Nombre de la institución: INSTITUTO TECNOLÓGICO DE COSTA RICA

Carrera: INGENIERÍA EN COMPUTACIÓN

Curso: TALLER DE PROGRAMACIÓN

Grupo: 4

Título del trabajo: QUIZ 4: INVESTIGACIÓN DESCRIPTIVA DE TÓPICOS DE COMPUTACIÓN: SISTEMA OPERATIVO, SISTEMAS NUMÉRICOS, ÉTICA Y MORAL, INTELIGENCIA ARTIFICIAL, CIBERSEGURIDAD

Autores: Ledvin Manuel Leiva Mata - 2023071280

Fecha de entrega: 21/05/2023

Semestre y año: Semestre 1 – año 2023

Nombre del profesor: William Mata Rodríguez

Contenido

1. Sistema Operativo

1.1 Funciones del sistema operativo

El sistema operativo es un componente esencial de cualquier computadora, ya sea un dispositivo móvil, una computadora personal o un servidor. Actúa como un intermediario entre el hardware y el software, facilitando la interacción entre el usuario y la máquina. Estas son algunas de las funciones básicas del sistema operativo:

1. **Gestión de recursos**: El sistema operativo administra y asigna los recursos de hardware, como la memoria, la CPU, los dispositivos de entrada/salida y el espacio de almacenamiento. Utiliza algoritmos y políticas para garantizar una asignación eficiente y justa de los recursos a los programas y procesos en ejecución.
2. **Interfaz de usuario**: Proporciona una interfaz que permite a los usuarios interactuar con la computadora. Puede ser una interfaz gráfica de usuario (GUI) o una interfaz de línea de comandos (CLI). La GUI utiliza elementos visuales como ventanas, iconos y menús desplegables para facilitar la interacción, mientras que la CLI permite al usuario ingresar comandos de texto para realizar tareas.
3. **Administración de archivos**: El sistema operativo gestiona los archivos en un sistema de archivos. Permite la creación, lectura, escritura y eliminación de archivos y directorios. También controla los permisos de acceso a los archivos y proporciona funciones para buscar y organizar archivos de manera eficiente.
4. **Administración de procesos**: El sistema operativo controla la ejecución de los procesos en la computadora. Un proceso es una instancia en ejecución de un programa. El sistema operativo asigna recursos a los procesos, los planifica y supervisa su ejecución. También permite la comunicación y sincronización entre los procesos.
5. **Gestión de la memoria**: Controla la asignación y liberación de memoria en la computadora. Administra la memoria física disponible y asigna porciones de ella a los procesos que la requieren. También realiza la traducción de direcciones virtuales a direcciones físicas y gestiona la memoria virtual si está disponible.

1.2 Características virtuales

Las características virtuales son las funcionalidades que se implementan y se proporcionan por el software, en lugar de depender exclusivamente de hardware físico. Estas características permiten una mayor flexibilidad, eficiencia y capacidad de adaptación en los sistemas informáticos. Algunas de ellas son:

1. **Máquinas virtuales**: Una máquina virtual es un entorno virtualizado que simula una computadora completa dentro de un sistema físico. Permite ejecutar múltiples sistemas operativos o aplicaciones en una misma máquina física, compartiendo los recursos de manera eficiente. Las máquinas virtuales proporcionan aislamiento y flexibilidad, lo que facilita el despliegue de entornos de prueba y desarrollo.

2. **Redes virtuales**: Las redes virtuales permiten la creación de redes lógicas a través de software, independientemente de la infraestructura física de red. Mediante la virtualización de switches, routers y firewalls, se pueden crear segmentos de red aislados y definir políticas de conectividad. Esto es especialmente útil en entornos de nube y virtualización, donde se requiere una gestión ágil y escalable de la conectividad de red.
3. **Almacenamiento virtualizado**:El almacenamiento virtualizado es una tecnología que hace que el hardware de almacenamiento sea más fácil de usar. Permite crear volúmenes y sistemas de archivos utilizando software en lugar de tener que lidiar directamente con el hardware físico. Esto simplifica la administración y el manejo del almacenamiento. Los dispositivos de almacenamiento físico se combinan y se presentan como un único recurso de almacenamiento, brindando flexibilidad en la asignación y gestión de espacio. Además, el almacenamiento virtualizado ofrece características como instantáneas (snapshots) y migración de datos en tiempo real.
4. **Escalabilidad elástica**: La escalabilidad elástica es una característica virtual que permite ajustar automáticamente la capacidad de cómputo, almacenamiento y recursos de red según la demanda. Los sistemas virtualizados pueden escalar horizontalmente (agregando más instancias virtuales) o verticalmente (asignando más recursos a una instancia virtual) de manera dinámica. Esto permite adaptarse a las fluctuaciones de carga de trabajo y garantizar un rendimiento óptimo sin interrupciones en los servicios.

1.3 Evolución del sistema operativo

Los sistemas operativos han avanzado significativamente desde sus inicios hasta la actualidad. Mientras se crean nuevas tecnologías y las necesidades de los usuarios se hacen mas exigentes, los sistemas operativos se han visto obligados a adaptarse. Algunas de las estabas de la evolución del sistema operativo son:

1. **Sistemas operativos de lote (Batch processing)**: En los primeros días de la informática, las tareas se ejecutaban en lotes, donde los programas y los datos se recopilaban y luego se procesaban en secuencia. Los sistemas operativos de lote, como el sistema operativo IBSYS y el sistema operativo UNIVAC, eran responsables de la administración de los trabajos, la asignación de recursos y la ejecución secuencial de los programas.

2. **Sistemas operativos de tiempo compartido**: A medida que las computadoras se volvieron más rápidas y potentes, se desarrollaron sistemas operativos de tiempo compartido, como el sistema operativo CTSS y el sistema operativo UNIX. Estos sistemas permitían que múltiples usuarios interactuaran con la computadora al mismo tiempo, compartiendo los recursos y ejecutando tareas concurrentemente. Se introdujeron conceptos como la multiprogramación y la administración de la memoria virtual para mejorar la eficiencia y la utilización de los recursos.

3. **Sistemas operativos de computadoras personales**: Cuando se popularizaron las computadoras personales en la década de 1980, surgieron sistemas operativos como MS-DOS y posteriormente Microsoft Windows. Estos sistemas operativos estaban diseñados para ser utilizados en computadoras de escritorio y ofrecían interfaces gráficas de usuario (GUI) que facilitaban la interacción y la ejecución de programas mediante el uso del mouse y las ventanas.

4. **Sistemas operativos de redes**: Con el incremento de las redes de computadoras, se desarrollaron sistemas operativos de redes como Novell NetWare y Windows NT. Estos sistemas permitían la comunicación y el intercambio de recursos entre computadoras conectadas en red, además se introdujeron características como el acceso remoto, el intercambio de archivos y la administración centralizada de recursos.

5. **Sistemas operativos móviles**: Con la llegada de los dispositivos móviles, se desarrollaron sistemas operativos específicos para satisfacer las necesidades de estos dispositivos. Ejemplos destacados son iOS de Apple, Android de Google y Windows Mobile el cual actualmente está descontinuado. Estos sistemas operativos móviles ofrecen interfaces táctiles, acceso a aplicaciones móviles y capacidades de conectividad inalámbrica.

6. **Sistemas operativos de nube**: Con el continuo desarrollo de la computación en la nube, se han desarrollado sistemas operativos diseñados para administrar y ejecutar servicios en la nube. Algunos ejemplos incluyen sistemas operativos como Kubernetes, que se utilizan para orquestar y administrar contenedores en entornos de nube, y sistemas operativos de proveedores de servicios en la nube como Amazon Web Services (AWS) y Microsoft Azure.

1.4 Arquitectura del sistema operativo

La arquitectura del sistema operativo se define como la estructura y organización interna del sistema operativo la cual establece como se gestionan y coordinan los componentes del sistema para dar soporte a los usuarios y aplicaciones. Estos son algunos de los componentes principales:

1.1 **Núcleo (Kernel**): El núcleo es el componente central del sistema operativo. Proporciona servicios básicos y es responsable de la gestión de recursos del sistema, como la asignación de memoria, la planificación de procesos, la gestión de dispositivos y el acceso a archivos. El núcleo interactúa directamente con el hardware y actúa como una capa de abstracción entre el hardware y los programas en ejecución.

1.2 **Sistema de archivos**: El sistema de archivos es responsable de la organización y gestión de los archivos en el sistema. Define la estructura de almacenamiento de los datos en el dispositivo de almacenamiento y proporciona funciones para crear, leer, escribir y eliminar archivos. El sistema de archivos también maneja los permisos de acceso a los archivos y la administración de directorios.

1.3 **Gestor de procesos**: El gestor de procesos se encarga de administrar los procesos en el sistema. Es responsable de la creación, ejecución, suspensión y terminación de los procesos. El gestor de procesos asigna los recursos necesarios, como la CPU y la memoria, a cada proceso y coordina su ejecución de manera eficiente.

1.4 **Gestor de memoria**: El gestor de memoria se encarga de administrar la memoria del sistema. Es responsable de asignar y liberar memoria a los procesos, así como de gestionar la memoria virtual si está disponible. El gestor de memoria utiliza técnicas como la paginación y la segmentación para optimizar el uso de la memoria y garantizar que cada proceso tenga acceso a la cantidad de memoria requerida.

1.5 **Gestor de dispositivos**: El gestor de dispositivos es responsable de la gestión de los dispositivos de entrada/salida (E/S) en el sistema. Proporciona una capa de abstracción entre los dispositivos de hardware y los programas que los utilizan. El gestor de dispositivos se encarga de la detección de dispositivos, el manejo de interrupciones, la asignación de recursos y la gestión de la comunicación entre los dispositivos y los programas.

Es importante destacar que la arquitectura del sistema operativo puede variar según el tipo de sistema operativo ya sea monolítico, microkernel o algún otro y también dependiendo de la plataforma en la que se ejecuta dígase computadoras personales, dispositivos móviles, servidores y demás.

2. Sistemas numéricos

2.1. Representación y operaciones aritméticas básicas

La representación y las operaciones aritméticas básicas son fundamentales en el campo de la computación. En el mundo de la informática, se necesita encontrar la manera de representar números y realizar operaciones matemáticas con ellos.

Cuando se habla de representación de números, se refiere a cómo los números son expresados en el mundo de las computadoras. En los sistemas informáticos, se utiliza principalmente tres formatos: binario (base 2), decimal (base 10) y hexadecimal (base 16). En la representación binaria, solo se utilizan dos dígitos, 0 y 1. En los sistemas informáticos, los números se representan en forma de "bits", donde cada bit puede ser 0 o 1. También existen métodos para representar números negativos, como el complemento base dos.

Las operaciones aritméticas básicas: suma, resta, multiplicación y división. Estas operaciones son esenciales para realizar cálculos en los sistemas informáticos.

La suma consiste en añadir dos números juntos. En los sistemas binarios, esto se hace bit a bit, teniendo en cuenta los acarreos generados en cada posición.

La resta es la operación inversa a la suma, donde restamos un número de otro. Al igual que en la suma, en los sistemas binarios, se realiza bit a bit, considerando los préstamos generados en cada posición.

La multiplicación implica repetir la suma de un número (multiplicando) según el valor de los dígitos del otro número (multiplicador). En los sistemas binarios, también se realiza bit a bit, teniendo en cuenta los desplazamientos y las sumas parciales.

La división es la operación de encontrar cuántas veces un número (divisor) cabe en otro número (dividendo). Al igual que en las otras operaciones, en los sistemas binarios, se realiza bit a bit, considerando los desplazamientos y las substracciones parciales.

Hoy en día los sistemas informáticos utilizan algoritmos y circuitos especializados para realizar estas operaciones de manera eficiente y rápida.

2.1.1. Sistema binario

El sistema binario es un sistema de numeración que utiliza solo dos dígitos: 0 y 1. A diferencia del sistema decimal, que utiliza diez dígitos (del 0 al 9), el sistema binario se basa en potencias de 2. Cada posición en un número binario representa una potencia de 2, comenzando desde la posición más a la derecha.

En el sistema binario, cada dígito se llama bit. Un bit puede tener dos posibles valores: 0 o 1. La secuencia de bits se utiliza para representar información en los sistemas digitales, como las computadoras.

La conversión entre el sistema decimal y el binario es común en informática. Para convertir un número decimal a binario, se divide sucesivamente por 2 y se toman los residuos en cada paso, hasta que el cociente sea 0. Luego, los residuos se escriben en orden inverso, de abajo hacia arriba, para obtener la representación binaria del número.

Por ejemplo, para convertir el número decimal 13 a binario:

13 ÷ 2 = 6 (residuo 1)

6 ÷ 2 = 3 (residuo 0)

3 ÷ 2 = 1 (residuo 1)

1 ÷ 2 = 0 (residuo 1)

Luego, los residuos se escriben en orden inverso: 1101. Por lo tanto, el número binario equivalente a 13 es 1101.

De manera similar, se puede convertir un número binario a decimal utilizando la posición de cada bit y multiplicándolo por la potencia correspondiente de 2.

2.1.2. Sistema octal

El sistema octal es un sistema de numeración que utiliza ocho dígitos: 0, 1, 2, 3, 4, 5, 6 y 7. Similar al sistema binario, el sistema octal se utiliza para representar números en base a potencias de 8.

En el sistema octal, cada posición en un número octal representa una potencia de 8, comenzando desde la posición más a la derecha. Al igual que en otros sistemas numéricos, los números octales pueden ser positivos o negativos.

La conversión entre el sistema decimal y el octal es similar a la conversión al sistema binario. Para convertir un número decimal a octal, se divide sucesivamente por 8 y se toman los residuos en cada paso, hasta que el cociente sea 0. Luego, los residuos se escriben en orden inverso, de abajo hacia arriba, para obtener la representación octal del número.

Por ejemplo, para convertir el número decimal 56 a octal:

56 ÷ 8 = 7 (residuo 0)

7 ÷ 8 = 0 (residuo 7)

Luego, los residuos se escriben en orden inverso: 70. Por lo tanto, el número octal equivalente a 56 es 70.

De manera similar, se puede convertir un número octal a decimal utilizando la posición de cada dígito y multiplicándolo por la potencia correspondiente de 8.

2.1.3. Sistema hexadecimal

El sistema hexadecimal es un sistema de numeración que utiliza dieciséis dígitos: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E y F. A diferencia del sistema decimal, que utiliza diez dígitos (del 0 al 9), el sistema hexadecimal se basa en potencias de 16. Los dígitos adicionales (A a F) se utilizan para representar valores numéricos del 10 al 15.

En el sistema hexadecimal, cada posición en un número hexadecimal representa una potencia de 16, comenzando desde la posición más a la derecha. Al igual que en otros sistemas numéricos, los números hexadecimales pueden ser positivos o negativos.

La conversión entre el sistema decimal y el hexadecimal se realiza dividiendo sucesivamente el número decimal por 16 y tomando los residuos en cada paso, hasta que el cociente sea 0. Luego, los residuos se escriben en orden inverso, de abajo hacia arriba, para obtener la representación hexadecimal del número. Los dígitos adicionales (A a F) se utilizan para representar valores numéricos del 10 al 15.

Por ejemplo, para convertir el número decimal 255 a hexadecimal:

255 ÷ 16 = 15 (residuo F)

15 ÷ 16 = 0 (residuo 15)

Luego, los residuos se escriben en orden inverso: FF. Por lo tanto, el número hexadecimal equivalente a 255 es FF.

De manera similar, se puede convertir un número hexadecimal a decimal utilizando la posición de cada dígito y multiplicándolo por la potencia correspondiente de 16.

El sistema hexadecimal es ampliamente utilizado en la informática y la programación, especialmente en áreas como la representación de direcciones de memoria, la representación de colores (como en el sistema RGB) y la manipulación de datos binarios.

2.2. Conversión entre bases: decimal, binario, octal, hexadecimal

La conversión entre diferentes bases numéricas, como decimal, binario, octal y hexadecimal, es una habilidad importante en informática y programación.

Conversión de decimal a binario:

1. Divide el número decimal sucesivamente por 2.
2. Escribe los residuos en orden inverso, de abajo hacia arriba.
3. El resultado será la representación binaria del número.

Ejemplo: Convertir el número decimal 25 a binario.

25 ÷ 2 = 12 (residuo 1)

12 ÷ 2 = 6 (residuo 0)

6 ÷ 2 = 3 (residuo 0)

3 ÷ 2 = 1 (residuo 1)

1 ÷ 2 = 0 (residuo 1)

La representación binaria de 25 es 11001.

Conversión de binario a decimal:

1. Multiplica cada dígito binario por la potencia correspondiente de 2.
2. Suma los resultados obtenidos.

Ejemplo: Convertir el número binario 11001 a decimal.

$1 * 2^4 + 1 * 2^3 + 0 * 2^2 + 0 * 2^1 + 1 * 2^0 = 16 + 8 + 0 + 0 + 1 = 25$.

Conversión de decimal a octal:

1. Divide el número decimal sucesivamente por 8.
2. Escribe los residuos en orden inverso, de abajo hacia arriba.
3. El resultado será la representación octal del número.

Ejemplo: Convertir el número decimal 42 a octal.

42 ÷ 8 = 5 (residuo 2)

5 ÷ 8 = 0 (residuo 5)

La representación octal de 42 es 52.

Conversión de octal a decimal:

1. Multiplica cada dígito octal por la potencia correspondiente de 8.
2. Suma los resultados obtenidos.

Ejemplo: Convertir el número octal 52 a decimal.

$5 * 8^1 + 2 * 8^0 = 40 + 2 = 42$.

Conversión de decimal a hexadecimal:

1. Divide el número decimal sucesivamente por 16.
2. Escribe los residuos en orden inverso, de abajo hacia arriba.
3. Utiliza los dígitos adicionales (A, B, C, D, E, F) para representar valores del 10 al 15 en el mismo orden.

Ejemplo: Convertir el número decimal 168 a hexadecimal.

168 ÷ 16 = 10 (residuo 8)

10 ÷ 16 = 0 (residuo 10)

La representación hexadecimal de 168 es A8.

Conversión de hexadecimal a decimal:

1. Multiplica cada dígito hexadecimal por la potencia correspondiente de 16.
2. Utiliza los dígitos adicionales (A, B, C, D, E, F) para representar valores del 10 al 15.
3. Suma los resultados obtenidos.

Ejemplo: Convertir el número hexadecimal A8 a decimal.

$10 * 16^1 + 8 * 16^0 = 160 + 8 = 168$.

2.3. Representación de los números enteros

Representar los números enteros en los sistemas digitales computadoras, teléfonos, entre otros, se realiza utilizando diferentes esquemas, los mas comunes son el binario y el complemento base dos.

Representación binaria:

En el sistema binario, los números enteros se representan utilizando únicamente los dígitos 0 y 1. La posición de cada bit representa una potencia de 2. El bit más a la derecha tiene una posición de 2^0, el siguiente tiene una posición de 2^1, el siguiente de 2^2 y así sucesivamente.

Por ejemplo, el número binario 1010 representa el número decimal 10. Cada dígito (0 o 1) en la secuencia binaria se multiplica por la potencia correspondiente de 2 y se suma el resultado.

Representación en complemento a dos:

El sistema complemento a dos es un esquema utilizado para representar números enteros tanto positivos como negativos. En este sistema, se utiliza el bit más significativo (el bit más a la izquierda) como el bit de signo. Si este bit es 0, el número es positivo; si es 1, el número es negativo.

La representación en complemento a dos se basa en la idea de complementar y sumar. Para representar un número negativo, se toma el valor absoluto del número en binario, se complementan todos los bits y luego se le suma 1 al resultado. Por ejemplo, para representar -5 en una representación de 8 bits:

El número 5 en binario es 00000101.

Se complementan todos los bits: 11111010.

Se le suma 1: 11111011.

Por lo tanto, la representación en complemento a dos de -5 en una representación de 8 bits es 11111011.

Nota: Es importante tener en cuenta que la cantidad de bits utilizados para representar números enteros en un sistema determinado afecta al rango de valores que se pueden representar. Por ejemplo, con 8 bits se pueden representar valores entre -128 y 127 en complemento a dos.

2.4. Representación de fracciones

Representar los números fraccionarios en los sistemas digitales se realiza utilizando diferentes métodos como el punto flotante y la representación en punto fijo.

Representación en punto flotante:

En la representación en punto flotante, se utilizan dos partes principales para representar una fracción: la mantisa y el exponente. La mantisa almacena la parte

significativa de la fracción, mientras que el exponente indica la posición decimal de la mantisa.

La mantisa suele ser representada en binario, y el exponente puede ser representado en binario o en otro sistema numérico, como el sistema decimal o el sistema binario codificado en exceso. Esta representación permite expresar tanto números fraccionarios como números enteros de gran magnitud o pequeña magnitud.

El estándar IEEE 754 es ampliamente utilizado para la representación en punto flotante en sistemas informáticos.

Representación en punto fijo:

En la representación en punto fijo, se asigna una posición fija para la parte entera y la parte fraccionaria de la fracción. Se decide de antemano la cantidad de bits que se utilizarán para representar la parte entera y la parte fraccionaria. Esto implica que el rango y la precisión de la representación están predeterminados.

Por ejemplo, si se decide utilizar 8 bits para representar una fracción en punto fijo, se pueden asignar, por ejemplo, 4 bits para la parte entera y 4 bits para la parte fraccionaria. Esto permitiría representar valores fraccionarios con una precisión limitada.

Es importante tener en cuenta que, en la representación en punto fijo, la posición decimal está fija y no puede ser ajustada dinámicamente. Esto puede limitar la capacidad de representar números fraccionarios con gran precisión o de manejar rangos amplios.

Estos son solo dos de los métodos más comunes utilizados para la representación de fracciones en sistemas digitales. Existen otros enfoques y técnicas, como el uso de números de coma flotante de precisión arbitraria (big float), que permiten mayor precisión y manejo de rangos más amplios.

3. Ética y moral

3.1 La ética y la moral asociadas con el uso de computadoras

La ética y la moral son aspectos fundamentales que deben considerarse en el uso de las computadoras y la tecnología en general. Estos conceptos están relacionados con los principios y valores que guían nuestras acciones y decisiones en el ámbito de la tecnología. Algunos puntos para destacar son:

1. **Privacidad y seguridad de la información:**
   La privacidad y la seguridad de la información son temas éticos cruciales. Los usuarios y los profesionales de la tecnología tienen la responsabilidad de proteger la información personal y confidencial de las personas. Esto implica tomar medidas para garantizar la seguridad de los datos, respetar la privacidad de los usuarios y cumplir con las leyes y regulaciones relacionadas con la protección de datos.
2. **Acceso equitativo y brecha digital:**
   El acceso equitativo a la tecnología es una preocupación ética. En un mundo cada vez más digitalizado, es importante garantizar que todas las personas tengan acceso a la tecnología y a los recursos digitales. La brecha digital, que se refiere a las desigualdades en el acceso y la habilidad para utilizar la tecnología, plantea cuestiones de justicia y equidad que deben abordarse de manera ética.
3. **Responsabilidad y transparencia:**
   Los profesionales de la tecnología tienen la responsabilidad de desarrollar y utilizar sistemas y aplicaciones de manera ética y transparente. Esto implica garantizar que los productos y servicios tecnológicos sean seguros, confiables y que cumplan con los estándares éticos y legales. También es importante ser transparente en cuanto a cómo se recopila, utiliza y comparte la información de los usuarios.
4. **Ética en la inteligencia artificial y la automatización:**
   La inteligencia artificial (IA) plantea desafíos éticos adicionales. Las decisiones tomadas por los sistemas de IA pueden tener un impacto significativo en la vida de las personas. La equidad, la justicia, la privacidad y la transparencia deben considerarse al desarrollar y utilizar sistemas de IA. Además, se deben evitar sesgos y discriminaciones injustas en los algoritmos y las decisiones automatizadas.
5. **Responsabilidad social y ambiental:**
   El uso de computadoras y tecnología también conlleva responsabilidades sociales y ambientales. Es importante considerar el impacto social de las tecnologías, como el empleo, la automatización y la exclusión social. Asimismo, la sostenibilidad ambiental debe ser tenida en cuenta, desde el diseño de hardware eficiente hasta el manejo adecuado de los desechos electrónicos.

3.2 Aspectos legales asociados con el uso de computadoras

El uso de computadoras y tecnología está sujeto a una serie de aspectos legales que deben ser considerados y respetados. Estos aspectos legales abarcan diferentes áreas y regulaciones, y su cumplimiento es crucial para garantizar un uso adecuado de las computadoras. Algunos de los aspectos legales más relevantes asociados con el uso de computadoras:

1. **Derechos de autor y propiedad intelectual:**
   Las leyes de derechos de autor y propiedad intelectual protegen las creaciones originales, como software, música, películas, libros y otros contenidos. Es importante respetar los derechos de autor y obtener las licencias adecuadas para utilizar y distribuir contenido protegido. El uso no autorizado de software, por ejemplo, puede ser una violación de la ley de derechos de autor.
2. **Privacidad y protección de datos:**
   Las leyes de privacidad y protección de datos regulan cómo se recopila, utiliza y almacena la información personal de los individuos. Es importante obtener el consentimiento adecuado para recopilar y utilizar datos personales y garantizar la seguridad de la información. Ejemplos de leyes relevantes incluyen el Reglamento General de Protección de Datos (RGPD) en la Unión Europea y leyes de privacidad como el California Consumer Privacy Act (CCPA) en Estados Unidos.
3. **Seguridad informática:**
   La seguridad informática es un aspecto legal importante. El acceso no autorizado a sistemas informáticos, el robo de información confidencial y los ataques cibernéticos son delitos punibles por la ley. Es necesario tomar medidas para proteger los sistemas y la información, y cumplir con las leyes y regulaciones relacionadas con la seguridad informática.
4. **Leyes de comercio electrónico:**
   El comercio electrónico y las transacciones en línea están regulados por leyes específicas. Estas leyes abarcan áreas como la protección del consumidor, la firma electrónica, la protección de datos en transacciones en línea y el cumplimiento de regulaciones fiscales. Es importante cumplir con las leyes de comercio electrónico aplicables al realizar transacciones en línea.
5. **Leyes de propiedad industrial:**
   Las leyes de propiedad industrial protegen las marcas registradas, patentes y diseños industriales. Estas leyes regulan el uso y la protección de marcas comerciales, invenciones y diseños, y garantizan que no se infrinjan los derechos de propiedad industrial de terceros.

3.3 Casos reales (mínimo 2) relacionados con el tema a nivel Costa Rica

1. El uso de ordenadores para seguir y controlar a los empleados.

En Costa Rica, como en muchos otros países, los empleadores utilizan cada vez más los ordenadores para rastrear y supervisar el trabajo de sus empleados. Esto se puede hacer a través de una variedad de medios, como el registro de pulsaciones de teclas, cámaras web y seguimiento por GPS. Aunque esta tecnología puede utilizarse para mejorar la productividad y la eficiencia, también plantea una serie de problemas éticos y morales.

Uno de ellos es que los empleados pueden sentir que se invade su intimidad. Cuando los empleadores son capaces de rastrear y supervisar cada pulsación del teclado y cada clic del ratón, puede dar la sensación de que siempre están siendo vigilados. Esto puede hacer que los empleados se sientan estresados y ansiosos, y también puede hacer que sean menos propensos a ser creativos o a asumir riesgos.

Otra preocupación es que el uso de la vigilancia informática pueda dar lugar a discriminación. Por ejemplo, si un empresario hace un seguimiento del tiempo que los empleados pasan en las redes sociales, es más probable que despida a los que considere menos productivos. Esto podría conducir a la discriminación contra ciertos grupos de empleados, como las mujeres y las minorías.

2. El uso de ordenadores para difundir información errónea.

Costa Rica es un país con un alto nivel de acceso a Internet. Esto significa que los ticos están cada vez más expuestos a la desinformación en línea. Esto puede ser un problema por varias razones.

En primer lugar, la desinformación puede llevar a la gente a tomar malas decisiones. Por ejemplo, si la gente cree que un determinado medicamento es peligroso, es posible que no lo tome, aunque sea el mejor tratamiento para su enfermedad. Esto puede provocar graves problemas de salud.

En segundo lugar, la desinformación puede erosionar la confianza en las instituciones. Si la gente cree que el gobierno le miente, es menos probable que siga las normas o participe en el proceso democrático. Esto puede provocar inestabilidad y conflictos.

En tercer lugar, la desinformación puede utilizarse para manipular a la gente. Por ejemplo, las campañas políticas utilizan a menudo la desinformación para intentar influir en los votantes. Esto puede llevar a la gente a votar por candidatos que no les benefician.

3.4 Casos reales (mínimo 2) relacionados con el tema a nivel internacional

1. El uso de ordenadores para crear deepfakes.

Los deepfakes son vídeos o imágenes que han sido manipulados para que parezca que alguien está diciendo o haciendo algo que en realidad nunca dijo o hizo. Los deepfakes pueden utilizarse para difundir información errónea, dañar la reputación de alguien o incluso cometer fraude.
Por ejemplo, en 2019, se creó un vídeo deepfake que hacía parecer que el expresidente de Estados Unidos Barack Obama respaldaba una estafa de criptodivisas. El video se compartió millones de veces en las redes sociales, y causó una gran confusión y daño a la reputación de Obama.
Los deepfakes son una grave amenaza para nuestra privacidad y nuestra seguridad. Es importante ser conscientes de los peligros de los deepfakes y tomar medidas para protegernos de ellos.

2. El uso de ordenadores para cometer ciberdelitos.

Ciberdelincuencia es un término amplio que se refiere a cualquier delito que se comete utilizando un ordenador o una red. La ciberdelincuencia puede incluir cosas como la piratería informática, el robo de identidad y el fraude.
La ciberdelincuencia es un problema creciente, y se estima que el coste global de la ciberdelincuencia asciende a billones de dólares. La ciberdelincuencia puede tener un impacto devastador en particulares y empresas.
Hay varias cosas que podemos hacer para protegernos de la ciberdelincuencia. Podemos utilizar contraseñas seguras, mantener nuestro software actualizado y tener cuidado con la información que compartimos en línea. También podemos informar a las autoridades de cualquier actividad sospechosa.

4. Inteligencia artificial.

4.1 Definición, ventajas e inconvenientes

Definición de la inteligencia artificial:

La inteligencia artificial se define como la capacidad de las máquinas para exhibir características y habilidades asociadas con la inteligencia humana, como el aprendizaje, la adaptación, el razonamiento lógico, la resolución de problemas y la toma de decisiones.

Ventajas de la inteligencia artificial:

1. **Automatización de tareas**: La IA permite automatizar tareas repetitivas y tediosas, lo que aumenta la eficiencia y libera a los humanos para tareas más complejas y creativas.
2. **Toma de decisiones basada en datos**: Los sistemas de IA pueden analizar grandes volúmenes de datos de manera rápida y precisa, lo que ayuda a tomar decisiones fundamentadas y mejorar la eficacia de los procesos empresariales.
3. **Capacidad de aprendizaje**: La IA puede aprender de forma autónoma a partir de los datos y mejorar su desempeño con el tiempo, lo que permite adaptarse a nuevas situaciones y optimizar resultados.
4. **Personalización y mejora de la experiencia del usuario**: La IA puede analizar los patrones de comportamiento de los usuarios y ofrecer experiencias personalizadas, como recomendaciones de productos o servicios adaptados a los intereses individuales.
5. **Avances en la investigación y la medicina**: La IA ha demostrado su capacidad para acelerar la investigación científica y médica, ayudando en el descubrimiento de nuevos medicamentos, diagnósticos precisos y tratamientos más efectivos.

Inconvenientes de la inteligencia artificial:

1. **Desplazamiento laboral**: La automatización impulsada por la IA puede llevar a la pérdida de empleos en ciertos sectores, lo que plantea desafíos sociales y económicos.
2. **Sesgo y discriminación**: Los sistemas de IA pueden estar sujetos a sesgos inherentes a los datos con los que se entrenan, lo que puede llevar a decisiones injustas o discriminatorias si no se maneja correctamente.
3. **Privacidad y seguridad**: El uso de la IA implica la recopilación y el análisis de grandes cantidades de datos personales, lo que plantea preocupaciones sobre la privacidad y la seguridad de la información.
4. **Falta de comprensión y transparencia**: Los algoritmos de IA a menudo son complejos y difíciles de interpretar. Esto puede plantear problemas éticos y legales, ya que es importante comprender cómo se toman las decisiones y qué datos se utilizan para ello.

5. **Dependencia tecnológica**: La dependencia excesiva de la IA puede llevar a problemas si los sistemas fallan o no funcionan correctamente, lo que resalta la importancia de contar con salvaguardias y soluciones de respaldo.

4.2 Impacto de la IA en la vida cotidiana

La inteligencia artificial (IA) ha tenido un impacto significativo en la vida cotidiana de las personas en diversos aspectos, algunos de los cambios se han producido por las siguientes razones:

1. **Asistentes virtuales**: Los asistentes virtuales como Siri, Alexa o Google Assistant utilizan técnicas de IA para reconocer y responder a comandos de voz. Estos asistentes nos permiten realizar tareas como realizar llamadas, enviar mensajes, reproducir música, buscar información en Internet o controlar dispositivos inteligentes en nuestro hogar.

2. **Recomendaciones personalizadas**: Los algoritmos de IA analizan nuestros patrones de comportamiento y preferencias para proporcionar recomendaciones personalizadas en servicios como Netflix, Spotify, Amazon y otras plataformas de comercio electrónico. Esto nos ayuda a descubrir nuevas películas, canciones, productos y servicios adaptados a nuestros gustos individuales.

3. **Traducción automática**: La IA ha mejorado significativamente la capacidad de traducción automática, lo que facilita la comunicación entre personas que hablan diferentes idiomas. Servicios como Google Translate o DeepL utilizan algoritmos de IA para traducir texto y voz en tiempo real, permitiéndonos comunicarnos más fácilmente con personas de todo el mundo.

4. **Detección de fraudes y seguridad**: Los sistemas de IA se utilizan para detectar patrones y anomalías en transacciones financieras, lo que ayuda a identificar y prevenir fraudes. Además, la IA también se utiliza en sistemas de seguridad como reconocimiento facial, identificación de huellas dactilares y detección de comportamientos sospechosos para garantizar la seguridad en lugares públicos y en el acceso a dispositivos.

5. **Automatización en el hogar**: La IA ha facilitado la automatización en el hogar a través de dispositivos inteligentes. Desde termostatos que ajustan automáticamente la temperatura, hasta sistemas de seguridad conectados y electrodomésticos inteligentes, la IA permite controlar y administrar diferentes aspectos de nuestro hogar de manera más eficiente y conveniente.

6. **Salud y diagnóstico médico**: La IA se ha aplicado en el campo de la salud para ayudar en el diagnóstico médico, analizando grandes cantidades de datos y detectando patrones que los médicos podrían pasar por alto. Esto ha llevado a una mayor precisión en el diagnóstico de enfermedades y ha mejorado los tratamientos personalizados.

4.3 Impacto de la IA en las empresas

La inteligencia artificial (IA) ha tenido un impacto significativo en las empresas, transformando la forma en que operan y ofrecen sus productos y servicios. A continuación, algunas áreas en las que la IA ha influido en el mundo empresarial son:

1. **Automatización de tareas**: La IA ha permitido la automatización de tareas rutinarias y repetitivas, lo que ha llevado a una mayor eficiencia y productividad en las empresas. Los sistemas de IA pueden realizar tareas como la recopilación y análisis de datos, la atención al cliente, la gestión de inventario y la optimización de procesos, liberando tiempo y recursos para que los empleados se enfoquen en actividades más estratégicas y de mayor valor.
2. **Análisis de datos y toma de decisiones**: La IA ha mejorado la capacidad de las empresas para analizar grandes volúmenes de datos de manera rápida y precisa. Los algoritmos de aprendizaje automático y el análisis predictivo permiten identificar patrones, tendencias y oportunidades comerciales. Esto ayuda a las empresas a tomar decisiones más informadas y basadas en datos, lo que puede tener un impacto significativo en la eficacia operativa y la toma de decisiones estratégicas.
3. **Personalización y experiencia del cliente**: La IA permite a las empresas ofrecer experiencias personalizadas a sus clientes. A través del análisis de datos, la IA puede comprender y predecir las preferencias individuales de los clientes, lo que facilita la personalización de productos, servicios y recomendaciones. Esto mejora la experiencia del cliente, aumenta la satisfacción y fomenta la lealtad hacia la marca.
4. **Servicio al cliente y chatbots**: Los sistemas de IA, como los chatbots, se utilizan cada vez más para brindar atención al cliente automatizada y asistencia en tiempo real. Los chatbots pueden responder preguntas comunes, proporcionar información y resolver problemas básicos, lo que reduce la carga de trabajo del personal de atención al cliente y mejora la eficiencia en la atención al cliente.
5. **Optimización de procesos y cadena de suministro**: La IA se utiliza para optimizar los procesos empresariales y la gestión de la cadena de suministro. Los algoritmos de IA pueden predecir la demanda, optimizar la planificación de inventario, identificar ineficiencias en los procesos de producción y logística, y proporcionar recomendaciones para mejorar la eficiencia y reducir los costos operativos.

6. **Seguridad cibernética**: La IA se ha convertido en una herramienta importante en la detección y prevención de amenazas cibernéticas. Los sistemas de IA pueden analizar grandes cantidades de datos en tiempo real para identificar patrones sospechosos y detectar posibles ataques cibernéticos. Esto ayuda a las empresas a proteger sus sistemas y datos de manera más efectiva.

Si bien la IA ofrece muchas ventajas para las empresas, también plantea desafíos, como la necesidad de abordar cuestiones éticas y de privacidad, garantizar la transparencia en los algoritmos y equilibrar el papel de la IA con la toma de decisiones humanas. Es fundamental que las empresas implementen la IA de manera responsable y ética, considerando el impacto en los empleados, los clientes y la sociedad en general.

4.4 Impacto de la IA en la educación desde el punto de la enseñanza

1. **Análisis de datos y predicción del rendimiento**: La IA puede analizar grandes volúmenes de datos educativos, como las calificaciones, el comportamiento de los estudiantes y los patrones de aprendizaje, para identificar tendencias y predecir el rendimiento futuro de los estudiantes. Esto ayuda a los educadores a intervenir de manera temprana y ofrecer apoyo adicional a los estudiantes que lo necesitan, mejorando así sus resultados académicos.
2. **Recursos educativos inteligentes**: La IA se utiliza para desarrollar recursos educativos interactivos e inteligentes. Estos recursos, como aplicaciones móviles, plataformas de aprendizaje en línea y simulaciones, utilizan técnicas de IA para adaptarse a las necesidades y estilos de aprendizaje de los estudiantes, ofreciendo contenido relevante y experiencias de aprendizaje enriquecedoras.
3. **Automatización de tareas administrativas**: La IA puede ayudar a automatizar tareas administrativas en las instituciones educativas, como la gestión de registros estudiantiles, la programación de horarios, la evaluación y el análisis de exámenes. Esto permite a los educadores dedicar más tiempo a la enseñanza y la interacción con los estudiantes.
4. **Acceso a la educación**: La IA también puede contribuir a mejorar el acceso a la educación en áreas remotas o desfavorecidas. A través de plataformas de aprendizaje en línea y sistemas de tutoría basados en IA, los estudiantes pueden acceder a recursos educativos y recibir instrucción de calidad, sin importar su ubicación geográfica.

Es importante destacar que la IA en la educación no pretende reemplazar a los educadores, sino complementar su labor y potenciar el proceso de enseñanza-aprendizaje. La interacción humana, la tutoría y el apoyo emocional siguen siendo fundamentales en el entorno educativo.

4.5 Impacto de la IA en la educación desde el punto de vista del aprendizaje

El impacto de la inteligencia artificial (IA) en la educación desde el punto de vista del aprendizaje ha sido significativo y prometedor, Algunos aspectos del impacto de la IA en el proceso de aprendizaje son:

1. **Personalización del aprendizaje**: La IA permite adaptar el proceso de enseñanza a las necesidades individuales de los estudiantes. Los sistemas de IA pueden analizar datos sobre el rendimiento y las preferencias de los estudiantes, y proporcionar recomendaciones y recursos personalizados para optimizar su aprendizaje. Esto ayuda a abordar las diferencias individuales y a mejorar la efectividad del aprendizaje.
2. **Tutoría y retroalimentación automatizada**: Los sistemas de IA pueden proporcionar tutoría y retroalimentación a los estudiantes de manera automatizada. Los chatbots educativos y los programas de tutoría basados en IA pueden responder preguntas, brindar explicaciones y evaluar el progreso de los estudiantes de forma instantánea y precisa. Esto facilita el acceso a la ayuda y el apoyo individualizado en cualquier momento y lugar.
3. **Acceso a recursos educativos y aprendizaje en línea**: La IA ha facilitado el acceso a recursos educativos y el aprendizaje en línea. Los sistemas de recomendación basados en IA pueden proporcionar a los estudiantes sugerencias de cursos, materiales y actividades relevantes según sus intereses y objetivos de aprendizaje. Además, la IA ha impulsado el desarrollo de plataformas y aplicaciones de aprendizaje en línea que utilizan técnicas de IA, como el procesamiento del lenguaje natural y el reconocimiento de voz, para ofrecer experiencias de aprendizaje interactivas y personalizadas.
4. **Identificación temprana de dificultades de aprendizaje**: La IA puede ayudar a identificar tempranamente las dificultades de aprendizaje de los estudiantes. Al analizar los datos de los estudiantes y utilizar modelos predictivos, la IA puede detectar patrones o señales que indiquen la necesidad de intervención o apoyo adicional. Esto permite a los educadores intervenir de manera oportuna y proporcionar estrategias de apoyo adecuadas para ayudar a los estudiantes a superar las dificultades y mejorar su rendimiento académico.

Es importante destacar que, si bien la IA ofrece muchas oportunidades y beneficios en el aprendizaje, también se plantean desafíos, como la necesidad de garantizar la privacidad y seguridad de los datos, abordar sesgos algorítmicos y mantener un equilibrio adecuado entre la tecnología y la interacción humana en el entorno educativo.

4.6 Algunas herramientas de IA (describa en términos generales ChatGPT y otras 2 herramientas)

ChatGPT: es un gran modelo de lenguaje, también conocido como IA conversacional o chatbot entrenado para ser informativo y comprensivo. Se ha entrenado a partir de una gran cantidad de datos de texto y puede comunicarse y generar texto similar al humano en respuesta a una amplia gama de peticiones y preguntas. Por ejemplo, ChatGPT puede proporcionar resúmenes de temas objetivos o crear historias.

Midjourney: es una nueva tecnología de IA capaz de crear imágenes a partir de descripciones de texto. Aún está en fase de desarrollo, pero ya se ha utilizado para crear algunas imágenes impresionantes. Para utilizar Midjourney, basta con escribir una descripción de la imagen que se quiere crear. Por ejemplo, puedes escribir "un hermoso paisaje de un bosque al atardecer" o "un retrato surrealista de una mujer con la piel azul y tres ojos". Midjourney generará entonces varias imágenes que coincidan con tu descripción.

GitHub Copilot: es una herramienta basada en IA que te ayuda a escribir código. Se basa en el modelo de lenguaje Codex de OpenAI, que ha sido entrenado en un conjunto masivo de datos de código. Para utilizar GitHub Copilot, sólo se necesita empezar a escribir en el editor de texto. A medida que se vaya desarrollando el código, GitHub Copilot sugerirá complementos para el código, las sugerencias pueden ser aceptadas o ser modificadas según la necesidad del momento.

5. Ciberseguridad

5.1 Definición, tipos, actores

Definición de la ciber seguridad: La ciberseguridad son las medidas y estrategias implementadas para proteger los sistemas de información y los activos digitales contra ataques y amenazas cibernéticas. Esto implica la implementación de políticas, prácticas, tecnologías y controles de seguridad adecuados para mitigar los riesgos y garantizar la confidencialidad, integridad y disponibilidad de los datos y los sistemas.

Tipos de amenazas: Existen diversos tipos de amenazas cibernéticas que pueden comprometer la seguridad de los sistemas. Algunas de las más comunes incluyen:

1. **Malware**: Software malicioso diseñado para dañar o infiltrarse en sistemas y redes.
2. **Ataques de denegación de servicio (DDoS)**: Intentos de sobrecargar un sistema o red con tráfico malicioso para hacerlo inaccesible.
3. **Phishing**: Intentos de engañar a los usuarios para que revelen información confidencial, como contraseñas o datos bancarios.
4. **Ingeniería social**: Manipulación psicológica para obtener información o acceso no autorizado.

5. **Ransomware**: Bloqueo de acceso a sistemas o datos hasta que se pague un rescate.
6. **Ataques de fuerza bruta**: Intentos repetidos y automáticos de adivinar contraseñas o claves de acceso.

Actores en ciberseguridad: En el ámbito de la ciberseguridad, hay diferentes actores involucrados:

1. **Atacantes**: Son individuos o grupos que llevan a cabo los ataques cibernéticos. Pueden ser hackers éticos, que buscan identificar y corregir vulnerabilidades, o ciberdelincuentes que buscan obtener beneficios ilícitos.
2. **Defensores**: Incluyen profesionales y equipos de seguridad que se dedican a proteger los sistemas y datos de las amenazas cibernéticas. Estos pueden ser expertos en seguridad informática, analistas de seguridad, administradores de sistemas y personal de seguridad de la información.
3. **Organismos gubernamentales**: Los gobiernos tienen un papel importante en la ciberseguridad, ya sea en la formulación de políticas, en la promoción de mejores prácticas o en la respuesta a amenazas cibernéticas.
4. **Empresas y organizaciones**: Las empresas y organizaciones son responsables de proteger sus propios sistemas y datos, y suelen contar con equipos de seguridad informática internos o recurren a proveedores de servicios de seguridad cibernética.
5. **Usuarios**: Los usuarios también desempeñan un papel importante en la ciberseguridad. Su comportamiento seguro, el uso de contraseñas robustas, la actualización de software y la conciencia de las amenazas pueden ayudar a prevenir ataques.

5.2 Estado del arte Costa Rica (qué hacen las empresas privadas y el gobierno, ofertas de capacitación)

Empresas privadas:

Muchas empresas privadas ofrecen formación en ciberseguridad a sus empleados. Esta formación puede cubrir una variedad de temas, como la concienciación básica sobre ciberseguridad, cómo detectar correos electrónicos de phishing y cómo proteger sus contraseñas, algunas de estas medidas son:

1. **Libros:**
   Estos libros pueden proporcionar información más detallada sobre las amenazas a la ciberseguridad, cómo protegerse de los ciberataques y cómo responder a los incidentes de ciberseguridad.
2. **Cursos en línea:**
   También hay una serie de cursos en línea que pueden enseñarte sobre ciberseguridad. Estos cursos pueden proporcionarle información más detallada sobre las amenazas a la ciberseguridad, cómo protegerse de los ciberataques y cómo responder a los incidentes de ciberseguridad.
3. **Cursos presenciales:**
   Muchas empresas privadas dan cursos de formación a sus empleados o forman a expertos en ciberseguridad para ser contratados por otras empresas.

Gobierno:

El gobierno de Costa Rica ofrece capacitación en ciberseguridad a los empleados del gobierno. Esta formación puede cubrir una variedad de temas, tales como la forma de proteger los sistemas gubernamentales de los ataques, la forma de responder a los incidentes de ciberseguridad, y la forma de investigar las amenazas de ciberseguridad.

5.3 Describa 2 casos de ciberataques a nivel nacional

Caso 1:

En abril de 2022, se lanzó un ataque de ransomware contra el gobierno de Costa Rica el cual fue realizado por un grupo conocido como Conti, el cual es un servicio de ransomware ruso. El ataque fue realizado explotando una vulnerabilidad en los sistemas operativos de Windows, obteniendo acceso a la red del gobierno. El ataque afectó a varios organismos gubernamentales, entre ellos el Ministerio de Hacienda, el Ministerio de Salud y el Ministerio de Seguridad Pública. Los hackers exigieron el pago de un rescate de 10 millones de dólares en Bitcoin. El gobierno se negó a pagar el rescate, y el ataque continuó durante varias semanas. El ataque causó importantes trastornos en las operaciones del gobierno, y se estima que el coste del ataque será de millones de dólares.

No hay información de como solucionaron el ataque. La forma de evitar posteriores ataques es mejorando los sistemas operativos que utilizan y formando a los especialistas en ciberseguridad que trabajan en el gobierno ya que se conoce que estos no están capacitados al máximo nivel.

Caso 2:

En julio de 2022, se lanzó un ciberataque contra la Caja Costarricense de Seguro Social (CCSS) realizado por un grupo ruso conocido como Hive. El ataque fue realizado explotando las vulnerabilidades en los sistemas operativos antiguos que utiliza la Caja. El ataque afectó a los sistemas informáticos de la CCSS, que se utilizan para procesar los pagos a los beneficiarios y gestionar las finanzas de la caja. El ataque causó importantes trastornos a las operaciones de la CCSS, y se estima que el coste del ataque será de millones de dólares.

No existe información de como se soluciono el ataque ya que la CCSS se reuso a pagar la cuota establecida para el rescate de los archivos. La forma de evitar posteriores ataques similares es actualizando a las ultimas versiones de los sistemas operativos ya que muchos hospitales y centros de salud utilizan versiones demasiado antiguas de Windows las cuales no tienen ni soporte ya del propio Microsoft.

5.4 Describa 2 casos de ciberataques a nivel internacional

Caso 1:

En 2017, el ataque de ransomware WannaCry afectó a más de 200.000 ordenadores en más de 150 países. El ataque fue lanzado por un grupo de hackers conocido como Shadow Brokers. Los hackers utilizaron una vulnerabilidad en el sistema operativo Windows para propagar el ransomware. El ransomware encriptó los archivos de los ordenadores infectados y exigió el pago de un rescate de 300 dólares en Bitcoin. El ataque causó importantes trastornos a empresas y organizaciones de todo el mundo. La manera de evitar este tipo de ataques es siempre actualizando a la última versión del sistema operativo y evitar descargar archivos de fuentes desconocidas.

Caso 2:

En 2018, el hackeo de SolarWinds afectó a más de 18.000 clientes de la empresa de software SolarWinds. Los hackers utilizaron una puerta trasera en el software Orion de SolarWinds para acceder a las redes de sus clientes. Los piratas informáticos pudieron robar datos sensibles de sus clientes, incluida propiedad intelectual y secretos gubernamentales. El ataque se atribuyó al gobierno ruso. La forma de evitar los ataques así es reforzando las vulnerabilidades existentes, ya que previamente por hackers éticos se conocían esas vulnerabilidades, pero no se hizo nada al respecto.

Referencias

Silberschatz, A., Galvin, P. B., & Gagne, G. (2018). Operating System Concepts (10th ed.). Wiley.

Tanenbaum, A. S., & Bos, H. (2014). Modern Operating Systems (4th ed.). Pearson Education.

Stallings, W. (2018). Operating Systems: Internals and Design Principles (9th ed.). Pearson Education.

Kusnetzky, D. (2013). Virtualization: A Manager's Guide (2nd ed.). O'Reilly Media.

Silberschatz, A., Galvin, P. B., & Gagne, G. (2018). Operating System Concepts (10th ed.). Wiley.

Tanenbaum, A. S., & Woodhull, A. S. (2014). Operating Systems: Design and Implementation (3rd ed.). Pearson Education.

Hennessey, J. L., & Patterson, D. A. (2017). Computer Architecture: A Quantitative Approach (6th ed.). Morgan Kaufmann.

Stallings, W. (2017). Computer Organization and Architecture: Designing for Performance (10th ed.). Pearson Education.

Tanenbaum, A. S., & Bos, H. (2014). Structured Computer Organization (6th ed.). Pearson Education.

Moor, J. H. (1985). What is computer ethics? Metaphilosophy, 16(4), 266-275.

Reed, C., Angelopoulos, C., & De Cristofaro, E. (Eds.). (2020). Handbook of Research on the Legal, Ethical, and Societal Implications of Computing and Artificial Intelligence. IGI Global.

Cyberlaw University of Miami. (2021). Technology Law and Policy. Recuperado de: https://cyberlaw.miami.edu/

Russell, S., & Norvig, P. (2016). Artificial Intelligence: A Modern Approach. Pearson.

Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep Learning.

Davenport, T. H., & Ronanki, R. (2018). Artificial Intelligence for the Real World. Harvard Business Review.

Brynjolfsson, E., & McAfee, A. (2017). The Business of Artificial Intelligence. Harvard Business Review.

Chui, M., et al. (2018). Artificial Intelligence: The Next Digital Frontier? McKinsey Global Institute.

Baker, R., et al. (2008). The State of Educational Data Mining in 2009: A Review and Future Visions. Journal of Educational Data Mining, 1(1), 3-17.

Johnson, L., et al. (2016). NMC/CoSN Horizon Report: 2016 K-12 Edition. The New Media Consortium.

Baker, R. S. (2010). Data Mining for Education. International Encyclopedia of Education, 2, 112-118.

Chounta, I. A., & Gajos, K. Z. (2019). Artificial Intelligence for Personalized Education. AI & Society, 34(1), 1-11.

Wikipedia, the Free Encyclopedia. (2023, March 8). Recuperado de https://en.wikipedia.org/wiki/WannaCry_ransomware_attack

Wikipedia, the Free Encyclopedia. (2023, March 8). Recuperado de https://en.wikipedia.org/wiki/SolarWinds_hack