LITORALPRESS

Fecha: 26-11-2020 **Visitas:** 110.774 **Favorabilidad:** ☐ No Definida
Fuente: Publimetro.cl
Título: **Ciberseguridad: ¿Cuánto sabemos los chilenos al respecto?**

Link: https://www.publimetro.cl/cl/estilo-vida/2020/11/26/ciberseguridad-chilenos.html

Ciberseguridad: ¿ Cuánto sabemos los chilenos al respecto? Mauricio Gálvez, jefe del área de ciberseguridad de TIVIT Chile conversó con Publimetro. En términos legales, Chile está avanzando poco a poco en la materia. La seguridad en Internet hoy es más importante que nunca. Esto, debido a que el mundo entero se volcó a las redes tras la pandemia del coronavirus. Y para avanzar en estas materias es clave el acceso a la información.

Por este motivo, Tivit, multinacional dedicada a estas materias con presencia en 10 países de América Latina, junto a la carrera de Ingeniería Civil Telemática de la Facultad de Ingeniería de la Universidad de Santiago (USACH), realizarán el próximo 27 de noviembre a las 15:00 horas una charla. ¿El tema? "¿ Cómo podemos navegar de forma segura por internet?, un tema que está tomando cada vez más importancia para las empresas en Chile.

Charla gratuita con la Usach El encuentro estará disponible vía streaming en la cuenta de YouTube de la carrera llamado "Ingeniería Civil en Telemática USACH". Esto, para todo aquel que quiera conocer un poco más sobre las tendencias en ciberseguridad y cómo enfrentar un ataque de esta clase. En esta charla, los asistentes podrán profundizar las tendencias de hiperconectividad, sobre su utilización y cómo afecta a diario a las personas. Además, se mencionará cómo el mundo y las personas dependen cada día más de los servicios digitalizados, por lo que se abordará el tema de los derechos y deberes en el uso del internet.

Getty Images ¿ Qué tan informados estamos los chilenos frente a estas materias? Para profundizar en el tema, conversamos con Mauricio Gálvez, jefe del área de ciberseguridad de TIVIT Chile. ¿Somos los chilenos realmente conscientes de la ciberseguridad? Actualmente y con base a los últimos eventos de ciberataques, que han sufrido grandes empresas, tales como Banco Estado y, últimamente, CENCOSUD, el público en general ha tomado conciencia y presta más atención al hacer uso de los distintos aplicativos disponibles en internet, entendiendo cuáles son las precauciones que se deben adoptar cuando se estén utilizando estos tipos de servicios. ¿Cómo evalúa a los organismos públicos en estas materias? Actualmente, el Ministerio de Interior y Seguridad Pública, mediante su equipo de respuesta ante Incidentes de Seguridad Informática CSIRT Chile, ha cumplido un rol fundamental en el monitoreo y comportamiento de los grupos "˜hacktvistas', donde constantemente están informando o declarando de manera proactiva la actividad de estos ciberataques y de cómo deben tomar acciones de mitigación para las distintas soluciones de seguridad que puedan tener las distintas entidades públicas o empresariales, tales como servicios de Firewall, IPS, IDS, Antivirus, etc. De manera de mantener lo más resguardado posible los datos las personas y evitar que sean víctimas de algún ciberataque.

Gentileza ¿ Qué modificaciones se hacen necesarias en la legislación en esta materia? Creo que las modificaciones que se han realizado a nivel de legislación han ido acordes con las que se ha estado presentando en los últimos años, lo que sí creo que se debería dar prioridad al proyecto de ley de sanciones a delitos informáticos, dado que hoy no existen sanciones ejemplificadoras para este tipo de delitos acá en Chile, lo que nos convierte en un lugar apetecido por los ciberdelincuentes. ¿Estamos atrasados en comparación a otros países de la región? Chile en temas de cultura de ciberseguridad ha ido madurando y entendiendo que ya no es un servicio de acompañamiento sino más bien es la línea base ante cualquier negocio con presencia en internet y uso de sus servicios.


Ciberseguridad: ¿Cuánto sabemos los chilenos al respecto?

En un año de gran aumento de la conectividad ¿ Sientes que hayan salido a la luz debilidades en ciberseguridad? ¿ Cuáles y cómo combatirlas? Correcto, el año 2020 la pandemia modificó drásticamente la dependencia de la conectividad. Como también agregó un vector más de amenaza. Hoy el concepto de la seguridad perimetral ya casi dejó de existir. Donde antes del año 2020 los trabajadores explotaban los recursos de sus empresas localmente en sus oficinas. Hoy esto cambió y los colaboradores explotan estos servicios remotamente desde cualquier lugar que tenga alguna conexión hacia internet. Acá es donde se detectaron varios problemas de empresas que debieron adoptar plataformas y procedimientos de seguridad. Para que sus colaboradores continuaran trabajando y explotando los recursos de la empresa de manera segura.

Gentileza Sin embargo, esto también requiere de campañas internas de concientización de seguridad, por parte de las empresas a todos sus colaboradores con la finalidad de mantenerlos informados sobre cuáles son los principales vectores de ataque cibernéticos y cómo poder mantenernos seguros.

Por tanto, hoy un colaborador con cultura cibernética, paso a ser la primera línea de defensa en ciberseguridad de una empresa. ¿Qué le recomendarías a las empresas y pymes para mejorar sus coberturas en ciberseguridad y mantenimiento de equipos? Hoy, básicamente existe un decálogo de las buenas prácticas para evitar eventos de seguridad. Y que no se conviertan en los tan temidos Incidentes de seguridad: Contar con plataformas o soluciones de seguridad. Mantener actualizado y en línea el antivirus puede evitar la entrada de amenazas que comprometa nuestros sistemas. Realizar los reinicios de

sistema operativo para que así sean aplicados las últimas actualizaciones de parches de seguridad. Proteger el protocolo RDP: Contar con políticas de respaldo periódico que se almacenen fuera de la red organizacional. Tratar de escanear todos los archivos adjuntos, antes de abrirlos, con un antivirus que detecte comportamientos para combatir los ransomwares. Mantener una buena estrategia de respaldo de información: sistemas de copias de seguridad que deben estar aisladas de la red; y políticas de seguridad. Lo anterior permitirá neutralizar el ataque, restaurar las operaciones y evitar el pago del rescate. Getty Y además… Jamás seguir la instrucción de deshabilitar las funciones de seguridad, si un correo electrónico o documento lo solicita. Establecer políticas seguridad en el sistema para impedir la ejecución de ficheros desde directorios comúnmente utilizados por Ransomware (App Data, Local App Data, etc. Disponer de sistemas antispam para correos electrónicos, de esta manera se reduce las posibilidades de infección a través de campañas masivas de malspam por correo electrónico. Mantener listas de control de acceso para las unidades mapeadas en red restringiendo los privilegios de escritura. Con esto podrá identificar el impacto generado por el cifrado de archivos, entendiendo que el secuestro de información se producirá en todas las unidades de red mapeadas en el equipo víctima. Y quizás los más importante seguir las normativas internacionales tales como ISO 27001:2013 en su control A. 7.2 .2 " Concienciación con educación y capacitación en seguridad de la información " o NIST PR.

AT-1: " Todos los usuarios se encuentran entrenados e informados ", a fin de tener bases para divulgar campañas educativas orientadas a nivel de usuarios respecto al correcto uso de las herramientas tecnológicas, haciendo énfasis en cómo proceder al recibir correos de orígenes desconocidos, objeto prevenir que sus usuarios sean víctimas de entes maliciosos.