SEGURIDAD EN SISTEMAS DISTRIBUIDOS

Jorge Rojas Zordan
Sub Gerente de Innovación y Desarrollo de Productos
jrojasz@novared.net

Agenda

- Evolución de las amenazas de seguridad
- Sistemas Distribuidos y Tendencias de Control
- Modelos de control
- Desafíos para el futuro

De la telaraña a la Nube

- A finales de los ‘90 el mundo vivió el boom de las **punto com**.
- En el 2000, Chile vivió el boom de la **Internet**.
- A finales de la década, el mundo se vuelca a las **redes sociales**.
- En los próximos años los **dispositivos móviles** marcarán otro cambio tecnológico

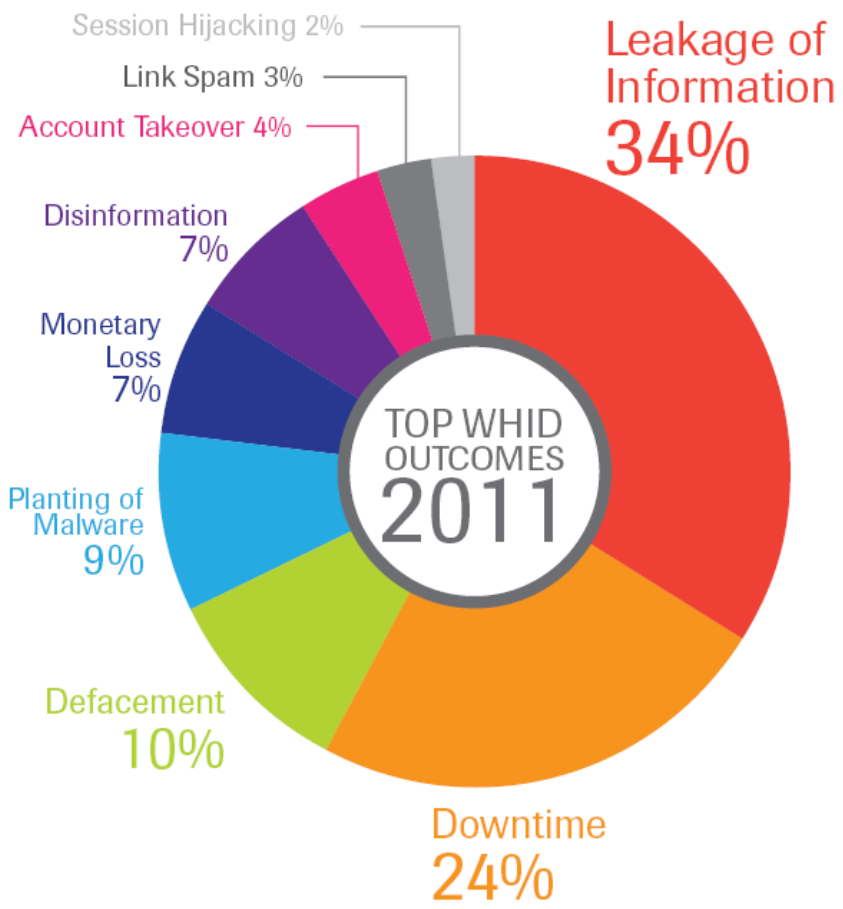
“Cada uno de estos avances nos obliga a pensar en cómo evolucionan los Riesgos”

Las 10 amenazas del 2011

1. Password de administración débiles o en blanco
2. Información sensible transmitida por redes sin encriptación
3. Servidores MS-SQL con password débiles o sin clave
4. Envenenamiento de tablas ARP
5. Acceso a Access Point fraudulentos
6. Uso de encriptación WEP
7. Suplantación de credenciales en proceso de autenticación NTLM
8. Mala configuración de reglas en FW (reglas any)
9. Información sensible almacenada fuera de zonas seguras
10. Información sensible trasmitida vía Bluetooth

Fuente: Trustwave security report 2012

Impactos causados por incidentes de seguridad en el 2011



Fuente: 2012 Verizon Data Breach Report

Confidencialidad

Disponibilidad

Integridad

Seguridad de la Información

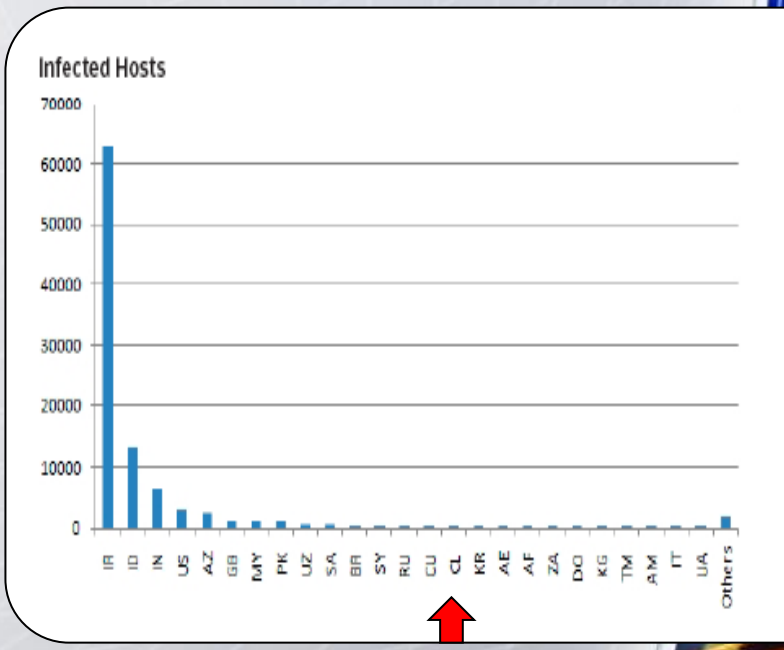
¿Riesgo en Chile?

- **Los riesgos en Chile no difieren de la realidad mundial**

- **Tarde o temprano, los riesgos que vemos en el extranjero llegarán a Chile**

Un ejemplo: Stuxnet

- Virus que ataca los sistemas de control industrial
- Propagación:
  - Dispositivos USB
  - Discos de red compartidos
  - Vulnerabilidad de colas de impresión windows
  - Vulnerabilidad de RPC de windows
  - Mecanismos P2P
- El 29 de Septiembre del 2010:
  - 100.000 host infectados en 155 países
  - Sobre 60.000 host infectados en Irán
  - **1041 host infectados en Chile**



Agenda

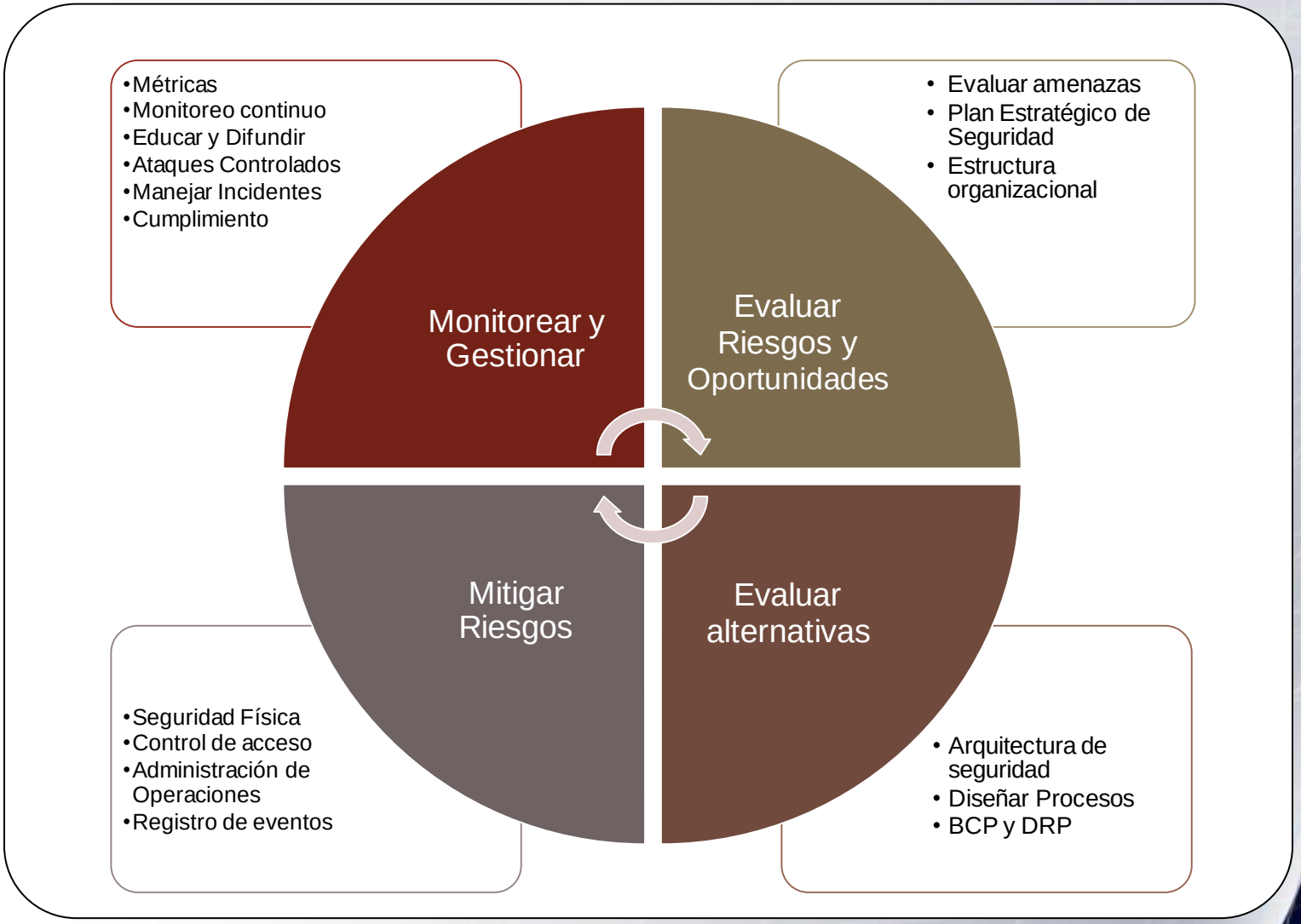
- Evolución de las amenazas de seguridad
- Sistemas Distribuidos y Tendencias de Control
- Modelos de control
- Desafíos para el futuro

Sistemas Distribuidos y Seguridad

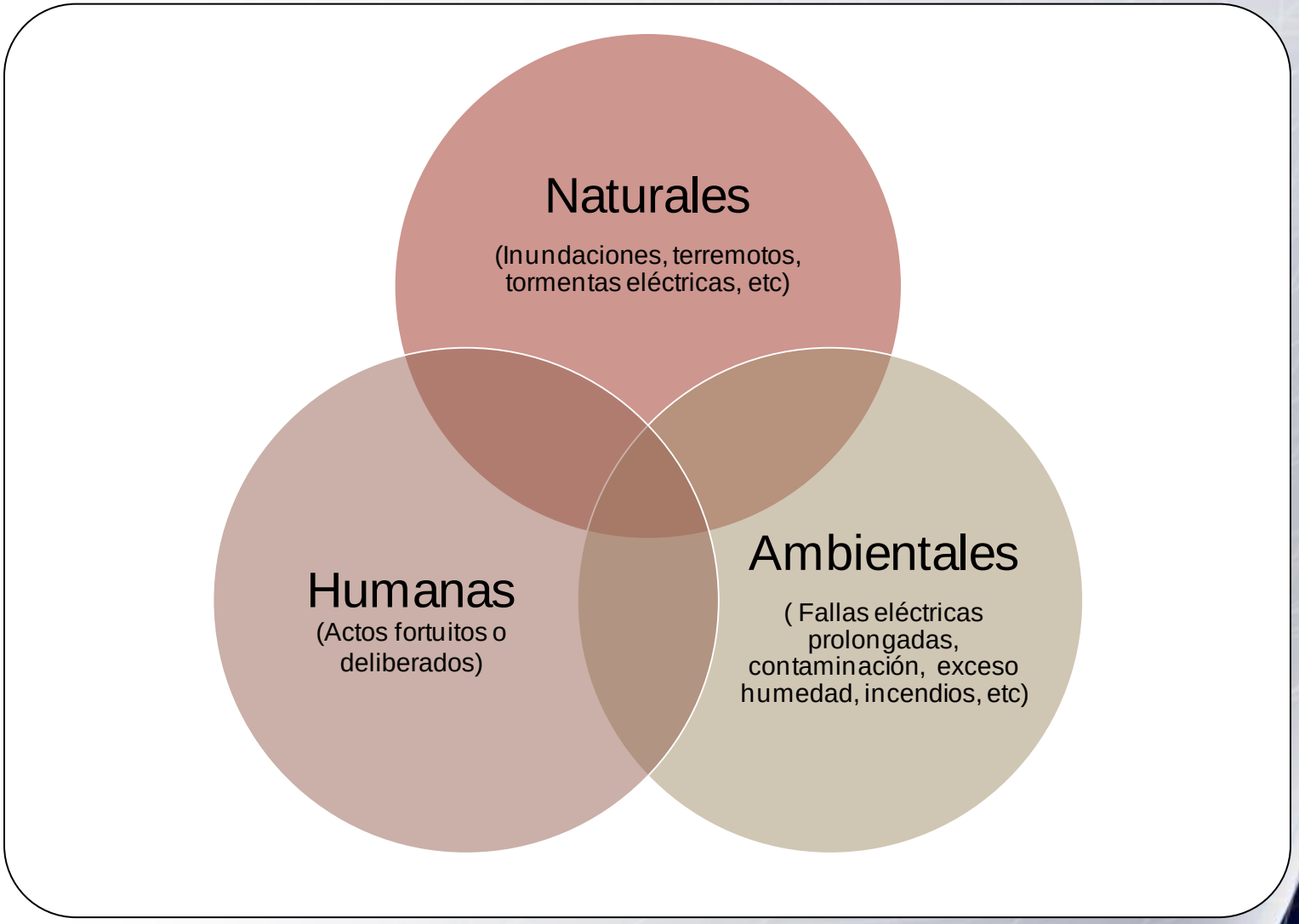
Características:

- Información distribuida en múltiples Datacenter
- Cadena de operación productivas altamente tecnologizada
- Múltiples grupos de usuarios con distintos roles y responsabilidades (internos y externos)
- Necesidad de acceso remoto de usuarios (internos y externos)
- La Red es un punto neurálgico de todo el sistema

La administración del riesgo Ti es un proceso continuo



Fuentes de Riesgo

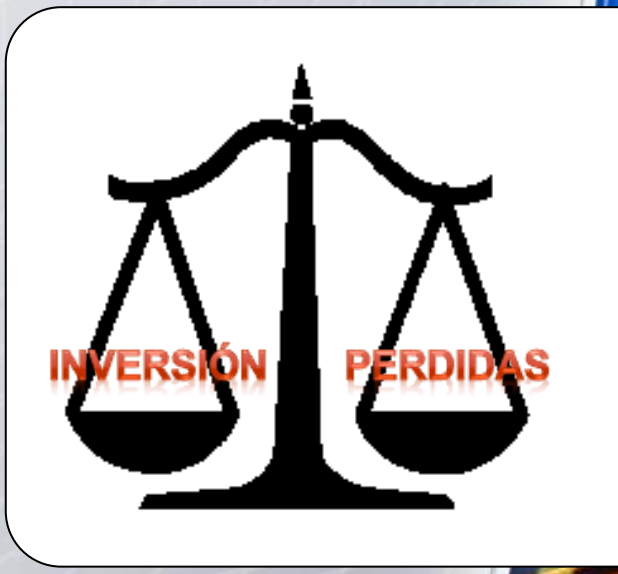


¿Como evaluar el impacto en mi negocio de una amenaza?

Estrategias para abordar el riesgo

Cuidar el balance entre Impacto en el negocio e Inversión en Seguridad

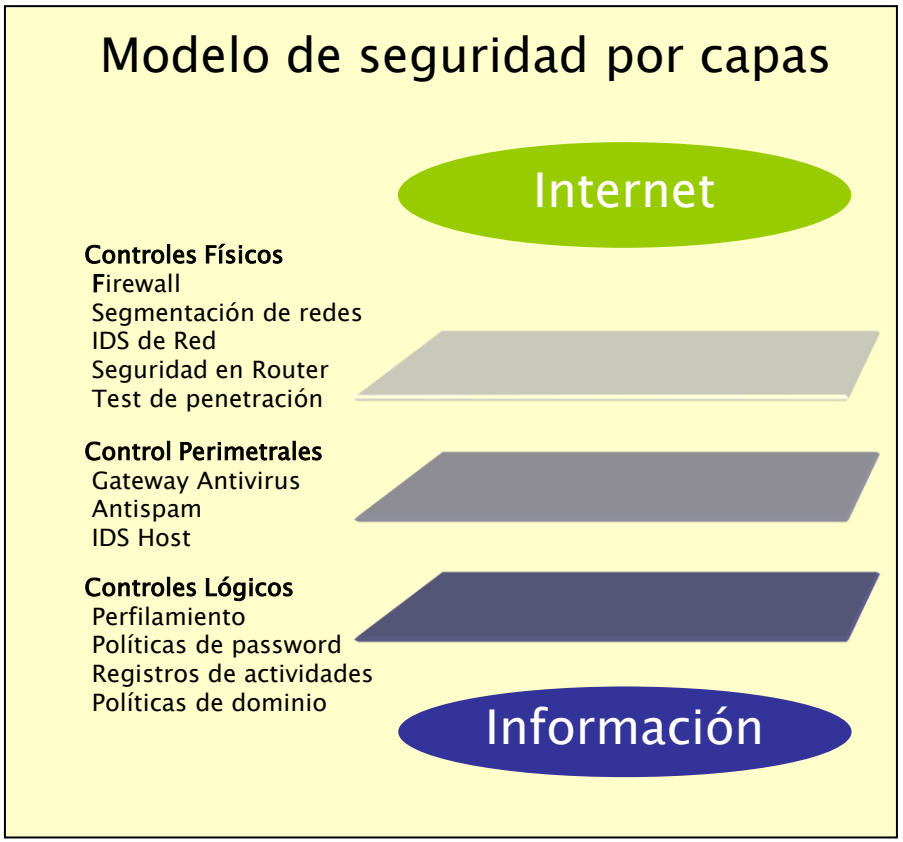
- **Mitigar una amenaza significa reducirla a un nivel aceptable.**
- **Aplicar el principio de Pareto**
  - **El 80% del riesgo puede ser mitigado utilizando 20% de los recursos.**
  - **Focalizarse en los riesgo importantes.**
  - **Esforzarse en mitigar riesgo al menor costo.**
  - **Mínimo impacto para el negocio.**
- **Evaluar múltiples alternativas y elegir la mejor**
- **En ciertas ocasiones un control compensatorio vale más que un control mitigador.**



Mitigar un riesgo implica mucho más que implementar una herramienta.

- **Implementar un control, significa:**
  - **Establecer una política o norma.**
  - **Dar a conocer esa política.**
  - **Establecer un monitoreo efectivo:**
    - **Detectivo**
    - **Preventivo**
  - **Dejar registro de la evidencia.**
  - **Validar la efectividad.**
  - **Buscar retroalimentación**
- **Un control que no deja evidencia, no existe.**

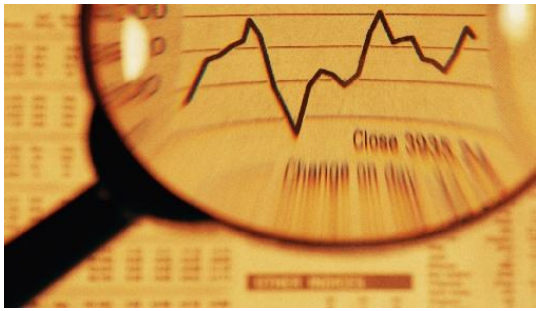
Implementar una estrategia de seguridad por capas

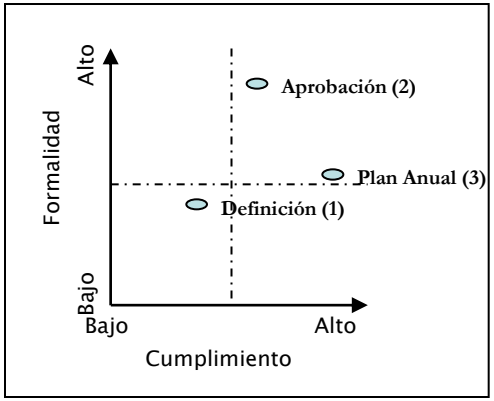


- **Analizar las amenazas desde el perímetro exterior (generalmente Internet) hasta el interior (información crítica).**
- **En cada capa o nivel, agregar controles complementarios a la capa anterior.**
- **Cada capa debe potenciar el nivel anterior.**
- **No debe permitir una conexión desde el perímetro exterior a la capa interna.**

Lo que no se mide, no se puede mejorar

- **¿Por qué necesitamos medir?**
  - **Para verificar el éxito o fracaso de la implementación del control.**
  - **Para mostrar el valor de nuestra labor.**
  - **Para mejorar nuestros objetivos.**
  - **Para predecir el comportamiento de las amenazas.**
  - **Para demostrar cumplimiento frente a reguladores externos y auditores.**





Adoptar un estándar, evita reinventar la rueda

- **Hay varios estándares de seguridad que pueden ayudarnos a establecer un marco de control de riesgo TI.**
  - **COBIT** (Control Objetives for Information and related Technology) recopilado por ISACA.
  - **BS 17.799 o ISO 27.001** (Information Security Management System)
  - **CBK** (Common Body of Knowledge) recopilado por ISC
  - **ITIL** (Information Technology Infrastructure Library) recopilada por el Gobierno Ingles.

Los controles más utilizados en Seguridad TI

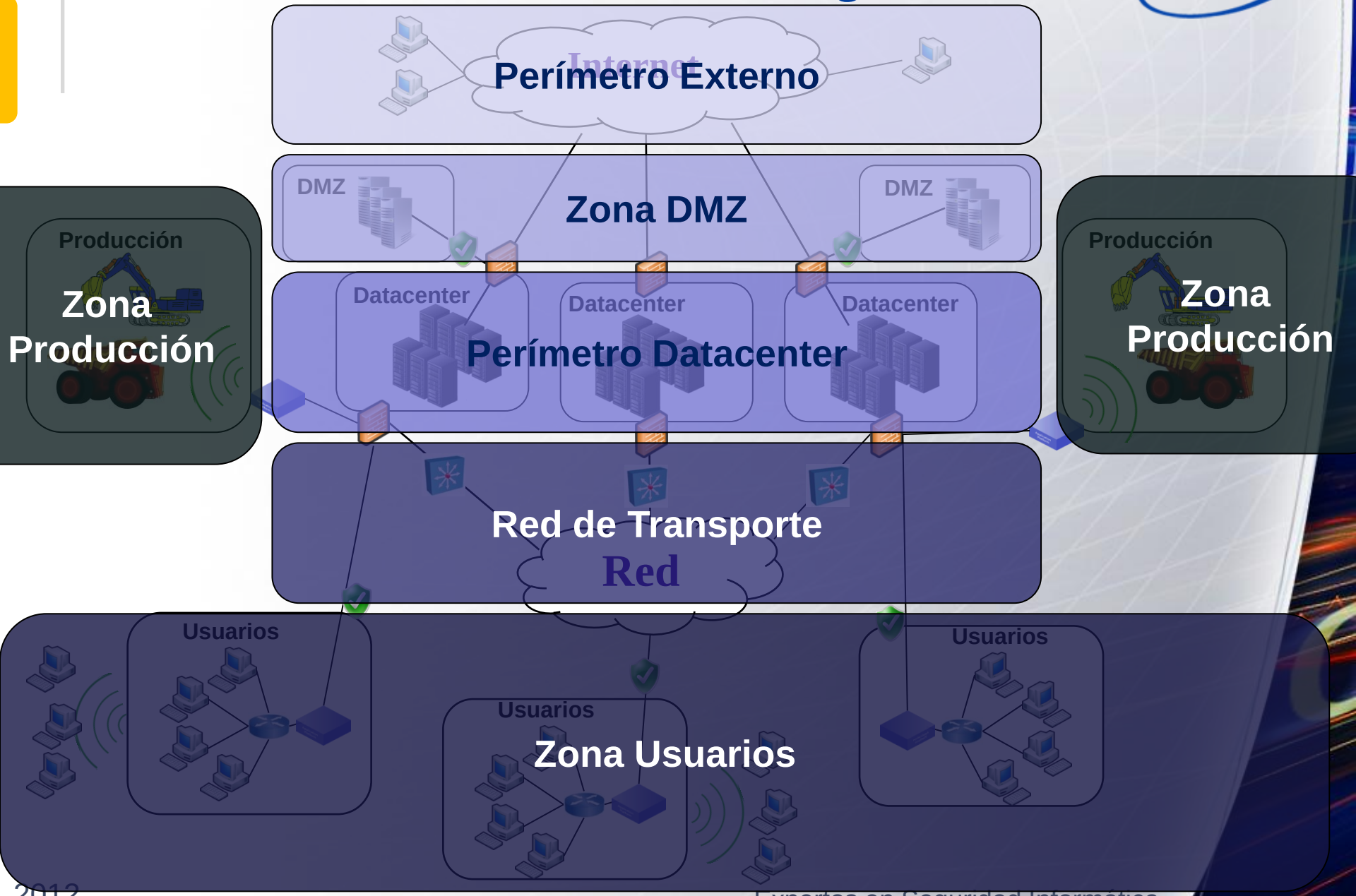
Firewall	94 %
Log de auditoría	83 %
Soluciones anti malware	83 %
Protocolos de seguridad Wireless	82 %
Recuperación de Desastres	78 %
Firma electrónica	69 %
Encriptación de datos (en transmisión)	67 %
Servicios de detección/prevención de intrusos	66 %
Encriptación de E-mail	60 %
Encriptación de datos (en storage)	44 %
Encriptación de dispositivos móviles	39 %
Autenticación por doble factor	33 %
Single sign on	29 %
Infraestructura de llave pública	26 %
Infraestructura DLP	24 %
Biometría	19 %

Fuente: 2009 HIMSS Security Survey

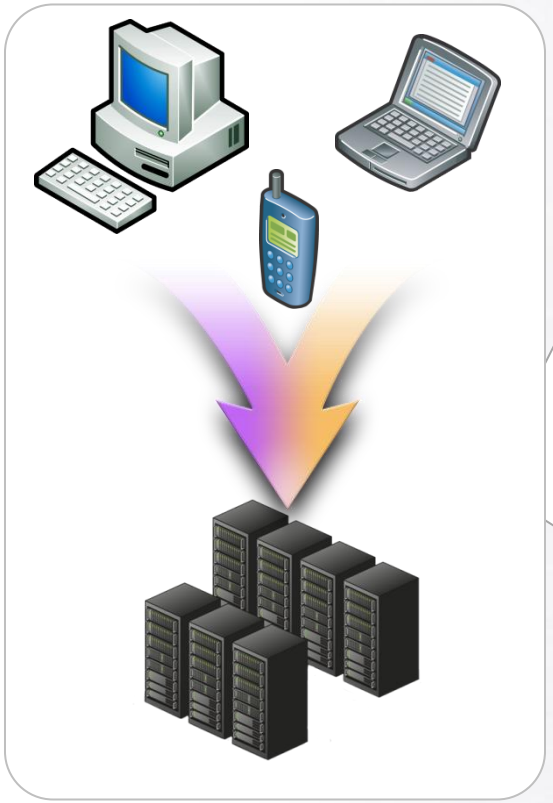
Agenda

- Evolución de las amenazas de seguridad
- Sistemas Distribuidos y Tendencias de Control
- **Modelos de control**
- Desafíos para el futuro

Identificar los Dominios de Seguridad



Perímetro Externo

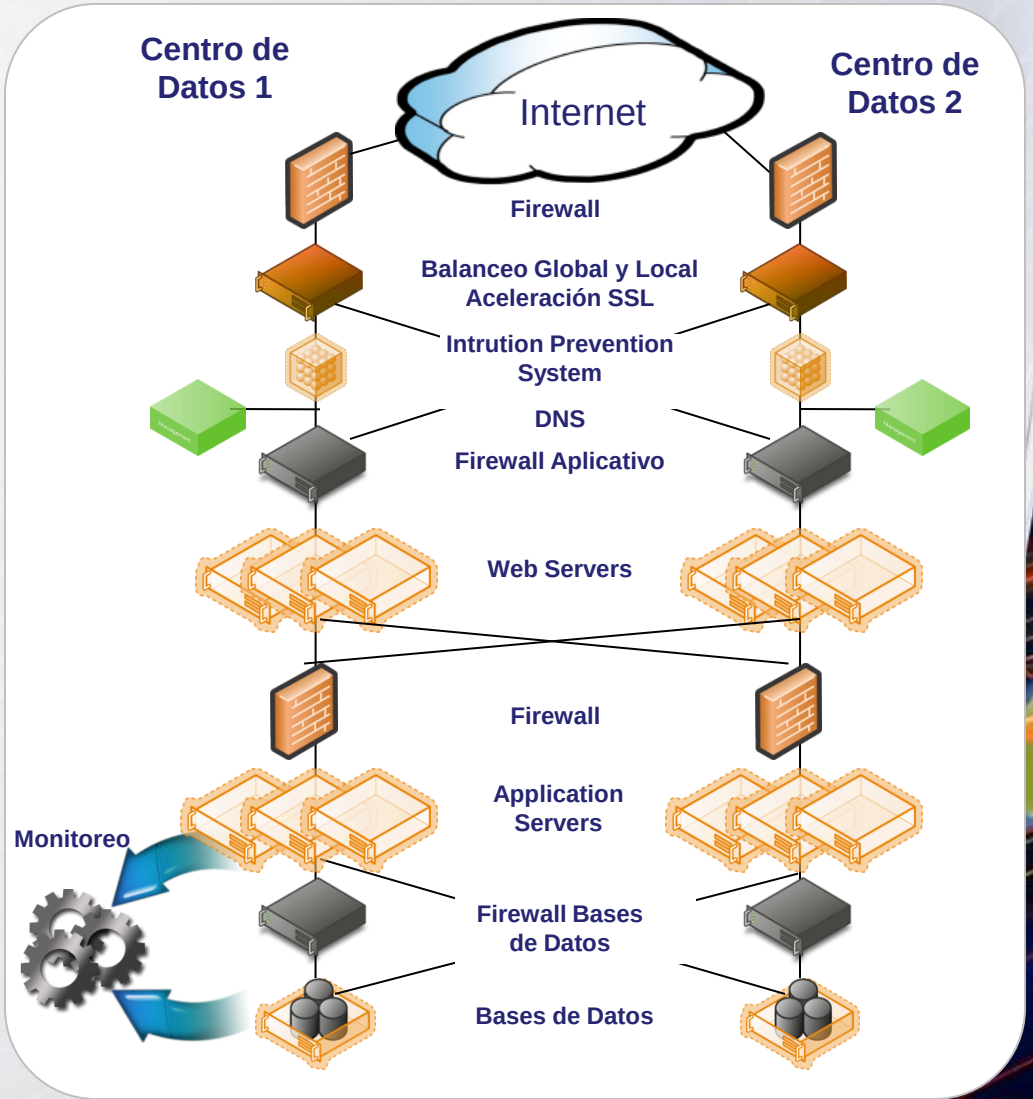


- Verificar cumplimiento de políticas de seguridad ante de establecer conexión.
- Establecer VPN o VPN SSL
- Utilizar portales cautivos de accesos

- Antimalware / Firewall / Host IPS
- Control de dispositivos externos (pendrive, dvd-write, ipod)
- Encriptación de Discos Duros

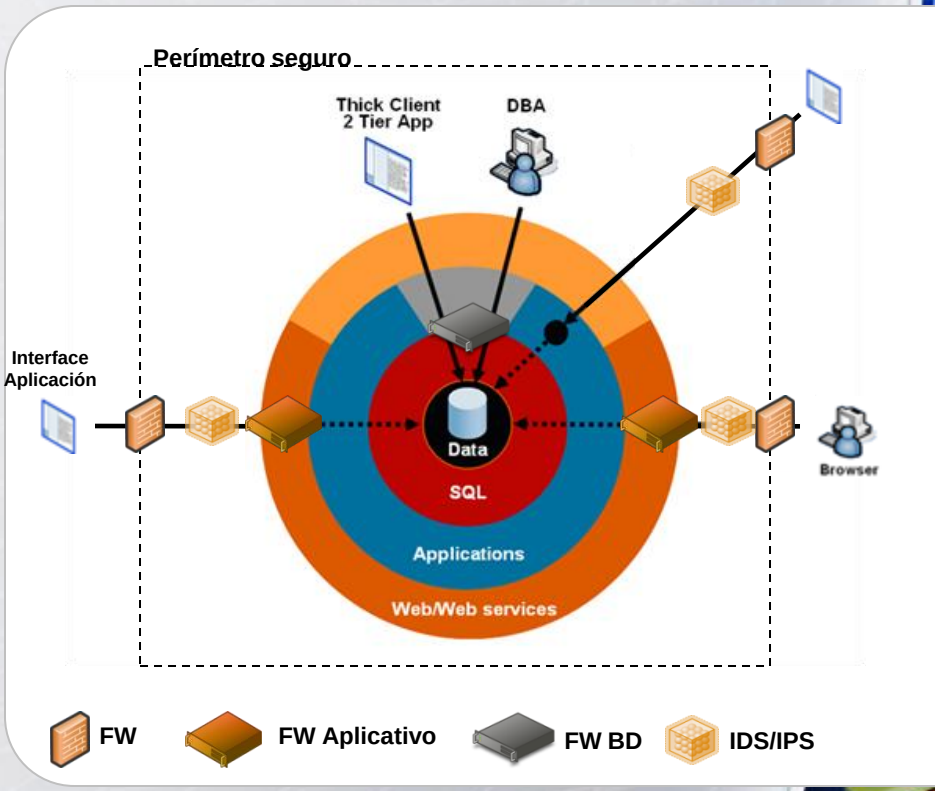
Zona DMZ

- Modelo altamente redundante
- Múltiples capas complementarias de controles
- A nivel de centros de procesamientos, el modelo es escalable
- Modelo escalable en todas sus capas
- Modelo soporta multimarcas
- Monitoreo 7 x 24 x 365

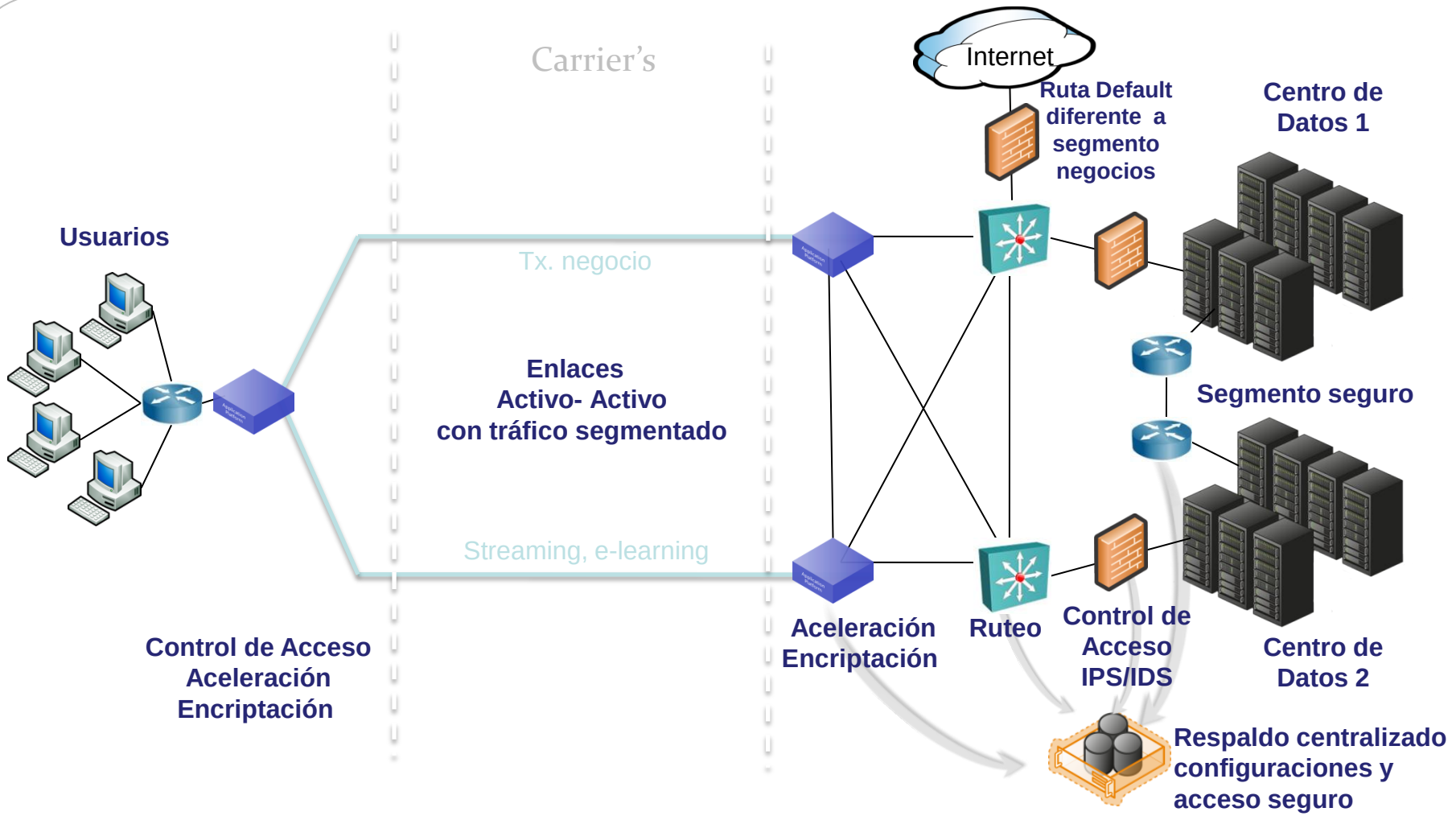


Perímetro Datacenter

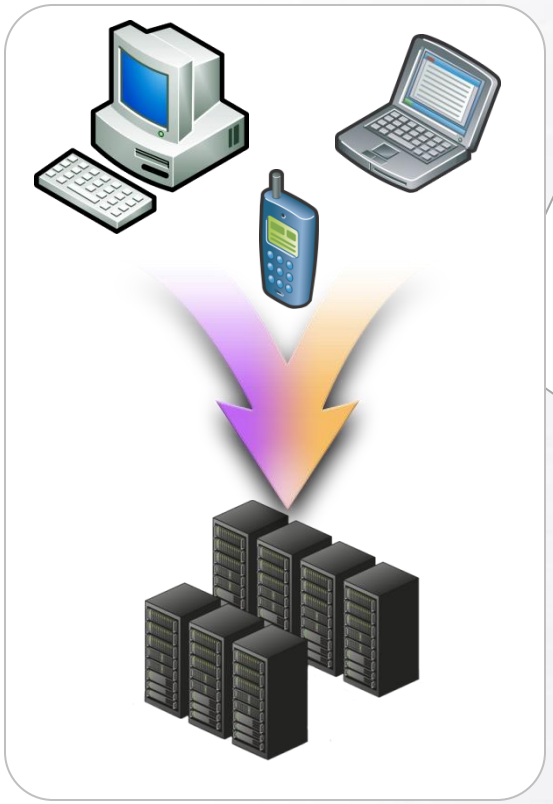
- Establece un perímetro de seguridad para los servicios Ti
- Modelo de control multicapas
- Sólo se exponen a usuarios, los servicios necesarios
- Protección de acceso a servicios de administración y soporte
- Monitoreo 7 x 24 x 365
- Utilizar encriptación de discos, file servers y/o los respaldos externos.



Red de Transporte



Zona Usuarios



- Antimalware / Firewall / Host IPS
- Control de dispositivos externos (pendrive, dvd-write, ipod)
- Encriptación de Discos Duros

- Escritorio controlado
- Control de fugas de información
- Control de contenidos
- Control de acceso a aplicaciones
- Control de licencias (inventario)

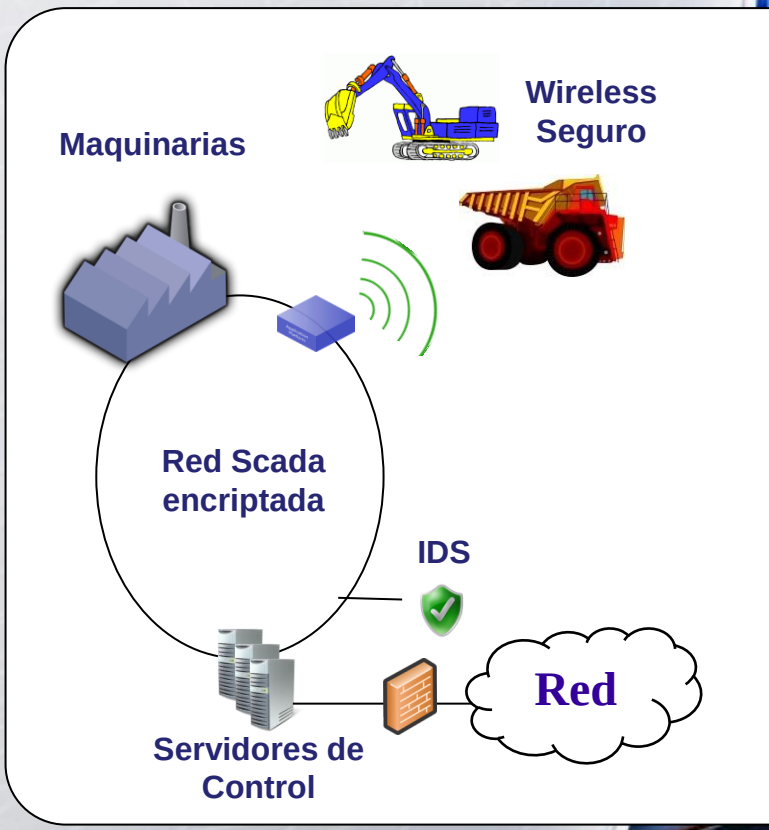
- Control de acceso a la red (NAC)

- Mecanismos acceso remoto

¿Qué ocurre con los dispositivos personales?

Zona Producción

- Red independiente y altamente redundante
- Transmisión de datos encriptados
- Seguritización de servidores de control
- Acceso muy restringido y controlado
- Monitoreo de seguridad frente a ataques y malware
- Control de inventario de hardware autorizado y no autorizado
- Control de inventario de software autorizado



15 Controles Críticos

1. Inventario de los dispositivos autorizados y no autorizados
2. Inventario de software autorizado y no autorizado
3. Seguridad de hardware y software en equipos portátiles, estaciones de trabajo y servidores
4. Seguridad en la red tales como firewall, enrutadores y conmutadores
5. Defesa perimetral
6. Mantenimiento, monitoreo y análisis de logs de auditoría
7. Seguridad de software de aplicación
8. Uso controlado de privilegios administrativos
9. Acceso controlado basado en “Necesidad de conocer”
10. Continua evaluación de vulnerabilidades y corrección
11. Monitoreo y control de cuentas de usuarios
12. Defensas contra malware
13. Limitación y control de puertos de red, protocolos y servicios
14. Control de dispositivos inalámbricos
15. Prevención de pérdidas de datos

Agenda

- Evolución de las amenazas de seguridad
- Sistemas Distribuidos y Tendencias de Control
- Modelos de control
- Desafíos para el futuro

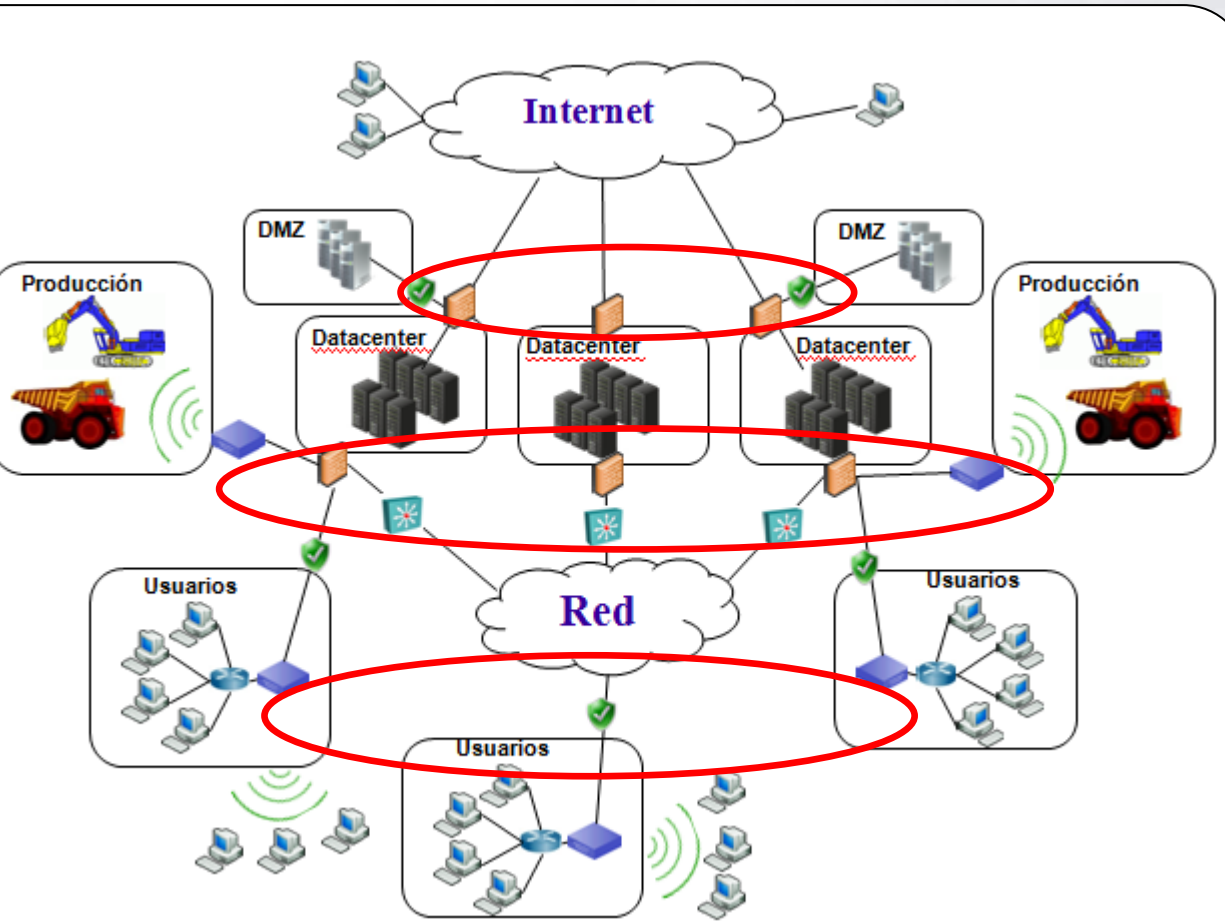
Los desafíos para la próxima década

- **Administración de dispositivos smartphones, tablets y notebook personales**
- **Unificación de las tecnologías y controles**
- **Administración central y unificada**
- **Mejorar entendimiento de la política de seguridad, de cara a los usuarios**
- **Orientar los controles a los aplicativos**

Administración de dispositivos smartphones, tablets y notebook personales

- **Autenticación integrada a Active Directory o Repositorio LDAP**
- **No importará la red donde está el usuario, sólo si fue autenticado o no**
- **Buscar controlar la información empresarial que radica en dispositivos externos**
- **Respaldo y Eliminación remota de información**

Unificación de Tecnologías y Controles



- Simplificar los elementos de control
- Lograr una administración mas eficiente y menos propensa a error humano
- Tener flexibilidad para establecer controles de acuerdo a la necesidades del negocio
- Mejorar eficiencia dentro de cada dominio

Unificación de Tecnologías de control

FW | **VPN** | **IPS** | **Anti Virus** | Anti Spam

Filtro URL | **DLP** | Análisis de Compor-tamiento

El uso de los distintos módulos deberá ser dinámico y acorde a las necesidades del negocio

Administración Central y Unificada

- **Integrar bajo una única gestión, al menos, los registros de eventos**
- **Establecer métricas de seguridad que permitan determinar desviaciones a las políticas de seguridad**
- **Integrar las evaluaciones de vulnerabilidades**
- **Monitorear 24 x 7 x 365**

Política de seguridad de cara al usuario

- **El usuario debe percibir que los controles de seguridad son de su responsabilidad:**
  - **Autenticación y Autorización**
  - **Resguardo de la información**
  - **Control de acceso**
  - **Control de contenidos**
  - **Clasificación de información**
- **Uso controlado de dispositivos externos (pendrives, discos USB, Iphone, etc)**

Orientar los controles a los aplicativos

Amenaza x Malware

14 OCT 2009 Hackers instalan malware en ordenadores utilizando YouTube de señuelo

Miles de páginas falsas de YouTube distribuyen Malware

publicado el miércoles 09 junio 2010 por Data en: Cybercrimen Google Curiosidades Web 2.0 Conceptos de Internet Noticias

Troyanos en Facebook

Publicado en Facebook, Tecnología por **dondado** el **24 noviembre 2008**

Facebook, además de ser una enorme red social, sirve como plataforma para ejecutar multitud de aplicaciones distintas, p.e. esos test que completas cada dos por tres y esos jueguecitos que absorven tú tiempo más de lo razonable, no son aplicaciones nativas de Facebook, simplemente se ejecutan ahí.

Saturación de Ancho de Banda

eltiempo.com / tecnología / internet

Congestión en Internet por saturación de redes debido a alta transferencia de datos

El consumo de ancho de banda de YouTube

June 12th, 2008 Posted in Internet

> El año pasado YouTube consumió tanto ancho de banda como el que consumió todo internet durante el año 2000.

Las redes sociales ocupan la banda ancha

Versión impresora Votar esta noticia (50 votos)

Facebook, YouTube y los vídeos, afectan a las aplicaciones críticas de negocio. La identificación de aplicaciones y control de las mismas continúa siendo el talón de Aquiles de la mayoría de las organizaciones. Así al menos lo afirma un estudio realizado por el especialista en sistemas de redes

Perdida de Productividad

Facebook y YouTube, las webs más visitadas desde el trabajo

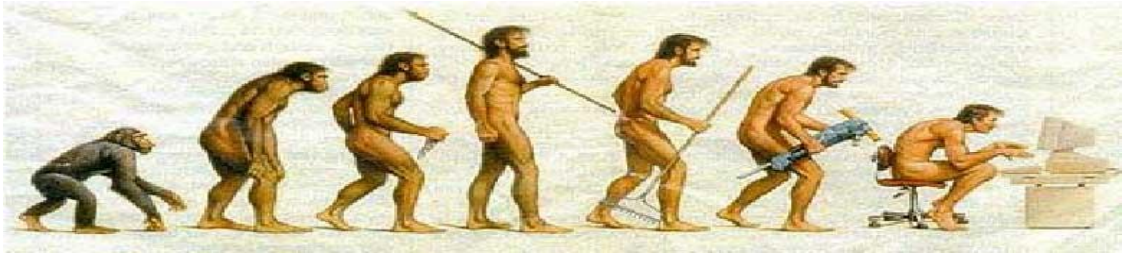
22 April 2010

¿Visitas Facebook o YouTube desde el trabajo?, no estás solo, ya que según un artículo de SC Magazine, las webs más visitadas desde el lugar de trabajo, tanto por visitas como por ancho de banda utilizado, son Facebook y YouTube, **siendo Facebook la página más visitada**, por encima de cualquier otra.

16 tweets retweet

Conclusiones

- **Tendremos que adecuar los controles de seguridad a las nuevas necesidades de negocio**
- **Las tecnologías cambiarán, pero dependerá de nosotros el sacarles el mejor partido**
- **La seguridad es dinámica y debemos reaccionar oportunamente**



“Es posible compatibilizar la funcionalidad de la red y el dinamismo del negocio, con un nivel de seguridad acorde”

Gracias por asistir a esta sesión…

Preguntas

SEGURIDAD EN SISTEMAS DISTRIBUIDOS

Jorge Rojas Zordan
Sub Gerente de Innovación y Desarrollo de Productos
jrojasz@novared.net