

LABORATORIO CIBERKIDS

OBJETIVO GENERAL

Desarrollar las competencias digitales de seguridad por medio de la aplicación de una propuesta educativa que integra ambientes virtuales de aprendizaje inmersivo y el desarrollo del pensamiento crítico de los niños@ y adolescente.

OBJETIVOS ESPECIFICO

- Identificar elementos que permitan comprender los riesgos y las amenazas en la red, y conocer medidas de protección y seguridad.
- Comprender términos habituales que permitan proteger activamente los datos personales y la privacidad.
- Desarrollar habilidades para controlar y minimizar riesgos relacionados con la tecnología en relación con la integridad física y psicológicas de los niños@ y adolescente.

IDENTIFICACIÓN DEL PROBLEMA

En la última década, Colombia ha experimentado un vertiginoso avance en el ámbito de las tecnologías de la información y comunicación (TIC), lo que ha impulsado el desarrollo económico y social del país. Sin embargo, este progreso tecnológico ha llevado consigo un aumento significativo en los riesgos y amenazas cibernéticas que afectan a individuos, empresas e instituciones gubernamentales por igual. Ante esta realidad, la ciberseguridad se ha convertido en un pilar fundamental para garantizar la protección de datos, la integridad de la infraestructura digital y el resguardo de la privacidad en Colombia. Los ciberataques, como el robo de información confidencial, el secuestro de datos y los fraudes electrónicos, han demostrado ser un desafío cada vez más sofisticado para la seguridad nacional y el bienestar de la sociedad. No solo las grandes corporaciones y organizaciones gubernamentales están en riesgo, sino también las pequeñas y medianas empresas, así como los ciudadanos comunes, quienes también son blanco de los delincuentes cibernéticos. La falta de preparación y conciencia en materia de ciberseguridad puede tener repercusiones devastadoras en la economía, la estabilidad social y la confianza en las tecnologías digitales.

ALCANCE DE LA PROPUESTA

La propuesta está relacionada con la aplicación de un proceso de capacitación en donde se cuenta con:

- Fase de preparación previa: Se establecen las instituciones en donde se va a aplicar la propuesta, y se identifican los individuos participantes niños y

adolescentes. En esta fase también se establecen los roles y las responsabilidades en la implementación de la propuesta.

- Fase de introducción: Se harán las capacitaciones pertinentes a los responsables de la implementación y se gestionarán los recursos tecnológicos correspondientes necesarios para la implementación.
- Fase de implementación: Se desarrollarán 5 sesiones (2 horas de aplicación, cada una), en donde se abordarán los temas de Ciber acoso (Bullying), Sexting, Robo de datos y noticias falsas, en donde el desarrollo de las actividades se complementa con un proceso de verificación de saberes que nos permitirá ir avanzando en la implementación.
- Fase de retroalimentación: Será un proceso constante que se iniciará al comenzar la implementación, de la propuesta por medio de la aplicación de una prueba diagnóstica y una prueba de saberes adquiridos. Ello permitirá identificar el avance de los participantes en el conocimiento de las competencias digitales sobre la seguridad. Al finalizar la implementación cada participante recibirá un título de CIBERGUARDIAN 1, como medio de reconocimiento por la labor realizada.

Para la aplicación de la propuesta es necesario un equipo electrónico (computador, Tablet, celular), internet y acceso a la plataforma, gratuita, Roblox.

INDICADORES DE RETROALIMENTACIÓN DEL PROYECTO

Para la retroalimentación general del proyecto se han establecido los siguientes indicadores de impacto en el proyecto:

- Fase de Preparación:
 1. Número de individuos impactados
 2. Porcentaje de participación por genero
 3. Porcentaje de participación por edades
 4. Porcentaje de tipo de participación (Directivo, Líder gestor, Participante)
 5. Número de dispositivos aprovechados para la implementación
 6. Tipo de dispositivos utilizados

- Fase de Introducción
 7. Número de líderes capacitados
 8. Porcentaje de participación por genero de líderes
 9. Porcentaje de participación por edades

- Fase de Implementación
 10. Índice de conocimientos previos sobre las temáticas
 11. Índice de conocimiento adquiridos sobre las temáticas

- Fase de implementación

Se generan las conclusiones de cada uno de los indicadores, con un proceso que permitirá generar los planes de mejoramiento para nuevas intervenciones.

¿QUÉ APRENDEREMOS?

01

Comprender situaciones que vulneran la ciberseguridad de las personas.

02

Establecer estrategias para poder atacar los problemas de ciberseguridad que se pueden presentar

03

Identificar y comprender definiciones importantes en el tema de la ciberseguridad.

SABEMOS QUE TIENES DUDAS... PEROTE NECESITAMOS

¡No estas solo!
somos muchas personas
interesadas en protegerte
a tí y a las personas que
más quieres.

Con estas actividades
encontrarás algunas
herramientas para ayudar a
otros en su ciberseguridad!!!
HAGÁMOSLO!!!

**Pondré todo de mí para ser un
ciberguardian**



American Company Col SAS. es una empresa especializada en el área de seguridad, con filosofía **PREVENTIVA**; nuestro principal interés radica en **ADELANTARNOS A CUALQUIER FENÓMENO QUE ATENTE CONTRA LA**



INTEGRIDAD PERSONAL O LOS INTERESES ECONÓMICOS DE NUESTROS CLIENTES, observando una constante actitud proactiva.

AMERICAN COMPANY COL SAS como una de las empresas líderes en la instalación y mantenimiento de los procesos de seguridad, ofrece la verificación plena de los diferentes aspectos que su compañía considere necesario para la no vulneración de intereses negativos que puedan afectar el desarrollo de importantes procesos de la compañía.