SOCHISI
DIGITAL SECURITY THINK TANK

Escuela Sochisi

¿Qué nuevo debemos saber de Seguridad para la Nube de lo que ya sabemos de Seguridad?

Ricardo Urbina M
rurbina@cloudsecurityalliance.cl
Enero 2021

CSA cloud security alliance®

Temario

- ¿Qué es CSA?
- Seguridad On Premise
- ¿Qué es la Nube?
- Gestión del Riesgo, Cuestiones Legales y Cumplimiento
- Gobierno de la Información
- Plano de Gestión y Continuidad del Negocio
- Seguridad de la Infraestructura, virtualización y Contendores
- Respuesta ante Incidentes
- Seguridad de Aplicaciones y Cifrado de Datos
- Gestión de Identidades, Derechos y Accesos
- Seguridad como Servicio

¿Qué es CSA?

Cloud Security Alliance (CSA) es una Organización Internacional sin fines de lucro, creada con el objeto de fomentar el uso de buenas prácticas de seguridad en el uso de Cloud Computing.

SEATTLE/Bellingham, WA // US HEADQUARTERS

EDINBURGH // UK HEADQUARTERS

Locales

29 Grupos Activos de Trabajo

SINGAPORE // ASIA PACIFIC HEADQUARTERS

cloud security alliance®

Seguridad On Premise

- Seguridad er
- Seguridad er
- Zero Trust
- Seguridad pc

Seguridad en la Nube

¿Qué es la Nube?

Servicios basados en tecnología que cumple con:

NIST ISO 17788

Multitenancy

CSA cloud security alliance®

Seguridad en la Nube

cloud security alliance®

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Special Publication 500-291, Version 2

NIST Cloud Computing Standards Roadmap

NIST Releases Evaluation of Cloud Computing Services Based on NIST SP 800-145 (NIST SP 500-322)

February 23, 2018

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Special Publication 500-292

NIST Cloud Computing Reference Architecture

NIST Releases Cloud Computing Service Metrics Description (NIST Special Publication 500-307)

April 24, 2018

ISO/IEC 17789:2014
Information technology — Cloud computing — Reference architecture

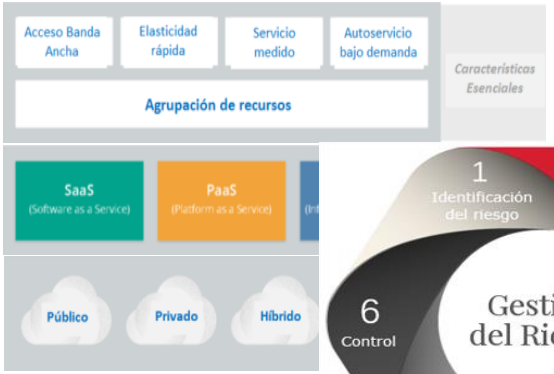
ISO/IEC 27017:2015(en)
Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services

ISO/IEC 27036-4:2016(en)
Information technology — Security techniques — Information security for supplier relationships — Part 4: Guidelines for security of cloud services

ISO/IEC 19086-4:2019(en)
Cloud computing — Service level agreement (SLA) framework — Part 4: Components of security and of protection of PII

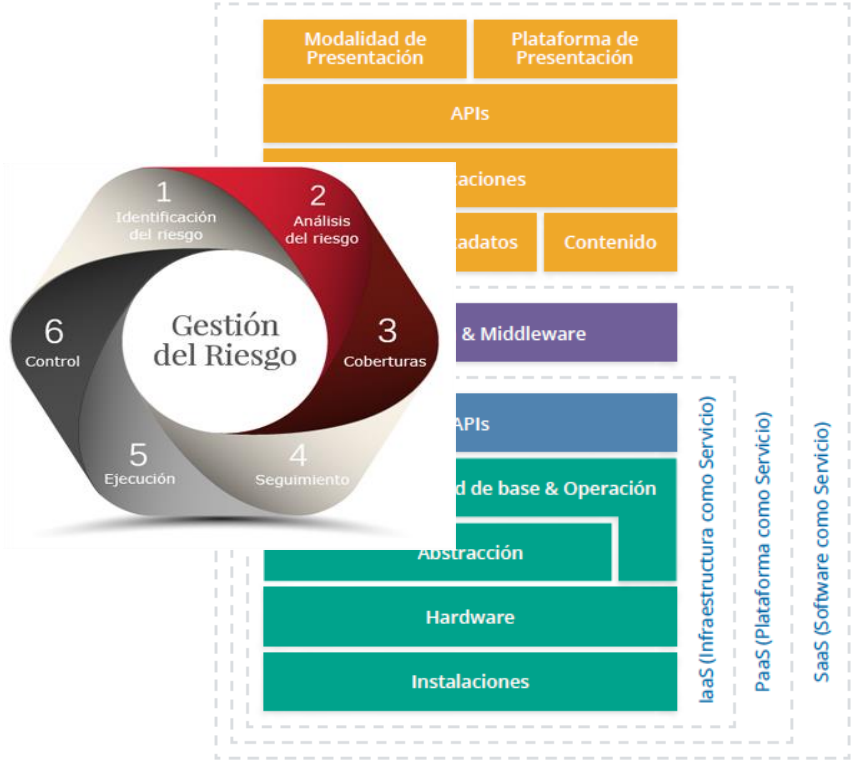
ISO/IEC TR 22678:2019(en)
Information technology — Cloud computing — Guidance for policy development
6.4.11 Trust and transparency

Seguridad en la Nube



cloud security alliance®

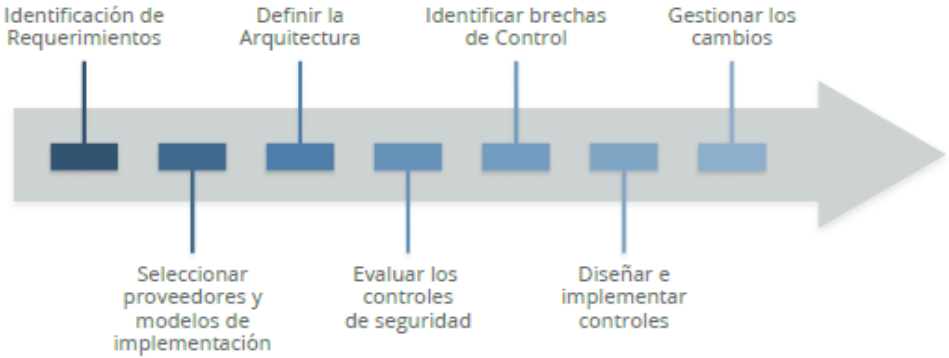
Seguridad en la Nube



cloud security alliance®

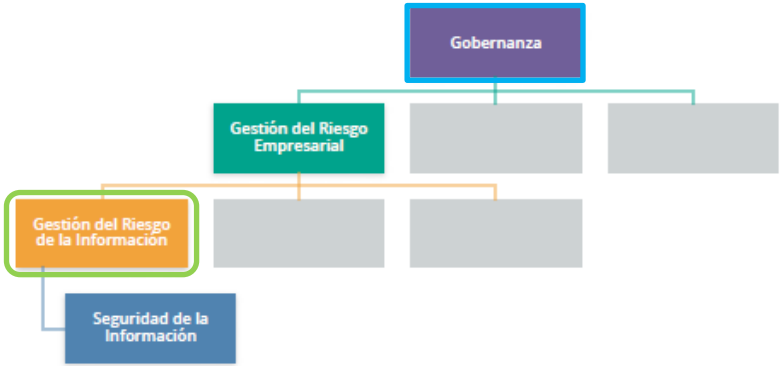
Seguridad en la Nube

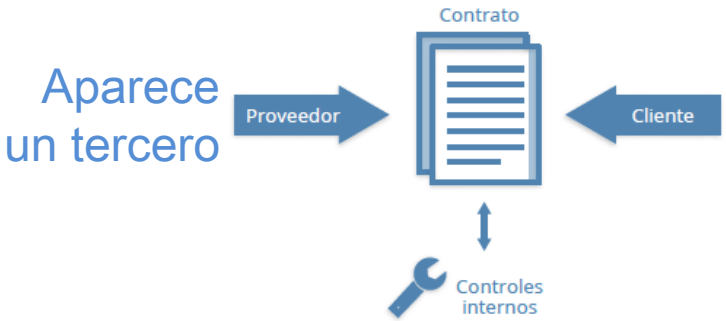
Modelo simple de proceso de seguridad en la Nube

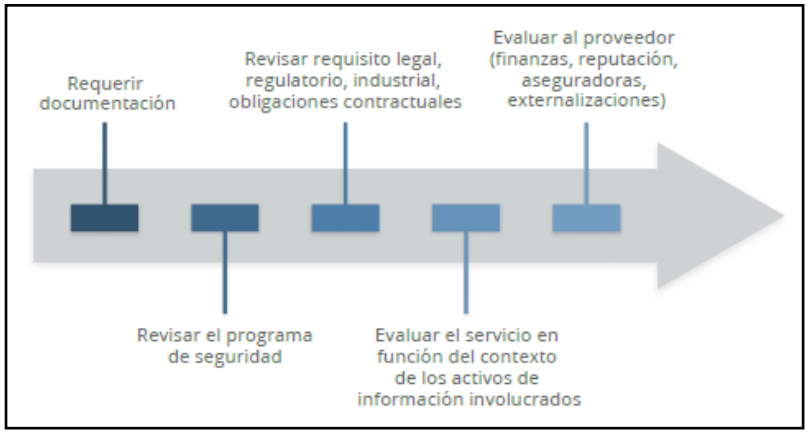


cloud security alliance®

Gestión del Riesgo y Cuestiones Legales



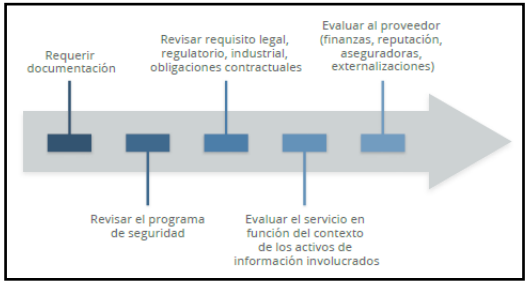




CSA cloud security alliance®

Cumplimiento

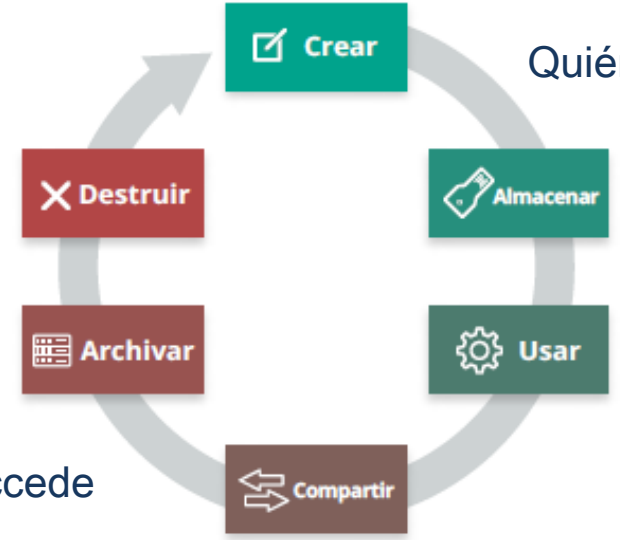
Proveedor



cloud security alliance®

Gobierno de la Información

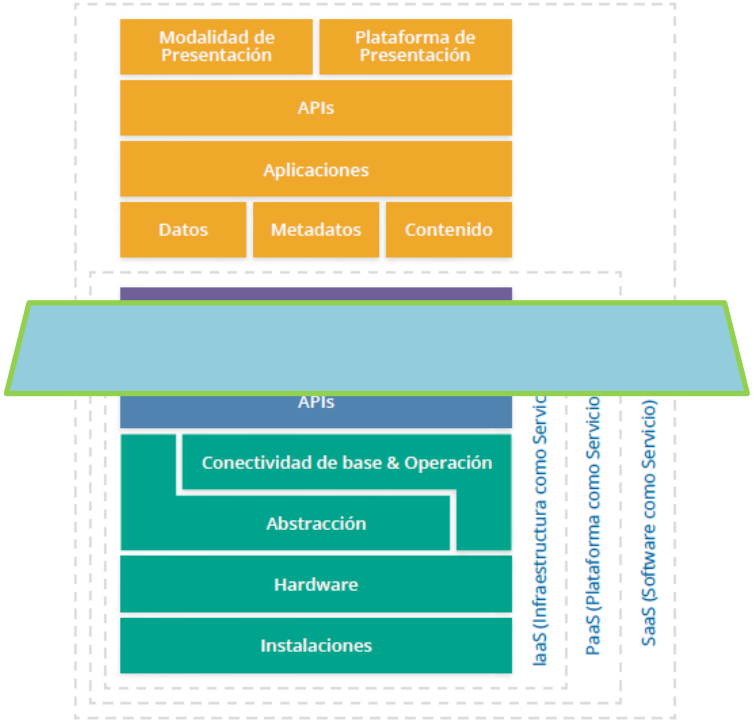
- ✓ Clasificación de la información
- ✓ Políticas de Gestión de la información
- ✓ Ubicación y políticas jurisdiccionales
- ✓ Autorizaciones
- ✓ Propiedad
- ✓ Custodia
- ✓ Privacidad
- ✓ Controles contractuales
- ✓ Controles de seguridad



Quién lo accede

Desde donde se accede

Plano de Gestión y Continuidad del Negocio

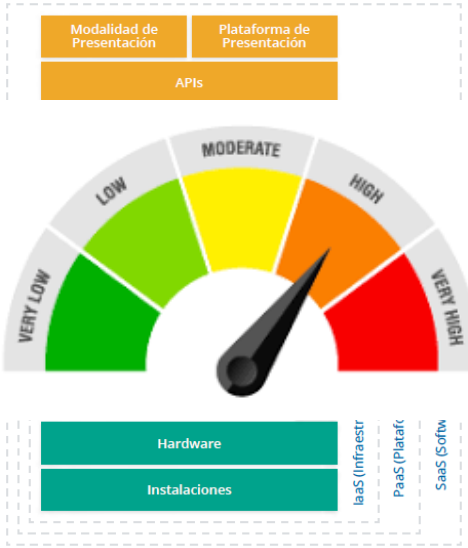


Plano de Administración (Management Plane)

El proveedor

El usuario

Plano de Gestión y Continuidad del Negocio



Continuidad de Negocio (BCP)
y
Recuperación ante Desastres (DR)

- ✓ Diseñar arquitectura considerando las posibles fallas
- ✓ Considerar desde el riesgo con peor escenario
- ✓ Incluir Alta Disponibilidad del proveedor en el diseño del servicio
- ✓ Preparase para una caída ordenada si el proveedor falla
- ✓ Tener claro el nivel de servicio comprometido por el proveedor y claridad de lo que implica

Seguridad de la Infraestructura, virtualización y Contendores

Recursos básicos empleados para crear una nube, esto es, procesadores, memoria, etc.) redes y almacenamiento

Infraestructura abstracta o virtual gestionada por un usuario de la nube

Tipos de redes:

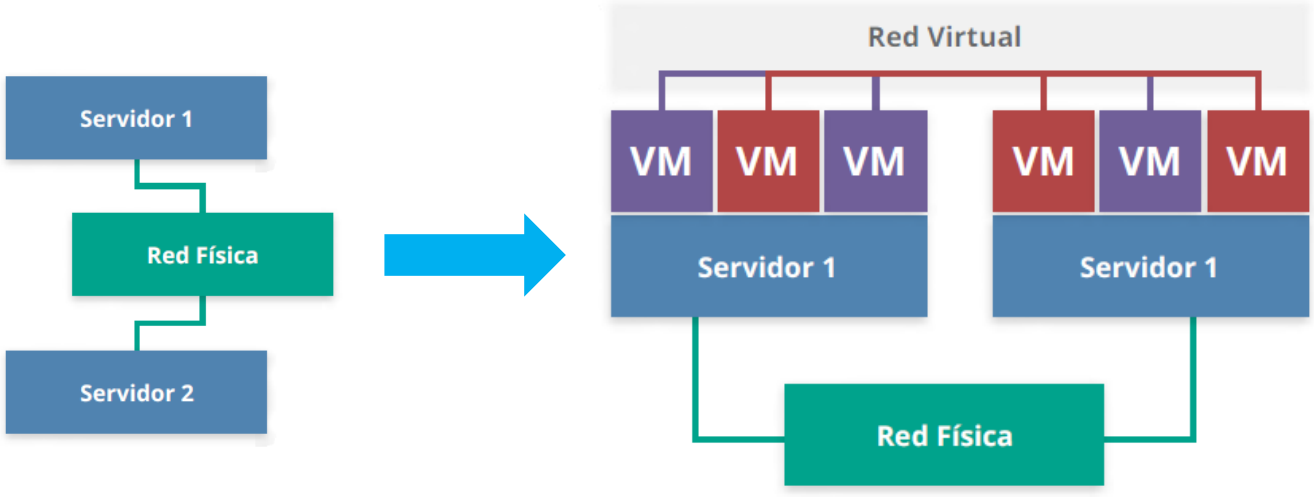
- Gestión
- Almacenamiento
- Servicio

VPN, virtual private network

SDN, Software Defined Networking

- ~~IDS (control físico con cajas)~~
- ✓ Equipos virtuales de control
- ✓ SDN aislamiento
- ✓ SDN grupos de seguridad
- ✓ SDN niega todo por defecto
- ✓ Microsegmentación y Perímetro definido por software (SDP)

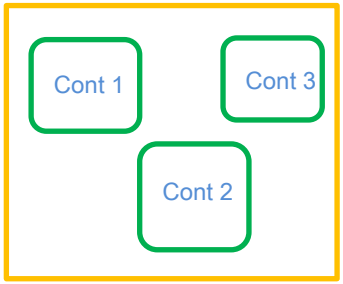
Seguridad de la Infraestructura, virtualización y Contendores



Seguridad de la Infraestructura, virtualización y Contendores

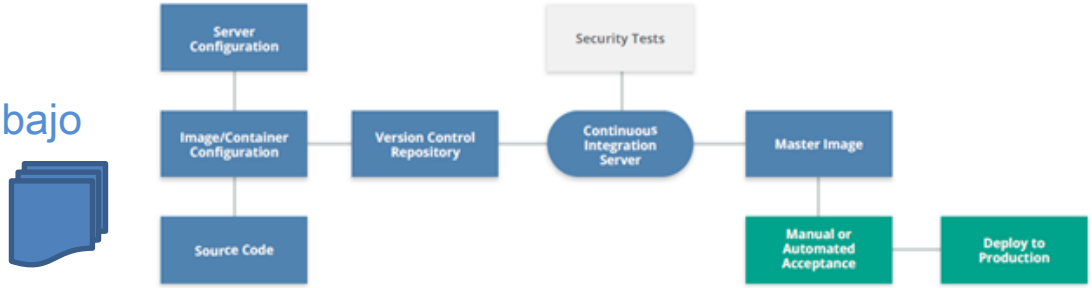
Máquinas virtuales (VM)

Contenedores



Serverless

Cargas de trabajo inmutables



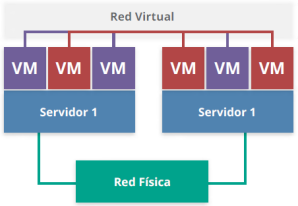
cloud security alliance®

Seguridad de la Infraestructura, virtualización y Contendores

Recomendaciones

Conocer la seguridad de la infraestructura del proveedor

- ✓ El modelo de seguridad compartida (capas)
- ✓ Certificaciones y cumplimientos



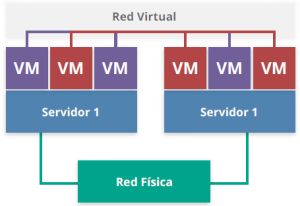
Red

- ✓ Preferible usar SDN
- ✓ Segmentar
- ✓ Denegar servicios por omisión
- ✓ Controlar por cargas de trabajo (grupos de seguridad)
- ✓ Reducir cuellos de botella

Seguridad de la Infraestructura, virtualización y Contendores

Procesamiento/carga de trabajo

- ✓ Usar inmutables cuando sea posible
- ✓ Mantener los más registros posibles
- ✓ Conocer limitaciones del diseño del proveedor



Contenedores

- ✓ Conocer capacidad de aislamiento de los contenedores
- ✓ Utilizar máquinas físicas o virtuales para aislar los contenedores
- ✓ Control de proceso de despliegue de contenedores aprobados
- ✓ Proteger las capas de gestión de los contenedores
- ✓ Controles de acceso basados en roles y autenticación robusta para acceder a contenedores y/o repositorios de éstos

Respuesta ante Incidentes

NIST800-61 REV2

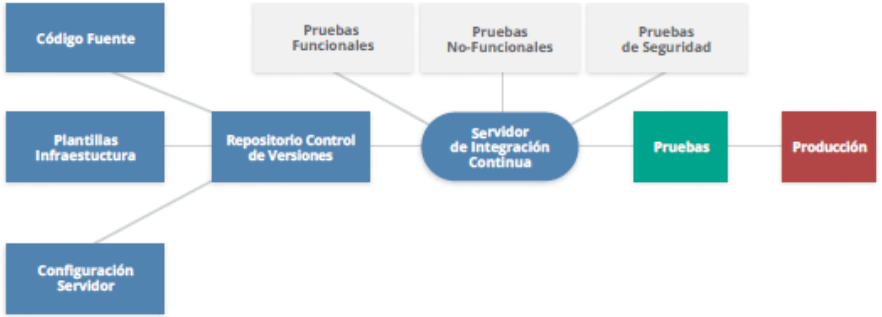
Diferencias con seguridad OnPremise

- ✓ SLA y Gobierno del proveedor de la nube
- ✓ Varía de acuerdo al modelo (IaaS, PaaS o SaaS)
- ✓ Herramientas de análisis forense
- ✓ Revisar muy bien capacidades para accionar las etapas (log, segregación, gestión vulnerabilidades, etc.)
- ✓ Conocer cadena de custodia
- ✓ Usar capacidades de nube para recuperación

Seguridad de Aplicaciones y Cifrado de Datos

Desarrollo y Diseño Seguro

Despliegue continuo



Seguridad de Aplicaciones y Cifrado de Datos

DevOps

- ✓ Estandarización
- ✓ Pruebas automatizadas
- ✓ Inmutables
- ✓ Mejoras en auditoría y gestión del cambio
- ✓ SecDevOps/DevOpsSec

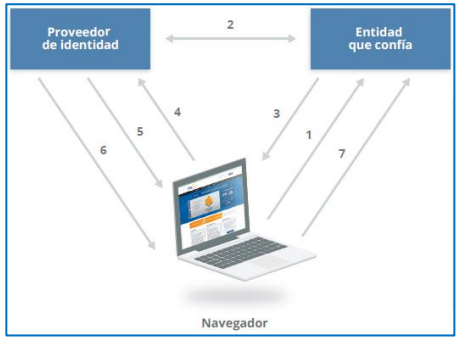
Integración Continua / Implementación Continua
CI / CD

- ✓ Considere utilizar las opciones de cifrado y almacenamiento gestionado que ofrezca el proveedor.
- ✓ Cuando sea posible, utilice claves gestionadas por el cliente.

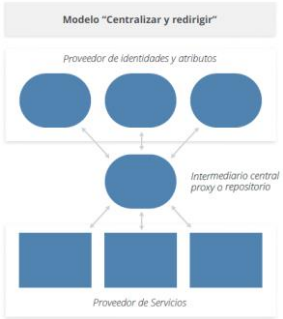
CSA cloud security alliance®

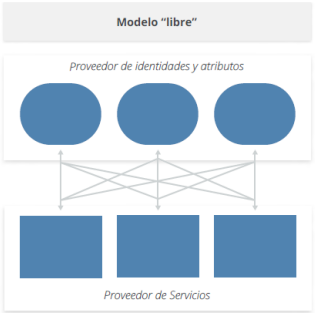
Gestión de Identidades, Derechos y Accesos

Gestión de identidades federada



1. El usuario envía su URL de OpenID
2. El proveedor de identidad y la identidad que confía fijan un secreto compartido.
3. El navegador es redirigido para obtener el token del proveedor de identidad.
4. Se pide al proveedor de identidad un token para el sitio que quiere ser accedido
5. Se autentica si es necesario
6. El token se envía al navegador
7. El token se presenta a la entidad que lo solicitó



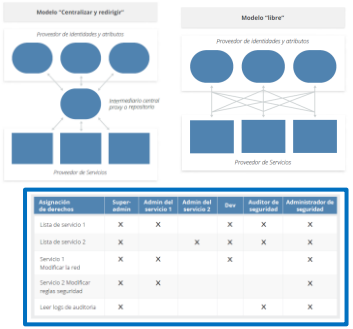


Asignación de derechos	Super-admin	Admin del servicio 1	Admin del servicio 2	Dev	Auditor de seguridad	Administrador de seguridad
Lista de servicio 1	X	X		X	X	X
Lista de servicio 2	X		X	X	X	X
Servicio 1 Modificar la red	X	X		X		X
Servicio 2 Modificar reglas seguridad	X	X				X
Leer logs de auditoria	X				X	X

Ejemplo de matriz de asignación de derechos

cloud security alliance®

Gestión de Identidades, Derechos y Accesos



Recomendaciones

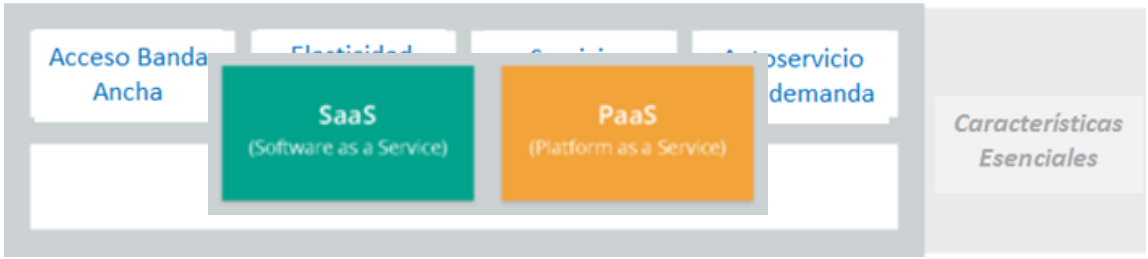
- Desarrollar un plan formal y entendible junto a procesos para gestionar identidades y autorizaciones en los servicios en la nube.
- Usar la técnica de federación, si es posible, para extender la gestión de identidades ya existente.
- Las identidades privilegiadas deberían usar siempre un factor de autenticación múltiple.
- Preferir control de acceso basado en atributos al control de acceso basado en roles.
- No hay protocolos mágicos: seleccione los casos de uso y las restricciones primero y luego busque el protocolo adecuado.

cloud security alliance®

Seguridad como Servicio

SecaaS

Servicios de Seguridad con atributos de los servicios en la Nube



Beneficios

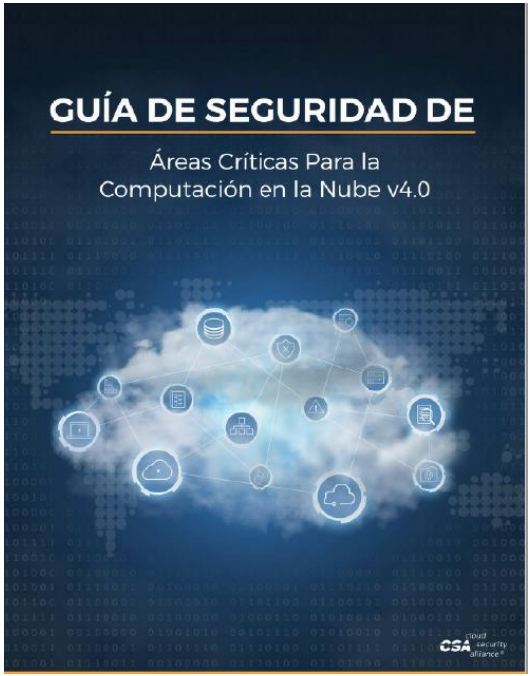
- Atributos servicios en la nube
- Personal y experiencia
- Intercambio de inteligencia
- Flexibilidad en la implementación
- Aislamiento de clientes
- Escalamiento y costos

Problemas potenciales

- Falta de visibilidad
- Manejo de datos regulados
- Fuga de datos
- Cambiar proveedor
- Migración a SecaaS

CSA cloud security alliance®

Documento de Referencia



https://cloudsecurityalliance.org/research/guidance/

cloud security alliance®

¿Preguntas?

SOCHISI
DIGITAL SECURITY THINK TANK

Escuela Sochisi

CSA cloud security alliance®

SOCHISI
DIGITAL SECURITY THINK TANK

Escuela Sochisi

https://cloudsecurityalliance.org/

contacto@cloudsecurityalliance.cl

@Cloudsa_cl

GROUPS Cloud Security Alliance, Chile Chapter

CSA cloud security alliance®