CONGRESO DE
PREVENCIÓN DEL FRAUDE Y SEGURIDAD

Construyendo **experiencias** desde un **entorno seguro.**

FECHA 15 - 16 DE NOVIEMBRE /2018
HOTEL GRAND HYATT BOGOTÁ

Facundo Turconi

¿Nos conectamos?

¿De dónde venimos ?

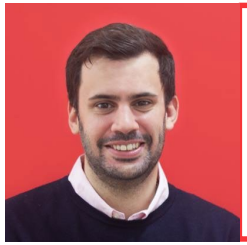
Facundo Turconi
(Fundador & CEO)

afluenta · Interbank · experian · BBVA

+15y en la industria financiera en Latam. +5y en online lending. Previamente, Gerente de Riesgos.

Juan I. Barreiro
(CFO & CM Arg)

afluenta · EY Building a better working world



+8y en online lending a lo largo de Latinoamérica.

Esteban Dávalos
(Lead Developer)

acceso crédito vehicular

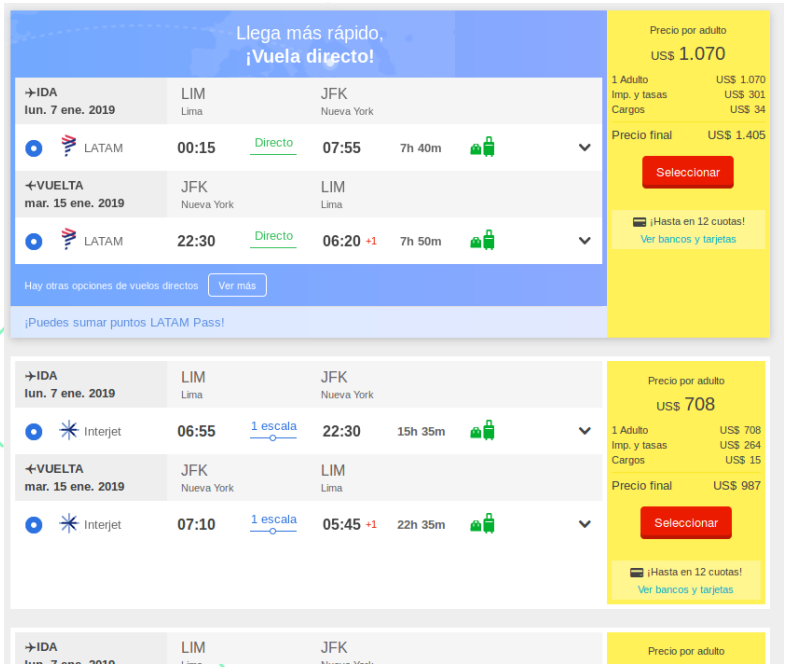
+8y desarrollando Software, amplio conocimiento en Infraestructura y Base de Datos.

John Rodriguez
(Lead Developer)

acceso crédito vehicular

+6y desarrollando Software, liderando el Back-End development.

¿Qué hacemos ?



pero para la industria financiera…

¿Qué hacemos ?

PaaS

Nuestra historia

¿Cómo una FinTech se integró a 14 Bancos?

El dilema inicial

¿API Solven

o

WS por cada Banco?

¿Por donde empezar ?

Integración de WS (mmm… Extranet?)

vamos de lo más fácil a lo más difícil…

A trabajar…

Vamos de a poco… servicio a servicio

desde los Workflows hasta los Cores…

¿Qué pasó ?

Teníamos algunos pendientes…

FESI - Ficha de Evaluación de Seguridad de Información (Sistemas, Servicios y Aplicaciones)

Sistema/Aplicación: Solven — Nivel de Cumplimiento: 68%

NOTA: Llenar los campos de color naranja y enviar las evidencias a Seguridad de Información BFP

Distribución	N°	Lineamiento de seguridad	Aplica al Proyecto?	Cumple?	Se tiene evidencia?	Está documentado?	Resultado
	41	La opción Reportes del Módulo de Seguridad considera un listado de usuarios que no ingresan al aplicativo por más de "x" días. X debe ser parametrizable.	Si	No			No cumple
	42	La opción Reportes del Módulo de Seguridad considera un reporte de auditoría de mantenimiento de la cuenta: quién creó/modificó/eliminó la cuenta, perfil que le fue asignado, fecha y hora, estación.	Si	No			No cumple
Base de Datos	43	El acceso a información personal y/o Dato sensible en la BD se concede y controla separando acciones como las de lectura, escritura y borrado.	Si	No			No cumple
	44	Las Bases de Datos de las aplicaciones que involucren información critica, valiosa o confidencial, permanecen encriptadas dentro del Banco o en los locales externos y su desencriptación se realiza sólo por las aplicaciones que trabajan con dicha información.	Si	No	No		No cumple
	45	La base de datos tiene activos los logs de auditoría de accesos y actividades de los usuarios.	Si	Si	Si		Cumple
	46	Las configuraciones de seguridad de la base de datos no considera los parámetros y/o configuraciones establecidas por default.	Si	Si	Si		Cumple
	47	Las cuentas instaladas por default han sido deshabilitas, bloqueadas y/o expiradas.	Si	Si	Si		Cumple
Web	49	Considera buenas prácticas de desarrollo seguro de aplicaciones basado en OWASP.	Si	Si	Si	No	Cumple
	50	El proyecto ha considerado contar con el servicio de monitoreo de phishing/páginas clonadas para el dominio de la pagina.	Si	No			No cumple
	51	Se cuenta con un sistema de reconocimiento para saber si el usuario que esta accediendo a una aplicación es humano o es una maquina (Se recomienda captchas de probada eficacia tomar como ejemplo	Si	Si	Si	No	Cumple

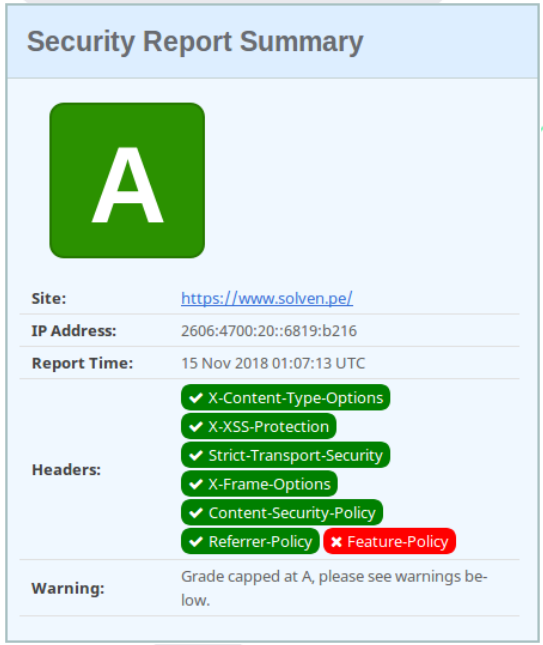
Y entonces…?

10 días después volvimos…

- 40% ¡check!
- Un plan (45 días: 90%).
- Una idea: ¡Hackear al Banco!

Mejor no…

Un test de seguridad es más razonable.



Conversemos nuevamente…

¿Nos conectamos?

Hablemos de Seguridad

Autenticación de las comunicaciones

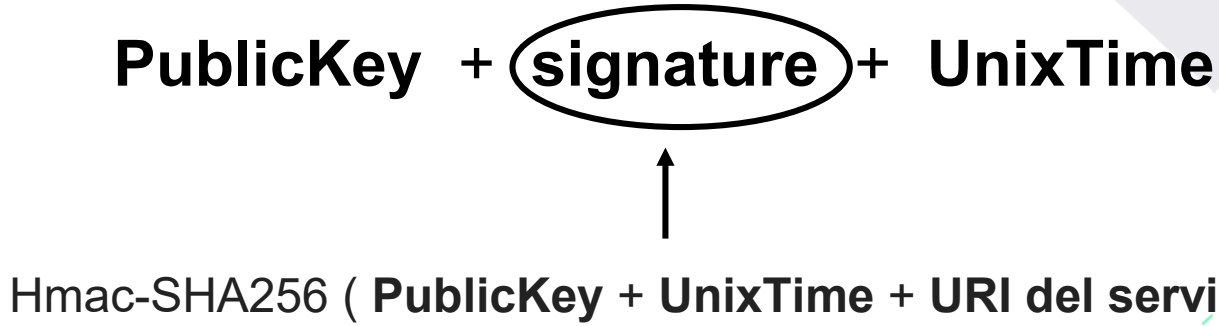
Entidades Financieras

Método más común:

ApiKey en cada request

Solven

Header de autenticación



Manejo de contingencias

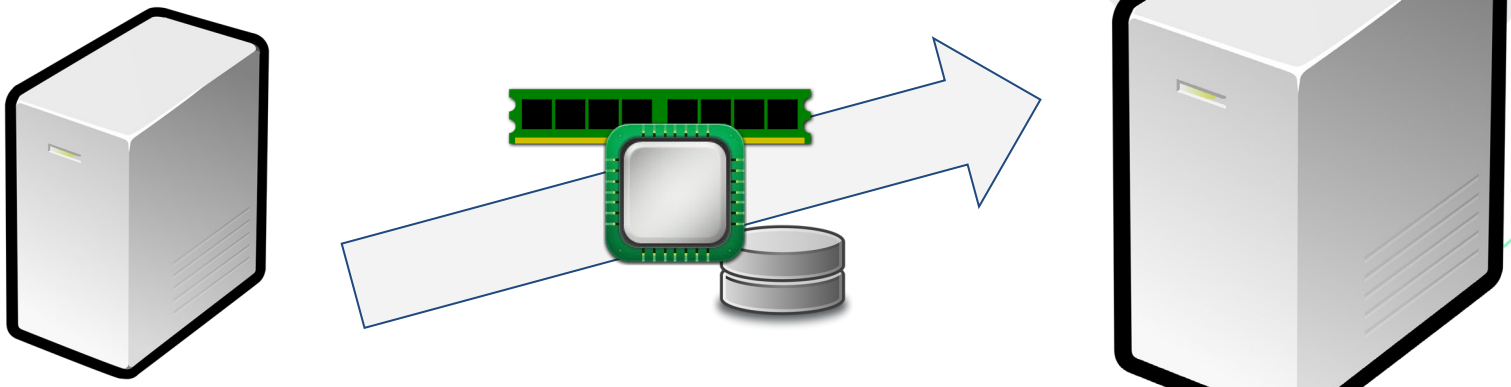
Los Web Services fallan

Solución:

Reintentos programados

Escalamiento y Alta Disponibilidad

Vertical

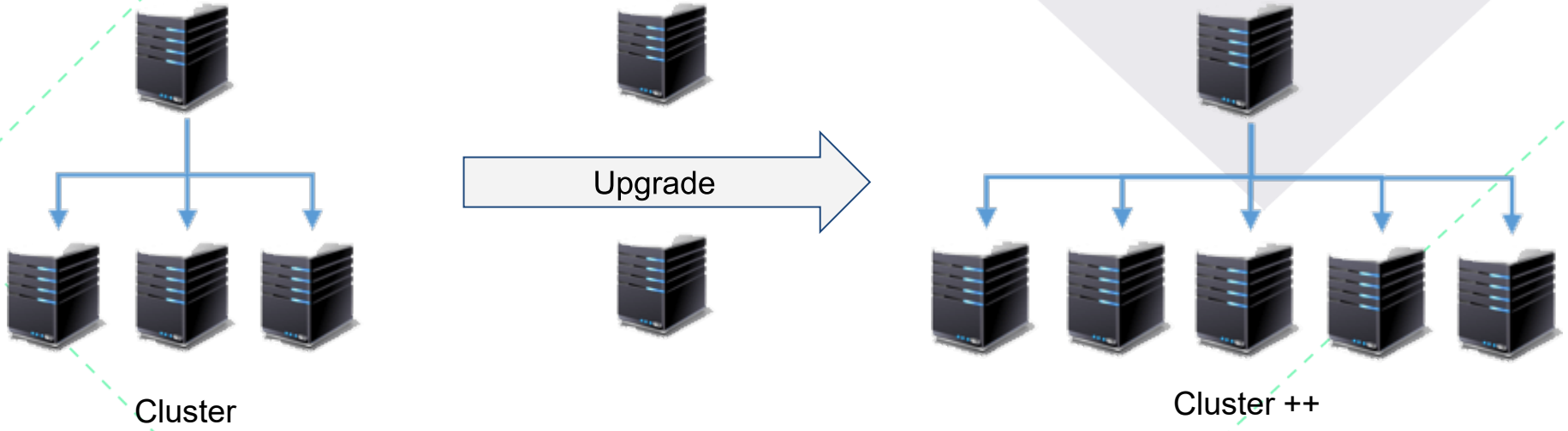


Servidor Standard

Recursos

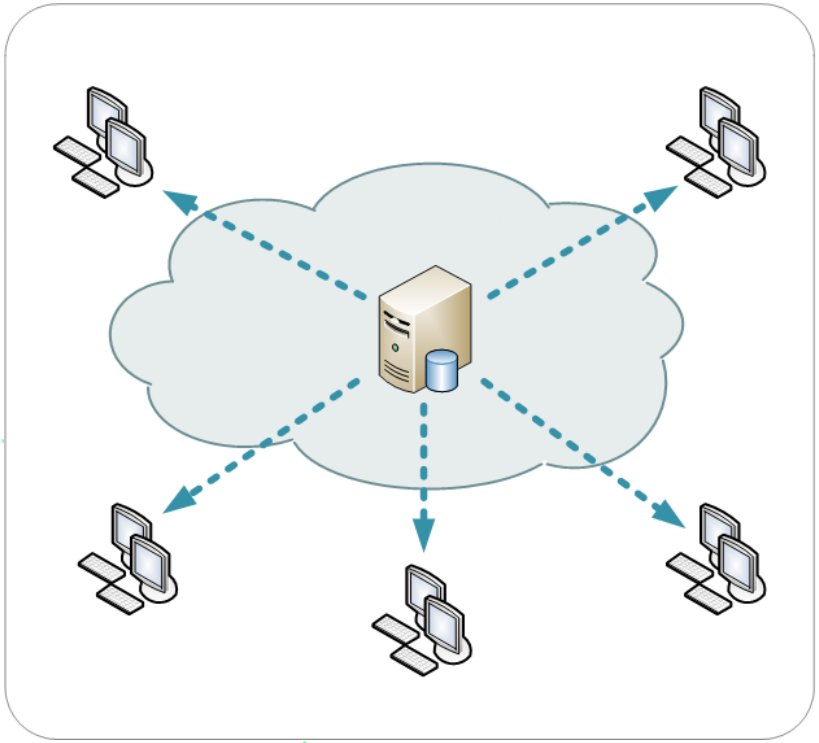
Super Servidor

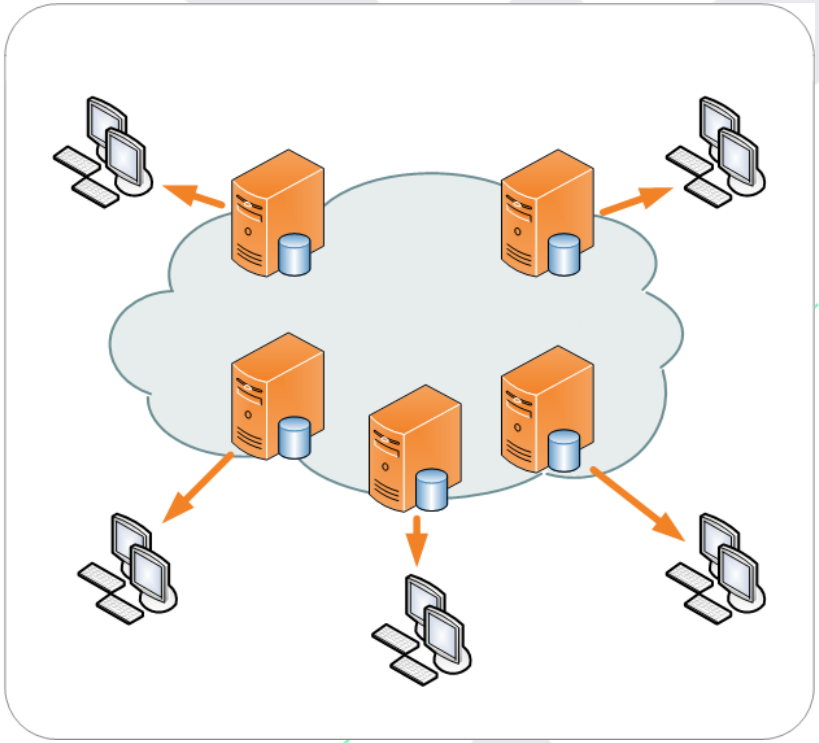
Horizontal



CDN

Mejoran la disponibilidad del servidor (uptime).





Protección de datos personales

Protección de Datos

PAISES DE AMERICA LATINA

- **PAISES CON LEYES GENERALES DE PROTECCION DE DATOS**

  Argentina – 2000
  Uruguay - 2008
  México – 2010
  Perú – 2011
  Costa Rica -2011
  Nicaragua – 2012
  Colombia – 2012
  República Dominicana-2013

- **PAISES CON PROYECTOS DE LEY SOBRE PROTECCION DE DATOS A ESTUDIO EN EL PARLAMENTO**

  Brasil
  Chile

Autenticación en la Extranet

Seguridad - Login

- Cambio periódico de contraseñas
- Máximo de sesiones activas simultáneas
- Bloqueo por intentos fallidos
- Log de actividad del usuario
- Autenticación de 2 a más factores
- Evitar reutilización de passwords

Buenas prácticas

Vulnerabilidades

- Ethical Hacking.
- Uso adecuado del método POST.
- Uso de Certificado Digital TLS v1.2.
- Protección contra ataques de denegación de servicio.
- Controlar errores emitidos por la aplicación.

Buenas Prácticas OWASP

Open Web Application Security Project

- Inyección de SQL.
- Autentificación rota.
- Exposición de data sensible.

Trabajemos juntos…

¿Qué se puede hacer para hacerlo más rápido?

- API flexible.
- Compromiso de los bancos para subirse a la ola digital.

Y ¿Cómo mejoramos la integración?

Siempre mediante el uso de APIs

Tips para Implementaciones sostenibles

- Log de comunicación de Web services
- Tabla de traducciones
- Usar SFTP
- Guardar variables de conexión en un lugar externo y seguro

¿Qué aprendimos?

- Creen que no podrían conectarse con una FinTech.
- Los Bancos suelen tener otras prioridades o no tienen dedicación completa para hacerlo.
- Más pequeños, más flexibles y rápidos, más predispuestos a integrar un nuevo canal.

¿Nos conectamos?

fturconi@solven.pe

+51 998 931099

www.solven.la