RIESGOS ASOCIADOS A INTERNET

ASTRID FABIOLA PINZÓN CUEVAS
JENNY ALEXANDRA BARÓN BOHORQUEZ

MAESTRÍA EN GESTIÓN DE LA TECNOLOGÍA EDUCATIVA
UNIVERSIDAD DE SANTANDER - UDES
2018

RIESGOS ASOCIADOS A INTERNET

Estudiantes:
Astrid Fabiola Pinzón Cuevas
Jenny Alexandra Barón Bohórquez

Docente: Mg. Paul Andrés Ospina Marín
Módulo: SISTEMAS E INFORMÁTICA

MAESTRÍA EN GESTIÓN DE LA TECNOLOGÍA EDUCATIVA
UNIVERSIDAD DE SANTANDER - UDES
2018

INTRODUCCION

Actualmente las instituciones educativas se ven en la necesidad de incorporar en sus establecimientos el uso del internet así como su buen manejo aplicando campañas de prevención y corrección en cuanto a los riesgos que se presentan ya sea por la cantidad de información la cual se provee sin responsabilidad, como la información errada que se obtiene mediante las redes sociales, afectando considerablemente e especial a la juventud. Por tal razón es importante conocer a fondo cada uno de los riesgos que se presentan con el fin de buscar alternativas de prevención y corrección.

RIESGOS ASOCIADOS A INTERNET

MATERIAL INAPROPIADO

Generalmente se trata de contenido pornográfico e información no censurada

Estrategias de mitigación

- Capacitación constante al personal para el reconocimiento de utilización peligrosa en el internet.
- Instalación de dispositivos de bloqueo a páginas sospechosas.
- Charlas a estudiantes sobre las consecuencias de envío y recepción de este tipo de información

CIBERACOSO O CYBERBLLING

Se trata de acosar o agredir a alguien con el ánimo de afectarlo psicológicamente, además de ridiculizarlo, criticarlo y excluirlo de un grupo, lo cual conlleva a que en ocasiones, estas víctimas tomen decisiones negativas que afectan significativamente sus vidas y las de sus familiares.

Estrategias de mitigación

- Vigilancia del uso de redes por parte de los estudiantes.
- Explicación a los jóvenes sobre las consecuencias legales que se acarrean al realizar dicha práctica.
- Diseñar campañas de prevención y redes de apoyo a estudiantes afectados.
-

GROOMING

Práctica de acoso y abuso sexual en contra de niños y jóvenes a través de redes sociales en donde los groomers (personas que buscan hacer daño a los menores) pretenden ganarse la confianza de los niños brindándoles atención, ofreciendo beneficios a cambio y mostrando una imagen que no es.

Buscan implementar miedo a los menores amenazándolos con exponer “secretos”.

Estrategias de mitigación

- Dialogo abierto y frecuente con los estudiantes.
- Instalación de software de control parental en el computador.
- No brindar confianza perfiles desconocidos.

MALWARE

Son programas informáticos diseñados por delincuentes para causar perjuicio, robando la información en general o tomando el control del equipo. Una de sus características en pasar inadvertido ante el usuario, lo cual no convierte en algo aún mas peligroso.

CLASES

Virus: Inserta parte de su código interno dentro de programas legítimos.

Gusano: Código malicioso diseñado para propagarse a través de cualquier medio.

Troyano: Código maliciosos que no se propaga automáticamente ni tampoco afecta los archivos.

Estrategias de mitigación

- Evitar descargar programas desconocidos.
- No seguir enlaces provenientes de correos o publicidad.
- Mantener un sistema operativo actualizado, así como el antivirus.
- Eliminar códigos maliciosos de forma constante.

SEXTING

Envío de mensajes sexuales por medio de celulares o computadores.

Estrategias de mitigación

- Dialogar con los estudiantes acerca de las consecuencias futuras que implica la divulgación de fotos o videos privados, ya sea por robo o extravío del dispositivo o por voluntad de su propietario, aclarando que la intensión de las personas puede cambiar de acuerdo a las circunstancias.
- Explicación acerca de que el contenido que se envía mediante el internet, queda cifrado en la multimedia así éste se borre, lo cual no es seguro.
- Acompañamiento continuo sin invasión a la privacidad.

SCAM

Consiste en estafas o fraudes por medios electrónicos.

Las cadenas de correos electrónicos engañosos en donde se pide un aporte económico o se ofrece un producto, servicio falso o estafa haciéndose pasar por la necesidad de algún familiar.

Estrategias de mitigación

- No brindar información personal, familiar o financiera a personas desconocidas.
- Documentarse de forma completa acerca de las paginas y perfiles que dien promocionar diversos productos.

ACCESO A MATERIAL INAPROPIADO

Estudiantes acceden a sitios pornográficos o contenidos de carácter delictivo o peligroso.

Estrategias de mitigación

- Entrenamiento a todo el personal de la institución en reconocimiento de paginas con intensiones e información negativa.
- Vigilancia continua mientras los estudiantes acceden a la red.
- Bloqueo de páginas inadecuadas.
- Dialogo con los padres de familia, acerca de la importancia de tener el computador en una zona visible de la vivienda.

INVASION DE LA PRIVACIDAD

Utilización de información personal para cometer robos o extorsiones.

Estrategias de mitigación

- Explicar a los estudiantes la importancia de abstenerse a dar información en especial en redes sociales o perfiles desconocidos.
- Enseñar a los estudiantes a desconfiar y no brindar información de ningún tipo a personas no conocidas

USO INCORRECTO DEL TIEMPO LIBRE

Los estudiantes permanecen gran parte de su tiempo utilizando la tecnología, ya sea en sus celulares o computadores, dejando de lado otro tipo de actividades relevantes en su cotidianidad, llegando a sufrir algún tipo de adicción, llevándolos en ocasiones a tener problemas de salud.

Estrategias de mitigación

- Vigilancia y seguimiento por parte de los padres de familia y docentes.
- Evitar ubicar los aparatos tecnológicos en la habitación de los menores.