Fundamentos del ciberespacio, la ciberseguridad y los delitos informáticos

Breve descripción:

Ese componente formativo establece las bases para comprender el ciberespacio, la ciberseguridad y los delitos informáticos. Se explorarán los conceptos esenciales de la seguridad digital, los riesgos asociados a la navegación en línea y las amenazas cibernéticas más comunes. Además, se analizarán las normativas vigentes y las estrategias de prevención para fortalecer la protección de la información y los sistemas informáticos.

Abril 2025

Tabla de contenido

Introducción

Este componente formativo permite comprender los fundamentos del ciberespacio, la ciberseguridad y los delitos informáticos, abordando su evolución, características y regulaciones vigentes. Su propósito es proporcionar a los aprendices las bases necesarias para identificar amenazas digitales, conocer las normativas de seguridad y entender el impacto del cibercrimen a nivel nacional e internacional. A través del análisis de conceptos clave y casos aplicados, se explorarán estrategias de prevención y respuesta para fortalecer la seguridad en entornos digitales. Para comprender la importancia del contenido y los temas abordados, se recomienda acceder al siguiente video:

Video 1. Fundamentos del ciberespacio, la ciberseguridad y los delitos informáticos

Enlace de reproducción del video

Síntesis del video: Fundamentos del ciberespacio, la ciberseguridad y los delitos informáticos
En este componente formativo, se exploran los fundamentos del ciberespacio, la ciberseguridad y los delitos informáticos, aspectos clave en un mundo cada vez más digitalizado. El ciberespacio es un entorno dinámico donde la información fluye a través de redes digitales. Comprender su historia, características y tipos permite reconocer su impacto en la sociedad y la tecnología. La ciberseguridad surge como una disciplina fundamental para proteger la integridad, disponibilidad y confidencialidad de la información. Se analizan su evolución, normas y estrategias para enfrentar los riesgos asociados al uso de tecnologías digitales. Por otro lado, los delitos informáticos representan un desafío global en constante crecimiento. Identificar a los actores del cibercrimen, los tipos de ataques y el contexto regulatorio permite comprender su impacto tanto en Colombia como en el mundo. Además, se presentan mecanismos para reportar y prevenir estos delitos, promoviendo una cultura de seguridad digital. Este componente brinda los conocimientos esenciales para identificar amenazas, aplicar medidas de protección y contribuir a un entorno digital más seguro. Con una adecuada comprensión del ciberespacio, la ciberseguridad y los delitos informáticos, se fortalece la capacidad de enfrentar los desafíos del mundo digital y proteger la información de manera efectiva.

1. Ciberespacio fundamentos y alcance

El ciberespacio es un entorno digital compuesto por redes interconectadas a través de Internet y otros sistemas de comunicación. Este espacio permite la interacción social, el comercio, la educación y la administración pública, transformando la forma en que las personas trabajan, aprenden y se relacionan. Sin embargo, su crecimiento también ha generado desafíos en seguridad digital y privacidad.

Más allá de la conectividad entre dispositivos, el ciberespacio se sustenta en una infraestructura tecnológica compleja que incluye servidores, centros de datos, computación en la nube y redes descentralizadas. Este ecosistema ha impulsado el desarrollo de la economía digital, dando lugar a nuevas formas de negocio como el comercio electrónico, las criptomonedas y la inteligencia artificial aplicada.

Las amenazas en el ciberespacio han evolucionado junto con la tecnología. Actualmente, los ataques cibernéticos incluyen ransomware, inteligencia artificial maliciosa, ingeniería social y espionaje digital. Estos riesgos afectan no solo a individuos y empresas, sino también a gobiernos, planteando desafíos en ciberseguridad y gobernanza digital.

Debido a su naturaleza global, la regulación del ciberespacio es un reto en constante evolución. Organismos como la ONU, la Unión Europea y la OEA han establecido marcos legales y políticas de cooperación internacional para abordar delitos cibernéticos y proteger los derechos digitales. Sin embargo, el avance tecnológico supera muchas veces las regulaciones existentes, lo que exige un enfoque dinámico en la legislación.

Comprender el ciberespacio es esencial para navegar de manera segura en un mundo digitalizado y para enfrentar los desafíos que surgen en este entorno en constante transformación.

1.1. Historia y evolución del ciberespacio

El ciberespacio es el resultado de décadas de avances en informática y telecomunicaciones. Su origen se remonta a la creación de las primeras computadoras electrónicas en la década de 1940, pero fue con el desarrollo de redes interconectadas cuando comenzó a tomar forma.

En 1969, la Agencia de Proyectos de Investigación Avanzados de Defensa de EE. UU. (DARPA) creó ARPANET, la primera red de computadoras, sentando las bases de lo que hoy conocemos como Internet. En la década de 1980, con la popularización de las computadoras personales, el acceso a las redes se amplió y permitió la comunicación digital a mayor escala.

El gran punto de inflexión llegó en 1991 con la invención de la World Wide Web (WWW) por Tim Berners-Lee, que facilitó la navegación de información en línea y aceleró la expansión del ciberespacio. A partir de mediados de los años 90, el auge de los foros, chats y redes sociales transformó este entorno en un espacio de interacción global.

Durante las décadas de 2000 y 2010, el crecimiento del ciberespacio fue impulsado por la proliferación de los teléfonos inteligentes, el comercio electrónico y plataformas como Facebook, Twitter y YouTube. Sin embargo, esta expansión también trajo desafíos como la seguridad en línea, la privacidad y la regulación de los derechos digitales.

Hoy en día, el ciberespacio sigue evolucionando con tecnologías emergentes como la inteligencia artificial, el Internet de las Cosas (IoT) y la realidad virtual, consolidándose como un entorno indispensable para la sociedad, aunque también plantea retos significativos en materia de ciberseguridad y protección de datos.

1.2. Características del ciberespacio

El ciberespacio es un entorno digital dinámico que ha transformado la manera en que las personas interactúan, trabajan y acceden a la información. Su naturaleza única lo diferencia de otros espacios de comunicación y transacción, ya que no está limitado por fronteras físicas ni restricciones temporales. A continuación, se presentan sus principales características:

- ✓ **Globalidad**: el ciberespacio trasciende fronteras geográficas y permite la interacción entre personas, organizaciones y sistemas en todo el mundo, facilitando la conectividad global.
- ✓ **Interactividad**: no se limita a la recepción de información; los usuarios pueden generar, modificar y compartir contenido en tiempo real, fomentando la participación activa.
- ✓ **Desmaterialización**: la información y las actividades en línea no dependen de un espacio físico, lo que permite la digitalización de documentos, servicios y transacciones.
- ✓ **Accesibilidad**: disponible las 24 horas del día desde diversos dispositivos conectados a la red, lo que facilita la inmediatez en el acceso a datos y servicios.

- ✓ **Anonimato relativo**: aunque existen mecanismos de identificación, los usuarios pueden interactuar sin revelar completamente su identidad, lo que puede ser tanto una ventaja como un riesgo.
- ✓ **Virtualidad**: aunque sus efectos pueden ser tangibles en la vida real, su existencia es completamente digital y no depende de estructuras físicas.
- ✓ **Conectividad constante**: la interconexión entre sistemas, dispositivos y personas es permanente, lo que permite el flujo ininterrumpido de información y servicios.

1.3. Tipos de ciberespacio

El ciberespacio no es un entorno uniforme, sino un ecosistema digital con múltiples áreas especializadas según su uso y accesibilidad. Se puede clasificar en función de sus propósitos, los actores involucrados y las regulaciones que lo rigen. A continuación, se presentan los principales tipos de ciberespacio:

1) **Ciberespacio público**

Comprende las áreas de Internet de libre acceso para todos los usuarios, como sitios web informativos, redes sociales abiertas y foros públicos. Es un espacio de intercambio global donde la información circula sin restricciones significativas.

2) **Ciberespacio privado**

Incluye redes digitales con acceso restringido, como sistemas internos de empresas, correos electrónicos corporativos y plataformas bancarias. La seguridad y la privacidad son esenciales en este entorno.

3) Ciberespacio comercial

Se centra en las actividades económicas y el comercio digital, abarcando tiendas en línea, plataformas de pago electrónico y servicios de suscripción. Su expansión ha transformado la forma en que se realizan transacciones a nivel global.

4) Ciberespacio gubernamental

Utilizado por entidades estatales para gestionar bases de datos oficiales, ofrecer servicios públicos y facilitar la comunicación con la ciudadanía. Su objetivo es optimizar la administración electrónica y garantizar la transparencia.

5) Ciberespacio militar o estratégico

Comprende la infraestructura digital utilizada para la defensa, la inteligencia y la seguridad nacional. Incluye sistemas de vigilancia, redes de comunicación militar y plataformas de ciberdefensa.

6) Ciberespacio educativo

Espacio destinado a la educación y la capacitación a través de plataformas de aprendizaje en línea, repositorios académicos y entornos virtuales. Su relevancia ha aumentado con la digitalización de la enseñanza.

7) Ciberespacio criminal

Incluye redes clandestinas y foros utilizados para actividades ilícitas, como el tráfico de datos, la ciberdelincuencia y los ataques informáticos. El "dark web" es un ejemplo representativo de este tipo de ciberespacio.

2. Principios, normativas e importancia de la ciberseguridad

La ciberseguridad es una disciplina esencial en el mundo digital, encargada de proteger sistemas informáticos, redes, dispositivos y datos frente a amenazas cibernéticas y ataques maliciosos. A medida que la tecnología avanza y la interconectividad aumenta, se ha vuelto fundamental para garantizar la privacidad, integridad y disponibilidad de la información en línea.

Se compone de un conjunto de prácticas, tecnologías y procesos diseñados para prevenir accesos no autorizados, daños o pérdidas de datos. Su objetivo principal es garantizar la confidencialidad, integridad y disponibilidad de la información, protegiendo tanto a individuos como a organizaciones de amenazas como virus, malware, ransomware, ataques de denegación de servicio (DDoS) y fraudes digitales.

En un mundo altamente interconectado, un solo ataque cibernético puede generar consecuencias devastadoras, desde el robo de identidad hasta la interrupción de infraestructuras críticas como redes de energía y sistemas de comunicación gubernamentales. No solo es crucial para empresas y gobiernos, sino también para los ciudadanos, ya que cada vez más actividades diarias dependen de internet y los sistemas digitales.

A medida que surgen nuevas tecnologías como la Inteligencia Artificial (IA) y el Internet de las Cosas (IoT), los ciberdelincuentes desarrollan métodos de ataque más sofisticados, aprovechando la creciente cantidad de dispositivos conectados. Por ello, la protección del ecosistema digital requiere un enfoque integral que combine herramientas avanzadas, normativas adecuadas y una sólida cultura de seguridad.

Para garantizar una protección eficaz, se emplean diversas herramientas y estrategias, como:

- ✓ Firewalls y antivirus para detectar y bloquear amenazas.
- ✓ Encriptación de datos para proteger la información sensible.
- ✓ Autenticación multifactor (MFA) para reforzar el acceso seguro.
- ✓ Monitoreo continuo de redes para identificar posibles vulnerabilidades.
- ✓ Capacitación en seguridad digital para reducir el riesgo de errores humanos.

Uno de los mayores desafíos en ciberseguridad es la falta de concienciación de los usuarios. Muchas brechas de seguridad ocurren debido a prácticas inseguras, como el uso de contraseñas débiles o la apertura de enlaces sospechosos. Por ello, es fundamental fomentar la educación en seguridad digital a nivel individual y organizacional.

La ciberseguridad es un pilar fundamental en la era digital y su relevancia seguirá en aumento. Proteger los datos y las infraestructuras tecnológicas requiere la combinación de tecnologías avanzadas, buenas prácticas organizativas y conciencia individual. A medida que los ataques evolucionan, también deben hacerlo las estrategias de defensa, asegurando así un entorno digital más seguro y confiable para todos.

- ✓ **La Ciberseguridad**

A continuación, se pueda acceder a un video sobre la ciberseguridad, en el cual se explican sus principios fundamentales y su importancia en el entorno digital. Acceda

al siguiente enlace:

https://www.youtube.com/embed/sk9dJtwZtlA?si=U6g45pfxhsFsiVZW

2.1. Historia y evolución de la ciberseguridad

La evolución de la ciberseguridad está directamente vinculada al desarrollo de la informática y la expansión de Internet. A medida que las tecnologías digitales han avanzado, también lo han hecho las amenazas cibernéticas, lo que ha llevado a la creación de nuevas estrategias y herramientas para proteger la información y las infraestructuras digitales. Desde los primeros sistemas cerrados hasta el mundo hiperconectado de hoy, la ciberseguridad ha pasado de ser una preocupación limitada a un ámbito técnico a convertirse en una prioridad global para gobiernos, empresas y ciudadanos. A continuación, se presentan los eventos más relevantes de cada década:

1) **Década de 1960-1970 - Los inicios de la ciberseguridad**

Durante estas décadas, las computadoras eran utilizadas principalmente en entornos cerrados, como universidades y organismos gubernamentales. La seguridad informática se limitaba a la protección del acceso físico a los mainframes, ya que la conectividad era prácticamente inexistente. Sin embargo, con la creación de redes experimentales como ARPANET, surgieron las primeras preocupaciones sobre la seguridad de la información.

2) **Década de 1980 - Profesionalización de la ciberseguridad**

Con la proliferación de computadoras personales y redes más amplias, la seguridad digital comenzó a ganar relevancia. En 1983, el término "ciberseguridad" comenzó a utilizarse para referirse a la protección de sistemas de información. En 1988, el gusano Morris infectó miles de computadoras a través de ARPANET, marcando el

primer gran ataque cibernético de la historia. Este evento impulsó la creación de herramientas como firewalls y software antivirus, así como la fundación de organismos especializados, como el National Computer Security Center (NCSC) en Estados Unidos.

3) **Década de 1990 - Auge de Internet y nuevas amenazas**

Con la masificación de Internet, surgieron nuevas amenazas como virus informáticos, malware y phishing. Se implementaron tecnologías como los firewalls comerciales y los protocolos de encriptación de datos, como SSL (Secure Sockets Layer), para proteger las transacciones en línea. Las instituciones financieras y empresas comenzaron a adoptar medidas más estrictas para proteger sus redes, aunque los ataques se hicieron cada vez más frecuentes y sofisticados.

4) **Década de 2000 - Expansión del comercio digital y los ciberataques**

La llegada de las redes sociales, el comercio electrónico y el Internet de las Cosas (IoT) amplió las vulnerabilidades cibernéticas. Ataques como el gusano “ILoveYou” (2000) y el Blaster Worm (2003) demostraron la capacidad destructiva del malware. En respuesta, se crearon roles especializados, como el Chief Information Security Officer (CISO), y se desarrollaron normativas como la ISO 27001 para estandarizar la seguridad de la información.

5) **Década de 2010 - Ciberseguridad como prioridad global**

La digitalización masiva y la interconectividad expusieron infraestructuras críticas, como redes eléctricas y sistemas de telecomunicaciones, a nuevos riesgos. Los ataques de denegación de servicio (DDoS) y el auge del ransomware pusieron en jaque a empresas y gobiernos. Además, surgieron las amenazas avanzadas persistentes (APT),

impulsadas por grupos organizados y actores estatales. En respuesta, la ciberseguridad comenzó a integrar inteligencia artificial y big data para detectar y mitigar amenazas en tiempo real.

6) **Década de 2020 - Nuevos desafíos en un mundo interconectado**

La pandemia de COVID-19 aceleró el teletrabajo y, con ello, las vulnerabilidades digitales. Los ataques de phishing, ransomware y filtraciones de datos aumentaron significativamente. Las organizaciones incrementaron sus inversiones en ciberseguridad y adoptaron políticas de ciberresiliencia. Actualmente, la seguridad digital enfrenta retos asociados a la inteligencia artificial, la computación cuántica, blockchain y el crecimiento del IoT, lo que ha llevado a los gobiernos a reforzar la regulación y la defensa cibernética a nivel mundial.

A lo largo de estas décadas, la ciberseguridad ha evolucionado en respuesta a la creciente interconexión de sistemas y al aumento de las amenazas cibernéticas. Lo que comenzó como una preocupación limitada a redes cerradas y sistemas gubernamentales, hoy en día afecta a todos los niveles de la sociedad, desde individuos hasta grandes corporaciones y gobiernos. A medida que las tecnologías avanzan, también lo hacen las tácticas de los ciberatacantes, lo que hace que la ciberseguridad siga siendo un desafío constante y de vital importancia. La historia de la ciberseguridad refleja una batalla continua por proteger la información, la privacidad y la infraestructura crítica, una batalla que continuará a medida que el ciberespacio siga evolucionando.

2.2. Características de la ciberseguridad

La ciberseguridad abarca una serie de principios y características fundamentales que buscan proteger la integridad, confidencialidad y disponibilidad de la información. Entre las principales características de la ciberseguridad se incluyen la confidencialidad, la integridad y la disponibilidad, pero también existen otras características esenciales que complementan y refuerzan la seguridad digital. Estas características incluyen la autenticidad, el no repudio, la escalabilidad, la resiliencia, la seguridad proactiva, el cumplimiento normativo y la transparencia, todas las cuales desempeñan un papel crucial en el diseño y la implementación de sistemas seguros. A continuación, se presentan las principales características:

1) **Confidencialidad**: este principio garantiza que solo las personas o entidades autorizadas puedan acceder a la información. La confidencialidad es crucial para proteger datos sensibles, como información personal, financiera o corporativa. Por ejemplo, se utilizan técnicas como la encriptación de datos para asegurar que incluso si la información es interceptada, no pueda ser leída sin la clave adecuada. Esta característica protege tanto a individuos como a organizaciones de accesos no autorizados que puedan comprometer su seguridad.
2) **Integridad**: asegura que la información no sea alterada de manera no autorizada. Esto implica que los datos sean precisos y completos, sin modificaciones maliciosas o accidentales. Se emplean mecanismos como las firmas digitales o códigos hash para verificar que los datos no hayan sido alterados. Por ejemplo, si un archivo es enviado a través de internet,

su integridad se puede verificar mediante un código hash, lo que permite comprobar si el archivo ha sido modificado durante el tránsito.

3) **Disponibilidad**: garantiza que los sistemas y datos sean accesibles cuando los usuarios autorizados los necesiten. Este principio es clave para asegurar que los servicios digitales estén siempre operativos, incluso frente a ataques. La protección contra ataques de denegación de servicio (DoS) o ataques DDoS es un ejemplo claro, ya que estos ataques buscan interrumpir la disponibilidad de un servicio online al sobrecargarlo con tráfico malicioso. Mediante la implementación de infraestructuras de respaldo y sistemas de redundancia, las organizaciones pueden mantener la disponibilidad de sus servicios incluso en situaciones críticas.
4) **Autenticidad**: garantiza que los usuarios, sistemas y dispositivos sean quienes dicen ser. En un entorno digital, la autenticidad es esencial para evitar fraudes y suplantaciones de identidad. Se asegura mediante métodos como autenticación multifactor (MFA), que exige más de un factor (contraseña, huella dactilar, código enviado a un teléfono, etc.) para verificar la identidad del usuario antes de permitir el acceso a un sistema.
5) **No repudio**: asegura que una vez que una transacción o acción es realizada, no pueda ser negada por la persona o entidad que la efectuó. Este principio es crucial para mantener la responsabilidad y la trazabilidad en las interacciones digitales. Los registros de auditoría y las firmas digitales juegan un papel clave en este aspecto, ya que permiten rastrear las acciones realizadas y verificar que no se pueda negar la ejecución de una acción en un sistema.

6) **Escalabilidad**: en ciberseguridad, la escalabilidad se refiere a la capacidad de un sistema para adaptarse y proteger una creciente cantidad de datos, usuarios o dispositivos sin comprometer la seguridad. A medida que las empresas y los usuarios aumentan su presencia en línea, las soluciones de ciberseguridad deben ser capaces de ajustarse para cubrir nuevas amenazas y el crecimiento de la infraestructura sin disminuir la efectividad de la protección.
7) **Resiliencia**: se refiere a la capacidad de un sistema para recuperarse rápidamente de un incidente de seguridad. No solo se trata de prevenir ataques, sino también de responder de manera rápida y efectiva ante incidentes. Los planes de recuperación ante desastres, los sistemas de respaldo y las copias de seguridad son fundamentales para garantizar que, en caso de un ataque, los sistemas puedan restaurarse lo más rápido posible sin grandes pérdidas de datos o interrupciones de servicio.
8) **Seguridad proactiva**: a diferencia de la seguridad reactiva, que responde a incidentes después de que ocurren, la seguridad proactiva implica anticiparse a las amenazas antes de que sucedan. Esto incluye la implementación de monitoreo constante, análisis de vulnerabilidades y el uso de inteligencia de amenazas para identificar patrones y posibles riesgos antes de que los atacantes los exploten.
9) **Cumplimiento normativo**: la ciberseguridad también implica cumplir con las leyes y regulaciones vigentes que afectan la protección de datos e infraestructura. Esto incluye marcos regulatorios como el Reglamento

General de Protección de Datos (GDPR) de la Unión Europea o la Ley de Privacidad del Consumidor de California (CCPA), que requieren que las organizaciones adopten medidas estrictas para proteger los datos personales de los usuarios. Cumplir con estos estándares no solo es una obligación legal, sino también una forma de ganar la confianza de los usuarios.

10) **Transparencia**: en ciberseguridad implica que las organizaciones comuniquen de manera clara y abierta las medidas de protección que están implementando, así como los riesgos potenciales. Las auditorías y los informes de seguridad ayudan a asegurar que las partes interesadas puedan evaluar cómo una organización maneja sus riesgos de seguridad.

Las características de la ciberseguridad no solo cubren la protección básica de la información, sino que también abordan aspectos esenciales como la autenticación, la resiliencia y el cumplimiento normativo, entre otros. La implementación efectiva de estas características es crucial para proteger tanto a individuos como a organizaciones de las amenazas digitales cada vez más sofisticadas. A medida que los sistemas digitales se expanden y evolucionan, la seguridad debe adaptarse para enfrentar nuevos desafíos, y estas características deben ser la base sobre la cual se construyan las estrategias de ciberseguridad.

2.3. Normas y regulaciones internacionales

Las normas y regulaciones internacionales en ciberseguridad establecen marcos de referencia, buenas prácticas y requisitos técnicos que permiten proteger la información en diversos contextos. Estas normativas son esenciales para guiar a organizaciones y gobiernos en la creación de políticas y sistemas de seguridad robustos,

ayudando a mitigar los riesgos cibernéticos y garantizar la protección de los datos. A continuación, se presentan algunas de las más reconocidas:

Tabla 1. Diferencias entre monitoreo y evaluación

Norma / Regulación	Descripción	Objetivo
ISO/IEC 27001	Estándar internacional para la gestión de la seguridad de la información (SGSI).	Establecer, implementar, mantener y mejorar un sistema de gestión de seguridad.
ISO/IEC 27002	Guía de controles de seguridad de la información basada en ISO 27001.	Apoyar en la selección de medidas de seguridad adecuadas.
NIST Cybersecurity Framework	Marco de referencia de ciberseguridad desarrollado por el National Institute of Standards and Technology.	Proporcionar directrices para mejorar la gestión de riesgos de ciberseguridad.
GDPR (Reglamento General de Protección de Datos)	Reglamento europeo que regula la protección de datos personales.	Garantizar los derechos de los usuarios, el consentimiento y el almacenamiento seguro de datos.
PCI-DSS (Payment Card Industry Data Security Standard)	Estándar para proteger los datos de tarjetas de pago.	Asegurar la protección de datos sensibles de las tarjetas de crédito/débito.

Norma / Regulación	Descripción	Objetivo
HIPAA (Health Insurance Portability and Accountability Act)	Estándar de protección de la información de salud personal en EE.UU.	Asegurar la privacidad y la protección de los datos de salud personales.
FISMA (Federal Information Security Management Act)	Norma para proteger los sistemas de información en agencias federales de EE.UU.	Establecer requisitos de seguridad para proteger las infraestructuras críticas del gobierno.
Cybersecurity Act of 2015	Ley de ciberseguridad de EE.UU. para fomentar la colaboración público-privada.	Mejorar la colaboración para enfrentar amenazas cibernéticas y fomentar el intercambio de información.
ISO/IEC 27018	Directrices para la protección de la información personal en la nube.	Proteger la privacidad de los datos personales en los servicios de computación en la nube.
SOC 2	Estándar de auditoría para la seguridad, confidencialidad, integridad, etc.	Asegurar que los servicios en la nube cumplan con los requisitos de seguridad y privacidad.
OECD Privacy Guidelines	Directrices internacionales de la OCDE para la protección de la privacidad.	Establecer estándares globales para la protección de la privacidad y los flujos de datos.

Estas normas no solo ofrecen un enfoque integral para la ciberseguridad, sino que también buscan armonizar las mejores prácticas a nivel mundial, permitiendo la protección de la información en entornos cada vez más globalizados y digitales.

2.4. Retos actuales en ciberseguridad

La ciberseguridad enfrenta múltiples desafíos debido a la evolución constante de las amenazas digitales y la creciente interconectividad global. A medida que las tecnologías avanzan, los atacantes desarrollan métodos más sofisticados para comprometer la seguridad de sistemas, redes y datos. Entre los principales retos se destacan:

1) **Ataques de ransomware**: este tipo de ataque ha aumentado exponencialmente, afectando tanto a empresas como a instituciones gubernamentales y hospitales. Los ciberdelincuentes encriptan los datos de la víctima y exigen un rescate para su recuperación.
2) **Falta de profesionales en ciberseguridad**: existe una creciente demanda de expertos en ciberseguridad, lo que genera una brecha de talento en muchas organizaciones que dificulta la implementación de estrategias de protección efectivas.
3) **Avances en inteligencia artificial y ataques automatizados**: el uso de IA y aprendizaje automático por parte de ciberdelincuentes permite la automatización de ataques más rápidos y difíciles de detectar. Al mismo tiempo, las empresas deben desarrollar herramientas de defensa igualmente sofisticadas.
4) **Protección de infraestructuras críticas**: sectores como la energía, el transporte y la salud dependen de sistemas digitales interconectados, lo

que los hace vulnerables a ataques cibernéticos que pueden tener consecuencias graves para la sociedad.

5) **Normativas y cumplimiento regulatorio**: la rápida evolución de las leyes de protección de datos y ciberseguridad en distintos países representa un reto para las organizaciones, que deben adaptarse continuamente a los nuevos requisitos legales.
6) **Seguridad en el Internet de las Cosas (IoT):** la proliferación de dispositivos conectados ha ampliado la superficie de ataque, ya que muchos de estos dispositivos carecen de medidas de seguridad adecuadas y pueden ser utilizados como puntos de entrada para ataques a redes más grandes.
7) **Amenazas internas**: no solo los ataques externos representan un peligro; los empleados con acceso a información sensible pueden ser un factor de riesgo si no se implementan controles adecuados, como la segmentación de accesos y la monitorización de actividades.
8) **Ciberseguridad en el teletrabajo**: el incremento del trabajo remoto ha expuesto a muchas organizaciones a nuevas vulnerabilidades, como el uso de redes personales inseguras y dispositivos sin protección adecuada.

Estos desafíos requieren una estrategia de ciberseguridad integral que combine tecnología avanzada, formación continua y políticas de seguridad actualizadas para mitigar los riesgos y proteger la información.

3. Delitos informáticos y su impacto

Los delitos informáticos, también conocidos como cibercrímenes, tienen sus orígenes en los primeros desarrollos de la informática y las redes digitales. Su

naturaleza y alcance han evolucionado significativamente con el tiempo. A continuación, se detalla la evolución de los delitos informáticos y su impacto:

1) Década de 1950-1970 - Los inicios de los delitos informáticos

El origen de los delitos informáticos está ligado al desarrollo temprano de la computación y las primeras redes de comunicación. En los años 50 y 60, las computadoras eran utilizadas principalmente en universidades, gobiernos y empresas. Durante esta época, no existía una infraestructura global como Internet, por lo que los delitos informáticos eran limitados. Sin embargo, el concepto de manipulación de sistemas informáticos comenzó a discutirse, sentando las bases para futuras amenazas.

2) Década de 1980 - El auge del malware y el fraude informático

Con la llegada de las computadoras personales y la expansión de las redes, surgieron los primeros delitos informáticos claramente definidos. Durante este período, el uso de malware (software malicioso) comenzó a ganar notoriedad, con los primeros virus diseñados para replicarse y dañar computadoras. Un ejemplo temprano fue el virus "Brain" en 1986, considerado uno de los primeros en afectar computadoras a gran escala. Además, se registraron casos de fraude informático y robo de datos, aprovechando las redes para cometer estafas financieras.

3) Década de 1990 - La expansión de Internet y los ciberataques

Con la proliferación de Internet, los delitos informáticos se diversificaron y se convirtieron en una preocupación global. La piratería informática (hacking) comenzó a afectar a gobiernos y empresas, con ataques dirigidos al robo de información confidencial. También surgieron los delitos cibernéticos financieros, como el phishing y el fraude en línea. En 1994, se reportó uno de los primeros casos importantes de

fraude con tarjetas de crédito en línea, marcando un punto de inflexión en la cibercriminalidad.

4) Década de 2000 - Cibercrimen organizado y ransomware

A medida que Internet se consolidó como una plataforma global de comunicación y comercio, los delitos informáticos se volvieron más organizados. Durante esta década, las organizaciones criminales comenzaron a utilizar la red para llevar a cabo actividades ilegales a gran escala, incluyendo el robo de datos personales y ataques DDoS (Denegación de Servicio Distribuido). Uno de los delitos informáticos más notorios de la época fue el ransomware, un tipo de ataque en el que los delincuentes cifran los archivos de la víctima y exigen un rescate para liberarlos. Ejemplos como el virus "Klez" a principios de los 2000 ilustran este creciente problema.

5) Década de 2010 - Amenazas avanzadas y filtraciones masivas

El auge del Internet de las Cosas (IoT), la computación en la nube y las redes sociales amplió el alcance de los delitos informáticos. Los ataques de ransomware se volvieron más sofisticados y las filtraciones de datos afectaron a millones de usuarios. Empresas de alto perfil, como Yahoo! y Equifax, sufrieron violaciones de seguridad masivas. Además, los ataques cibernéticos patrocinados por estados y las Amenazas Persistentes Avanzadas (APT) se convirtieron en una preocupación creciente, con hackers infiltrándose en sistemas gubernamentales y empresariales para el espionaje político, económico y militar.

6) Década de 2020 - Ciberataques sofisticados y nuevas tecnologías

La actualidad ha sido testigo de un aumento en la sofisticación de los delitos informáticos. Entre los ataques más comunes se encuentran el phishing dirigido, el

fraude financiero mediante criptomonedas y los ciberataques a infraestructuras críticas, como hospitales y redes eléctricas. La pandemia de COVID-19 impulsó el teletrabajo y, con él, un incremento en los ciberataques, como el ransomware. Además, los cibercriminales están empleando inteligencia artificial y machine learning para hacer sus ataques más complejos y evasivos. Asimismo, los ataques a la cadena de suministro han aumentado, comprometiendo a proveedores de software para infiltrarse en las redes de sus clientes.

Los delitos informáticos han evolucionado desde simples actos de hacking hasta operaciones criminales altamente organizadas que afectan a individuos, empresas y gobiernos en todo el mundo. Con el avance de la tecnología, las amenazas continúan diversificándose, lo que hace imprescindible la adopción de estrategias de ciberseguridad robustas y la colaboración internacional para mitigar estos riesgos. La innovación en seguridad digital, junto con la concienciación de los usuarios, seguirá siendo clave para enfrentar los desafíos del cibercrimen en el futuro.

3.1. Actores del cibercrimen

En el panorama actual de la ciberseguridad, comprender quiénes son los responsables de las amenazas digitales es tan importante como conocer las técnicas que emplean. Los actores del cibercrimen son individuos o grupos que utilizan la tecnología con fines maliciosos, ya sea para obtener beneficios económicos, causar daño, robar información o interrumpir servicios. Estos actores no son homogéneos, ya que varían en sus motivaciones, nivel de sofisticación, recursos y objetivos.

Desde piratas informáticos solitarios que buscan notoriedad hasta organizaciones criminales bien estructuradas e incluso actores patrocinados por “Estados”, el cibercrimen ha evolucionado hacia un ecosistema complejo y dinámico. Identificar y

clasificar a estos actores permite a los profesionales de la seguridad anticipar amenazas, diseñar estrategias de defensa efectivas y fortalecer la resiliencia de los sistemas digitales.

A continuación, se describen algunos de los principales actores del cibercrimen:

- ✓ **Black Hat Hackers**: expertos en informática que explotan vulnerabildades con fines ilícitos, como el robo de datos o la distribución de malware.
- ✓ **Ciberterroristas**: utilizan ataques informáticos para causar daño a entidades gubernamentales o infraestructuras críticas.
- ✓ **Crimenes organizados:** redes delicitivas que operan en la web oscura para cometer fraudes, extorsiones y otros delitos financieros.
- ✓ **Insiders:** empleados o exempleados que abusan de su acceso a sistemas internos para sabotaje, robo de información o espionaje corporativo.
- ✓ **Hacktivistas:** individuos o grupos que emplean ataques cibernéticos con motivaciones políticas o ideológicas, como filtración de documentos confidenciales.
- ✓ **Actores patrocinados por Estados**: grupos respaldados por gobiernos que realizan ciberespionaje, sabotaje o ataques dirigidos contra otras naciones.

La comprensión de los actores del cibercrimen es fundamental para diseñar estrategias de defensa efectivas y mitigar los riesgos asociados a las amenazas digitales. Cada uno de estos actores opera con motivaciones y metodologías distintas, lo que obliga a las organizaciones y gobiernos a mantenerse en constante actualización para enfrentar nuevos desafíos en seguridad informática. La cooperación internacional, la educación en ciberseguridad y el desarrollo de tecnologías avanzadas son esenciales

para contrarrestar el impacto de estas actividades maliciosas y proteger la integridad de la información en un entorno digital cada vez más complejo.

3.2. Tipos de delitos informáticos

Los delitos informáticos abarcan una amplia gama de actividades ilícitas que afectan a individuos, empresas y gobiernos. Algunos de los más comunes incluyen:

- ✓ **Cibercrimen financiero**: fraudes como el robo de tarjetas de crédito, phishing, suplantación de identidad y estafas en línea, con el objetivo de obtener beneficios económicos de manera fraudulenta.
- ✓ **Malware**: desarrollo y propagación de software malicioso (ransomware, troyanos, virus) para robar información, dañar sistemas o extorsionar a las víctimas mediante el secuestro de datos.
- ✓ **Ataques a infraestructuras críticas**: ciberataques dirigidos a sistemas esenciales, como redes de energía, transporte, salud y servicios financieros, con el fin de interrumpir su funcionamiento o comprometer su seguridad.
- ✓ **Ciberespionaje**: robo de información confidencial por parte de actores estatales o grupos organizados, con el propósito de obtener ventajas políticas, económicas o militares a través de la infiltración en sistemas estratégicos.
- ✓ **Delitos contra la privacidad**: uso indebido de datos personales para extorsión, suplantación de identidad o comercialización ilegal en la web oscura, lo que compromete la seguridad y derechos de las víctimas.

- ✓ **Ataques DDoS (Denegación de Servicio Distribuida)**: saturación intencional de un sistema con tráfico falso para afectar su disponibilidad, generando interrupciones en plataformas y servicios en línea.
- ✓ **Delitos sexuales en línea**: actividades ilícitas como la explotación infantil, distribución de material de abuso sexual, el ciberacoso y el grooming, que afectan la integridad y seguridad de las personas en entornos digitales.

Los delitos informáticos continúan evolucionando a medida que la tecnología avanza, lo que representa un desafío constante para las autoridades y los profesionales de la ciberseguridad. La sofisticación de los ataques, junto con la expansión del acceso a Internet y el crecimiento del cibercrimen organizado, hace imprescindible la implementación de estrategias de prevención, detección y respuesta efectivas. La cooperación internacional, el desarrollo de marcos normativos actualizados y la concienciación de los usuarios son clave para mitigar los riesgos y fortalecer la seguridad en el entorno digital.

3.3. Delitos informáticos en Colombia y regulación vigente

En Colombia, los delitos informáticos están regulados por la Ley 1273 de 2009, que modificó el Código Penal para incluir sanciones específicas relacionadas con el acceso no autorizado, la alteración de datos y el uso indebido de tecnologías de la información y las comunicaciones. Esta normativa protege la integridad de los sistemas informáticos, la confidencialidad de la información y la privacidad de los usuarios.

Los principales delitos contemplados en la ley incluyen:

- ✓ **Acceso abusivo a sistemas informáticos**: ingreso no autorizado a redes, bases de datos o plataformas digitales.

- ✓ **Interceptación de datos informáticos**: captura ilegal de información transmitida en redes privadas o públicas.
- ✓ **Uso de software malicioso**: creación, propagación o utilización de programas diseñados para causar daño o vulnerar la seguridad digital.
- ✓ **Violación de datos personales**: recopilación, modificación o divulgación no autorizada de información privada con fines ilícitos.
- ✓ **Interferencia en sistemas o datos**: alteración, eliminación o daño de información almacenada en medios electrónicos.
- ✓ **Fraude informático**: manipulación de sistemas informáticos para obtener beneficios económicos de manera ilícita.

La Ley 1273 de 2009 establece penas de prisión y multas, cuya severidad varía según la naturaleza y el impacto del delito cometido. Además, refuerza la responsabilidad de las instituciones y empresas en la protección de datos y la seguridad de la información, promoviendo el desarrollo de estrategias de prevención y respuesta ante amenazas cibernéticas.

3.4. Contexto mundial y tendencias actuales

Los delitos informáticos son una preocupación global que afecta a individuos, empresas, gobiernos y otras organizaciones en todo el mundo. A medida que la tecnología ha avanzado y el Internet se ha convertido en un pilar fundamental de la vida diaria, las amenazas cibernéticas han evolucionado y se han sofisticado. Los delitos informáticos son un fenómeno creciente y no se limitan a un solo país o región, sino que afectan a nivel global, atravesando fronteras y presentando desafíos tanto para las leyes nacionales como para la cooperación internacional. Los delitos informáticos tienen su origen en las primeras computadoras conectadas en redes. Durante las

primeras décadas de la informática, los delitos informáticos eran limitados, principalmente por el acceso no autorizado a sistemas. Sin embargo, a medida que el Internet y las redes globales crecieron, los ciberdelincuentes encontraron nuevas formas de atacar sistemas y robar información valiosa, lo que impulsó el desarrollo de legislación específica y organismos especializados en la lucha contra estos delitos.

En las últimas dos décadas, los delitos informáticos han crecido de manera exponencial, impulsados por la expansión del uso de tecnologías como los smartphones, las computadoras portátiles, el Internet de las Cosas (IoT) y el comercio electrónico. Además, la pandemia de COVID-19 aceleró la digitalización de las actividades cotidianas, lo que resultó en un aumento significativo de los ciberataques, especialmente los de ransomware y el fraude en línea. Los cibercriminales ahora operan en organizaciones criminales estructuradas, con objetivos financieros, políticos y, en algunos casos, militares.

Dentro de las tendencias actuales, uno de los ataques más graves es el ransomware, donde los ciberdelincuentes secuestran los sistemas de las víctimas, cifran sus datos y exigen un pago, generalmente en criptomonedas, para restaurar el acceso. Además, la expansión del teletrabajo durante la pandemia ha abierto nuevas oportunidades para los ciberdelincuentes, con un aumento de los ataques de phishing dirigidos a empleados que utilizan plataformas de colaboración remota.

El cibercrimen patrocinado por el Estado también ha aumentado, con ataques a infraestructuras críticas y elecciones. Un ejemplo claro es el ciberataque a las elecciones presidenciales de EE. UU. en 2016, donde se acusó a actores rusos de interferir en el proceso electoral. Asimismo, el robo de datos y la privacidad sigue

siendo una amenaza persistente, como lo evidenció el ataque a Facebook en 2021, que expuso los datos personales de más de 530 millones de usuarios.

La creciente popularidad de las criptomonedas también ha facilitado actividades ilegales, como el lavado de dinero y el uso de mercados oscuros en la web. Además, el cibercrimen se ha extendido al ámbito de la desinformación, donde los cibercriminales manipulan la opinión pública mediante fake news y bots en redes sociales, afectando elecciones, movilizaciones y creando caos social.

A pesar de los esfuerzos por mejorar la cooperación internacional, la lucha contra los delitos informáticos enfrenta desafíos debido a la falta de un marco legal homogéneo a nivel global y las diferencias en las capacidades tecnológicas entre países. Los ciberdelincuentes, a menudo, explotan estas diferencias y la falta de regulación uniforme, lo que complica aún más la respuesta efectiva frente a estas amenazas.

3.5. Desafíos globales en la lucha contra el cibercrimen

La lucha contra el cibercrimen enfrenta una serie de retos complejos debido a la naturaleza transnacional de los delitos, las variaciones en las legislaciones de diferentes países y la rápida evolución de las tecnologías utilizadas por los ciberdelincuentes. Estos desafíos requieren una cooperación más efectiva entre países, una actualización constante de las normativas y el uso de tecnologías avanzadas tanto por las autoridades como por los delincuentes. A continuación, se describen algunos de los principales obstáculos que dificultan la lucha global contra el cibercrimen:

- ✓ **Falta de cooperación internacional**: aunque existen acuerdos como la Convención de Budapest (un tratado internacional para combatir la cibercriminalidad), las diferencias en las leyes nacionales y la falta de

cooperación efectiva entre países dificultan la persecución de ciberdelincuentes, especialmente cuando estos operan en territorios con legislaciones débiles o inexistentes en cuanto a delitos informáticos.

- ✓ **Desafíos legales y regulatorios**: las leyes de ciberseguridad y privacidad aún están en proceso de estandarizarse globalmente. Muchos países no cuentan con legislación específica que aborde todos los aspectos de los delitos informáticos, lo que permite que los ciberdelincuentes exploten brechas legales y operen sin temor a sanciones adecuadas.
- ✓ **Evolución rápida de las amenazas**: los ciberdelincuentes son cada vez más sofisticados y utilizan tecnologías avanzadas, como inteligencia artificial y machine learning, para mejorar sus ataques, lo que representa un reto para los gobiernos y las empresas, que deben adaptarse constantemente a nuevas amenazas. Además, la automatización y el uso de herramientas como ransomware-as-a- han permitido a actores menos especializados lanzar ataques cibernéticos de gran escala.
- ✓ **Falta de recursos en países en desarrollo**: muchos países no cuentan con los recursos humanos y tecnológicos necesarios para enfrentar el cibercrimen de manera efectiva. Esto genera una disparidad en la capacidad de los diferentes países para proteger sus infraestructuras críticas, regular las actividades en línea y perseguir a los responsables de delitos informáticos.

La lucha contra el cibercrimen requiere de un enfoque integral que implique la colaboración internacional, la actualización constante de las normativas y el desarrollo de tecnologías avanzadas para contrarrestar las tácticas cada vez más sofisticadas de los

ciberdelincuentes. Solo mediante la cooperación y el fortalecimiento de las capacidades nacionales e internacionales se podrá enfrentar esta amenaza global de manera efectiva.

3.6. Mecanismos de reporte y prevención

En Colombia, la lucha contra los delitos informáticos no solo depende de la acción de las autoridades, sino también de la colaboración de la ciudadanía y las empresas. Es fundamental que los individuos y las organizaciones conozcan los mecanismos disponibles para reportar cualquier incidente de ciberseguridad, así como las medidas preventivas que se deben tomar para evitar ser víctimas de delitos informáticos. A continuación, se describen los principales mecanismos de reporte:

- ✓ **Fiscalía General de la Nación**: la Fiscalía cuenta con un grupo especializado en delitos informáticos llamado la Unidad de Delitos Informáticos, encargada de investigar y procesar los delitos relacionados con el uso indebido de tecnología. Las personas pueden presentar denuncias sobre accesos no autorizados, fraudes electrónicos, y otros delitos informáticos tanto de forma virtual como presencial.
- ✓ **En línea**: a través de la página web de la Fiscalía General de la Nación, los ciudadanos pueden realizar denuncias de manera virtual. Esta opción facilita el proceso y permite la presentación de pruebas de forma directa y eficiente.
- ✓ **De forma presencial**: los ciudadanos también pueden acudir a las oficinas de la Fiscalía o a las estaciones de policía para presentar una denuncia formal en persona. Esto es útil cuando se requiere el acompañamiento directo de las autoridades.

- ✓ **Policía Nacional de Colombia**: la Dirección de Investigación Criminal (DIJIN) de la Policía Nacional también cuenta con un área especializada en delitos informáticos. Las denuncias se pueden realizar en cualquier estación de policía, permitiendo que las autoridades inicien investigaciones de manera inmediata.
- ✓ **Sistemas de atención en línea**: existen plataformas como el Centro Cibernético Policial (CCP), en las cuales se pueden reportar incidentes de seguridad cibernética, fraudes, y otros delitos digitales. Este sistema proporciona un medio rápido y eficaz para que los ciudadanos reporten problemas de seguridad en línea.
- ✓ **Proveedores de servicios digitales**: si el incidente está relacionado con plataformas o servicios en línea (como redes sociales, plataformas bancarias, comercio electrónico, etc.), es posible contactar directamente con los administradores o el soporte técnico de esos servicios para que se tomen medidas de seguridad y protección. Muchas de estas plataformas cuentan con protocolos de seguridad que permiten actuar rápidamente ante situaciones de riesgo.

También es importante destacar las medidas de prevención que se pueden utilizar:

- ✓ **Mantener el software actualizado**: es fundamental tener siempre las últimas actualizaciones de los sistemas operativos y aplicaciones, ya que estas correcciones suelen contener parches de seguridad importantes.
- ✓ **Utilizar contraseñas robustas y autenticación multifactor (MFA)**: las contraseñas fuertes, combinadas con métodos adicionales de verificación,

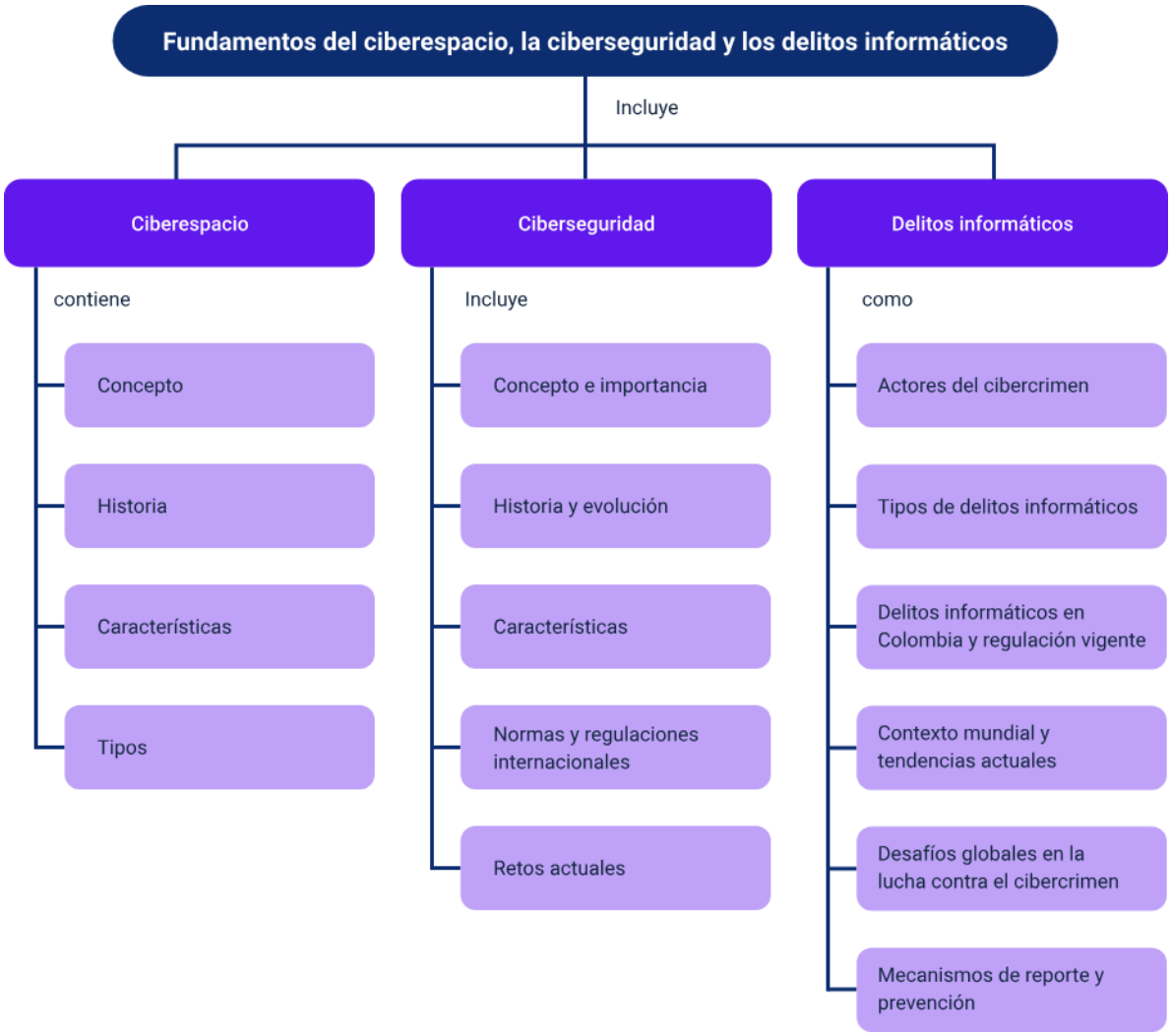
como la autenticación en dos pasos, pueden prevenir accesos no autorizados.

- ✓ **Realizar copias de seguridad regulares**: tener copias de seguridad actualizadas permite restaurar datos en caso de un ataque como el ransomware o cualquier otro incidente que comprometa la información.
- ✓ **Estar al tanto de las últimas amenazas informáticas**: la educación continua sobre las amenazas más recientes, como el phishing y el malware, es esencial para evitar caer en engaños cibernéticos.
- ✓ **Concienciación y formación en ciberseguridad**: las organizaciones y personas deben recibir formación en buenas prácticas de ciberseguridad, como el reconocimiento de correos electrónicos sospechosos o sitios web fraudulentos.
- ✓ **Uso de software antivirus y firewall**: implementar medidas de protección adicionales como antivirus y firewalls ayuda a bloquear ataques potenciales y proteger los sistemas ante accesos no autorizados.

El reporte oportuno de los delitos informáticos es esencial para combatir el cibercrimen de manera efectiva. La colaboración entre la ciudadanía, las autoridades y los proveedores de servicios digitales es fundamental para crear un entorno más seguro y protegido frente a las amenazas cibernéticas. Adicionalmente, aplicar medidas de prevención contribuye significativamente a reducir el riesgo de ser víctima de estos delitos.

Síntesis

El ciberespacio es un entorno digital en constante evolución que ha transformado la interacción global, dando origen a la ciberseguridad como una disciplina clave para proteger la información y los sistemas tecnológicos. A lo largo de su historia, la ciberseguridad ha desarrollado normativas y principios esenciales para mitigar riesgos y enfrentar desafíos como los delitos informáticos, los cuales afectan a individuos, empresas y gobiernos a nivel mundial. Estos delitos, cometidos por diversos actores del cibercrimen, incluyen fraudes electrónicos, robo de datos y ataques a infraestructuras críticas, lo que ha impulsado la creación de regulaciones y estrategias de prevención. En Colombia y en el mundo, la lucha contra el cibercrimen enfrenta desafíos como la falta de cooperación internacional y la rápida evolución de las amenazas digitales. Para contrarrestar estos riesgos, existen mecanismos de reporte y medidas de prevención que buscan fortalecer la seguridad digital y la protección de la información.


Fundamentos del ciberespacio, la ciberseguridad y los delitos informáticos
Incluye
Ciberespacio
Ciberseguridad
Delitos informáticos
contiene
Concepto
Historia
Características
Tipos
Incluye
Concepto e importancia
Historia y evolución
Características
Normas y regulaciones internacionales
Retos actuales
como
Actores del cibercrimen
Tipos de delitos informáticos
Delitos informáticos en Colombia y regulación vigente
Contexto mundial y tendencias actuales
Desafíos globales en la lucha contra el cibercrimen
Mecanismos de reporte y prevención

Material Complementario

Tema	Referencia	Tipo de material	Enlace del recurso
Actores del cibercrimen	Ecosistema de Recursos Educativos Digitales SENA. (2022). Tipos de hackers [Video]. YouTube.	Video	https://www.youtube.com/watch?v=Puk3JZ5R_Ic
Mecanismos de reporte y prevención	Ecosistema de Recursos Educativos Digitales SENA. (2022). Seguridad de la información [Video]. YouTube.	Video	https://www.youtube.com/watch?v=OC8x73OfV6s
Mecanismos de reporte y prevención	Ecosistema de Recursos Educativos Digitales SENA. (2021). Herramientas y estrategias de protección: antivirus gratuitos [Video]. YouTube.	Video	https://www.youtube.com/watch?v=jqL1RwFft-0

Glosario

Ciberespacio: entorno digital global de interconexión.

Ciberseguridad: protección de sistemas y datos contra amenazas digitales.

Contraseña fuerte: una contraseña que es difícil de adivinar o descifrar. Normalmente, incluye una combinación de letras mayúsculas y minúsculas, números y caracteres especiales, y tiene una longitud considerable.

Firewall: herramienta de seguridad que monitorea y controla el tráfico de red, permitiendo o bloqueando el acceso a un sistema o red según reglas de seguridad predefinidas.

Fraude electrónico: uso de la tecnología y de Internet para realizar actividades fraudulentas, como el robo de identidad, el acceso no autorizado a cuentas bancarias o el uso indebido de tarjetas de crédito para obtener beneficios económicos.

Hacking ético: práctica de evaluar la seguridad de sistemas informáticos de manera legal y con permiso, buscando vulnerabilidades para corregirlas antes de que los ciberdelincuentes puedan explotarlas.

Malware: abreviatura de "software malicioso", es cualquier software diseñado para dañar, interrumpir o acceder a sistemas informáticos sin el consentimiento del propietario. Incluye virus, troyanos, gusanos, etc.

Phishing: técnica de engaño para obtener información confidencial.

Ransomware: programa maligno que bloquea archivos hasta recibir un pago.

Referencias bibliográficas

Dempsey, J. X., & Carlin, J. P. (2024). Cybersecurity law fundamentals.

Departamento Administrativo de la Función Pública. (2009). Ley 1273 de 2009 - Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado, denominado "de la protección de la información y de los datos". https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

Europol. (2024). Internet Organised Crime Threat Assessment (IOCTA) 2024. https://www.europol.europa.eu/cms/sites/default/files/documents/Internet%20Organised%20Crime%20Threat%20Assessment%20IOCTA%202024.pdf

Ferrer, E. A. (2023). Estudios de cibercrimen. Ediciones Olejnik.

Lux, L. M., & Calderón, G. O. (2020). The crime of cyber fraud: Definition and delimitation. Revista Chilena de Derecho y Tecnología, 9(1), 151-184.

Madariaga, A. S. (2024). Código penal y código de procedimiento penal: Comentado jurisprudencialmente. Grupo Editorial Ibañez.

Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). (2016, junio 29). Los delincuentes cibernéticos no toman vacaciones: consejos para que se proteja en la red. Ministerio de Tecnologías de la Información y las Comunicaciones. https://www.mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/15607:Los-delincuentes-ciberneticos-no-toman-vacaciones-consejos-para-que-se-proteja-en-la-red

National Institute of Standards and Technology (NIST). (2024). The NIST Cybersecurity Framework (CSF) 2.0. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

Paredes, A. R. Z., Quevedo, I. M. S., & Chalacán, L. J. M. (2020). Seguridad informática en las PyMES de la ciudad de Quevedo. Journal of Business and Entrepreneurial Studies: JBES, 4(2), 232-241.

Paya-Santos, C., & Luque-Juárez, J. M. (2021). El sistema de inteligencia criminal ante las nuevas amenazas y oportunidades del ciberespacio. Revista Científica General José María Córdova, 19(36), 1121-1136. https://doi.org/10.21830/19006586.855

Créditos

Nombre	Cargo	Centro de Formación y Regional
Milady Tatiana Villamil Castellanos	Responsable Ecosistema de Recursos Educativos Digitales (RED)	Dirección General
Diana Rocío Possos Beltrán	Responsable de línea de producción	Centro de Comercio y Servicios - Regional Tolima
Javier Eduardo Díaz Machuca	Experto temático	Centro de Comercio y Servicios - Regional Tolima
Viviana Esperanza Herrera Quiñonez	Evaluadora instruccional	Centro de Comercio y Servicios - Regional Tolima
Oscar Ivan Uribe Ortiz	Diseñador web	Centro de Comercio y Servicios - Regional Tolima
Juan Daniel Polanco Muñoz	Diseñador web	Centro de Comercio y Servicios - Regional Tolima
Sebastian Trujillo Afanador	Desarrollador Fullstack	Centro de Comercio y Servicios - Regional Tolima
Ernesto Navarro Jaimes	Animador y productor audiovisual	Centro de Comercio y Servicios - Regional Tolima
Jorge Eduardo Rueda Peña	Evaluador de contenidos inclusivos y accesibles	Centro de Comercio y Servicios - Regional Tolima

Nombre	Cargo	Centro de Formación y Regional
Jorge Bustos Gómez	Validador y vinculador de recursos educativos digitales	Centro de Comercio y Servicios - Regional Tolima