**Janne Oman Herrera Pineda 18310146**

**Inteligencia Artificial**

La Inteligencia Artificial (IA) es la combinación de algoritmos planteados con el propósito de crear máquinas que presenten las mismas capacidades que el ser humano.

TIPOS DE INTELIGENCIA ARTIFICIAL

Sistemas que piensan como humanos  
  
Automatizan actividades como la toma de decisiones, la resolución de problemas y el aprendizaje. Un ejemplo son las redes neuronales artificiales.

 Sistemas que actúan como humanos  
  
Se trata de computadoras que realizan tareas de forma similar a como lo hacen las personas. Es el caso de los robots.

Sistemas que piensan racionalmente  
  
Intentan emular el pensamiento lógico racional de los humanos, es decir, se investiga cómo lograr que las máquinas puedan percibir, razonar y actuar en consecuencia. Los sistemas expertos se engloban en este grupo.

Sistemas que actúan racionalmente  
  
idealmente, son aquellos que tratan de imitar de manera racional el comportamiento humano, como los agentes inteligentes.

Ejemplos de Inteligencia Artificial:

Asistentes de voz.

Smartphones.

Análisis de hábitos.

**Redes 5G**

Esta nueva tecnología móvil aumentará la velocidad de conexión, reducirá al mínimo la latencia (el tiempo de respuesta de la web) y multiplicará exponencialmente el número de dispositivos conectados. En otras palabras: estaremos conectados a todo, todo el día, y en el menor tiempo posible.

La denominación de 5G se refiere a la quinta generación de redes móviles que conocemos. El 5G permitirá navegar hasta a 10 GBps (gigabytes por segundo), 10 veces más rápido que las principales ofertas de fibra óptica del mercado.

Ejemplos de tecnología 5G:

Cirugía remota.

Desactivación de explosivos.

Computación en la nube

**Ciberseguridad**

La ciberseguridad es la práctica de defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos.

El término se aplica en diferentes contextos, desde los negocios hasta la informática móvil, y puede dividirse en algunas categorías comunes.

La seguridad de red es la práctica de proteger una red informática de los intrusos, ya sean atacantes dirigidos o malware oportunista.

La seguridad de las aplicaciones se enfoca en mantener el software y los dispositivos libres de amenazas. Una aplicación afectada podría brindar acceso a los datos que está destinada a proteger. La seguridad eficaz comienza en la etapa de diseño, mucho antes de la implementación de un programa o dispositivo.

La seguridad de la información protege la integridad y la privacidad de los datos, tanto en el almacenamiento como en el tránsito.

La seguridad operativa incluye los procesos y decisiones para manejar y proteger los recursos de datos. Los permisos que tienen los usuarios para acceder a una red y los procedimientos que determinan cómo y dónde pueden almacenarse o compartirse los datos se incluyen en esta categoría.

La recuperación ante desastres y la continuidad del negocio definen la forma en que una organización responde a un incidente de ciberseguridad o a cualquier otro evento que cause que se detengan sus operaciones o se pierdan datos. Las políticas de recuperación ante desastres dictan la forma en que la organización restaura sus operaciones e información para volver a la misma capacidad operativa que antes del evento. La continuidad del negocio es el plan al que recurre la organización cuando intenta operar sin determinados recursos.

La capacitación del usuario final aborda el factor de ciberseguridad más impredecible: las personas. Si se incumplen las buenas prácticas de seguridad, cualquier persona puede introducir accidentalmente un virus en un sistema que de otro modo sería seguro. Enseñarles a los usuarios a eliminar los archivos adjuntos de correos electrónicos sospechosos, a no conectar unidades USB no identificadas y otras lecciones importantes es fundamental para la seguridad de cualquier organización.

**Blockchain, identidad digital autogestionada**

El blockchain o cadena de bloques es un tipo de red que su distribución facilita el desarrollo de tecnologías como la criptomoneda y lo conocido como internet del valor.

El blockchain, es una tecnología que nos ofrece la posibilidad de crear un libro de contabilidad que se distribuye mediante una red de ordenadores sin tener la necesidad de contar con un servidor o base de datos central.

Por este motivo, el poder de cómputo que presentan los nodos en la red se utiliza para introducir información y para protegerla frente a la realización de modificaciones que no han sido autorizadas. Como consecuencia, el blockchain ofrece la posibilidad de alcanzar niveles de seguridad muy elevados si lo comparamos con otras tecnologías.

¿Cómo funciona la tecnología blockchain?

Para que la tecnología blockchain funcione se necesita crear un software específico para la misma. El software permite que los ordenadores generen una red que funciona con el blockchain de manera distribuida. Como sucede en el caso del software de Bitcoin y otras criptomonedas. De forma general, el software presenta un carácter abierto y protegido mediante licencias de software libre. Esto indica que son público, transparentes y que se pueden utilizar, revisar y realizar contribuciones por cualquier persona.

Al no contar con una base de datos ni servidos localizado, a la red blockchain se le atribuye la característica de ser una red distribuida. Lo que esto significa es que la información se encuentra replicada en todos los ordenadores del mundo que se encuentren conectados a la misma blockchain. Más del 50% de los ordenadores que forman la red blockchain no sean de la misma persona o empresa, se puede decir que la red se encuentra descentralizada. Con todo esto podemos afirmar que no tiene un centro de emisión, control o poder.

La red blockchain solo es una base de datos en la que se puede leer y escribir nuevos registros. Todo esto sin poder realizar modificaciones en lo que ya existe. Los registros se encuentran guardados en ella de tal forma que se encuentran vinculados mediante una función matemática muy avanzada. Esto hace imposible que se pueda incluir algo que no sea coherente con el resto de registros que se encuentran incluidos.

Ejemplos de Blockchain:

Identidades digitales

Almacenamiento en la nube

Sistema de votación

**Realidad virtual y realidad aumentada**

La realidad virtual se podría definir como un sistema informático que genera en tiempo real representaciones de la realidad, que de hecho no son más que ilusiones ya que se trata de una realidad perceptiva sin ningún soporte físico y que únicamente se da en el interior de los ordenadores.  
  
La simulación que hace la realidad virtual se puede referir a escenas virtuales, creando un mundo virtual que sólo existe en el ordenador de lugares u objetos que existen en la realidad. También permite capturar la voluntad implícita del usuario en sus movimientos naturales proyectándolos en el mundo virtual que estamos generando, proyectando en el mundo virtual movimientos reales.

Las aplicaciones que en la actualidad encontramos de la realidad virtual a actividades de la vida cotidiana son muchas y diversas. Hay que destacar: la reconstrucción de la herencia cultural, la medicina, la simulación de multitudes y la sensación de presencia.

Ejemplos de Realidad virtual y aumentada:

Seguridad e investigación policial

Videojuegos

realidad aumentada para brindar soporte de autoservicio