Keylogger

Ministerio de Educación,
Deporte y Cultura

REPÚBLICA
DEL ECUADOR

EQUIPO TÉCNICO
Soledad Albán Montalvo
Hamilton Cabrera Brunes
Víctor Pazmiño Puma

DISEÑO, DIAGRAMACIÓN E ILUSTRACIÓN
Adolfo Vasco Cruz

EQUIPO TÉCNICO EXTERNO

Marcelo Javier Sotaminga Cinilin

Primera Edición, 2026

Av. Amazonas N34-451 y Av. Atahualpa
Quito-Ecuador
www.educacion.gob.ec

Ministerio de Educación, Deporte y Cultura

REPÚBLICA DEL ECUADOR

Contenido

1. Introducción

En la era digital, donde la tecnología se integra cada vez más en nuestra vida cotidiana y en el ámbito educativo, es fundamental comprender y gestionar los riesgos asociados al uso de internet y los dispositivos electrónicos. Uno de estos riesgos, a menudo invisible, pero con consecuencias significativas es el *keylogger*. Este documento conceptual tiene como objetivo principal desglosar la naturaleza de los keyloggers, su impacto potencial y, lo más importante, cómo podemos protegernos de ellos.

La importancia de abordar este tema en el contexto educativo radica en la necesidad de formar ciudadanos digitales responsables y conscientes de los peligros inherentes al entorno virtual. Los estudiantes, al ser usuarios activos de la tecnología, son particularmente vulnerables a este tipo de amenazas si no poseen el conocimiento y las herramientas adecuadas para identificarlas y prevenirlas. La educación digital no solo implica el desarrollo de habilidades tecnológicas, sino también la promoción de una ciudadanía digital crítica y segura.

Este documento busca empoderar a la comunidad educativa a través de un enfoque práctico y preventivo, abordando el riesgo del keylogger, siguiendo una ruta de aprendizaje estructurada en tres pilares fundamentales: conocer, identificar y prevenir.

2. Ruta de aprendizaje

2.1 Conocer el riesgo

Definición técnica y pedagógica del keylogger

Un *keylogger* (del inglés *key*, 'tecla', y *logger*, 'registrador') es un *hardware* o *software* malicioso diseñado para registrar y almacenar cada pulsación de tecla que un usuario realiza en un dispositivo, ya sea una computadora o un teléfono móvil[1]. Su propósito principal es capturar información sensible sin el conocimiento o consentimiento del usuario, como contraseñas, datos bancarios, conversaciones privadas y cualquier otra información digitada. Desde una perspectiva pedagógica, podemos entender el keylogger como una herramienta de espionaje digital que vulnera la privacidad y la seguridad de la información personal, transformando la interacción cotidiana con la tecnología en un riesgo potencial de exposición y robo de datos.

Contexto global y nacional del uso malicioso de keyloggers

Los keyloggers forman parte de un ecosistema de amenazas cibernéticas en constante evolución, donde los infostealers (programas maliciosos diseñados para robar información sensible) han consolidado su presencia como una de las amenazas más persistentes y lucrativas. En la primera mitad de 2025, se ha observado un crecimiento notable en el volumen y diversidad de estas amenazas, con una actividad intensa en regiones como Latinoamérica, especialmente en Brasil, México y Argentina.[2]

Aunque los keyloggers pueden utilizarse con fines legítimos, como el monitoreo parental o empresarial (con el debido consentimiento y marco legal), su uso malicioso es predominante en el ámbito del cibercrimen. La información capturada por los keyloggers, que incluye contraseñas, datos personales, bancarios, correos electrónicos, historiales de búsqueda y capturas de pantalla, es valiosa para los ciberdelincuentes, quienes la utilizan para cometer fraudes, robos de identidad, espionaje corporativo o para facilitar ataques más complejos como el ransomware.

1 https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/que-es-un-keylogger

2 https://www.infobae.com/tecno/2025/07/05/conoce-las-seis-amenazas-que-dominan-el-cibercrimen-en-2025-los-infostealers-se-tomaron-nuestra-privacidad/

Características y tipos de keyloggers

Los keyloggers se clasifican principalmente en dos categorías: basados en software y basados en hardware:

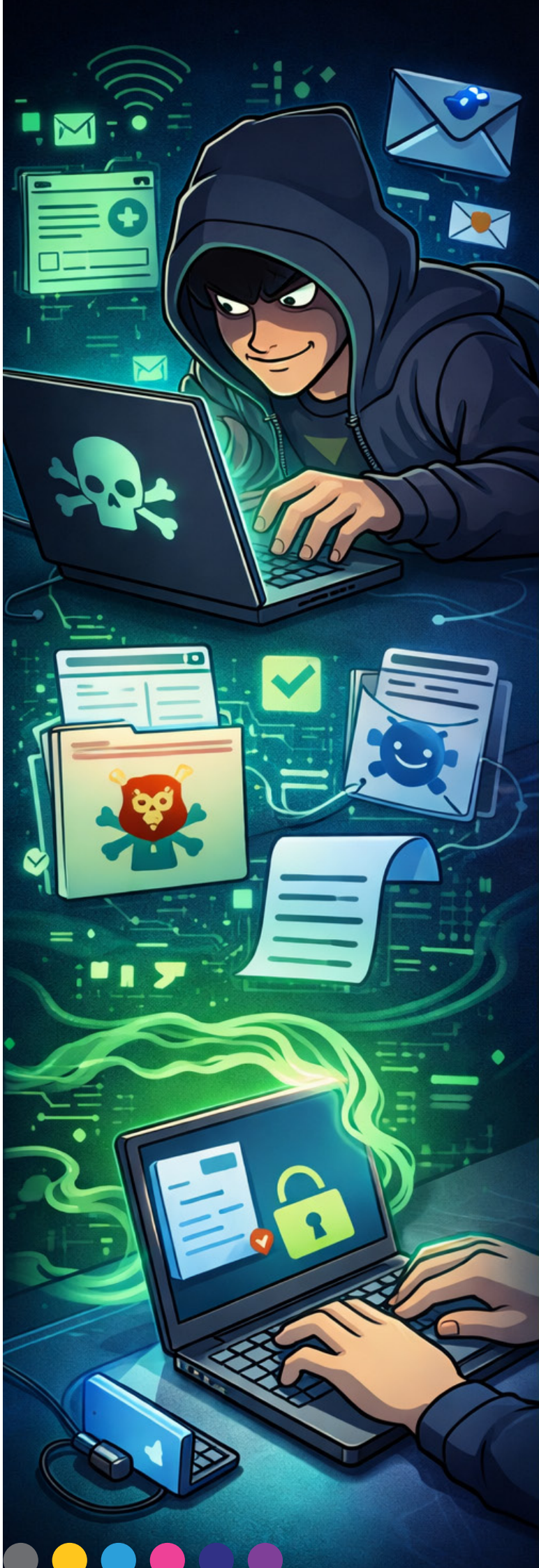
- **Keyloggers basados en software:** Son programas maliciosos que se instalan en el dispositivo de la víctima sin su conocimiento y sin su consentimiento. Operan en segundo plano, registrando las pulsaciones de teclas y enviando la información a un atacante.

- Pueden ser parte de un malware más grande o ser distribuidos a través de correos electrónicos de phishing, descargas de software no confiable o sitios web maliciosos.

- **Keyloggers basados en hardware:** Son dispositivos físicos que se conectan entre el teclado y la computadora, o incluso pueden estar integrados en el propio teclado o en un dispositivo USB. Estos dispositivos registran las pulsaciones de teclas directamente, sin necesidad de instalar software en el sistema operativo.

- Son más difíciles de detectar para el usuario promedio, ya que no aparecen como un proceso en el sistema.

Además de estas categorías principales, existen variantes como los keyloggers inalámbricos, que transmiten los datos de forma remota, y aquellos asociados a software espía que realizan capturas de pantalla o evaden teclados virtuales.



Datos o estudios relevantes

Si bien las estadísticas específicas sobre la prevalencia de keyloggers pueden variar y a menudo se agrupan dentro de categorías más amplias de malware, la actividad de los infostealers, que frecuentemente incluyen funcionalidades de keylogging, ofrece una perspectiva de su impacto. Por ejemplo, **LummaStealer** fue el infostealer más detectado por los sistemas de ESET en Latinoamérica en 2025, con más de 4.000 detecciones únicas. Este malware, distribuido a través de falsos instaladores, malvertising, redes sociales y correos electrónicos infectados, puede incluir módulos de keylogger, exfiltración de datos y ejecución de comandos remotos.

Otros casos documentados de malware que incorporan keylogging incluyen a **Amadey**, que actúa como infostealer y cargador de otras amenazas, y **Formbook** y **Xloader**, que roban credenciales a través de formularios web y capturas de teclado.[3] Estos ejemplos subrayan la sofisticación de las amenazas actuales y la importancia de la vigilancia constante.

2.2. Identificar el riesgo

Señales de alerta (síntomas de infección por keylogger)

Detectar un keylogger puede ser un desafío, ya que están diseñados para operar de forma sigilosa. Sin embargo, existen algunas señales que podrían indicar la presencia de uno en un dispositivo:

- **Rendimiento lento del dispositivo:** La computadora o el celular funcionan más lentos de lo habitual.
- **Retraso en la escritura:** Las palabras tardan en aparecer en la pantalla después de ser tecleadas.
- **Mensajes de error inusuales:** Aparición frecuente de mensajes de error en el sistema operativo o durante la navegación web.
- **Navegación web lenta:** La conexión a internet parece más lenta de lo normal.
- **Actividad inusual en el Administrador de Tareas (Windows):** Procesos desconocidos que consumen una cantidad significativa de memoria o CPU.

3 https://www.infobae.com/tecno/2025/07/05/conoce-las-seis-amenazas-que-dominan-el-cibercrimen-en-2025-los-infostealers-se-tomaron-nuestra-privacidad/

Situaciones o patrones de uso malicioso

Los keyloggers rara vez se instalan por sí solos; generalmente son parte de un ataque más amplio o se distribuyen a través de técnicas de ingeniería social. Las situaciones más comunes que pueden llevar a una infección por keylogger incluyen:

- **Ataques de Phishing:** Correos electrónicos, mensajes o sitios web falsos que imitan a entidades legítimas (bancos, redes sociales, servicios de correo) para engañar al usuario y que descargue un archivo adjunto malicioso o haga clic en un enlace que instala el keylogger.

- **Descargas de software no confiable:** La instalación de programas de fuentes no oficiales, cracks, o software pirata a menudo viene acompañada de malware, incluyendo keyloggers.

- **Malvertising:** Anuncios maliciosos en línea que, al hacer clic, redirigen a sitios web comprometidos que descargan automáticamente el keylogger (drive-by downloads).

- **Dispositivos USB infectados:** Conectar un pendrive o cualquier otro dispositivo USB infectado a una computadora puede transferir el keylogger.

- **Redes Wi-Fi públicas inseguras:** El uso de redes Wi-Fi abiertas y no seguras puede exponer el dispositivo a ataques de intercepción de datos o a la inyección de malware.

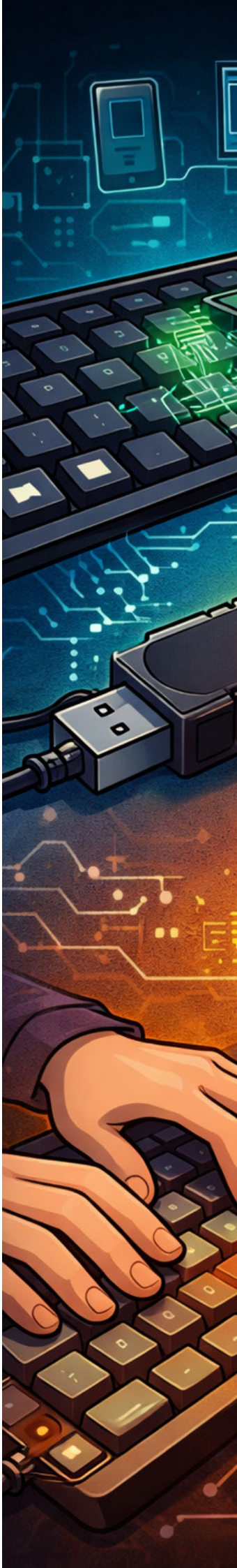
Factores de riesgo en estudiantes

Los estudiantes, debido a su constante interacción con la tecnología y, en ocasiones, a una menor conciencia sobre los riesgos de ciberseguridad, pueden ser particularmente vulnerables. Algunos factores de riesgo específicos incluyen:

- **Uso de software sin supervisión:** La descarga e instalación de aplicaciones o juegos sin el conocimiento o la supervisión de un adulto puede facilitar la instalación de keyloggers.

- **Descargas inseguras:** Acceder a sitios web de descarga de contenido pirata (música, películas, juegos) o de software no verificado, que son fuentes comunes de malware.

- **Uso de dispositivos compartidos o públicos:** Utilizar computadoras en bibliotecas, cibercafés o escuelas sin las debidas precauciones, donde los keyloggers de hardware o software podrían haber sido instalados.



- **Falta de conocimiento sobre phishing:** No reconocer las señales de un correo electrónico o mensaje de phishing, lo que los lleva a hacer clic en enlaces maliciosos o descargar archivos infectados.

- **Configuración de privacidad y seguridad inadecuada:** No configurar correctamente la privacidad en redes sociales o no utilizar contraseñas fuertes y únicas.

Casos simulados

Para ilustrar cómo un keylogger puede afectar a un estudiante, consideremos los siguientes escenarios:

- **Caso 1: El juego descargado.** Un estudiante descarga un juego popular de un sitio web no oficial para evitar pagar. El instalador del juego contiene un keylogger oculto. Una vez instalado, el keylogger comienza a registrar todas las pulsaciones de las teclas. Días después, 3el estudiante intenta acceder a su cuenta de correo electrónico o a una plataforma de juegos en línea, y descubre que su contraseña ha sido cambiada. El atacante, al tener acceso a las credenciales, puede robar información personal, acceder a otras cuentas vinculadas o incluso vender la información en el mercado negro.

- **Caso 2: El correo electrónico de la red social.** Un estudiante recibe un correo electrónico que parece ser de una red social popular, indicando que su cuenta ha sido comprometida y que debe hacer clic en un enlace para verificar su identidad. El enlace redirige a una página de inicio de sesión falsa, donde el estudiante ingresa su nombre de usuario y contraseña. La página falsa no solo captura las credenciales, sino que también descarga un keylogger en el dispositivo del estudiante. Ahora, el atacante no solo tiene acceso a la cuenta de la red social, sino que también puede registrar cualquier otra información que el estudiante escriba, como contraseñas de otras cuentas, conversaciones privadas o información personal.

Consecuencias posibles

Las consecuencias de una infección por keylogger pueden ser graves y abarcar diferentes ámbitos:

- **Privacidad:** La principal consecuencia es la violación de la privacidad. Los keyloggers pueden capturar conversaciones privadas, correos electrónicos, información personal y cualquier otro dato sensible que se escriba en el dispositivo. Esta información puede ser utilizada para extorsión, acoso o simplemente para ser vendida en el mercado negro.

- **Seguridad:** La seguridad de las cuentas en línea se ve comprometida. Los atacantes pueden robar contraseñas de correo electrónico, redes sociales, cuentas bancarias, plataformas de juegos y cualquier otro servicio en línea. Esto puede llevar a la pérdida de acceso a las cuentas, al robo de identidad, a pérdidas financieras y a la propagación de malware a los contactos de la víctima.

- **Legales:** El uso de keyloggers para espiar a otros sin su consentimiento es ilegal en la mayoría de los países y puede tener consecuencias legales para el atacante. Para la víctima, las consecuencias legales pueden surgir si el atacante utiliza su identidad para cometer delitos o si la información robada se utiliza para fines ilícitos.

2.3 Prevenir el riesgo

Estrategias para que el estudiante reconozca y evite keyloggers

La prevención es la mejor defensa contra los keyloggers. Es fundamental que los estudiantes desarrollen hábitos de ciberseguridad sólidos para protegerse. Algunas estrategias clave incluyen:

- **Pensar antes de hacer clic:** Ser escéptico/a ante correos electrónicos, mensajes o enlaces inesperados, especialmente si solicitan información personal o parecen demasiado buenos para ser verdad.
- **Verificar la fuente:** Antes de descargar cualquier software, verificar que la fuente sea oficial y confiable.
- **Utilizar contraseñas seguras y únicas:** Crear contraseñas complejas que combinen letras, números y símbolos, y utilizar una contraseña diferente para cada cuenta.
- **Activar la autenticación de dos factores (2FA):** Añadir una capa adicional de seguridad a las cuentas en línea, que requiere un segundo método de verificación además de la contraseña.
- **Ser consciente de la información que se comparte:** Evitar compartir información personal sensible en línea, especialmente en foros públicos o redes sociales.
- **Utilizar teclados virtuales:** Para ingresar información sensible, como contraseñas bancarias, utilizar los teclados virtuales que ofrecen muchos sitios web, ya que los keyloggers de software a menudo no pueden registrar las pulsaciones de estos teclados.

Keylogger

Buenas prácticas para docentes y familias

Los docentes y las familias desempeñan un papel crucial en la protección de los estudiantes contra los keyloggers. Algunas buenas prácticas incluyen:

- **Instalar y mantener actualizado un software antivirus y anti-malware:** Asegurarse de que todos los dispositivos utilizados por los estudiantes tengan un software de seguridad confiable y que se actualice regularmente.

- **Utilizar un firewall:** Activar el firewall en los dispositivos para bloquear conexiones sospechosas.

- **Mantener el software actualizado:** Instalar las actualizaciones del sistema operativo y de las aplicaciones tan pronto como estén disponibles, ya que a menudo incluyen parches de seguridad que protegen contra las últimas amenazas.

- **Configurar cuentas de usuario con privilegios limitados:** En las computadoras familiares, crear cuentas de usuario estándar para los estudiantes, que no tengan permisos para instalar software. Esto puede evitar que instalen accidentalmente keyloggers u otro malware.

- **Fomentar la comunicación abierta:** Crear un ambiente de confianza donde los estudiantes se sientan cómodos hablando sobre sus experiencias en línea y reportando cualquier actividad sospechosa.

- **Educar sobre los riesgos:** Hablar con los estudiantes sobre los riesgos de los keyloggers y otras amenazas en línea, y enseñarles a reconocer las señales de peligro.

Derechos digitales implicados

La protección contra los keyloggers está directamente relacionada con la protección de los derechos digitales fundamentales, como el derecho a la privacidad y el derecho a la integridad de la información. **El derecho a la privacidad** implica el derecho a controlar la propia información personal y a que no sea recopilada o utilizada sin consentimiento. **El derecho a la integridad** de la información se refiere al derecho a que la información personal sea precisa y no sea alterada o destruida sin autorización. Los keyloggers violan ambos derechos al recopilar información personal sin consentimiento y al poner en riesgo la seguridad y la integridad de esa información.

Herramientas y recursos útiles

Existen numerosas herramientas y recursos disponibles para ayudar a protegerse contra los keyloggers:

- **Software antivirus y antimalware:** Soluciones de seguridad de empresas como Kaspersky, Bitdefender, Malwarebytes y Avast ofrecen protección contra una amplia gama de malware, incluyendo keyloggers.

- **Administradores de contraseñas:** Herramientas como LastPass, 1Password o Bitwarden ayudan a generar y almacenar contraseñas seguras y únicas para cada cuenta, y pueden autocompletar las credenciales sin necesidad de escribirlas, lo que reduce el riesgo de que sean capturadas por un keylogger.

- **Guías y recursos educativos:** Organizaciones como INCIBE (Instituto Nacional de Ciberseguridad de España), la Oficina de Seguridad del Internauta (OSI)[4] y Common Sense Media[5] ofrecen guías, artículos y recursos educativos para padres, docentes y estudiantes sobre ciberseguridad y ciudadanía digital.

4 https://www.incibe.es/incibe

5 https://www.commonsense.org/education/digital-citizenship

3. Enfoque educativo

La enseñanza sobre los keyloggers y la ciberseguridad en general se puede integrar de manera transversal en el currículo escolar, especialmente en asignaturas como Tecnología de la Información y la Comunicación (TIC), Ciudadanía Digital y Ética. En **TIC**, se pueden abordar los aspectos técnicos de los keyloggers, cómo funcionan y cómo protegerse de ellos. En **Ciudadanía Digital,** se puede discutir el impacto de los keyloggers en la privacidad y la seguridad, y cómo ser un ciudadano digital responsable. En Ética, se pueden analizar las implicaciones morales y legales del uso de keyloggers y otras formas de espionaje digital.

Principios pedagógicos

Para que la enseñanza sobre ciberseguridad sea efectiva, es importante utilizar principios pedagógicos que fomenten la participación y el compromiso de los estudiantes. Algunos de estos principios incluyen:

- **Inclusión:** Asegurarse de que todos los estudiantes, independientemente de su nivel de habilidad tecnológica, tengan la oportunidad de aprender y participar.
- **Aprendizaje activo:** Utilizar actividades prácticas, como simulaciones de phishing o análisis de casos, para que los estudiantes puedan aplicar lo que han aprendido en situaciones realistas.
- **Gamificación:** Utilizar elementos de juego, como desafíos, recompensas y competencias, para hacer que el aprendizaje sobre ciberseguridad sea más divertido y atractivo.

Rol del estudiante como protagonista

Es fundamental que los estudiantes asuman un papel activo en su propia educación sobre ciberseguridad. Se les debe alentar a investigar, hacer preguntas, compartir sus experiencias y colaborar con sus compañeros para encontrar soluciones a los desafíos de seguridad en línea. Al convertirse en protagonistas de su propio aprendizaje, los estudiantes no solo adquieren conocimientos y habilidades, sino que también desarrollan un sentido de responsabilidad y autonomía que les permitirá navegar por el mundo digital de manera segura y confiada.

4. Anexos

4.1 Glosario de términos clave

- **Antimalware**: Software que detecta y elimina programas maliciosos como virus, troyanos o keyloggers.
- **Antivirus**: Programa diseñado para proteger los dispositivos contra amenazas informáticas.
- **Autenticación**: Proceso para verificar la identidad de un usuario antes de otorgar acceso.
- **Captura**: Registro de información en pantalla o del teclado, a menudo utilizado por software espía.
- **Cibercrimen**: Actividades delictivas realizadas a través de medios digitales o tecnológicos.
- **Ciberseguridad**: Conjunto de medidas y prácticas para proteger dispositivos e información digital.
- **Descarga**: Transferencia de archivos desde internet al dispositivo; puede contener malware.
- **Espionaje digital**: Obtención secreta de información personal mediante herramientas tecnológicas.
- **Firewall**: Sistema que bloquea accesos no autorizados a una red o dispositivo.
- **Infostealer**: Tipo de malware que roba datos sensibles como contraseñas, mensajes o archivos.
- **Ingeniería social**: Técnica de manipulación para engañar a personas y obtener información confidencial.

- **Keylogger**: Programa o dispositivo que registra todo lo que se escribe en un teclado.

- **Malvertising**: Publicidad en línea maliciosa que puede instalar software no deseado.

- **Malware**: Término general para describir cualquier software dañino o malicioso.

- **Phishing**: Fraude que intenta obtener datos personales haciéndose pasar por una entidad confiable.

- **Privacidad**: Derecho a mantener protegida la información personal y decidir quién accede a ella.

- **Redes públicas**: Conexiones Wi-Fi abiertas, vulnerables a ataques e interceptación de datos.

- **Ransomware**: Malware que bloquea el acceso a los datos y exige un pago para liberarlos.

- **Suplantación de identidad**: Acción de hacerse pasar por otra persona para engañar o cometer fraude.

- **Teclado virtual**: Herramienta digital que permite ingresar texto sin usar el teclado físico, útil contra keyloggers.

5. Referencias Bibliográficas

Argentina.gob.ar. (2025, junio). ¿Qué es un keylogger? https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/que-es-un-keylogger

GoDaddy. (2024, junio 14). *Keyloggers: Qué son, tipos, cómo funcionan y cómo protegerse.* https://www.godaddy.com/resources/es/seguridad/que-es-un-keylogger-y-como-protegerte

Hexn Markets LLC. (2024, julio 11). ¿Qué son los keystroke keyloggers y cómo detectarlos? https://hexn.io/es/blog/-53

Infobae. (2025, 5 de julio). *Conoce las seis amenazas que dominan el cibercrimen en 2025: los infostealers se tomaron nuestra privacidad.* https://www.infobae.com/tecno/2025/07/05/conoce-las-seis-amenazas-que-dominan-el-cibercrimen-en-2025-los-infostealers-se-tomaron-nuestra-privacidad/

LISA Institute. (s. f.). *Qué son los keyloggers: Tipos, modus operandi, medidas preventivas y consejos.* https://www.lisainstitute.com/blogs/blog/keyloggers-tipos-modus-operandi-medidas-preventivas-consejos

Ministerio de Educación,
Deporte y Cultura

@MinisterioEducacionEcuador

@Educacion_Ec

www.educacion.gob.ec