Universidad de los Andes Colombia | Departamento de Ingeniería de Sistemas y Computación

FOROS ISIS

5to FORO

en Seguridad de la Información

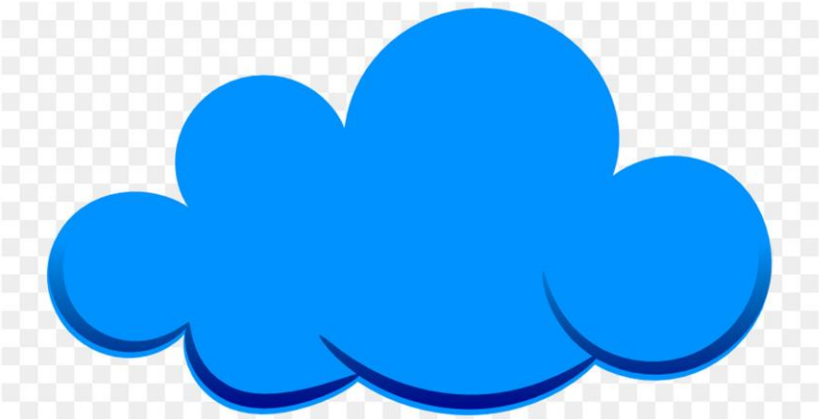
RETOS Y SOLUCIONES

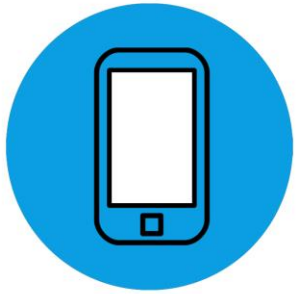
PARA LA PRIVACIDAD EN UN MUNDO CONECTADO

Universidad de los Andes | Vigilada Mineducación.

Reconocimiento como Universidad: Decreto 1297 del 30 de mayo de 1964 | Reconocimiento Personería Jurídica: Resolución 28 del 23 de febrero de 1949 Minjusticia.

5to FORO
en Seguridad de la Información





Privacidad de datos en Cloud - AWS

Johan Barrios

Tipos de nube

Nube privada

Herramientas que permiten escalabilidad y auto servicios en arquitectura propietaria

Infrastructura como servicio (IaaS)

Cómputo, almacenamiento y redes escalables por demanda alojadas por un proveedor

Plataforma como servicio (PaaS)

Grupo de herramientas necesarias para el desarrollo de aplicaciones alojadas por un proveedor

Software como servicio (SaaS)

Aplicaciones alojadas por un proveedor y consumidad por clients a través de internet.

5to FORO en Seguridad de la Información

Tipos de nube

Nube personal

Capacidades alojadas por el proveedor desde el almacenamiento, hasta la transmisión de medios, la colaboración, accesibles a través de cuentas personales

Productos

computación

Almacenamiento

Base de datos

Migración

Redes y entrega de contenido

Herramientas para desarrolladores

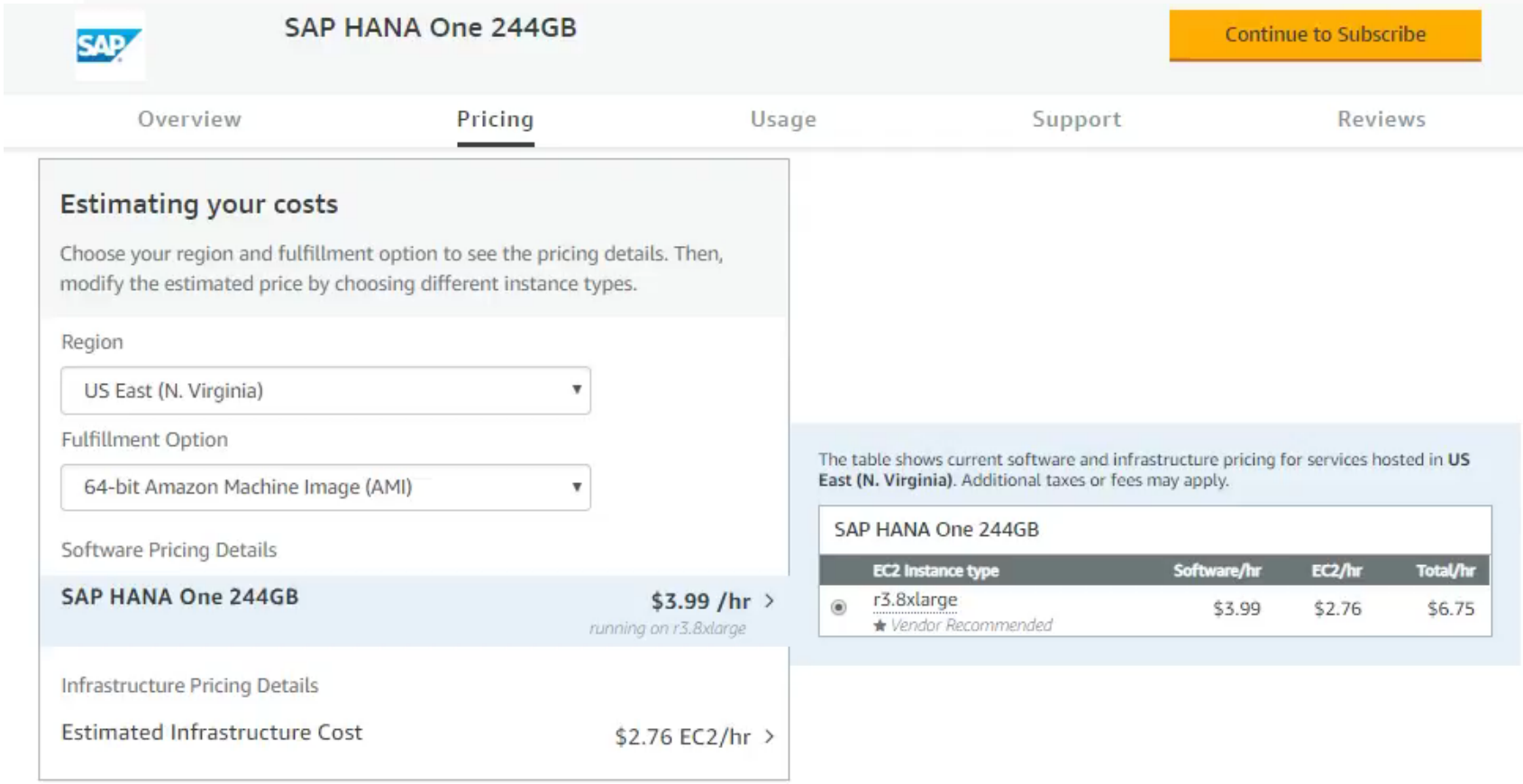
Servicios multimedia

Herramientas de administración

Seguridad, identidad y conformidad

5to FORO
en Seguridad de la Información

Sencillez



5 to FORO
en Seguridad de la Información

Consideraciones

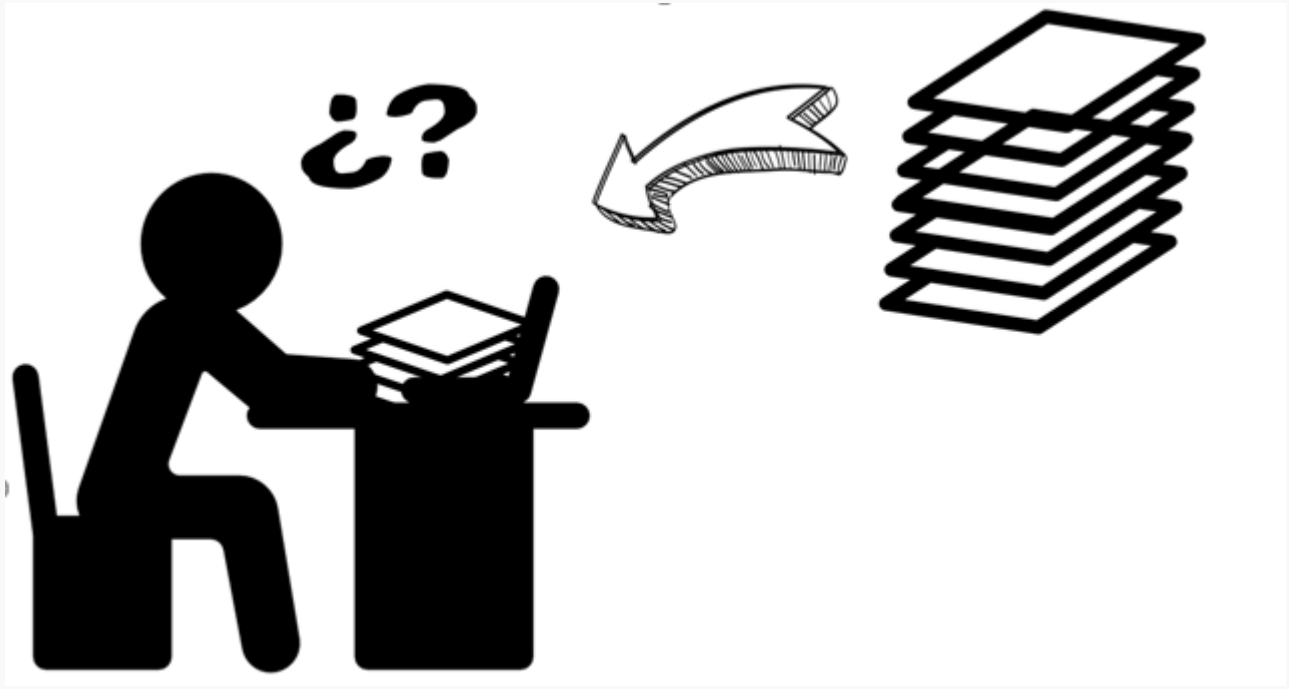
1. Comprender y cumplir con varias leyes de privacidad jurisdiccional.

2. Comprenda cómo su proveedor de servicios en la nube protegerá sus datos.

3. Explore diferentes tecnologías y herramientas de cifrado

Data privacy in the cloud - Deloitte 2016

Acuerdos legales sobre privacidad



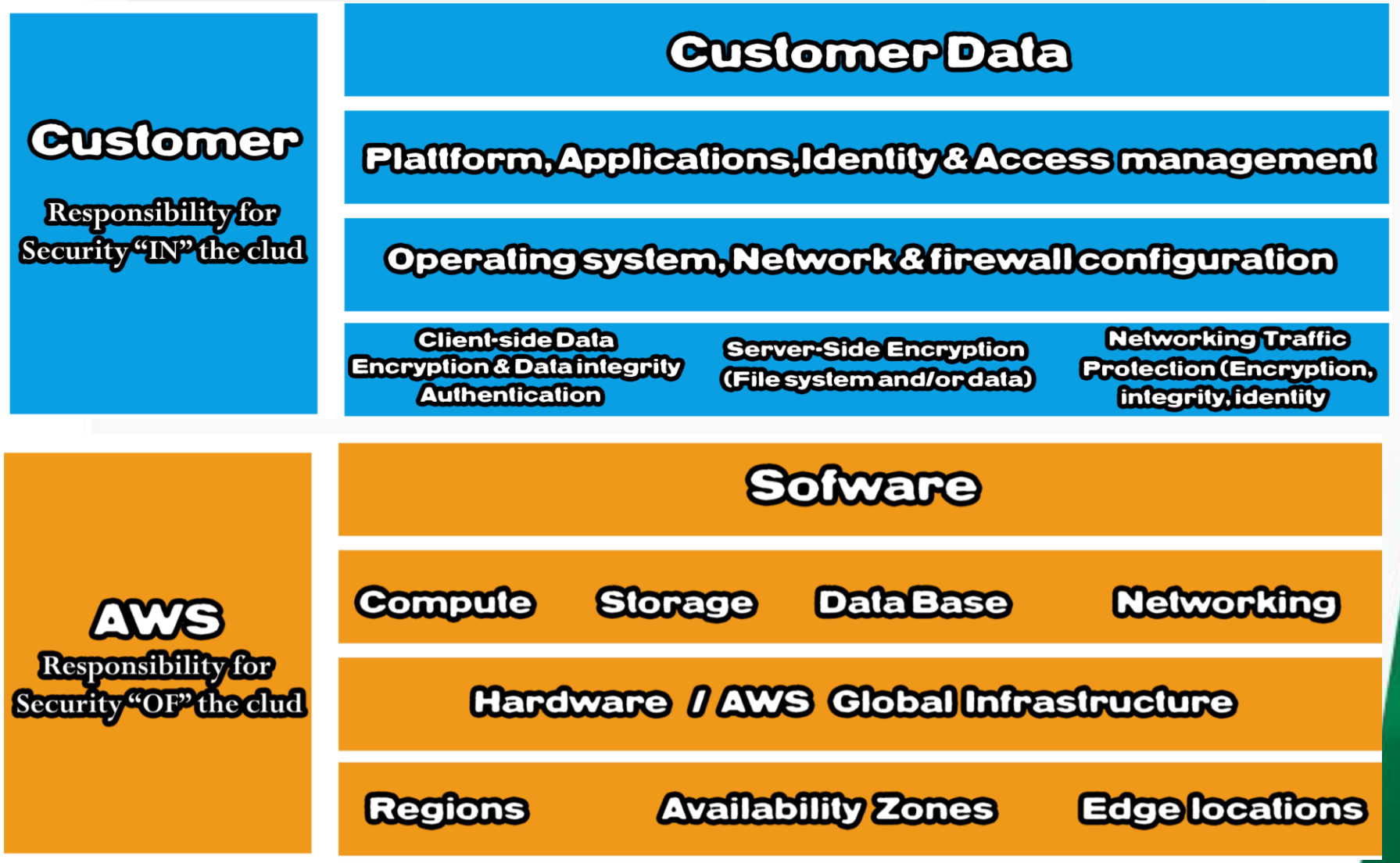
Industria y Comercio
SUPERINTENDENCIA

GDPR

Privacy Shield
Framework

5 to FORO
en Seguridad de la Información

Seguridad Cloud
Responsabilidad compartida



Acuerdos legales sobre privacidad

Debemos solucionar en conjunto con los proveedores las siguientes dudas :

- **El contenido estará seguro?**
- **Dónde estará el contenido almacenado?**
- **Quién tendrá acceso al contenido?**

Ciclo de vida de los datos

Soluciones de seguridad existen disponibles en la nube

Cifrado de Datos

Cifrado de Redes

SIEM

Seguridad y gestión de eventos

Entrenamiento profesional en la nube

Detección y prevención de intrusos
Análisis de vulnerabilidades
Control de acceso
Analítica de logs
Control de accesos privilegiados
Data Leak Prevention

2018-Cloud-Security-Report

5to FORO en Seguridad de la Información

Arquitectura de la Nube

Expectativa

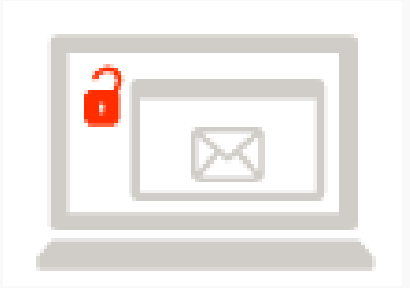
Realidad

5to FORO en Seguridad de la Información

¿Cuáles crees que son las mayores amenazas de seguridad en nubes públicas?

Perdida de la configuración

Acceso no Autorizado



Interfaces inseguras

Elevación de privilegios de cuentas de servicios o tráfico

5to FORO en Seguridad de la Información

2018-Cloud-Security-Report

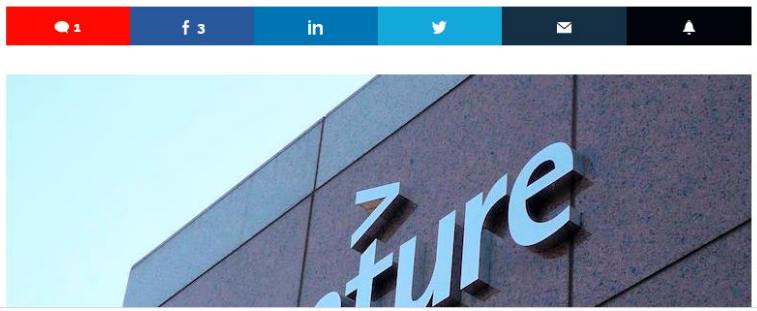
7% de todos los servidores Amazon S3 están expuestos, lo que explica el reciente aumento de las filtraciones de datos

Accenture

Accenture left a huge trove of highly sensitive data on exposed servers

The four exposed servers had no password, but contained the "keys to the kingdom."

By Zack Whittaker for Zero Day | October 10, 2017 -- 13:00 GMT (06:00 PDT) | Topic: Security



Technology and cloud giant Accenture has confirmed it inadvertently left a massive store of private data across four unsecured cloud servers, exposing highly sensitive passwords and secret decryption keys that could have inflicted considerable damage on the company and its customers.

The servers, hosted on Amazon's S3 storage service, contained hundreds of gigabytes of data for the company's enterprise cloud offering, which the company claims provides support to the majority of the Fortune 100.

The data could be downloaded without a password by anyone who knew the servers' web addresses.

Chris Vickery, director of cyber risk research at security firm UpGuard, found the data and privately told Accenture of the exposure in mid-September. The four servers were quietly secured the next day.

According to Vickery, the four servers contained data that amounted to the "keys to the kingdom," he told *ZDNet* on a call last week.

Here are 2017's biggest hacks, leaks, and data breaches — so far

Dozens of data breaches, millions of people affected.

Read More

7% de todos los servidores Amazon S3 están expuestos, lo que explica el reciente aumento de las filtraciones de datos

Time Warner Cable

Millions of Time Warner Cable Customer Records Exposed in Third-Party Data Leak

Dell Cameron
9/01/17 12:12pm • Filed to: DATA BREACH

67.8K 27 6

Roughly four million records containing the personal details of Time Warner Cable (TWC) customers were discovered stored on an Amazon server without a password late last month.

The files, more than 600GB in size, were discovered on August 24 by the Kromtech Security Center while its researchers were investigating an unrelated data breach at World Wrestling Entertainment. Two Amazon S3 buckets were eventually found and linked to BroadSoft, a global communications company that partners with service providers, including AT&T and TWC.

Not all of the TWC records contained information about unique customers. Some contained duplicative information, meaning the breach ultimately exposed less than four million customers. Due to the size of the cache, however, the researchers could not immediately say precisely how many were affected. The leaked data included usernames, emails addresses, MAC addresses, device serial numbers, and financial transaction information—though it does not appear that any Social Security numbers or credit card information was exposed.

Time Warner Cable was purchased by Charter Communications last year and is now called Spectrum, though the leaked records date back from this year to at least 2010.

Almacenamiento inadecuado

Uber

Uber Data Breach Exposed Personal Information of 20 Million Users

A data breach in 2016 exposed the names, phone numbers and email addresses of more than 20 million people who use Uber Technologies Inc.'s service in the U.S., authorities said on Thursday, as they chastised the ride-hailing company for not revealing the lapse earlier.

The Federal Trade Commission said Uber failed to disclose the leak last year as the agency investigated and sanctioned the company for a similar data breach that happened in 2014. Bloomberg News reported the breach in November.

"After misleading consumers about its privacy and security practices, Uber compounded its misconduct," said Maureen Ohlhausen, the acting FTC chairman. She announced an expansion of last year's settlement with the company and said the new agreement was "designed to ensure that Uber does not engage in similar misconduct in the future."

In the 2016 breach, intruders in a data-storage service run by Amazon.com Inc. obtained unencrypted consumer personal information relating to U.S. riders and drivers, including 25.6 million names and email addresses, 22.1 million names and mobile phone numbers, and 607,000 names and driver's license numbers, the FTC said in a complaint.

Qué hace falta?

Desarrollar una estrategia de seguridad integral

Seleccionar cuidadosamente las plataformas de seguridad que respaldan esa estrategia

Desarrollar el programa de seguridad utilizando las herramientas y los controles descritos

PREGUNTAS?

5to FORO
en Seguridad de la Información