INGENIERÍA E INNOVACIÓN

SEPTIEMBRE 2023 maff_zapata_110 oscarsequera12 Roldanillo, Valle 2023

“A UN CLIC DE PERDERLO TODO”

“Según **los datos más recientes,** en 2022 **se realizaron 20 mil** millones de intentos de **ciberataques contra Colombia. Los tres tipos** de delitos cibernéticos **más frecuentes son el robo** de identidad, **las estafas** de pagos en línea y **los códigos** o software **maliciosos” https://www.mintic.gov.co**

Por Maria Fernanda Fernández Zapata.
Oscar Andrés Sequera Martínez

La ciberseguridad es la práctica de proteger sistemas, redes y programas de ataques digitales. Generalmente, estos ciberataques tienen como objetivo acceder, modificar o destruir información sensible; extorsionar a los usuarios o interrumpir la continuidad de un negocio y/o empresa. (CISCO, 2023)

Fuente: Jhoan Hernández

Entrevista al docente Ricardo Buitrago

“EL FUTURO ES **HOY**”

Revista IEI: ¿Cuáles son las amenazas cibernéticas más comunes que enfrentamos en la actualidad?

Ing. Ricardo Buitrago: *La principal* amenaza y la más importante es la ignorancia, el desconocimiento es el que nos hace cometer errores; un virus no es capaz de ingresar a una red, a una empresa, si no ha habido un error humano de adentro. Por ejemplo: Las cuentas hackeadas por phishing, esto es debido a que nos dejamos engañar gracias a la ignorancia. *La segunda* amenaza, son los llamados malware, que buscan infectar cierto archivo y, al darle clic, podrán acceder a nuestra máquina, robarnos alguna identidad o hacerse pasar por nosotros. *La tercera* amenaza son los bugs, los cuales vuelven a las máquinas como zombis, generando ataques simultáneos con un solo objetivo. *La cuarta* amenaza es el Spam que, en conjunto con la inteligencia artificial, nuestro sistema de correo electrónico, detecta que quizás ese correo contiene una serie de virus y lo marcan automáticamente como Spam. *La quinta* amenaza son los hogares inseguros, quizás cuando en nuestros hogares instalamos un router y lo dejamos predeterminado, no le colocamos ninguna seguridad, o le compartimos nuestra contraseña a muchas personas, no sabemos qué están haciendo esas otras personas en la red y eso también nos arrastra porque, si esa otra persona hace parte de mi red y está haciendo cosas indebidas, pues, si descargó un virus, este se va a esparcir por la red y yo también me veré perjudicado. *La sexta* amenaza son aquellos mensajes que nos llegan a nuestros celulares, como; “usted ha sido ganador de cierta cantidad de dinero” y le damos clic en ese mensaje; hay que tener conciencia de que nada es gratis en la vida. *La séptima* amenaza son los Ransomware, los cuales encriptan la información con una contraseña y para poder acceder a ella se debe pagar una alta suma de dinero.

Revista IEI: ¿Cuáles son las medidas básicas que una persona o empresa, debería tomar para protegerse contra ataques cibernéticos?

R.B: Principalmente la educación y la formación. Hacer al menos un curso básico. Y contratar a expertos en el área.

Fuente: bing.com

Imagen ilustrada con IA Bing

Revista IEI: ¿Cuál es el papel de la educación y la concienciación en la prevención de ataques cibernéticos?

R.B: La educación lo es todo. La ciberseguridad no debería acoger solo a los estudiantes de sistemas o informática, ya que debería ser algo transversal debido a que hoy en día, todo gira en torno a la tecnología, todo está conectado, todos estamos interconectados.

Revista IEI: ¿Cuáles son las habilidades y conocimientos necesarios para trabajar en el campo de la ciberseguridad?

R.B: Hay 3 bases fundamentales para este campo: La programación; uso y manejo de sistemas operativos, especialmente Linux; y las Redes de los datos.

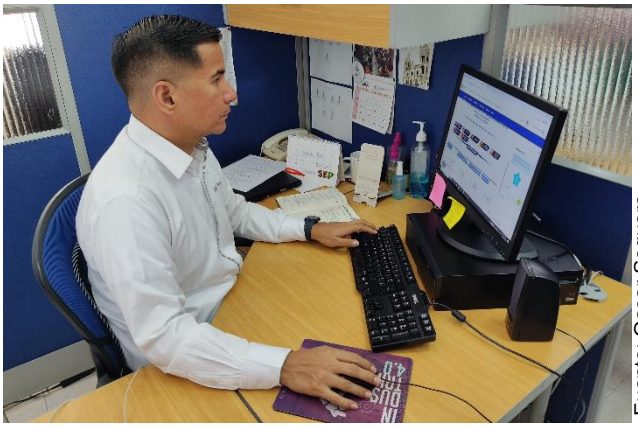
Revista IEI: ¿Puede compartir un ejemplo de un incidente de ciberseguridad del que haya sido testigo o que haya enfrentado en su trabajo?

R.B: Hace muchos años un cliente en la ciudad de Cali, una empresa comercial a nivel nacional e internacional la cual no estoy autorizado para dar nombre. Un día llegaron a la empresa y notaron que toda la información estaba encriptada, estaba con RANSOMWARE y proceden a llamarme, yo era el ingeniero de soporte nivel 1. A pesar de que contaban con métodos de ciberseguridad como un firewall, había ingresado un Ransomware por un correo electrónico en modo phishing. Lo único que nos pudo salvar fue una copia de seguridad del servidor que se había montado en el router en modo oculto, es decir, el disco duro externo no estaba conectado directamente al servidor, de no ser por eso, también lo hubieran encriptado; el disco duro estaba conectado al USB del router, por tal motivo, el disco duro no era visible en la red. El servidor lo había configurado para que hiciera *backup* (respaldo) a una hora específica todos los días. Gracias a Dios esa fue la solución.

Revista IEI: ¿Qué consejos daría a alguien que esté considerando una carrera en ciberseguridad?

R.B: Es una carrera prometedora, ya que la tecnología va a pasos gigantescos. “Es una carrera del futuro, pero el futuro no es a 10 años, el futuro es HOY.”

“¿Están seguros nuestros datos en el INTEP?”



Fuente: Oscar Sequera

Entrevista a Juan Manuel Franco, Webmaster INTEP

Revista IEI: ¿Qué medidas de seguridad usan para salvaguardar la base de datos del INTEP?

Juan Manuel Franco: Las dependencias Registro y Control Académico, Sección Financiera, y el Centro de Biblioteca e Información Científica son los que contienen las bases de datos de los estudiantes y docentes de la institución. Las medidas de seguridad que se han implementado, por **políticas de seguridad de la información son:**

-Límites de acceso a la información
-Copia de seguridad
-Seguridad perimetral bajo Firewall de Sophos

Revista IEI: ¿El INTEP ha sido víctima de algún ciberataque?

J.M.F: Si, hace 10 años ocurrió un ciberataque, fue manipulado el sitio Web a la página principal del INTEP, pero se recuperó, ya que se tenía la copia de seguridad.

Revista IEI: ¿Qué medidas han tomado frente a amenazas cibernéticas?

J.M.F: El equipo de trabajo encargado de la Infraestructura Tecnológica de la institución, monitorean y realizan revisiones para mantener a los sistemas actualizados, se utilizaron las contraseñas seguras de acceso a las distintas plataformas que utiliza el acceso del sistema operativo, correo electrónico institucional, sistema de información institucional, software contable, etc.

¡TIPS PARA EVITAR SER UNA VÍCTIMA MÁS!

- Usa contraseñas seguras (may, min, símbolos y números)
- Ten cuidado con los mensajes o correos electrónicos sospechosos.
- Evita instalar apps y/o programas de dudosa procedencia (craqueados)
- Revisa constantemente los movimientos de tus cuentas bancarias.
- Evita conectarte a redes de Wi-Fi públicas.
- Realiza copias de seguridad.
- Habilita un firewall en tu router.
- Utiliza software antivirus
- Actualiza tus conocimientos

“ESTAFA A UN CLIC” ¡CASO DE LA VIDA REAL!

Fuente: Perfil de Facebook

Lorena Gálvez, Magíster en Comunicación

¡VICTÍMA DE MINERÍA SOCIAL!

Por medio de la minería social se buscan perfiles de personas. En este caso la que salió perjudicada fui yo, dicen que se hizo a través de mi celular. Seguramente le dí “like” a una imagen o al aceptar las cookies a través de un periódico que vi en la internet, por medio de esta pudieron acceder a mi correo, mis contraseñas y a través de ellas se me hizo un robo más o menos de unos 15 MILLONES DE PESOS de la TARJETA DE CRÉDITO.

Yo actué muy rápido y puse la denuncia. Las personas encargadas de la entidad bancaria me dijeron que como había actuado tan rápido posiblemente iba a salir a mi favor y, ASI FUE. A los 5 días me responden diciendo que el caso se resolvió a mi favor, que no le debo nada a la entidad y que simplemente fui presunta de un robo. Me enviaron unas indicaciones, fueron; No recibir llamadas para cambio de contraseñas, no recibir correos para cambio de contraseñas, no dar la información bancaria y, en lo posible, SIEMPRE ir a una entidad física.

A pesar de todo yo fui a los entes judiciales, puse la demanda a la policía por medio del correo e hice la demanda a la fiscalía, ellos tomaron mi caso, sin embargo, nunca se me dio una respuesta, simplemente unos correos que me enviaron con los datos de mi denuncia.

Finalmente me cuido de dar “Like” a cualquier información, pero sobre todo de ser más responsable, de estar pendiente de mi cuenta bancaria, cuáles son mis movimientos diarios para que esto no me vuelva a suceder, también, le coloqué un tope a mis transferencias diarias, hice cambio de mis contraseñas y reduje todo el porcentaje de mi tarjeta de crédito.

Esto es una experiencia que nos deja claro que, los ladrones no solamente están allí de manera física, sino que hay cantidad de personas que no vemos que son muy inteligentes y usan esa inteligencia para hacerle daño a otras personas. (Gálvez, 2023)

Fuentes:
Docente Ricardo Buitrago INTEP, Roldanillo Valle
Docente Lorena Gálvez INTEP, Roldanillo Valle
Webmaster Juan Manuel Franco INTEP, Roldanillo Valle
www.bing.com
https://chat.openai.com
https://www.cisco.com/c/es_mx/products/security/what-is-cybersecurity.html