# Ciberseguridad: Una necesidad urgente para las empresas en 2023

De acuerdo con cifras del más reciente estudio de Verizon sobre ciberseguridad y violación de datos en empresas en 2022, el 82% de las infracciones involucraron el factor humano, incluidos los ataques sociales, los errores y el uso indebido de los datos. De hecho, según las investigaciones que llevó a cabo Proofpoint para su informe "State of the Phish 2022", el 86% de las organizaciones han sufrido ataques de phishing a través del correo electrónico en 2021.

Así, en términos regionales, una organización en América Latina está siendo atacada (por amenazas en general) una media de 1.586 veces por semana, según el Reporte de Threat Intelligence de Check Point Software sobre regiones geográficas.

Conscientes de la relevancia de este tema y con la intención de educar cada vez más acerca de los retos con respecto a la seguridad informática que tienen hoy las empresas, la Broward International University BIU, ha llevado a cabo de manera virtual el conversatorio sobre ciberseguridad. Este, desarrollado en el marco del Día de la Seguridad Informática, ha contado con la participación de expertos en el tema como la Dra. Ing. Rina Familia, Dr. Ing. Santiago Pérez y Msc Ing. Higinio Faccini, moderado por el Dr. José Luis Córica, Director del Simposio STEM BIU 2022 y Decano de la Escuela de Educación de **BIU University**.

# Manejo de datos

Según los expertos, lo primero es tener **conciencia del manejo que damos a los datos**, desde el usuario final hasta la empresa misma, deben contemplar siempre la extensión y el cuidado que se da a los datos en las diferentes plataformas y apps que se usan día a día, especialmente a la información sensible. Muchas veces se considera que para tener una buena seguridad informática no hay que hacer grandes esfuerzos, cuando es una de las inversiones más relevantes que hoy en día debe tener una empresa.

Además, se asume que **los ataques cibernéticos siempre se generan desde entes externos,** sin embargo, se ha demostrado que los ataques pueden venir también desde adentro de las organizaciones, es decir, al haber un componente humano, aun en la forma en que se implementan los sistemas de seguridad, hay personas que tienen acceso a datos sensibles, y es allí cuando pueden ocurrir casos de mal manejo de los datos, por esto es muy importante implementar sistemas de seguridad tanto internos como externos, indica la Dra. Ing. Rina Familia.

Para la implementación de una estrategia completa de sistemas de seguridad, es importante el factor humano, algunos expertos consideran que este es el eslabón más débil en temas de ciberseguridad, ya que a veces los ciberdelincuentes utilizan elementos de carácter psicológico para acceder a los sistemas informáticos. La actualización constante del personal que maneja la data en las organizaciones y la capacitación constante acerca del manejo de los datos como accesos y credenciales, debe ser primordial para reducir los riesgos y asegurar desde la gestión humana el buen manejo de la información, asegura el Dr. Ing. Santiago Pérez.

## ¿Cuáles son los delitos más comunes hoy en día en ciberseguridad?

Cuando hay vacíos en la seguridad informática, se pueden presentar dos tipos de vulnerabilidad, incidente de ciberseguridad y ataque; un incidente es una actividad donde por ejemplo un usuario que quizás no tenga los conocimientos necesarios, abre un correo electrónico en su empresa y este puede traer un malware, o desde el punto de vista físico (“Hardware”) un incidente puede ser que un servidor tenga un corte de energía eléctrica y haya vulnerabilidad.

Cuando hablamos de ataque, es definido como incidente de ciberseguridad, pero pensado con una intención clara, es decir, cuando hay robo de datos, contraseñas, a usuarios e incluso obtener datos confidenciales de la competencia, indica en su intervención el Msc Ing. Higinio Faccini.

## ¿Cómo asumir estos nuevos retos como organización?

Las organizaciones deben asumir la problemática de la ciberseguridad, creando un comité que involucre a los sectores más importantes de la compañía (incluyendo personal del área IT), para que definan todos los mecanismos, protocolos, herramientas, recursos y antivirus con los cuales se blindará la organización.

Hoy en día con la digitalización de las compañías, cada uno de

los puestos de trabajo es esencial para la ciberseguridad, más en este momento en que las redes han progresado, dejando de ser solo de datos administrativos (Nombres, correos, teléfonos, entre otros) estas ahora contienen información altamente delicada como finanzas, gestión comercial, incluso empresas con datos del internet de las cosas (IoT), cobrando así mucha relevancia la protección que se ejerza de toda la infraestructura informática de una empresa, concluyen los expertos.