

# HP Fortify

¿Confías en la seguridad de tu software?



Victor Rojo

Solutions Architect – HP ESP

# Victor Rojo

- Programador experimentado y pragmático que ha sido gerente y director de desarrollo de software y tecnología
- 12 años de experiencia en el “campo de batalla” en empresas de Telecomunicaciones, Pensiones, Manufactura y Consultoría
- Ingeniero en Electrónica con Especialidad en Sistemas Digitales en la Universidad Autónoma Metropolitana – Azcapotzalco
- Escribió su primer programa para Atari en 1988



# Agenda

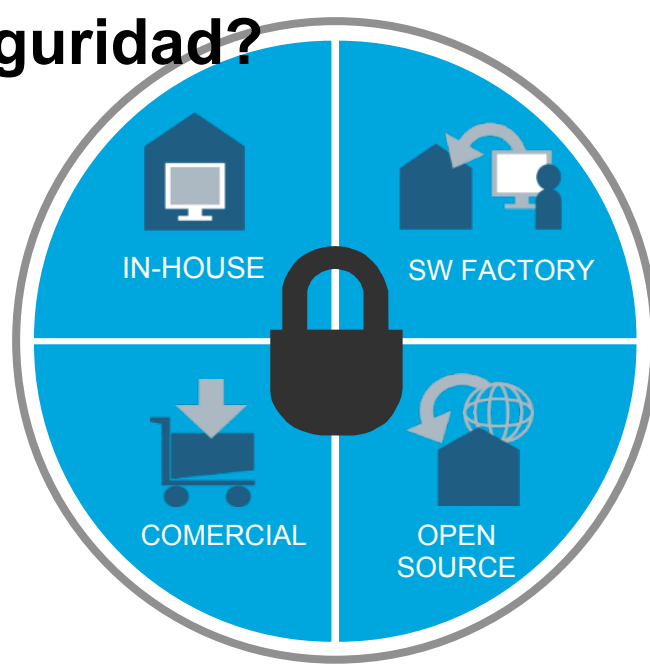
- ¿Donde hay aplicaciones?
- ¿Confiabilidad o seguridad?
- El reto de la seguridad en el software
- ¿Qué es la seguridad aplicativa?
- Software Security Assurance (SSA) Framework
- Portafolio de Soluciones HP Fortify
- Posicionamiento en la industria
- Mitos sobre las soluciones HP Fortify
- Resumen



# ¿Dónde hay aplicaciones?



# ¿Confiabilidad o seguridad?



**Un software *confiable* hace lo que se supone que debe hacer...**

**Una software *seguro* hace lo que se supone que debe hacer...**

# ¿Confiabilidad o seguridad?



# El reto en la seguridad en el software



Beneficios

Seguridad Aplicativa

Situación Actual



**Activos Digitales**  
Documentos, Contratos  
Finanzas, Clientes  
Pacientes, Planes/  
Roadmaps  
Patentes, Transacciones



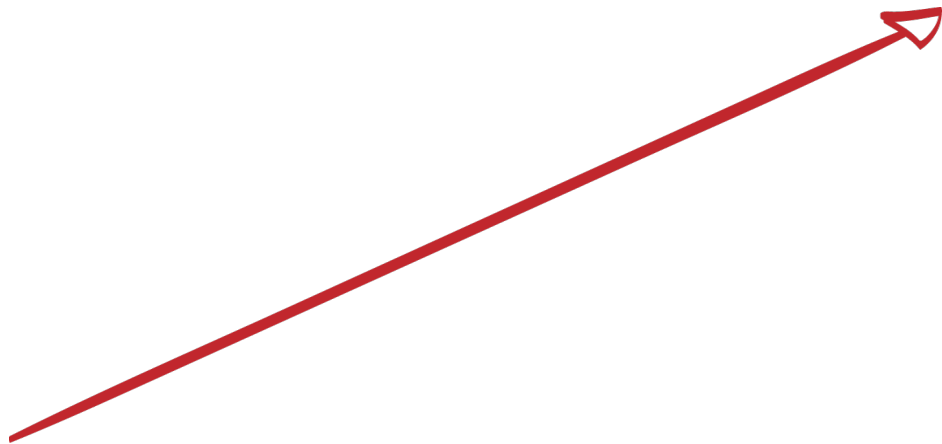
Beneficios

Seguridad Aplicativa

Situación Actual



**Activos Digitales**  
Documentos, Contratos  
Finanzas, Clientes  
Pacientes, Planes/  
Roadmaps  
Patentes, Transacciones



**Amenazas**  
USD\$280B



© Copyright 2012 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.



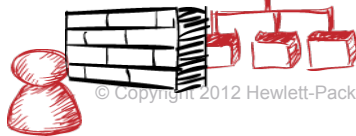
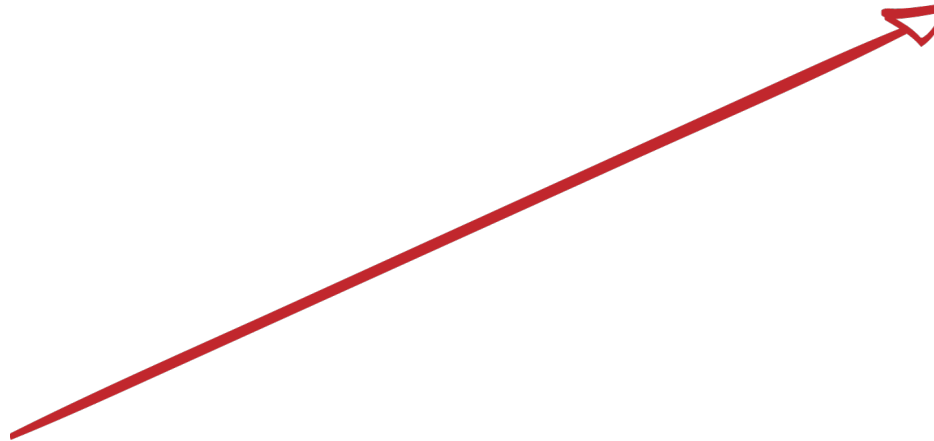
Beneficios

Seguridad Aplicativa

Situación Actual



**Activos Digitales**  
Documentos, Contratos  
Finanzas, Clientes  
Pacientes, Planes/  
Roadmaps  
Patentes, Transacciones



**Amenazas**  
USD\$280B

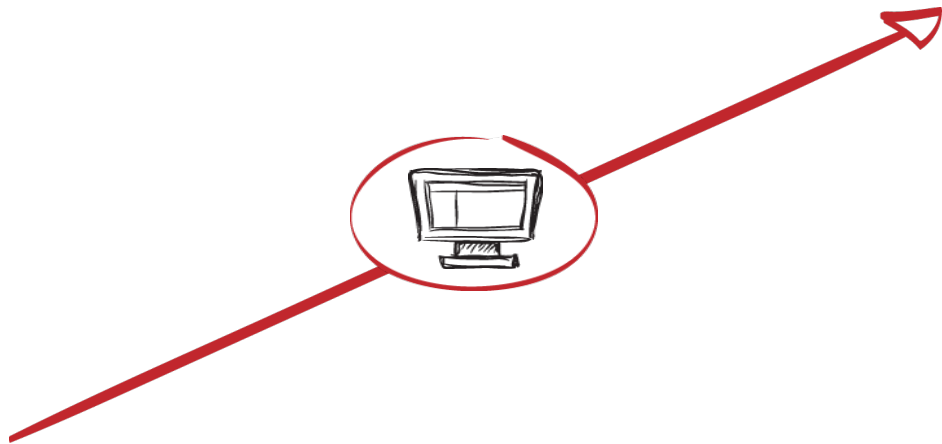
© Copyright 2012 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.



Beneficios

Seguridad Aplicativa

Situación Actual



**Activos Digitales**  
Documentos, Contratos  
Finanzas, Clientes  
Pacientes, Planes/  
Roadmaps  
Patentes, Transacciones

**Amenazas**  
USD\$280B



Beneficios

Seguridad Aplicativa

Situación Actual

Dev ≠  
Comprometido



**Activos Digitales**  
Documentos, Contratos  
Finanzas, Clientes  
Pacientes, Planes/  
Roadmaps  
Patentes, Transacciones



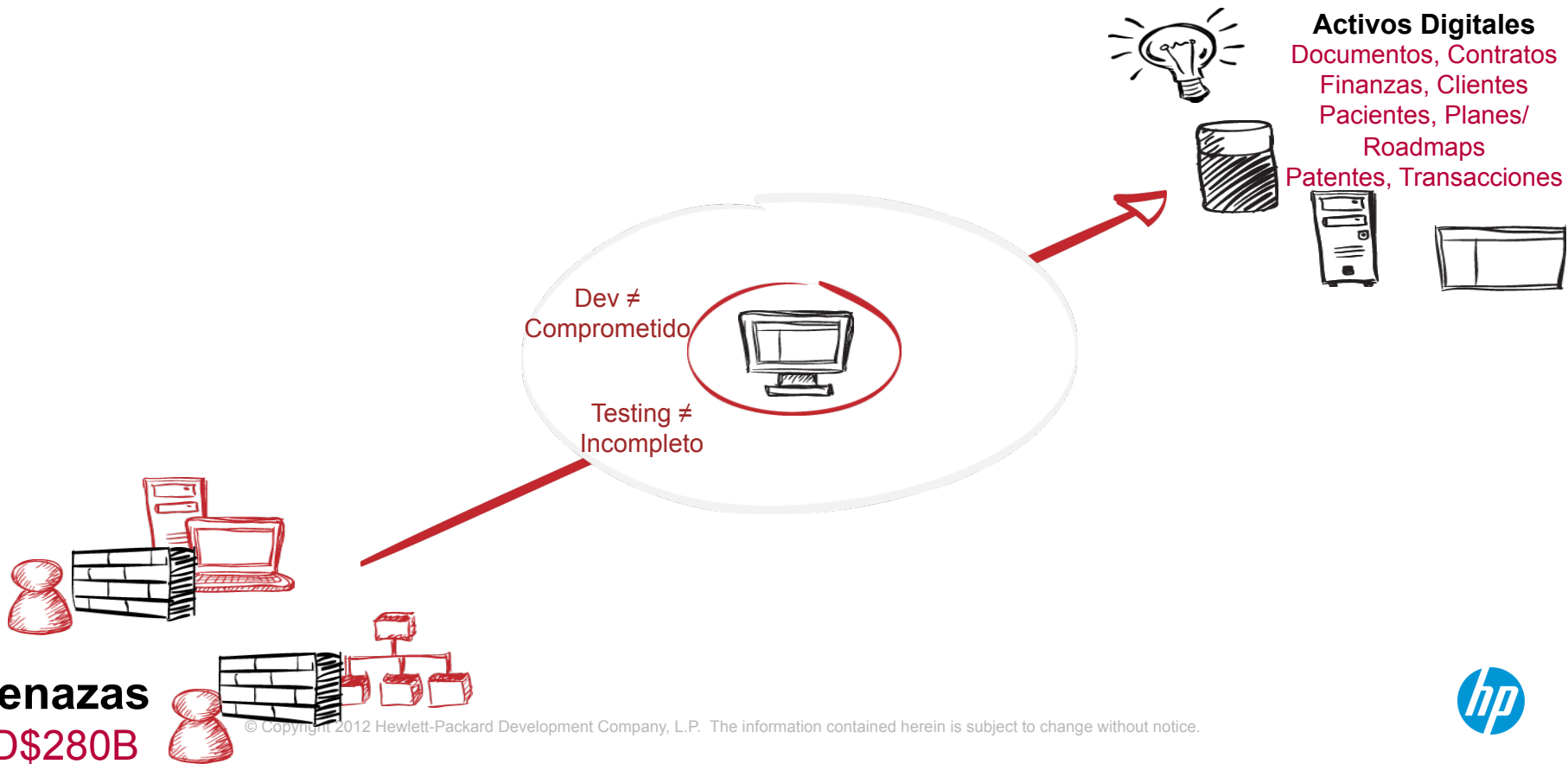
**Amenazas**  
USD\$280B



Beneficios

Seguridad Aplicativa

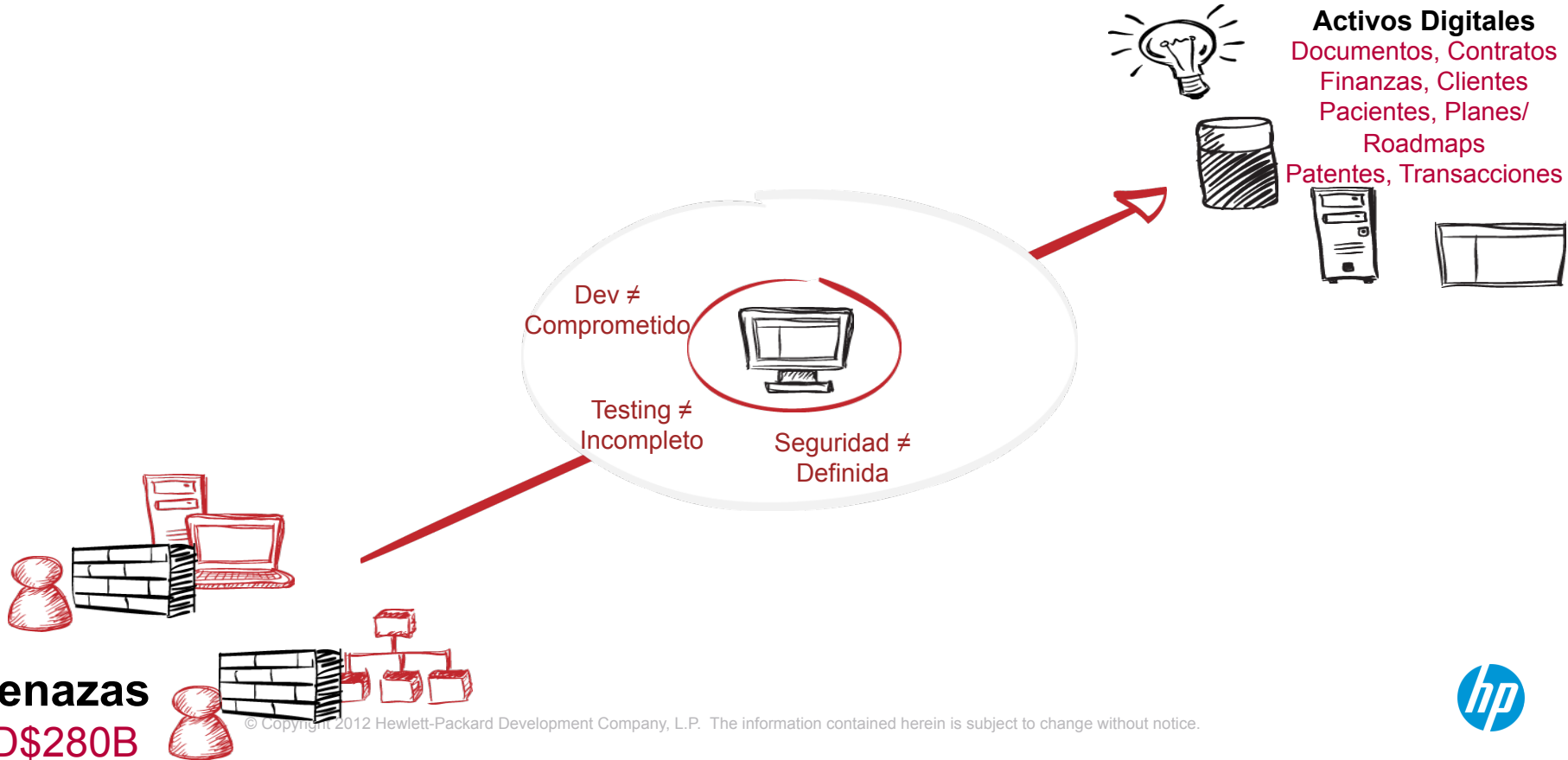
Situación Actual



## Beneficios

## Seguridad Aplicativa

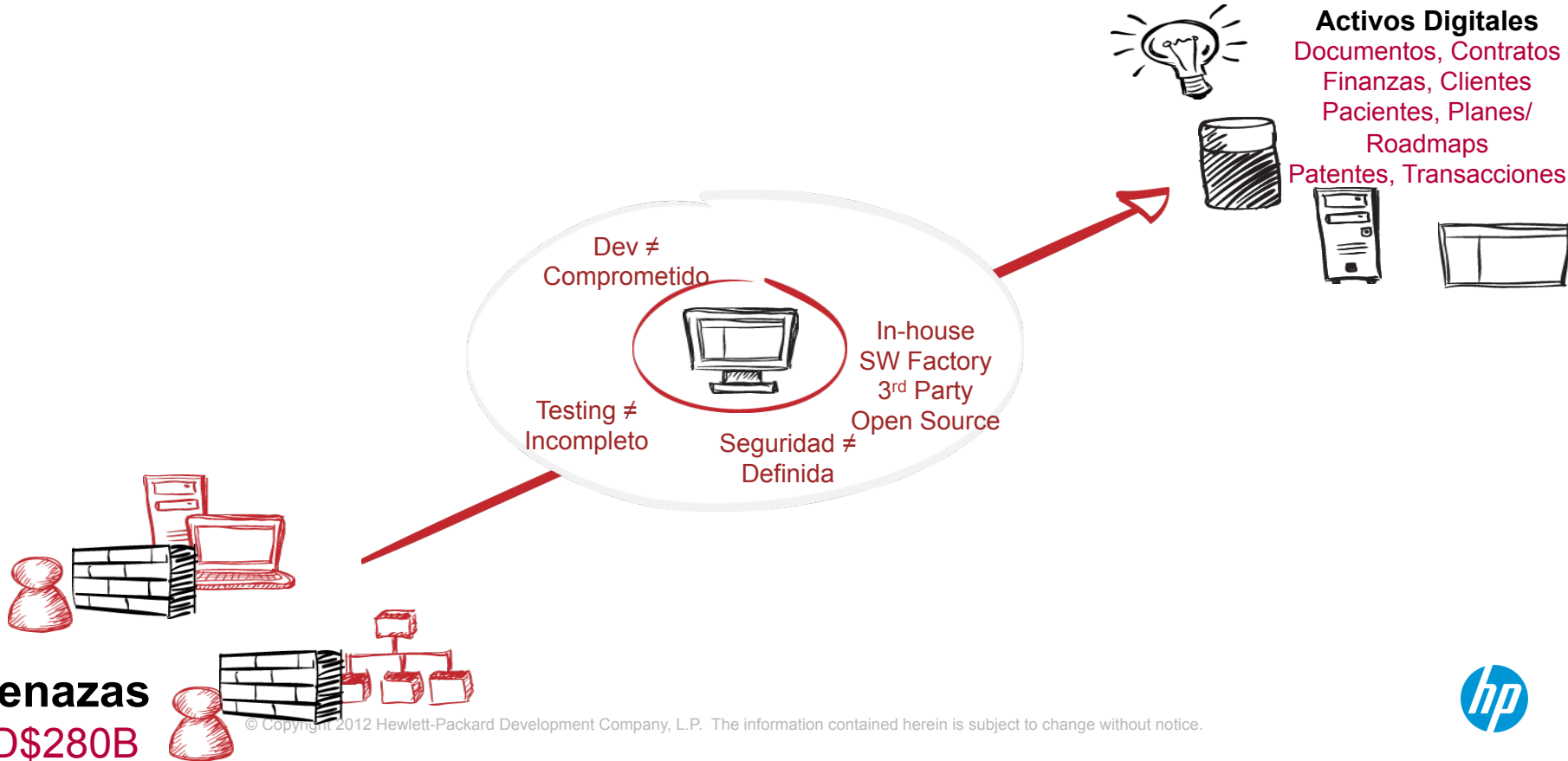
## Situación Actual



# Beneficios

# Seguridad Aplicativa

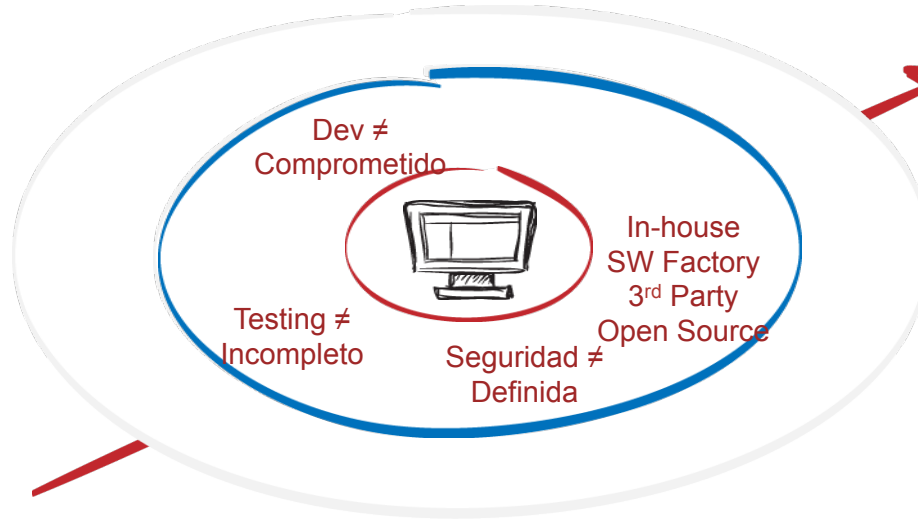
# Situación Actual



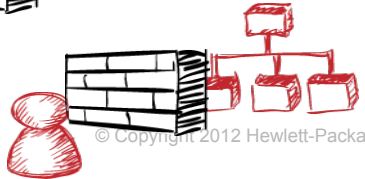
# Beneficios

# Seguridad Aplicativa

# Situación Actual



**Activos Digitales**  
Documentos, Contratos  
Finanzas, Clientes  
Pacientes, Planes/  
Roadmaps  
Patentes, Transacciones



**Amenazas**  
USD\$280B

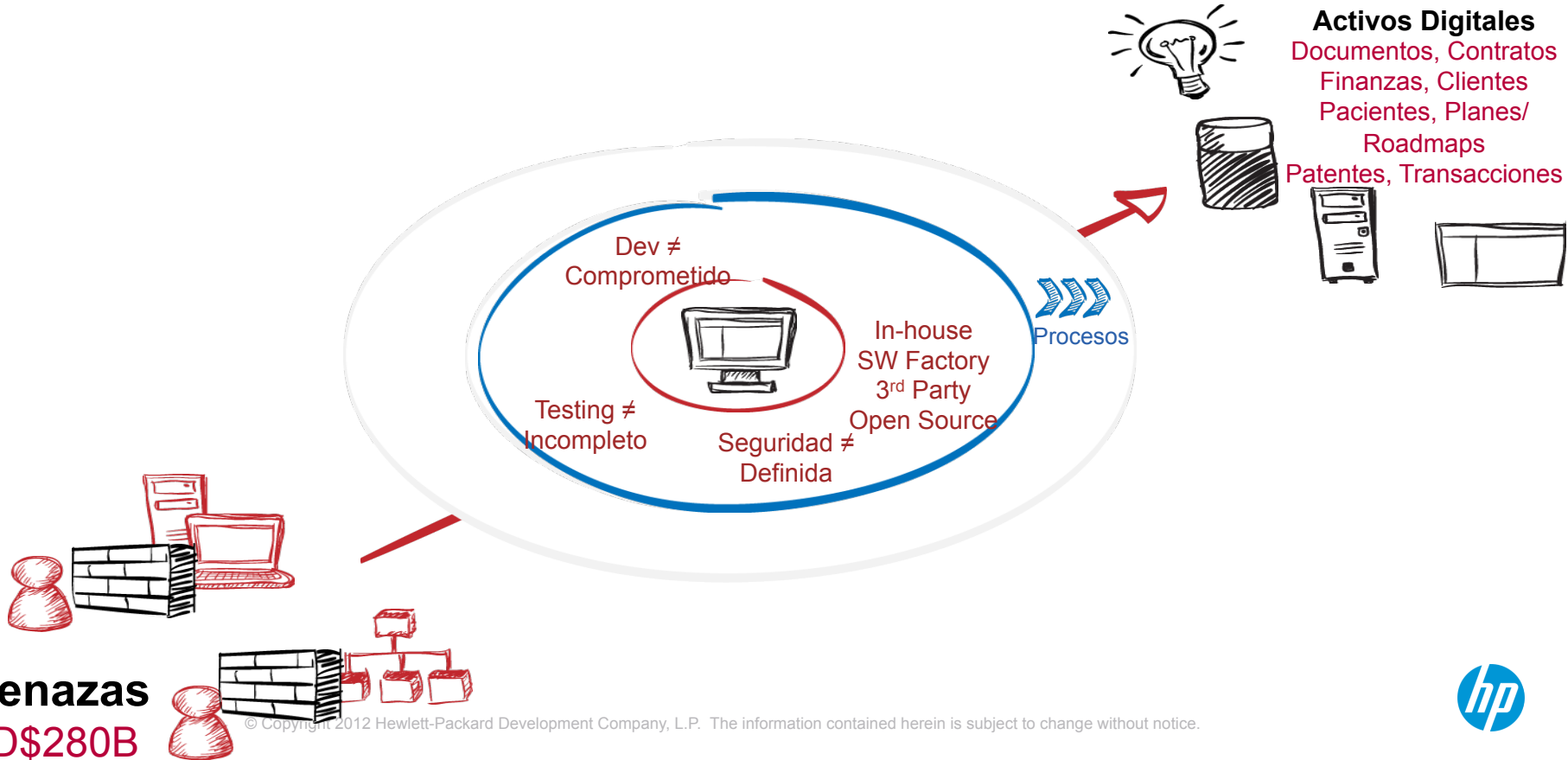




Beneficios

Seguridad Aplicativa

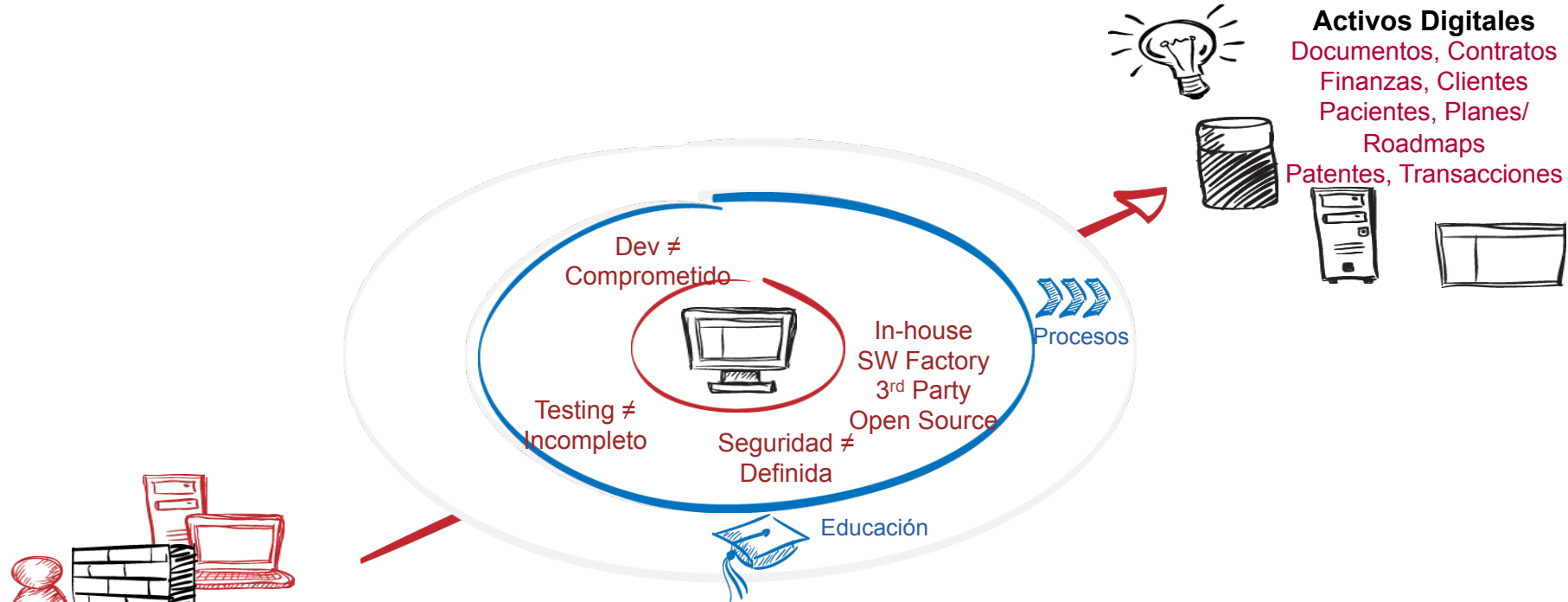
Situación Actual



Beneficios

Seguridad Aplicativa

Situación Actual



**Amenazas**

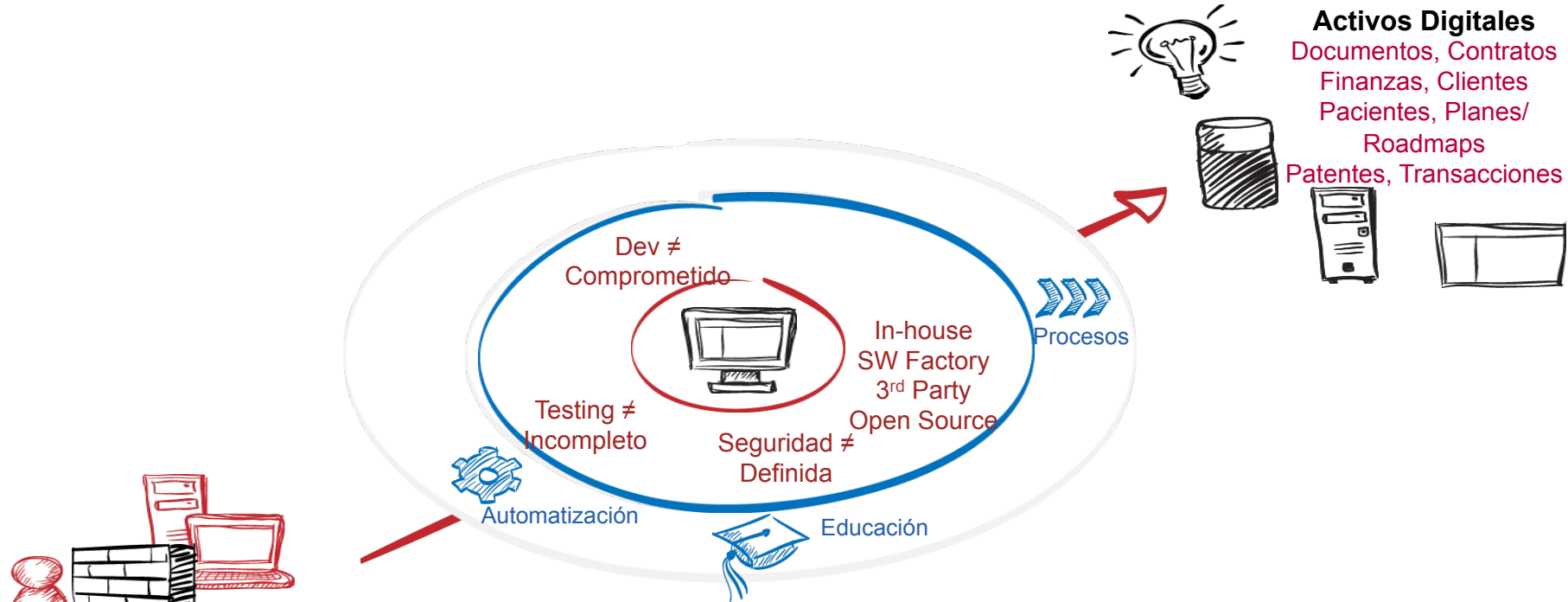
USD\$280B



# Beneficios

# Seguridad Aplicativa

# Situación Actual



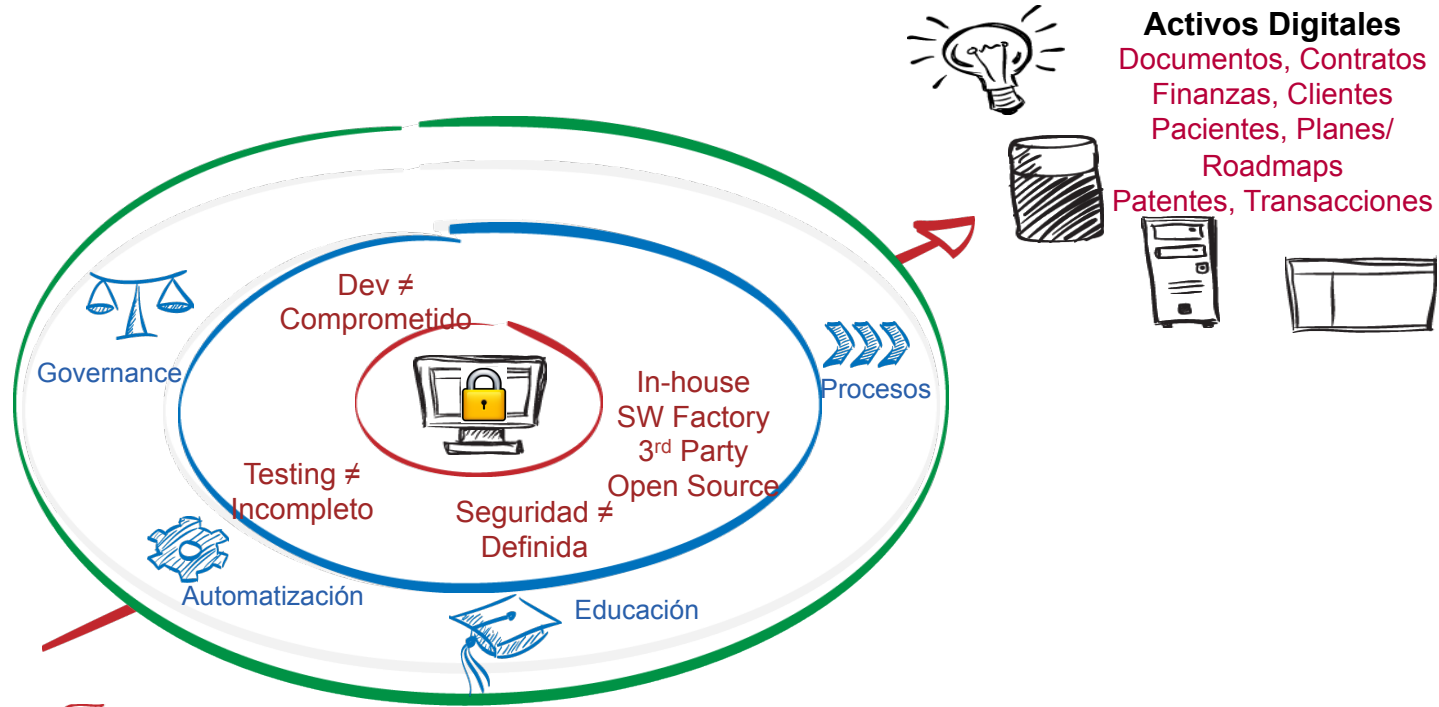
**Amenazas**  
USD\$280B



Beneficios

Seguridad Aplicativa

Situación Actual



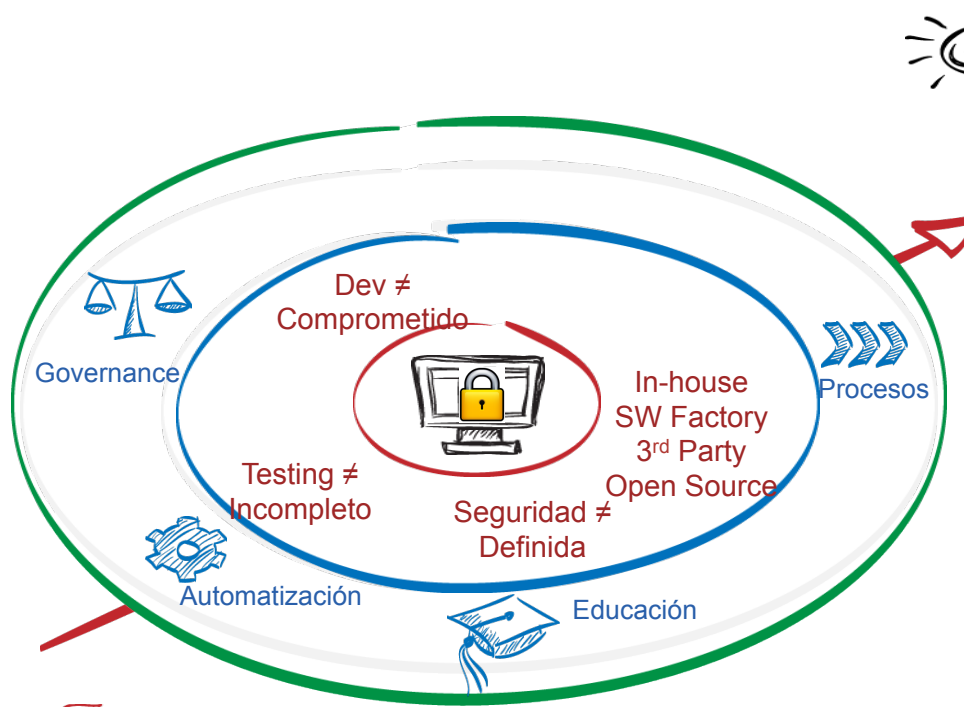
**Amenazas**  
USD\$280B



# Beneficios

# Seguridad Aplicativa

# Situación Actual



**Activos Digitales**  
Documentos, Contratos  
Finanzas, Clientes  
Pacientes, Planes/  
Roadmaps  
Patentes, Transacciones

**Valor para el negocio**

Nivel de Riesgo

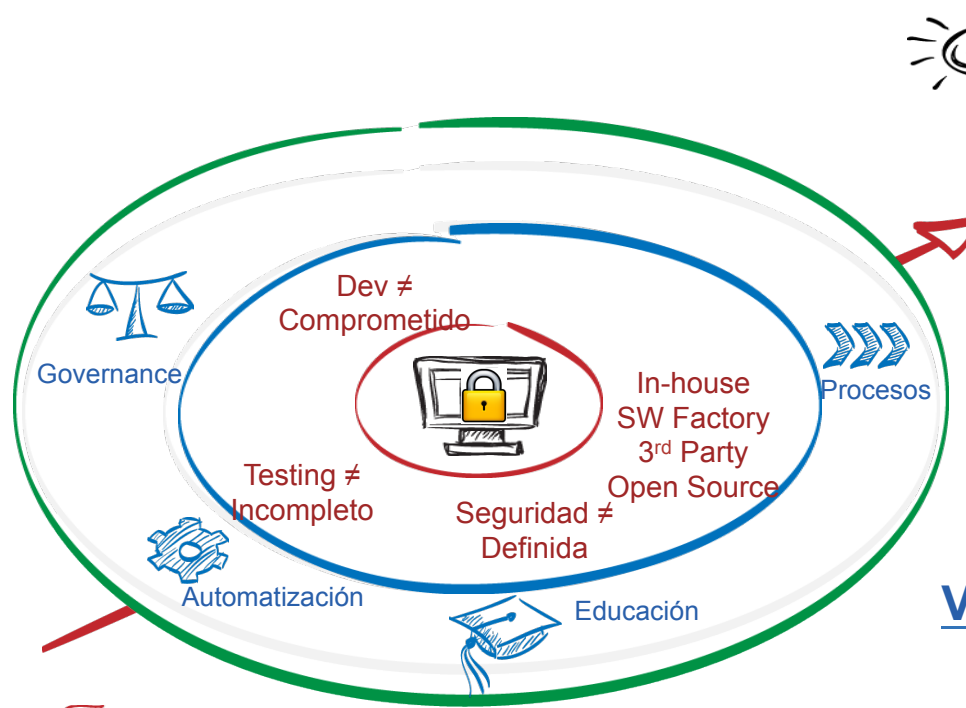
**Amenazas**  
USD\$280B



# Beneficios

# Seguridad Aplicativa

# Situación Actual



**Activos Digitales**  
Documentos, Contratos  
Finanzas, Clientes  
Pacientes, Planes/  
Roadmaps  
Patentes, Transacciones



Valor para el negocio

Nivel de Riesgo

Costos de SW Dev



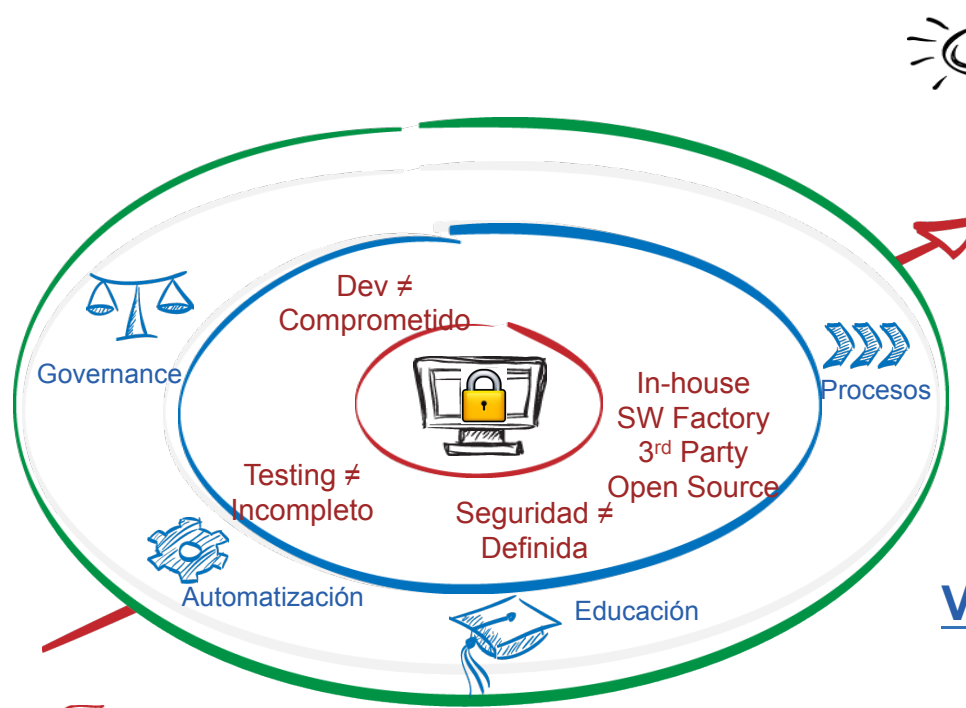
**Amenazas**  
USD\$280B



# Beneficios

# Seguridad Aplicativa

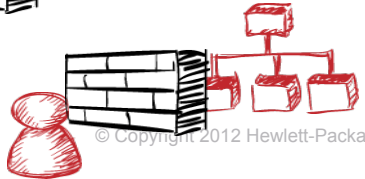
# Situación Actual






**Activos Digitales**  
 Documentos, Contratos  
 Finanzas, Clientes  
 Pacientes, Planes/  
 Roadmaps  
 Patentes, Transacciones



**Amenazas**  
 USD\$280B



**Valor para el negocio**

Nivel de Riesgo   
 Costos de SW Dev   
 Ahorros \$\$ 



# HP Fortify Software Security Assurance (SSA) Framework



- Alineado con el modelo de madurez de seguridad en el software (SAMM – [www.opensamm.org](http://www.opensamm.org))
- Modelo sistemático para organizar, implementar y medir las capacidades de seguridad aplicativa
- Consta de cuatro disciplinas y doce áreas funcionales que cubren todos los aspectos de seguridad en el software
- Integra la experiencia de HP Fortify con alrededor de 500 implementaciones a nivel global



# Portafolio de Soluciones

**Análisis Estático**

Fortify Static Code Analyzer (SCA)

Fortify *on Demand*

**Análisis Dinámico**

WebInspect, QAINspect, WI Enterprise

Fortify *on Demand*

**Protección**

Fortify Runtime

**Remediación y Prevención**

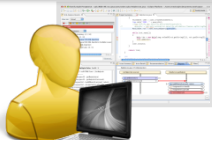
IDE Plugins  
Audit  
Workbench  
Scan Wizard

**Administración de Vulnerabilidades (Estático, Dinámico, Runtime)**

HP Fortify Software Security Center

**Governance**

Fortify Governance Module (SSC Server Add-on)



**Desarrolladores y Especialistas de Seguridad**

-Packard Developer



**Audidores y Gerentes de Seguridad, Líderes de Proyecto**

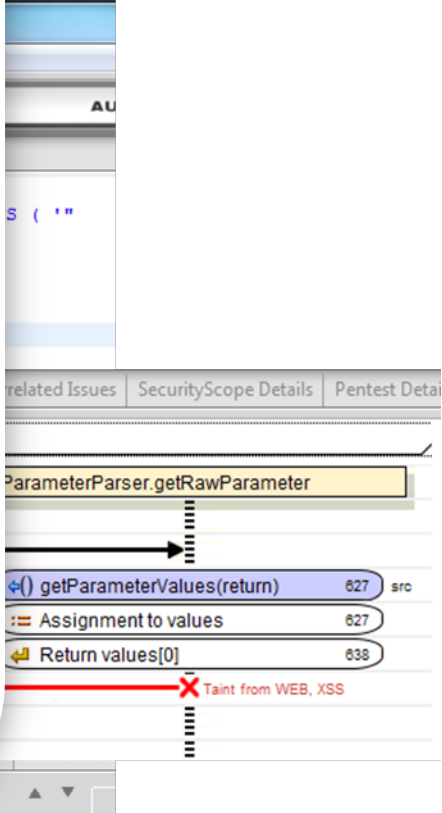
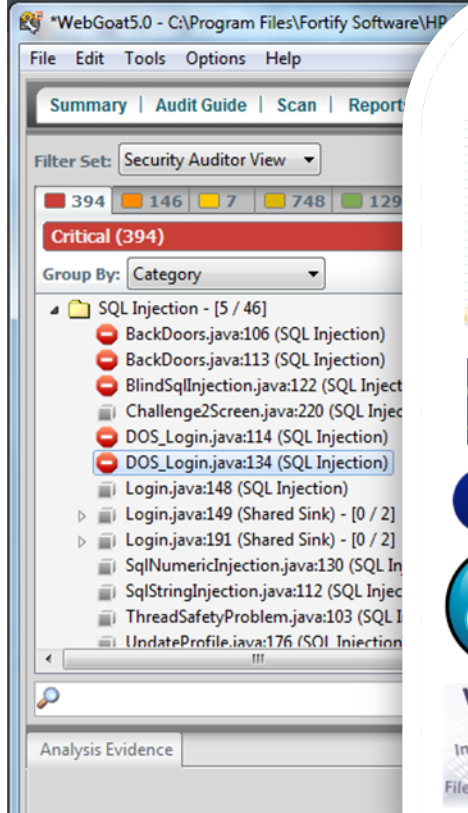
Subject to change without notice.



**Project, Security, and Management Stakeholders**



# Fortify SCA (Static Code Analyzer)



# HP Fortify Software Security Center (SSC)

### Alerts

[Manage](#) | [Preferences](#)

Show Read Alerts

4 records found

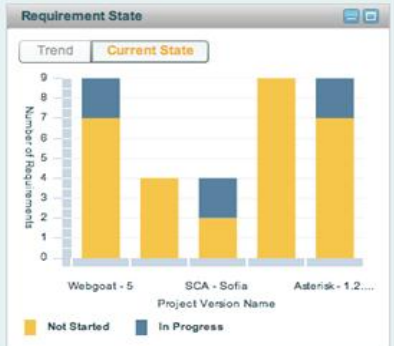
Select item and...

Date	Project Ve	Alert Trigg	Current Value
01-20-200	SCA - Sofi	Allocate Ti	Awaiting Sign C
01-15-200	SCA - Sofi	Allocate tin	Awaiting Sign C
01-15-200	SCA - Sofi	Allocate Ti	Awaiting Sign C
01-15-200	SCA - Sofi	Allocate Ti	Document Reje

### Document Status

Select item and...

Name
Webgoat-5
SPLC-1
Asterisk-1.2.10
SCA-Sofia
Riches Bank-1.0

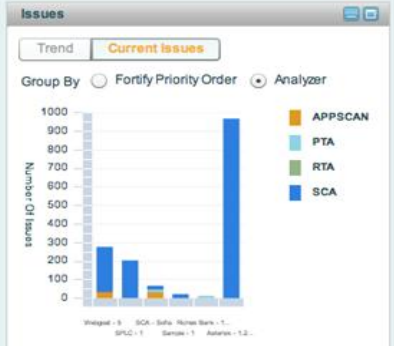
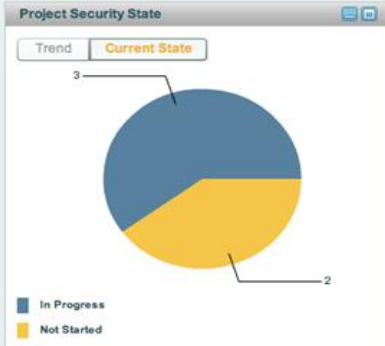
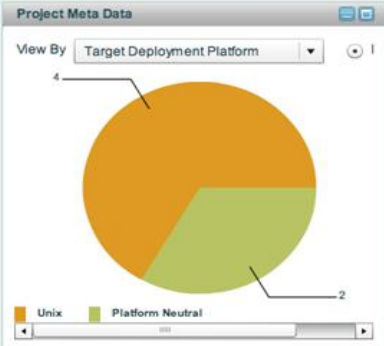


### Audit Status

6 records found

Select item and...

Project Version	Last Upload	Total Issu	Audit Perc
Asterisk - 1.2.10	01-22-2009...	968	0.21%
Riches Bank - 1	01-22-2009...	14	0.00%
SCA - Sofia	01-15-2009...	67	0.00%
SPLC - 1	01-26-2009...	204	0.00%
Sample - 1	01-16-2009...	22	0.00%
Webgoat - 5	01-16-2009...	277	0.00%



# HP WebInspect

The screenshot displays the HP WebInspect interface for a 'New Web Site Assessment' of 'http://zero.webappsecurity.com/'. The interface is divided into several sections:

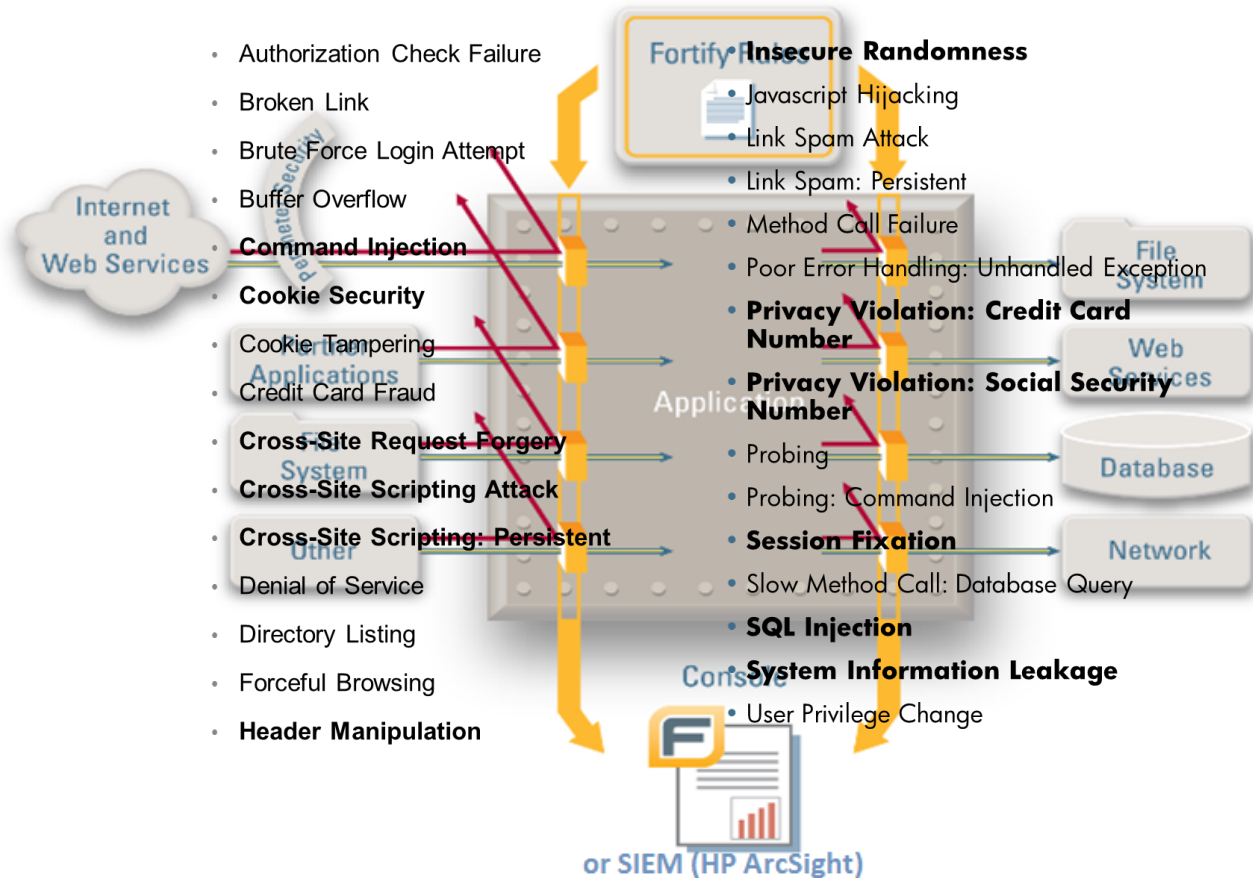
- Site:** A tree view on the left showing the directory structure of the scanned site, including folders like '\_private', '\_vt\_bin', 'admin', 'aspnet\_client', 'backup', 'cgi-bin', 'cookietest', 'CVS', 'db', 'error\_log', 'errors', 'htbin', 'images', 'include', 'linking', 'login', 'scripts', 'stabs', 'test', and 'testing'.
- Scan Info:** A sidebar menu with options like Dashboard, Traffic Monitor, Notes, Session Info, Host Info, P3P Info, AJAX, Certificates, Comments, Cookies, E-mails, Forms, Hidden, Scripts, Broken Links, Offsite Links, and Parameters.
- Scan Dashboard:** The main central area showing scan progress:
  - Crawl:** 348 of 348 (100% complete)
  - Audit:** 854 of 854 (100% complete)
  - Scan Status:** Completed with a green checkmark.
  - Activity:** Crawling and Auditing are active, with Req/Sec and Evt/Sec values shown as '-'.
  - Other:** Script Execution is active with an Evt/Sec value of '-'.
  - Vulnerabilities:** A bar chart showing the distribution of findings: Critical (106), High (92), Medium (8), Low (66), Info (22), and Best Practices (25).
  - Attack Type Table:**

Attack Type	Attacks	Critical	High	Medium	Low	Info	Best Practices
Manipulation	2,597	103	52	0	2	0	0
Exploratory	10,111	1	26	4	37	8	6
Other	6,216	2	14	4	27	14	19
- Summary Metrics (Right Panel):**
  - Scan:** Duration: 00:09:59, Policy: Standard
  - Crawl:** Hosts: 1, Sessions: 78
  - Audit:** Attacks Sent: 18,924, Issues: 319
  - Network:** Total Requests: 20,001, Failed Requests: 0, Script Includes: 0, Macro Requests: 40, 404 Probes: 219, 404 Check Redirects: 56, Verify Requests: 0, Logouts: 28, Macro Playbacks: 40, AJAX Requests: 0, Script Events: 227, Kilobytes Sent: 14,543K
- Vulnerabilities List (Bottom):** A table listing specific findings:
 

Risk	Count	Description
Critical	48	Cross-Site Scripting
Critical	6	Database Server Error Message
Critical	4	SQL Injection Confirmed (No Data Extraction)
Critical	1	IIS Global Server Variables Disclosure (global.asa.bak)
Critical	47	Microsoft ASP.NET or ASP Unicode Conversion Cross-Site Scripting
Critical	7	Unencrypted Login Form
Critical	6	Logins Sent Over Unencrypted Connection
Critical	3	Admin Section Must Require Authentication
Critical	1	Web on Administrative Access Purposes



# HP Fortify Runtime – Real Time Protection



# Fortify Training

- Entrenamiento con clases abiertas en Sunnyvale, California, USA
- Entrenamiento en sitio con instructores certificados de HP ESP Fortify
- Computer Based Training (CBTs)
- Plataforma de E-Learning



# HP Fortify OnDemand

Fortify on Demand

## Executive Summary

**Company:** BigBankESMP  
**Project:** SPLC  
**Version:** 1.0  
**Static Analysis Date:** July 15, 2009  
**Dynamic Analysis Date:** N/A

**Fortify Security Rating**

★★★★★  
64 issues

Based on impact and likelihood of issues (see Appendix A).

**Static:** ✓ | **Dynamic:** ✗

**Application Type:** E-Commerce  
**Technology Stack:** Java/J2EE  
**Interfaces:** Web Services (SOA)  
 Web Access

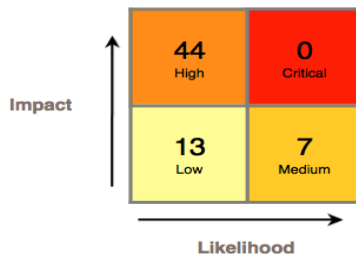
**Project Type:** Application  
**Data Classification:** Customer personally identifiable

### Top 5 Prevalent Categories



- Cross-Site Scripting: 35
- Cross-Site Request Forgery: 13
- SQL Injection: 5
- SQL Injection: Hibernate: 3
- Unreleased Resource: Streams: 3
- Other: 5

### Issues by Priority

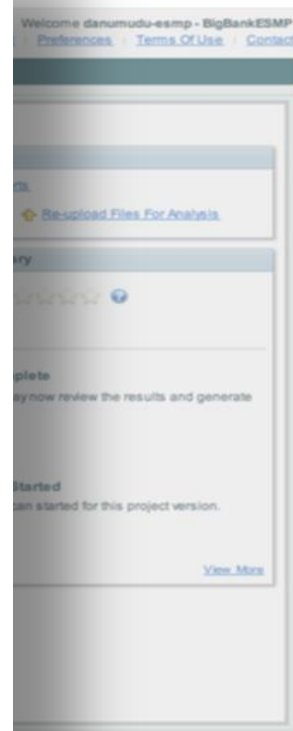
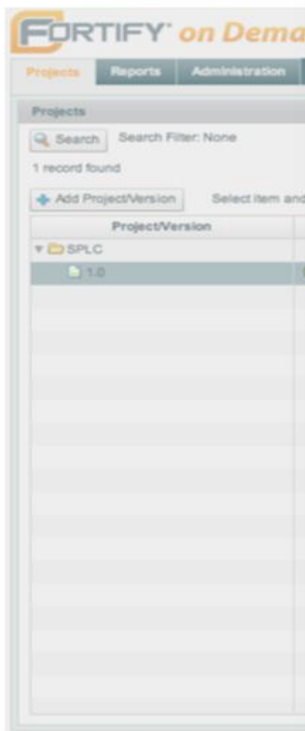


### Issues by Attack Vector

Attack Vector	Issues
Database	2
Network	0
Web	41
Web Service	0
Other	21
<b>Total</b>	<b>64</b>

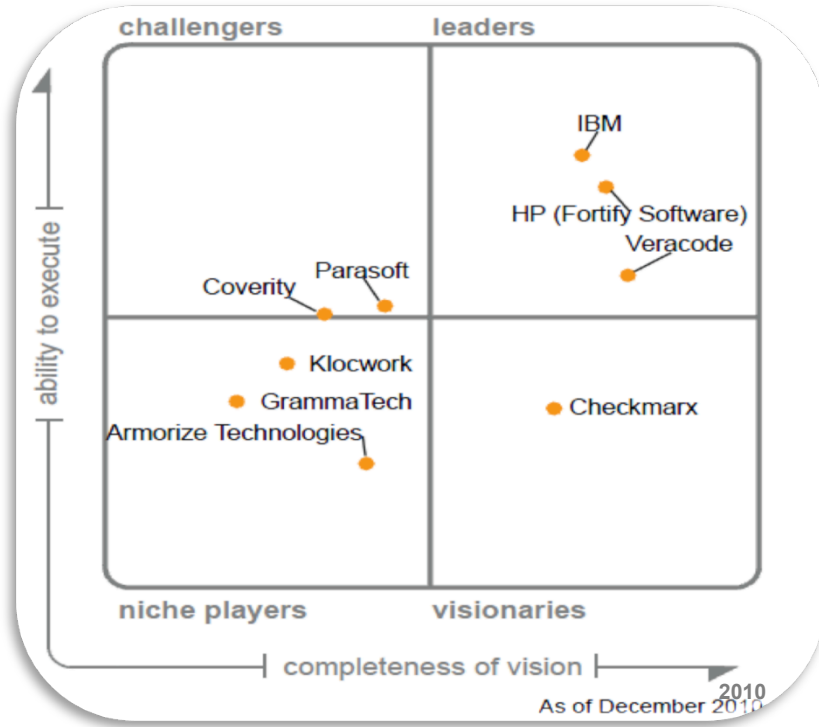
### Remediation Roadmap

To Achieve	Major Fixes	Minor Fixes
★★★★★	0	0
★★★★☆	0	0
★★★☆☆	0	44
★★★★☆	0	0
★★★★★	0	0
<b>Total</b>	<b>0</b>	<b>44</b>



# Posicionamiento en la industria

## Static



## Dynamic





# Posicionamiento en la industria



BNSF



GEICO



HSBC

KOREAN



DOWNNEY SAVINGS  
The Friendlier, Easier Place to Bank



Over **1000** enterprise customers

- **9 of the 10** largest banks
- **10 of the top 10** telecomm firms
- **5 of top 5** insurance firms
- **9 of the top 10** ISVs
- **6 of the top 10** aerospace and defense
- **All branches** of U.S. armed services

Plus...

- **Largest** app security research group
- **500+** vulnerability categories
- **21** programming languages
- **The most** platforms and IDEs

//CODiE//  
2011 SIIA CODIE WINNER



# Mitos sobre las soluciones HP Fortify

**Si los desarrolladores la usan, desaparecen los problemas**

**Falso**

**Leyendo el manual aprendes sin el apoyo de un especialista**

**Falso**

**Esta es una poderosa herramienta que te da todos los errores de seguridad y quedas certificado**

**Falso**



# Resumen

HP Fortify es una solución cuya propuesta de valor es:

- **Agilizar los tiempos** para efectuar las pruebas de seguridad en el código
- **Prevenir problemas de seguridad** desde etapas tempranas del ciclo de desarrollo
- **Reducir los costos** asociados a la corrección de problemas de seguridad detectados en producción
- **Investigación y actualización permanente** sobre las vulnerabilidades nuevas y existentes
- Ayudar a **evitar penalizaciones por incumplimiento de regulaciones** internas, locales o de industria y SLAS
- **Acelerar los tiempos de ejecución de las auditorías** externas e internas
- **Proteger la reputación e imagen pública del cliente** por hackeos
- **Tiempos de respuesta menores** ante un incidente de seguridad





# ¡Gracias!

Victor Rojo

[victor.rojo@hp.com](mailto:victor.rojo@hp.com)

+52 1 55 1069 31 57