



Cloud Security en IaaS

Una visión de Seguridad desde el Data Center



tecnológicagente



OWASP
LATAM TOUR 2013
18th March - 5th April



Marzo 2013

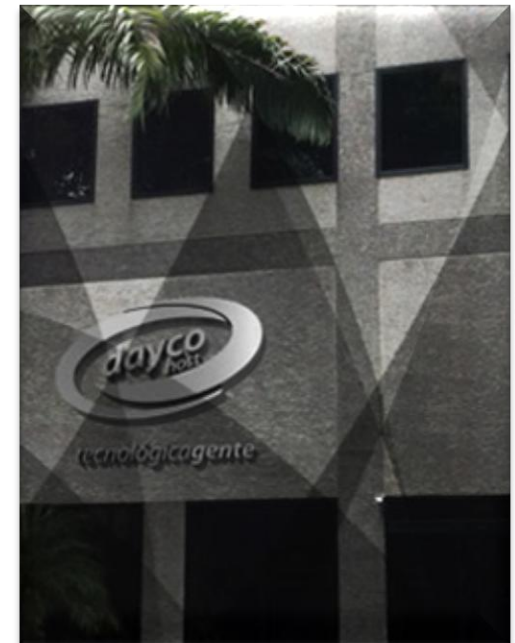
Introducción

Con el auge de la nube como alternativa de negocios y recuperación ante desastres, surgen nuevos retos de seguridad para los Data Center al ofrecer servicios híbridos o privados en esquemas de IaaS.

Cloud Security en IaaS.

Agenda.

1. ¿Qué es Cloud Computing? Arquitectura, Modelos de Servicio y Despliegue en el Cloud.
2. Retos de Seguridad en el Cloud.
 - Escalabilidad y Flexibilidad.
 - Mantenimiento de Infraestructura.
 - Respuesta a incidentes de seguridad.
 - Auditoría y Cumplimiento.
3. Modelo de confianza.
4. Desde el Data Center...

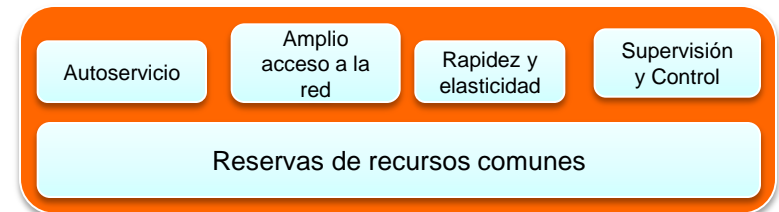


Cloud Computing.

Características.

Surge como un modelo “a la carta” para asignación y consumo de recursos de computación; abarca servicios, aplicaciones, redes, almacenamiento, información e infraestructura a implementar en ambientes rápidos y escalables:

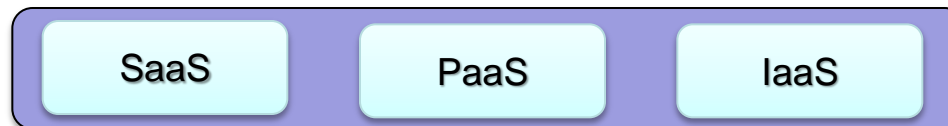
- Autoservicio
- Amplio acceso a la red
- Rapidez y elasticidad
- Supervisión y Control
- Reservas de recursos en común



Cloud Computing.

Modelos de Servicio.

Modelo de Cloud	Descripción
Software as a Service (SaaS)	Utiliza aplicaciones del proveedor en un entorno de nube.
Platform as a Service (PaaS)	Pueden desplegarse aplicaciones propias o adquiridas con entornos soportados por el proveedor.
Infrastructure as a Service (IaaS)	Se suministra procesamiento, almacenamiento, redes y otros recursos; así se delega control sobre los sistemas operativos, almacenamiento, aplicaciones y componentes de red (limitado).



Cloud Computing.

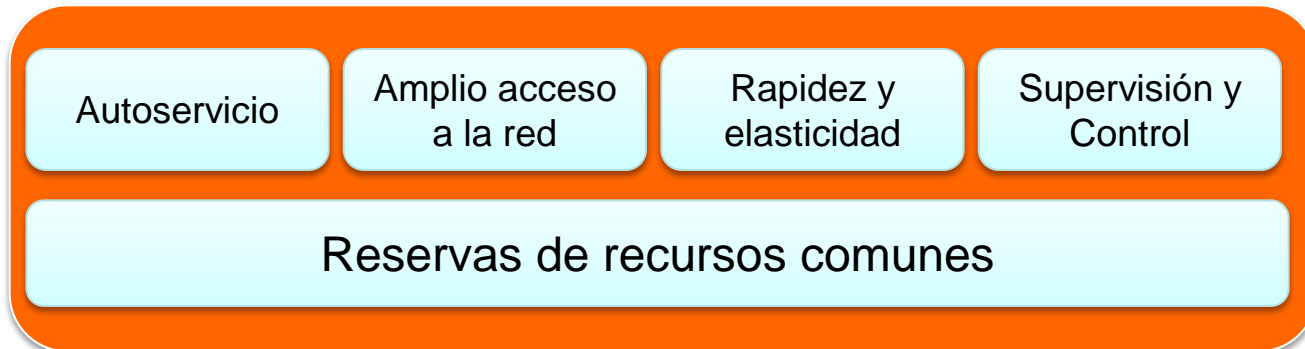
Despliegue.

Tipo de Cloud	Descripción
Nube Pública	A disposición del público en general. Se adquiere.
Nube Privada	A disposición de un grupo limitado u organización. Por lo general la maneja un tercero.
Nube Híbrida	Una o más nubes privadas y/o públicas, que a través de sistemas interoperables comparten información y aplican portabilidad.
Nube Comunitaria.	Infraestructura compartida por varias organizaciones y es soportada por una comunidad específica.

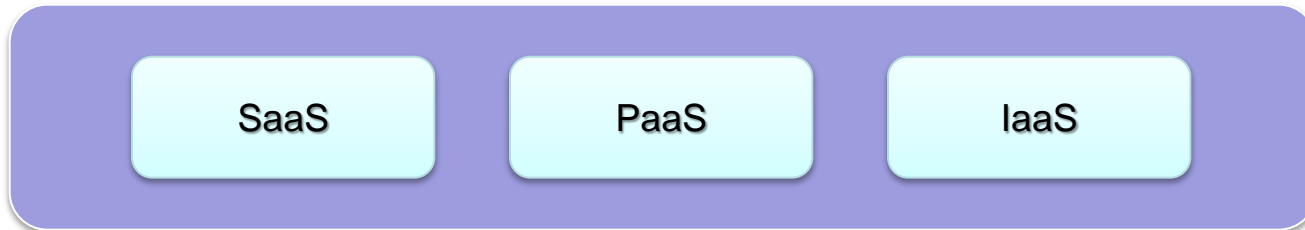


Cloud Computing.

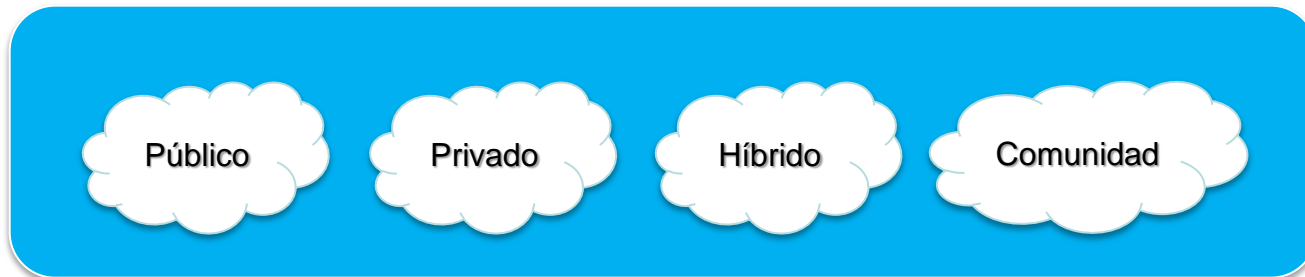
Arquitectura.



**Características
Esenciales**



**Modelo de
Servicios**



**Modelos de
Despliegue**

Cloud Computing.

Taxonomía.

Infrastructure Services

Storage

- Amazon S3 & EBS
- Rackspace Cloud Files
- Nirvanix
- AT&T Synaptic
- Zetta

Cloud Broker

- RightScale
- enStratus
- Kaavo
- Elastra
- CloudKick
- CloudSwitch

Compute

- Amazon EC2
- Serve Path GoGrid
- Rackspace Cloud Servers
- Joyent Cloud
- Flexiant Flexiscale
- ElasticHosts
- Terremark
- ITRICITY
- LayeredTech
- Savvis Cloud Compute
- Verizon CaaS
- AT&T Synaptic
- Sungard Enterprise Cloud
- Navisite

Services Management

- Scalr
- CohesiveFT
- Ylastic
- CloudFoundry
- NewRelic
- Cloud42
- Amazon CloudWatch
- Amazon VPC

CLOUD TAXONOMY

Cloud Software

SaaS Data Security

- Navajo
- PerspecSys

Data

- 10Gen MongoDB
- Apache CouchDB
- Apache HBase
- Hypertable
- Tokyo Cabinet
- Cassandra
- memcached
- Clustrix
- FlockDB
- Gizzard
- Redis
- BerkeleyDB
- Voldemort
- Terrastore

Compute

- Globus Toolkit
- Xeround
- Sun Grid Engine
- Hadoop
- OpenCloud
- Gigaspace
- DataSynapse

Cloud Management

- CA Turn-key Cloud
- OpenNebula
- Open.ControlTier
- Enomaly Enomalism
- VMware vCloud
- CohesiveFT VPN Cubed
- Hyperic
- Eucalyptus
- Puppet Labs
- Appistry
- IBM CloudBurst
- Cisco UCS
- Zenoss
- Surgient

File Storage

- EMC Atmos
- ParaScale
- Zmamba
- CTERA
- Appistry

Platform Services

General Purpose

- Force.com
- Etelos
- LongJump
- Rollbase
- Bungee Connect
- Google App Engine
- Engine Yard
- Caspio
- Qrimp
- MS Azure
- Mosso Cloud Sites
- VMforce
- Intuit Partner Platform
- Joyent Smart Platform

Business Intelligence

- Aster DB
- Quantivo
- Cloud9 Analytics
- K2 Analytics
- LogiXML
- Oco
- PivotLink
- Clario Analytics
- ColdLight Neuron
- Vertica

Integration

- Amazon SQS
- Amazon SNS
- Boomi
- SnapLogic
- IBM Cast Iron
- gnip
- Appian Anywhere
- HubSpan
- Informatica On-Demand

Development & Testing

- Keynote Systems
- SOASTA
- SkyTap
- Aptana
- LoadStorm
- Collabnet
- Rational Software Delivery Services

Database

- Amazon SimpleDB
- Mosso Drizzle
- Amazon RDS

Software Services

Financials

- Concur
- Xero
- Workday
- Expensify
- Intuit Quickbooks Online

Content Management

- Clickability
- SpringCM
- CrownPoint

Collaboration

- Box.net
- CubeTree
- SocialText
- Basecamp
- Assembla
- DropBox

Sales

- Xactly
- StreetSmarts
- Success Metrics

Desktop Productivity

- Zoho
- Google Apps
- HyperOffice
- MS Office
- Web Apps

Billing

- Aria Systems
- eVapt
- Redi2
- Zuora

Social Networks

- Ning
- Zembly
- Amitive
- Jive SBS

CRM

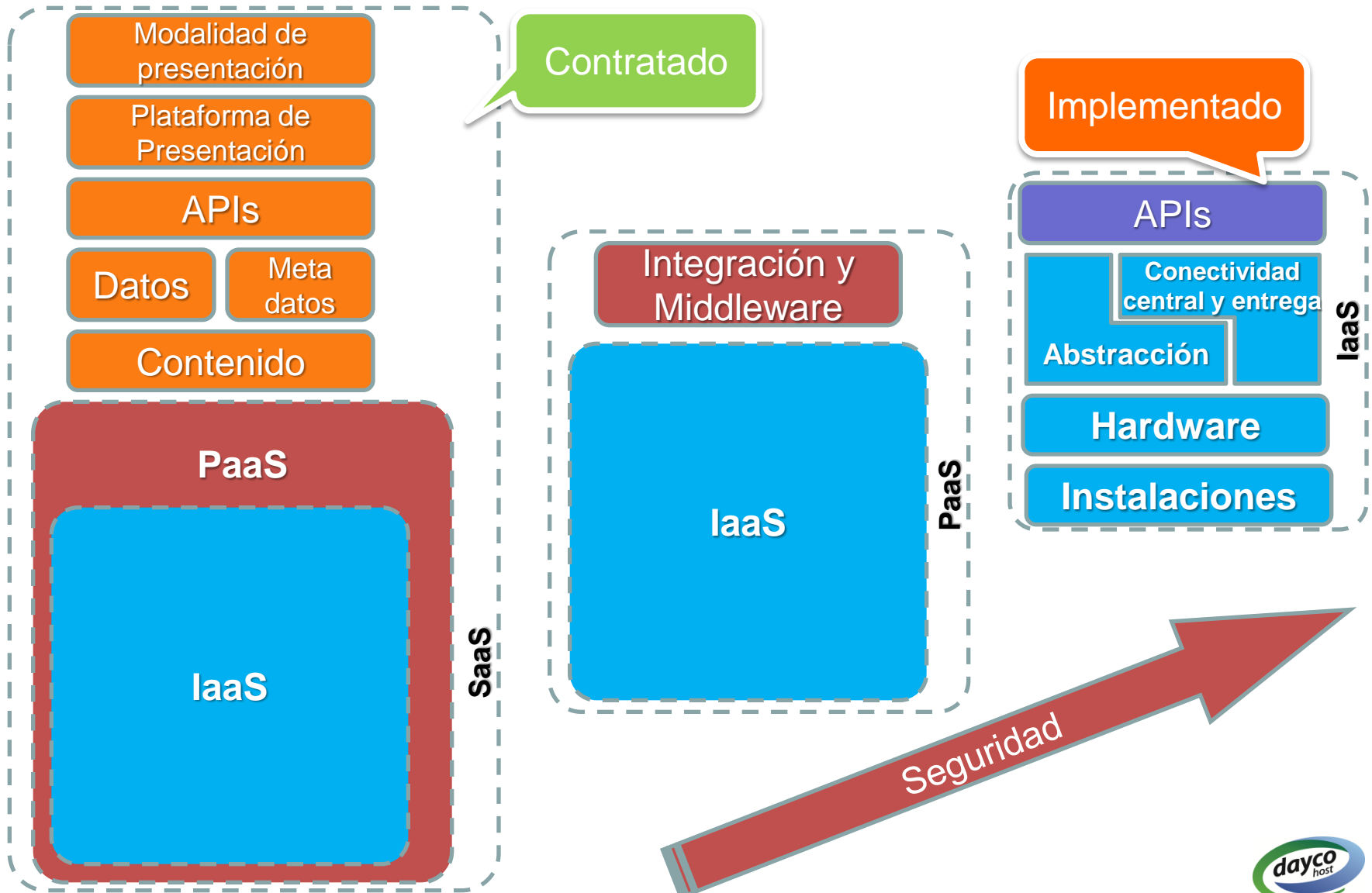
- NetSuite
- Parature
- Responsys
- Rightnow
- LiveOps
- MSDynamics
- Salesforce.com
- Oracle On Demand

Document Management

- NetDocuments
- DocLanding
- Knowledge TreeLive
- SpringCM

Cloud Security en IaaS.

Flexibilidad vs. Escalabilidad



Cloud Security en IaaS.

Retos: Escalabilidad y Flexibilidad

- **VM basadas en Hipervisor.** Utilización de máquinas virtuales sin formatos interoperables, presenta problemas de compatibilidad en migración de metadatos y software entre proveedores.
- **Almacenamiento en IaaS.** Dependencia en alto grado de aplicaciones que manejan las políticas de almacenamiento limitará la selección de un proveedor.
- **Portabilidad de los datos.** A medida que se almacenan datos en la nube, su vinculación resulta una preocupación considerando escenarios de excepción donde el proveedor “*limite*” la cantidad de contenido que pueda “*retirarse*” en períodos de tiempo finito.



Cloud Security en IaaS.

Retos: Escalabilidad y Flexibilidad

- **Capacidad de crecimiento.** El diseño inicial de la infraestructura influirá directamente en las capacidades de crecimiento de los servicios ofrecidos por el proveedor.
- **Diseño de Red.** Un buen diseño de red será la diferencia entre el despliegue efectivo y eventuales migraciones de un proveedor a otro.
- **Servicios de Seguridad Administrada.** El uso de soluciones de siguiente generación que permitan flexibilidad en el despliegue e integración de las aplicaciones del cliente.



Cloud Security en IaaS.

Retos: Mantenimiento de Infraestructura.

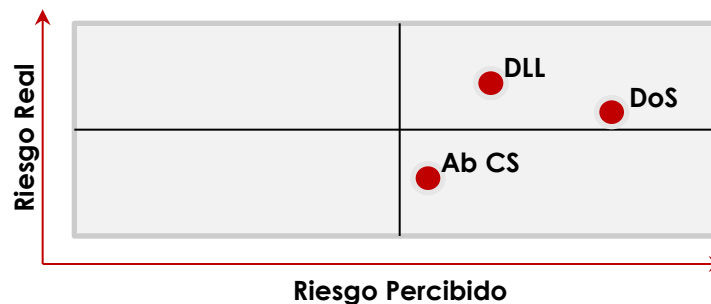
CLIENTE	PROVEEDOR
Sistema de Gestión de Identidad / Autenticación. <ul style="list-style-type: none"> Mantenimiento y Gestión. 	Sistemas de alojamiento, comunicaciones.
Gestión de Parches y Actualizaciones. <ul style="list-style-type: none"> Despliegue de actualizaciones, fixes y workarounds. 	Sistemas de climatización, suministro principal y alterno de electricidad.
Mantenimiento de Plataforma de Seguridad. <ul style="list-style-type: none"> IDS / IPS / FW / Antivirus / Webfilter / AntiSpam. 	Seguridad física, Contingencia, DRP.
Gestión de Registros. <ul style="list-style-type: none"> Recolección y correlación de los registros de control de seguridad. 	



Cloud Security en IaaS.

Amenazas y Contramedidas

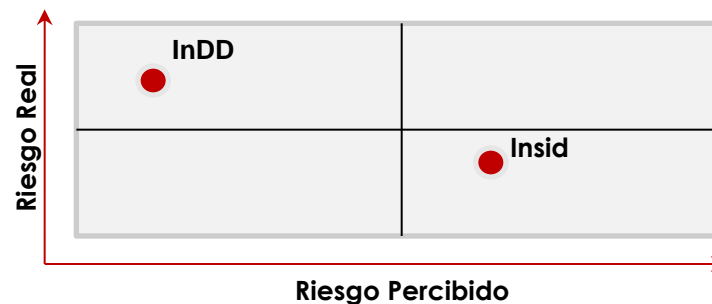
- **Denegación de Servicios (DoS).**
 - Baseline de Seguridad, Capacity Planning, arquitecturas robustas, seguras y escalables, manejo de ciberataques, blackholing, análisis-in-deep, control de tráfico interno.
- **Fuga de Datos / Pérdida de Datos (DLL).**
 - Análisis de Riesgo, Encriptación, Validación de Integridad, Políticas de Borrado Seguro, Manejo de ambientes Producción / No Producción, Resiliencia.
- **Abuso de Servicios de Cloud (Ab CS).**
 - Política de uso aceptable, SLA, manejo de ciberataques.



Cloud Security en IaaS.

Amenazas y Contramedidas

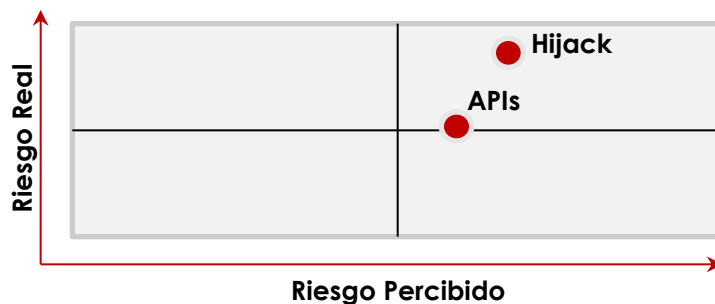
- **Debida Diligencia Insuficiente (InDD).**
 - Baseline de Seguridad, Gestión y manejo de Riesgos, BIA, BCP, DRP, Seguridad en redes y aplicaciones.
- **Insiders / Errores Humanos (Insid).**
 - Auditorías internas / externas, entrenamiento, políticas de seguridad de información, acceso restringido, roles y responsabilidades, segregación de funciones, encriptación, need-to-know.



Cloud Security en IaaS.

Amenazas y Contramedidas

- **Hijacking / Suplantación.**
 - Políticas de restricción de acceso, manejo de ciberataques, autenticación de varios factores, detección de intrusiones, AAA, credenciales intransferibles, revocación de privilegios.
- **Aplicaciones Inseguras (APIs).**
 - Verificación de vulnerabilidades, arquitecturas robustas y seguras, Políticas de restricción de acceso, manejo de ciberataques.



Cloud Security en IaaS.

Retos: Auditoría y Cumplimiento

- **eDiscovery.** Investigación electrónica, un *issue* durante las gestiones de preservación de evidencia, pesquisa o litigio.
- **Implementación de Estándares.** Uso de estándares (ISO 27000, NIST), vital en asegurar procesos de gestión de información y protección de datos.
- **Debida diligencia.** En la gestión y custodia de los datos junto con el need-to-know y la segregación de funciones.
- **Jurisdicción.** Aspecto fundamental, la delimitación de responsabilidades en el hospedaje de datos y entrega de información a los cuerpos de investigación.



Cloud Security en IaaS.

Retos: Auditoría y Cumplimiento

- **SLA.** Los acuerdos de niveles de servicio pasan a ser la piedra angular en la respuesta y cumplimiento.
- **Verificación de Vulnerabilidades.** La gestión de los proveedores de Cloud se soporta en las verificaciones periódicas de infraestructura para esquemas IaaS.
- **Soportes y Registros de la Plataforma.** Herramientas de auditoría esenciales para el establecimiento de hechos.
- **Procedimientos y documentación del Proveedor.** Como soporte sustancial en la gestión de riesgos (procedimientos, protocolos de acción, DRP, BCP, tratamiento de incidentes y ciberataques).



Cloud Security en IaaS.

Modelo de Confianza

- **Estratégico:**
 - Capacity Planning de la Arquitectura
 - Certificaciones Internacionales (ISO 20K / ISO 27K)
 - Comprensión de SLA, Contratos, Convenios.
 - Informes de rendimiento, CTQ, métricas.
- **Táctico:**
 - Manejo y mitigación de riesgos.
 - Procesos operativos para la adquisición de sistemas o servicios
 - Gestión de cambios, pase a producción.
 - Manejo de problemas.
- **Operativo**
 - Disminución del error humano.
 - Gestión efectiva de incidentes.
 - Pruebas continuas en Infraestructura
 - Planes de Contingencia y Recuperación ante Desastres



Cloud Security en IaaS.

Desde el Datacenter...

- La Nube Daycohost.
- ISO 20K.
- Proyecto Parque Tecnológico.



Mazo 2013

Daycohost Evoluciona

Desde el Datacenter...

Pasa a convertirse de una empresa de Hosting y servicios de infraestructura de Data Center a **una empresa de referencia en Venezuela en servicios de TI**

De una empresa enfocada en ofrecer ventajas en el uso y operación de las plataformas de operación requeridas por las empresas para operar sus aplicaciones a **una empresa que integra, opera y gestiona soluciones de servicio más complejas que agregan directamente valor a los negocios de nuestros clientes**

Hitos más Significativos

Desde el Datacenter...

- **+ de 400 clientes** en el sector de empresas e instituciones
- + de 3.000 clientes en Servicios Web
- + de 5.000 servicios instalados y en operación
- **Crecimiento** interanual en ingresos de **35%-40%**
- Aprox. (150) empleados directos
- Infraestructura totalmente operativa con **diseño N+1** y con capacidades instaladas para instalar nuevos servicios
- Plataformas de Servicios basadas en **tecnología de punta**: Virtualización y Consolidación de servicios

A donde vamos

Desde el Datacenter...

- A seguir manteniéndonos como la marca local **LIDER** en servicios de Data Center
- **Ampliar** nuestra penetración en los diferentes sectores del mercado: **Públicos** y **Privados** con soluciones cada vez más **robustas** y orientadas a agregar valor
- Desarrollar **Alianzas** con proveedores e integradores de servicios, a través de los cuales buscaremos integrar **Soluciones más Innovadoras**
- Ampliar el **Portafolio de Servicios** incorporando a los actuales de Data Center, nuevos servicios tanto en ambiente **CLOUD** como Servicios Profesionales
- A mantener la **flexibilidad** en el diseño de soluciones de acuerdo a los requerimientos de nuestros clientes y el tiempo de respuesta en la implementación de las mismas, como un factor clave de **competitividad** de la empresa

A donde vamos

Desde el Datacenter...

- A seguir fortaleciendo la **Calidad de Servicio** como el gran diferenciador de nuestra empresa, por lo que estamos reforzando la VP de Atención al Cliente a través de la mejora continua de los procesos de atención, resolución y operación del Data Center bajo el estándar **ITIL** y arrancando, recientemente, un proyecto de certificación de servicio **ISO 20000**
- Mantener la rigurosidad y **robustez de la infraestructura** de operación para ofrecer **100% de disponibilidad de servicio**, tecnología de punta, alternativas de interconexión, puntos de presencia nacionales e internacionales. Esta infraestructura, desarrollada bajo estándares internacionales, también estará siendo certificada de acuerdo a las mejores prácticas de la industria
- Mantener y desarrollar nuestro **Talento Humano** como nuestro activo más importante y fundamental generando bases de conocimiento que faciliten el uso y disponibilidad de la tecnología a nuestros clientes
- A convertir la cercanía de **Dayco host** en un elemento relevante y diferenciador, ya que no solamente se trata de su cercanía física sino de la cercanía de su lenguaje, comunicación y trato con los clientes que va más allá de la relación de un proveedor, **convirtiéndonos en un aliado experto y de fácil acceso**

Parque Tecnológico

Desde el Datacenter...

- Terreno de **6.000 m²** ubicado en la Zona Industrial El Bosque, Av. Domingo Olavarría con Calle Hans Neumann, parcela #7, Valencia, Edo. Carabobo
- Inversión total estimada de **Bs. 180.000.000** para la construcción de obras civiles y equipamiento
- Puesta en operación: **T4-2013**
- Conformado por:
 - ✓ Primer Centro de Datos en Venezuela con certificación internacional (**TIER III**)
 - ✓ Centro de Entrenamiento
 - ✓ Centro de Innovación (I+D+I)
- Diseño y construcción basado en el uso de materiales que permiten el **ahorro energético** a través del uso de **paneles solares**, apoyando la conciencia ecológica
- **Alineado** con las normas y estándares exigidos por **SUDEBAN** para la operación de **Centros Alternos de la Banca**

PARQUE TECNOLÓGICO

Diseño Arquitectónico 3D





tecnológica gente

Gracias...



***Ing. Omar Alvarado
CISO***

C/EH – GSEC – ISO27kLA

ISACA # 532740

SANS # 32340

OWASP # 15530060

daycohost.com

Torre Dayco, Calle Londres, Urb. Las Mercedes,
Caracas-Venezuela, 1060A

+58 212 999.9100 / Fax +58 212 999.9101