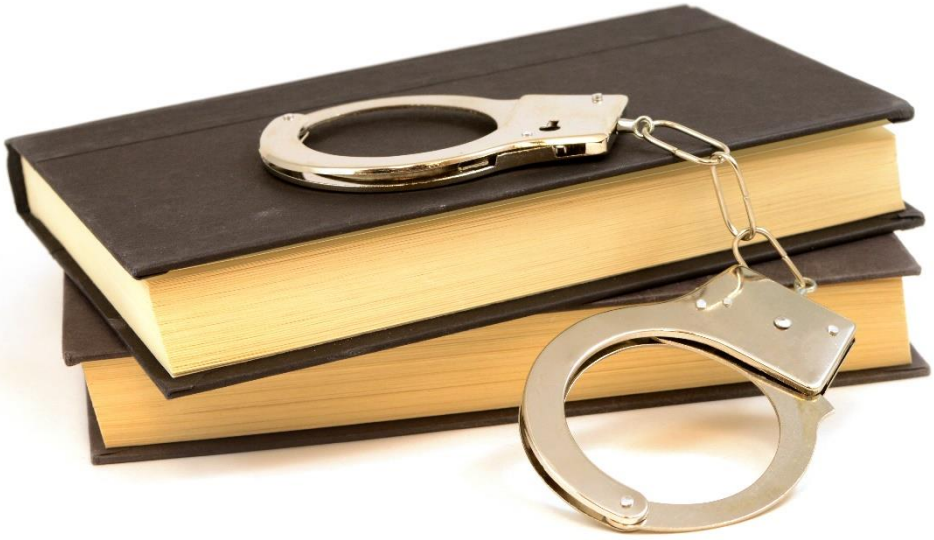
TEMARIOS
ENPDF

TEMARIO

POLICÍA NACIONAL

Bloque III: Materias Técnico-Científicas
ADMINISTRACIÓN GENERAL DEL ESTADO
Ed.2024



ed.tema_
digital

TEMARIO POLICÍA NACIONAL
ADMINISTRACIÓN GENERAL DEL ESTADO
Bloque III: Materias Técnico-Científicas
Ed. 2024
ISBN: 978-84-1383-883-0

Editado por: iEditorial
E-mail: info@ieditorial.com
Web: www.ieditorial.net

Diseño de cubierta: iEditorial
Impreso en España. Printed in Spain

TEMARIO

Bloque III: Materias Técnico-Científicas

Tema 38.Fundamentos de sistemas operativos: Funciones de un sistema operativo. Tipologías: MS/DOS; UNIX; Linux; Windows; MAC OS. Sistemas operativos móviles: iOS, Android. Sistemas de almacenamiento. Sistemas de archivos.

Tema 39.Redes informáticas: modelo OSI. Modelo TCP/IP. Dispositivos de red: concentradores (hubs); conmutadores (switches); encaminadores (routers); cortafuegos (firewall); servidores DHCP; servidores DNS; servidores proxy. Direccionamiento IP: clase de redes; IPv4; IPv6.

Tema 40.Inteligencia: dato, información e inteligencia. Tipologías de Inteligencia. Ciclo de la Inteligencia. Inteligencia de Fuentes Abiertas (OSINT). Surface Web. Deep Web. Dark Web. Dark Net.

Tema 41.Ciberdelincuencia y agentes de la Amenaza: Botnet; Business E-mail Compromise; Cartas nigerianas; Cryptojacking; Denegación de servicio; Ingeniería social; Inyección SQL; Malware; Pharming; Phishing; Spear phishing; Ransomware; Skimming; Spoofing; Spyware, Troyano; XSS; Zero-day. Cibercriminales. Crimen as Service. Hacktivistas. Insider threat. APTs. Cyber Kill Chain.

Tema 42.Origen de las armas de fuego. Definición, clasificación, categorías y funcionamiento de las armas de fuego: especial referencia al reglamento de armas. Cartucho: definición y componentes. Armas prohibidas. Documentación que ampara la tenencia y porte de armas. Balística forense.

Tema 43.El vehículo prioritario. Definición de vehículo prioritario. Facultades de los conductores de vehículos prioritarios. Comportamiento de los demás conductores respecto de los vehículos prioritarios. La conducción de vehículos en situación de emergencia. Utilización de las señales de emergencia.

Tema 44.La Seguridad en la Conducción de Vehículos Prioritarios. Definición de Seguridad Activa y Pasiva. Sistemas de Seguridad Activa y Pasiva en vehículos tipo turismo y motocicleta. Influencia de los Sistemas de Seguridad en los accidentes de tráfico. Repercusión de los Sistemas de Seguridad en la conducción policial y traslado de detenidos.

Tema 45.Prevención de Riesgos Laborales en Seguridad Vial. Factores del Tráfico y su influencia en la siniestralidad vial. Factor Humano, Factor Ambiental y Factor Vehículo. Riesgos Laborales en la conducción de vehículos prioritarios. Equipos de Protección Individual del conductor y pasajeros de vehículos policiales. Estrategias y mantenimiento preventivo del vehículo prioritario.

TEMA 38

Fundamentos de sistemas operativos: funciones de un sistema operativo. Tipologías: ms/dos; Unix; Linux; Windows; Mac Os. Sistemas operativos móviles: iOS, Android. Sistemas de almacenamiento. Sistemas de archivos

Introducción

Los sistemas operativos son el corazón de cualquier computadora, actuando como intermediarios entre el usuario y el hardware. Su desarrollo ha sido fundamental para la evolución de la informática, permitiendo que los usuarios interactúen con dispositivos de manera eficiente y efectiva. Un sistema operativo (SO) no solo gestiona los recursos del hardware, sino que también proporciona un entorno en el que se pueden ejecutar aplicaciones y programas.

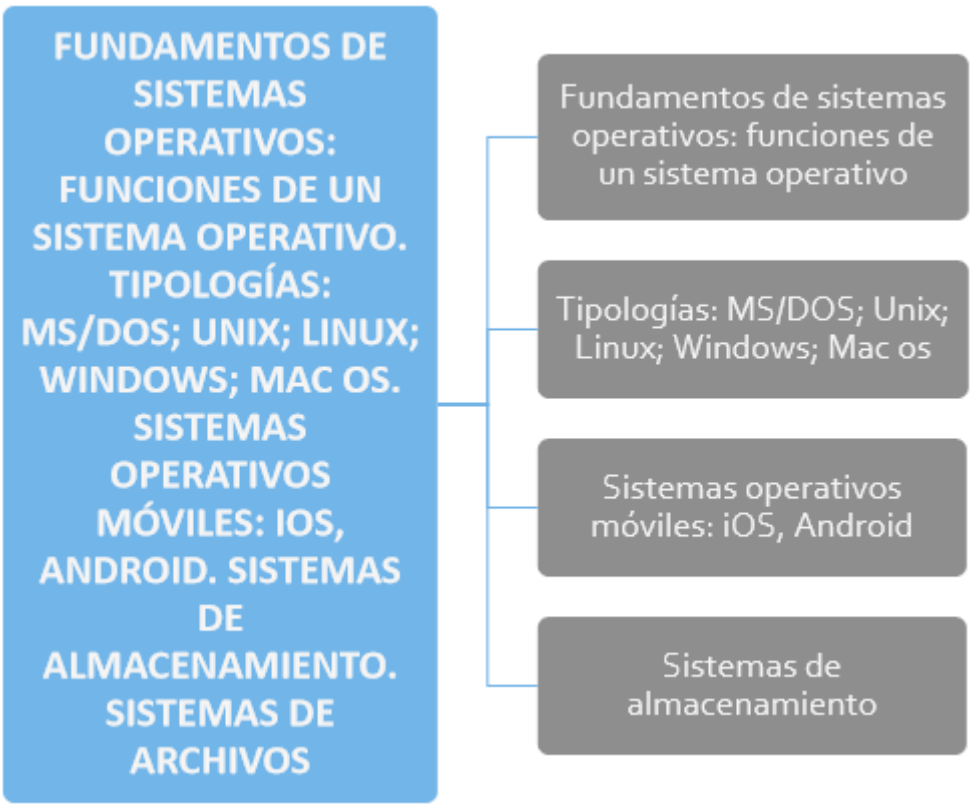
A través de funciones esenciales como la gestión de procesos, memoria, dispositivos y archivos, los sistemas operativos garantizan que las computadoras funcionen de manera óptima y segura. Además, la evolución de los sistemas operativos ha dado lugar a diversas tipologías y plataformas, incluyendo sistemas operativos de escritorio como Windows y macOS, así como sistemas operativos móviles como Android e iOS.

Con el avance de la tecnología, los sistemas operativos se enfrentan a nuevos desafíos en términos de seguridad, eficiencia y facilidad de uso, lo que los convierte en un área de estudio crucial para cualquier persona interesada en la informática y la tecnología.

Objetivos

- Comprender las funciones fundamentales de un sistema operativo y su importancia en la interacción entre el usuario y el hardware de la computadora.
- Analizar las diferentes tipologías de sistemas operativos, incluyendo sus características y aplicaciones en entornos de escritorio y móviles.
- Explorar los desafíos actuales en el desarrollo de sistemas operativos, centrándose en la seguridad, la gestión de recursos y la experiencia del usuario.

Mapa Conceptual



1. Fundamentos de sistemas operativos: funciones de un sistema operativo

Un sistema operativo (SO) es un conjunto fundamental de programas y software que permite la interacción entre el usuario y el hardware de una computadora, facilitando una gestión eficiente de los recursos del sistema. A nivel básico, se encarga de iniciar su trabajo tan pronto como se enciende el ordenador, coordinando y gestionando tanto el hardware como las aplicaciones que dependen de él para funcionar. El sistema operativo es el software central que organiza la manera en que todos los componentes de un ordenador, desde los discos duros hasta los periféricos, se comunican entre sí y con el usuario.

El sistema operativo cumple una función esencial como gestor de todos los recursos del sistema, ya que administra el acceso a dispositivos de entrada y salida como discos, impresoras, monitores, altavoces y otros componentes fundamentales. Sin un sistema operativo, el hardware de un ordenador sería inútil, ya que no habría forma de gestionar la interacción entre el usuario y el sistema ni de ejecutar las aplicaciones o programas que realizan las tareas necesarias. A lo largo de este texto, se detallarán las funciones y componentes clave de un sistema operativo, su historia, sus diferentes tipos y ejemplos, la importancia que tiene en el ámbito tecnológico actual, así como algunos de los desafíos que enfrenta en su desarrollo y evolución.

FUNCIONES PRINCIPALES DEL SISTEMA OPERATIVO

El sistema operativo cumple varias funciones clave que hacen posible la operación de una computadora. Estas funciones incluyen la gestión de procesos, la gestión de memoria, la administración de dispositivos y la gestión de archivos. Cada una de estas áreas es fundamental para garantizar que el ordenador funcione de manera eficiente y segura.

GESTIÓN DE PROCESOS

La gestión de procesos es una de las funciones esenciales del sistema operativo. Un proceso es básicamente un programa en ejecución, y el sistema operativo debe asegurarse de que cada proceso reciba el tiempo necesario de la CPU para realizar sus tareas. Esto es especialmente importante en sistemas multitarea, donde múltiples procesos se ejecutan al mismo tiempo.

El sistema operativo decide qué procesos deben ejecutarse, cuánto tiempo debe dedicarse a cada uno y en qué orden. Además, se encarga de suspender o finalizar procesos según sea necesario.

En los sistemas multitarea, la CPU alterna rápidamente entre diferentes procesos, lo que da la impresión de que todos los programas se están ejecutando simultáneamente, aunque en realidad, la CPU solo está ejecutando un proceso en un momento determinado. Esta técnica se llama multiprogramación y es esencial para maximizar la eficiencia del sistema.

El sistema operativo también gestiona la comunicación entre procesos, ya que muchos programas necesitan interactuar entre sí. Por ejemplo, un navegador web puede necesitar interactuar con el sistema de archivos para guardar o cargar documentos. El sistema operativo proporciona mecanismos de sincronización y comunicación entre procesos (IPC, por sus siglas en inglés) que permiten que estos intercambien información de manera segura y eficiente.

GESTIÓN DE LA MEMORIA

Otro componente crítico de un sistema operativo es la gestión de la memoria. El sistema operativo debe asegurarse de que cada proceso tenga suficiente espacio en la memoria principal (RAM) para funcionar. La RAM es un recurso limitado, y el sistema operativo debe asignar de manera eficiente la memoria a los diferentes procesos para evitar que se interfieran entre sí.

Una de las técnicas más importantes en la gestión de la memoria es el uso de memoria virtual. Cuando la RAM no es suficiente para alojar todos los procesos que se están ejecutando, el sistema operativo utiliza una parte del disco duro como una extensión de la memoria. Esta técnica permite que los sistemas ejecuten programas más grandes de lo que permitiría la cantidad de RAM disponible. El sistema operativo se encarga de mover datos entre la memoria RAM y el disco duro según sea necesario, de manera que los programas se ejecuten de manera fluida.

El sistema operativo también debe manejar la fragmentación de la memoria, que ocurre cuando la memoria se divide en pequeños bloques no contiguos a medida que se crean y eliminan procesos.

TEMA 39

Redes informáticas: modelo OSI. Modelo TCP/IP. Dispositivos de red: concentradores (hubs); conmutadores (switches); encaminadores (routers); cortafuegos (firewall); servidores DHCP; servidores DNS; servidores proxy. Direccionamiento IP: clase de redes; IPv4; IPv6

Introducción

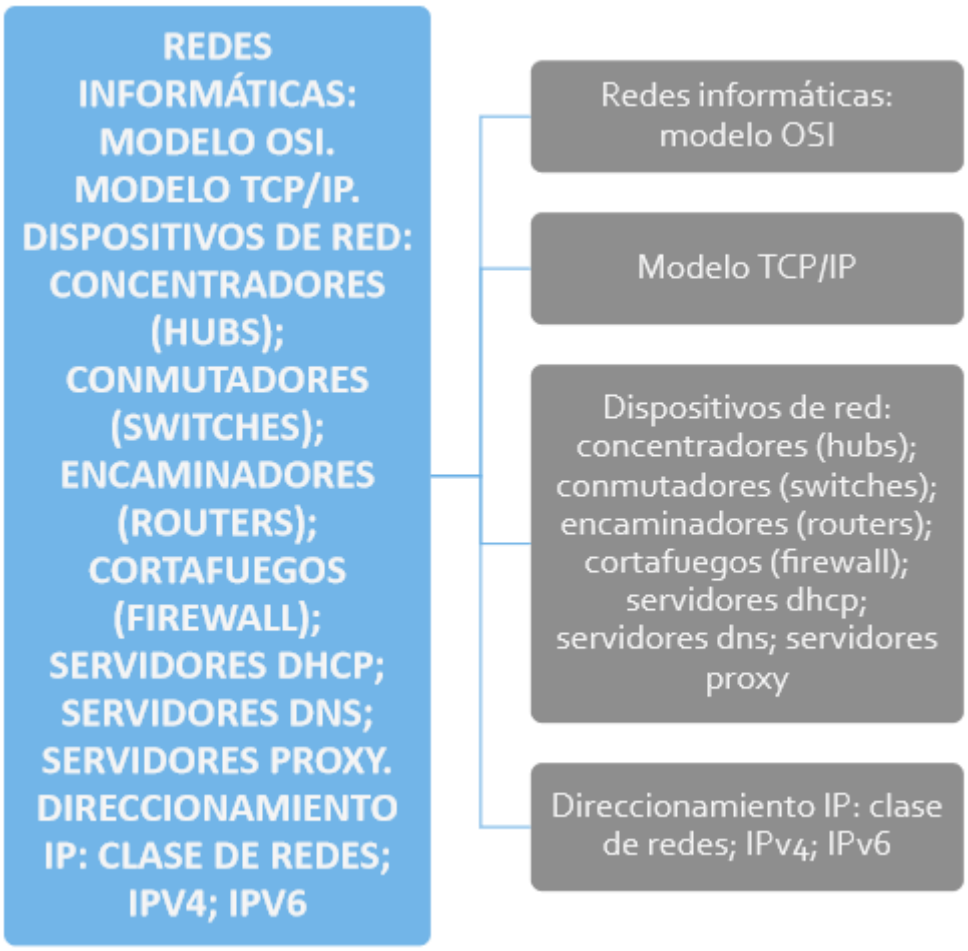
Las redes informáticas han transformado la forma en que nos comunicamos y compartimos información en el mundo moderno. Con la creciente interconexión de dispositivos y sistemas, es esencial comprender los modelos y protocolos que permiten esta comunicación. Entre los más destacados se encuentran el modelo OSI (Open Systems Interconnection) y el modelo TCP/IP (Transmission Control Protocol/Internet Protocol). Estos modelos proporcionan un marco conceptual que ayuda a estandarizar la comunicación entre diferentes sistemas y a facilitar la interoperabilidad entre dispositivos de distintos fabricantes.

El modelo OSI se divide en siete capas, cada una con funciones específicas que van desde la transmisión de datos a nivel físico hasta la interacción con aplicaciones de usuario. Por otro lado, el modelo TCP/IP, que es más utilizado en la actualidad, se compone de cuatro capas y se centra en la entrega confiable de datos a través de redes interconectadas.

Objetivos

- Comprender la estructura y funciones de los modelos OSI y TCP/IP, así como su relevancia en la comunicación de redes informáticas.
- Analizar las diferentes capas de ambos modelos y los protocolos asociados que permiten la transmisión eficiente de datos entre dispositivos.
- Evaluar la importancia del direccionamiento IP y los dispositivos de red en la configuración y mantenimiento de redes informáticas modernas.

Mapa Conceptual



1. Redes informáticas: modelo OSI

El **modelo OSI (Open Systems Interconnection)** es un marco conceptual creado por la Organización Internacional de Normalización (ISO) para estandarizar y facilitar la comunicación entre diferentes sistemas de redes informáticas. Introducido en 1984, este modelo proporciona una visión estructurada y modular de cómo se gestionan las redes de datos. El modelo OSI se divide en siete capas, donde cada una tiene funciones específicas y trabaja en conjunto con las demás para permitir la transmisión de datos a través de una red de manera eficiente y coherente. Estas capas siguen una jerarquía que va desde el manejo de hardware en la parte inferior hasta la interacción con aplicaciones de usuario en la parte superior.

Este modelo describe el proceso de transmisión de datos en redes distribuyéndolo en diferentes capas. Cada capa está diseñada para llevar a cabo un conjunto de funciones específicas y recibe los datos de la capa directamente superior o inferior, dependiendo del caso. Esta arquitectura permite que la comunicación entre sistemas heterogéneos sea posible, ya que cada capa sigue estándares abiertos e interoperables, lo que permite que productos y sistemas de distintos fabricantes se comuniquen de forma eficiente.

El modelo OSI no es un protocolo específico, sino una estructura que los protocolos de red siguen para realizar las operaciones de comunicación. Algunos protocolos que se han creado en base a este modelo incluyen TCP/IP, IPX/SPX, y más.

A continuación, se describe cada una de las siete capas del modelo OSI, comenzando desde la capa más baja, que interactúa directamente con el hardware, hasta la más alta, que interactúa con las aplicaciones del usuario.

CAPA FÍSICA (PHYSICAL LAYER)

La Capa Física es la más baja del modelo OSI y se encarga de la transmisión de los datos en forma de señales eléctricas, ópticas o electromagnéticas a través del medio físico, que puede ser un cable de cobre, fibra óptica, o incluso ondas de radio en el caso de redes inalámbricas. Esta capa define las características físicas del medio de transmisión, como los tipos de conectores, los niveles de voltaje y las frecuencias de señal, entre otros.

Las principales funciones de la capa física incluyen la modulación, demodulación, sincronización de señales y control de la tasa de transmisión de bits. También establece los medios para la comunicación de datos en términos de distancia, velocidad y topología. Es crucial para garantizar que los bits individuales (0s y 1s) puedan viajar correctamente entre los dispositivos conectados a la red. En esta capa, los dispositivos de hardware como repetidores, hubs, cables y adaptadores de red son esenciales.

CAPA DE ENLACE DE DATOS (DATA LINK LAYER)

La Capa de Enlace de Datos proporciona los medios para la transferencia confiable de datos entre dos dispositivos directamente conectados en una red física. Esta capa se divide en dos subcapas:

- **Control de Enlace Lógico (LLC)**: Responsable de mantener las comunicaciones entre los dispositivos y gestionar los errores que puedan ocurrir durante la transmisión de datos.
- **Control de Acceso al Medio (MAC):** Encargada de regular el acceso al medio físico para evitar colisiones de datos en redes compartidas.

Entre las tareas más importantes de esta capa se encuentran el empaquetado de los datos en tramas (frames) para su transmisión y la detección y corrección de errores en el nivel de enlace. El direccionamiento físico (direcciones MAC) también se define aquí, permitiendo que los dispositivos en una red local (LAN) se identifiquen y se comuniquen entre sí. Ejemplos de tecnologías que operan en esta capa incluyen Ethernet, WiFi, y Bluetooth.

CAPA DE RED (NETWORK LAYER)

La Capa de Red es responsable del enrutamiento de los paquetes de datos entre diferentes redes, asegurando que los datos lleguen a su destino final a través de la red global. Mientras que la capa de enlace de datos solo se ocupa de la transmisión de datos dentro de una red local, la capa de red maneja las comunicaciones entre redes, permitiendo la interconexión de múltiples redes.

Esta capa se encarga del direccionamiento lógico y de encontrar las mejores rutas para la entrega de datos, basándose en los protocolos de enrutamiento. El protocolo IP (Internet Protocol), uno de los más importantes de la red, opera en esta capa, y permite la identificación única de cada dispositivo conectado a la red mediante direcciones IP.

TEMA 40

Inteligencia: dato, información e inteligencia. Tipologías de Inteligencia. Ciclo de la Inteligencia. Inteligencia de Fuentes Abiertas (OSINT). Surface Web. Deep Web. Dark Web. Dark Net

Introducción

En la actualidad, el acceso a la información en Internet ha evolucionado de manera significativa, dando lugar a diferentes capas de contenido que conforman el vasto ecosistema digital. Entre estas capas, se encuentran la Surface Web, la Deep Web y la Dark Web, cada una con características y propósitos distintos. La Surface Web es la parte más visible y accesible de Internet, donde los usuarios pueden interactuar con sitios web corporativos, blogs, redes sociales y foros.

Por otro lado, la Deep Web abarca una gran cantidad de información que no está indexada por los motores de búsqueda, incluyendo bases de datos académicas y contenido privado, lo que la convierte en un recurso invaluable para diversas instituciones.

Finalmente, la Dark Web, aunque a menudo asociada con actividades ilegales, también alberga espacios para la libertad de expresión y el activismo. Comprender estas capas de Internet es esencial para navegar de manera segura y efectiva en el mundo digital actual, así como para abordar las implicaciones éticas y legales que surgen de su uso.

Objetivos

- Analizar las características y diferencias entre la Surface Web, la Deep Web y la Dark Web, proporcionando una comprensión clara de su estructura y contenido.
- Explorar la importancia de la seguridad y privacidad en la navegación de la Deep Web y la Dark Web, así como los desafíos asociados con el acceso a estas capas de información.
- Evaluar las implicaciones éticas y legales que surgen del uso de la Dark Web, considerando tanto sus aspectos positivos como negativos en el contexto social y legal actual.

Mapa Conceptual

1. Inteligencia: dato, información e inteligencia

La ciberseguridad se entiende como un conjunto integral de estrategias y acciones destinadas a proteger las redes y sistemas que componen el ciberespacio. Esto implica la detección y mitigación de intrusiones, la respuesta y recuperación ante incidentes, así como la preservación de la confidencialidad, disponibilidad e integridad de la información. Para garantizar estos aspectos, es fundamental que las organizaciones implementen normativas específicas que contemplen todas las medidas necesarias para salvaguardar los puestos de trabajo. Esta normativa debe revisarse de manera regular para verificar su cumplimiento y actualizarse en función de cualquier cambio en los equipos, sistemas o la incorporación de nuevos servicios.

La divulgación de políticas relativas al uso de equipos y servicios, como el correo electrónico y el almacenamiento, es esencial para informar a los empleados sobre sus responsabilidades en materia de seguridad. En este sentido, el personal es considerado un componente clave dentro de la estructura de seguridad de una organización, ya que su concienciación y formación son determinantes para fortalecer la protección de los sistemas. De acuerdo con el Real Decreto 3/2010, modificado por el Real Decreto 951/2015, que establece principios y requisitos mínimos de seguridad, se requiere que las organizaciones realicen planes de formación y sensibilización entre su personal para fomentar una cultura de seguridad adecuada.

Las auditorías desempeñan un papel crucial en la verificación del cumplimiento de las normativas de seguridad. Estas auditorías permiten llevar a cabo revisiones independientes de los registros y actividades del sistema, asegurando que los controles implementados son adecuados y que se están siguiendo las políticas de seguridad y los procedimientos operativos establecidos. Además, las auditorías ayudan a identificar posibles infracciones de seguridad y ofrecen recomendaciones para realizar modificaciones pertinentes en los controles, políticas y procedimientos existentes, garantizando así un enfoque proactivo en la gestión de la ciberseguridad.

A medida que la tecnología evoluciona y las amenazas cibernéticas se vuelven más sofisticadas, la ciberseguridad sigue siendo una prioridad para las organizaciones en 2024. La inversión en tecnología avanzada, la formación continua del personal y la implementación de prácticas de seguridad robustas son esenciales para proteger la información y los sistemas críticos de cualquier entidad.

Atendiendo a lo expuesto se debe precisar que la inteligencia, en el contexto de la gestión del conocimiento y la toma de decisiones, se estructura a partir de tres conceptos fundamentales: dato, información e inteligencia. Estos elementos se encuentran interrelacionados y forman una jerarquía que permite transformar datos en conocimiento útil y aplicable.

DATO

El dato es la unidad más básica y elemental en esta jerarquía. Se refiere a hechos, cifras o símbolos que, por sí mismos, carecen de significado. Los datos pueden ser cuantitativos o cualitativos y pueden presentarse en diversas formas, como números, palabras o imágenes. Por ejemplo, una serie de números que representan las ventas de un producto en un mes son datos. Los datos son esenciales porque son la materia prima sobre la cual se construye la información, pero por sí solos no permiten la toma de decisiones.

INFORMACIÓN

La información se obtiene al procesar y organizar datos de manera que adquieran significado y contexto. Este proceso implica la interpretación de los datos, permitiendo que sean útiles para el análisis y la toma de decisiones. Por ejemplo, al analizar los datos de ventas de un producto, se puede determinar que ha habido un aumento del 20% en comparación con el mes anterior. Esta transformación de datos en información permite identificar tendencias, patrones y relaciones, facilitando la comprensión de situaciones complejas.

INTELIGENCIA

La inteligencia se refiere a la capacidad de analizar y aplicar la información obtenida para generar conocimiento y tomar decisiones informadas. Es el resultado de un proceso que implica la interpretación crítica de la información, la evaluación de diferentes escenarios y la elaboración de estrategias basadas en ese análisis. La inteligencia permite a las organizaciones anticipar problemas, identificar oportunidades y responder de manera proactiva a los cambios en su entorno. En un contexto empresarial, por ejemplo, la inteligencia competitiva implica analizar la información del mercado y de la competencia para desarrollar estrategias que mejoren la posición de la empresa.

TEMA 41

Ciberdelincuencia y agentes de la amenaza: botnet; Business E-mail Compromise; cartas nigerianas; cryptojacking; denegación de servicio; ingeniería social; inyección SQL; malware; pharming; phishing; spear phishing; ransomware; skimming; spoofing; spyware, troyano; XSS; zero-day. Cibercriminales. Crimen as Service. Hacktivistas. Insider threat. APTs. Cyber Kill Chain

Introducción

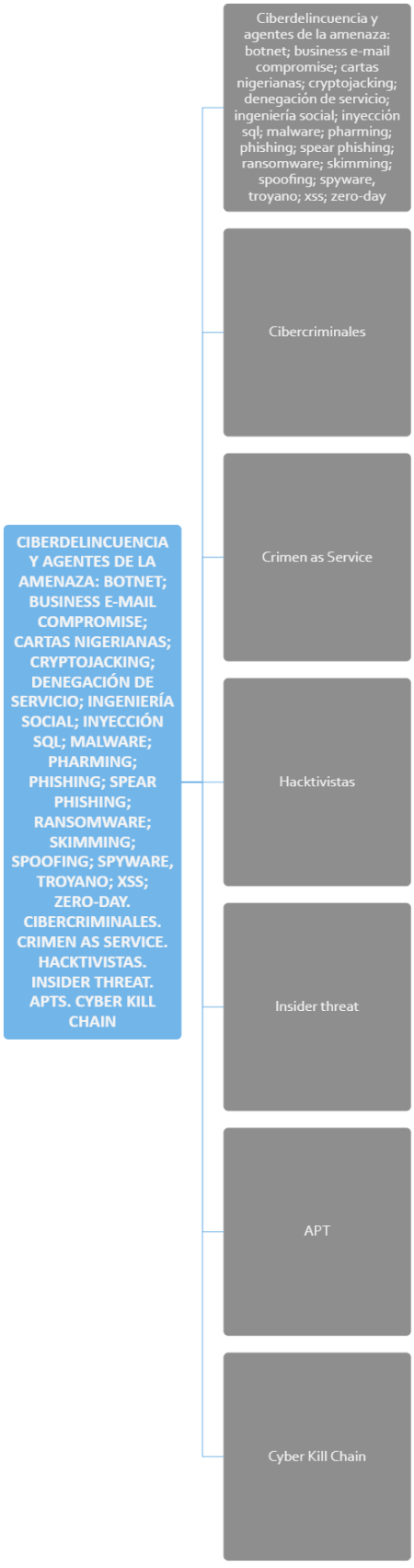
La ciberdelincuencia se ha convertido en una de las principales amenazas en el mundo digital, donde tanto usuarios individuales como empresas se ven expuestos a múltiples tipos de ataques. Estos crímenes abarcan desde técnicas clásicas, como el phishing y la denegación de servicio, hasta ataques más sofisticados, como el cryptojacking, los ataques de día cero (zero-day) y la inyección SQL. Además, agentes de la amenaza, como las botnets, el malware y los troyanos, son utilizados por los delincuentes para obtener acceso no autorizado, robar información o interrumpir servicios.

Dentro de este panorama, surgen distintos actores que participan en la ciberdelincuencia, incluyendo los cibercriminales organizados, los hacktivistas, las amenazas internas (insider threats) y los llamados APTs (Amenazas Persistentes Avanzadas). Junto con estos actores, el modelo "Crimen as a Service" permite que herramientas y servicios de ciberdelincuencia sean accesibles a un mayor número de personas. Para entender y contrarrestar estas amenazas, se han desarrollado marcos como el Cyber Kill Chain, que desglosa las etapas de un ataque para poder detectarlo y neutralizarlo a tiempo.

Objetivos

- Comprender los diferentes tipos de ciberdelitos y agentes de amenaza, como botnets, ransomware, phishing, entre otros, y su impacto en la seguridad informática.
- Identificar los principales actores involucrados en la ciberdelincuencia, como cibercriminales, hacktivistas y amenazas internas, y conocer sus motivaciones y métodos.
- Analizar las fases del Cyber Kill Chain y su utilidad en la prevención y respuesta ante ataques cibernéticos, así como el concepto de "Crimen as a Service" y su relevancia en la economía digital del cibercrimen.

Mapa Conceptual



1. Ciberdelincuencia y agentes de la amenaza: botnet; business e-mail compromise; cartas nigerianas; cryptojacking; denegación de servicio; ingeniería social; inyección sql; malware; pharming; phishing; spear phishing; ransomware; skimming; spoofing; spyware, troyano; xss; zero-day

1.1. Botnet

Una **botnet** es una red de dispositivos informáticos, comúnmente referidos como "bots" o "zombis", que han sido infectados con software malicioso (malware) y que pueden ser controlados de forma remota por un atacante. Estos dispositivos pueden incluir computadoras personales, servidores, dispositivos IoT (Internet de las Cosas) y cualquier otro dispositivo que tenga conexión a Internet. Las botnets son utilizadas para llevar a cabo una variedad de actividades maliciosas, que incluyen, pero no se limitan a, ataques DDoS (Denegación de Servicio Distribuida), envío de spam, robo de información sensible y minería de criptomonedas.

ELEMENTOS ESENCIALES DE UNA BOTNET

La estructura y funcionalidad de una botnet pueden ser complejas y multifacéticas. A continuación, se presentan los componentes y elementos esenciales que definen el funcionamiento de una botnet.

Dispositivos Bot (Bots)

Los bots son los componentes fundamentales de una botnet. Se refieren a cualquier dispositivo que ha sido comprometido y está bajo el control del atacante. Estos dispositivos pueden variar ampliamente en su naturaleza y capacidades:

- **Computadoras de Escritorio y Portátiles:** Estos son los dispositivos más comunes utilizados en botnets. Pueden ser infectados a través de técnicas como el phishing, descarga de software malicioso o vulnerabilidades en el sistema operativo.
- **Dispositivos Móviles:** Los smartphones y tabletas también pueden ser convertidos en bots. Las aplicaciones maliciosas o el acceso a redes Wi-Fi inseguras pueden ser métodos de infección.
- **Dispositivos IoT:** Con la proliferación de dispositivos conectados a Internet, como cámaras de seguridad, termostatos y asistentes inteligentes, estos dispositivos son cada vez más utilizados en botnets debido a su falta de seguridad y configuraciones predeterminadas débiles.

Métodos de Infección

Para construir una botnet, los atacantes emplean diversas técnicas de infección que permiten que el malware se instale en los dispositivos de las víctimas:

- Malware: Programas diseñados para infiltrarse y dañar o comprometer dispositivos. Esto puede incluir troyanos, gusanos y virus. El malware puede ser distribuido a través de correos electrónicos maliciosos, sitios web comprometidos o descargas de software.
- Exploits de Vulnerabilidad: Los atacantes a menudo aprovechan las vulnerabilidades en el software o hardware de un dispositivo para instalar el malware. Esto puede incluir fallos en el sistema operativo, aplicaciones desactualizadas o configuraciones inseguras.
- Ingeniería Social: Las técnicas de ingeniería social, como el phishing, son métodos efectivos para engañar a los usuarios y hacer que instalen el malware por sí mismos. Esto puede incluir correos electrónicos fraudulentos que imitan organizaciones legítimas.

TEMA 42

Origen de las armas de fuego. Definición, clasificación, categorías y funcionamiento de las armas de fuego: especial referencia al reglamento de armas. Cartucho: definición y componentes. Armas prohibidas. Documentación que ampara la tenencia y porte de armas. Balística forense

Introducción

Las armas de fuego han tenido un desarrollo histórico significativo desde su origen, marcando un avance crucial en la tecnología bélica y la seguridad. Su evolución, desde rudimentarios dispositivos de pólvora hasta las armas modernas, ha influido notablemente en los ámbitos militar, civil y policial. En la actualidad, el uso y la regulación de las armas de fuego están estrictamente controlados a través de normativas específicas, como el Reglamento de Armas en España, que clasifica, categoriza y define su funcionamiento, así como los requisitos legales para su posesión y porte.

El estudio de las armas de fuego abarca también la balística forense, una disciplina clave en la investigación criminal, que permite analizar proyectiles y armas relacionadas con hechos delictivos.

Este conocimiento es esencial para el personal de seguridad y cuerpos de seguridad del Estado, tanto en su manejo correcto como en la identificación de armas prohibidas y en el cumplimiento de los procedimientos legales que regulan su uso.

Objetivos

- Conocer el origen, evolución y desarrollo de las armas de fuego, comprendiendo su impacto histórico y su relevancia actual.
- Entender la clasificación y categorías de las armas de fuego, según el Reglamento de Armas, y el funcionamiento de sus principales componentes, como el cartucho.
- Identificar las armas prohibidas y los requisitos documentales necesarios para la tenencia y porte de armas, así como los principios básicos de la balística forense en investigaciones criminales.

Mapa Conceptual

1. Origen de las armas de fuego

A lo largo de la historia, la humanidad ha buscado crear y utilizar armas con diversos propósitos, tales como la obtención de alimentos, la defensa personal y el enfrentamiento con adversarios. En sus primeras etapas, el ser humano se valió de los recursos naturales que le rodeaban para fabricar instrumentos rudimentarios que le permitieran atacar y defenderse. Durante la prehistoria, la piedra se convirtió en uno de los materiales más utilizados, siendo transformada por el hombre en armas y herramientas. Este proceso comenzó de manera primitiva, con la búsqueda de filos cortantes, y progresivamente se fueron incorporando otros elementos, como ramas sueltas y huesos de animales. De esta combinación de materiales nacieron armas más sofisticadas, tales como cuchillos, lanzas, hachas y flechas, marcando una de las primeras etapas de evolución en la fabricación de armas.

Con el paso del tiempo y el desarrollo de las sociedades, la **estructura y esencia de las armas** fueron sometidas a constantes modificaciones. Con la consolidación de los primeros sentimientos de identidad nacional y patriotismo, se expandieron los medios de ataque y defensa, lo que refleja un aumento en la complejidad y diversidad de los armamentos. Este fenómeno lleva a la consideración de que es prácticamente imposible entender la historia de la humanidad sin tener en cuenta la evolución de sus armas. Desde sus inicios, estas han estado intrínsecamente ligadas al progreso del ser humano, diferenciándolo de otras especies y facilitando tanto la creación de nuevas civilizaciones como la destrucción de aquellas que existieron previamente.

A medida que la humanidad avanzó, también lo hicieron las **herramientas y armas** que utilizaba. La transición de las armas blancas a una variedad de armamento que incluye proyectiles propulsados por diferentes fuentes de energía marcó un cambio significativo en la capacidad del ser humano para cazar y combatir. Entre las armas que surgieron, se encuentran la lanza, que depende de la fuerza muscular del usuario; el arco, que aprovecha la elasticidad de ciertos materiales; la honda, que utiliza la fuerza centrífuga para lanzar proyectiles; y, más notablemente, las armas de fuego, que se basan en la expansión de gases para impulsar sus proyectiles.

La **invención de la pólvora** representa un punto de inflexión en la historia del armamento. Este invento marcó el inicio de la era de las armas de fuego, las cuales son un desarrollo directo de la utilización de pólvora. La invención de este explosivo, aunque su origen exacto no está completamente documentado, se atribuye a China en el siglo IX. La pólvora se utilizaba inicialmente en fuegos artificiales y posteriormente en armamento. Con el tiempo, el conocimiento sobre su composición y uso se extendió hacia occidente a través de rutas comerciales, como la famosa Ruta de la Seda. Los árabes, actuando como intermediarios comerciales de productos lujosos, también jugaron un papel importante en la difusión de este conocimiento, introduciendo la pólvora en Europa alrededor del año 1200.

Uno de los personajes históricos asociados con la utilización de la pólvora en Europa es **Berthold Schwarz**, un monje alemán apodado "el monje negro", quien es mencionado en algunas fuentes como el primer individuo en emplear pólvora para propulsar un proyectil a inicios del siglo XIV. Sin embargo, hay quienes sostienen que los árabes ya habían utilizado pólvora con este propósito en la península ibérica durante ese mismo periodo.

La **composición original de la pólvora medieval** se caracterizaba por un 50% de salitre (nitrato potásico), 25% de azufre y 25% de carbón. Esta mezcla era más inflamable y generaba más humo y fogonazo en comparación con la pólvora negra utilizada posteriormente en la guerra, cuya proporción era diferente: 75% de salitre, 15% de azufre y 10% de carbón.

Respecto a la **aparición de las armas de fuego**, las primeras referencias conocidas se sitúan en China en el siglo XIII, donde se empleaban prototipos de cañones fabricados inicialmente de bambú y más tarde de bronce, diseñados para lanzar proyectiles a larga distancia utilizando pólvora como fuerza propulsora. En Europa, la documentación sobre la posesión y uso de estas armas de fuego comenzó a surgir a partir de la primera mitad del siglo XIV.

La **evolución de las armas a lo largo de la historia** no solo ha estado marcada por innovaciones tecnológicas, sino también por cambios en la estructura social y política de las civilizaciones. Cada nueva invención o mejora en el diseño de las armas ha tenido repercusiones significativas en la forma en que las sociedades se han organizado y defendido, destaca

TEMA 43

El vehículo prioritario. Definición de vehículo prioritario. Facultades de los conductores de vehículos prioritarios. Comportamiento de los demás conductores respecto de los vehículos prioritarios. La conducción de vehículos en situación de emergencia. Utilización de las señales de emergencia

Introducción

Los vehículos prioritarios son aquellos que, durante la prestación de servicios de urgencia, gozan de prerrogativas especiales en la circulación vial, como la prioridad de paso y la superación de los límites de velocidad. Estos vehículos, como los de policía, bomberos y ambulancias, deben cumplir con requisitos técnicos específicos, como la instalación de señales acústicas y luminosas. Además, la conducción de vehículos en situaciones de emergencia requiere un uso responsable y eficiente de las facultades otorgadas a sus conductores, quienes deben garantizar la seguridad tanto de los demás usuarios de la vía como la propia.

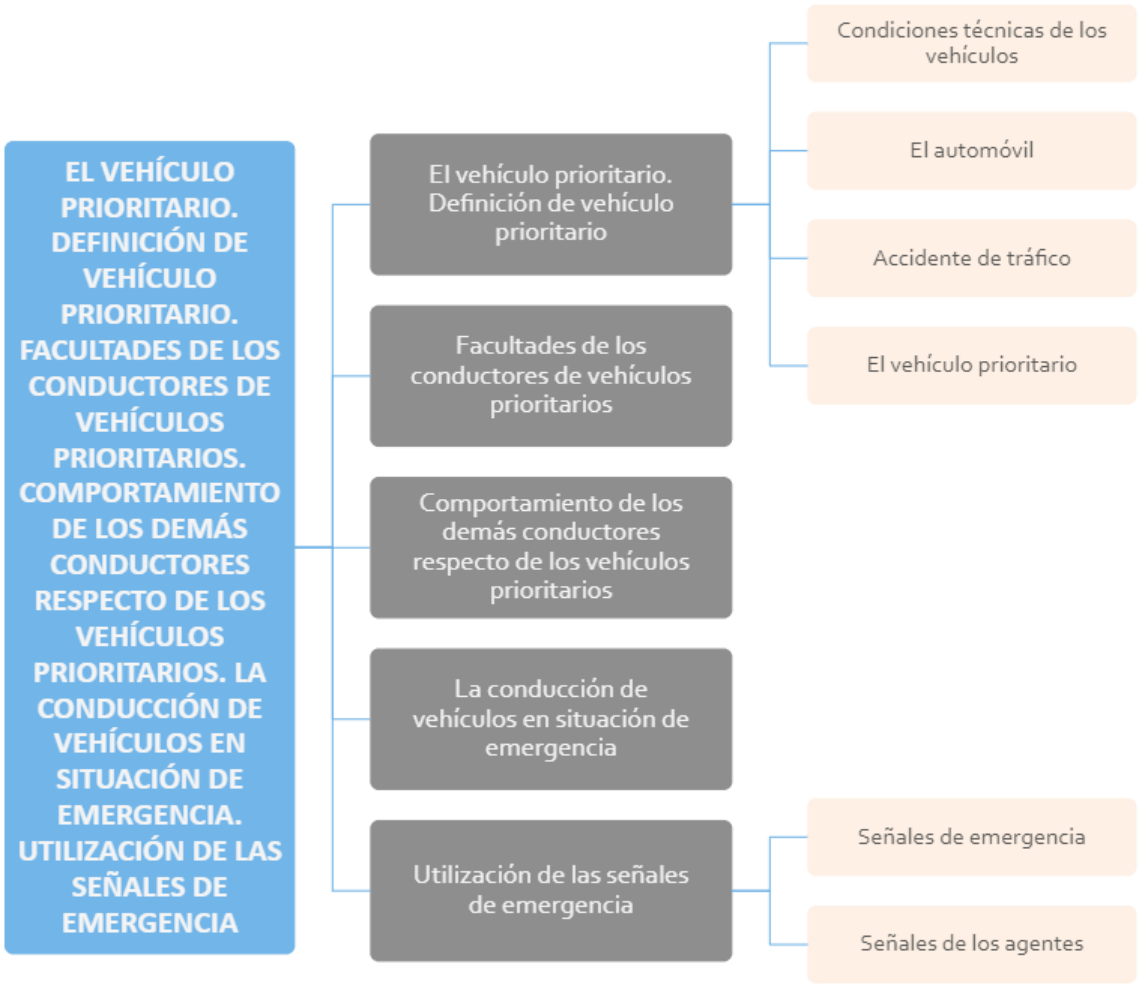
El comportamiento de los demás conductores es crucial en la interacción con vehículos prioritarios. La normativa establece que deben facilitar el paso de estos vehículos deteniéndose o apartándose de la vía cuando se aproximen con señales de emergencia activadas.

La adecuada utilización de estas señales, junto con el respeto a las indicaciones de los agentes, es esencial para la fluidez del tráfico y la correcta gestión de situaciones críticas.

Objetivos

- Definir el concepto de vehículo prioritario y describir sus condiciones técnicas específicas.
- Analizar las facultades otorgadas a los conductores de vehículos prioritarios en situaciones de emergencia, incluyendo el uso de señales acústicas y luminosas.
- Identificar las normas de comportamiento que los demás conductores deben seguir en presencia de un vehículo prioritario y las consecuencias de no cumplirlas.

Mapa Conceptual



1. El vehículo prioritario. Definición de vehículo prioritario

Según el Diccionario de la Real Academia Española, un **vehículo** se define como un medio de transporte de personas o cosas. Este término proviene etimológicamente del latín "vehiculum", que significa "medio de transporte". Esta palabra se forma a partir de la raíz del verbo "vehere", que se traduce como "transportar" o "llevar", junto con el sufijo "-culum", que no solo indica un significado diminutivo, sino que también tiene un valor instrumental, evidenciando su función como medio de transporte.

Para una definición más precisa desde el ámbito jurídico, es necesario referirse a la **Ley sobre Tráfico, Circulación de Vehículos a Motor y Seguridad Vial (LSV).** En su artículo 2, se establece el ámbito de aplicación de esta ley, que es relevante para comprender el contexto en el que se regula el uso de vehículos. Este artículo indica que los preceptos de la ley son aplicables en todo el territorio nacional y son de obligatoria observancia para los titulares y usuarios de las vías y terrenos públicos aptos para la circulación, tanto en entornos urbanos como interurbanos. Además, se extiende a las vías y terrenos que, aunque no tengan tal aptitud, sean de uso común. En ausencia de otras normativas, la ley también se aplicará a los titulares de las vías y terrenos privados que sean utilizados por una colectividad indeterminada de usuarios.

Esta **definición y ámbito de aplicación** son fundamentales para entender las regulaciones que rigen el uso de vehículos en España, así como las responsabilidades y derechos de los usuarios en relación con las vías públicas y privadas.

1.1. Condiciones técnicas de los vehículos

Las **condiciones técnicas de los vehículos** se determinan en el art. 11 del Reglamento General de Vehículos el cual dispone de forma expresa que las condiciones técnicas que deben cumplir los vehículos de motor, sus partes y sus piezas, para que puedan ser matriculados o puestos en circulación, con las limitaciones, excepciones y especificaciones que se establecen en la reglamentación que se recoge en el anexo I, son las que se indican en los puntos siguientes:

1. Deben estar construidos y mantenidos de forma que el campo de visión del conductor hacia delante, hacia la derecha y hacia la izquierda le permita una visibilidad diáfana sobre toda la vía por la que circule.
2. Deben estar provistos de uno o varios retrovisores, según la categoría del vehículo.

   El número, las dimensiones y la disposición de los espejos retrovisores deberán reunir los requisitos que se establecen en el anexo III y en la reglamentación que se recoge en el anexo I y permitir al conductor ver la circulación por detrás del vehículo.
3. Los elementos transparentes del habitáculo que afecten al campo de visión del conductor no deben deformar de modo apreciable los objetos vistos a su través, ni producir confusión entre los colores utilizados en la señalización vial.
4. Si el vehículo está provisto de un parabrisas de dimensiones y forma tales que el conductor, desde su puesto de conducción, no pueda ver normalmente la vía hacia delante más que a través de los elementos transparentes de dicho parabrisas, deberá estar provisto de dispositivos limpiaparabrisas y lavaparabrisas, de acuerdo con la reglamentación recogida en el anexo I.

   Dispondrán, además, de dispositivos antihielo y antivaho si así lo exige la reglamentación que se recoge en el anexo I.
5. Deben estar provistos de un mecanismo adecuado que permita al conductor mantener la dirección del vehículo y modificarla con facilidad, rapidez y seguridad.

TEMA 44

La seguridad en la conducción de vehículos prioritarios. Definición de seguridad activa y pasiva. Sistemas de seguridad activa y pasiva en vehículos tipo turismo y motocicleta. Influencia de los sistemas de seguridad en los accidentes de tráfico. Repercusión de los sistemas de seguridad en la conducción policial y traslado de detenidos

Introducción

La seguridad en la conducción de vehículos prioritarios es un aspecto fundamental para minimizar los riesgos asociados a la conducción de emergencias, especialmente en situaciones que requieren alta velocidad o maniobras complejas. La implementación de sistemas de seguridad activa y pasiva en vehículos, tanto tipo turismo como motocicletas, es esencial para prevenir accidentes y reducir la gravedad de los mismos. Estos sistemas permiten optimizar el control del vehículo y proteger a los ocupantes en caso de colisión.

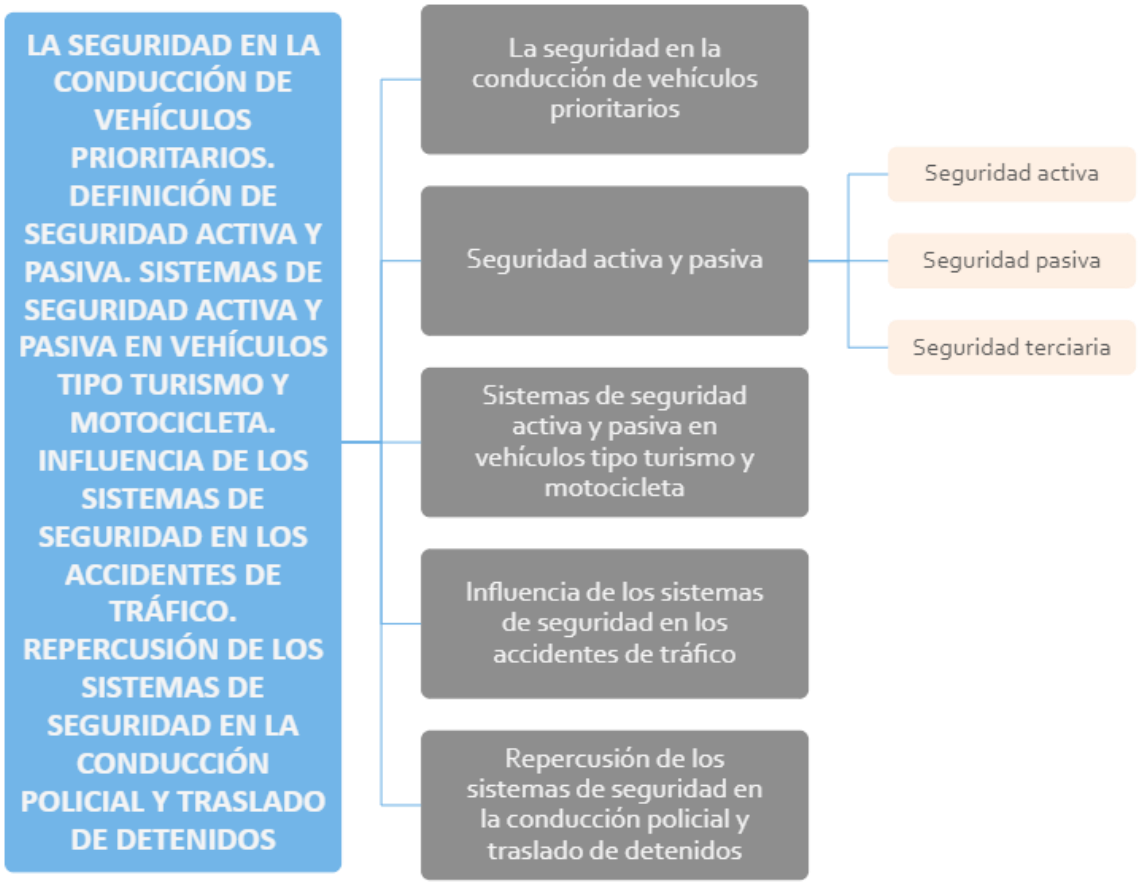
El estudio de la seguridad en la conducción prioritaria implica conocer la distinción entre seguridad activa, encargada de evitar accidentes, y seguridad pasiva, orientada a proteger a los ocupantes durante el impacto.

Además, es necesario analizar cómo estos sistemas repercuten en la seguridad de los agentes policiales y en el traslado de detenidos, garantizando un entorno más seguro para todos los implicados.

Objetivos

- Diferenciar entre los conceptos de seguridad activa, pasiva y terciaria, y su aplicación en vehículos tipo turismo y motocicletas.
- Analizar la influencia de los sistemas de seguridad en la reducción de accidentes de tráfico y la mitigación de sus consecuencias.
- Evaluar la repercusión de los sistemas de seguridad en la conducción policial y en el traslado seguro de detenidos, identificando las mejores prácticas.

Mapa Conceptual



1. La seguridad en la conducción de vehículos prioritarios

En el contexto de la regulación del tráfico y la seguridad vial, los vehículos prioritarios son aquellos que, por su función y la naturaleza del servicio que prestan, disponen de prerrogativas especiales en la circulación vial cuando se encuentran en un servicio urgente. Estos vehículos están exentos, bajo ciertas condiciones, del cumplimiento estricto de algunas normas de tráfico para asegurar la prestación rápida y eficiente de sus servicios esenciales. Su uso está generalmente reservado para situaciones de emergencia en las que es necesario reducir los tiempos de respuesta para proteger la vida, la salud o la seguridad de las personas y bienes.

Entre los **vehículos prioritarios en España** se encuentran:

- Vehículos de policía.
- Vehículos de extinción de incendios.
- Vehículos de protección civil y salvamento.
- Vehículos de asistencia sanitaria (tanto pública como privada).

La **prioridad en la circulación** se les otorga cuando cumplen las condiciones reglamentarias de aviso acústico y luminoso, tal y como estipula el Reglamento General de Circulación (RGC), de acuerdo con su artículo 68. Esto garantiza que estos vehículos puedan atravesar el tráfico de manera más ágil y segura.

ELEMENTOS ESENCIALES EN LA CONDUCCIÓN DE VEHÍCULOS PRIORITARIOS

La **conducción de vehículos prioritarios en España** está sujeta a una normativa específica que regula tanto los derechos y prerrogativas de estos vehículos como los deberes y responsabilidades de sus conductores. Los principales elementos esenciales de la conducción de estos vehículos incluyen:

Condiciones para Considerarse Prioritario

Un vehículo solo puede considerarse prioritario cuando se encuentra en servicio urgente y está debidamente identificado mediante:

- **Señal luminosa (Señal V-1):** Según el art. 68 del RGC, esta señal es de color azul y debe estar homologada conforme al Reglamento CEPE/ONU 65. Debe ser visible desde todas las direcciones y a una distancia mínima de 50 metros. Se coloca en la parte superior del vehículo, o, en el caso de motocicletas, en la parte trasera sobre un cabezal telescópico.
- **Señal acústica:** Se utiliza conjuntamente con la señal luminosa, mediante dispositivos acústicos especiales (sirenas). Las señales acústicas deben emplearse de manera intermitente y con una frecuencia que no genere confusión, con el objetivo de alertar a los usuarios de la vía.

Además, en situaciones en las que el uso de señales acústicas pueda causar peligro o molestia innecesaria (por ejemplo, en zonas cercanas a hospitales), los conductores pueden optar por utilizar únicamente la señal luminosa. Este es el caso en situaciones de no peligro tal como se recoge en el art. 68 del RGC.

Prioridad de Paso y Exención de Normas

En virtud del artículo 67 del RGC, los vehículos en servicio de urgencia tienen prioridad de paso sobre el resto de los vehículos y otros usuarios de la vía. Esto incluye la capacidad de:

Circular por encima de los límites de velocidad.

No cumplir con otras normas de tráfico o señales bajo determinadas condiciones (art. 25 de la LSV).

No obstante, los conductores de estos vehículos deben ejercer una prudencia extrema, especialmente en intersecciones o cruces de semáforos. A pesar de su derecho de paso, deben asegurarse de que no existe riesgo de colisión con otros vehículos o atropellos a peatones.

TEMA 45

Prevención de riesgos laborales en seguridad vial. Factores del tráfico y su influencia en la siniestralidad vial. Factor humano, factor ambiental y factor vehículo. Riesgos laborales en la conducción de vehículos prioritarios. Equipos de Protección Individual del conductor y pasajeros de vehículos policiales. Estrategias y mantenimiento preventivo del vehículo prioritario

Introducción

La prevención de riesgos laborales en seguridad vial es fundamental para garantizar la seguridad de los trabajadores que, en el desempeño de sus funciones, deben conducir vehículos, especialmente aquellos considerados prioritarios, como los utilizados por fuerzas policiales y servicios de emergencia. La correcta identificación y gestión de los factores que influyen en la siniestralidad vial, tanto del entorno como del conductor y el vehículo, es esencial para reducir los accidentes y mitigar sus consecuencias.

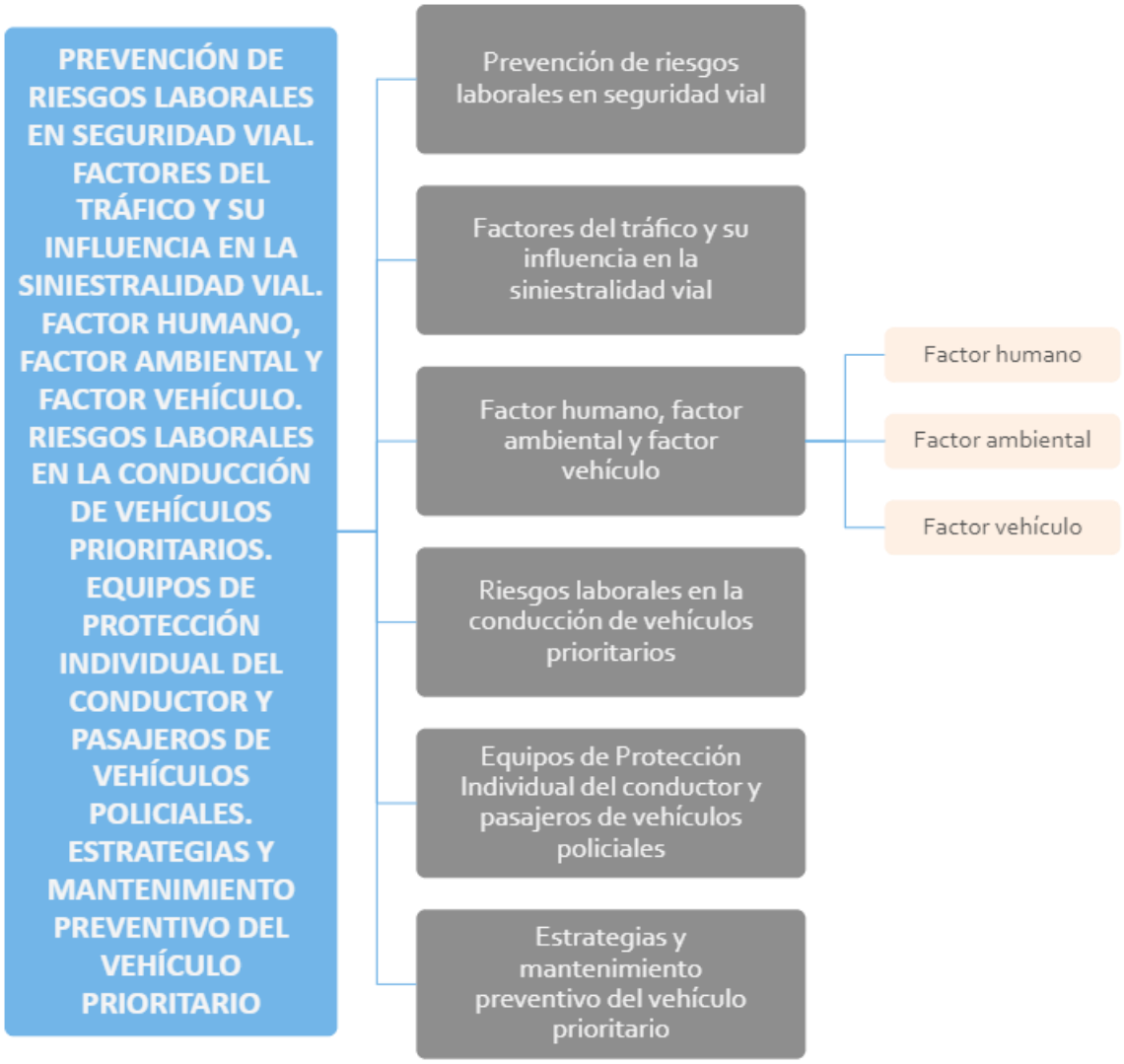
Este tema aborda la influencia de los factores del tráfico en la siniestralidad vial, con especial atención a los riesgos laborales asociados a la conducción de vehículos prioritarios.

Se detallarán aspectos clave como el factor humano, ambiental y del vehículo, así como el uso adecuado de equipos de protección individual y las estrategias de mantenimiento preventivo para minimizar los riesgos durante la conducción de estos vehículos.

Objetivos

- Analizar los factores del tráfico y su influencia en la siniestralidad vial, con especial atención a los factores humano, ambiental y del vehículo.
- Identificar los riesgos laborales específicos de la conducción de vehículos prioritarios y las medidas preventivas para mitigarlos.
- Conocer la importancia de los equipos de protección individual y las estrategias de mantenimiento preventivo del vehículo prioritario para garantizar la seguridad de conductores y pasajeros.

Mapa Conceptual



1. Prevención de riesgos laborales en seguridad vial

La **prevención de riesgos laborales** en el contexto de la seguridad vial es un aspecto crítico que se relaciona directamente con la protección de la salud y la integridad física de los trabajadores que utilizan vehículos como parte de su actividad laboral. La intersección entre el trabajo y la seguridad vial abarca una amplia gama de factores que deben ser considerados para minimizar los riesgos de accidentes de tráfico y sus consecuencias. Este análisis abordará la definición, los elementos esenciales y la regulación que rige esta materia en España.

La **prevención de riesgos laborales en seguridad vial** se define como el conjunto de acciones, normativas y procedimientos diseñados para identificar, evaluar y controlar los riesgos asociados a la conducción de vehículos en el ámbito laboral. Esto incluye cualquier actividad que implique el uso de vehículos de motor para el transporte de personas o mercancías, ya sea en el ámbito de la empresa o en el contexto de desplazamientos a nivel profesional.

La **identificación de riesgos** es el primer paso en la prevención de accidentes de tráfico en el ámbito laboral. Esto implica un análisis de las condiciones de trabajo, que incluye factores como el estado de las carreteras, la visibilidad, las condiciones meteorológicas y el estado mecánico de los vehículos. También es fundamental evaluar el entorno laboral, considerando los lugares de trabajo y las rutas más frecuentes, identificando aquellos que representan un mayor riesgo de accidentes. Además, se debe tener en cuenta la identificación de comportamientos de riesgo, analizando el comportamiento de los conductores y posibles distracciones que puedan afectar la seguridad vial.

La **evaluación de riesgos** consiste en analizar la probabilidad y las consecuencias de los accidentes identificados en la etapa anterior. Esto se puede realizar mediante matrices de riesgo, que ayudan a clasificar y priorizar los riesgos en función de su probabilidad de ocurrencia y la gravedad de sus consecuencias. También es recomendable revisar estadísticas de accidentes laborales para identificar patrones y áreas de mejora.

Una vez identificados y evaluados los riesgos, se deben establecer medidas de prevención y protección. Estas medidas pueden incluir la formación y concienciación de los empleados sobre conducción segura, normas de tráfico y gestión del estrés al volante. También es esencial implementar un mantenimiento regular de los vehículos para asegurar que estén en condiciones óptimas de funcionamiento. En algunos casos, el uso de elementos de protección como chalecos reflectantes, cascos o sistemas de seguridad puede ser necesario. Además, es fundamental establecer políticas de movilidad segura que regulen los desplazamientos laborales y el uso de vehículos de empresa.

La **vigilancia de la salud** es otra dimensión crucial en la prevención de riesgos laborales en seguridad vial, ya que es esencial para detectar condiciones que puedan afectar la capacidad de los empleados para conducir de manera segura. Esto incluye controles médicos regulares, como evaluaciones de salud que incluyan pruebas de visión, audición y chequeos de condiciones médicas que puedan influir en la conducción. También se debe realizar una evaluación de riesgos psicosociales para detectar factores como el estrés, la fatiga y otros problemas psicológicos que puedan impactar en el desempeño del conductor.

Llevar un registro adecuado de todas las actividades relacionadas con la prevención de riesgos laborales en seguridad vial es fundamental. Esto incluye informes de accidentes, que documentan todos los incidentes ocurridos, independientemente de su gravedad, para facilitar el análisis y la mejora continua. Además, es importante mantener un registro de los planes de formación realizados, incluyendo asistencia y resultados, así como de los protocolos de mantenimiento realizados en los vehículos.

La **investigación de accidentes laborales** es un elemento esencial para la mejora continua de la seguridad vial en el trabajo. Esto implica un análisis de las causas de los accidentes, identificando factores humanos, mecánicos y ambientales, así como la elaboración de recomendaciones basadas en los hallazgos de la investigación para evitar la repetición de incidentes similares.