Retorno seguro: consejos de seguridad en línea para estudiantes y educadores (as)

❖ Regresan las clases y este año escolar continúa para muchos(as) en modalidad educativa virtual. ¿Qué tanto nos preparamos para usar de forma segura y responsable el Internet en nuestros hogares y centros educativos?

Retomar la rutina de regreso a la virtualidad para las clases y la socialización de los niños, niñas y adolescentes es una buena oportunidad para establecer nuevos hábitos para el uso seguro de Internet.

No es necesario ser una persona experta en informática para adoptar medidas, lo importante es hacer un pequeño esfuerzo por estar al día, intentar conocer las herramientas y utilizarlas de forma correcta para tener un entorno digital seguro.

Las plataformas y aplicaciones educativas presentan muchas ventajas a la hora de utilizarlas dentro del aula o en la modalidad de clases a distancia, pero el buen uso de estas herramientas es responsabilidad tanto de educadores, padres y madres de familia y de niños, niñas y adolescentes.

Según datos del Ministerio de Educación Pública, después de nueve meses de educación a distancia, este febrero, 1.196.152 estudiantes volvieron a los centros educativos, bajo un modelo de educación combinada en que se alternan las clases presenciales con el seguimiento a distancia, el cual se realiza en su mayoría a través de plataformas tecnológicas y aplicaciones en dispositivos móviles.

Sin embargo, la presencia y uso de las tecnologías y de Internet en las actividades educativas, también abre la puerta a situaciones de riesgo para el personal docente y estudiantil. Algunos de estos riesgos se vinculan a manifestaciones de violencia como son el ciberacoso escolar, la pérdida de **privacidad**, la suplantación **de identidad**, entre otros.

Considerando que muchas de las clases virtuales se realizan mediante diversas plataformas, ha surgido un nuevo riesgo en línea que ocurre cuando una persona se une a una reunión en estas plataforma sin haber sido invitada. Dicho riesgo ha sido bautizado como “Bombing” y se han reportado este tipo de incidentes en todo el mundo. La mayoría de los casos, la persona desconocida que ingresa comparte en la pantalla material relacionado con el abuso y la explotación sexual de menores.

Por eso, tanto en el hogar como en el centro educativo, es importante implementar una serie de pautas que nos permitirán enfrentar de una forma segura y responsable este curso lectivo de la mano de las herramientas tecnológicas.

En el Hogar

Lo primero es procurar contar con un espacio adecuado, bien iluminado, con mesa y silla adecuadas para mantener una buena postura. Ya sea si se conecta desde el celular, una tableta o una computadora, se debe asegurar que estos dispositivos cuenten con un antivirus y que se actualice con regularidad. Siempre es recomendable que las personas adultas mantengan cierta supervisión durante las lecciones para evitar que surjan distracciones con otras herramientas o aplicaciones. Es muy importante que los padres y madres de familia dialoguen previo con las personas estudiantes sobre pautas, consejos y cómo actuar en caso de situaciones de riesgo.

Al acceder a la plataforma, debemos asegurarnos que lo estamos haciendo con los enlaces correctos y a través de redes seguras. En el caso de las clases virtuales, es importante que los y las estudiantes no utilicen sobrenombres o “nicknames” para ingresar, para que la persona docente pueda reconocer que se trata de un miembro de la clase y no una persona extraña. Nunca se deben revelar o compartir contraseñas personales o de acceso a clases con personas que no hayan sido autorizadas por los docentes.

En el centro educativo

Además de las medidas en el hogar, es necesario que se establezcan normas en el Centro Educativo, sobre el uso, el tiempo y la forma de interacción entre estudiantes y docentes durante las lecciones virtuales

Se recomienda designar en cada Centro Educativo a una persona responsable de la seguridad y uso de las redes para que periódicamente evalúe su eficacia y se pueda asegurar tanto a estudiantes como docentes una red protegida para impartir y recibir lecciones.

Además, se debe compartir los enlaces e información de las clases a través de medios oficiales, pero no publicarlas en blogs o redes sociales donde cualquiera pueda tener acceso a la información.

Consejos para docentes

El personal docente debe establecer claramente desde el inicio de las sesiones las reglas que se deben seguir durante la clase virtual, en especial respecto al uso de la palabra, compartir pantalla y realizar apuntes en la pantalla.

Cuando se deba mostrar la pantalla del docente ya sea en la clase o a través de la aplicación, es recomendable compartirla cuando ya se haya seleccionado el contenido deseado evitando mostrar contenido personal o profesional irrelevante para el grupo. También se debe tener cuidado de no teclear las contraseñas a la vista de nadie, impedir que el navegador las recuerde y acordarse de cerrar sesión siempre en las páginas web.

Si durante la clase se deben visualizar videos hay que recordar que si se encuentran en plataformas de Internet, como por ejemplo YouTube, corremos el riesgo de cargar vídeos imprevistos, estar viendo publicidad inapropiada, o tener mayores distracciones con banners publicitarios y sugerencias de otros vídeos. Para evitarlo se puede elegir y copiar la dirección del video previamente y desactivar la reproducción automática.

Cuando se utilizan recursos en línea es importante habilitar la configuración de búsqueda segura o Safesearch en buscadores y asegurarse de los **requisitos legales y términos de uso** antes de utilizar una aplicación online con el alumnado: política de tratamiento de datos personales, la edad mínima de utilización y los derechos sobre los trabajos desarrollados por los alumnos/as para esa plataforma.

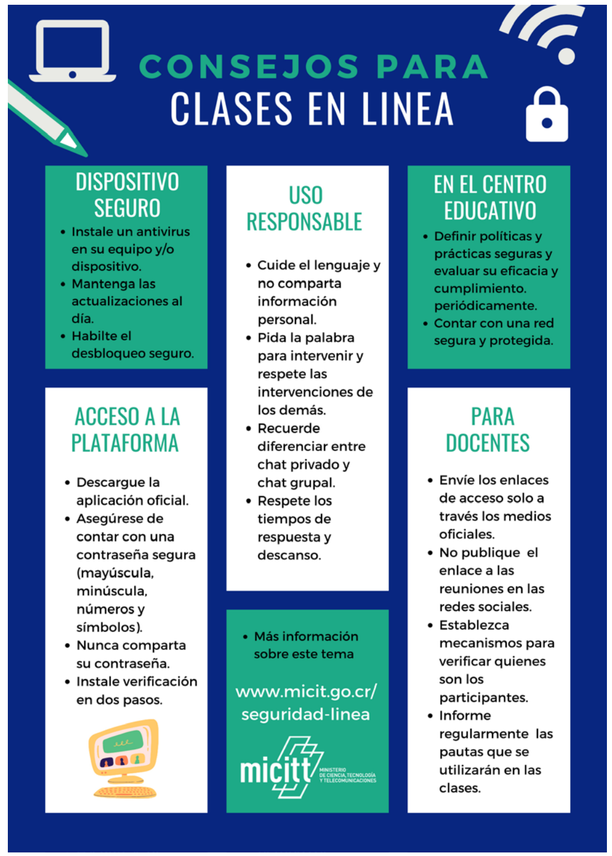
En el enlace:
www.micit.go.cr/seguridad-linea puede consultar más información sobre cómo gestionar los riesgos en línea y aprovechar las oportunidades que nos ofrecen las herramientas tecnológicas en la educación.

Los educadores pueden ayudar a los niños (as) y jóvenes a utilizar la tecnología de manera sensata y segura:

- Asegurarse de que la escuela ha definido políticas y prácticas seguras sobre el acceso y uso de la tecnología dentro de sus instalaciones por los diferentes interesados (as) y cómo se gestiona los incidentes de protección de la infancia en línea.
- Contribuir al desarrollo de las aptitudes digitales y la alfabetización digital mediante la inclusión de la educación cívica digital en sus planes de estudio.
- Es importante incluir conceptos de aprendizaje social y emocional dentro de la enseñanza de la seguridad en línea, ya que estos contribuirán a que los y las estudiantes comprendan y gestionan sus emociones para tener relaciones saludables y respetuosas, tanto en línea como en el mundo real.
- Asegurarse de que todos conocen la política de uso aceptable y cómo se utiliza. Es importante que esa política esté adaptada a las distintas edades.
- Comprobar que la política de la escuela contra el acoso hace referencia a la intimidación por Internet y teléfonos móviles u otros aparatos, y que existen sanciones eficaces para los que no respetan esa política.
- Nombrar una persona coordinadora de la seguridad en línea.
- Asegurarse de que la red de la escuela es segura y está protegida
- Recurrir exclusivamente a un proveedor de servicio Internet acreditado.
- Utilizar herramientas de filtrado/supervisión de contenidos
- Enseñar seguridad en línea a todos los niños y jóvenes y precisar dónde, cómo y cuándo se impartirán.
- Asegurarse de que todo el personal (incluido el personal auxiliar) ha recibido la formación adecuada y que pone periódicamente al día sus conocimientos.
- Tener un único punto de contacto en la escuela y poder recopilar y registrar los incidentes de seguridad en línea, que permitirá a la escuela conocer mejor las cuestiones o tendencias que se deben considerar.

Fuente: Unión Internacional de Telecomunicaciones (UIT) 2020

Fotografías: Freepik Company S.L. - www.freepik.com
Imagen: Elaboración MICITT con información de UIT e IS4K.es



Agradecimiento
Dirección de Evolución y Mercado de Telecomunicaciones
Ministerio de Ciencia, Tecnología y Telecomunicaciones