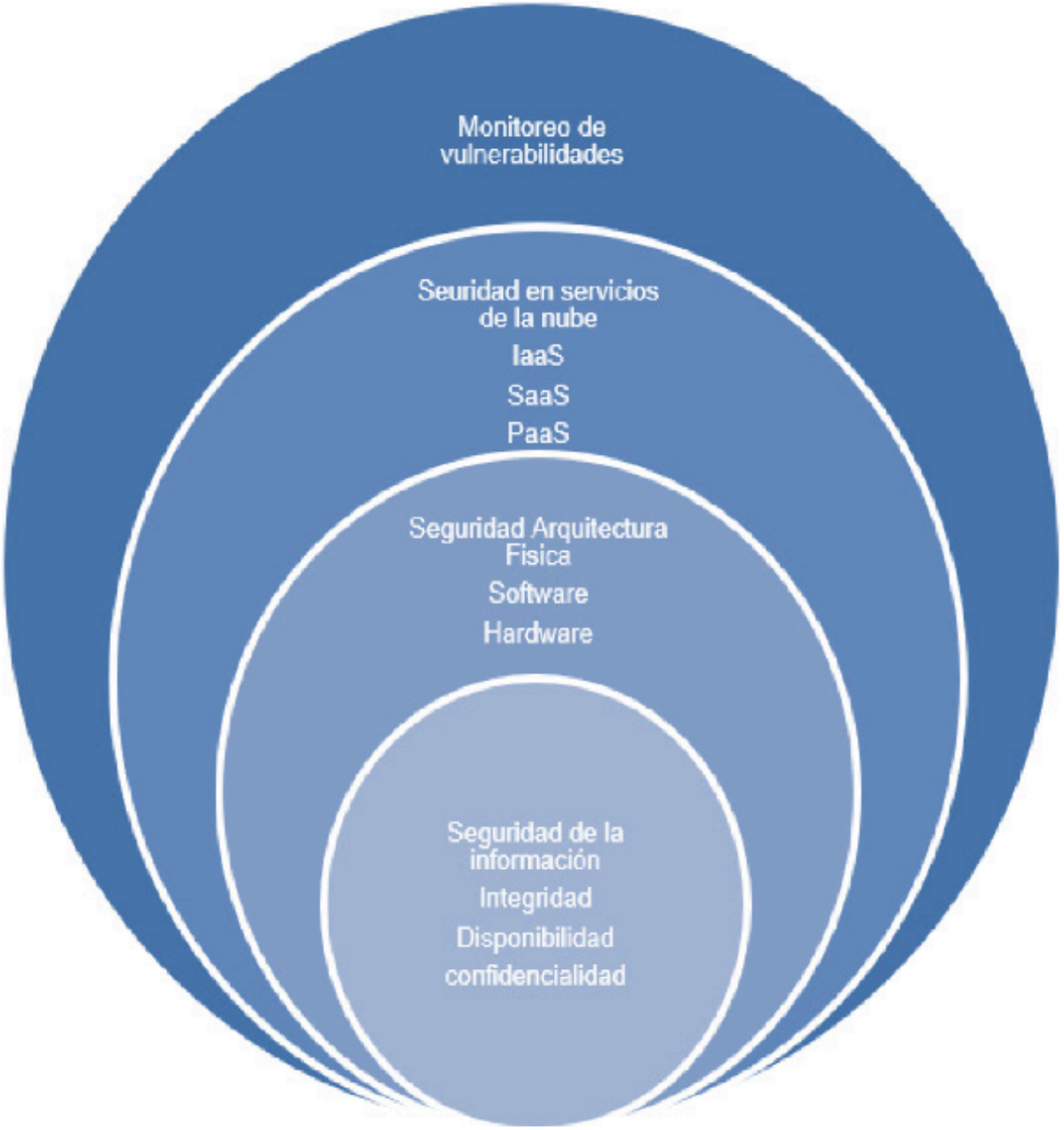
# Esquema para la Esquema para la seguridad de los servicios en la nube

El Cloud Computing o computación en la nube es una de las más recientes y actualizadas tecnologías de la información y la comunicación que tiene como principal característica el que no es necesario acceder a esta desde un equipo específico.




Ciclo de vida de los datos:El Ciclo de vida de los datos, lo cual es necesario gestionar la información de manera adecuada, a

través de principios que permitan mejorar el uso eficiente,tiene fases que requieren seguridad en sus distintos niveles


## Seguridad en la Computación en la Nube

En los últimos años el interés en la Computación en la Nube se ha incrementado rápidamente debido a las ventajas que ofrece este paradigma, mayor flexibilidad y disponibilidad de recursos a un menor costo. Sin embargo, la seguridad y la privacidad constituyen una de las principales preocupaciones para las empresas.

## Las nueve amenazas a la seguridad:

1. Violación de datos privados.
2. Pérdida de datos.
3. Secuestro de cuentas o servicios (*hijacking*).
4. Interfaces y APIs inseguras.
5. Negación de servicio.
6. Persona interna mal intencionada (*insider*).
7. Abuso de servicios en la nube. El uso de recursos.
8. Due diligence insuficiente.
9. Vulnerabilidades en tecnologías compartidas.

## Evaluación de los riesgos de seguridad:antes de contratar un proveedor en la nube es necesario evaluar:

- Privilegios en el acceso de usuarios.
- Cumplimiento de la normativa.

- Ubicación de los datos.
- Separación de los datos.
- Recuperación.
- Soporte a la investigación.
- Viabilidad a largo plazo

## Pautas de seguridad y privacidad en nubes públicas

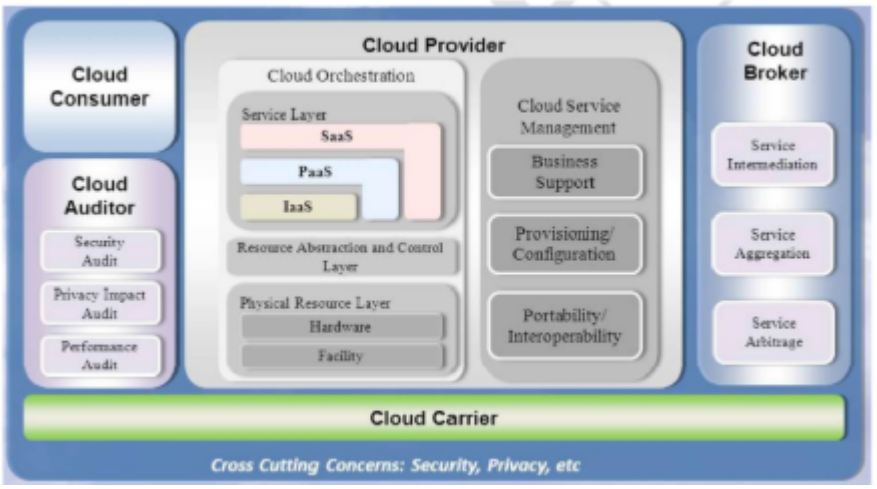
Las cuestiones de seguridad y privacidad que pueden tener impacto a largo plazo en una infraestructura en la nube pública, y en muchos casos, para otros modelos de despliegue son:

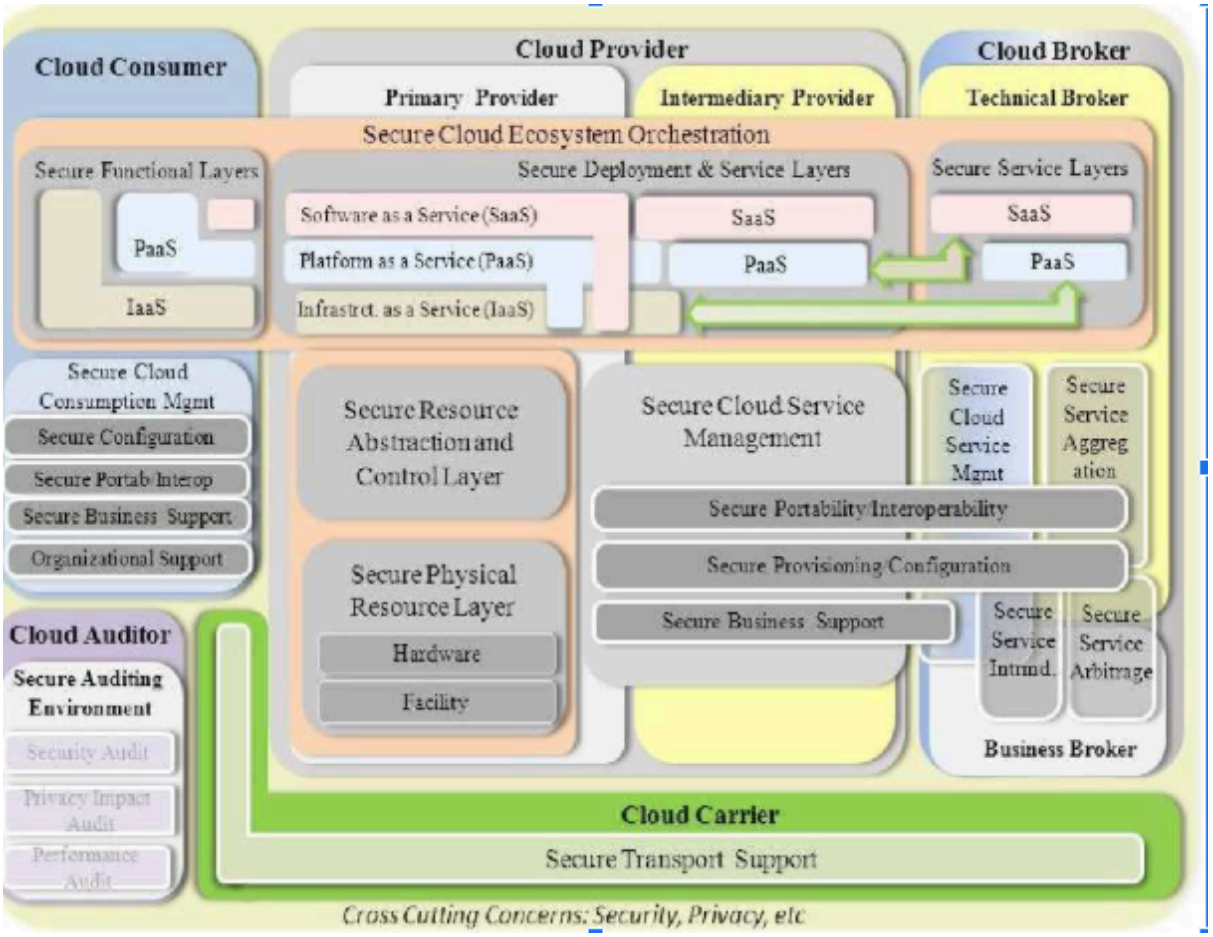
1. Gobernabilidad.
2. Cumplimiento.
3. Confianza.
4. Arquitectura.
5. Gestión de la identidad y el acceso.
6. Aislamiento del software.
7. Proteccion de datos.
8. Disponibilidad.
9. Respuesta incidentes.

## Arquitectura de Referencia de Seguridad del NIST

- Identifica un conjunto de componentes de seguridad los cuales se pueden implementar en un ecosistema en la nube para asegurar el entorno, la operación y la migración de datos hacia la nube.
- Proporciona un conjunto de componentes de seguridad y responsabilidades para cada actor en la nube, según el modelo de despliegue y servicios.
- Define un modelo de arquitectura formal centrado en la seguridad para la NCCAR.
- Proporciona diferentes enfoques para el análisis de datos.
- Teniendo en cuenta:
  - ❖ Los modelos de servicio. (nube pública, privada, híbrida)
  - ❖ Los modelos de despliegue. (IaaS, PaaS, SaaS)
  - ❖ Los actores definidos.

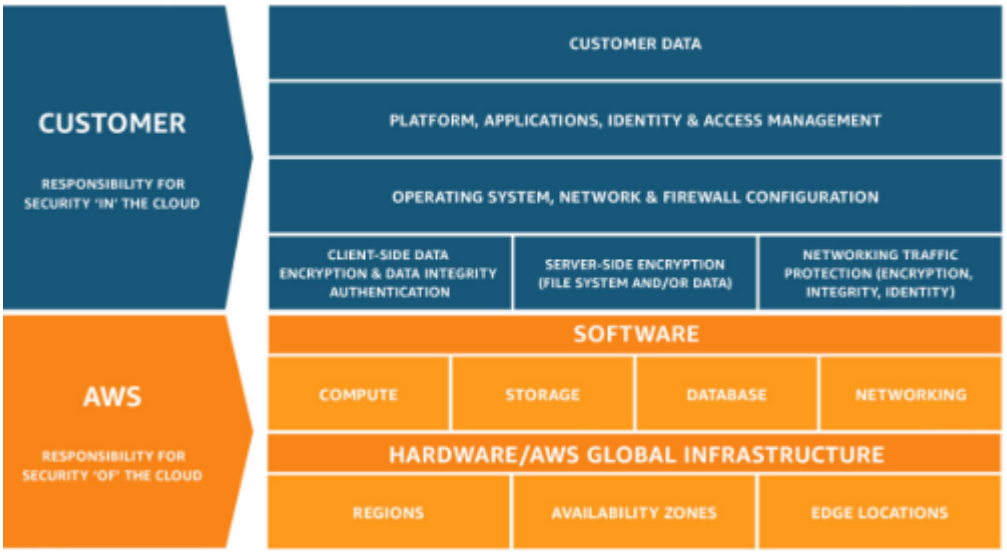
## Modelo Formal de la NCC-SRA




En primer plano los componentes de la arquitectura de seguridad para cada uno de los actores ilustrados en segundo plano.

## Modelo de Seguridad Compartida de AWS




Responsabilidad de AWS:en relación con la "seguridad de la nube": AWS es responsable de proteger la infraestructura que ejecuta todos los servicios provistos en la nube de AWS. Esta infraestructura está conformada por el hardware, el software, las redes y las instalaciones que ejecutan los servicios de la nube de AWS.

Responsabilidad del cliente: en relación con la "seguridad en la nube":
estará determinada por los servicios de la nube de AWS que el cliente seleccione. Esto determina el alcance del trabajo de configuración a cargo del cliente como parte de sus responsabilidades de seguridad. Ejemplo, un servicio como Amazon Elastic Compute Cloud (Amazon EC2) se clasifica como Infraestructura como servicio (IaaS) y, requiere que el cliente realice las tareas de administración y configuración de seguridad necesarias.
Los clientes son responsables de la administración del sistema operativo huésped (incluidos los parches de seguridad y las actualizaciones), de cualquier utilidad o software de aplicaciones que el cliente haya instalado en las instancias y de la configuración del firewall provisto por AWS (llamado grupo de seguridad) en cada instancia.

## Los riesgos de la información en la nube

# Una nube para cada necesidad

Los recursos son propios de la empresa que los implanta.

Infraestructura mixta

La infraestructura y los recursos se encuentran disponibles para el público en general a través de Internet.

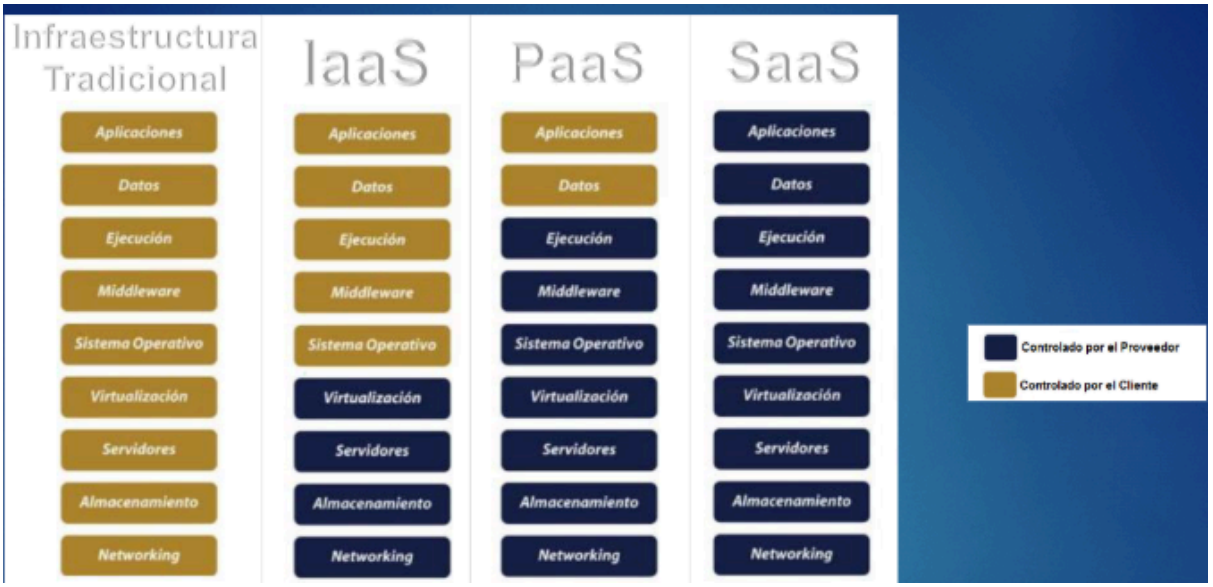



* Gestionadas por la propia organización
* Mayor seguridad y privacidad de datos

* Elevado costo
* Dependencia interna

* Se accede desde cualquier lugar
* Fácilmente escalable
* Bajo costo

* Recursos compartidos
* Seguridad terciarizada
* Requieren contratos de servicio




Pérdida de Gobernanza:El cliente necesariamente cede al proveedor el control de una serie de cuestiones que pueden influir en la seguridad de sus datos e infraestructura. Al mismo tiempo pueden existir deficiencias en los acuerdos de nivel de servicio (SLA).

- Responsabilidades poco claras en los contratos
- Prestaciones no contempladas en los SLA
- Subcontrataciones del Proveedor
- Fallos en la cadena de suministro

Vinculación:Si no se garantiza la portabilidad del servicio la migración de datos o de tecnologías de un proveedor a otro puede traer serios problemas.

- Necesidad de migración programada de un proveedor a otro.
- Quiebra del proveedor.
- Crisis de confianza con el proveedor.
- Portabilidad o Interfaces deficientes.

Cumplimiento:Se deben alcanzar los requisitos legales y normativos, se debe garantizar la posibilidad de efectuar una auditoría de los servicios brindados por el proveedor.

- Poca transparencia en los contratos y subcontratos relacionados.

- Auditoría no disponible para clientes.
- Falta de cumplimiento del proveedor que afecte certificaciones del cliente.

Agotamiento de recursos:Los servicios en la nube son otorgados bajo demanda, el aprovisionamiento de recursos debe ser el adecuado.

- Sobredimensionamiento de la infraestructura > Pérdidas económicas
- Subdimensionamiento de la infraestructura > Servicio no disponible
- Daños de imagen / Imposibilidad de operar

Fallos de aislamiento:Asociados principalmente a redes públicas donde los recursos son compartidos por múltiples usuarios de diferentes organizaciones.

- Errores en mecanismos de aislamiento lógico
- Falta de protección de datos (encriptación)
- Errores en mecanismos de autenticación

El impacto de aislamientos deficientes puede derivar en la pérdida o modificación de todos los datos.

Supresión insegura de datos:Cuando se solicita suprimir un objeto de la nube pueden efectuarse eliminaciones no es definitivas, permitiendo la recuperación del dato a futuro.

- Imposibilidad técnica del proveedor para efectuar eliminación definitiva
- Migración de Proveedor y reubicación de hardware.

Utilizar encriptación reduce el riesgo considerablemente.

Fuga de Datos:El mismo riesgo que se presenta en las infraestructuras tradicionales pero potenciado porque en la nube existe mayor cantidad de datos en tránsito y mecanismos de carga y descarga de información masiva.

- Ataques MITM
- Falta de cláusulas de confidencialidad o de no divulgación en el contrato
- Empleados malintencionados en los proveedores de nube

Utilizar encriptación reduce el riesgo considerablemente.

Órdenes Judiciales y Jurisdicciones:En caso de confiscación de hardware por una orden judicial se presenta el riesgo de divulgación de datos de clientes ajenos que comparten dicho hardware.
Además, los datos de los clientes se pueden resguardar en múltiples jurisdicciones.

- Fallas en el aislamiento
- Jurisdicciones de alto riesgo
- Falta de información sobre Jurisdicción de los datos

Los centros de datos ubicados en países de alto riesgo podrían ser confiscados por la fuerza de sus autoridades locales.

Protección de datos:El incumplimiento de la legislación en materia de protección de datos puede dar lugar a la imposición de sanciones administrativas, civiles e incluso penales, que varían en función de cada país.

- Infracciones de la ley
- Pérdida de control por parte del cliente
- Máquinas virtuales en un mismo equipo físico
- Publicación indebida de información personal legalmente protegida.

El cliente será el principal responsable del procesamiento de los datos personales, incluso cuando dicho procesamiento lo realice el proveedor.

Congestión o fallos en la red:Internet es el punto de acceso a las infraestructuras en la nube, fallos o congestiones en la red así como problemas en los navegadores afectarán la disponibilidad y el servicio.

- Desastres naturales
- Ataques de DoS
- Fallos en los dispositivos de red

Es un riesgo que afecta a miles de clientes a la vez.

Ataques de ingeniería social:Es el arte de engañar a las personas para que revelen información sensible.

- Robo de credenciales
- Robo de información sensible

- Malware

La mejor defensa es la concientización de nuestros usuarios.

Compromiso de los registros (logs):Los registros operativos y de seguridad estarán distribuidos en máquinas virtuales del proveedor lo cual podrá generar limitaciones al momento de requerir su análisis.

- Falta de acceso a los logs por parte del cliente
- Gestión de incidentes con visibilidad parcial
- Incumplimientos regulatorios en el tiempo de guarda

Los registros de log y la gestión de incidentes centralizada minimiza el riesgo.

## CONCLUSIONES

- Revisión de Contratos por todas las áreas involucradas
- Revisión de Acuerdos de Servicio (SLA)
- Encripción de Datos
- Auditoría periódica del proveedor
- Conocer la Jurisdicción de los datos
- Gestionar los Incidentes y logs en forma centralizada
- Mantener un adecuado dimensionamiento de la infraestructura
- Capacitar a nuestros recursos humanos en éste nuevo paradigma

## Inteligencia artificial (Cloud IA)

La Inteligencia Artificial es una disciplina dentro de las ciencias de la computación.
Consiste en el desarrollo de un tipo de algoritmos en el ámbito del software y del hardware para ejecutarlos de la manera más eficiente posible tanto con respecto al consumo energético como de tiempo de ejecución.
La inteligencia artificial se puede organizar de varias maneras, según las etapas de desarrollo o las acciones que se están realizando.

# Las 4 etapas de desarrollo

Máquinas recreativas:limitada que solo reacciona a diferentes tipos de estímulos basados en reglas preprogramadas.

Memoria limitada:la mayor parte de la IA moderna es de memoria limitada. Puede usar la memoria para mejorar con el tiempo mediante el entrenamiento con datos nuevos, por lo general, a través de una red neuronal artificial o algún otro modelo de entrenamiento.

Teoría de la mente:Actualmente no existe IA con teoría de la mente. El término hace referencia a IA que puede emular la mente humana y tiene capacidades de toma de decisiones similares a las de un ser humano

Autoconocimiento:Una máquina mítica que tiene conocimiento de su propia existencia y tiene las capacidades intelectuales y emocionales de un ser humano.

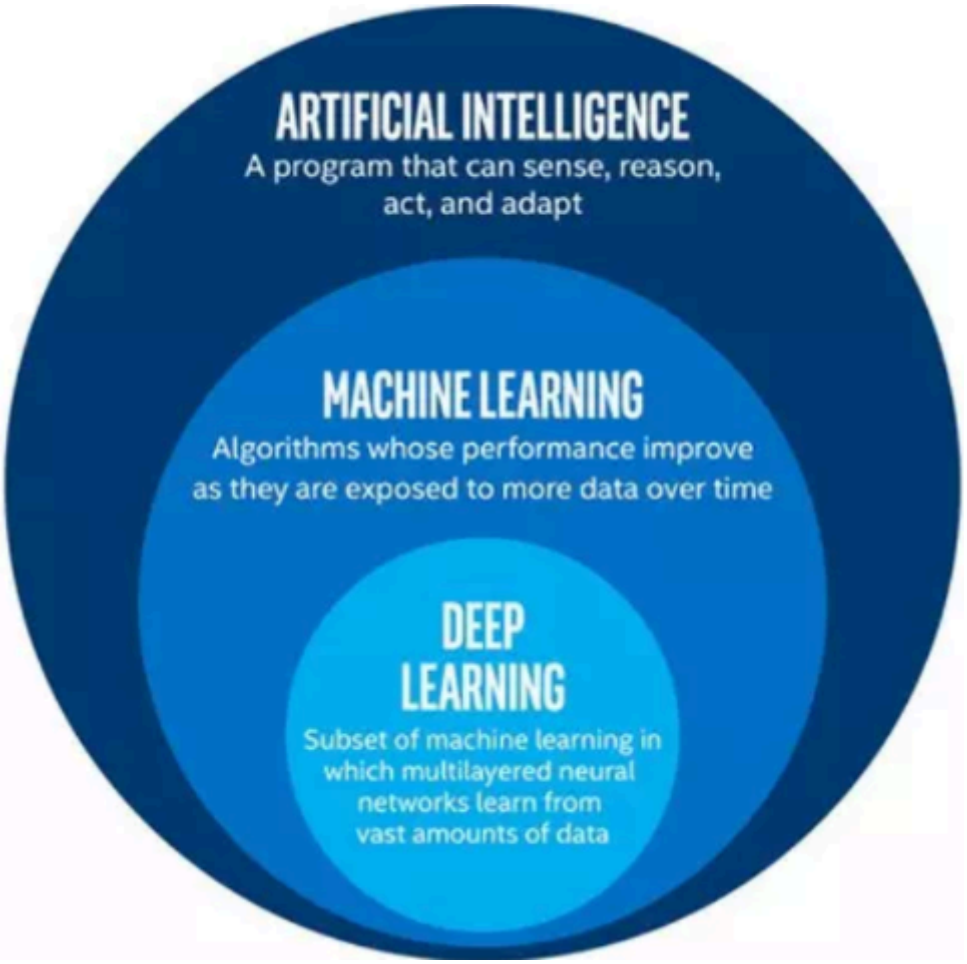

TIPOS:

Diferencia: la Inteligencia Artificial de otros programas de ordenador es que no hay que programarla específicamente para cada escenario. Podemos enseñarle cosas ML (Machine Learning, aprendizaje automático) O también puede aprender por sí mismo DL (Deep Learning).

Definiciones:
IA (Inteligencia Artificial): una máquina que es capaz de imitar el razonamiento humano.

ML (Machine Learning): un subconjunto de Inteligencia Artificial donde las personas «entrenan» a las máquinas para reconocer patrones basados en datos y hacer sus predicciones.

DL (Deep Learning): un subconjunto de ML en el que la máquina es capaz de razonar y sacar sus propias conclusiones, aprendiendo por sí misma.




## Modelos de entrenamiento de IA

Aprendizaje automático: Datos de entrenamiento – memoria limitada
Aprendizaje supervisado:Supervisado en función a los datos que se le proporciona

Aprendizaje no supervisado:aprende patrones en función de datos no etiquetados (datos no estructurados)
Aprendizaje por refuerzo:términos generales como “aprender haciendo”. Un "agente" aprende a realizar una tarea mediante prueba y error

## Tipos de redes neuronales artificiales

Un tipo común de modelo de entrenamiento en la IA es una red neuronal artificial, que se basa a grandes rasgos en el cerebro humano.

1-Las redes neuronales pre alimentadas (FF)
2-Las redes neuronales recurrentes (RNN)
3-Las RNN de memoria a largo/corto plazo (LSTM)
4-Las redes neuronales convolucionales (CNN)
5-Las redes generativas adversarias (GAN)

Terminator, Matrix y otros relatos de ciencia-ficción en la cultura popular.
IA todavía está bastante lejos; por ejemplo, Alexa puede ser un buen mayordomo, pero no puede pasar el famoso test de Turing.
Actualmente, tenemos una forma bastante limitada de Inteligencia Artificial.
Estamos lejos de la rebelión de las máquinas

ML (Machine Learning):Toda inteligencia para saber ha de aprender, por lo que necesita datos para sacar conclusiones a partir de los mismos.
Un programa normal lo que hace es ejecutarse.
Un algoritmo de inteligencia artificial está pensado para aprender y esto significa corregir errores.

DL (Deep Learning):Desde 2018, esta es la vanguardia de la Inteligencia Artificial. Pensemos como un aprendizaje automático con profundas «redes neuronales» que procesan los datos de manera similar al cerebro humano.
Deep Learning es el aprendizaje automático, en el que el ordenador es capaz de aprender por sí mismo (aunque va mucho más allá de los gatos, claro, pues actualmente las máquinas ya son capaces de captar muchos más parámetros dentro de las fotos, como el paisaje, por ejemplo).
El Deep Learning requiere muchos más datos iniciales y potencia de cómputo que el Machine Learning, eso sí, pero compañías como

Facebook o Amazon ya están comenzando a implementarlo.

La inteligencia artificial (IA) está creciendo a una velocidad sin precedentes.

La nube juega un papel importante en el desarrollo y uso de esta tecnología.

En particular, dos herramientas en la nube tienen un gran impacto en la IA:

Amazon Web Services (AWS)
Google Cloud Platform (GCP).

AWS proporciona una amplia gama de herramientas de IA, desde el procesamiento de lenguaje natural (NLP) y el aprendizaje profundo hasta la inteligencia empresarial y la robótica.
GCP, por otro lado, cuenta con TensorFlow, una plataforma ampliamente utilizada para el aprendizaje automático y la creación de modelos de IA.
Ambas herramientas de la nube juegan un papel importante en el desarrollo de la IA, y permiten a los desarrolladores e investigadores acceder a la potencia de la nube para crear modelos de IA más sofisticados y personalizados.
La conclusión es que la nube es fundamental en el desarrollo de la IA, y AWS y GCP son dos de las mejores herramientas disponibles en la actualidad.

## Beneficios

- ❑ Automatización
- ❑ Rápido y preciso
- ❑ Reduce errores humanos
- ❑ Disponibilidad Infinita
- ❑ Elimina tareas repetitivas
- ❑ Investigación y desarrollo acelerados

## Productos y servicios relacionados Google Cloud

- ❑ Infraestructura IA:Opciones para que todas las empresas entrenen modelos de aprendizaje .

- Vertex AI:Compila e implementa y escala modelos AA mas rápido con herramientas.

- Document AI:Automatiza la captura de datos en gran escala
- Contact center AI:Entrega un servicio de atención al cliente de alta calidad y eficiencia.

- AutoML:Entrena modelos de aprendizaje automáticos personalizados y de alta calidad.

- Recomendaciones IA:Ofrece recomendaciones de productos altamente especializadas a gran escala.