Sistemas de información fiables y valiosos

Valencia Chapter

Análisis de riesgos antes de migrar a la nube

Florencio Cano Gabarda

CISA, 27001 Lead Auditor

Responsable Seguridad Online ISACA Valencia

seguridad@isacavalencia.org - @florenciocano

Fecha: 23 de mayo de 2012

LA NUBE
Definición

NIST: Modelo de organización informática que permite:

- Acceso ubicuo a los recursos
- Acceso bajo demanda a recursos compartidos que pueden ser incrementados o reducidos rápidamente sin excesivos costes de gestión o intervención del proveedor

LA NUBE
Características

- Autoservicio bajo demanda
- Acceso a través de la red
- Piscina de recursos (resource pooling)
- Elasticidad
- Medición

LA NUBE
Modelos de servicio

- SaaS: Software-as-a-service
- PaaS: Platform-as-a-service
- IaaS: Infraestructura-as-a-service

LA NUBE
Beneficios

- Acceso a recursos informáticos a un precio razonable gracias a la economía de escala
- Pago por uso
- Alta disponibilidad
- Mayor seguridad
- Menor inversión en mantenimiento
- Menor espacio necesario
- Ubicuidad sencilla

RIESGOS


TAKING RISK
There's a fine line between taking a calculated risk and doing something dumb.

RIESGOS

RIESGO = f(VALOR, AMENAZA, VULNERABILIDAD, PROBABILIDAD, IMPACTO)

METODOLOGÍAS DE ANÁLISIS DE RIESGOS

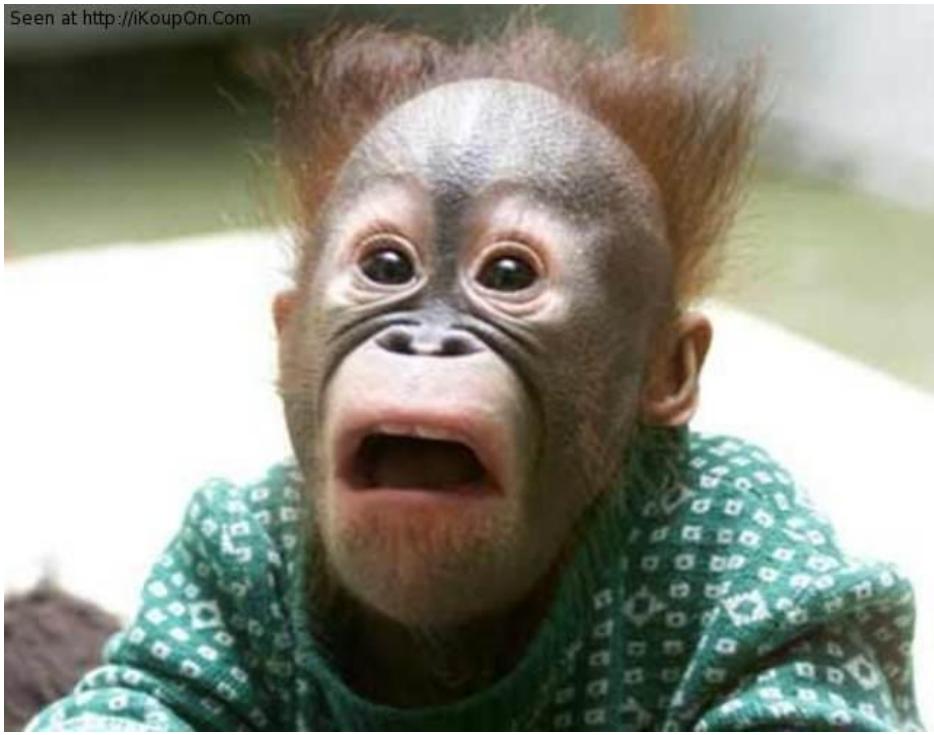
- MAGERIT
- OCTAVE
- MEHARI
- ISO 27005

PROCESO DE GOBIERNO DEL ANÁLISIS DE RIESGOS

- COBIT 5
  - EDM03 GARANTIZAR LA OPTIMIZACIÓN DEL RIESGOS (ENSURE RISK OPTIMISATION)
    - *EDM03.01 EVALUAR GESTIÓN DEL RIESGO (EVALUATE RISK MANAGEMENT)*
    - *EDM03.02 GESTÍÓN DEL RIESGO (DIRECT RISK MANAGEMENT)*
    - *EDM03.03 MONITORIZAR LA GESTIÓN DEL RIESGO (MONITOR RISK MANAGEMENT)*

AMENAZAS

- Perdida de control sobre la información
- Pérdida de datos
- No saber si se protegen adecuadamente nuestros datos
- No poder recuperar nuestros datos si queremos cambiar de proveedor
- Infringir alguna legislación en materia de protección de datos



AMENAZAS

- NO FUD (FEAR, UNCERTAINTY, DOUBT)

AMENAZAS

ISACA
Sistemas de información fiables y valiosos
Valencia Chapter

- DreamHost Database Hack Forces Mass Password Reset
- Companies left staggering or totally knocked out because of server problems in the Amazon datacenter
- PlayStation Network outages
- Twitter Experiences Delays in Delivering to Facebook and SMS
- Twitter Experiences Tweet Delivery Delay
- Heroku Shared Database Experienced Hardware Failure
- Heroku Users Unable to Provision New Dedicated Databases
- Google Fixes Gmail Outage That Affected Millions of Users
- Fraunhofer detecta deficiencias de seguridad en Dropbox, Mozy & Co.

AMENAZAS

- Incumplimiento legal
  - LOPD
  - Esquema Nacional de Seguridad
  - Legislación sobre datos sensibles como:
    - *Tarjetas de crédito*
    - *Datos sanitarios*
    - *…*
- Robo o daño de nuestros datos en la nube
- Pérdida de control sobre los datos
- Falta de disponibilidad en el acceso a los datos

AMENAZAS

OCASIONAN:

- Multas
- Daño a la imagen de la empresa/organización
- Pérdida de clientes/confianza
- **Mayor** inversión en recursos
- **Menor** flexibilidad para operar. Pérdida de oportunidad de negocio.

VULNERABILIDADES

- Contrato inadecuado o incompleto con el proveedor del servicio
  - Ausencia de garantías de cumplimiento legal
  - Ausencia de acuerdos de nivel de servicio
  - Ausencia de garantía de la ubicación de los datos
- Selección inadecuada del proveedor
- Desconocimiento de la ubicación de los datos
- Ausencia de monitorización del servicio recibido
- Ausencia de auditorías de segunda o tercera parte en el proveedor

GESTIÓN DEL RIESGO

- COBIT 5
  - Nivel de riesgo aceptable (Risk appetite/tolerance)
  - Objetivo: mantener el nivel de riesgo por debajo del nivel de riesgo aceptable
  - Reducir el riesgo mediante la aplicación de controles

ALGUNOS CONTROLES

- COBIT 5
- ISO 27001
- Nubes privadas
- Revisión y negociación de los contratos y niveles de servicio con los proveedores
- Selección adecuada de proveedores
- Monitorización de los servicios en la nube
- Procedimientos y políticas internas de uso de la nube adecuados

ISACA®
Sistemas de información fiables y valiosos
Valencia Chapter

ISACA®
Trust in, and value from, information systems

IT GOVERNANCE INSTITUTE®

GRACIAS POR SU ATENCIÓN

CISA® Certified Information Systems Auditor®
An ISACA® Certification

CISM® Certified Information Security Manager®
An ISACA® Certification

CGEIT® Certified in the Governance of Enterprise IT®
An ISACA® Certification

CRISC™ Certified in Risk and Information Systems Control™
An ISACA® Certification