Tecnología, Informática y Sociedad: Construyendo una Huella Digital Responsable

UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS
FACULTAD DE CIENCIAS Y EDUCACIÓN

Facultad de Ciencias y Educación

Maestría en Educación en Tecnología

Autores:

Edith Cortés

William Camilo Rodríguez Mejía

Maestría en Educación en Tecnología

2024

Índice

Índice **3**
Tabla de figuras **3**
Introducción **5**
Descripción General del Curso: Tecnología, Informática y Sociedad: Construyendo una Huella Digital Responsable **7**
PRIMER MOMENTO: Introducción al Curso 7
PRIMER MOMENTO: Exploración Inicial 7
SEGUNDO MOMENTO: Conexión y Motivación 7
TERCER MOMENTO: 1 Interacción y Construcción 8
TERCER MOMENTO: 2 Interacción y Construcción 8
TERCER MOMENTO: 3 Interacción y Construcción 8
Tecnología, Informática y Sociedad: Construyendo una Huella Digital responsable **9**
Tecnología, Informática y Sociedad **9**
Perspectivas de formación 9
Perspectiva Crítica: Evaluando el Impacto Social y Ambiental de la Tecnología. 9
Perspectiva Ética: Desarrollando una postura ética frente al uso responsable de la tecnología 10
Perspectiva Política: Participación juvenil en la toma de decisiones tecnológicas 10
Protección Frente a Delitos Digitales en Colombia: Estrategias Legales y Educativas para Combatir Delitos Informáticos 10
Delitos Informáticos en Colombia: Tipos de Cibercrimen y su Impacto en los Jóvenes 11
Tipos de Delitos Informáticos 12
Modalidades de Delitos: Modos Operandi de los Delitos Digitales más Comunes 13
Estrategias de Prevención y Atención: Acciones para Prevenir y Responder a Delitos Cibernéticos 13
Huellas Digitales: Gestionando tu Huella Digital de Manera Responsable y Segura 15
Referencias **16**

Tabla de figuras

Figura 1 Delitos cibernéticos más denunciados por la ciudadanía en Colombia *11*

Introducción

En la era digital actual, nuestras vidas están más interconectadas que nunca. Cada acción que realizamos en línea deja una huella, desde nuestras interacciones en redes sociales, hasta las compras que hacemos y los sitios web que visitamos. Esta **huella digital** nos representa en el vasto mundo virtual y, si bien puede traernos muchos beneficios, también nos expone a riesgos que es necesario conocer y gestionar.

La privacidad y seguridad de los datos se han convertido en aspectos fundamentales en la era digital, donde la rápida expansión de la tecnología y la interconectividad global han transformado profundamente la forma en que interactuamos, almacenamos y compartimos información. Desde la protección de datos personales hasta la seguridad de infraestructuras críticas, las organizaciones y los individuos enfrentan desafíos cada vez más complejos debido al incremento de ciberamenazas y violaciones de seguridad.

Este documento explora de manera integral las amenazas más relevantes a la privacidad y seguridad de los datos, así como las soluciones técnicas y estrategias necesarias para mitigar estos riesgos. Asimismo, se destaca la importancia de la educación y la concienciación, no solo en el ámbito profesional, sino también a nivel de usuario, como componentes clave para fomentar una cultura de seguridad y responsabilidad en el entorno digital.

A través de un análisis de casos emblemáticos y una discusión sobre tecnologías emergentes, como la inteligencia artificial y el blockchain, se presenta un enfoque holístico para abordar los desafíos actuales. Además, se subraya el papel crucial que desempeñan organizaciones que han liderado esfuerzos educativos para capacitar a jóvenes y niños en el uso seguro y consciente de la tecnología. Este trabajo

tiene como objetivo no solo resaltar la necesidad de implementar medidas de seguridad más robustas, sino también de cultivar una ciudadanía digital responsable que pueda enfrentar los retos del futuro tecnológico.

Este Entorno Virtual de Aprendizaje (EVA) tiene como objetivo ayudarte a comprender cómo tus acciones en línea pueden tener implicaciones éticas, sociales y de seguridad tanto para ti como para tu entorno. A lo largo del curso, aprenderás a gestionar de forma crítica y responsable tu **huella digital**, protegiendo tu privacidad y seguridad, mientras actúas de forma ética en el mundo digital.

Descripción General del Curso: Tecnología, Informática y Sociedad: Construyendo una Huella Digital Responsable

Este curso está diseñado para explorar y desarrollar competencias en el uso ético y seguro de la tecnología dentro del contexto educativo. A través de un enfoque interactivo y participativo, los estudiantes identificarán, analizarán y reflexionarán sobre los riesgos tecnológicos que enfrentan en su vida diaria, promoviendo una conciencia crítica sobre el impacto de la tecnología en la sociedad, la ética y el medio ambiente.

PRIMER MOMENTO: Introducción al Curso

Se presentará el objetivo del curso, su relevancia y los temas que se abordarán. Se establecerá un contexto para el aprendizaje, fomentando la curiosidad y la motivación en los estudiantes.

PRIMER MOMENTO: Exploración Inicial

Los estudiantes realizarán una exploración inicial sobre los conceptos de tecnología, informática y huella digital. Se llevarán a cabo discusiones grupales para identificar sus conocimientos previos y expectativas respecto al curso.

SEGUNDO MOMENTO: Conexión y Motivación

Se utilizarán recursos multimedia y actividades interactivas para conectar los temas del curso con la vida cotidiana de los estudiantes. Se buscará motivar a los participantes a involucrarse activamente en el proceso de aprendizaje.

TERCER MOMENTO: 1 Interacción y Construcción

Los estudiantes trabajarán en grupos para identificar y comprender los riesgos éticos, sociales y ambientales asociados con el uso de la tecnología. Se fomentará la creatividad en la creación de carteles ilustrativos que sensibilicen sobre las consecuencias del uso inapropiado de la tecnología.

TERCER MOMENTO: 2 Interacción y Construcción

En este momento, los estudiantes desarrollarán un protocolo de seguridad personal y uso ético de la tecnología. Este protocolo abordará medidas para proteger la información personal y fomentar un comportamiento responsable en línea, presentándose junto con un recurso multimedia.

TERCER MOMENTO: 3 Interacción y Construcción

Finalmente, los estudiantes presentarán sus protocolos y participarán en un debate crítico, evaluando la aplicabilidad y efectividad de las estrategias propuestas. Este momento culminará con una reflexión personal sobre cómo aplicar lo aprendido en su vida diaria.

Tecnología, Informática y Sociedad:

Construyendo una Huella Digital responsable

Tecnología, Informática y Sociedad

En la IED San Cayetano, el componente de Tecnología, Informática y Sociedad busca formar a los estudiantes en perspectiva crítica, ética y política. Tecnología se refiere a las herramientas y sistemas que facilitan la creación y uso de información, mientras que Informática abarca el manejo de datos y la programación, capacitando a los jóvenes para desarrollar soluciones digitales. La Sociedad examina el contexto social y cultural en el que se utilizan estas tecnologías, enfatizando la importancia de tomar decisiones responsables. Esta formación integral es crucial para que los estudiantes se conviertan en ciudadanos críticos y responsables en un mundo donde los delitos digitales son cada vez más comunes.

Perspectivas de formación

Perspectiva Crítica: Evaluando el Impacto Social y Ambiental de la Tecnología.

- Fomentar el pensamiento crítico: Es esencial que los estudiantes analicen el impacto de la tecnología en la sociedad y el medio ambiente, lo que les ayudará a comprender los riesgos asociados con su uso.
- Promover la sensibilización: Los jóvenes deben ser conscientes de los efectos sociales y culturales de la tecnología, evaluando las herramientas que utilizan y reconociendo potenciales amenazas, como los delitos informáticos.

Perspectiva Ética: Desarrollando una postura ética frente al uso responsable de la tecnología

- Generar criterios para valorar el uso de la tecnología: Esto implica reconocer su potencial, así como sus impactos negativos en la vida cotidiana.
- Desarrollar una postura ética: Los estudiantes deben tomar decisiones informadas que consideren las consecuencias sociales, ambientales y culturales de sus acciones, incluyendo la responsabilidad de reportar y prevenir delitos digitales.

Perspectiva Política: Participación juvenil en la toma de decisiones tecnológicas

- Involucrar a los jóvenes en la toma de decisiones: Es fundamental que los estudiantes participen en discusiones sobre la generación y uso de productos tecnológicos, así como en el debate público sobre políticas que busquen mitigar los impactos negativos de la tecnología.
- Fomentar la participación: Al involucrarse en la formulación de políticas, los estudiantes pueden ayudar a promover un uso responsable y sostenible de la tecnología, apoyando iniciativas como la Cartilla Metodológica de Atención de Delitos Informáticos, desarrollada por la fiscalía general de la Nación y la Policía Nacional.

Protección Frente a Delitos Digitales en Colombia: Estrategias Legales y Educativas para Combatir Delitos Informáticos

En Colombia, la protección de los ciudadanos contra delitos digitales ha adquirido una relevancia significativa en las políticas de seguridad y justicia. Varios actores trabajan conjuntamente para desarrollar estrategias efectivas en la lucha contra

estos delitos, reflejando la necesidad de una educación integral en el ámbito de la tecnología. Algunos aspectos relevantes de la Cartilla Metodológica de Atención de Delitos Informáticos son:

La cartilla busca proporcionar un marco metodológico claro para la atención y manejo de delitos informáticos, unificando criterios y procedimientos entre los diferentes actores involucrados en la investigación y prevención.

Actores Involucrados

- Fiscalía General de la Nación: Encargada de investigar y judicializar delitos informáticos.
- Policía Nacional: Responsable de la recolección de evidencias y atención inicial de denuncias.
- Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC): Promueve la educación y prevención sobre delitos informáticos.
- Organizaciones de la sociedad civil: Apoyan en la sensibilización sobre el uso seguro de las tecnologías.

Delitos Informáticos en Colombia: Tipos de Cibercrimen y su Impacto en los Jóvenes

- Ataques a DNS: Vulnerabilidad en el protocolo IP que redirige el tráfico de usuarios a sitios web maliciosos.
- Ataque de Denegación de Servicios (DoS) y Ataque Distribuido de Denegación de Servicios (DDoS): Bloqueo de un servidor mediante la sobrecarga de recursos.
- Atacante Interno: Ataques realizados por personas dentro de la organización, como fraudes o robos.

- Banker: Malware dirigido a instituciones financieras para robar información.
- BEC (Business Email Compromise): Fraude mediante correos electrónicos que engañan a las personas para que envíen dinero o información confidencial.
- Botnet: Red de dispositivos infectados controlados remotamente para llevar a cabo ataques masivos.
- Buffer Overflow: Ataque que provoca un desbordamiento de la memoria, permitiendo al atacante tomar el control del sistema.
- Cambiazo: Fraude que ocurre durante transacciones con tarjetas, donde se intercambia la tarjeta original por otra similar.
- Carding: Uso no autorizado de datos de tarjetas de crédito.
- Phishing: Técnica de ingeniería social que busca robar información confidencial mediante correos falsos.
- Ransomware: Malware que cifra archivos y exige un rescate para liberarlos.
- Smishing: Phishing a través de mensajes de texto.
- Spoofing: Suplantación de identidad para obtener información sensible.

Tipos de Delitos Informáticos

La cartilla clasifica los delitos informáticos en categorías que incluyen, entre otros:

- Fraude electrónico: Uso de medios digitales para engañar y obtener beneficios económicos.
- Acoso cibernético: Hostigamiento a través de plataformas digitales.
- Phishing: Robar información personal mediante engaños.

- Malware y virus: Software malicioso que afecta la seguridad de los dispositivos.

Modalidades de Delitos: Modos Operandi de los Delitos Digitales más Comunes

Las modalidades varían según la técnica utilizada, como:

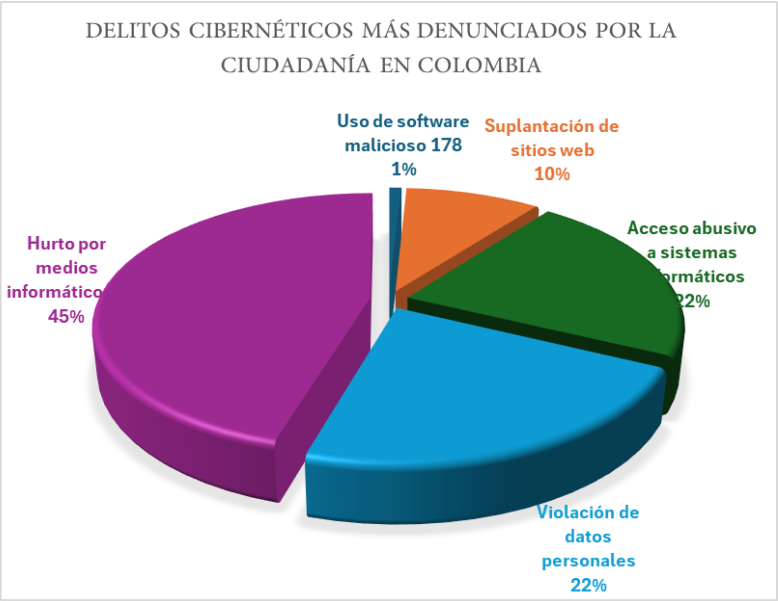
- Uso de redes sociales para extorsión.
- Creación de páginas web falsas para robar información.
- Acceso no autorizado a sistemas y redes.

Estrategias de Prevención y Atención: Acciones para Prevenir y Responder a Delitos Cibernéticos

- Capacitación y sensibilización: Talleres y campañas educativas para informar a la ciudadanía sobre prevención de delitos informáticos.
- Líneas directas de denuncia: Canales accesibles para reportar delitos de manera segura.
- Coordinación interinstitucional: Fortalecimiento de la colaboración entre diferentes entidades para optimizar la respuesta ante incidentes.

Los jóvenes no son ajenos a los delitos cibernéticos, ya que pueden ser víctimas de varias actividades delictivas. Según el informe de (LinkTIC, 2024), los delitos cibernéticos se distribuyen de la siguiente manera:

Figura 1 Delitos cibernéticos más denunciados por la ciudadanía en Colombia



Nota: construcción propia, fuente LinkTIC "Ciberseguridad en Colombia: panorama completo de su estado en 2023" (2024)

Con un total de 21.060 incidentes reportados, los más comunes son el hurto por medios informáticos y el acceso abusivo a sistemas, lo que resalta la necesidad de implementar mejores protocolos de seguridad por parte de cada estudiante, con la finalidad que su huella digital no se vea afectada de manera permanente.

Para (IBM, 2023), la huella digital es el rastro único de datos que una persona u organización deja al interactuar en Internet. Incluye tanto acciones visibles, como publicaciones en redes sociales, como datos más sutiles, como cookies y la información que se recopila automáticamente. Esta huella digital puede ser activa controlada directamente por el usuario u organización, o pasiva generada sin su control directo, como reseñas o menciones externas.

Huellas Digitales: Gestionando tu Huella Digital de Manera Responsable y Segura

La huella digital es como las migajas que dejamos cuando usamos internet. Cada vez que publicas algo en redes sociales, realizas una compra en línea o incluso buscas algo en Google, estás dejando un rastro que puede ser usado por otros.

Las huellas digitales son importantes porque su tamaño y contenido pueden influir en varios aspectos críticos para una empresa. Afectan su ciberseguridad, ya que cada activo conectado a Internet puede ser un potencial objetivo de ataques. También impactan en su reputación en línea, ya que una huella positiva o negativa puede influir en la percepción pública de la marca. Además, el manejo adecuado de la huella digital es crucial para el cumplimiento normativo, dado que muchas regulaciones exigen la protección de la privacidad de los datos personales y empresariales, integrando políticas de seguridad en los procesos informáticos en la web.

Según (Fepropaz Fundación, 2023) la privacidad se refiere al derecho de las personas a controlar el uso y acceso a su información personal, mientras que la seguridad se enfoca en proteger la integridad y confidencialidad de los datos.

La evolución de la protección de datos comenzó en la década de 1960, y hoy en día, normativas como el Reglamento General de Protección de Datos (GDPR) en Europa o la Ley de Privacidad del Consumidor de California (CCPA) buscan regular el manejo de información personal. Aun así, los avances tecnológicos rápidos, la falta de conciencia sobre seguridad digital y el valor comercial de los datos personales complican la situación.

Las soluciones técnicas como el cifrado, autenticación robusta y control de acceso son esenciales, pero también lo es la educación y la concientización sobre buenas prácticas de seguridad. Nuevas tecnologías como la inteligencia artificial y blockchain también ofrecen formas innovadoras de proteger los datos.

Referencias

Fepropaz Fundación. (2023, Julio 23). *La privacidad y seguridad de los datos en la era digital: retos y soluciones*. Fundación Fepropaz. Retrieved September 29, 2024, from https://fepropaz.com/privacidad-y-seguridad-de-datos/

Fiscalía General de la Nación y Policía Nacional de Colombia. (2023). *Cartilla metodológica de atención de delitos informáticos.* https://www.fiscalia.gov.co/colombia/wp-content/uploads/Cartilla-Metodologica-de-Atencion-de-Delitos-Informaticos.pdf#:~:text=Ley%201273%20de%202009,%E2%80%93%20Ley%20de%20Delitos%20Inform%C3%A1ticos

IBM. (2023, diciembre 19). *¿Qué es una huella digital?* IBM. https://www.ibm.com/es-es/topics/digital-footprint

LinkTIC. (2024, February 13). *Ciberseguridad en Colombia: panorama completo de su estado en 2023 – Linktic*. Linktic. Retrieved September 29, 2024, from https://linktic.com/blog/panorama-completo-de-la-ciberseguridad-en-colombia/

Ministerio de Educación Nacional. (2022). *Orientaciones curriculares para el área de tecnología e informática en la educación básica y media.* Ministerio de Educación Nacional. https://www.mineducacion.gov.co/1780/articles-411706_recurso_5.pdf