¿Sabías que tu información está en riesgo? ¡Entérate!

La Oficina de las Tecnologías de la Información y las Comunicaciones (OTIC), presenta algunas pautas para evitar infecciones y prevenir el ataque de Ransomware, virus que secuestra la información mediante cifrado y pide un valor de rescate.

Para protegerte debes:

1. Realizar periódicamente copias de seguridad de la información más importante. Si tu información es crítica, haz copias de respaldo diarias. Los soportes donde se realicen las copias de seguridad solo deben estar conectados en el momento de hacer la copia para evitar que, ante una infección, estos se vean también afectados.

Esta es la única medida de seguridad que garantiza poder recuperar la información "secuestrada" al 100%.

2. Ser precavido a la hora de descargar y ejecutar archivos procedentes de Internet. Sobre todo con los archivos adjuntos en correos electrónicos, en especial aquellos de asuntos aparentemente importantes de la Policía, la Fiscalía y la DIAN. La mejor forma de actuar es no descargarlos, aunque sean de un contacto conocido.

En caso de estarlos esperando, los puedes descargar.

3. Mantener actualizado el sistema operativo, software y antivirus Symantec Corporativo de la Universidad Nacional de Colombia. Así evitarás que, aprovechando alguna vulnerabilidad, te infecten.

Si no mantienes tus equipos actualizados, te expondrás a todo tipo de riesgos, pues estamos en la era de oleadas de ataques cibernéticos de escala mundial. Los ataques más comunes son robo de información, pérdida de privacidad, perjuicio económico, suplantación de identidad, entre otros.

4. Apagar el equipo después del horario laboral. Si no es necesario que tengas tu PC encendido, apágalo diariamente, en especial los fines de semana pues son los días en los que los equipos son objeto de innumerables ataques.

5. Utilizar contraseñas robustas ya que algunas infecciones se extienden a unidades compartidas de almacenamiento por usar contraseñas débiles, como por ejemplo abc123, 12345, tu nombre, tu apellido, tu teléfono, tu cédula, entre otras.

6. Desactivar la reproducción automática en los dispositivos de almacenamiento externo que conectes. Las USB y los discos portables deben ser desinfectados cada vez que se conectan a diferentes equipos para evitar traslado de virus entre las oficinas o entre la oficina y el hogar. Si puedes prescindir de los medios de almacenamiento portables, no los uses, así mitigas los riesgos sobre la información desde la fuente del problema.

7. Utilizar una cuenta con privilegios limitados para el uso habitual y una cuenta con privilegios de administrador únicamente para gestionar configuraciones o instalar aplicaciones. Esto evita que si eres víctima de software malicioso no se escalen privilegios altos, minimizando el impacto sobre los sistemas y los datos. El administrador se usa para realizar cambios en la configuración, instalar una nueva aplicación, dar de alta un nuevo usuario, entre otros. Al finalizar estas tareas, debes seguir trabajando con una cuenta estándar.

8. Utilizar en los PCs solo softwares licenciados de la Universidad Nacional de Colombia y otros específicos con licenciamiento libre avalados por la OTIC y siguiendo las directivas técnicas de la Dirección Nacional de Tecnologías de la Información y las Comunicaciones (DNTIC) para protegernos del Ransomware y otros programas maliciosos.

No está permitido utilizar softwares portables ilegales y/o instalar softwares ilegales, **si un integrante de la comunidad universitaria lo hace o patrocina esta práctica, comete falta grave y queda sujeto a sanciones legales.**

9. La precaución se extiende a los dispositivos móviles. Se debe tener la misma prudencia al abrir enlaces en los correos, mensajería instantánea y redes sociales, aunque sean de contactos conocidos. También ser precavidos al descargar ficheros adjuntos, pues algunos de ellos pudieron ser infectados y suplantados.

10. Las copias de respaldo no deben almacenarse en el mismo equipo de trabajo. Se requiere una copia externa local en discos portables dedicados solo para este uso o en los servicios virtuales de internet (Google Drive, Dropbox, etc.).

11. Recuerda que, si la única copia de tu información está en tu equipo local, tu información está en alto riesgo de pérdida, ya sea por fallas de hardware o de software malicioso. Solicita un recurso compartido de almacenamiento en la OTIC.

12. Si requieres apoyo técnico o información adicional sobre la seguridad de tu información y de cómo protegerla, comunícate con la OTIC.

Te invitamos a conocer las Políticas y directrices técnicas de la DNTIC

Políticas protección de datos

Política General de Seguridad de la información

Directrices Técnicas

Directriz Técnica No. 10A

Directriz Técnica No. 16

Directriz Técnica No .18

Sitio web DNTIC

Oficina de Tecnologías de Información y Comunicaciones
Vicerrectoría
Sede Medellín

UNIVERSIDAD NACIONAL DE COLOMBIA