ORGANIZA:

CISO Convergence

Curso

RIESGOS TÉCNICOS Y LEGALES EN EL CLOUD

20 y 21 de enero
17 a 20 hrs

Relatores

Benito Venegas

Master© en Seguridad de la Información Empresarial, con más de 20 años de experiencia en empresas internacionales. Trabajando con Cloud Service Providers desde 2006.

Andrés Pumarino

Abogado, socio Legaltrust, Magíster en Negocios, profesor especializado en derecho y tecnología.

Valor general: $48.000

INFORMACIÓN E INSCRIPCIONES

www.cloud.cisoconvergence.com

CURSO

RIESGOS TÉCNICOS Y LEGALES EN EL CLOUD

OBJETIVO DEL CURSO

Con esta actividad buscamos concientizar a los participantes que Cloud es muy útil, sobre todo en épocas de pandemia. Para ello entregaremos, basado en la experiencia de los relatores, los detalles que puedan ayudar a tomar una sólida decisión respecto al uso de Cloud en sus organizaciones, destacando los elementos básicos de los riesgos para que el interlocutor pueda implementar y/o modificar sus políticas de seguridad, de acuerdo a los servicios prestado por un CSP.

PROGRAMA

1.- Definición de modelos de Cloud existentes:

- IaaS / PaaS / SaaS

2.- Modelos de implementación de Cloud computing

- Cloud privado (Productos Oracle, HW propio con VMWare/Xen/Linux KVM/Microsoft Hyper V/etc
- Cloud público (AWS, GCP, Azure)
- Cloud híbrido (Open Stack y CSP; orquestación agnóstica)

3.- Riesgos a considerar para áreas Legales, de Gobierno y Gestión TI, Compliance

- Pregunta antes de comenzar: ¿Sus organizaciones mantienen una política de seguridad de la información?
- ¿Cuál modelo es menos riesgoso? SaaS? IaaS? PaaS?On-premise/datacenter?
- Cloud defaults, son lo suficientemente seguros?
  Antivirus, Firewall, WAF no son configuraciones implementadas por default
  ¿Estoy a salvo de un ataque Ransomware?
  Exposición accidental de datos sensibles
- Pérdida de control y visibilidad sobre sus recursos
- Auto servicio de recursos on-demand simplifica el abuso
- ¿Cuál es su política de seguridad de la información en su organización, respecto a uso de recursos en Cloud?
- Gestión de acceso, contraseñas y MFAAccesos no autorizados
- ¿Eliminación de los datos, es incompleta?
- Datos en Cloud pérdidos. ¿Dónde está el backup?
- Vendor Lock-in complica migrarse a otros CSP (en el futuro)
- Desarrolladores certificados o aprendiendo sobre la marcha? Quien utiliza mejor los recursos en Cloud? Entrenamiento continuo
- Mala configuración y gestión de cambio inadecuado
- Falta de arquitectura y estrategia de seguridad en la nube
- Migración y uso de la nube: Logs de auditoria (AWS Cloudtrial; GCP Cloud Audit logs; Azure Activity Logs); ¿Quién utilizó mi nube?

CISO Convergence

CURSO

RIESGOS TÉCNICOS Y LEGALES EN EL CLOUD

PROGRAMA

4.- Aspectos contractuales relacionados con el Cloud Computing

Aspectos precontractuales del Cloud Computing:

- Preguntas iniciales sobre migración y mapas de rutas.
- Evaluación de seguridad y del impacto en el tratamiento de datos personales.

Aspectos contractuales:

- Obligación de las partes.
- Privacidad y protección de datos personales.
- Propiedad Intelectual.
- Seguridad de la Información, Confidencialidad y otras obligaciones.
- Regulación sectorial, si procediese.
- Localización de los datos y aspectos de sobernía.
- SLA.
- Responsablilidad.
- Duración, suspensión y terminación del contrato.

DIRIGIDO A

Gerencias de Tecnología
Gerencias de Gestión de Riesgo TI
Gerencias de Desarrollo de software (para productos API, Web Services, Web servers en general, aplicaciones de acceso basado en Cloud/Nube)

Duración: 6 horas pedagógicas.
Modalidad: Online, con posibilidad de conectarse vía Webex o por website de acceso restringido (user/password).

CISO Convergence