Ciberseguridad

Los riesgos de la información en la nube

Banco Nación

AGENDA

- Introducción
- Tipos de Infraestructuras
- Tipos de Servicios
- Casos prácticos
- Riesgos asociados
- Conclusiones

Introducción

Qué es la nube ?

Los “servicios en la nube” o “cloud computing” son un modelo que permite el acceso a datos y recursos informáticos a través de Internet, permitiendo a los usuarios acceder en forma inmediata a datos y aplicaciones, independientemente del lugar y dispositivo móvil o fijo que utilicen.

- ✓ Los recursos se ofrecen como servicio
- ✓ Son escalables y flexibles
- ✓ Se ajustan a la necesidad del cliente

El origen del término se relaciona con el uso común para representar gráficamente Internet como si fuera una nube.

Cloud, Nube.

Introducción

Cómo surgió la idea?

La convergencia de ciertas cuestiones del mercado impulsó el desarrollo de servicios típicamente internos de las empresas en desarrollos prestados por terceros a través de Internet.

- ✓ La globalización
- ✓ La movilidad
- ✓ La necesidad de estar siempre conectados y compartir información
- ✓ Los avances en tecnología y velocidad de las comunicaciones

Uno de los pioneros en la nube fue Salesforce.com que en 1999 introdujo el concepto de entrega de aplicaciones empresariales mediante una página web. Le siguió Amazon al lanzar Amazon Web Service en 2002, luego llegó Google Docs en 2006 que trajo la nube a la vanguardia.

Introducción

Un caso de uso típico de servicio en la nube es el correo electrónico. Varias empresas ya han dado el salto de mantener su correo corporativo allí, permitiendo mejorar sustancialmente la disponibilidad y movilidad de los usuarios.



El servicio incluye además

- ✓ Amplio espacio de almacenamiento
- ✓ Agendas corporativas
- ✓ Soluciones Antispam y Antivirus
- ✓ Soporte técnico 7 x 24

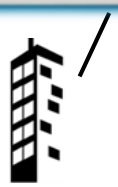
Banco Nación

Tipos de Infraestructuras

Una nube para cada necesidad

Los recursos son propios de la empresa que los implanta.

Privada



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

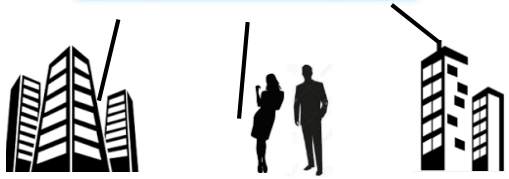
* Elevado costo
* Dependencia interna

Infraestructura mixta

Híbrida

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

Pública

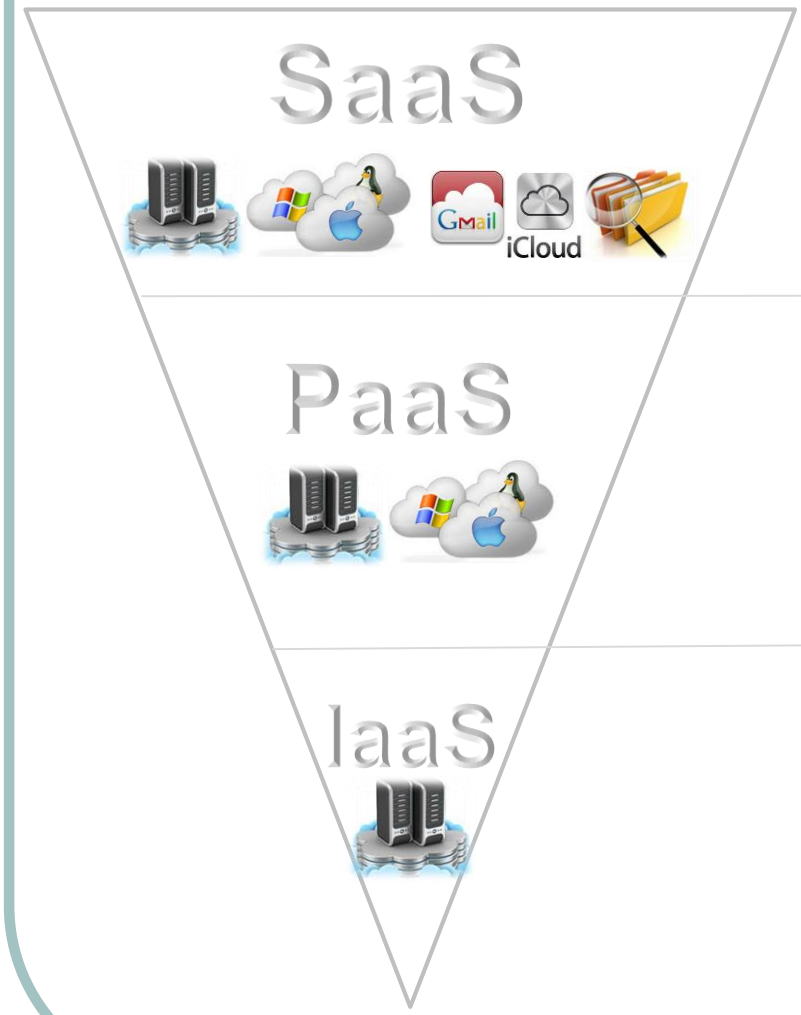


* Se accede desde cualquier lugar
* Fácilmente escalable
* Bajo costo

* Recursos compartidos
* Seguridad terciarizada
* Requieren contratos de servicio

Tipos de Servicios

Los servicios que nos ofrece la nube



Software como servicio: El proveedor ofrece aplicaciones para que sean utilizadas por el usuario desde distintos dispositivos. El suscriptor no administra ni controla la infraestructura en la que se basa el servicio.

Plataforma como servicio: El proveedor brinda una plataforma de procesamiento, donde el suscriptor puede desplegar y ejecutar sus propios servicios o aplicaciones. El suscriptor posee control sobre las aplicaciones.

Infraestructura como servicio: El proveedor brinda una infraestructura, donde el suscriptor puede desplegar y ejecutar software. El suscriptor posee control sobre el Sistema Operativo, aplicaciones y ciertos componentes de la red.

Tipos de Servicios

Quién controla qué?

Infraestructura Tradicional	IaaS	PaaS	SaaS
Aplicaciones	Aplicaciones	Aplicaciones	Aplicaciones
Datos	Datos	Datos	Datos
Ejecución	Ejecución	Ejecución	Ejecución
Middleware	Middleware	Middleware	Middleware
Sistema Operativo	Sistema Operativo	Sistema Operativo	Sistema Operativo
Virtualización	Virtualización	Virtualización	Virtualización
Servidores	Servidores	Servidores	Servidores
Almacenamiento	Almacenamiento	Almacenamiento	Almacenamiento
Networking	Networking	Networking	Networking

Controlado por el Proveedor

Controlado por el Cliente

amazon web services

rackspace the open cloud company

Google app engine

Windows Azure

Gmail

Google Drive

iCloud

Dropbox

Banco Nación

Casos prácticos

Oportunidades e Innovaciones en la nube

Organizaciones como amazon descubrieron que la estructura de servicios en la nube aumentaba la eficiencia con la que trabajaban sus Data Centers, así identificaron un nicho de negocio comercializando éste tipo de estructuras como servicio.

Recientemente Microsoft anunció que llevaba *la nube al océano*, instalando un centro de datos submarino bajo el proyecto “Natik” a fin de abaratar costos relacionados con la energía necesaria para “enfriar” los equipos.

Casos prácticos

Soluciones de CRM:
Automatización de la fuerza de ventas, proporcionan al CRM la capacidad de conseguir más ganancias, aumentar la productividad y mejorar la velocidad.

Soluciones de Storage:
Ofrecen a los desarrolladores y los profesionales de TI un almacenamiento seguro, duradero y altamente escalable.

Soluciones MDM:
Ofrecen servicios de administración centralizada de dispositivos móviles empresariales, mejorando el despliegue y administración de los mismos.

NETFLIX

amazon web services

Algunos proveedores de SaaS corren sus aplicaciones sobre servicios IaaS o PaaS ofrecidos por otros, como por ejemplo, Netflix (SaaS) que corre sobre servicios IaaS y PaaS de Amazon Web Services.

Banco Nación

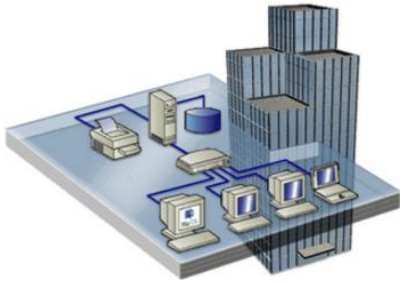
El nuevo paradigma tecnológico

Los servicios en la nube proliferan día a día ofreciendo distintas y atractivas soluciones a las empresas, en principio pareciera la solución ideal que brinda movilidad, flexibilidad y rentabilidad a nuestro negocio

¿qué debemos considerar para no ser alcanzados por la tormenta?

Riesgos en la nube

Riesgos Tradicionales

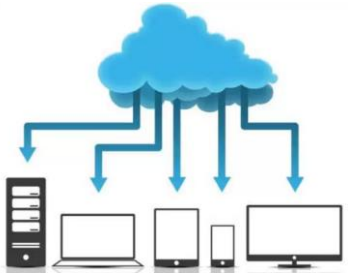


- ✓ Robo de Información
- ✓ Fuga de Información
- ✓ Fraude interno o externo
- ✓ Denegación de Servicio
- ✓ Escalada de Privilegios
- ✓ Malware
- ✓ Desarrollos inseguros
- ✓ Contingencia ineficiente
- ✓ Errores humanos
- ✓ Desastres naturales
- ✓ SLA deficientes
- ✓ Y más….

Riesgos de la Nube

- ✓ Pérdida de Gobernanza
- ✓ Fallos en el acceso a Internet
- ✓ Riesgos del hipervisor
- ✓ Infraestructuras compartidas
- ✓ Suplantación de identidad
- ✓ Aspectos legales de los datos
- ✓ Migración de Proveedor
- ✓ Y más…

Riesgos Particulares



- ✓ Pública o Privada?
- ✓ SaaS / PaaS o IaaS ?

- ✓ CRM ?
- ✓ MENSAJERÍA ?
- ✓ DATA CENTER ?
- ✓ MDM?
- ✓ DESARROLLO DE SW ?

Banco Nación

Riesgos en la nube

- ✓ Riesgos Organizativos
- ✓ Riesgos Técnicos
- ✓ Riesgos Legales
- ✓ Riesgos No específicos

Riesgos Organizativos

Pérdida de Gobernanza

Probabilidad: MUY ALTA
Impacto: MUY ALTO

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

Los clientes son responsables de la seguridad e integridad de sus datos, incluso en la nube.

Riesgos Organizativos

Vinculación

Probabilidad: ALTA
Impacto: MEDIO

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.

Antes de incorporar nuestros datos en la nube aseguremos que podremos sacarlos toda vez que los necesitemos.

Riesgos Organizativos

Cumplimiento

Probabilidad: MUY ALTA
Impacto: ALTO

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. (Ej. PCI)

Los contratos deben ser revisados por todas las áreas intervinientes.

Riesgos Técnicos

Agotamiento de recursos

Probabilidad: BAJA
Impacto: MUY ALTO

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

El aprovisionamiento debe estar bien dimensionado y deben existir cláusulas de ajuste a demanda.

Riesgos Técnicos

Fallos de aislamiento

Probabilidad: ALTA
Impacto: MUY ALTO

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.

Riesgos Técnicos

Supresión insegura de datos

Probabilidad: MEDIA
Impacto: MUY ALTO

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 encripción reduce el riesgo considerablemente.

Riesgos Técnicos

Fuga de Datos

Probabilidad: MEDIA
Impacto: ALTO

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 clausulas de confidencialidad o de no divulgación en el contrato
- ✓ Empleados malintencionados en los proveedores de nube

Utilizar encripción reduce el riesgo considerablemente.

Riesgos Legales

Órdenes Judiciales y Jurisdicciones

Probabilidad: MUY ALTA
Impacto: ALTO

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.

Riesgos Legales

Protección de datos

Probabilidad: ALTA
Impacto: ALTO

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.

Riesgos No Específicos

Congestión o fallos en la red

Probabilidad: MEDIA
Impacto: MUY ALTO

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.

Riesgos No Específicos

Ataques de ingeniería social

Probabilidad: MEDIA
Impacto: ALTO

Es el arte de engañar a las personas para que revele información sensible.

- ✓ Robo de credenciales
- ✓ Robo de información sensible
- ✓ Malware

La mejor defensa es la concientización de nuestros usuarios.

Riesgos No Específicos

Compromiso de los registros (logs)

Probabilidad: BAJA
Impacto: MEDIO

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.

- ✓ 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

Banco Nación

CONCLUSIONES

- ✓ Gestionar los Incidentes y logs en forma centralizada
- ✓ Mantener un adecuado dimensionamiento de la infraestructura
- ✓ Capacitar a nuestros recursos humanos en éste nuevo paradigma

Evaluar los riesgos particulares sin desatender los riesgos tradicionales

Banco Nación

“Los indiscutibles beneficios de la nube, puede resultar un dolor de cabeza para los CISOs, es esencial incluir a los departamentos de TI y Legales desde el inicio para realizar una adecuada toma de decisiones”

REFERENCIAS

- Gartner, 2008, Assessing the Security Risks of Cloud Computing
- NIST, 2011, Guidelines on Security and Privacy in Public Cloud Computing
- Instituto Nacional de Ciberseguridad de España, 2011, Riesgos y amenazas en cloud computing
- ENISA, 2011, Computación en nube
- Management Solution, 2012, La nube: Oportunidades y retos para los integrantes de la cadena de valor

Gracias!

Ing. Fernando Mattson, CISM
fmattson@bna.com.ar

Banco Nación