Centro de Respuestas a Incidentes Informáticos
CIP - CSIRT Académico UNAD

Boletín Informativo
Número **Cinco**

¿A qué están expuestos Niños y Jóvenes en Internet?

ECBπ
Escuela de Ciencias Básicas, Tecnología e Ingeniería

VIEM
Vicerrectoría de Innovación y Emprendimiento

Semillero de Investigación
Ceros y Unos

Medio de Divulgación del Centro de Respuestas a Incidentes Informáticos: CIP – CSIRT Académico UNAD

E-boletín Informativo CIP- CSIRT Académico UNAD

Edición electrónica, financiada por la Universidad Nacional Abierta y a Distancia (UNAD)

Medio de divulgación: Correo Electrónico, Sitio Web

Incluye: Noticias, alertas o informes relacionados con la disciplina de la ciberseguridad

Número Cinco
Mayo de 2022

Universidad Nacional Abierta y a Distancia (UNAD)
Vicerrectoría de Innovación y Emprendimiento (VIEM)
Escuela de Ciencias Básicas Tecnología Ingeniería (ECBTI)
CIP – CSIRT Académico UNAD

Vicerrectoría de Innovación y Emprendimiento (VIEM)
Ing. Andrés Ernesto Salinas - Vicerrector

Escuela de Ciencias Básicas Tecnología e Ingeniería (ECBTI)
Ing. Claudio Camilo González Clavijo – Decano

Especialización en Seguridad Informática (ECBTI)
Ing. Sonia Ximena Moreno Molano – Líder Programa de Especialización en Seguridad Informática

Semillero de Investigación Ceros y Unos, adscrito al Grupo de Byte InDesign

Centro de Respuestas a Incidentes Informáticos
CIP – CSIRT Académico UNAD
Ing. Luis Fernando Zambrano Hernández – Director CIP CSIRT Académico UNAD

Responsable de la Edición
Ing. Luis Fernando Zambrano Hernández

Estado legal:
Periodicidad: Quincenal
ISSN: **2806-0164**

Universidad Nacional Abierta y a Distancia
Calle 14 sur No. 14-23 |Bogotá D.C
Correo electrónico: csirt@unad.edu.co
Página web: https://csirt.unad.edu.co

Tabla de Contenido

Boletín informativo Número 5

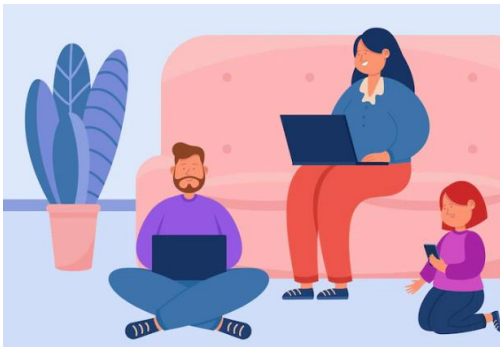
Mayo 3 de 2022

¿A qué están expuestos Niños y Jóvenes en Internet?

Autor: Luis Fernando Zambrano Hernández
ORCID: https://orcid.org/0000-0002-4690-3526

Introducción

El Instituto Colombiano de Bienestar Familiar – ICBF, en artículo publicado con fecha de 17 de febrero de 2022, plantea cuatros riesgos cibernéticos a los cuales están expuestos los menores de edad en el momento de usar Internet o algún tipo de red Social.[1] Además indica que el tiempo de navegación de un menor en Internet supera las 5 horas diarias. Esto, sin duda alguna genera la exposición del menor frente a un ataque informático.



Recuperado de: https://www.freepik.es/

El presente Boletín, contextualiza los siguientes riesgos Cibernéticos

- Ciber dependencia
- Ciberacoso
- Grooming
- Retos Virales o Challenger

[1] https://www.icbf.gov.co/mis-manos-te-ensenan/conoce-los-riesgos-ciberneticos-los-que-se-enfrentan-los-ninos-y-ninas-y-como

Desarrollo

El ICBF, propone que la familias o personas que cuidan a los menores, fortalezcan los canales de comunicación a partir de la confianza con el ánimo de poder generar espacios de dialogo donde: en conjunto se planteen pautas relacionadas con el buen uso de internet y cómo si se presentará algún tipo de evento se pueda denunciar a través de la Línea **141** de protección a niños, niñas y adolescentes o al CAI Virtual de la Policía Nacional de Colombia[2].

A continuación, se relacionan otras líneas de atención planteadas por el ICBF:

Línea gratuita nacional ICBF: **018000 91 80 80**
Disponible lunes a viernes 8:00 am a 5:00 pm

PBX: **+57 601 4377630**
Disponible de lunes a viernes de 8:00 a.m. a 5:00 p.m.

Ahora bien, teniendo presente el propósito de este boletín, el CSIRT Académico UNAD presenta en qué consisten los riesgos mencionados.

Ciber dependencia:

Son comportamientos convertidos en imprescindibles respecto al uso de una herramienta digital, bien sea: computador, celular o consolas de video juegos. donde se invierte tiempo excesivo, generando interferencias en las actividades de la vida cotidiana[3].

¿Cómo identificar a un ciber dependiente?

- Presenta ansiedad por no estar con el dispositivo
- Puede buscar reconocimiento en grupos o redes sociales, creando publicaciones que generen expectativa
- Presenta necesidad de tener asociadas varias cuentas de redes sociales o correos electrónicos

[2] https://caivirtual.policia.gov.co/contenido/adenunciar-1

[3] https://www.enticconfio.gov.co/La_familia_clave_para_combatir_la_ciberdependencia#:~:text=La%20ciberdependencia%20se%20entiende%20como,curso%20normal%20de%20la%20vida.

Ciberacoso

La UNICEF lo presenta como *"acoso o intimidación por medio de las tecnologías digitales"*[4]. Este se puede presentar a través de redes sociales, plataformas de juegos o a través de telefonía celular. El objetivo del atacante es el de atemorizar a la víctima o buscar su humillación realizando las siguientes acciones:

- Difusión de imágenes o videos comprometedores de la víctima a través de medios digitales
- Envió de mensajes dirigidos a la víctima que contengan mensajes hirientes o amenazantes

UNICEF en al artículo relacionado como recurso bibliográfico indica cuales son las consecuencias que presenta una persona que sufre de ciber acoso:

- De forma mental: *"Se siente preocupada, avergonzada, estúpida y hasta asustada o enfadada"*
- De forma emocional: "Se siente avergonzada y pierde interés en lo que le gusta"
- De forma física: *"Se siente cansada (pierde el sueño) o sufre dolores de estómago y de cabeza"*

Grooming

Este riesgo se cataloga como la acción a través de un medio digital que ejerce un adulto al acosar de forma sexual a un menor de edad[5]. Para esta acción el atacante suele crear perfiles falsos, por lo general haciéndose pasar por un joven de la edad de la víctima con el fin de generar confianza y acercamiento, su objetivo es el de obtener de la víctima:

- Imágenes que atenten contra su reputación. Por lo general de contenido o material de abuso sexual
- Propiciar encuentros físicos o personales con el fin de cometer algún tipo de abuso sexual

Esta acción puede generar en la victima consecuencias de orden físicas o psicológicas.

La Organización **Save The Children,** muestra cuales pueden ser las fases que un **atacante** realiza en el momento de acercarse a su víctima[6]:

- **Crea un vínculo de confianza:** a través de engaños o sobornos, el ciber atacante busca contactar a su víctima logrando generar un canal de confianza donde la victima expone sus problemas, para luego, a partir de esta información chantajearla.
- **Aislar a la víctima:** intentando desasociarlo de la relación de confianza con su familia, dejándolo desprotegido en insistiéndole a la víctima que todo quede en secreto.
- **Valora su exposición al riesgo:** preguntando a la víctima si algún familiar cercano o conocido, sabe de su relación con él e intenta conocer si otra persona accede al dispositivo con el que la víctima interactúa.
- **Genera conversaciones relacionadas con sexo:** buscando que la víctima conozca vocabulario.
- **Realiza peticiones de naturaleza sexual:** En esta fase, el atacante ejecuta su objetivo, el cual es el de manipular a su víctima para que acceda a sus peticiones. La manipulación, las amenazas y el chantaje toman la relevancia para que la víctima acceda.

Retos Virales o Challenger

Este tipo de riesgo de riesgo busca que la víctima imite una acción vista en video a través de redes sociales, con el fin de realizarla y subir el contenido a plataformas digitales. Por lo general al finalizar el reto se **postula a otra víctima** para que lo realice[7].

Estos retos pueden estar relacionados con:

- Pérdida de peso
- Ingesta o consumo de productos peligrosos
- Autolesiones o suicido

[4] https://www.unicef.org/es/end-violence/ciberacoso-que-es-y-como-detenerlo
[5] https://www.argentina.gob.ar/grooming
[6] https://www.savethechildren.es/actualidad/grooming-que-es-como-detectarlo-y-prevenirlo
[7] https://www.asociacionrea.org/peligros-en-internet-retos-virales/

Buenas prácticas para la protección de menores en internet

Es importante que niños y jóvenes a través de sus padres puedan realizar las siguientes acciones:

- Establecer canales de comunicación entre padres e hijos, donde se plantee y debata los aspectos positivos y negativos del uso de Internet y de las redes sociales.
- Hacer uso de herramientas de control parental[8] en las redes de datos del hogar o en los sistemas operativos donde los menores tengan acceso para la conexión hacia internet
- Acordar horarios para acceder a redes sociales o Internet teniendo presente que esta actividad podría ser acompañada o supervisada por el responsable del menor
- Generar la consciencia de revisar en conjunto y de forma aleatoria el dispositivo tecnológico con el cual está accediendo a Internet o a redes sociales.

Canales de comunicación

El CIP CSIRT Académico UNAD, actualmente cuenta con los siguientes canales de comunicación:

- **Correo**: csirt@unad.edu.co
- **Twitter**: @csirtunad
- **Página web**: https://csirt.unad.edu.co

[8] *"Mecanismo usado por adultos para controlar en diferentes sitios web, sistemas operativos o equipos el acceso y uso que los menores de edad le dan a internet"* Recuperado de: https://edu.gcfglobal.org/es/seguridad-en-internet/que-es-el-control-parental/1/

Recursos Bibliográficos Consultados

[1] Conoce los riesgos cibernéticos a los que se enfrentan los niños y niñas y cómo prevenirlos [en línea]. ICBF [fecha de consulta: 30/04/2022] Disponible en: https://www.icbf.gov.co/mis-manos-te-ensenan/conoce-los-riesgos-ciberneticos-los-que-se-enfrentan-los-ninos-y-ninas-y-como

[2] Adenunciar! [en línea]. CAI Virtual [fecha de consulta: 30/04/2022] Disponible en: https://caivirtual.policia.gov.co/contenido/adenunciar-1

[3] La familia: clave para combatir la ciber dependencia [en línea]. MINTIC. [fecha de consulta: 30/04/2022] Disponible en: https://www.enticconfio.gov.co/La_familia_clave_para_combatir_la_ciberdependencia#:~:text=La%20ciberdependencia%20se%20entiende%20como,curso%20normal%20de%20la%20vida.

[4] Ciberacoso: Qué es y cómo detenerlo [en línea]. UNICEF [fecha de consulta: 30/04/2022] Disponible en: https://www.unicef.org/es/end-violence/ciberacoso-que-es-y-como-detenerlo

[5] Grooming [en línea]. Gobierno de Argentina [fecha de consulta: 30/04/2022] Disponible en: https://www.argentina.gob.ar/grooming

[6] Grooming Qué Es, Cómo Detectarlo Y Prevenirlo [en línea]. Save The Children [fecha de consulta: 30/04/2022] Disponible en: https://www.savethechildren.es/actualidad/grooming-que-es-como-detectarlo-y-prevenirlo

[7] Peligros en Internet: Retos virales [en línea]. REA [fecha de consulta: 30/04/2022] Disponible en: https://www.asociacionrea.org/peligros-en-internet-retos-virales/

[8] ¿Qué es el control parental? [en línea]. GCF Global [fecha de consulta: 30/04/2022] Disponible en: https://edu.gcfglobal.org/es/seguridad-en-internet/que-es-el-control-parental/1/