La mayoría de los empleados de las empresas tienen una capacitación insuficiente, *todavía hay muchos usuarios que no tienen instalado un antivirus en su smartphone y lo utilizan para temas de trabajo; o en su equipo doméstico que utilizan para el teletrabajo y tampoco lo tienen convenientemente parchado,*

“No tienen una cultura de la ciberseguridad suficiente, y esto hace que tengamos que extremar nuestras medidas protección*”, declaró.*

width="900" loading="lazy">

Las **buenas prácticas de protección** de una organización nos dicen que tenemos que desarrollar **una estrategia basada en tres pasos:**

1.Realizar un análisis de riesgos el cual mediante herramientas que nos mandan paso a paso, se van a categorizar todos los activos que tenemos que proteger dentro de la organización.

La probabilidad de que cada uno de esos equipos sufra algún tipo de ataque o amenaza, generalmente estas herramientas nos permiten conocer qué tipo de problemas pueden estar viéndose afectados.

“Existen múltiples herramientas, a mí en lo personal me gusta el modelo que desarrollaron en España basado en metodología MAGERIT es la metodología sobre la que se basa la herramienta PILAR, desarrollada por el Centro Criptológico Nacional (CCN), tiene una versión gratuita.

“Hay herramientas como la propia del Instituto Nacional de Ciberseguridad, INCIBE, para empresas con un análisis de riesgo muy sencillo, pero que podemos hacerlo todo lo complejo que queramos”, compartió.

2.Establecer una política de seguridad en donde designemos claramente los roles que tiene cada uno de los usuarios de nuestra organización, la capacitación que necesitan para poder utilizar cualquier tipo de dispositivo de manera segura.

3. Adoptar un sistema de gestión, conforme a un modelo de buenas prácticas.

*“Dos son los modelos que se recomiendan a nivel internacional I**SO 27,001** que es la norma quizá más extendida de sistemas de gestión de ciberseguridad en una organización.*

Otra que es idéntica en cuanto a su propósito, según el experto, es el **NIST Cybersecurity Framework,** el cual va diciendo a los usuarios hasta qué punto van mejorando en una escala del 1 al 5 cada uno de los pasos que deben seguir para proteger su organización,

***“Cualquier empresa tiene un 100 por ciento de probabilidades de sufrir un ataque en algún momento,** deberemos de tener un plan de continuidad de negocio, un plan de respuesta que comenzará por tener copias de seguridad periódicas, con pequeños intervalos, de manera que en el caso que se vea comprometido o sospechamos que ha habido algún tipo de daño o de acceso, podamos recuperar la información”, concluyó.*

SEGURO QUERRÁS LEER TAMBIÉN: