La información de tu compañía puede estar en riesgo, lee más acerca de cómo evitarlo.

Como consecuencia de la pandemia una parte de la población migró su trabajo a modalidad remota, en donde no solo se trasladaron equipos a los hogares de los trabajadores de una empresa, sino también el acceso a información de vital importancia para las compañías.

La realidad es que hace un año nadie pensaba en este presente además que el riesgo de ciberataques era menor, pero durante el último año esta cifra aumentó, según la revista Innovación en un 600% en América Latina y se registra que, de cada tres ataques, dos son dirigidos a empresas.

Esta cadena organizada de ciberdelincuencia no solo afecta a la información personal del computador (accesos, discos duros,

proyecciones numéricas, documentos personales), también el riesgo puede ocasionar daños colaterales a la data sensible de los clientes de un negocio, si los sistemas de seguridad de la compañía no son lo suficientemente seguros.

Por esta razón te compartimos varios consejos sobre seguridad digital:

Contrata una nube confiable
Trabaja con proveedores de nube confiables y regulados por el gobierno que garanticen la seguridad de tu información, la estabilidad del servicio, y un nivel de redundancia aceptable para acceder a tu data durante cualquier eventualidad.

Realiza campañas de sensibilización sobre ciberseguridad con tus colaboradores.
Todos los colaboradores de una empresa deben entender que el mayor nivel de amenazas se deriva del phishing* y de las campañas en redes sociales, correos y WhatsApp. Por eso debemos aprender a dudar más del contenido en línea y revisar su origen para confirmar su veracidad, sobre todo, hay que evitar llenar formularios o abrir archivos que provengan de desconocidos.

Implementa políticas de administración en la conexión remota
Implementa herramientas como antivirus corporativos a los dispositivos portátiles y computadores de escritorio, que, debido al teletrabajo, se encuentran fuera del dominio de la empresa y pierden la protección del Firewall.
Controla rigurosamente la red de tu empresa a través de conexiones remotas que pasen por el Firewall antes de entrar a tu dominio.

Hosting Confiable
Consigue un servidor de host confiable, que cuente con protocolos que aseguren las puertas de comunicación y presenten un nivel de redundancia en el exterior para proteger la exposición de tu página web en caso de desastres naturales

y/o físicos del servidor.

Teleconferencias confiables
Cuida que las reuniones en línea no sean abiertas y en plataformas para videoconferencias seguras, además limita el acceso a través de formularios o inscripciones para evitar el ingreso de personas que pudieran vulnerar tu seguridad.

Refuerza las contraseñas de todos los dispositivos de red
Todos los dispositivos de tu empresa deben utilizar contraseñas alfanuméricas, combinación de mayúsculas y minúsculas, caracteres especiales, longitud mínima y máxima, grabación cifrada y no predeterminadas para reducir futuros ataques debido al fácil acceso. Regula el cambio de contraseña de forma periódica.

Protege las redes de tu empresa
Implementa un dispositivo Firewall de primera línea para el ingreso a tu red, protegiendo así todos tus segmentos de red que hayas establecido y evitar que intrusos que buscan robar datos vulnerables puedan ingresar a tu red.

Sigue estas recomendaciones, comunica a tu empresa cualquier anomalía que se presente durante el teletrabajo o en oficina, y, además, refuerza la seguridad de tu negocio con una póliza que te cubra de amenazas cibernéticas. Al asegurar la información de tu empresa y la de tus clientes, conservas la tranquilidad y confianza depositada en tu compañía.

Redacción: *Diego Mendoza.*

***Phishing:** Término informático que distingue a un conjunto de técnicas que persiguen el engaño a una víctima ganándose su confianza haciéndose pasar por una persona, empresa o servicio de confianza, para manipularla y hacer que realice acciones que no debería realizar.*