TIC

TALENTO TECH

REGIÓN 3

CAUCA – NARIÑO

LECCIÓN 3 – UNIDAD 2

Universidad Tecnológica de Pereira | faceIT

Lección 3: Prevención de ciber ataques:

Hemos visto que existen muchas formas por medio de las cuales, atacantes pueden robar datos y hacer daño con la información adquirida. Sin embargo, existen buenas prácticas con los datos que mitigan y evitan la gran mayoría de los ataques.

Tanto para uso personal como organizacional es importante implementarlas y usarlas constantemente, evitando pérdidas de información. Algunas opciones son sencillas y fortalecen considerablemente la seguridad de la información.

1. **Aislar las responsabilidades de los usuarios:** En una red corporativa o en aplicaciones conectadas a internet, es importante separar las responsabilidades de los usuarios. Es decir, no todos deben tener acceso a toda la información disponible sino a la que sea de interés para cada usuario. Separando roles es una técnica útil para evitar brechas de seguridad.

2. Uso de contraseñas seguras y doble factor de autenticación. Una contraseña segura es aquella que toma mucho tiempo descifrar por fuerza bruta o con el uso de diccionarios de información. Esto se logra siguiendo algunas reglas básicas que se verán en la siguiente unidad. Asi mismo, el doble factor de autenticación crea una capa adicional de seguridad que evita el robo de datos a pesar de que se hayan expuesto contraseñas.

3. Usar redes privadas virtuales: Las redes privadas virtuales o VPN son técnicas de encriptar las comunicaciones por internet. Son muy seguras y mitigan el riesgo de que terceros malintencionados descifren los datos con computadores en el medio de las comunicaciones (man in the middle). En lecciones siguientes se hablará en detalle del funcionamiento de las VPN y la seguridad que ofrecen.

4. Emplear cortafuegos: El cortafuegos (firewall) son programas que bloquean las conexiones entrantes y salientes por puertos no autorizados. Evitan trafico malicioso como el de programas de tipo malware, para que estos no se puedan comunicar con internet. También evitan que atacantes tomen el control de equipos.

5. Usar software libre o software con licencias El uso de software adquirido por medios ilegales es un riesgo de seguridad. A veces el software ilegal es obtenido por medio de internet o por medio de conocidos quienes afirman tener un instalador que no requiere licencias. El software pirateado fue alterado para que funcione sin requerir las licencias de los desarrolladores. Sin embargo, quienes alteran el software para no emplear licencias, también instalan todo tipo de malware que puede ocasionar brechas de información y comprometer la seguridad de todos los datos. Incluso se conocen casos de software pirata que registran todas las teclas pulsadas en el computador y las envían a internet. Todo esto aparte de que legalmente existen sanciones para las personas y empresas que usen y copien software pirata.

Para evitarlo es recomendable adquirir legalmente las licencias de software, o, en caso de que una licencia sea muy costosa, se puede optar por alternativas de software libre y gratuito (no todo software libre es gratuito).

El software libre es aquel al cual podemos tener acceso al código fuente, modificarlo y mejorarlo a nuestro gusto. La ventaja de que el código sea accesible es que se puede saber si el software tiene brechas de seguridad.

También es recomendable siempre asegurarse de que se está visitando el sitio oficial del software que se quiere descargar. En ocasiones, se suele utilizar un buscador para encontrar enlaces de descarga del software y los usuarios son redirigidos a páginas con malware que engañan a los usuarios haciéndoles pensar que son sitios confiables para obtener software.

5. Formación en ciberseguridad: La mejor inversión en seguridad es formar al personal y capacitarlo en identificar riesgos y mitigarlos. De esta forma se evitan muchos de los ataques comunes y se desarrollan espacios de trabajo seguros.