Riesgos y amenazas en la red: Seguridad por Diseño

Jesús Feliz Fernández

Congreso Colegio Oficial de Ingenieros de Telecomunicación
Telecomunicaciones en Edificios Inteligentes
17 de Octubre de 2019

www.incibe.es

INSTITUTO NACIONAL DE CIBERSEGURIDAD

NATIONAL CYBERSECURITY INSTITUTE OF SPAIN

incibe_

GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

Agenda

- **Evolución y contexto tecnológico actual**
- **Redes y Sistemas: conceptos básicos**
- **Riesgos y vectores de ataque en la red interna**
- **Seguridad por diseño**
- **Algunos elementos de protección en red recomendados**
- **¿Y la GDPR?**
- **Retos y conclusiones**

Evolución y contexto tecnológico actual

Enorme evolución tecnológica en los últimos 40 años.

¿Se ha tocado techo? ¿Se trata de una curva exponencial?

Evolución y contexto tecnológico actual

Sector Automovilístico

1986

2001

2016

Evolución y contexto tecnológico actual

Imagen

4K Blu-ray Disc™

Evolución y contexto tecnológico actual

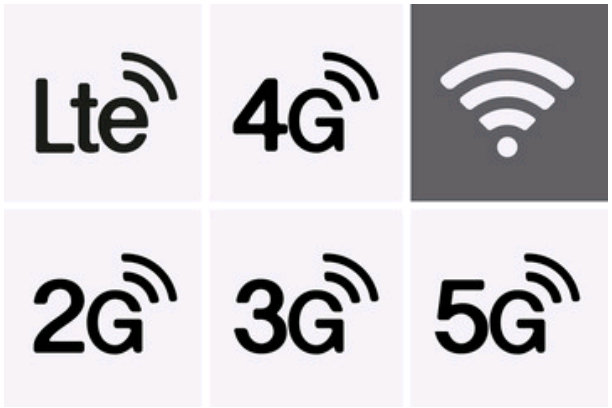
Sonido

Evolución y contexto tecnológico actual

Impresoras

Evolución y contexto tecnológico actual

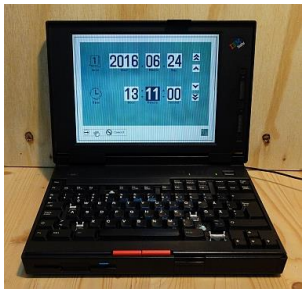
Comunicaciones



1996: 33.6kbps
2006: 10Mbps -> **x 300**
2016: 300Mbps -> **x 30**
Límite de oficina

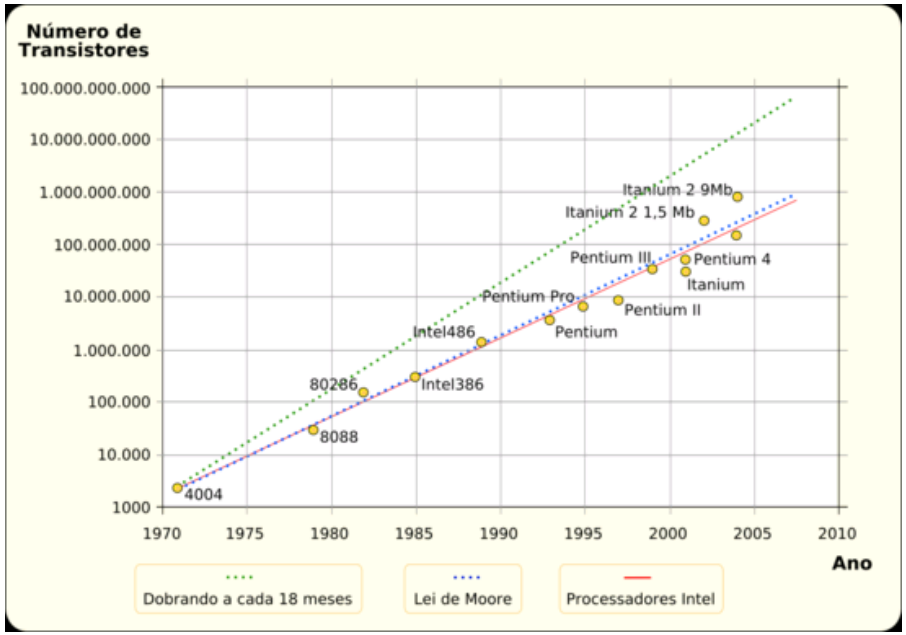
Evolución y contexto tecnológico actual

Computación



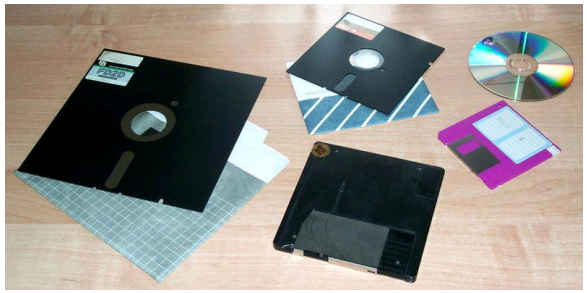
Osborne 1 – 1981 ThinkPad 345 - 1995 ThinkPad edge - 2010 ThinkPad 2019

La Ley de Moore “se deja de cumplir”



Evolución y contexto tecnológico actual

Almacenamiento



1996: 4GB
2006: 500GB -> **x 125**
2016: 4000GB -> **x 8**

Evolución y contexto tecnológico actual

¿Va a existir entonces un frenazo evolutivo?

Evolución y contexto tecnológico actual

¿Va a existir entonces un frenazo evolutivo?

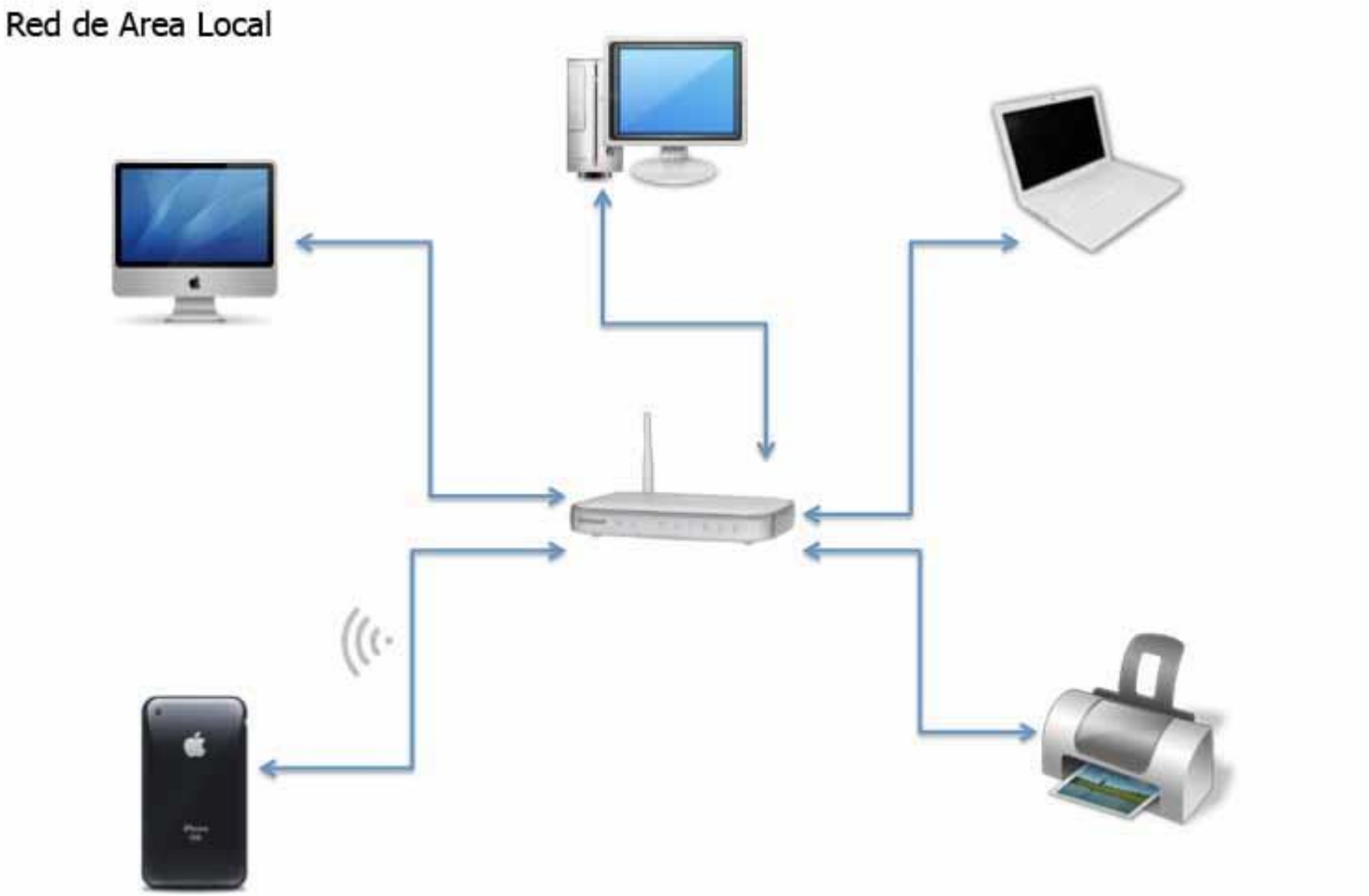
En absoluto, pero sí estamos viviendo un cambio sustancial en el concepto, que introduce a nuevos actores.

Redes y Sistemas Operativos: conceptos

Servidor

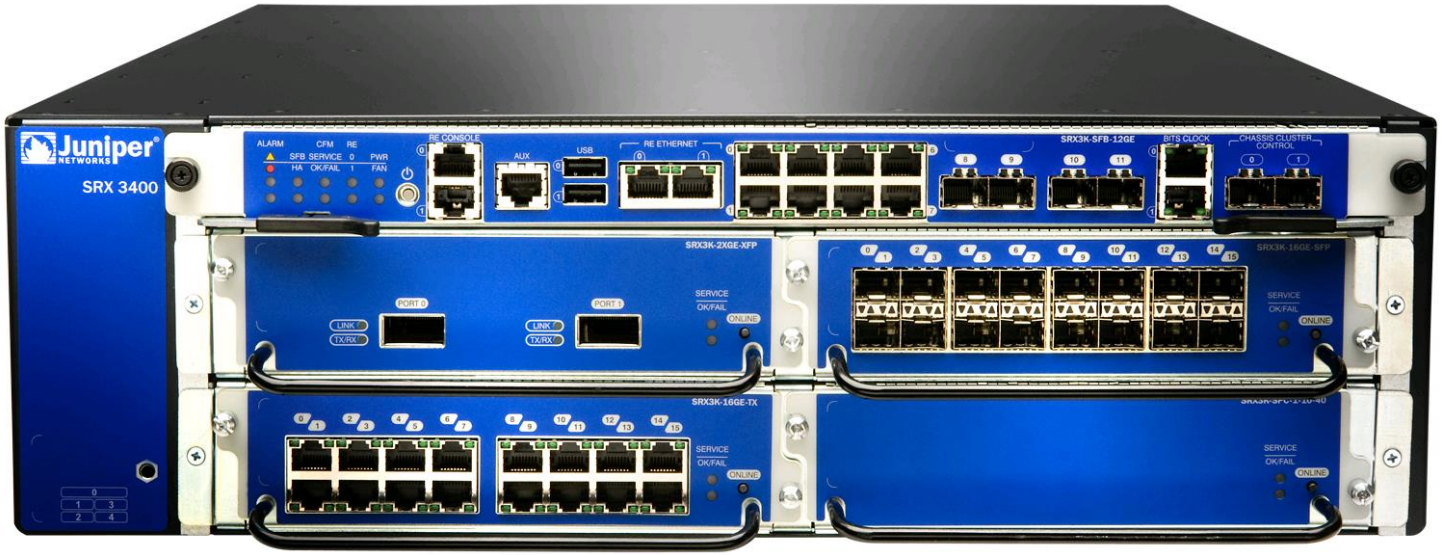
Switch

Redes y Sistemas Operativos: conceptos



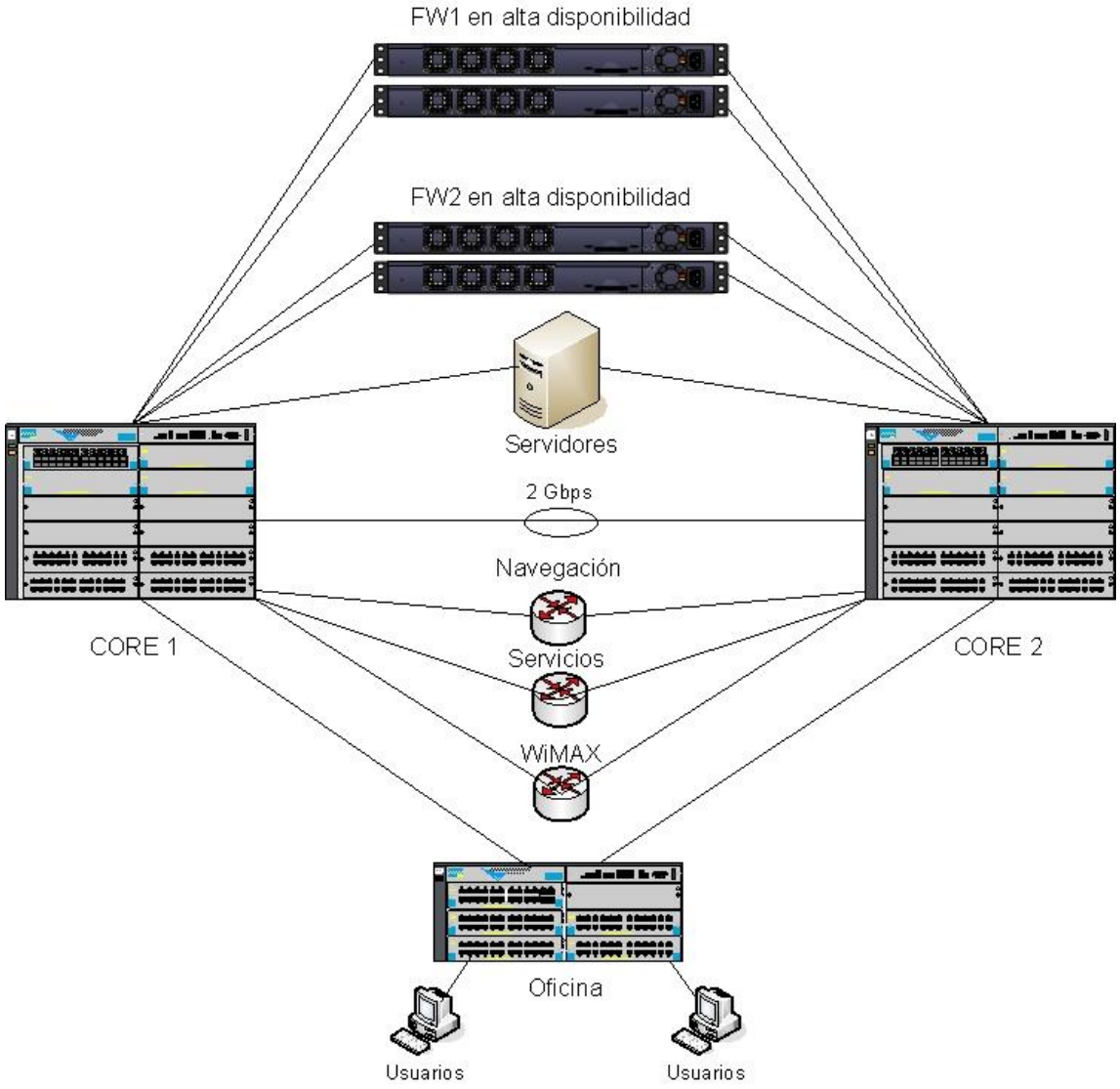
Redes y Sistemas Operativos: conceptos

Elementos básicos: Router y Firewall



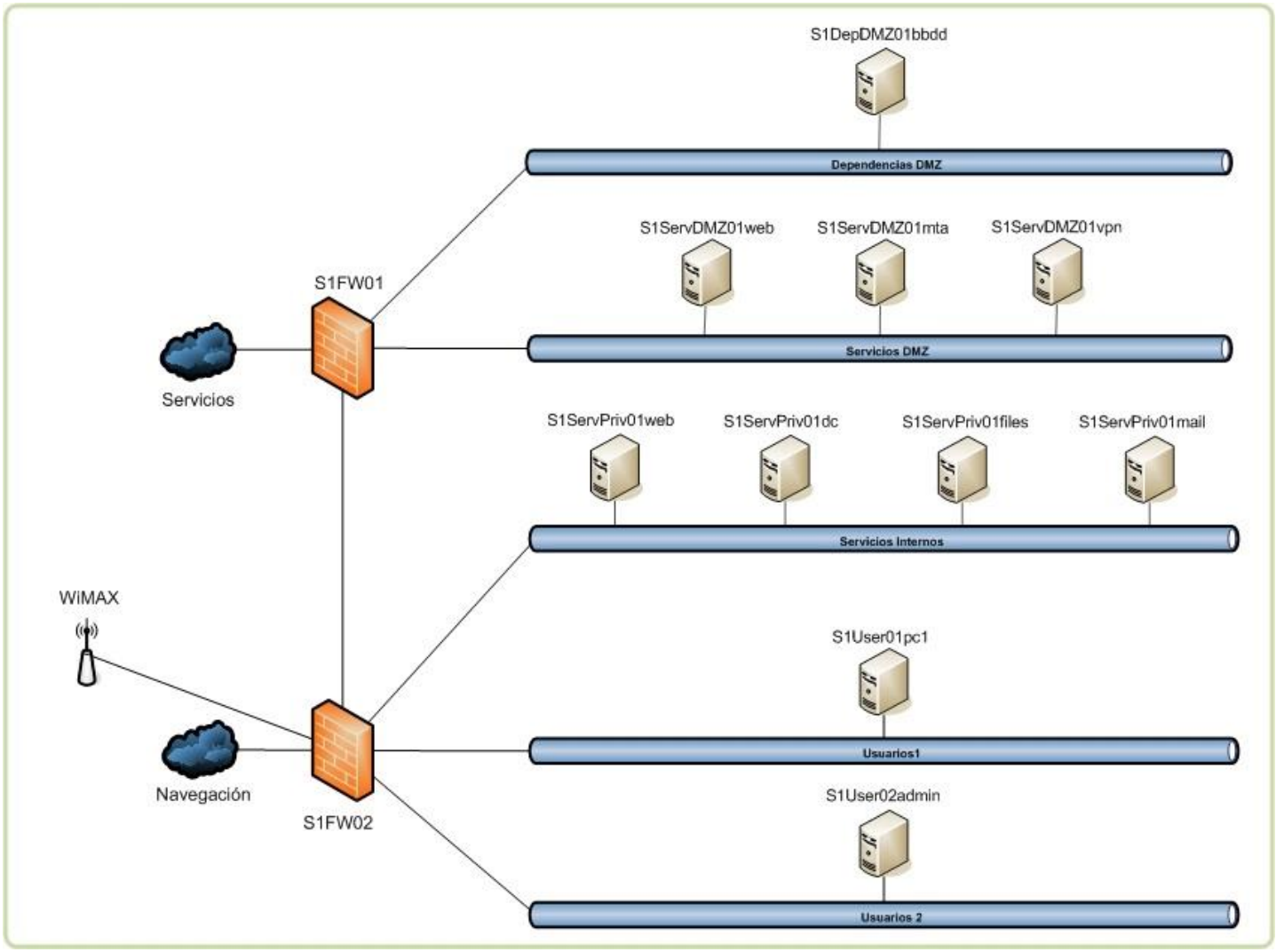
Redes y Sistemas Operativos: conceptos

Esquema físico de una red de servicios



Redes y Sistemas Operativos

Esquema lógico de una red de servicios



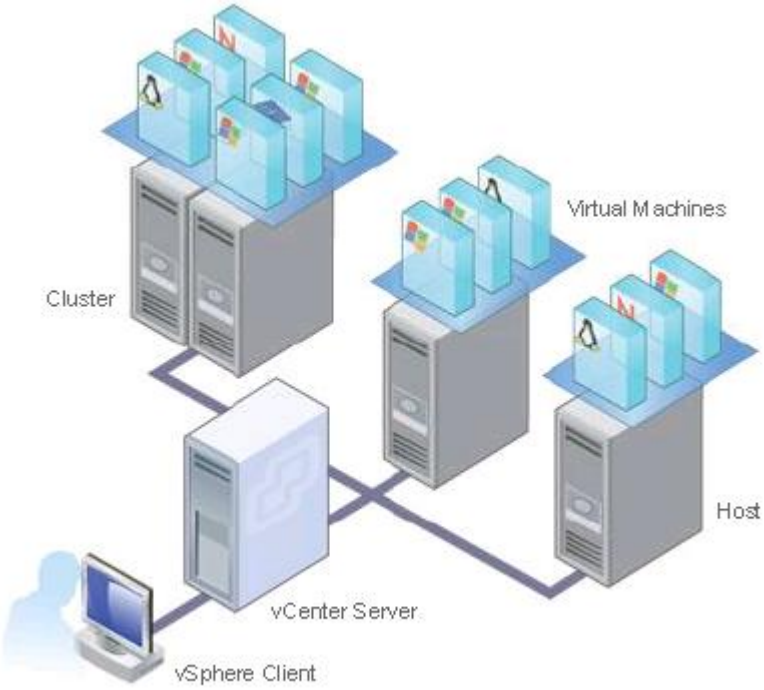
Redes y Sistemas Operativos

Sistemas Operativos

solaris™

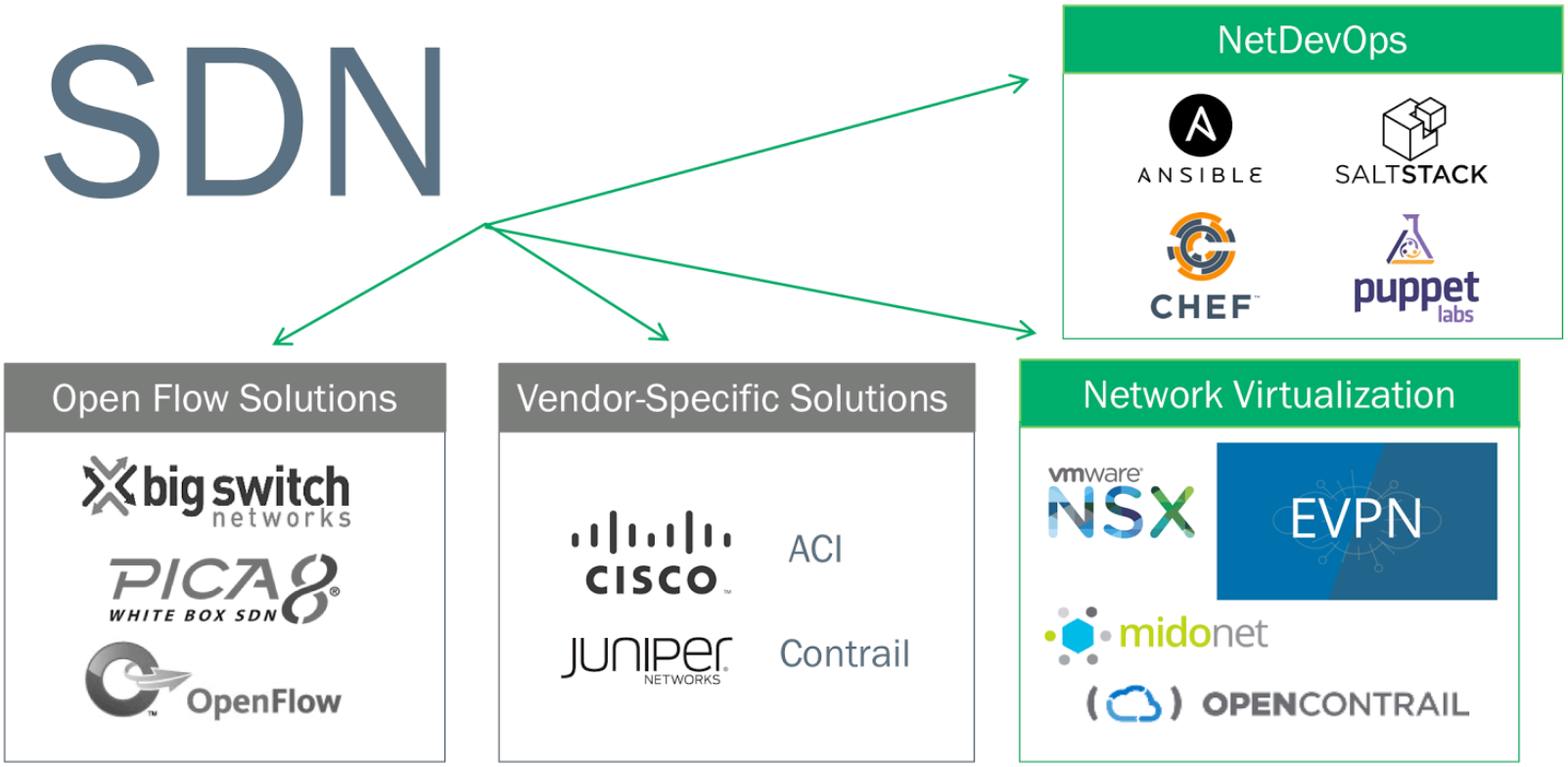
Mundo real vs Virtual

Virtualización de servidores



Mundo real vs Virtual

Virtualización de redes – Redes definidas por software



Cloud Pública y Privada

¿Qué es la nube?

Nube pública

Microsoft Azure

amazon web services™

Google Cloud Platform

MIRANTIS

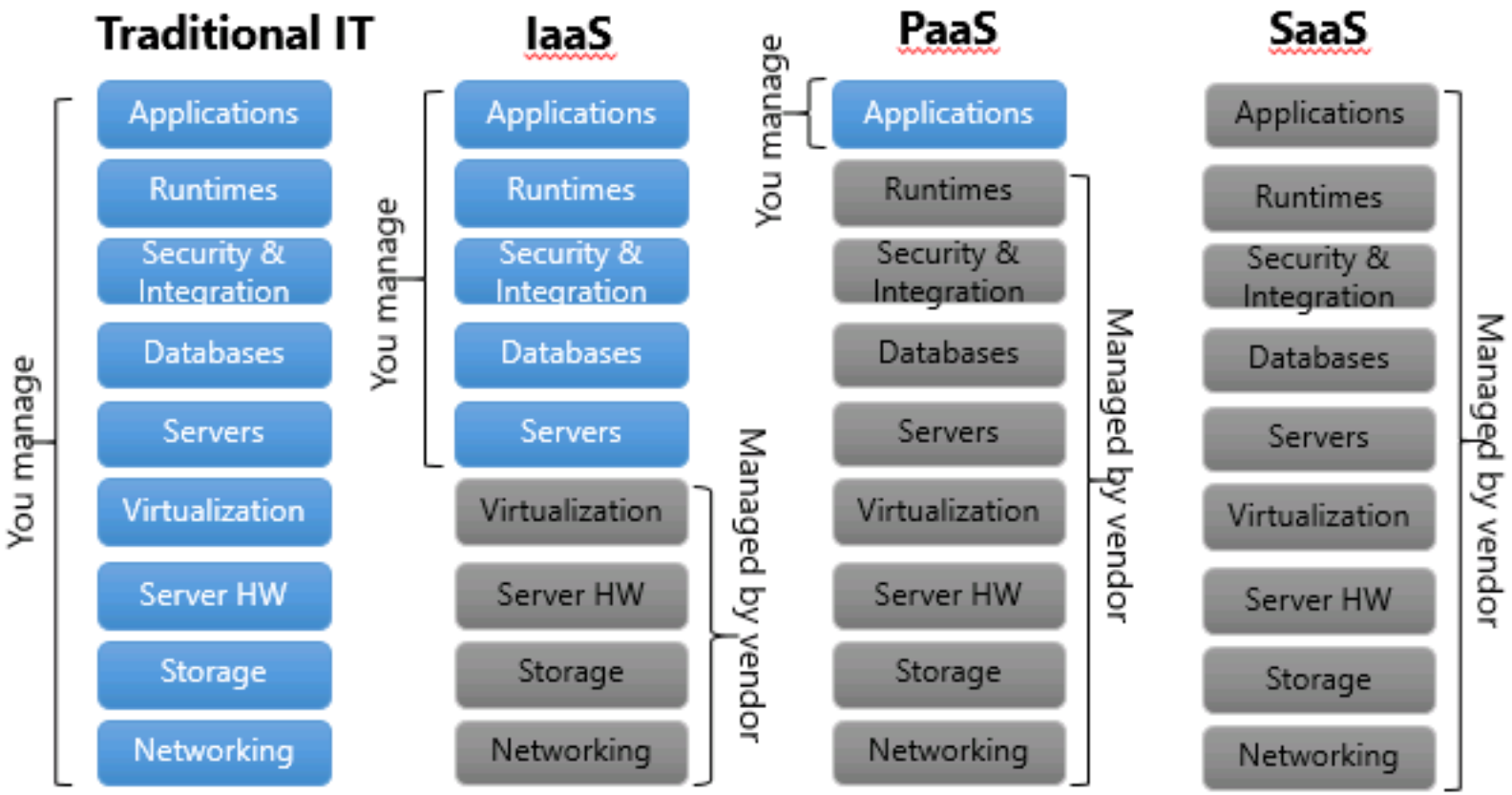
Nube privada

openstack™ CLOUD SOFTWARE

vmware vCloud Air Network

OpenNebula.org The Open Source Toolkit for Cloud Computing

Cloud Pública y Privada



Tratamiento de la información

Big Data

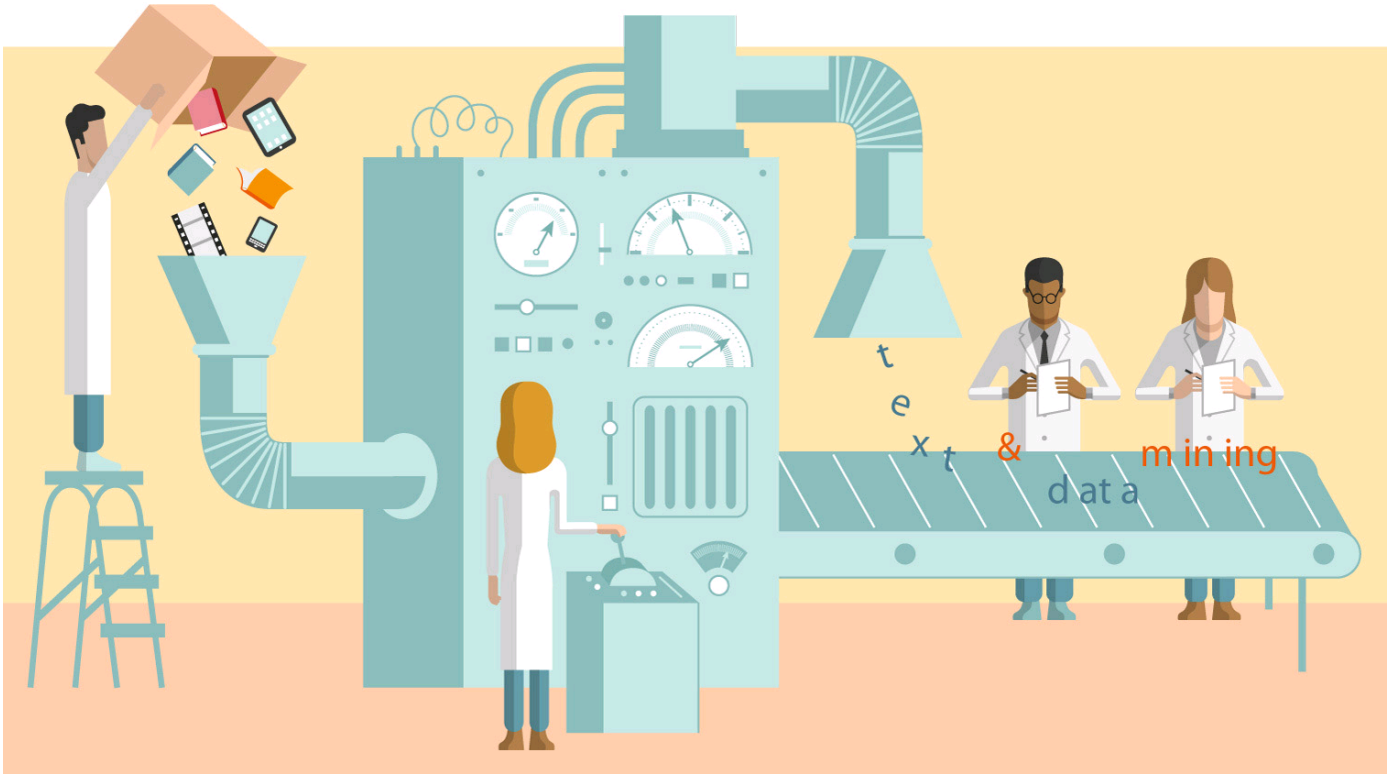
Predicción del Lenguaje Natural

Indicadores de compromiso

Data mining

Inteligencia Artificial

Business Inteligence



¿Qué tienen en común?

¿Qué tienen en común?

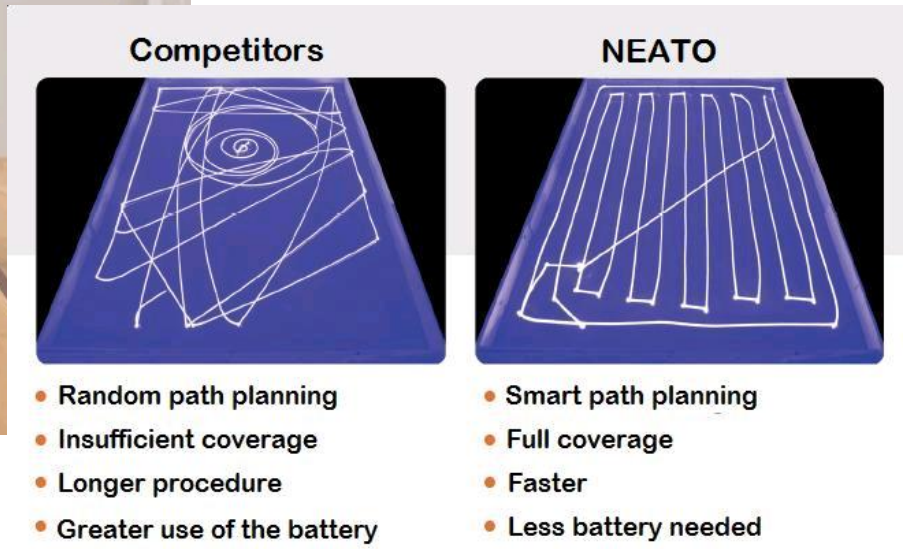
Todos están conectados

Retos

¿Somos conscientes de los riesgos?

Retos

¿Somos conscientes de los riesgos?



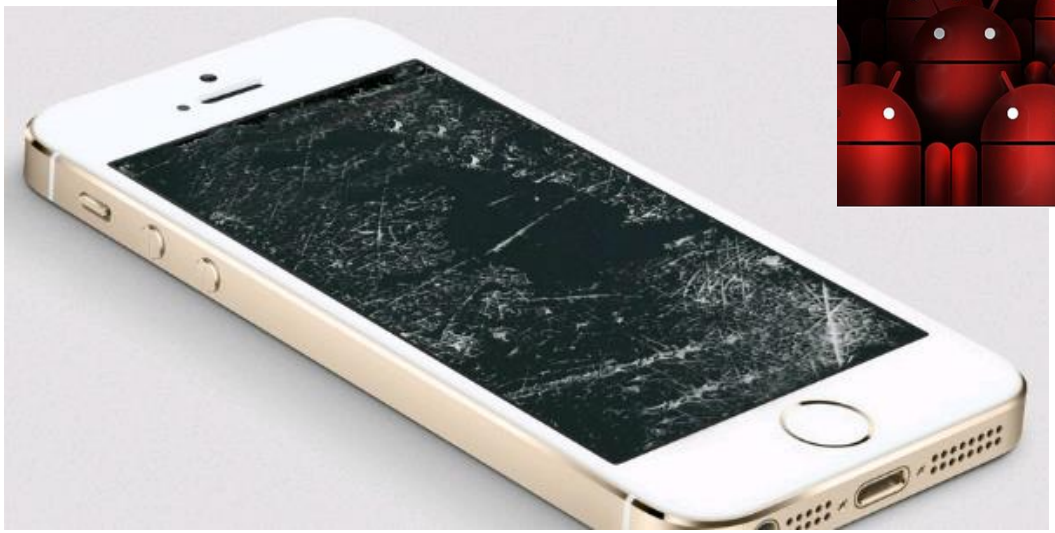
https://youtu.be/3GMNe1GLKvg?t=113

Retos

¿Somos conscientes de los riesgos?

Retos

¿Realmente Somos conscientes de los riesgos?



¿Cuántos de vosotros tiene su Smartphone protegido?

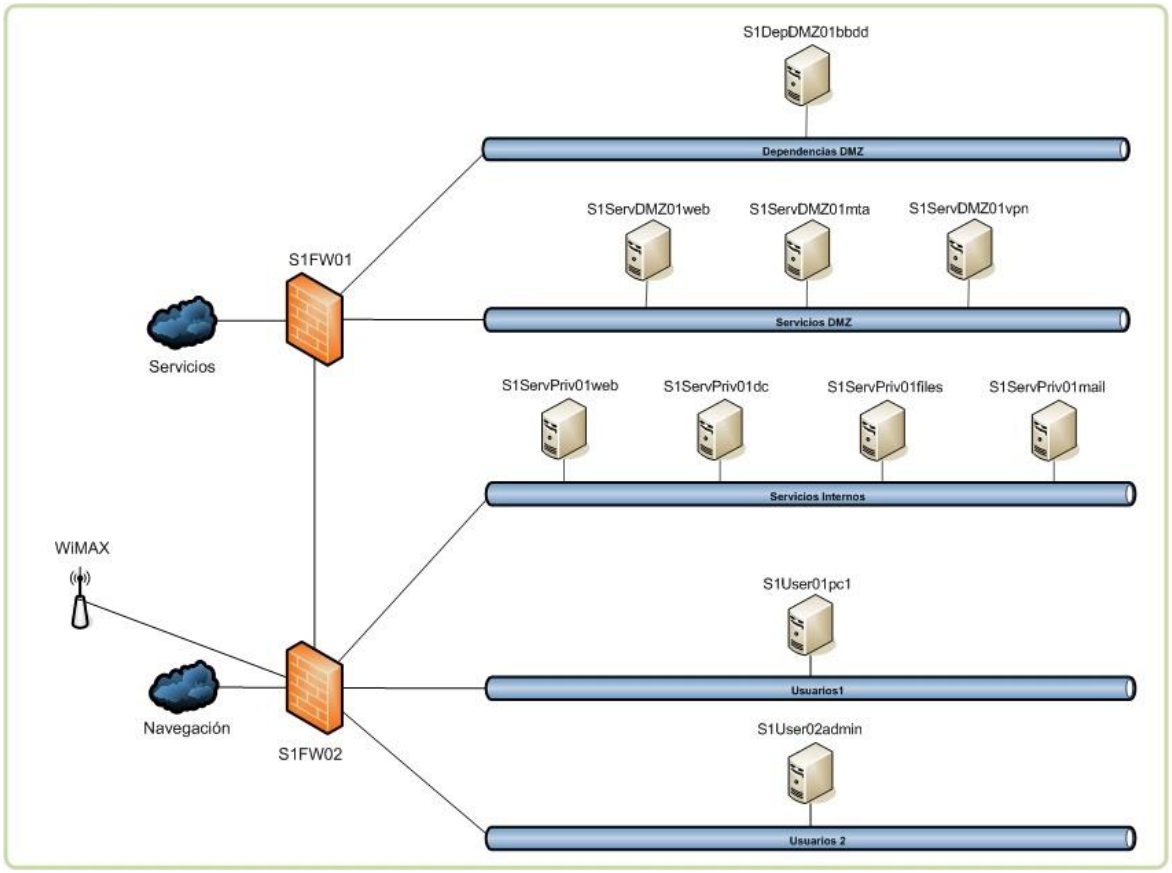
Riesgos y vectores de ataque en la red interna

Riesgos y vectores de ataque en la red interna

Breve recordatorio: modelo OSI

Riesgos y vectores de ataque en la red interna

Conoce tu modelo de red



Riesgos y vectores de ataque en la red interna

1. Denegación de servicio

Existen diversas técnicas que permiten a un atacante causar una baja o denegación del servicio prestado. Una denegación de servicio puede causar graves daños, tanto a nivel de imagen como a nivel operativo, en una organización. La práctica habitual es realizar un **bloqueo de comunicaciones** o un **bloqueo de servicios.**

Riesgos y vectores de ataque en la red interna

2. Seguridad en las comunicaciones

Una **comunicación insegura** es aquella por la que viaja información de carácter sensible y que no dispone de los mecanismos de cifrado necesarios para que no pueda ser interpretada por un sujeto diferente del emisor o receptor. **El cifrado** de las comunicaciones **supone un coste**, tanto en aumento de ancho de banda como en carga de proceso, por tanto debe aplicarse en las ocasiones en que sea necesario. Asimismo, debe garantizar **integridad** y **autenticidad** en las comunicaciones.

Entre los diferentes protocolos y técnicas de cifrado de comunicaciones, caben destacar dos tipos fundamentales que afectan a una red telemática de prestación de servicios. Ambos son complementarios: **cifrado extremo a extremo** y **cifrado de servicio**.

Riesgos y vectores de ataque en la red interna

3. Tráfico no autorizado

¿Qué es el tráfico no autorizado?
¿Es importante?

Riesgos y vectores de ataque en la red interna

3. Tráfico no autorizado

Existen diferentes motivos por los que un determinado tráfico o acceso puede no estar permitido en una red telemática. Esto depende de numerosos factores, entre los que destacan los siguientes:

-**Políticas de uso de la red**: el propietario puede decidir que en su infraestructura deben utilizarse sólo aquellos servicios y recursos que él considera necesarios.

-**Acceso a contenido malicioso**: el usuario puede acceder a servicios maliciosos y ser infectado por un malware que realice cualquier actividad perjudicial.

-**Ataque dirigido**: un equipo de usuario infectado puede formar parte de una red Botnet, o red de equipos zombie, y ser utilizado para atacar a un tercero sin conocimiento de la organización.

-**Acceso a información no autorizada**: intrusión externa, empleado desleal, etc.

Riesgos y vectores de ataque en la red interna

4. Movimientos laterales

Son aquellos producidos entre máquinas pertenecientes al mismo segmento de red y que, por lo tanto, no están separadas por ningún cortafuegos. El origen puede ser:

-**Externo**: un atacante malicioso que ha conseguido acceso a una máquina que utiliza como salto lateral en la red.

-**Interno**: un usuario de la organización con acceso lógico a ese segmento de red.

Riesgos y vectores de ataque en la red interna

5. Fuga de información

Desde el punto de vista de red, se trata de un tipo de tráfico no autorizado. Sin embargo, debido a su relevancia, merece un punto dedicado.

La fuga de información a través de la red supone uno de los mayores riesgos en la corporación y, de nuevo, puede producirse por un atacante externo o por un usuario interno.

Riesgos y vectores de ataque en la red interna

6. Seguridad física

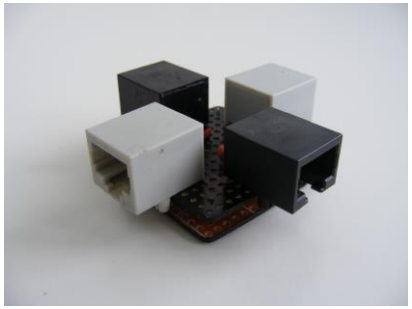
Los ataques a la infraestructura física de red son producidos por un inadecuado aislamiento de los componentes.

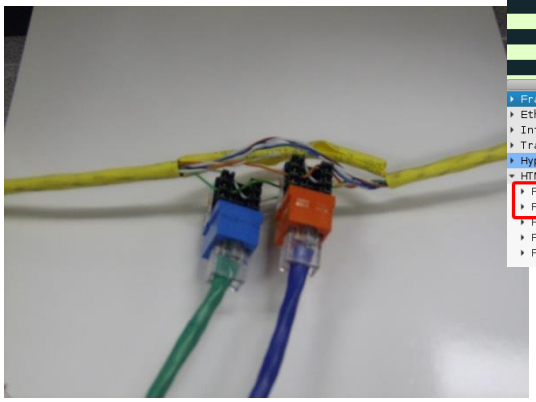
Conexión de equipos no autorizados

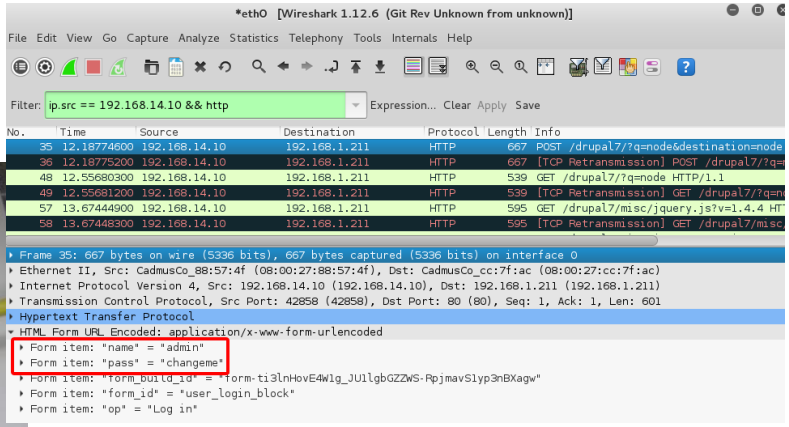
Riesgos y vectores de ataque en la red interna

6. Seguridad física

Sabotaje de elementos de red





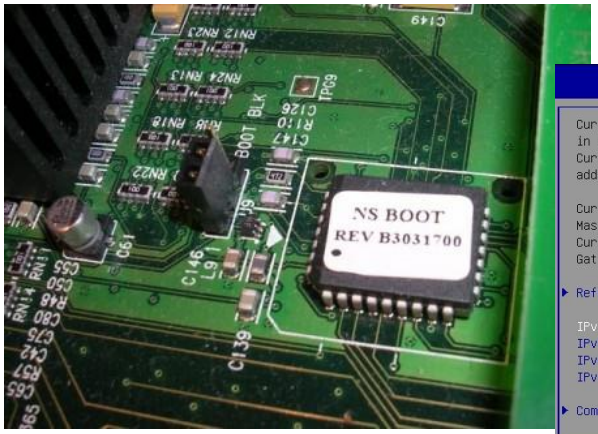


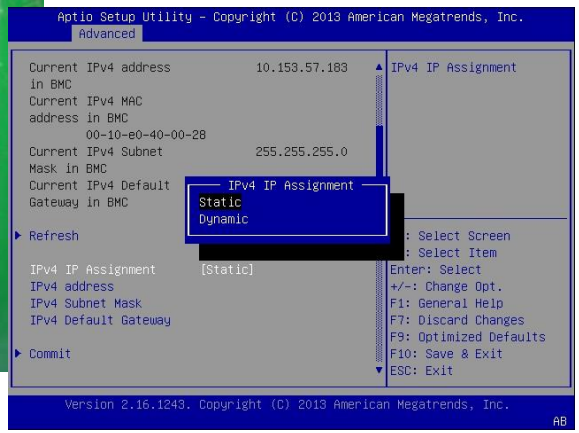
¡Ojo a las emisiones electromagnéticas!

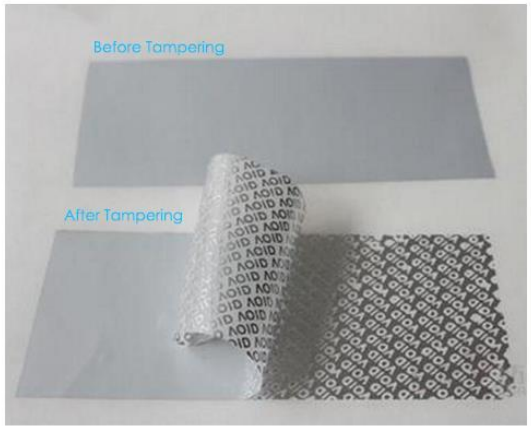
Riesgos y vectores de ataque en la red interna

6. Seguridad física

Sabotaje de dispositivos





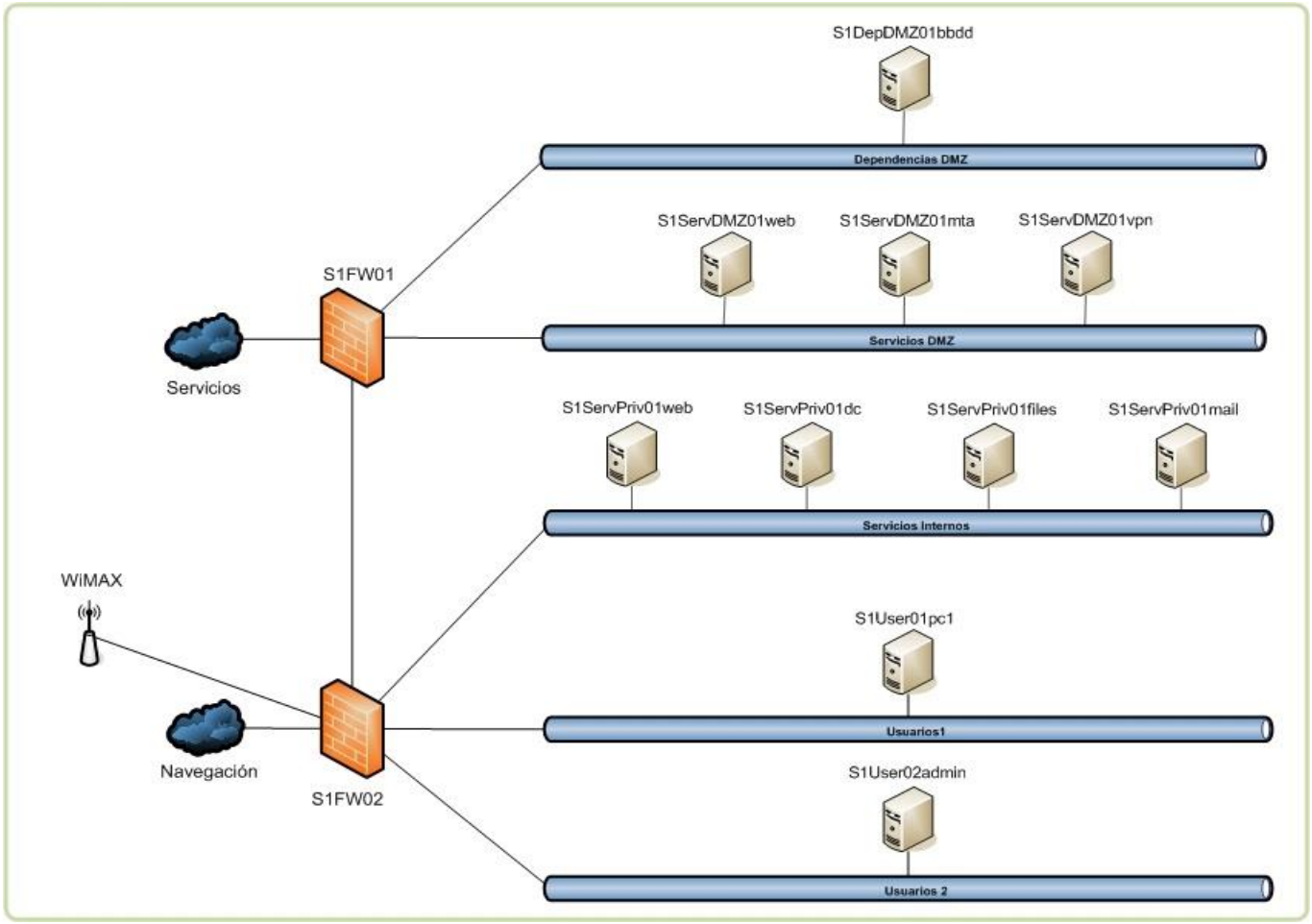


Seguridad por diseño

¿Necesito seguridad? La importancia de un análisis de riesgos

Seguridad por diseño

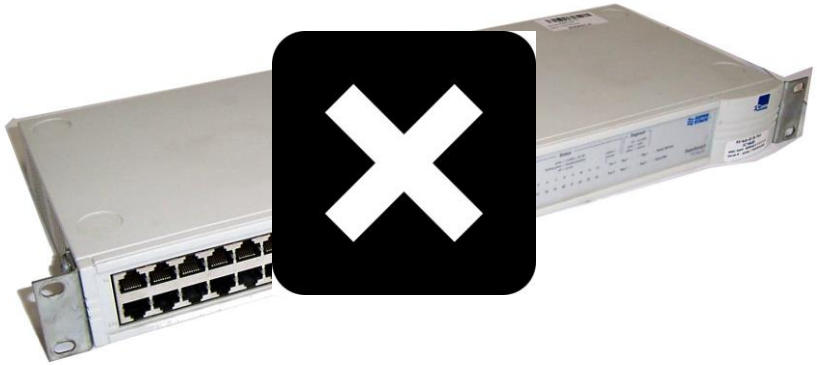
Red segmentada



Seguridad por diseño

Descartar elementos inseguros por defecto:

Switch



HUB

Seguridad por diseño

Características mínimas de seguridad en electrónica de red

-**Redundancia de todos sus componentes**
-**Soporte de fabricante**
-**Control de colas de tráfico**
-**Puertos de port mirror suficientes o uso de TAPs**
-**DHCP Snooping**
-**DAI**
-**IP Source Guard**
-**STP root guard**
-**VLAN privadas**
-**Aplicación de reglas de filtrado entre hosts (ACLs)**
-**Protección contra tormentas de broadcast**
-**Integración con solución NAC**
-**Seguridad puerto/MAC**

Seguridad por diseño

Si se utiliza enrutamiento no filtrado…

El enrutamiento permite comunicar redes diferentes entre sí a través de uno o varios routers.

¿Diferencia entre router y cortafuegos?

Buenas prácticas de seguridad en el enrutado:

-**Enrutamiento estático, en la medida de lo posible.**
-**Evitar NAT entre redes internas, en la medida de lo posible.**
-**No enrutar tráfico multi destino y de protocolos innecesarios por defecto.**
-**Evitar el enrutamiento en switch capa 3, en la medida de lo posible.**

Seguridad por diseño

Si se utiliza enrutamiento filtrado en capas 3/4…

El enrutamiento filtrado, normalmente a través de cortafuegos, permite comunicar redes diferentes entre sí permitiendo sólo el tráfico deseado.

Buenas prácticas de seguridad en enrutamiento filtrado básico L4:

- **Política de bloqueo por defecto.**
- **Restringir lo máximo posible: IP, protocolo L4 y puerto, si procede.**
- **Aplicar reglas de bloqueo de tráfico mal formado, etc.**

No podemos hacer mucho más. Los cortafuegos L4 son insuficientes.

Seguridad por diseño

Interconexión entre entornos

Entorno confiable:

Aquel controlado que cumple con los mecanismos de seguridad y procesos implantados. Normalmente se trata del entorno productivo.

Entorno no confiable:

Aquel controlado sólo parcialmente o no controlado, donde existen máquinas, redes o servicios que pueden suponer un riesgo para el entorno productivo. Ejemplo: accesos externos, entornos de desarrollo, laboratorios, pruebas, etc.

¿Cómo interconectar un entorno confiable con uno no confiable?

Desde máquinas de salto hasta diodos de datos

Seguridad por diseño

Operación y administración de servicios

La administración y operación de las redes y servicios es un reto desde el punto de vista de la seguridad.

- **Redes paralelas para Backup, NAS y cualquier otro acceso sin enrutamiento (!)**
- **Ojo con la dirección de la conexión (!)**

Seguridad por diseño

Un diseño seguro supone un gran ahorro de costes

Algunos elementos recomendados de protección en red

Algunos elementos recomendados

Conceptos previos

Dispositivos fuera de banda:

- **Port Mirror**
- **Tap**
- **…**

Dispositivos en línea:

- **Capa 2**
- **Capa 3 (4,7)**
- **Cualquier dispositivo intermedio**

Algunos elementos recomendados

Nada nuevo:

- **IDS**
- **IPS**
- **NAC**
- **Proxy de navegación**
- **Proxy inverso / Balanceador**
- **Firewall L7**

¿Dónde está el límite entre protección de red y protección de servicios?

- **WAF**
- **DBF**
- **Endpoint**
- **PAM**
- **SIEM**
- **…**

Hagamos un buen diseño, una buena parametrización y utilicemos sólo lo necesario

Algunos elementos recomendados

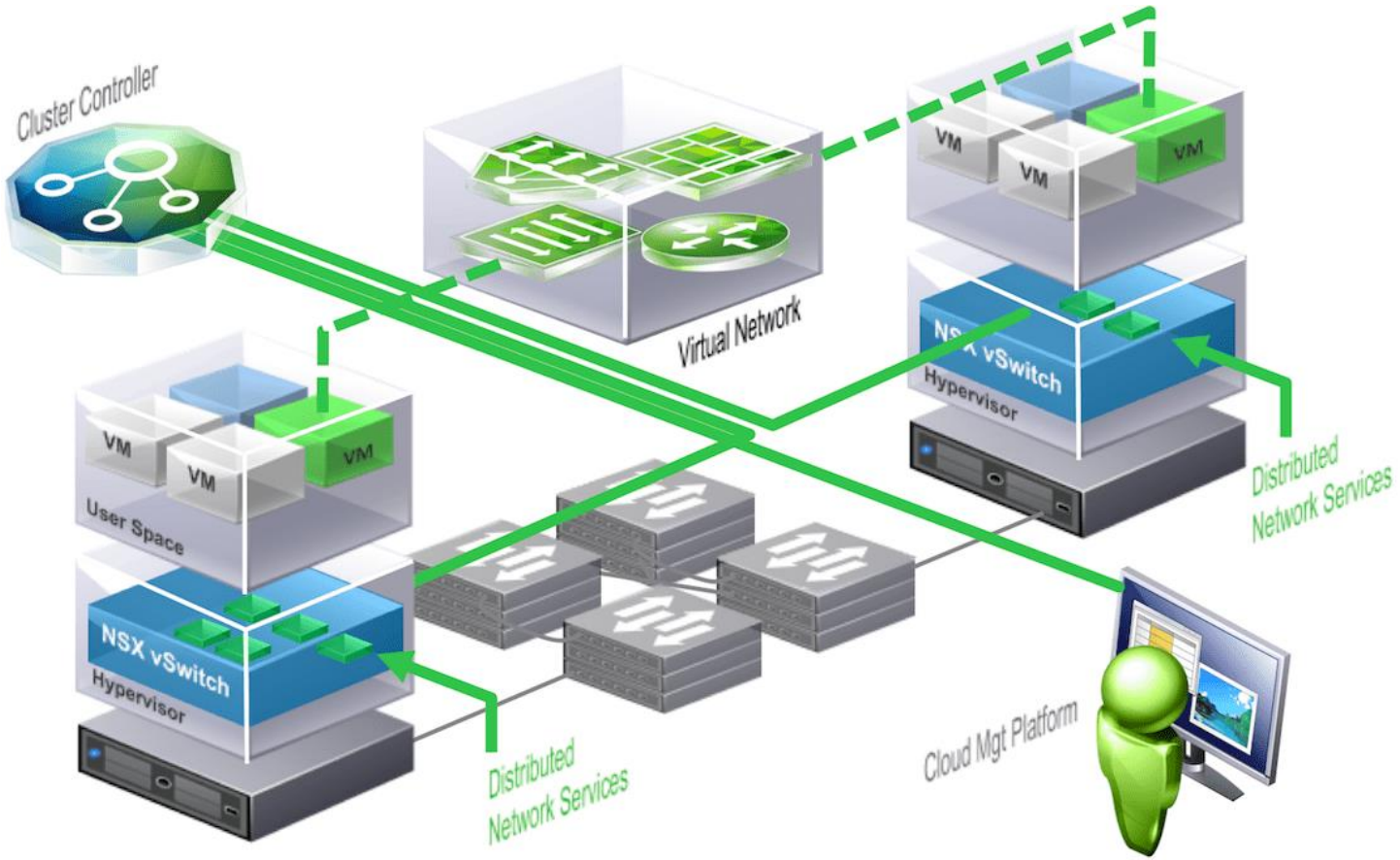
Mención especial para los dispositivos en capa 7

- **Es “imprescindible” trabajar en capa 7**
- **Permite analizar tráfico a nivel de aplicación**
- **Se puede aplicar a cualquier modo: enrutado, bridge, port mirror, etc**
- **Garantiza, en la medida de lo posible, que el tráfico es el esperado**

¡Ojo con el tráfico cifrado!

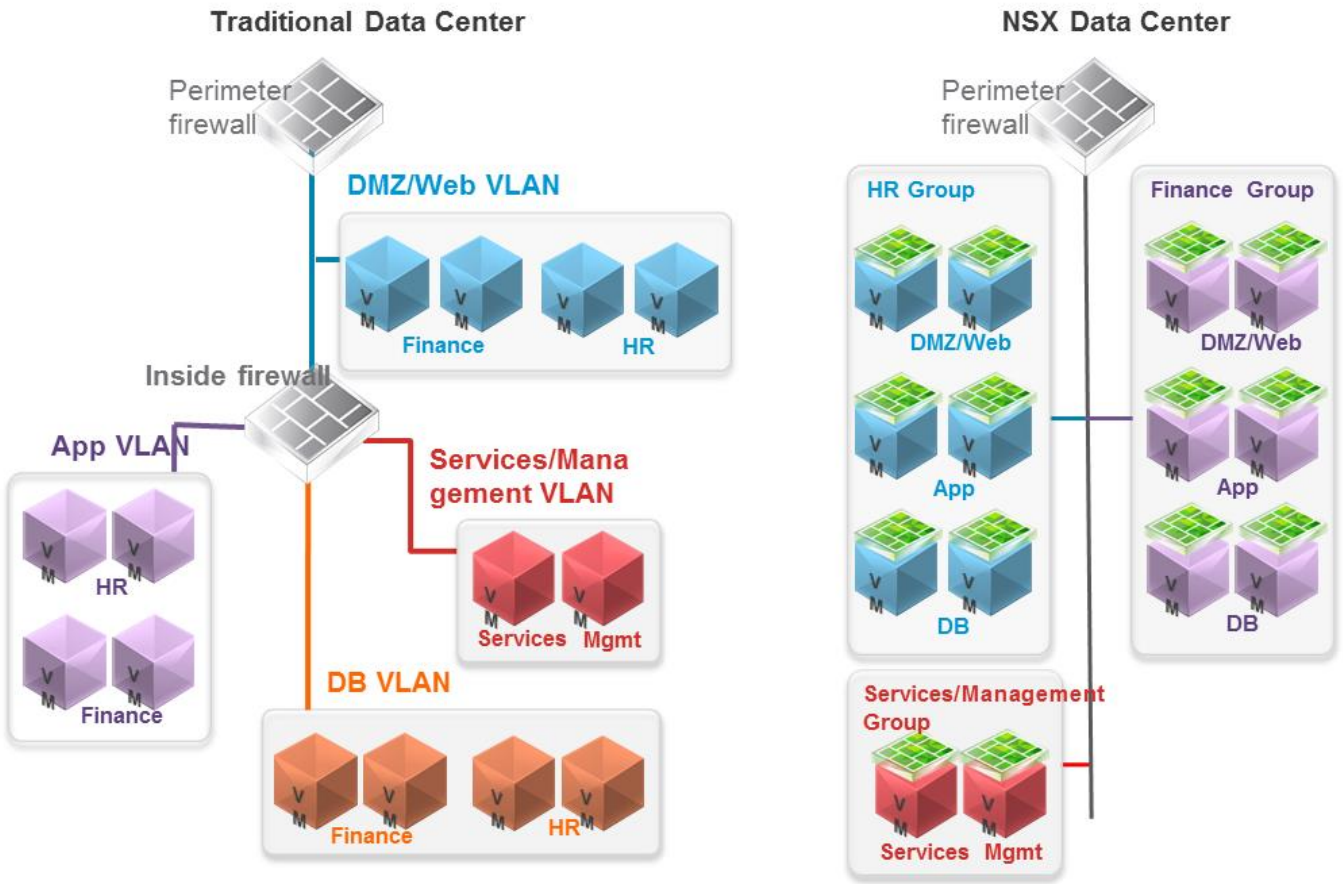
Algunos elementos recomendados

Mención especial para las redes SDN y Microsegmentación: L2~L3



Algunos elementos recomendados

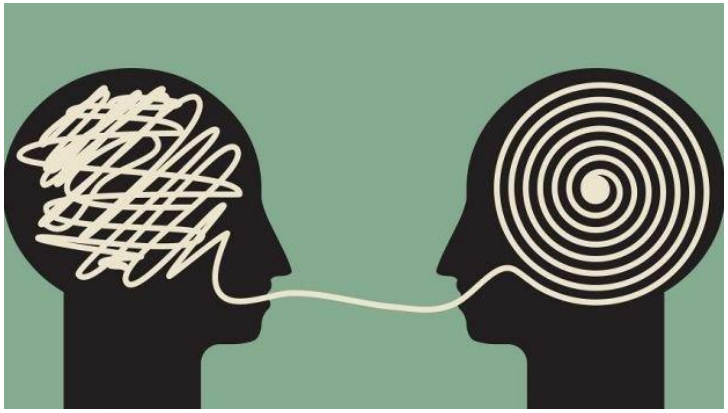
Mención especial para las redes SDN y Microsegmentación: L2 ~ L3



¿Y la GDPR?

Recomendaciones

- **Asesorarse sobre el tipo de dato a proteger**
- **Realizar un análisis de riesgos**
- **Ser conscientes de las amenazas existentes**
- **Estudiar los marcos regulatorios y condiciones de los proveedores Cloud**
- **Aplicar los mecanismos de bastionado y diseño oportunos**
- **Garantizar el mantenimiento y mejora continua de todos los sistemas**
- **De momento, no existe ninguna certificación específica oficial, pero es recomendable aplicar, al menos, ISO27002 (SGSI) e ISO27701 (Privacidad)**
- **Contar con un equipo jurídico especializado**



Retos y conclusiones generales

- **Introducir la seguridad en el proceso de diseño.**
- **Asumir la seguridad como parte de nuestra responsabilidad.**
- **Comprender y aplicar los marcos regulatorios vigentes.**
- **Convertir la regulación en oportunidad.**
- **No nos debemos conformar con el “check”. Aplicar el *ingenio*.**

Retos y conclusiones

Tenemos un enorme y bonito reto por delante :-)

Muchas gracias.

Jesus.feliz@incibe.es

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

Fuente de imágenes y derechos de autor

- Diapositivas 16, 17 y 27: el propio autor
- Resto de imágenes: buscador de imágenes de www.google.es
- Autor: Jesús Feliz Fernández. INCIBE.