



Architect of an Open World™

## Osakidetza

Javier Zapata Victori, Director de la BU de Seguridad  
Bull (España), S.A.

**LIBERATE IT**

# Agenda

- Introducción: ¿Por qué implantar una solución de protección integral del puesto de trabajo?
- Problema de negocio y solución implantada
- El proyecto: implantación, valor obtenido y el futuro



# El nuevo escenario del *malware*

- Incremento en el nº de vulnerabilidades y sofisticación de los ataques
  - En 2007 se produjo tanto malware como en los 20 años anteriores juntos (F-Secure) ... y la tendencia es exponencial
  - Cada vez más, a través de la web o el e-mail
- Proliferación de herramientas para crear malware (Neosploit, Mpack) y mercado de vulnerabilidades
- Ataques generalizados → ataques dirigidos
- Ataques visibles → ataques no detectados
- El antivirus tradicional no llega a cubrir todo el espectro de amenazas
- Los dispositivos de cliente ganan en funcionalidad, movilidad y salen del perímetro
- Uso no profesional: redes sociales, descargas de Internet...



# El mercado de las vulnerabilidades

Vulnerability/Exploit	Value	Source
“Some exploits”	\$200,000 - \$250,000	Gov’t official referring to what “some people” pay [9]
Significant, reliable exploit	\$125,000	Adriel Desautels, SNOSoft [11, 22, 13]
Internet Explorer	\$60,000 - \$120,000	H.D. Moore [22]
Vista exploit	\$50,000	Raimund Genes, Trend Micro [24]
“Weaponized exploit”	\$20,000-\$30,000	David Maynor, SecureWorks [18]
ZDI, iDefense purchases	\$2,000-\$10,000	David Maynor, SecureWorks [18]
WMF exploit	\$4000	Alexander Gostev, Kaspersky [26]
Microsoft Excel	≥ \$1200	Ebay auction site [21, 25]
Mozilla	\$500	Mozilla bug bounty program [4]

Table 1: Estimates on exploit values.

## The Legitimate Vulnerability Market

*Inside the Secretive World of 0-day Exploit Sales*

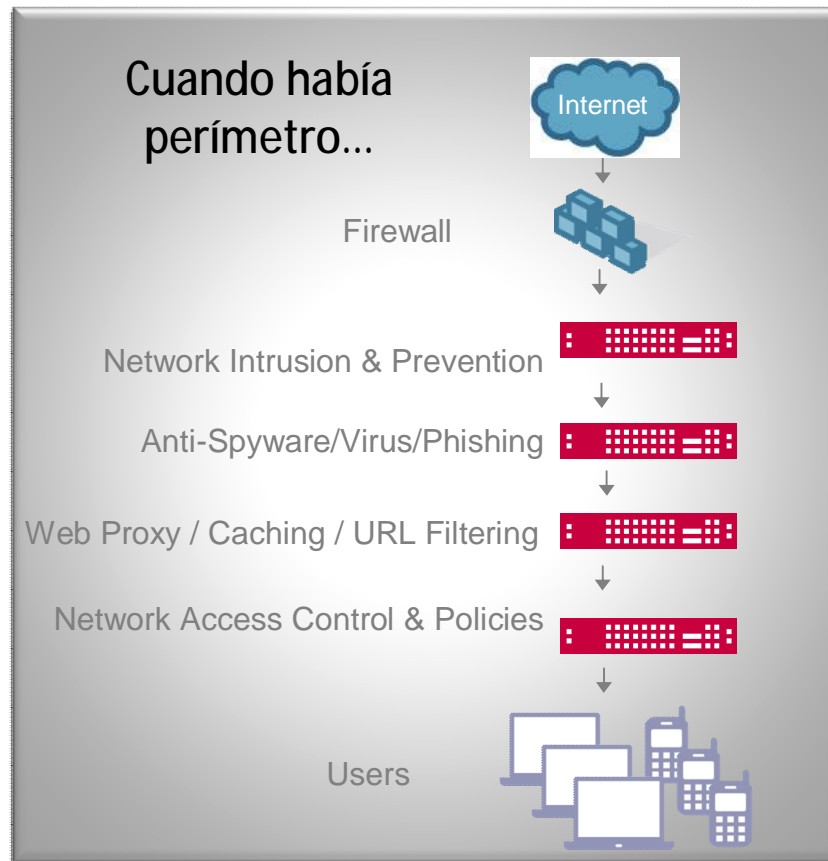
Charlie Miller, PhD, CISSP

Independent Security Evaluators

[www.securityevaluators.com](http://www.securityevaluators.com)



# El perímetro se ha desvanecido



# Componentes de una EPP

## Futuro

Backup gestionado

## Extensiones

Security Configuration Management (SCM)  
Análisis de vulnerabilidades  
Control de Aplicaciones  
NAC (integración) y remediación de infecciones

## Adicional

Full-disk encryption  
DLP (Data Loss Prevention)  
Port control  
URL filtering (lista negra)

## Inicial

Anti-malware (virus, troyanos, spyware...)  
HIPS (Host-based Intrusion Prevention System)  
Firewall Personal

# Agenda

- Introducción: ¿Por qué implantar una solución de protección integral del puesto de trabajo?
- Problema de negocio y solución implantada
- El proyecto: implantación, valor obtenido y el futuro





- Servicio Vasco de Salud
- **Atención Primaria:** 7 comarcas sanitarias, 131 Unidades de Atención Primaria y 320 centros de salud
- **Atención Hospitalaria:** 12 Hospitales de Agudos y 4 Hospitales de media y Larga Estancia
- **Salud Mental:** 4 Hospitales psiquiátricos monográficos, 5 servicios de psiquiatría integrados en Hospitales de Agudos y 3 áreas de salud mental extrahospitalarias.
- **Emergencias**
- **Centro Vasco de Transfusión y Tejidos humanos:**
- **Osatek:** gestión, administración y explotación de servicios por imagen de tecnología puntera.



## Problema de Negocio

- Renovar una plataforma de seguridad del Endpoint, adecuándola al nº perímetro del parque informático
  - PCs: 14,000
  - Servidores: 400
  - Portátiles: 600
  - Móviles / PDAs: 800
- Necesidad de un despliegue muy rápido
- Extender la protección a nuevos dispositivos móviles
  - PDAs, portátiles, ...
- Administración centralizada, con soporte a la toma de decisiones
- Aprovechar las nuevas tecnologías de seguridad para hacer frente al nuevo escenario de riesgos



# Aprovechar las nuevas tecnologías

- Adelantarse a nuevas normativas de seguridad más restrictivas, tipo LOPD.
- Evitar fugas de datos sensibles.
- Prevenir amenazas que pudieran derivar en publicación de datos médicos.
- Conocer el nivel de seguridad de la organización en cada momento.



# Necesidades funcionales

- Protección del parque informático contra virus, código malicioso y otro tipo de amenazas [Ya disponible, a renovar]
- Nuevas:
  - Gestión de Vulnerabilidades del parque informático
  - Detección y Prevención de Intrusiones
  - Protección de la información en Plataformas Colaborativas (Exchange, SharePoint)
  - Protección de la Información en dispositivos itinerantes
- Soporte actual y futuro de cumplimiento normativo
  - LOPD



# Requisitos (I)

- **Puestos y Servidores (Windows):**
  - **Workstations** (Windows XP y Windows 7): Antivirus y AntiSpyware.
  - **Servidores** (Windows 2003, previsible Windows 2008): Antivirus y AntiSpyware.
  - **Servidores Unix:** Red Hat Linux, HPUNIX, AIX
- **Portátiles (Windows XP y Windows 7):** Módulos específicos Antivirus, AntiSpy, IDS/IPS Local, cifrado de datos
- **Móviles (Windows Mobile, Symbian):** Antivirus y análisis de amenazas en todas sus interfaces (web, email, sms, mms, wifi, bluetooth...) y cifrado de datos



## Requisitos (II)

- Correo Electrónico: Microsoft Exchange 2003: Antivirus, filtrado de adjuntos
- Gestor Documental: MS Sharepoint
- Entornos Virtualizados: analizar la adaptación
- IDS/IPS: red interna / externa, múltiples sondas, gestión centralizada y *throughput* de 10 Gbps
- Gestión Centralizada
  - Integración con Directorio Activo
  - Gestión conjunta de todos los productos, incluso los externos al dominio
  - Administración delegada
  - Informes y consultas personalizables y programables de forma periódica
  - Alertas



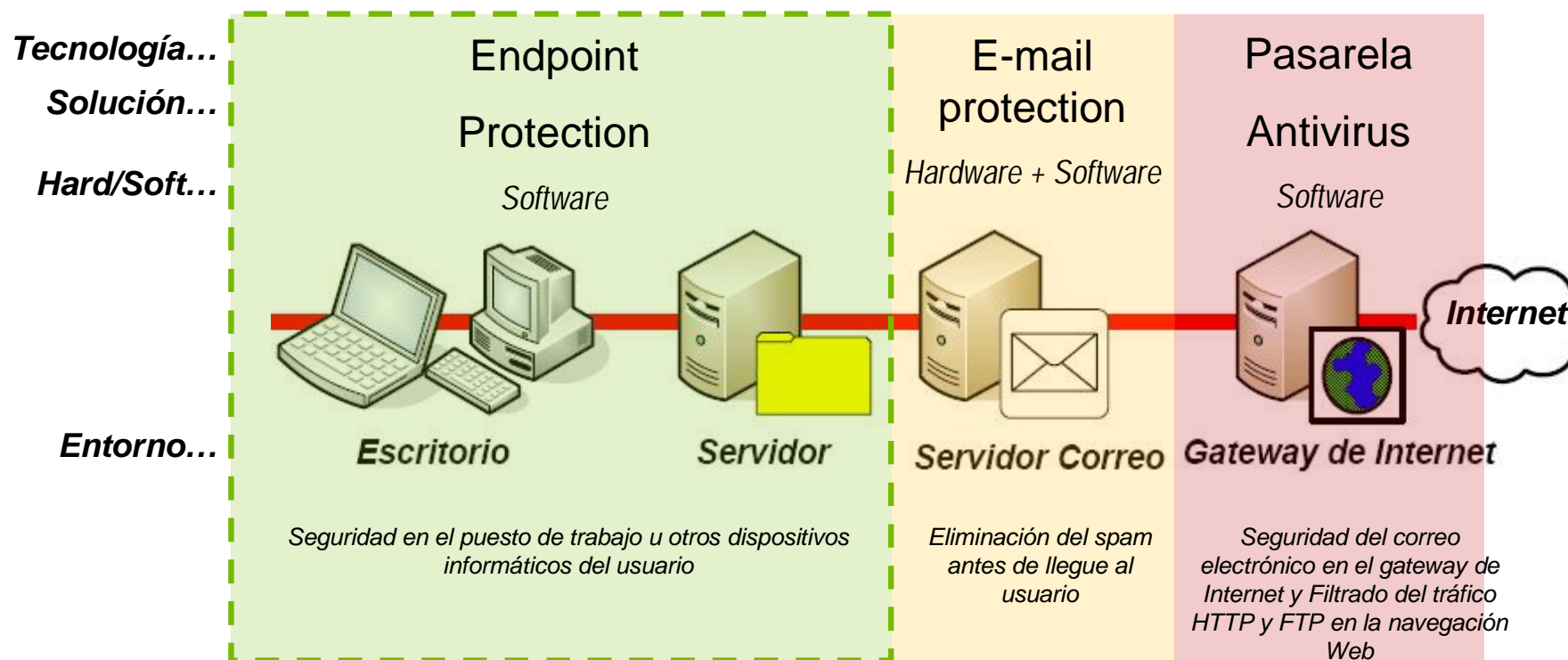
# Agenda

- Introducción: ¿Por qué implantar una solución de protección integral del puesto de trabajo?
- Problema de negocio y solución implantada
- El proyecto: implantación, valor obtenido y el futuro



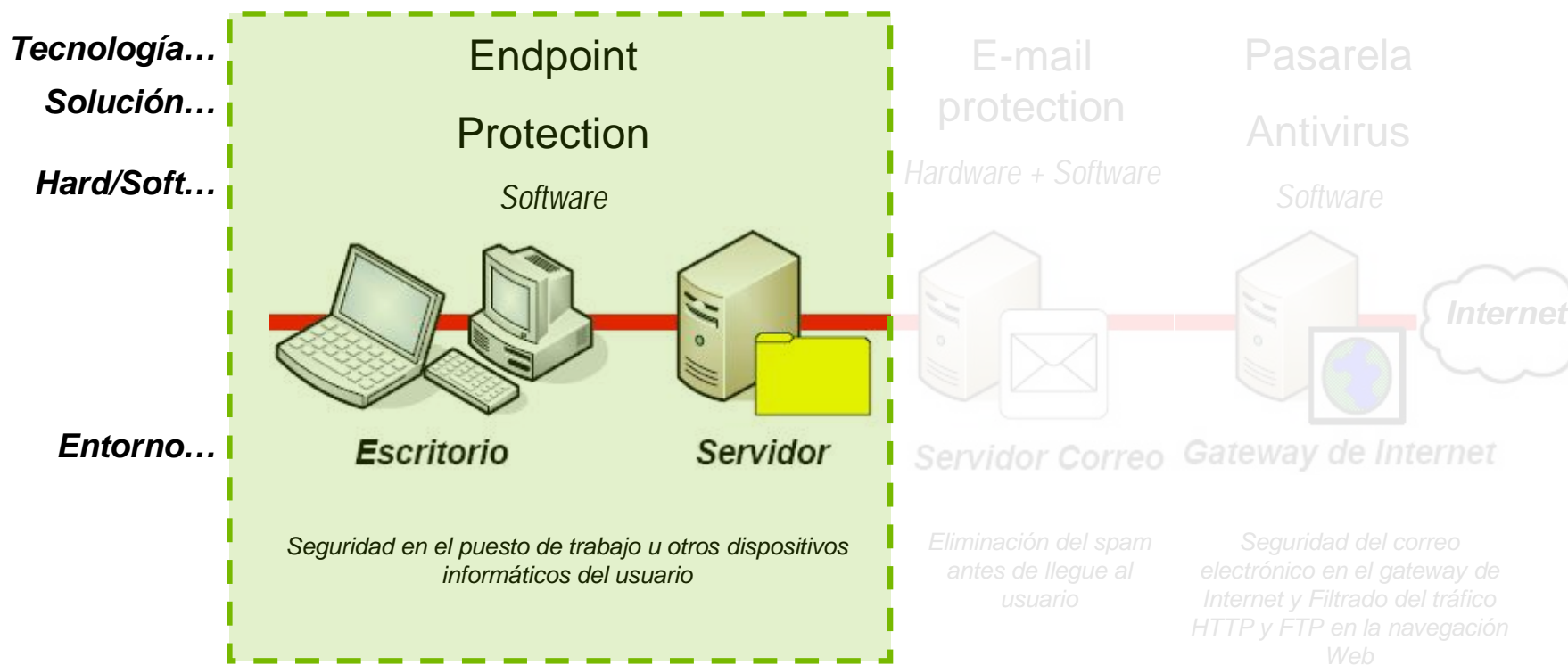
# Alcance del proyecto

- Etapas de seguridad en Osakidetza:



# Alcance del proyecto

## - Etapas de seguridad en Osakidetza:



# Arquitectura Lógica Integrada de la Solución

3

Gracias al Gestor de Vulnerabilidades, se puede escanear la plataforma para valorar la gravedad del ataque

- Endpoint Encryption
- Encrypted Media



- Gestión de Vulnerabilidades



- IPS



1 Se detecta un ataque contra un servidor corporativo

2

A través de EPO, se Puede conocer datos avanzados de la plataforma

Servicio de Correo

Portal Sharepoint

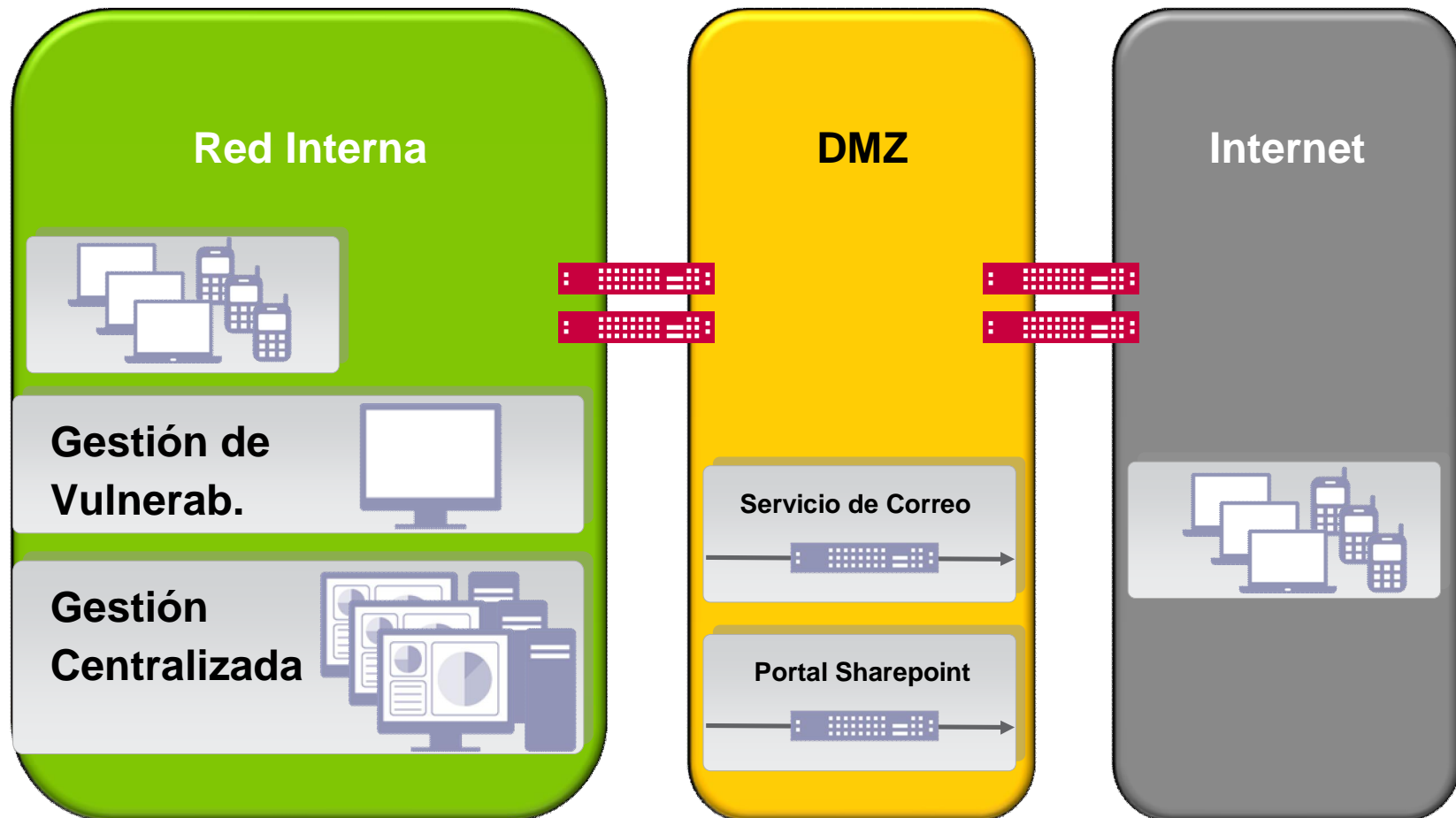
Gestión Centralizada

Modo Desconectado

LAN Corporativa Segura

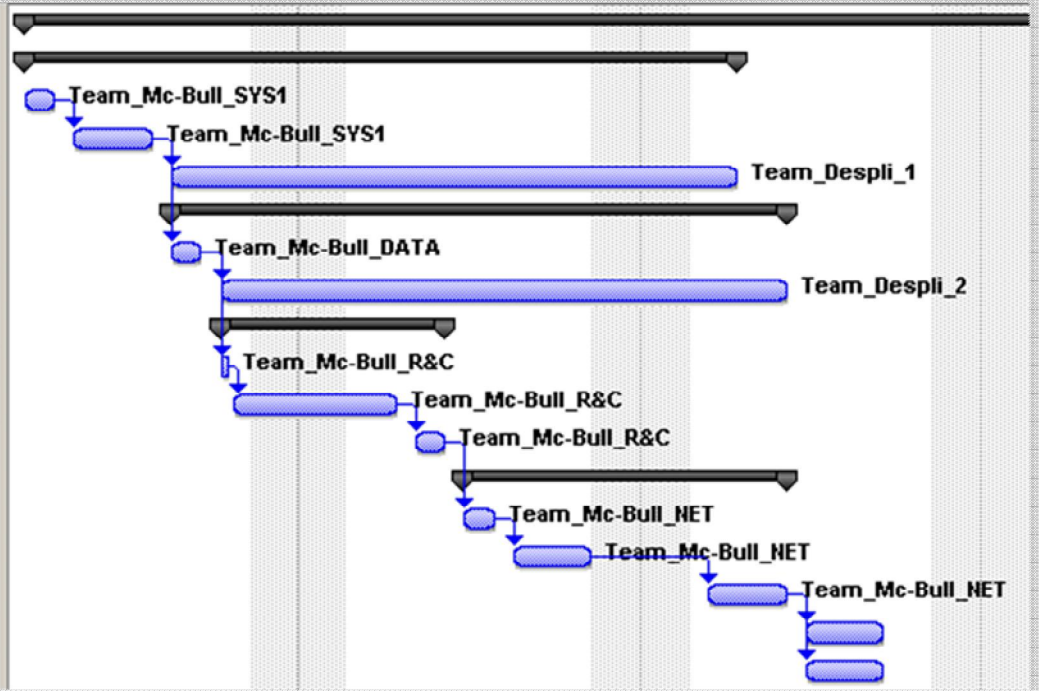
Información DMZ

# Arquitectura física de red



# Plan de Proyecto

[-] Proyecto de Seguridad (Osakidetza)	88 días
[-] Protección de nodo	11 días
Migración Consola Central	1 día
Pilotos	2 días
Migración-Despliegue	8 días
[-] Protección del dato	9 días
Piloto despliegue - 10 máquinas	1 día
Despliegue	8 días
[-] Risk & Compliance	3 días
Inicialización VM appliance	0,5 días
Definición de escaneos base	1,5 días
Análisis de resultados y ajuste escaneos	1 día
[-] Protección de red	5 días
Instalación y configuración inicial NSP Manager	1 día
Conexión de sensores y política inicial	2 días
Ajuste fino de las políticas	2 días
<b>Formación</b>	2 días
<b>Documentación</b>	2 días



**Duración: 14 días**

## Lo que fue bien...

- Duración y ejecución del despliegue
- Calidad en la Gestión del Proyecto: planificación, ejecución y control



## ... y lo que no fue tan bien (y cómo se solucionó)

- Adaptación del cifrado al proceso de renovación de contraseñas del dominio
  - Des-sincronización entre dominio y Plataforma Cifrado
  - Doble nivel de seguridad **J**



## Valor aportado a Osakidetza

- Transición no traumática de la protección que ya se tenía
- Anticipación a la protección de nuevos medios y canales de información (PDAs y móviles)
- Cifrado para el cumplimiento de la LOPD
- Mejora en el perfil de protección
  - Reducción de la superficie vulnerable
  - Defensa en profundidad
  - Protección de la información



# Conclusiones de proyecto

- Preparación para el futuro
- Importancia de proteger el **interior de la organización**
  - El entorno del usuario (PC, portátiles,...), es una importante fuente de riesgos para los activos de información
- La información que viaja en determinados dispositivos se ha convertido en un activo cuya protección es crítica
  - Implicaciones mediáticas
  - Implicaciones legales





**Osakidetza**



Architect of an Open World™

**LIBERATE IT**



**Javier Zapata Victori**  
Director BU Seguridad  
Security & Network Solutions, SNS  
Bull (España), S.A.  
[Javier.zapata@bull.es](mailto:Javier.zapata@bull.es)