UNIVERSIDAD TECNOLOGICA NACIONAL

Ingeniería en Sistemas de Información

Ciberseguridad

Docente: Ing. Gabriela Nicolao

Ayudantes: Ing. Luciano Sebastianelli, Matías Baghdassarian

UNIVERSIDAD TECNOLOGICA NACIONAL

Seguridad Cloud

Definición (Estándar NIST 800-145)

UNIVERSIDAD TECNOLOGICA NACIONAL

- Modelo para permitir el acceso de red, de forma práctica y bajo demanda, a un conjunto de recursos de computación configurables que pueden ser suministrados y desplegados rápidamente con una mínima gestión o interacción con el proveedor de servicio.
- El modelo Cloud se compone de:
  - **5 características esenciales**: Amplio acceso a la red, Elasticidad rápida, Servicio medido, Autoservicio a demanda y Agrupación de recursos.
  - **3 modelos de servicios**: SaaS, PaaS, IaaS.
  - **4 modelos de despliegue**: Público, Privado, Híbrido y Comunidad.

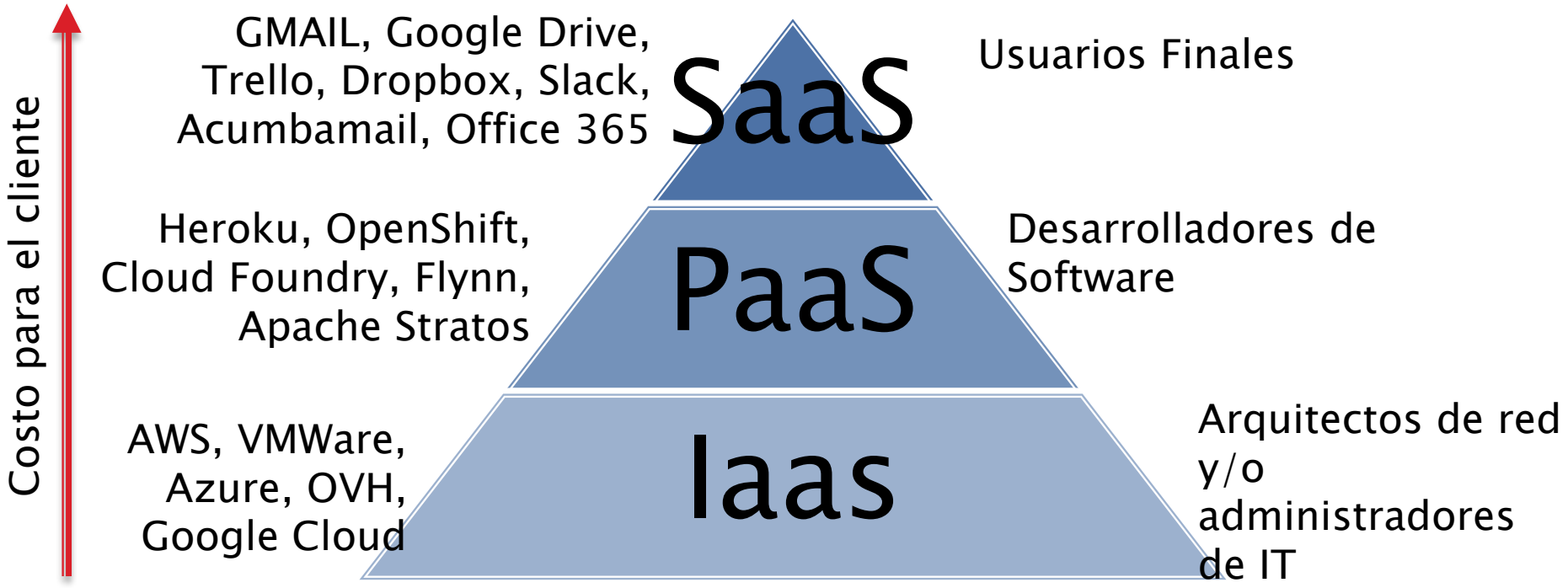
Características Esenciales

UNIVERSIDAD TECNOLOGICA NACIONAL

- Autoservicio bajo demanda
- Amplio acceso a través de las redes
- Agrupación de recursos
- Elasticidad rápida
- Servicio medido

Modelos de servicio

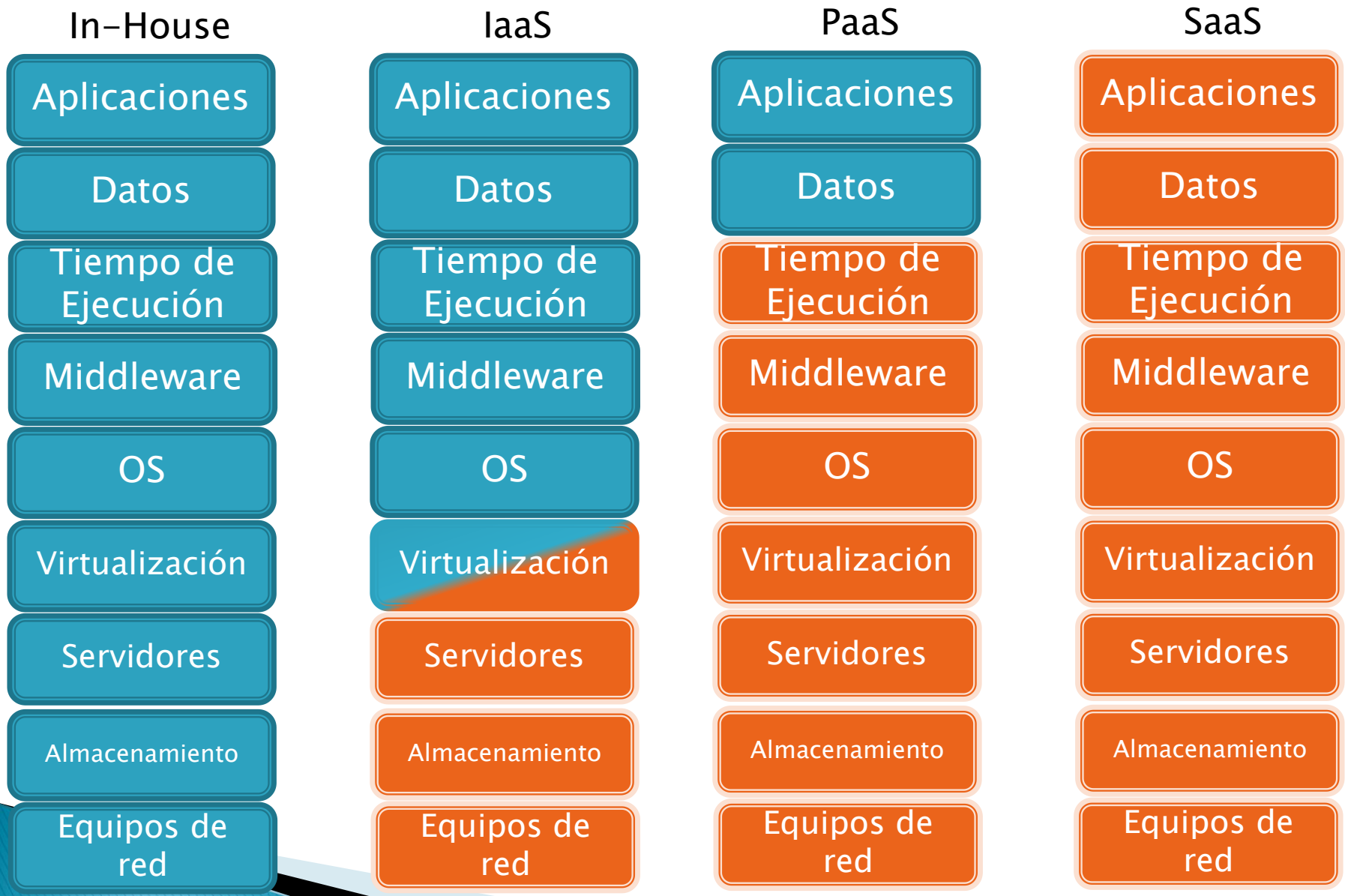
UNIVERSIDAD TECNOLOGICA NACIONAL



Responsabilidad Compartida

Gestionado por tu empresa
Gestionado por un proveedor

UNIVERSIDAD TECNOLOGICA NACIONAL



Modelos de despliegue

UNIVERSIDAD TECNOLOGICA NACIONAL

Nube Comunidad

- Se comparte con otras organizaciones de intereses similares
- Colaborativa

Nube Híbrida

- Combinación de 2 o más modelos de nube
- Para organizaciones que tienen que balancear el acceso a los datos con exigencias regulatorias

Nube Pública

- Compartida con el público general
- Grandes cantidades de espacio, escalable
- Recomendado para desarrollo de software y proyectos colaborativos

Nube Privada

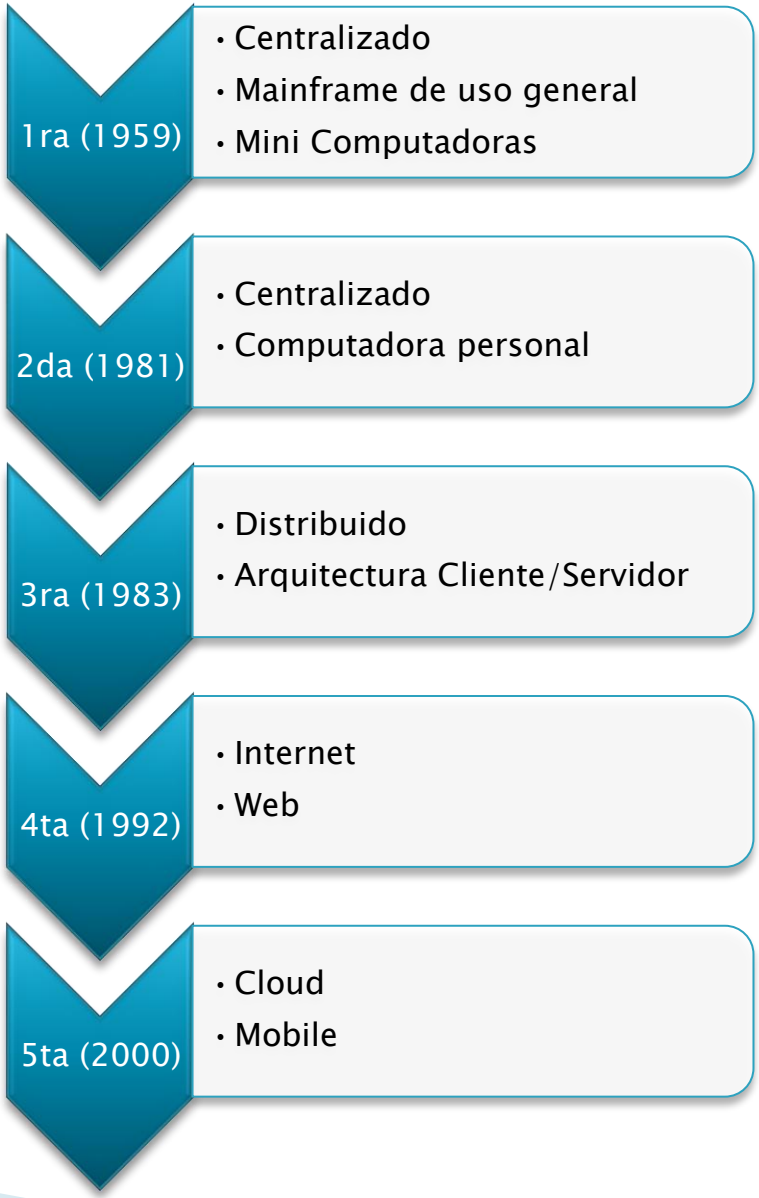
- Propia de la organización
- Reside detrás de un Firewall
- Para organizaciones con muchas exigencias regulatorias

Conceptos

UNIVERSIDAD TECNOLOGICA NACIONAL

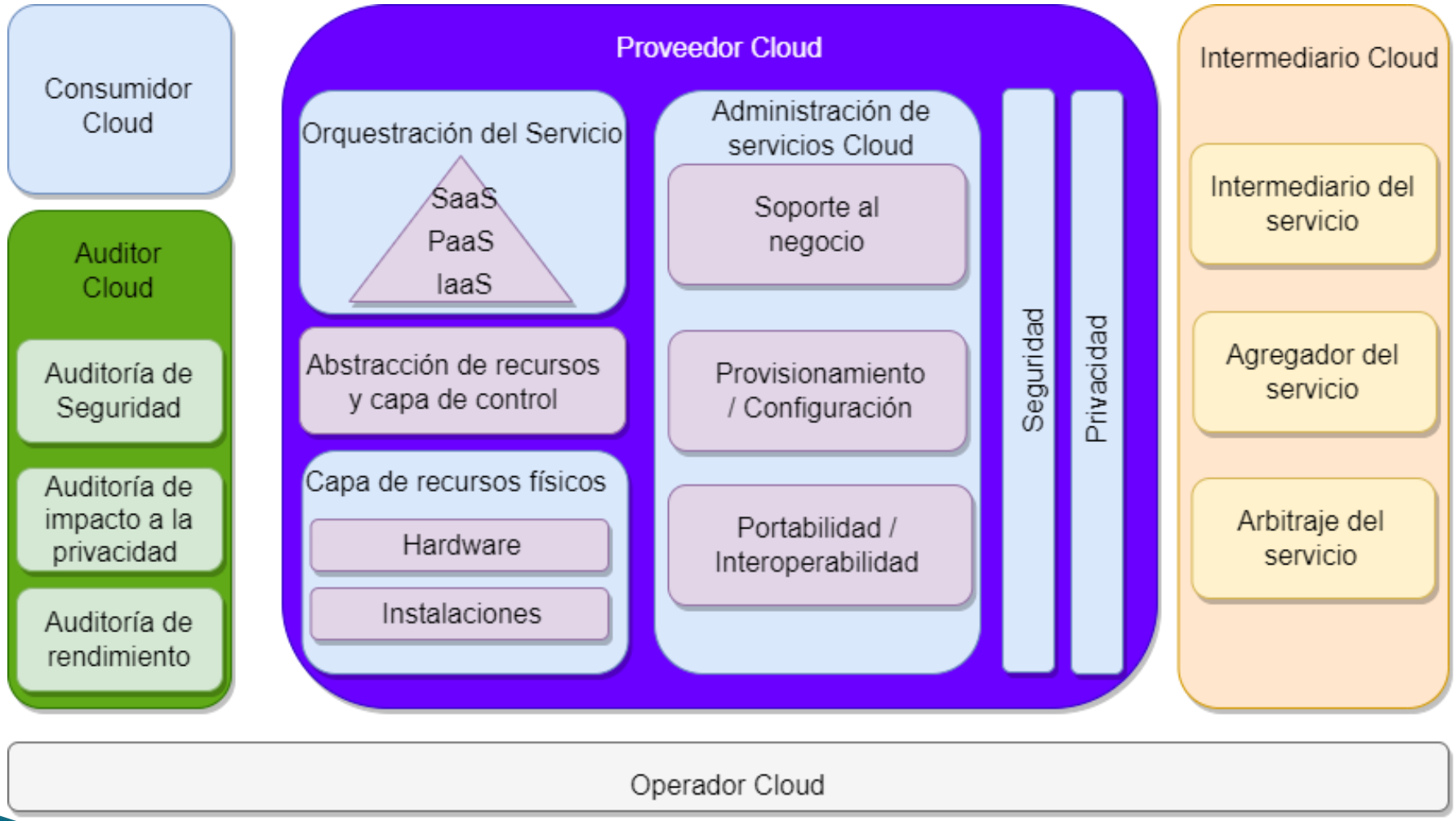
Evoluciones de Infraestructura IT

UNIVERSIDAD TECNOLOGICA NACIONAL



Actores Cloud según NIST

UNIVERSIDAD TECNOLOGICA NACIONAL



La nube democratiza el acceso a las TICs

Ventajas

- Pago por uso
- Acceso desde cualquier lado
- Recursos compartidos
- Escalabilidad
- Eficiencia de costos
- Barrera de entrada baja
- Facilidad de mantenimiento
- Fiabilidad
- Calidad del servicio
- Facilidad de uso

Desventajas

- Rendimiento compartido
- Control
- Seguridad y Privacidad
- Costo
- Dependencia de conectividad
- Fallas del proveedor

Top 11 de Amenazas a Cloud Computing según CSA

UNIVERSIDAD TECNOLOGICA NACIONAL

- Gestión insuficiente de identidad, credenciales y acceso.
- Interfaces inseguras e interfaces de programación de aplicaciones (API).
- Mala configuración y controles de cambio inadecuados.
- Falta de estrategia y arquitectura de seguridad Cloud.
- Desarrollo inseguro.
- Recursos de 3ros inseguros.
- Vulnerabilidades del sistema.
- Violaciones de datos accidental (accidental disclosure)
- Mala configuración y explotación de cargas de trabajo serverless y de containers.
- Crimen organizado/Hackers/ Amenazas persistentes avanzadas (APTs)
- Exfiltración de datos.

Seguridad Cloud

UNIVERSIDAD TECNOLOGICA NACIONAL

- Categorías
  - Seguridad los datos.
  - Gestión de identidades y accesos (IAM).
  - Gobernanza (políticas de prevención, detección y mitigación de amenazas).
  - Planificación de la retención de datos (DR) y la continuidad del negocio (BC).
  - Cumplimiento legal.
- Objetivos
  - Permitir la recuperación de datos en caso de pérdida de datos.
  - Proteger el almacenamiento y las redes contra el robo de datos malicioso.
  - Evitar los errores humanos o negligencias que causan la fuga de datos.
  - Reducir el impacto de cualquier compromiso de datos o sistemas.

Seguridad Cloud

UNIVERSIDAD TECNOLOGICA NACIONAL

- Riesgos
  - Acceso no autorizado.
  - Perdida o robo de datos.
  - Plataformas informáticas heredadas incompatibles.
  - Interrupciones de los servicios de almacenamiento de datos de terceros.
  - Amenazas internas.
  - Amenazas externas.
  - Incumplimientos contractuales.
  - APIs inseguras.
  - Desconfiguración de servicios/Pérdida de visibilidad.
- Preocupaciones
  - Privacidad.

Seguridad Cloud

UNIVERSIDAD TECNOLOGICA NACIONAL

- Recomendaciones
  - Cifrado de las comunicaciones con la nube en su totalidad.
  - Cifrado de datos especialmente confidenciales, como las credenciales de las cuentas.
  - Cifrado de extremo a extremo de todos los datos que se suben a la nube.
  - Modificar configuración predeterminada.
  - No exponer almacenamiento en la nube.
  - Activar controles de seguridad proporcionados por el proveedor de servicios.
  - Usar contraseñas “seguras” y activar MFA.
  - Revisar políticas de retención de datos de usuarios y clientes.

Más Información

UNIVERSIDAD TECNOLOGICA NACIONAL

- NIST Special Publication 800-144, Guidelines on Security and Privacy in Public Cloud Computing, December 2011.
- NIST Special Publication 800-145, NIST Definition of Cloud Computing, September 2011.
- NIST Special Publication 800-146, Cloud Computing Synopsis and Recommendations, May 2012.
- NIST Special Publication 500-291, NIST Cloud Computing Standards Roadmap, July 2011.
- NIST Special Publication 500-292, NIST Cloud Computing Reference Architecture, September 2011.

UNIVERSIDAD TECNOLOGICA NACIONAL

PREGUNTAS?