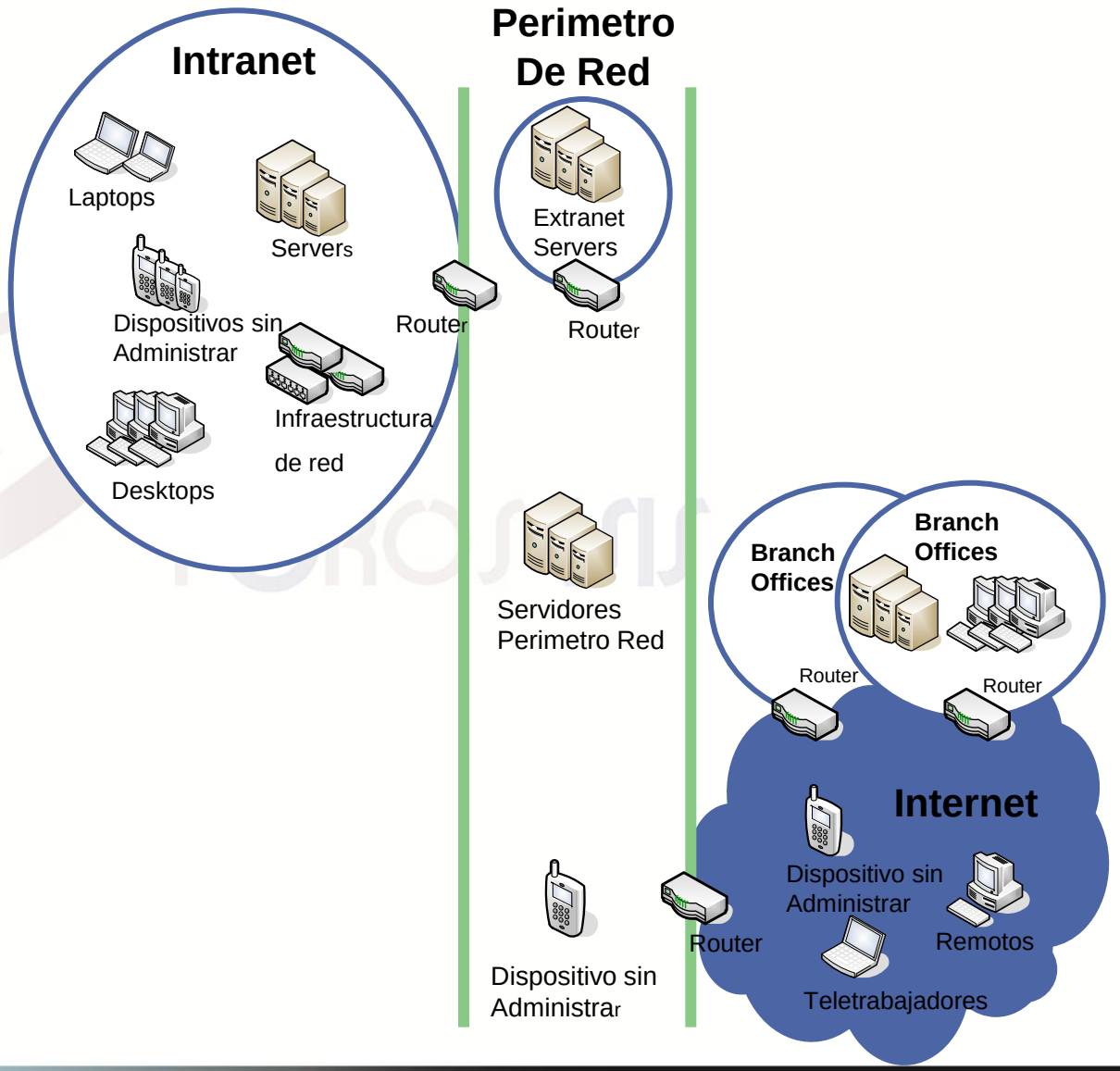
Visión Estratégica de Seguridad Informática en el Sector de Telecomunicaciones

Ing. Jahir Molina
Director de Operaciones TIC
Emtelco S.A
2013

Agenda

- Introducción
- Visión empresarial y Estrategia de Seguridad
- Alineación de la Estrategia de Seguridad
- Retos
- Tendencias
- Resumen

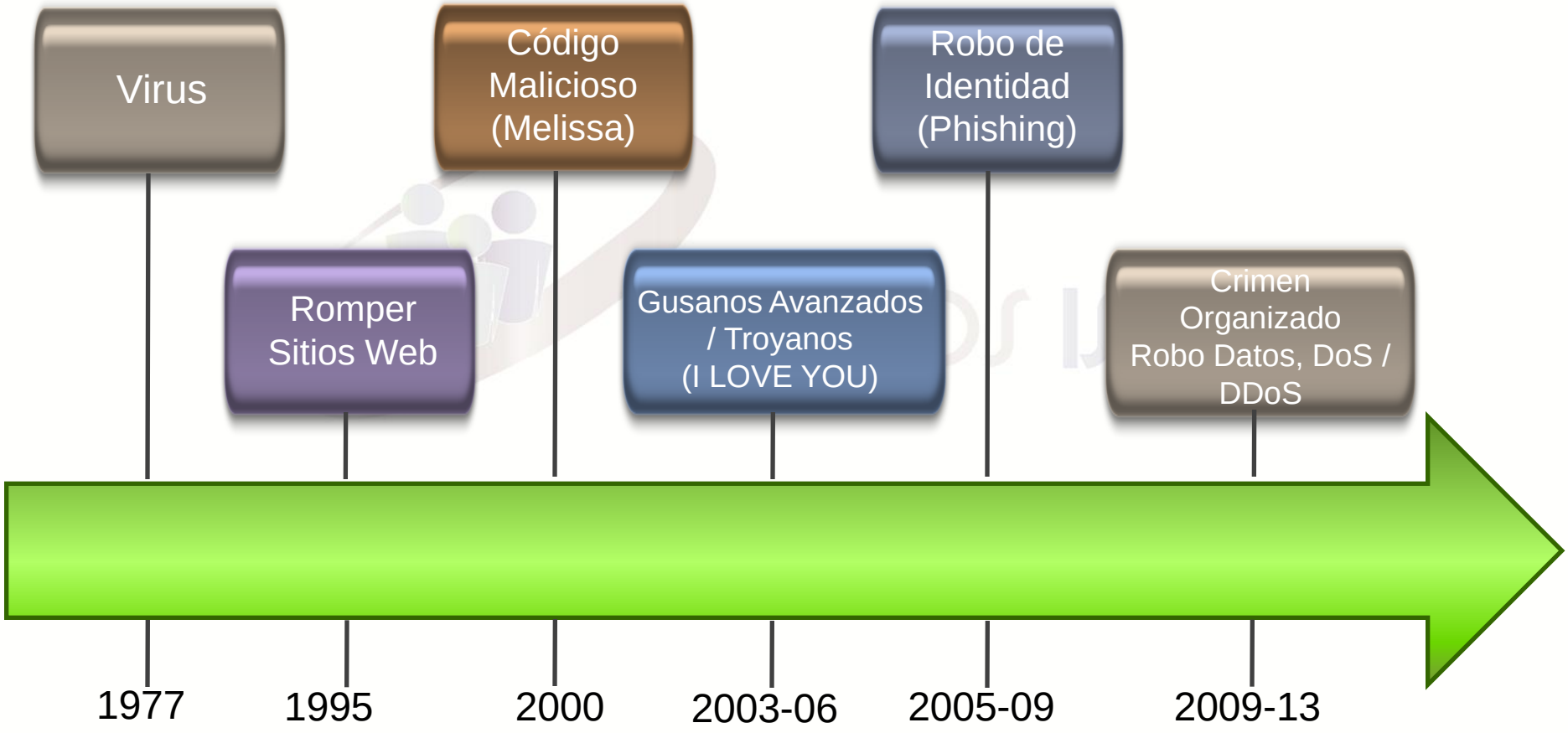
La Complejidad de las Redes Hoy



Tendencias y convergencias

- La computación ubicua, conectividad de red y la movilidad
- Computación embebida
- Alta seguridad
- IPv6
- VoIP
- Datos/Voz/Video

Tipos de Ataques a las Redes



Evolución de los tipos de ataques

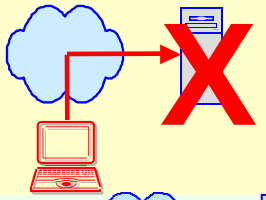
- Enfoque de los ataques
  - 2000: Infraestructura (servidor, infraestructura de red)
  - 2013: El usuario (cliente, browser)
- Nivel de ataques
  - 2000: Red, Sistemas operativos
  - 2013: Aplicaciones
- Objetivo de los atacantes
  - 2000: Reconocimiento, orgullo, aprobación
  - 2013: Ganancias monetarias
- Modo de ataque
  - 2000: Amenazas genéricas (“click and attack”)
  - 2013: Ataques diseñados, específicos…
- Organización de los atacantes
  - 2000: Atacantes solitarios
  - 2013: Crimen organizado

Como se puede observar, los atacantes pusieron en la cuenta oficial (**@BurgerKing**) el **logo, el nombre y el sitio web de la competencia**. Este incidente es uno más de los que ocurren diariamente por no usar contraseñas fuertes en los servicios críticos, y en el caso de cuentas corporativas se pone más en evidencia la criticidad del caso.

Modelo de Amenazas (Simplificado)

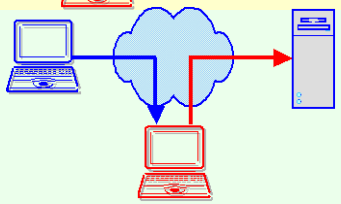
1 – Destrucción (ataques a la disponibilidad):

– Destrucción de información y/o recursos de la red



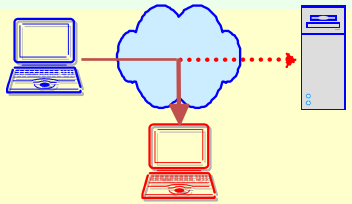
2 - Corrupción (ataque a la integridad):

– Manipulación no autorizada de un activo



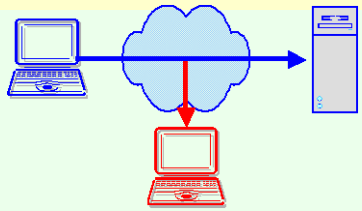
3 - Remoción (ataque a la disponibilidad):

– El robo, eliminación o pérdida de información y / u otros recursos



4 - Divulgación (ataque a la confidencialidad):

– El acceso no autorizado a un activo



5 - Interruption (ataques a la disponibilidad):

– Interrupción de los servicios. Red no está disponible o no utilizables

Visión Empresarial y Su Conexión Con Una Estrategia De Seguridad

Definición de Una Arquitectura de Seguridad

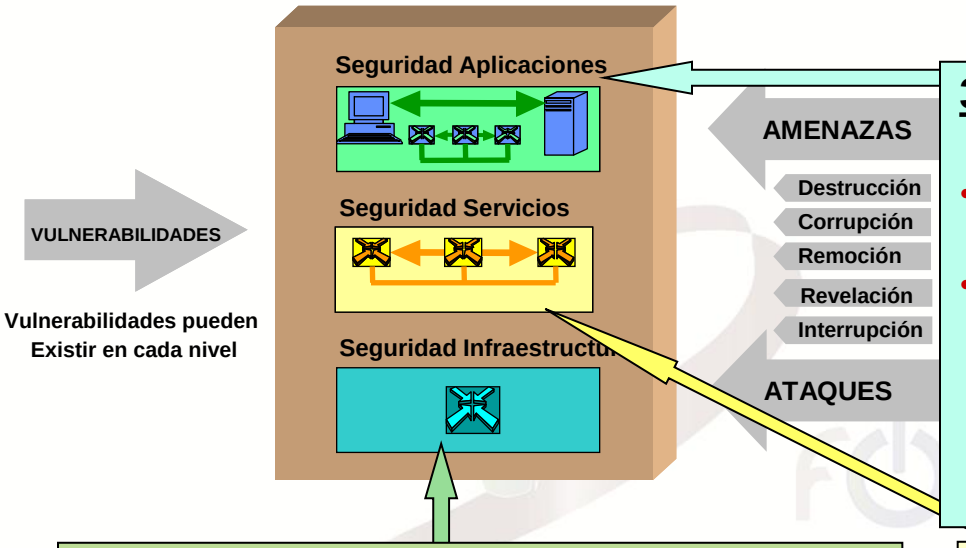
¿Qué tipo de protección que se necesita y contra qué amenazas?

¿Cuáles son los distintos tipos de equipos de redes y agrupaciones de instalaciones que necesitan ser protegidos?

¿Cuáles son los diversos tipos de actividades de la red que necesitan ser protegidas?

Enfoque: Riesgos en los sistemas de información

3 Niveles de Seguridad



3 – Nivel de Seguridad de Aplicaciones:

- Aplicaciones basadas en red usadas por los usuarios finales
- Ejemplos:
  - navegación por la Web
  - Directorio de la corporación
  - Email
  - E-commerce

1 – Nivel Seguridad de Infraestructura:

- Bloques fundamentales de construcción de servicios de red y aplicaciones
- Ejemplos:
  - Routers, switches individuales, servidores
  - Enlaces WAN Punto-a-Punto
  - Enlaces Ethernet

2 - Nivel de Seguridad de Servicios:

- Servicios asignados a usuarios finales
- Ejemplos:
  - Frame Relay, ATM, IP
  - Celular, Wi-Fi,
  - VoIP, QoS, mensajería instantánea, servicios de localización (GPS)
  - servicios de llamadas gratuitas

- **Cada nivel de seguridad tiene amenazas y vulnerabilidades únicas**
- **Seguridad Infraestructura => Seguridad Servicios => Seguridad Aplicaciones**

Ocho Medidas de seguridad frente a la amplitud de las vulnerabilidades

- Limitar y controlar el acceso a los elementos de red, servicios y aplicaciones
- Ejemplos: contraseñas, ACL, firewall

Control Acceso

- Proporcionar prueba de identidad
- Examples: secreto compartido, PKI, firma digital, certificate digital

Autenticación

- Prevenir capacidad de negar que la actividad en la red se produjo
- Ejemplos: los registros del sistema, las firmas digitales

No Repudio

- Asegurese de la confidencialidad de los datos
- Example: Cifrado

Confidencialidad Datos

- Asegurar que la información sólo fluye desde la fuente al destino
- Ejemplos: VPN, MPLS, L2TP

Seguridad Comunicación

- Asegurarse que el dato se recibe como se envió y se recupero como se almacenó
- Examples: MD5, firmas digitales, anti-virus

Integridad Datos

- Asegúrese que los elementos de red, servicios y aplicaciones sean disponibles para los usuarios legítimos
- Ejemplos: IDS / IPS, redundancia de red, BC / DR

Disponibilidad

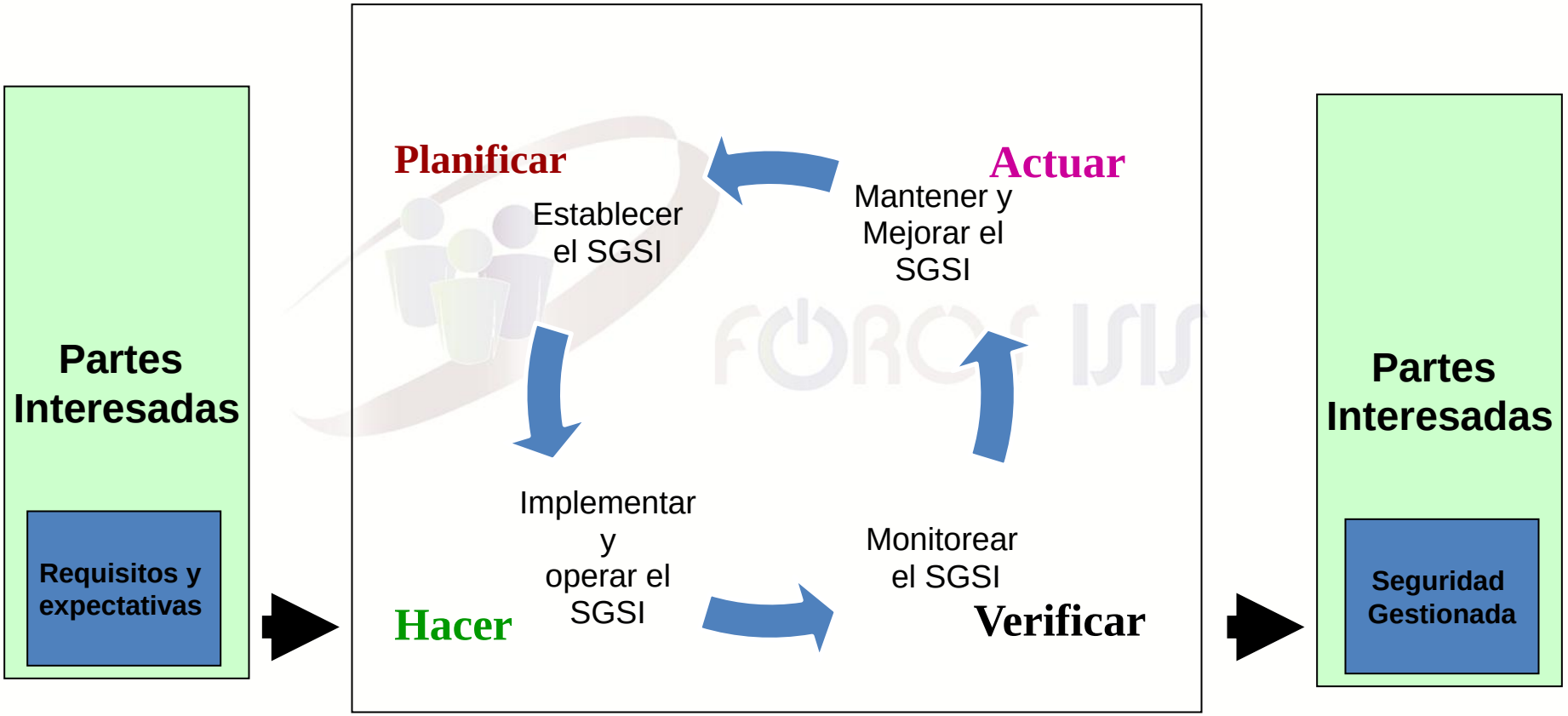
- Garantizar la identificación y uso de la red se mantiene como privado
- Ejemplos: NAT, cifrado

Privacidad

Ocho Dimensiones aplicables a cada perspectiva de seguridad (nivel y plano)

Alinear la Estrategia de Seguridad

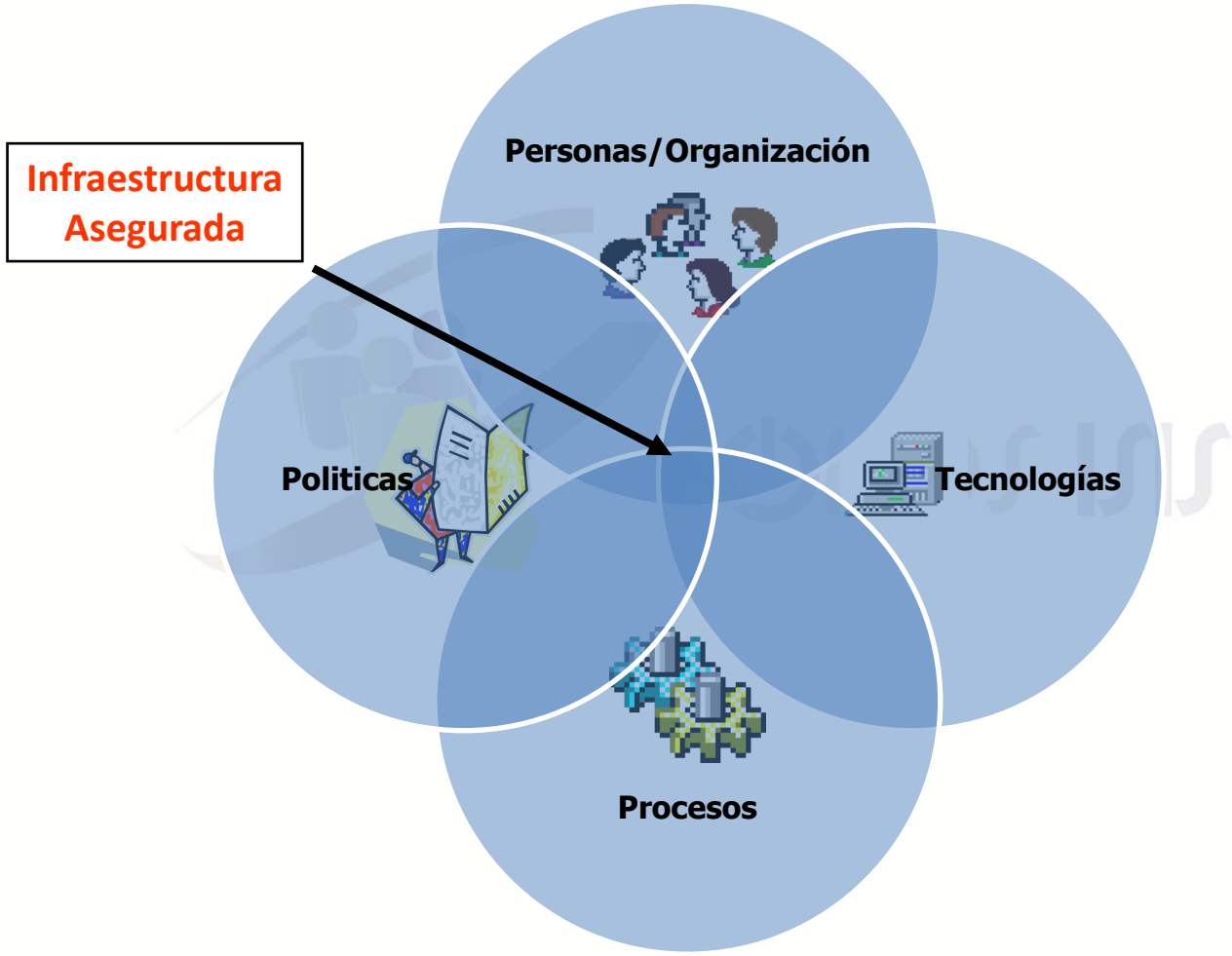
Modelo utilizado para establecer, implementar, monitorear y mejorar la estrategia de SGSI.



ESTRATEGIA DE SEGURIDAD

- Política de Seguridad
- Organización de la información
- Gestión de Activos
- Seguridad del Recurso Humano
- Seguridad física y ambiental
- Control Acceso
- Gestión de las Comunicaciones
- Gestión de Incidentes
- Continuidad del Negocio
- Cumplimiento Regulatorio

El Reto a Futuro: Organización



El Reto a Futuro: Control

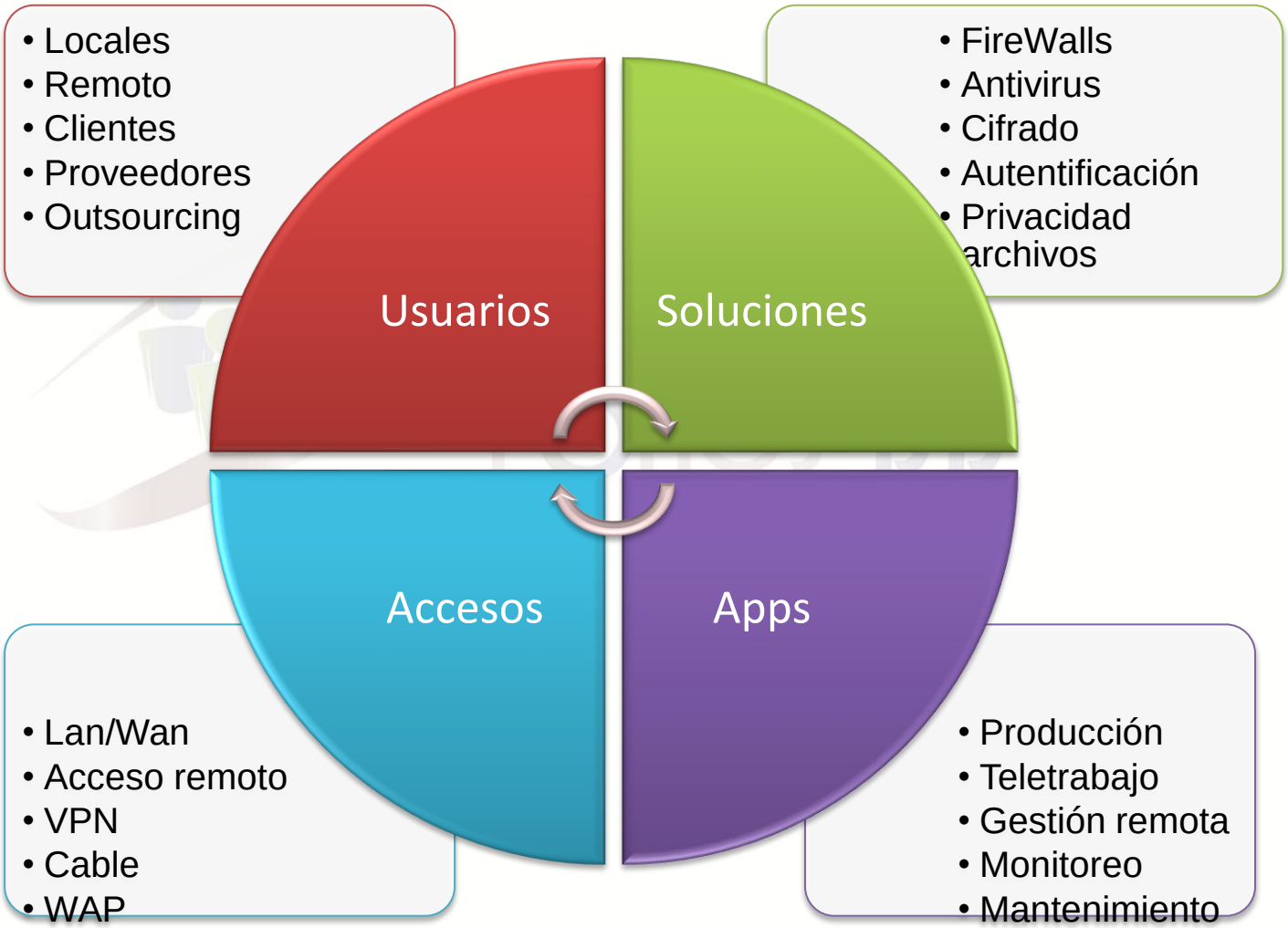
- Los dispositivos inteligentes
  - televisión
  - Computadoras
  - Tabletas
  - teléfono móvil
  - (Un único dispositivo para proporcionar de extremo a extremo, el acceso seguro sin problemas)

- Simplicidad de Aplicaciones
  - Preferencia de interfaz única, sencilla y segura de acceder a aplicaciones o contenido
  - Interface Ubicua - navegador web

- Infraestructura Fléxible

Debido a estas áreas de la evolución, las redes de hoy se definen más por los servicios que apoyan que por demarcación tradicional de la Infraestructura Física.

El Reto a Futuro: Integración



Tendencias

Redes Sociales	• Facebook, Twitter • Skype
Malware Para Dispositivos Móviles	• Android • Tablets, TV, Blue-Ray
Vulnerabilidades	• Java • Adobe
Juegos	• Desarrollo de juegos más interactivos en red • Exposición de las redes a posibles hackers
Geolocalización	• Nueva especificación HTML5 • funciones de geolocalización activadas, dejando potencialmente geo-objetos en cualquier dispositivo con un navegador web.

Tendencias

Windows8	• se ejecuta en PC, en las tabletas y teléfonos inteligentes. • Nuevos programas de ataque más sofisticados
BYOD	• Almacenamiento de claves en equipos inseguros • Proliferación de equipos = Menor control
Cloud	• explotación de redes no seguras de comunicación • pérdida de control de los recursos informáticos físicos
Autenticación	• “Tokenización” de la data, teletrabajo • Aseguramiento de dispositivos y almacenamientos externos
Internet de Dispositivos	• Equipos conectados uno a uno vía internet • domótica controlada por internet y sistemas de alarma. • Ipv6: autos con dirección IP

Para Cerrar…

La seguridad es **un asunto de todos**

Se requiere de la colaboración de todas las áreas (**No es un problema de TI solamente)**

La seguridad debe ser diseñada por **adelantado**

La seguridad debe ser un **esfuerzo continuo**

Abordar sistemáticamente las **vulnerabilidades (propiedades intrínsecas de las redes / sistemas)** es la clave

La protección puede proporcionarse **independientemente** de lo que las amenazas puedan ser (que están cambiando constantemente y pueden ser desconocidas)

Resumen: Proporcionar un enfoque holístico a la seguridad de la red

Ver la seguridad de la red con un punto de vista integral: de principio a fin

Aplicar a cualquier tipo de tecnología de red

- WiFi, Cableada, redes ópticas, Nube
- Voz, datos, video, redes convergentes

Aplicar a cualquier red

- Redes proveedoras de servicios
- Lan/Man/Wan
- Redes privadas
- Productivas, pruebas/desarrollo, redes administrativas
- Data center

Siempre alineados con cualquier regulación: PCI, SOX, etc

Preguntas?

Gracias por su asistencia

e-mail: jmolinaz@emtelco.com.co

@jahirmz