



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)



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

## Juan I. Barreiro

(CFO & CM Arg)



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

## Esteban Dávalos

(Lead Developer)



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

## John Rodriguez

(Lead Developer)



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

# ¿Qué hacemos ?

| Llega más rápido, ¡Vuela directo!                             |                   |                   |          |        |  | Precio por adulto<br>US\$ 1.070 |                                    |                                   |
|---|-------------------|-------------------|----------|--------|--|---------------------------------|------------------------------------|-----------------------------------|
| <b>→IDA</b><br>Lun. 7 ene. 2019                               | LIM<br>Lima       | JFK<br>Nueva York |          |        |  |                                 | 1 Adulto<br>Imp. y tasas<br>Cargos | US\$ 1.070<br>US\$ 301<br>US\$ 34 |
| LATAM   | 00:15             | Directo           | 07:55    | 7h 40m |  | Precio final                    | US\$ 1.405                         |                                   |
| <b>Seleccionar</b>  |                   |                   |          |        |  |                                 |                                    |                                   |
| ¡Hasta en 12 cuotas!<br><a href="#">Ver bancos y tarjetas</a> |                   |                   |          |        |  |                                 |                                    |                                   |
| <b>←VUELTA</b><br>mar. 15 ene. 2019                           | JFK<br>Nueva York | LIM<br>Lima       |          |        |  |                                 |                                    |                                   |
| LATAM   | 22:30             | Directo           | 06:20 +1 | 7h 50m |  |                                 |                                    |                                   |
| <b>Seleccionar</b>  |                   |                   |          |        |  |                                 |                                    |                                   |
| ¡Hasta en 12 cuotas!<br><a href="#">Ver bancos y tarjetas</a> |                   |                   |          |        |  |                                 |                                    |                                   |

| Llega más rápido, ¡Vuela directo!                             |                   |                   |          |         |  | Precio por adulto<br>US\$ 708 |                                    |                                 |
|---|-------------------|-------------------|----------|---------|--|-------------------------------|------------------------------------|---------------------------------|
| <b>→IDA</b><br>Lun. 7 ene. 2019                               | LIM<br>Lima       | JFK<br>Nueva York |          |         |  |                               | 1 Adulto<br>Imp. y tasas<br>Cargos | US\$ 708<br>US\$ 264<br>US\$ 15 |
| Interjet  | 06:55             | 1 escala          | 22:30    | 15h 35m |  | Precio final                  | US\$ 987                           |                                 |
| <b>Seleccionar</b>  |                   |                   |          |         |  |                               |                                    |                                 |
| ¡Hasta en 12 cuotas!<br><a href="#">Ver bancos y tarjetas</a> |                   |                   |          |         |  |                               |                                    |                                 |
| <b>←VUELTA</b><br>mar. 15 ene. 2019                           | JFK<br>Nueva York | LIM<br>Lima       |          |         |  |                               |                                    |                                 |
| Interjet  | 07:10             | 1 escala          | 05:45 +1 | 22h 35m |  |                               |                                    |                                 |
| <b>Seleccionar</b>  |                   |                   |          |         |  |                               |                                    |                                 |
| ¡Hasta en 12 cuotas!<br><a href="#">Ver bancos y tarjetas</a> |                   |                   |          |         |  |                               |                                    |                                 |

**= SIMILAR**  
¡Esta es la oferta más similar a lo que solicitaste!

**S/ 3 136**

**S/ 214.30 / 24 meses**

TEA 49.71 %    TCEA 67.75 %

**¡La quiero!**

Ver cronograma

**+ DINERO**  
¿Necesitas más plazo para tu crédito?  
Tenemos esta otra opción para ti.

**S/ 4 100**

**S/ 204.84 / 48 meses**

TEA 49.71 %    TCEA 66.66 %

**¡La quiero!**

Ver cronograma

pero para la industria financiera...

# ¿Qué hacemos ?

solven

Compartamos<sup>®</sup>  
Financiera

S/ 7 200 (18 meses)



Dame unos segundos mientras proceso la información y realizo algunos cálculos

✓ Análisis completo

Revisando bases de datos externas

Revisando tus antecedentes financieros

Calculando tus niveles de endeudamiento

Realizando una estimación de tu perfil



Una empresa de  
**GENTERA**

Operado por Solven

[Términos y condiciones](#)

[Preguntas frecuentes](#)



# 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?)



The screenshot displays the so/ven web application interface. On the left is a sidebar menu with the following items:

- Funcionarios
- Solicitudes a verificar (highlighted)
- Creación de cliente/crédito
- Créditos a desembolsar
- Créditos desembolsados
- Reportes

The main content area is titled "SOLICITUDES A VERIFICAR" and contains a table with the following columns:

| #                                    | Fecha Generación | Crédito | Producto | Tipo Doc. | Número Doc. | Nombres |
|--------------------------------------|------------------|---------|----------|-----------|-------------|---------|
| Ningún dato disponible en esta tabla |                  |         |          |           |             |         |

vamos de lo más fácil a lo más difícil...

A trabajar...

Vamos de a poco... servicio a servicio



The screenshot displays the so/ven web application interface. On the left is a sidebar menu with the following items:

- FUNCIONARIOS
- Solicitudes a verificar (selected)
- Creación de cliente/crédito
- Créditos a desembolsar
- Créditos desembolsados
- Reportes

The main content area is titled "SOLICITUDES A VERIFICAR" and contains a table with the following columns:

| #                                    | Fecha Generación | Crédito | Producto | Tipo Doc. | Número Doc. | Nombres |
|--------------------------------------|------------------|---------|----------|-----------|-------------|---------|
| Ningún dato disponible en esta tabla |                  |         |          |           |             |         |

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: <b>Solven</b>   |    |  |                     | Nivel de Cumplimiento: <b>68%</b> |                     |                   |           |
| NOTA: Llenar los campos de color naranja y enviar las evidencias a Seguridad de Información BFP |    |  |                     |                                   |                     |                   |           |
| Distribución  | Nº | 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 crítica, 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 deshabilitadas, 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 página.  | SI                  | No                                |                     |                   | No cumple |
|   | 51 | Se cuenta con un sistema de reconocimiento para saber si el usuario que está accediendo a una aplicación es humano o es una máquina (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.

**Security Report Summary**



**Site:** <https://bancaportinternet.interbank.pe/>

**IP Address:** 200.48.23.30

**Report Time:** 15 Nov 2018 01:06:57 UTC

**Headers:**

- ✗ Strict-Transport-Security
- ✗ Content-Security-Policy
- ✗ X-Frame-Options
- ✗ X-XSS-Protection
- ✗ X-Content-Type-Options
- ✗ Referrer-Policy
- ✗ Feature-Policy

**Security Report Summary**



**Site:** <https://kueski.com/>

**IP Address:** 52.5.104.43

**Report Time:** 15 Nov 2018 01:11:45 UTC

**Headers:**

- ✓ X-XSS-Protection
- ✓ X-Content-Type-Options
- ✓ X-Frame-Options
- ✗ Strict-Transport-Security
- ✗ Content-Security-Policy
- ✗ Referrer-Policy
- ✗ Feature-Policy

**Security Report Summary**



**Site:** <https://www.solven.pe/>

**IP Address:** 2606:4700:20::6819:b216

**Report Time:** 15 Nov 2018 01:07:13 UTC

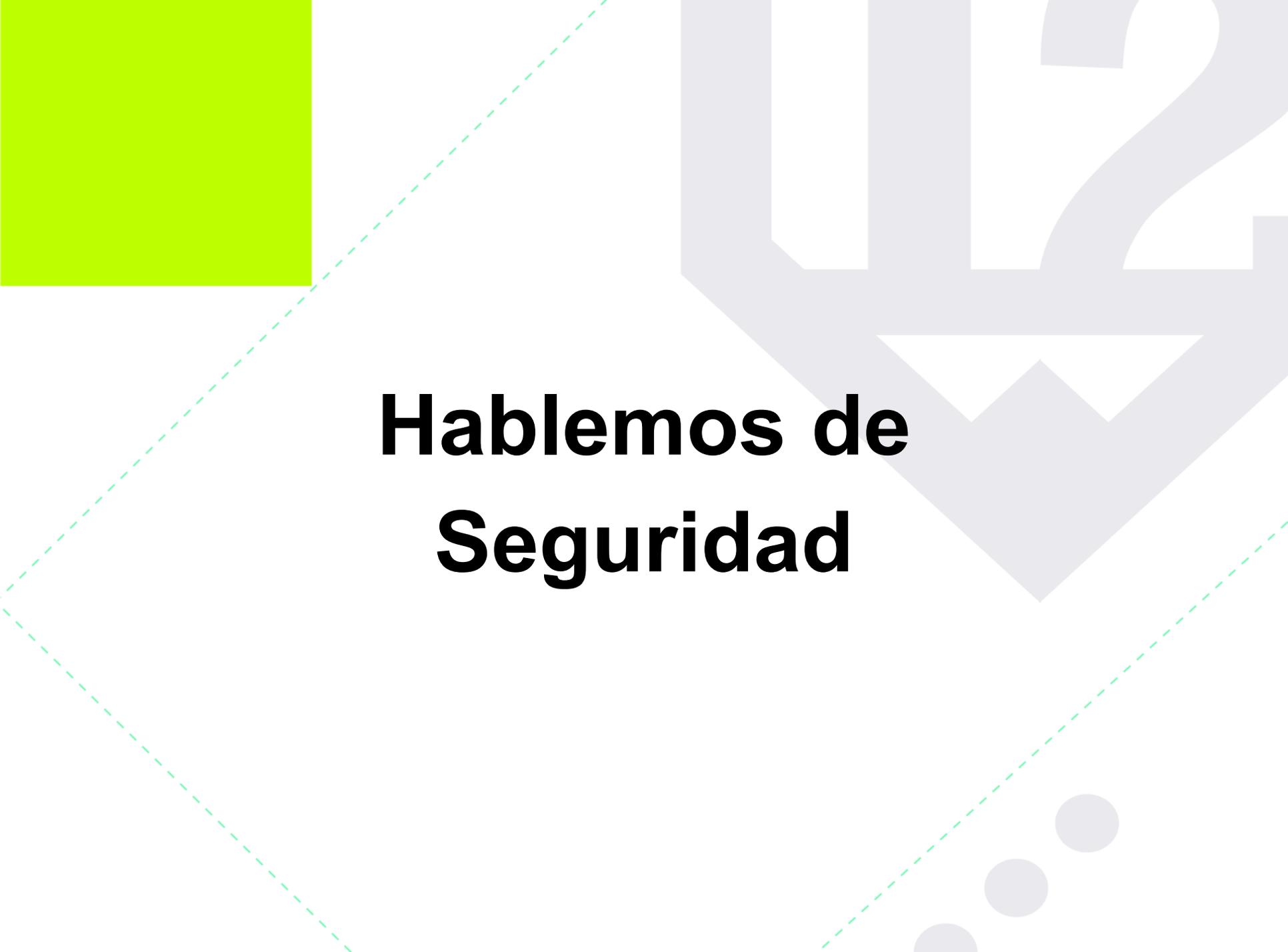
**Headers:**

- ✓ X-Content-Type-Options
- ✓ X-XSS-Protection
- ✓ Strict-Transport-Security
- ✓ X-Frame-Options
- ✓ Content-Security-Policy
- ✓ Referrer-Policy
- ✗ Feature-Policy

**Warning:** Grade capped at A, please see warnings below.

Conversemos nuevamente...  
¿Nos conectamos?





# **Hablemos de Seguridad**



# **Autenticación de las comunicaciones**

**Entidades Financieras**

Método más común:

**ApiKey en cada request**

**Solven**

# Header de autenticación

**PublicKey + signature + UnixTime**



Hmac-SHA256 ( **PublicKey + UnixTime + URI del servicio** )

# Manejo de contingencias

Los Web Services fallan

**Solución:**

**Reintentos programados**

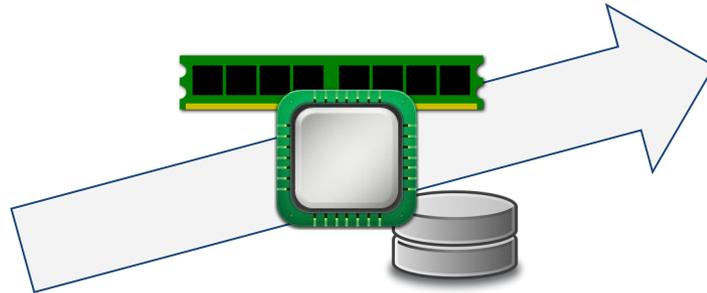


# **Escalamiento y Alta Disponibilidad**

# Vertical



Servidor Standard



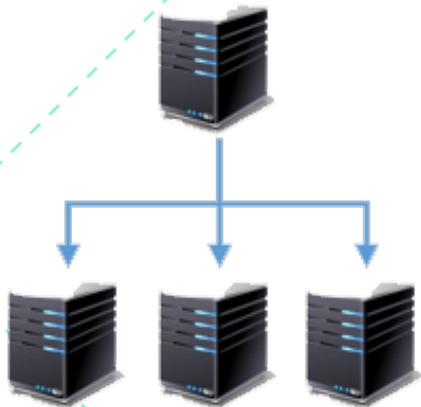
Recursos



Super Servidor

# Horizontal

so/ven



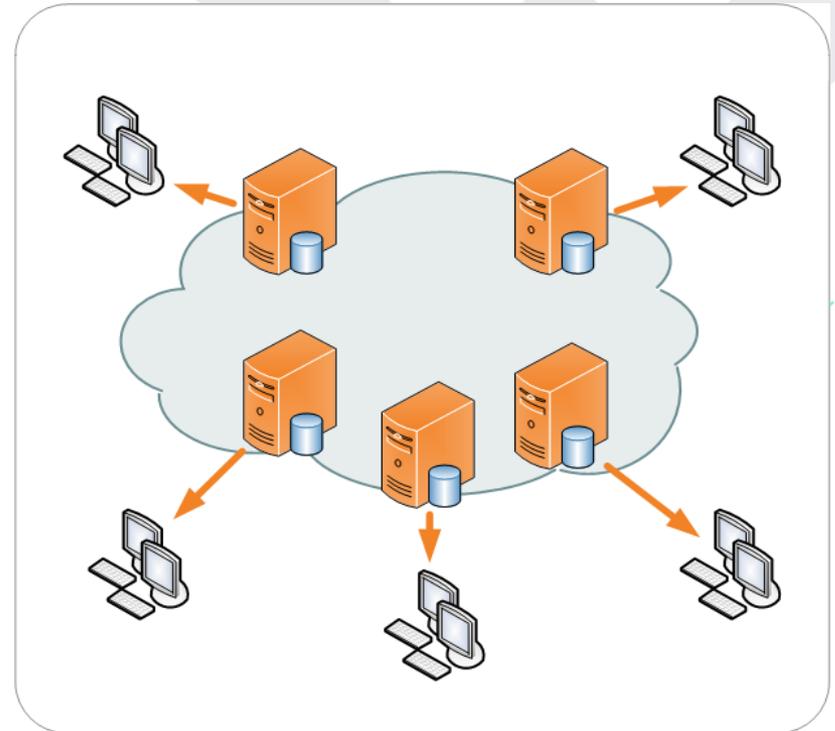
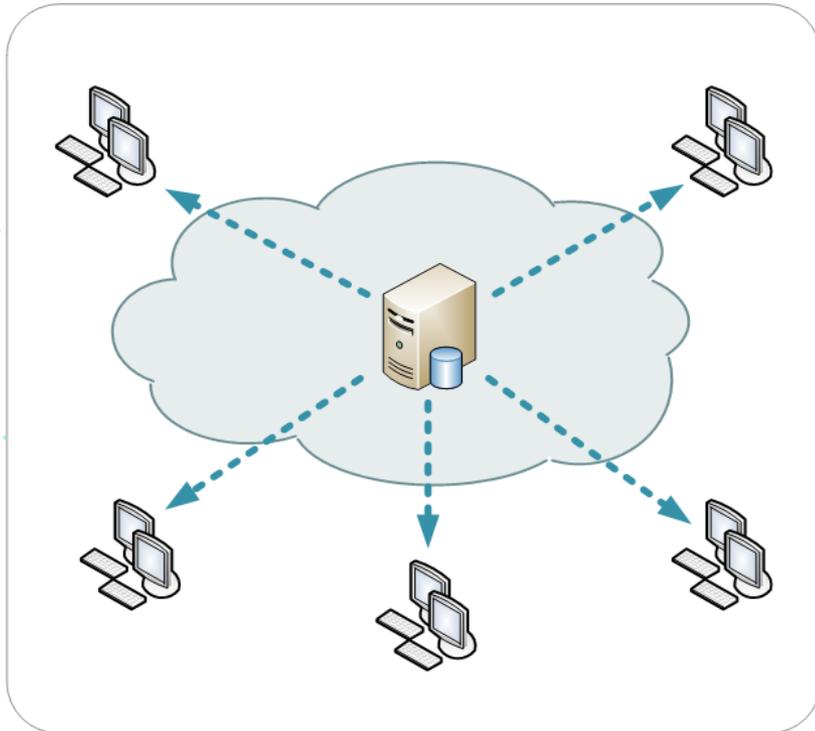
Cluster



Cluster ++

# 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

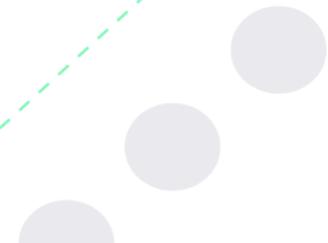
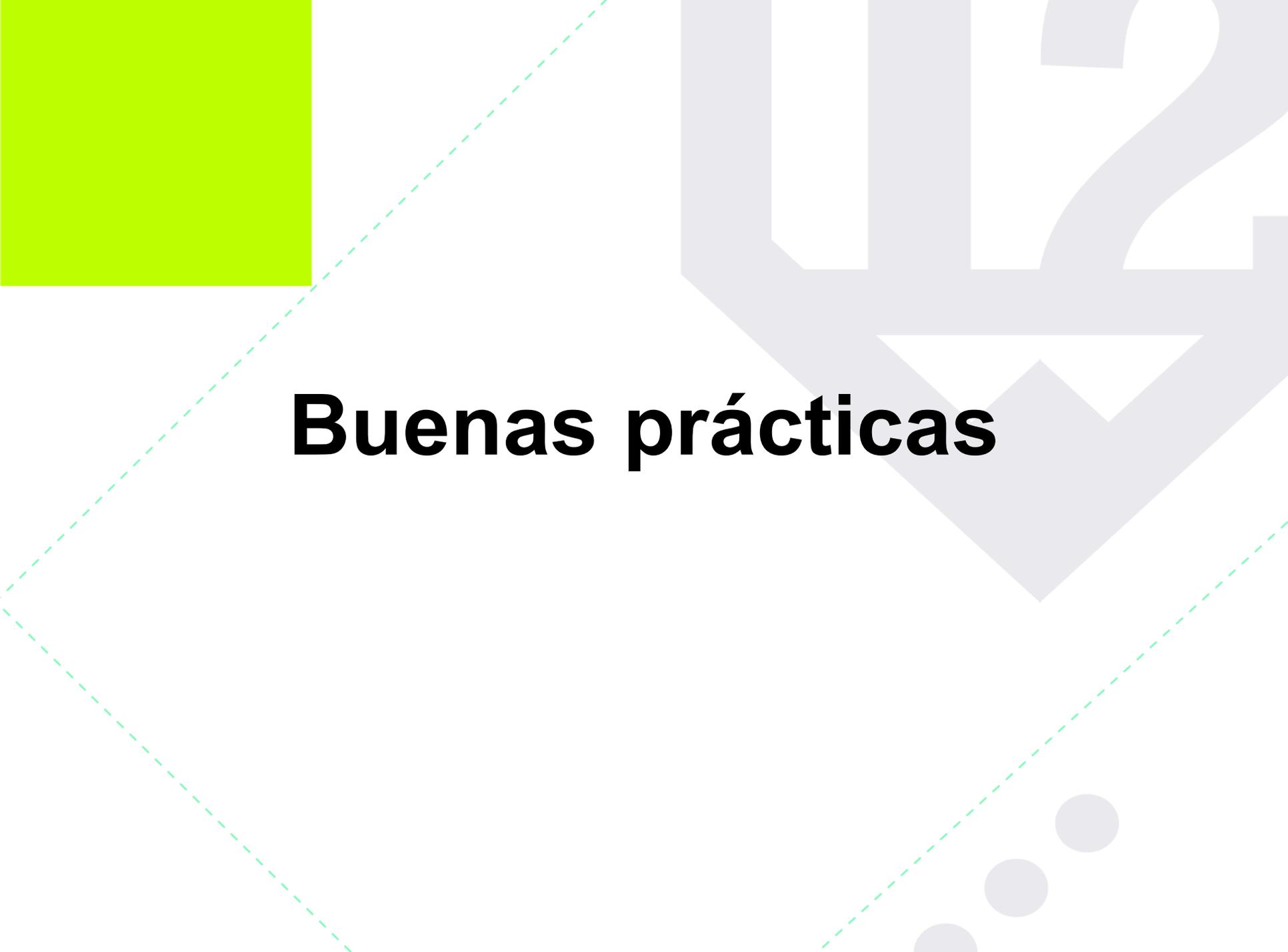




# **Autenticación en la Extranet**

## 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**

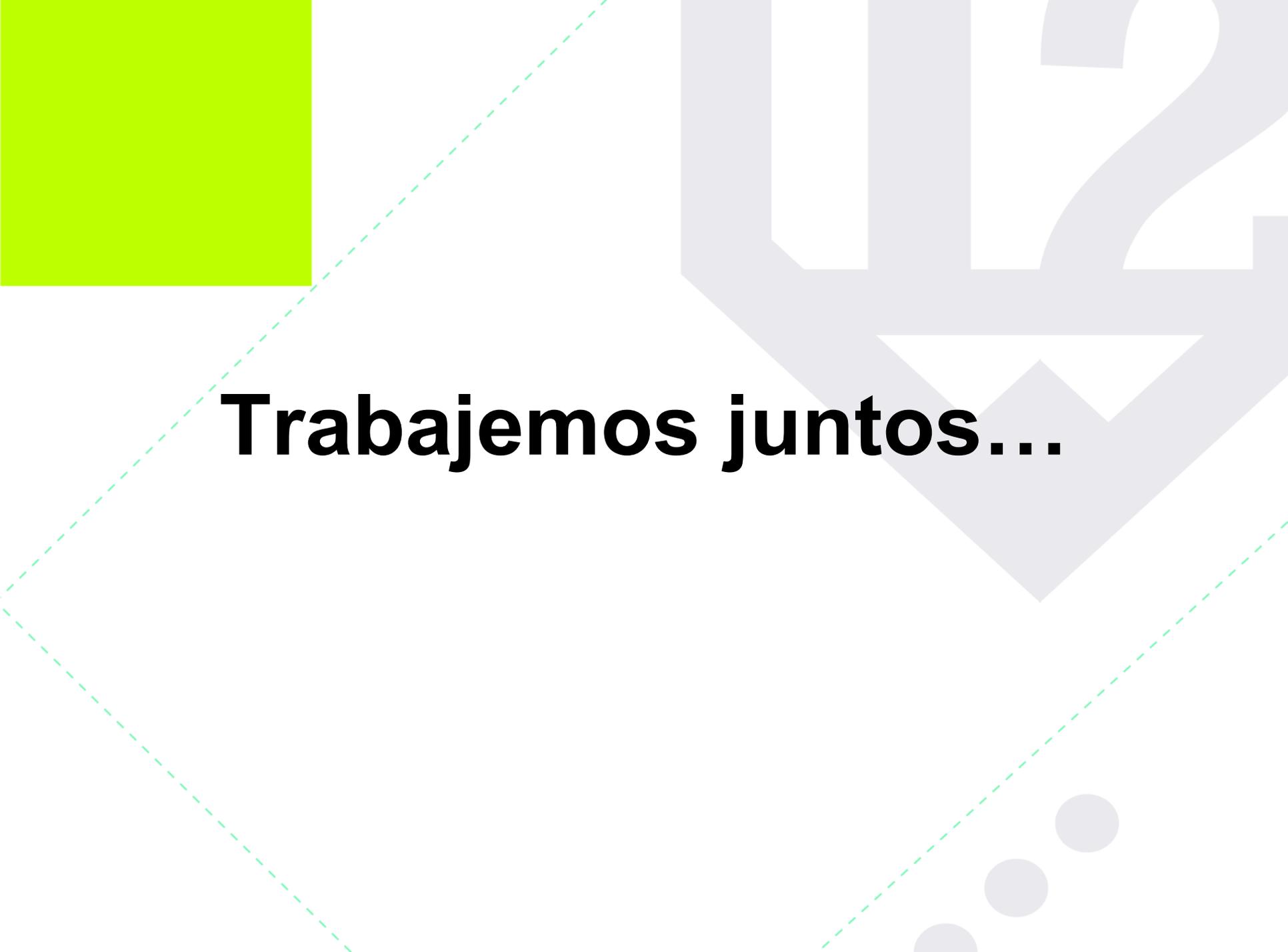
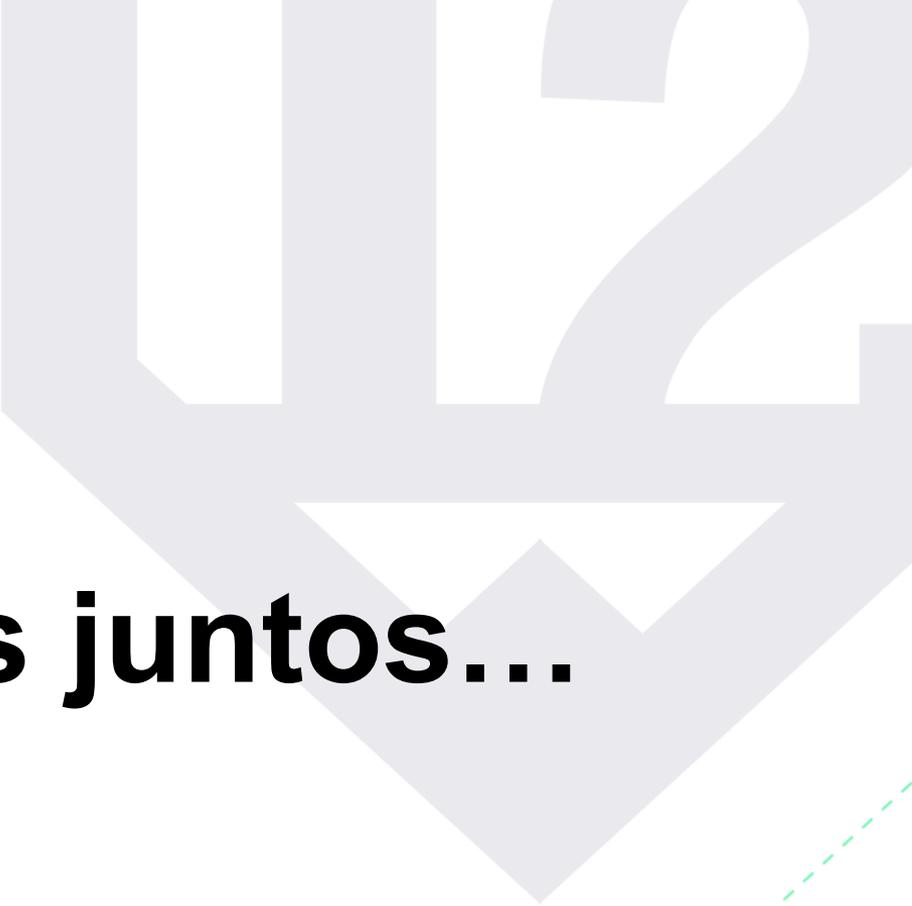
# Vulnerabilidades

- 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.
- Autenticación 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](mailto:fturconi@solven.pe)

+51 998 931099

[www.solven.la](http://www.solven.la)

