Desarrollo seguro de Aplicaciones Web basado en OWASP

Por: Carlos Carreño,

OCP, ScrumMaster, Solution Architect

Email: ccarrenovi@Gmail.com

Unidad 7 Implementación segura de aplicaciones

- Diseño de implementación segura
- Hardening de sofware de base
- Topología de la instalación
- Web Services y Web Mobile
- Aseguramiento de S.O y software de base
- Servidores Web (ej: IIS, Apache)
- Interpretes (ej: PHP, Java, ASP .NET)
- Application Server (ej: Tomcat, JBOSS)
- Prevención de revelación de información
- Seguridad en el proceso de implementación.

Autor: ccarrenovi@Gmail.com

Diseño de implementación segura

- Usa una metodología segura

METODOLOGÍA DE DESARROLLO SEGURO	EMPRESA	METODOLOGÍA
Microsoft Security Development Lifecycle	Microsoft	Tradicional
Oracle Software Security Assurance	Oracle	Tradicional
Comprehensive Lightweight Application Security Process	OWASP	Tradicional
Team Software Process Secure	Software Engineer Institute	Tradicional
Software Assurance Maturity Model	OWASP	Tradicional
Building Security In Maturity Model	Cigital	Ágil
Agile Development Using Microsoft Security Development Lifecycle	Microsoft	Ágil

… continua

- Las mas recomendables

Microsoft® Security Development Lifecycle

Directiva obligatoria en Microsoft desde 2004:

- **Más popular y utilizado.**
- **Abundante documentación de los procesos.**

OWASP Open Web Application Security Project

OpenSAMM

Flexibilidad de aplicación empresarial

- **4 Funciones de Negocio**
- **12 Actividades de Seguridad**

… continua

- Actividades de seguridad
  - *ESTRATEGIA Y ORIENTACIÓN (Top 10 OWASP, CERT, CWE)*
  - *FORMACIÓN EN SEGURIDAD de los grupos implicados en el desarrollo.*
  - *Identificación y DEFINICIÓN DE RIESGOS de negocio del cliente.*
  - *Obtención y validación de los REQUISITOS DE SEGURIDAD.*
  - *Análisis y MODELADO DE AMENAZAS que proteja la superficie de ataques.*
  - *REVISIÓN DEL DISEÑO.*
  - *REVISIÓN DEL CÓDIGO.*
  - *TESTING DE SEGURIDAD.*
  - *VALIDACIÓN DE SALIDAS garantizando la seguridad del código liberado.*
  - *EVALUACIÓN Y MÉTRICAS confirmando el seguimiento de la seguridad.*
  - *Implantación de un PLAN DE RESPUESTA A INCIDENTES.*

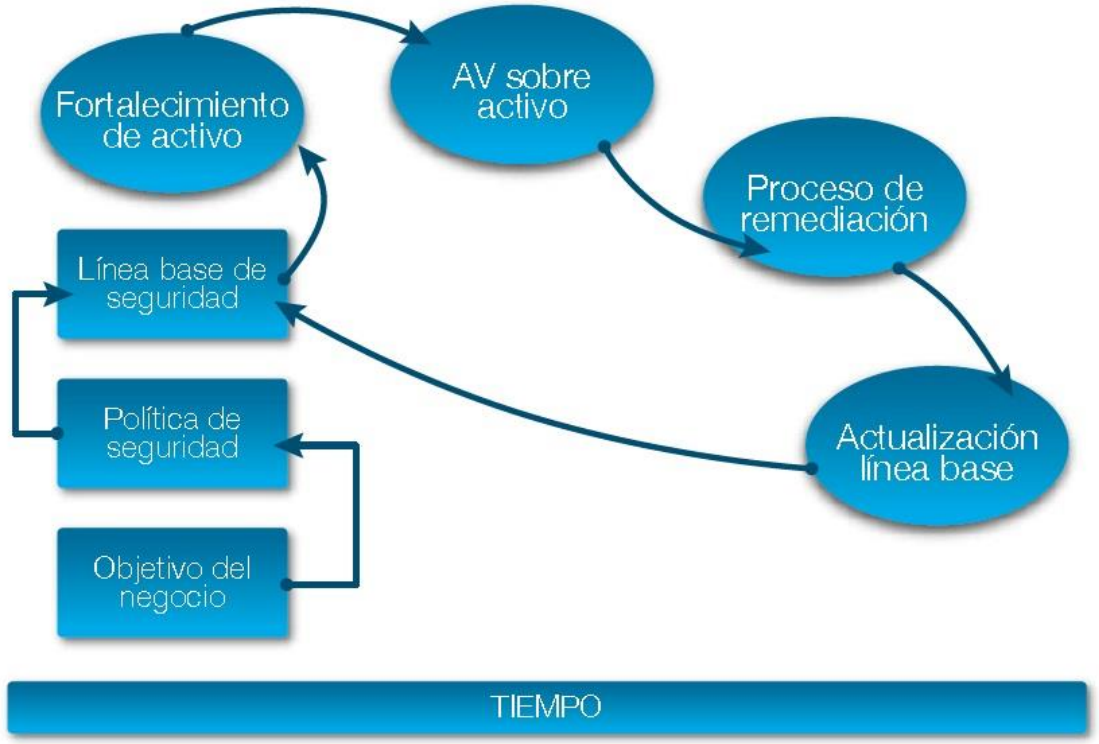
Observatorio de Seguridad

Repositorio de vulnerabilidades y gestión del conocimiento

Estado del proyecto

Hardening de sofware de base

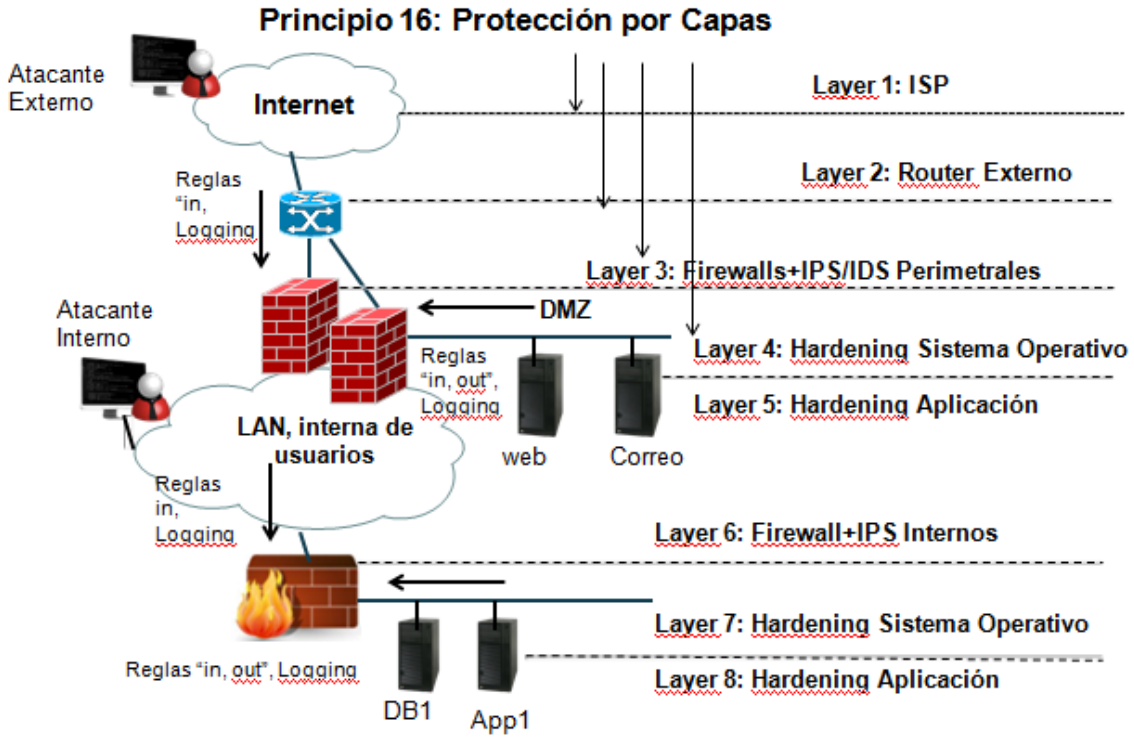
- **Hardening** (palabra en inglés que significa endurecimiento) en seguridad informática es el proceso de asegurar un sistema mediante la reducción de vulnerabilidades en el mismo, esto se logra eliminando **software**, servicios, usuarios, etc; innecesarios en el sistema; así como cerrando puertos que tampoco estén en uso.



Autor: ccarrenovi@Gmail.com

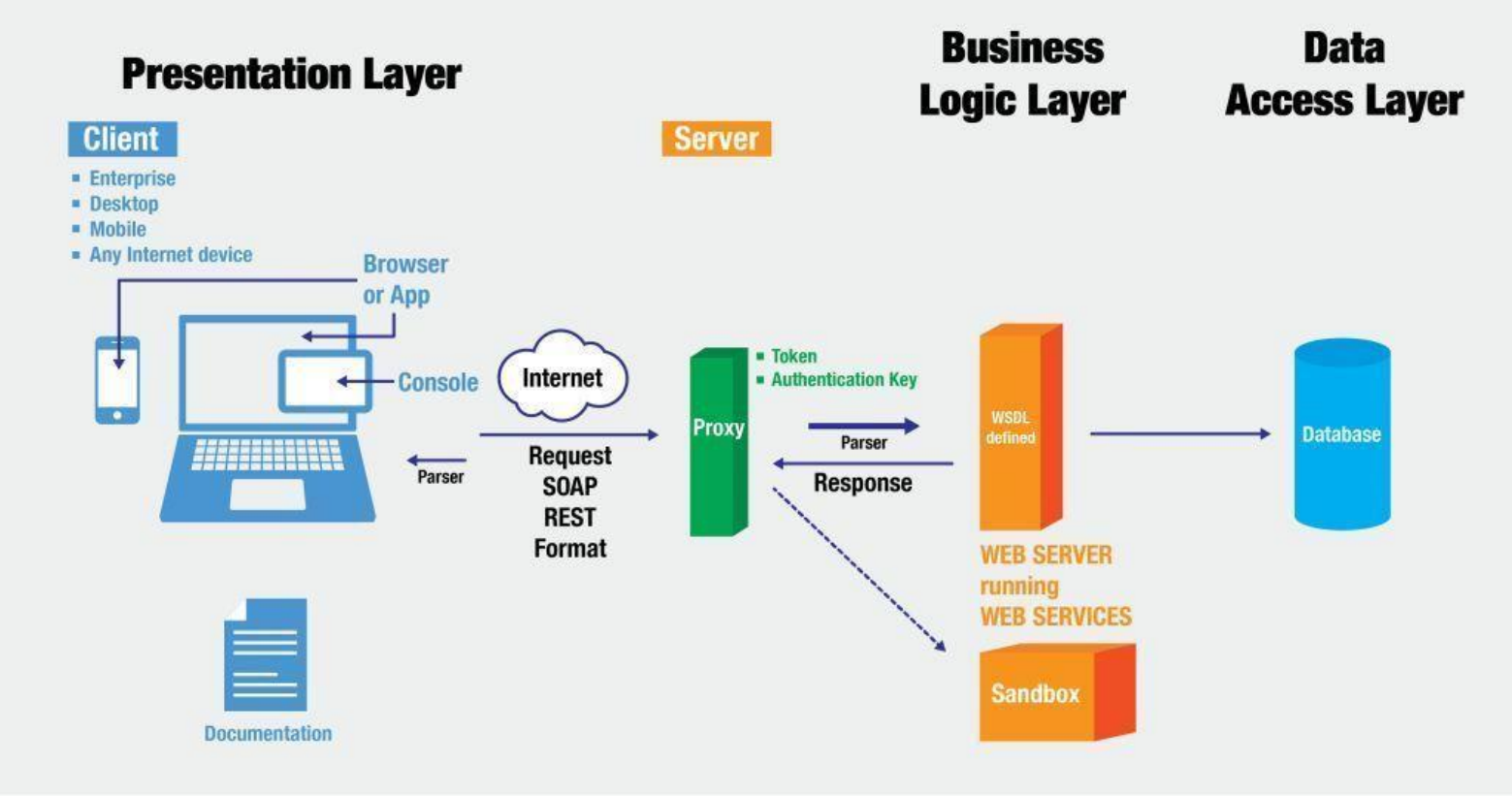
Topología de la instalación

- Protección por capas recomendación de NIST



Web Services y Web Mobile

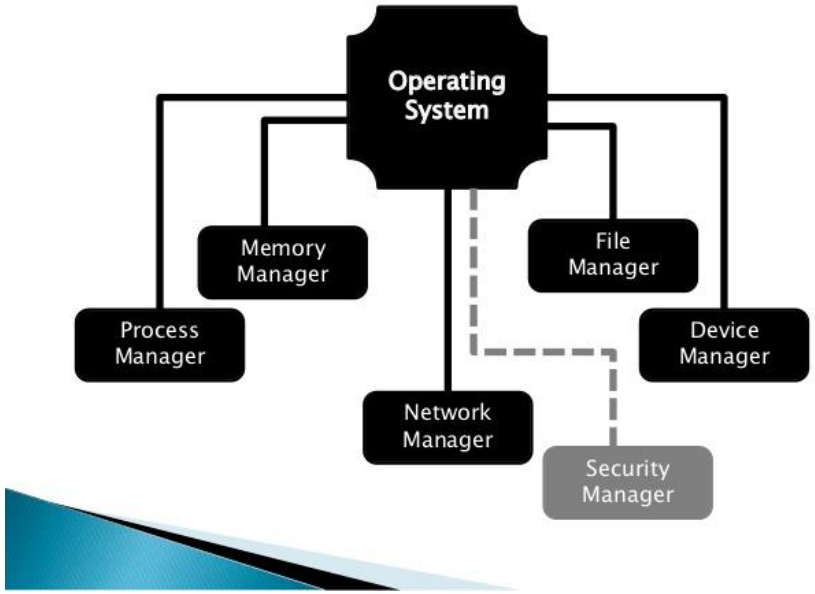
- Breaking down del servicio web

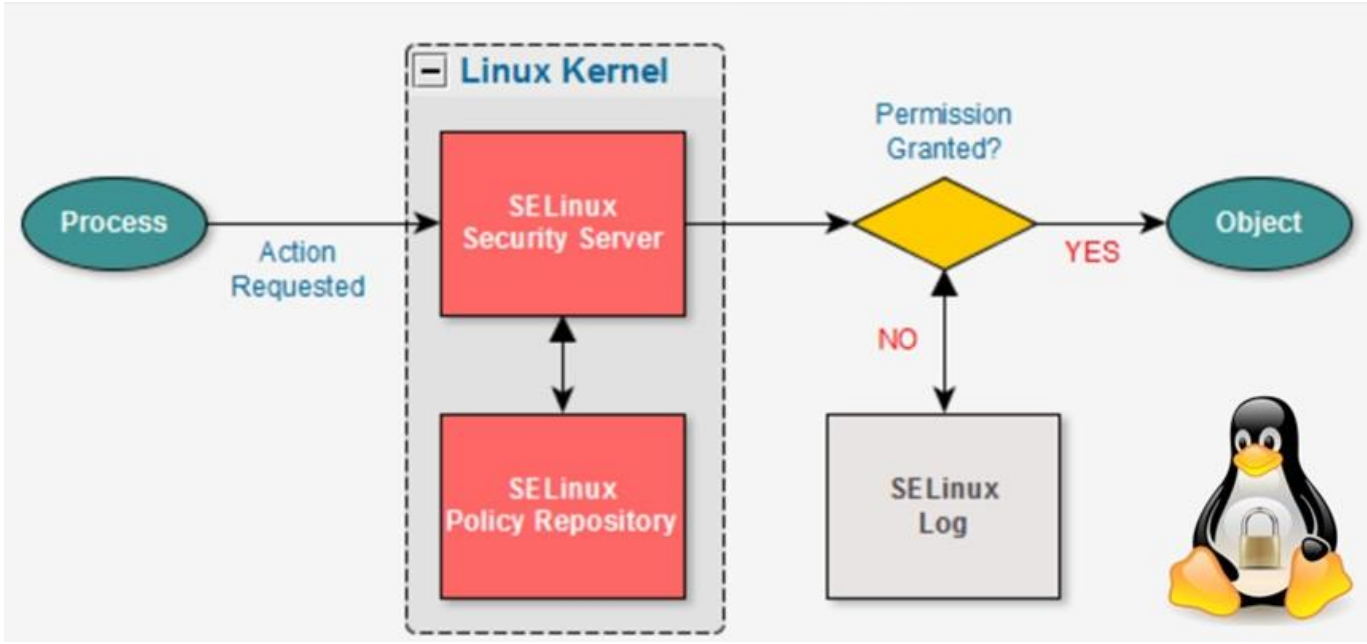


Autor: ccarrenovi@Gmail.com

Aseguramiento de S.O y software de base

- Seguridad del S.O.

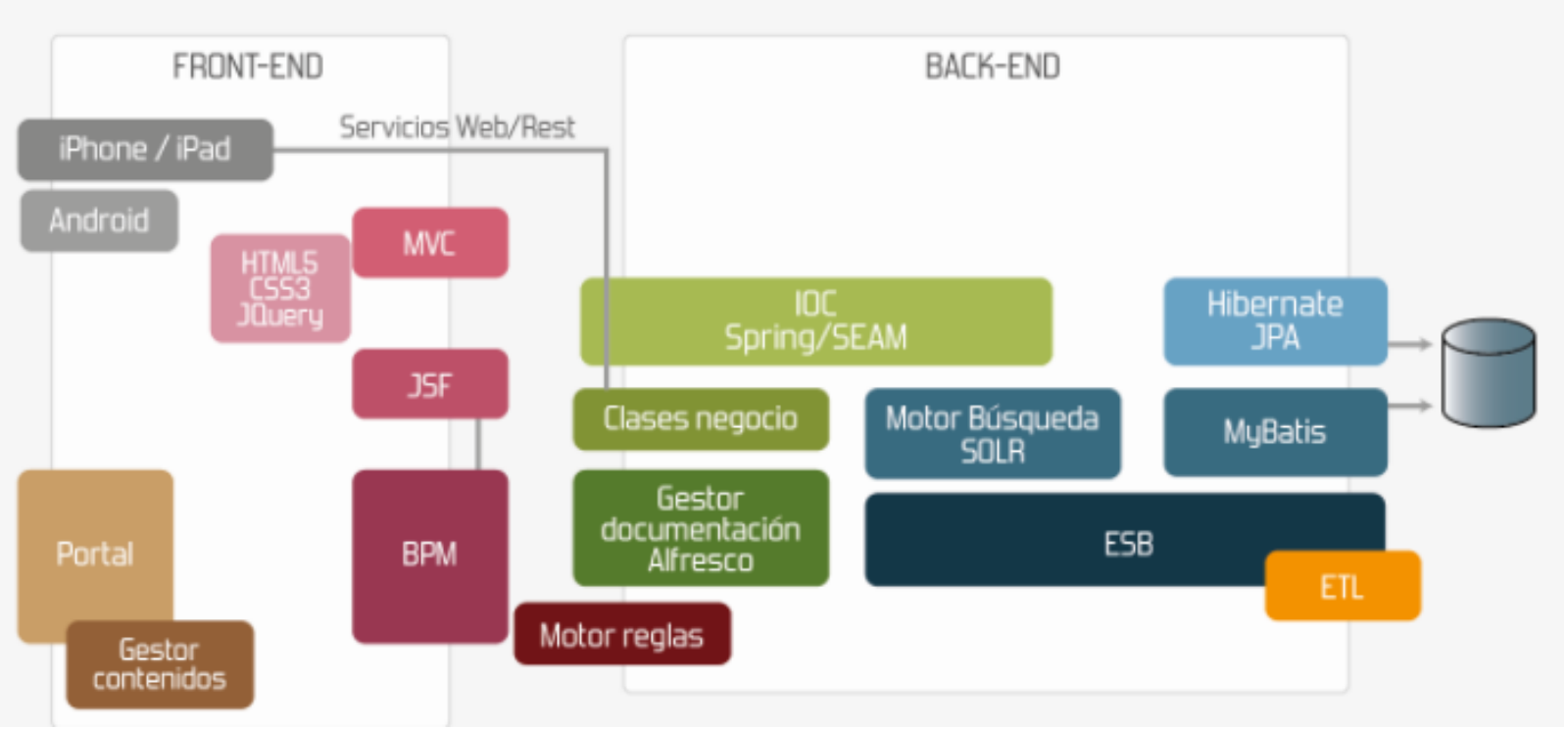




Autor: ccarrenovi@Gmail.com

… continua

- Software de Middleware



Autor: ccarrenovi@Gmail.com

Servidores Web

- IIS
- Apache Web Server
- Undertow

Autor: ccarrenovi@Gmail.com

Interpretes

- PHP
- Java
- .NET ASP

Application Server

- JBoss
- Tomcat
- Weblogic
- IBM Websphere

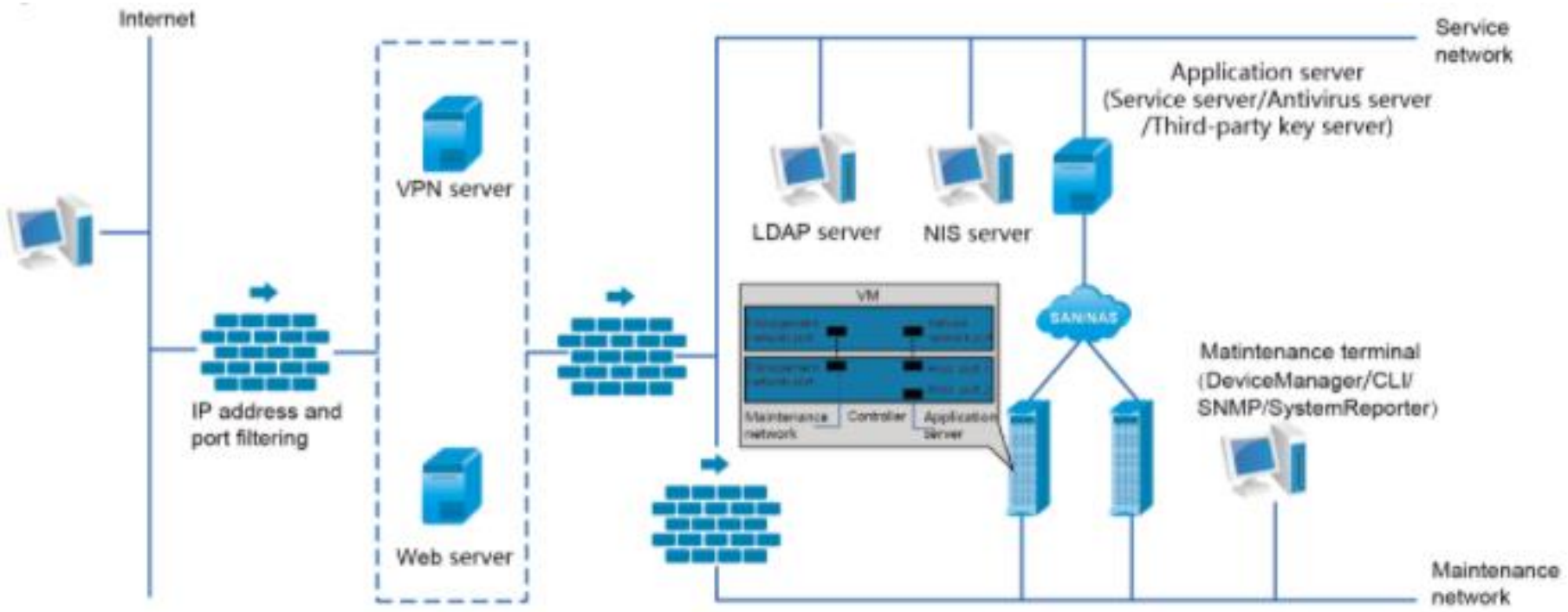
Autor: ccarrenovi@Gmail.com

Prevención de revelación de información

- Vector de Ataque Exposición de Información Sensible
- ¿Como prevenir?
  - *Para prevenir esta vulnerabilidad es posible utilizar la **log obfuscation** y **data obfuscation**, criptografía el canal de comunicación y utilizar Two-way SSL.*
  - *Es importante no almacenar datos sensibles si no hay necesidad, y **criptografiarlos**, tanto cuando están en reposo como en tránsito.*
  - ***Deshabilite siempre el «autocompletar»** en formularios y el caché en páginas que contengan datos sensibles.*

Seguridad en el proceso de implementación

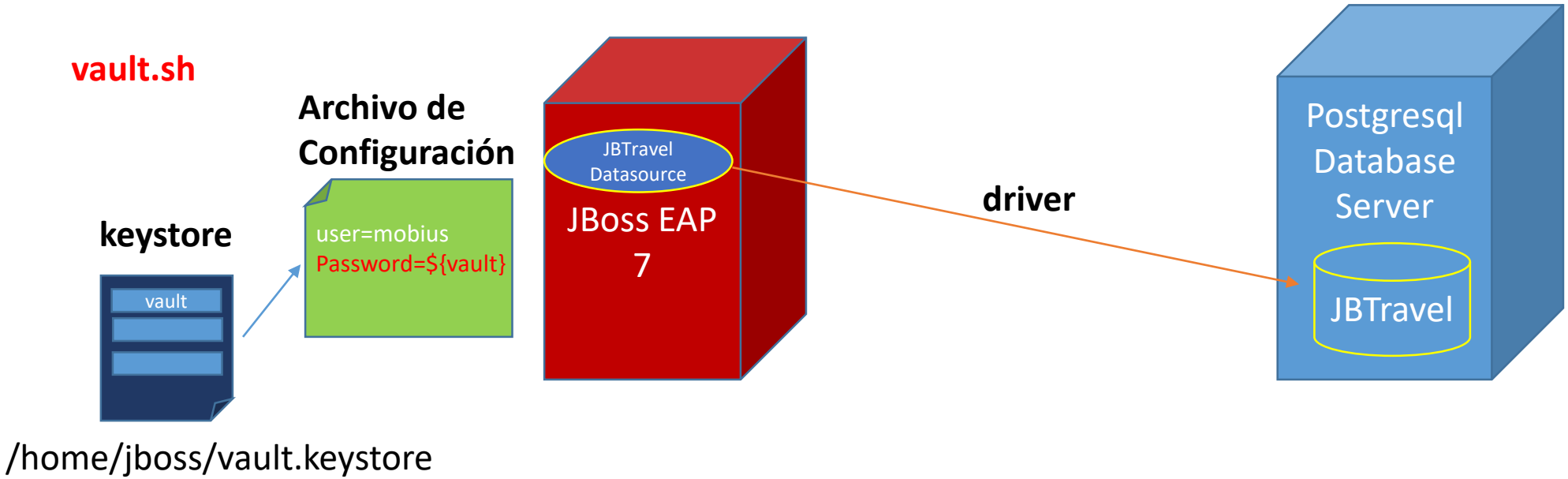
- Seguridad en el despliegue. Ejemplo: Huawei



Lab

- LAB Protección de Datos Sensibles en el servidor de aplicaciones Red Hat JBoss EAP

Escenario Lab 6




```
# useradd jboss
# passwd jboss
```