GOBIERNO DEL PARAGUAY | MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

CERT-PY

GUÍA DE CIBERSEGURIDAD
PARA ESTUDIANTES

ENERO 2025

ÍNDICE

Introducción

La tecnología ha revolucionado la educación, permitiendo a los estudiantes acceder a una gran cantidad de recursos en línea y nuevas formas de aprendizaje. Sin embargo, junto con estos avances también surgen desafíos relacionados con la ciberseguridad. Los riesgos en Internet, como el robo de identidad, el malware y los ataques de ingeniería social, pueden afectar la privacidad y seguridad de los estudiantes.

El objetivo de esta guía, elaborada por el Centro de Respuestas ante Incidentes Cibernéticos (CERT-PY), es proporcionar a los estudiantes los conocimientos y herramientas necesarias para proteger su información y navegar de manera segura en el entorno digital. A lo largo del documento, se presentan las principales amenazas en Internet, desde el malware y el phishing hasta el uso seguro de redes y dispositivos. Además, se ofrecen recomendaciones prácticas para evitar caer en fraudes, proteger la privacidad en línea y adoptar buenas prácticas en el uso de la tecnología.

En un mundo cada vez más conectado, es fundamental que los estudiantes comprendan la importancia de la ciberseguridad y asuman un rol activo en la protección de su identidad digital. Con un conocimiento adecuado y la aplicación de medidas preventivas, es posible aprovechar los beneficios de la tecnología de manera segura y responsable.

¿Qué es la ciberseguridad?

La ciberseguridad, es el conjunto de medidas tecnológicas, administrativas y legales que se toman para proteger los sistemas informáticos, las redes y los datos de accesos no autorizados, ataques maliciosos, robo de información o cualquier otra amenaza que pueda comprometer la confidencialidad, integridad y disponibilidad de la información.

¿Por qué es tan importante la ciberseguridad?

El mundo de hoy está más conectado que nunca. La economía global depende de que las personas puedan comunicarse en diferentes zonas horarias y tener acceso a información importante desde cualquier lugar. La ciberseguridad facilita la productividad e innovación al darles a las personas confianza para trabajar y socializar online. Los procesos y las soluciones adecuadas permiten que los negocios y gobiernos aprovechen la tecnología para mejorar la forma en que se comunican y entregan sus servicios sin aumentar el riesgo de ataques.

¿Qué amenazas acechan en Internet?

Internet ofrece un sinfín de oportunidades, pero también es un entorno donde diversas amenazas pueden comprometer nuestra seguridad, privacidad y bienestar. Estas amenazas son innumerables y están en constante evolución, pero entre las más comunes se encuentran las siguientes:

1. Malware

El malware es un término general que engloba programas maliciosos diseñados para infiltrarse, dañar o tomar control de sistemas informáticos.

- **Virus**
  Un virus es un programa que se adjunta a archivos legítimos y, al ejecutarse, se replica infectando otros archivos. Su propósito puede ser dañar el sistema, corromper datos o robar información.
  - **Propagación:** Requiere la interacción del usuario, como abrir un archivo infectado.
  - **Ejemplo:** Un virus que se propaga a través de archivos adjuntos de correo electrónico.
- **Gusanos**
  Los gusanos son similares a los virus, pero no necesitan adjuntarse a un archivo ni requerir la acción del usuario para propagarse. Pueden replicarse automáticamente y extenderse a través de redes.

- **Objetivo:** Saturar redes, consumir recursos del sistema y, en ocasiones, instalar otros tipos de malware.

- **Ejemplo:** El gusano "WannaCry" que afectó sistemas a nivel mundial en 2017.

- **Troyanos**
  El troyano se disfraza de software legítimo para engañar al usuario y lograr su instalación. Una vez dentro del sistema, puede realizar actividades maliciosas, como abrir puertas traseras para otros ataques.

  - **Propósito:** Espiar, robar información o instalar más malware.

  - **Ejemplo:** Un programa gratuito que promete acelerar tu computadora, pero roba datos personales.

- **Ransomware**
  El ransomware bloquea el acceso a los datos del sistema o los cifra, exigiendo un rescate (generalmente en criptomonedas) para devolver el acceso.

  - **Impacto:** Puede paralizar sistemas empresariales, gubernamentales e individuales.

  - **Ejemplo:** El ransomware "CryptoLocker", que cifra archivos y pide un pago para descifrarlos.

- **Spyware**
  El spyware espía al usuario recopilando información personal o monitoreando su actividad sin su consentimiento.

  - **Objetivo:** Obtener datos sensibles como contraseñas, historial de navegación o credenciales bancarias.

  - **Ejemplo:** Un spyware que registra pulsaciones de teclas (keylogger) para robar contraseñas.

- **Adware**
  El adware muestra anuncios no deseados o intrusivos en el dispositivo del usuario. Aunque no siempre es dañino, puede ser una puerta de entrada para otros tipos de malware.

  - **Propósito:** Generar ingresos mediante la publicidad o redirigir a sitios sospechosos.

  - **Ejemplo:** Ventanas emergentes constantes con anuncios engañosos.

- **Rootkits**
  Los rootkits son herramientas diseñadas para obtener acceso administrativo (root) en un sistema y ocultar la presencia de malware.

  - **Peligro:** Permiten al atacante el control total del sistema afectado.
  - **Ejemplo:** Rootkits que deshabilitan el software de seguridad y permiten la instalación de otros programas maliciosos.

- **Keyloggers**
  Los keyloggers registran las pulsaciones de teclas del usuario, lo que permite a los atacantes obtener contraseñas, nombres de usuario y otra información sensible.

  - **Uso frecuente:** Robo de credenciales bancarias o de redes sociales.

- **Botnets**
  Las botnets son redes de dispositivos infectados (bots) que son controlados de forma remota por ciberdelincuentes. Se utilizan para actividades como ataques DDoS, envío de spam o minería de criptomonedas.

  - **Ejemplo:** Una botnet que utiliza miles de computadoras infectadas para derribar un sitio web mediante un ataque DDoS.

- **Malware móvil**
  Es un malware diseñado específicamente para dispositivos móviles. Puede robar datos personales, realizar compras no autorizadas o incluso rastrear la ubicación del usuario.

  - **Ejemplo**: Aplicaciones falsas descargadas desde tiendas no oficiales que contienen malware.

Objetivos de los malware

- Robar información confidencial, como contraseñas o datos financieros.
- Controlar dispositivos para actividades ilícitas, como minería de criptomonedas o ataques a otros sistemas.
- Extorsionar a las víctimas mediante ransomware, exigiendo pagos para recuperar el acceso a sus archivos.
- Dañar sistemas para interrumpir sus operaciones o inutilizarlos.

2. Ataques informáticos

Los ataques informáticos abarcan una amplia gama de técnicas empleadas por ciberdelincuentes para acceder a sistemas sin autorización o interrumpir su funcionamiento.

Objetivos:

- Obtener acceso no autorizado a sistemas y redes para robar información o instalar malware.
- Sabotear servicios o infraestructura mediante ataques DDoS (denegación de servicio).
- Engañar a los usuarios mediante phishing para obtener credenciales o información sensible.
- Explotar vulnerabilidades en software o hardware para tomar el control de sistemas.

Uno de los más conocidos es el phishing que es un tipo de ataque en el que los ciberdelincuentes intentan engañar a los usuarios para que revelen información personal, como contraseñas o datos de tarjetas de crédito. Pueden hacerlo enviando correos electrónicos o mensajes de texto que parecen legítimos, pero que en realidad son falsos.

3. Robo de identidad y de datos personales

El robo de identidad implica la obtención no autorizada de información personal, que luego es utilizada para realizar actividades fraudulentas.

Objetivos:

- Cometer fraudes financieros, como acceder a cuentas bancarias o realizar compras ilegales.
- Suplantar a la víctima para obtener beneficios en su nombre, como líneas de crédito o servicios.
- Difundir información personal con fines de chantaje o daño reputacional.
- Vender datos en el mercado negro a otros delincuentes.

Recomendaciones de ciberseguridad para el uso seguro de las redes y dispositivos

En caso de que los estudiantes utilicen dispositivos personales para las actividades de educación en línea, aunque estos no cuenten con políticas de seguridad rigurosas, pueden reducir sus vulnerabilidades poniendo en práctica las siguientes recomendaciones:

1. Sistema Operativo

Mantener actualizados los sistemas operativos y las aplicaciones de los dispositivos, incluidas las computadoras personales (PC), los teléfonos inteligentes y las tabletas. Estas actualizaciones normalmente incluyen cambios importantes que mejoran el rendimiento y la seguridad de los equipos; muchos de estos programas, incluso, se actualizan de manera automática. Se recomienda activar funcionalidades de protección, como el cortafuegos (firewall), incorporadas en los sistemas operativos más comunes. Un cortafuegos es la primera línea de defensa ante un ataque a una

red desde Internet y permite proteger el equipo de programas maliciosos o de atacantes que intenten conectarse al equipo de forma remota.

Además, permite establecer reglas para indicar qué conexiones de red se deben aceptar y cuáles no. Al mismo tiempo, admite el intercambio normal de datos entre la computadora y servicios verificados de Internet.

2. Antivirus

Los antivirus son programas que ayudan a proteger los dispositivos contra la mayoría de los virus, gusanos y troyanos y otros tipos de malware que pueden infectar a los dispositivos. Por ello se recomienda:

- Instalar y mantener actualizados los antivirus, prefiriendo aquellos que incorporan funcionalidades de protección contra malware y cortafuegos (firewall), también conocidos como “suites de seguridad”.

- Evitar tener dos antivirus en un mismo dispositivo. Tener dos antivirus activos no significa mayor protección; de hecho, puede ocasionar diferentes problemas en el sistema. Un antivirus que esté trabajando se convertirá en un “software malicioso” a los ojos del otro, el cual intentará bloquearlo y eliminarlo, y se corre el riesgo de afectar el desempeño del sistema por el consumo extra de recursos.

- Todas las instalaciones y actualizaciones de programas y aplicaciones deben hacerse desde el sitio web oficial del fabricante o desde las tiendas oficiales de apps verificando la identidad del autor de la aplicación, evitando descargar e instalar aquellas de dudosa procedencia.

3. Red Wi-Fi

Una parte clave de la educación en línea es asegurar las redes en el hogar. Es común usar routers Wi-Fi, pero para evitar accesos no autorizados, es esencial configurar una contraseña en la red. Los routers ofrecen diferentes tipos de contraseñas y cifrados para proteger la conexión. Las redes sin cifrado no son recomendables.

Se sugiere cambiar las contraseñas predeterminadas por una contraseña robusta, que incluya mayúsculas, minúsculas, números y símbolos, y sea lo más larga posible. También es importante no compartir la contraseña con otras personas, ya que podrían acceder a todos los dispositivos conectados. Finalmente, se recomienda evitar usar redes Wi-Fi públicas abiertas para compartir información sensible.

4. Contraseñas

Las contraseñas son esenciales para proteger la información en dispositivos y cuentas, pero muchas personas optan por contraseñas fáciles de recordar, lo que las hace vulnerables a los ciberdelincuentes.

Para mejorar la seguridad, se recomienda:

- Utilizar contraseñas largas y únicas para cada cuenta o dispositivo.
- Evitar combinaciones simples como fechas de nacimiento o palabras comunes.
- Usar contraseñas de al menos 16 caracteres con mayúsculas, minúsculas, números y caracteres especiales.
- No escribir contraseñas en papeles ni almacenar archivos accesibles.
- Activar la autenticación de dos factores para una capa extra de seguridad.
- Nunca compartir contraseñas o códigos de inicio de sesión.
- Cambiar las contraseñas con regularidad para prevenir accesos no autorizados.

Ataques con Ingeniería social

Los ataques de ingeniería social buscan engañar a los usuarios para robar información sensible, como contraseñas. Para minimizar el riesgo, se recomienda:

- Estar alerta ante mensajes de remitentes desconocidos (llamadas, correos, SMS, enlaces, etc.).
- Antes de hacer clic en enlaces o descargar archivos, preguntarse si se esperaba la información, si se reconoce al remitente y si se solicita realizar alguna acción.
- Desconfiar de mensajes genéricos o urgentes que intentan provocar reacciones rápidas.
- Identificar señales de fraude, como errores ortográficos, imágenes de baja calidad o mensajes sin personalización.
- En comunicaciones financieras, nunca hacer clic en enlaces ni proporcionar información de acceso; en su lugar, contactar directamente a la institución para verificar.

Navegación segura

A efecto de promover la navegación segura en Internet, se sugiere adoptar las siguientes recomendaciones:

- Ingresar solo a sitios web confiables, escribiendo uno mismo la dirección de la página a la que se quiere acceder y evitando utilizar enlaces proporcionados por terceros.
- Conocer y aplicar las funcionalidades de “navegación privada” o “navegación segura”, que impiden el almacenamiento del historial en el navegador, así como imágenes, nombres de usuario y contraseñas.
- Cuando se realicen transacciones o intercambio de información sensible, asegurarse de que la dirección de la página web comience con “https” (no “http”), con un candado verde, lo que contribuye a mantener segura la información transmitida.

- Desactivar la compartición de tu ubicación geográfica, a menos que sea estrictamente necesario.
- Evitar el ingreso de información personal en formularios dudosos. Si te encuentras ante un formulario que solicita información delicada (por ejemplo, nombre de usuario y contraseña), es recomendable verificar la legitimidad del sitio antes de responder.
- Al terminar de navegar en Internet, es importante cerrar la sesión, sobre todo si se utiliza un equipo compartido, para evitar que otras personas tengan acceso a cuentas e información privada.

Uso seguro de las herramientas en la nube

La nube permite almacenar y administrar datos, así como ejecutar aplicaciones en línea, entre muchas otras funciones. Con relación al almacenamiento, la nube permite acceder a archivos y datos desde cualquier dispositivo conectado a Internet; es decir, la información está disponible en cualquier lugar en el que te encuentres y siempre que la necesites.

Para hacer uso de los servicios de la nube de manera segura y evitar el robo o mala utilización de la información almacenada, es conveniente tener en mente las siguientes recomendaciones:

- Tener conocimiento de las condiciones de uso y las políticas de privacidad antes de utilizar cualquier servicio en la nube.
- Utilizar servicios de almacenamiento que cuenten con cifrado “https” y certificado de seguridad. Esto lo puedes verificar en la barra de direcciones de tu navegador de Internet.
- No subir a la nube información sensible con acceso público o abierto. Se recomienda utilizar herramientas de cifrado, como es el uso de carpetas con contraseña y acceso restringido.
- Verificar periódicamente los archivos y carpetas que tenemos compartidos desde nuestra cuenta, a fin de deshabilitar los enlaces y acceso a terceros que ya no sean necesarios.
- Utilizar contraseñas robustas para acceder al servicio y, preferentemente, activar el doble factor de autenticación o verificación en dos pasos.
- Realizar periódicamente un respaldo de la información almacenada en la nube en otro tipo de dispositivo, por ejemplo, en un disco duro externo debidamente protegido por contraseña. De esa manera, se mantiene el acceso a la información en caso de cualquier contratiempo, como una conexión limitada a Internet.
- Cerrar la sesión de la nube al concluir las actividades que se estén realizando.

Conclusión

La ciberseguridad es una responsabilidad compartida que requiere el compromiso de todos los usuarios de la tecnología, incluidos los estudiantes. A lo largo de esta guía, hemos explorado las principales amenazas digitales y las estrategias para prevenir ataques y proteger la información personal.

En un entorno donde los riesgos digitales evolucionan constantemente, es fundamental que los estudiantes adopten hábitos seguros, como el uso de contraseñas robustas, la verificación de fuentes en línea, la instalación de software de seguridad actualizado y la desconfianza ante mensajes sospechosos. Además, es clave fomentar una cultura de seguridad digital en la que cada estudiante sea consciente de los peligros y actúe con precaución al interactuar en el mundo digital.

La educación en ciberseguridad no solo protege la información personal, sino que también contribuye a un entorno en línea más seguro para todos. Al aplicar los principios y recomendaciones de esta guía, los estudiantes podrán disfrutar de la tecnología con confianza y sin poner en riesgo su seguridad.

FUENTE:

- https://www.gob.mx/cms/uploads/attachment/file/896412/Gu_a_de_Ciberseguridad_en_apoyo_a_la_educacion.pdf
- https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/guia-para-madres-padres-docentes-amenazas-internet