Evolución de la Seguridad de la Información para las telecomunicaciones de una empresa eléctrica

Jorge Costa

jcosta@ute.com.uy

www.ute.com.uy

Particularidades de los servicios de telecomunicaciones en empresas eléctricas

- Las empresas eléctricas requieren sistemas de telecomunicaciones confiables para:
  - servicios operativos necesarios para monitorear, operar y proteger la red eléctrica (teleprotección, telecontrol, telemedida, gestión remota de dispositivos operativos de terceros)
  - servicios de apoyo a la operación del sistema eléctrico (Comunicaciones operativas de voz, localización vehicular, video para apoyo de la operación)
  - Servicios corporativos (sistemas de información corporativa, telefonía, etc.)

Qué entendemos por información?

- Conjunto de datos dotados de un significado y un propósito, que puede ser llegar a ser tan relevante como la gestión de la red eléctrica.

Seguridad para qué?

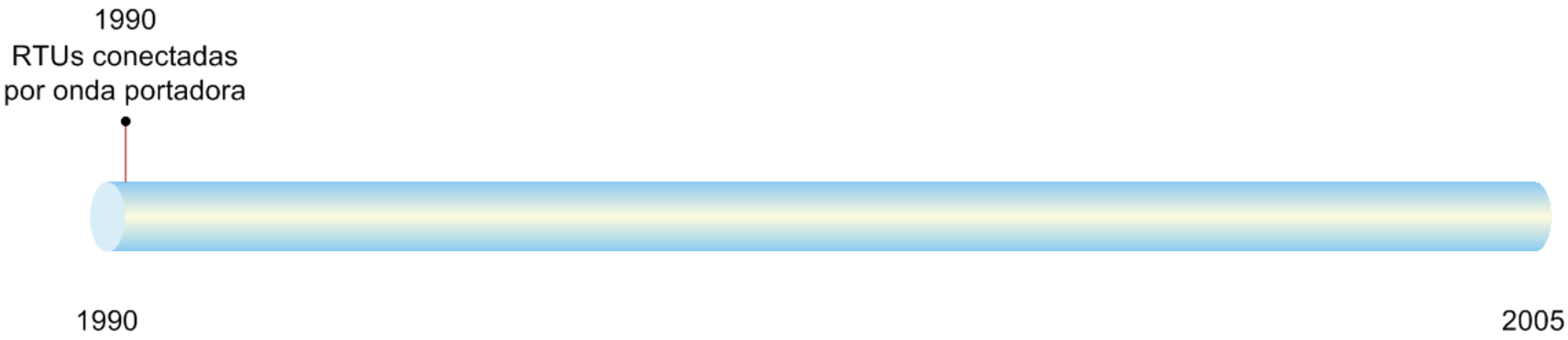
- Disponibilidad: Para asegurar que los datos serán accesibles en el momento en que sean requeridos
- Autenticación: confirmación de la identidad declarada por aquellos usuarios que acceden a los datos o que pueden modificar configuraciones
- Integridad: confirmación de que los datos que han sido enviados, recibidos o almacenados son completos y no han sido modificados
- Confidencialidad: protección de las comunicaciones o los datos almacenados contra su interceptación y/o lectura por parte de personas no autorizadas

Evolución

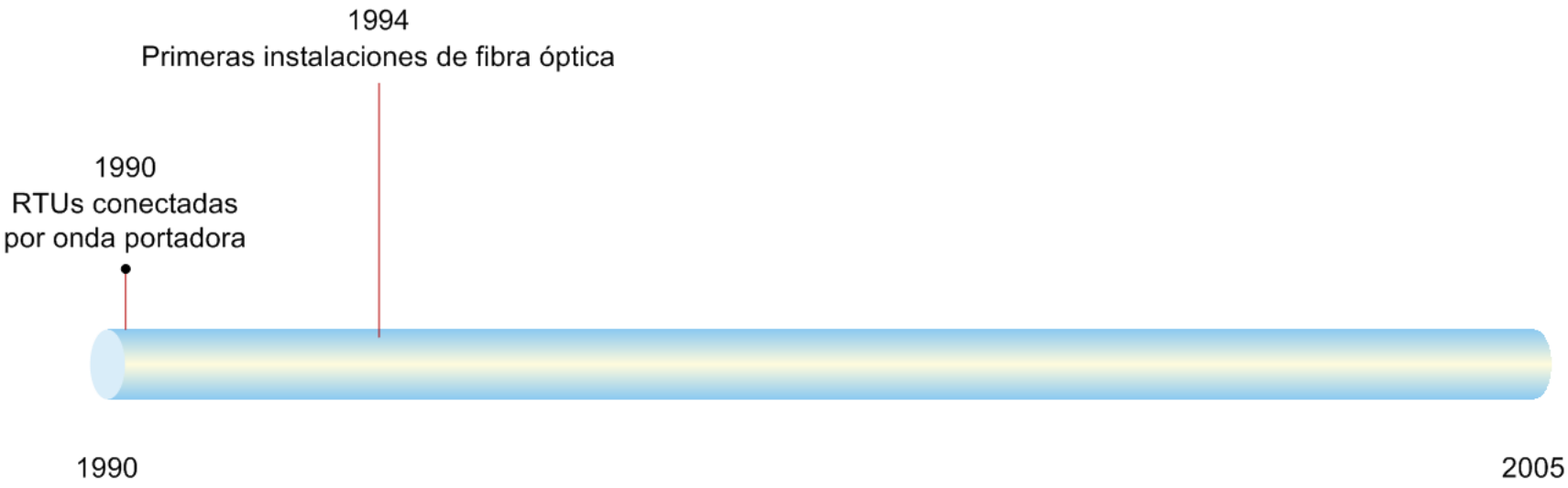
1990

2005

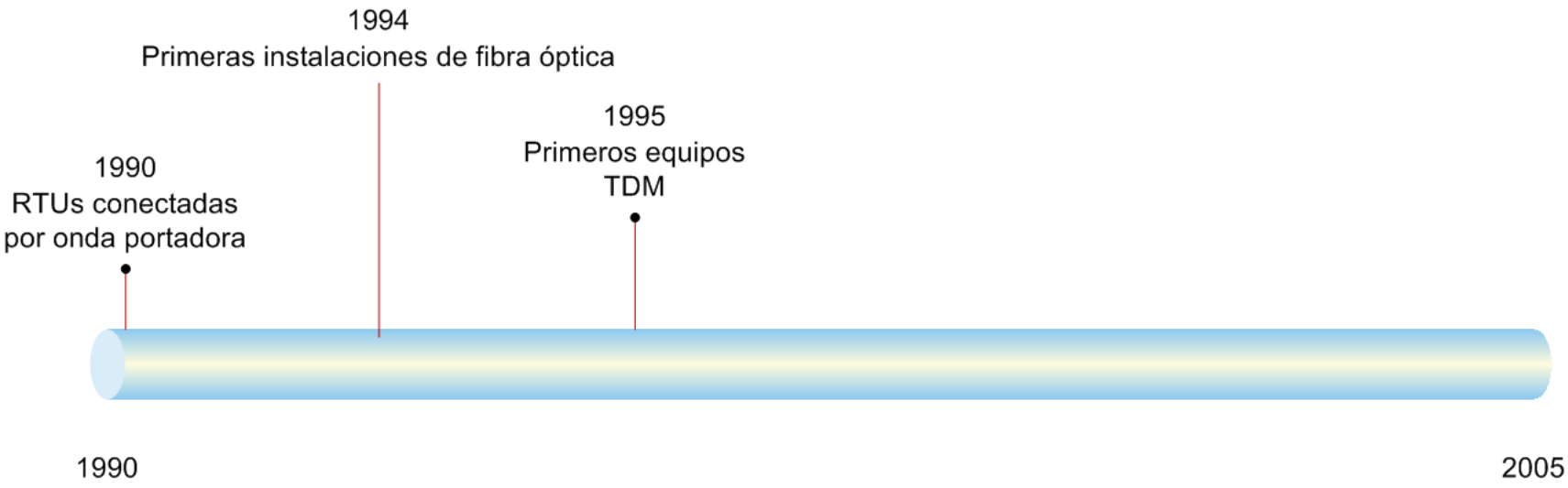
Evolución



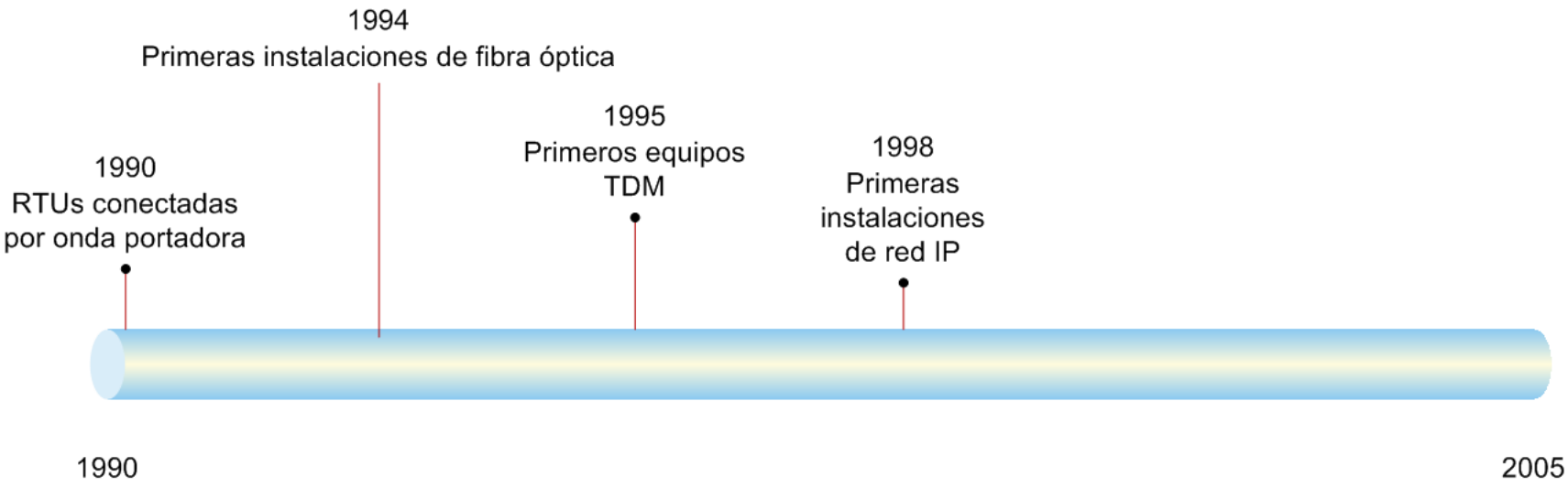
Evolución


1994
Primeras instalaciones de fibra óptica
1990
RTUs conectadas
por onda portadora
1990
2005

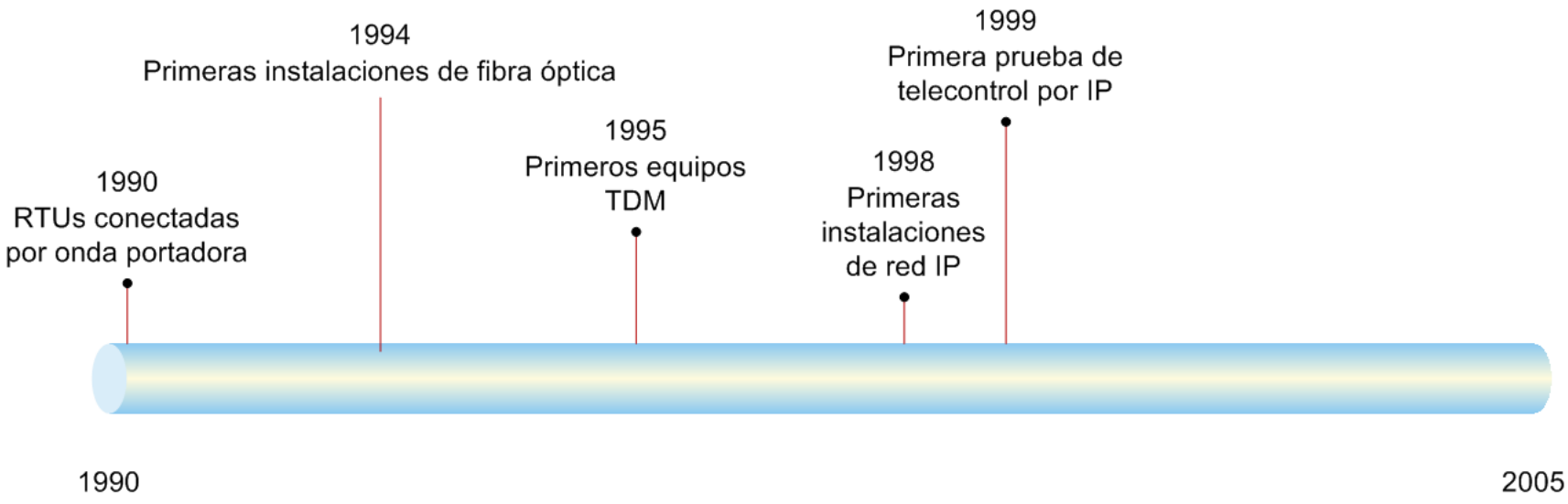
Evolución


1994
Primeras instalaciones de fibra óptica
1995
Primeros equipos
TDM
1990
RTUs conectadas
por onda portadora
1990
2005

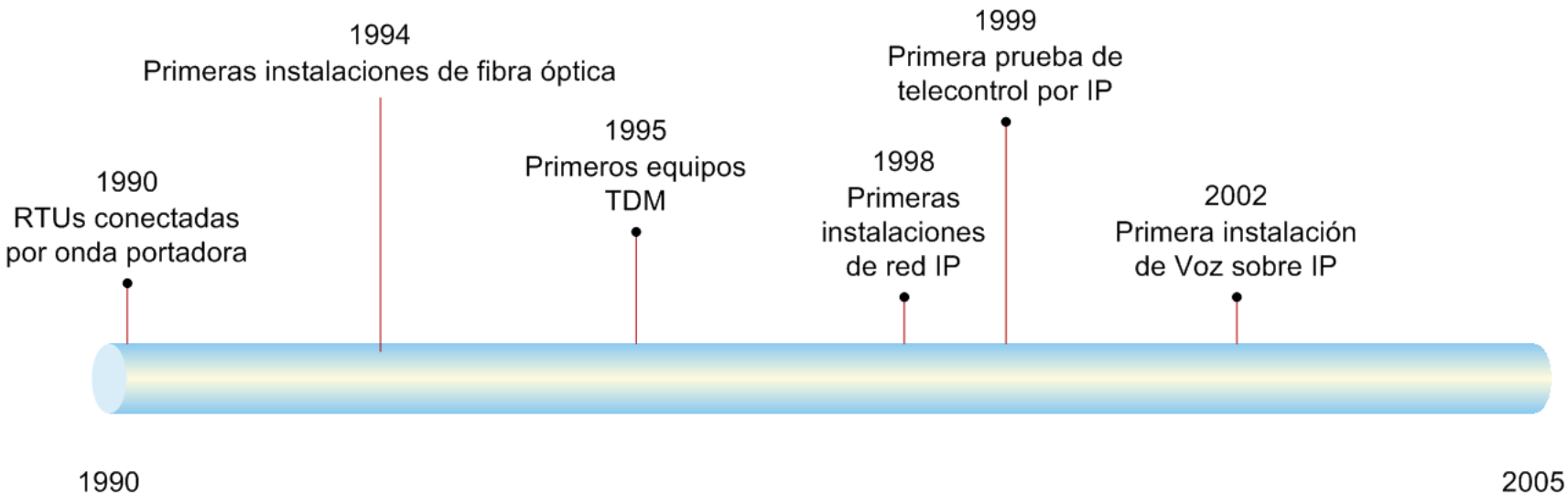
Evolución


1994
Primeras instalaciones de fibra óptica
1990
RTUs conectadas
por onda portadora
1995
Primeros equipos
TDM
1998
Primeras
instalaciones
de red IP
1990
2005

Evolución


1990
RTUs conectadas
por onda portadora
1994
Primeras instalaciones de fibra óptica
1995
Primeros equipos
TDM
1998
Primeras
instalaciones
de red IP
1999
Primera prueba de
telecontrol por IP
1990
2005

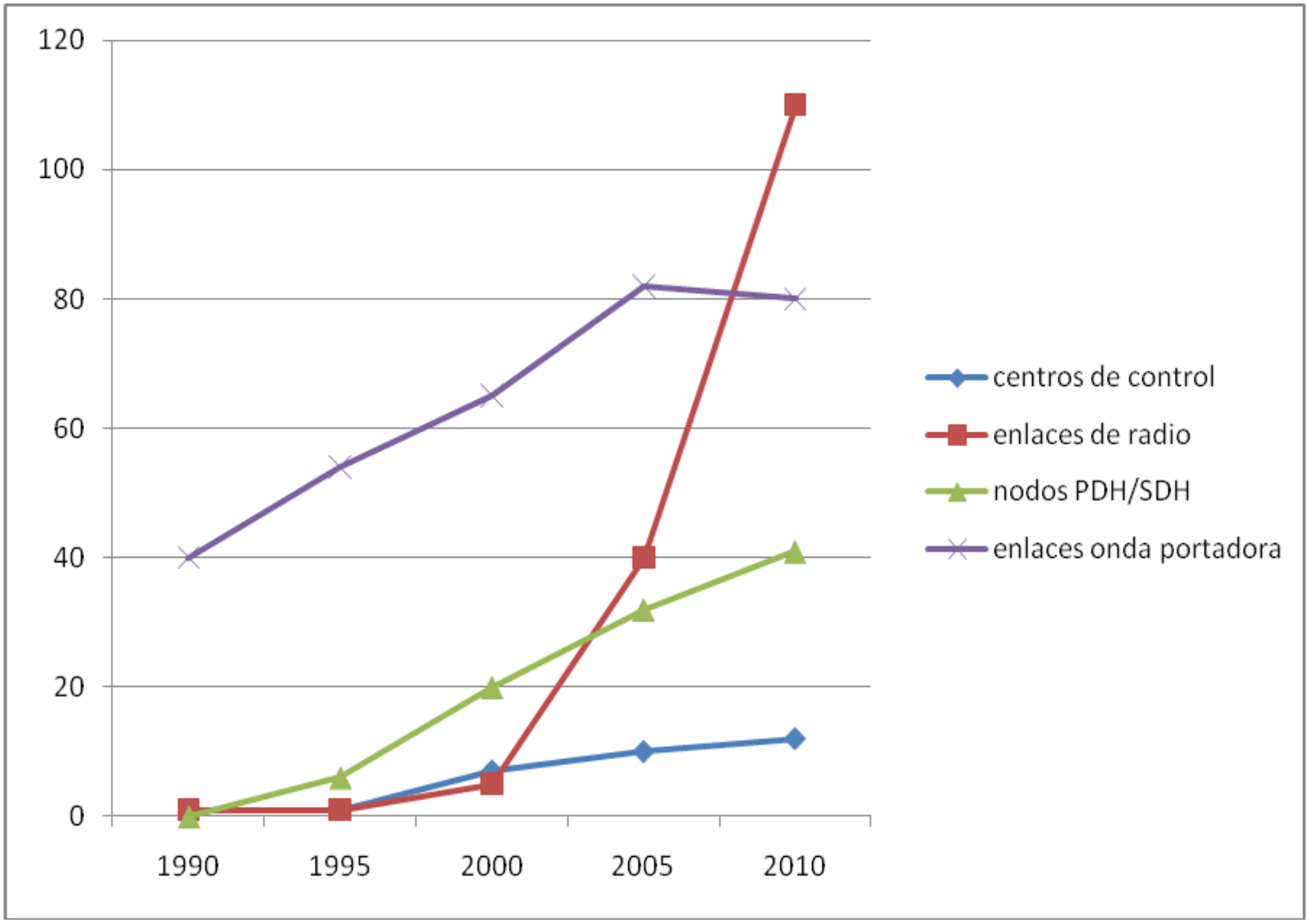
Evolución


1990
RTUs conectadas por onda portadora
1994
Primeras instalaciones de fibra óptica
1995
Primeros equipos TDM
1998
Primeras instalaciones de red IP
1999
Primera prueba de telecontrol por IP
2002
Primera instalación de Voz sobre IP
1990
2005

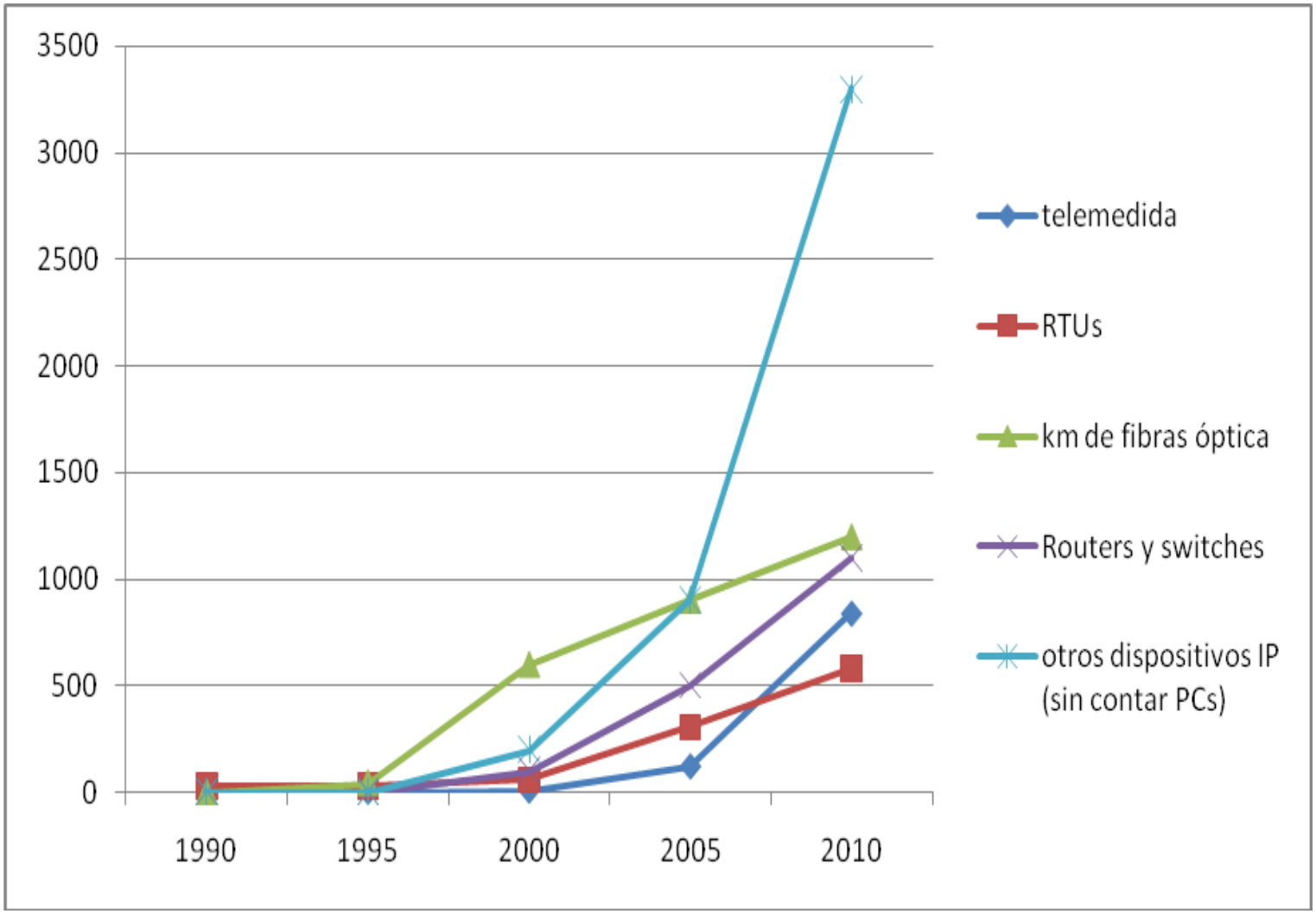
Evolución

- A partir de allí comienza un proceso de creciente incorporación de servicios que se trasmiten por la red IP debido principalmente a:
  - las facilidades que ofrece este medio para extender una red existente
  - los costos decrecientes de los equipos
  - el desarrollo de protocolos que mitigaran las carencias que traía desde su origen esta red: seguridad, calidad de servicio, etc.
  - el aumento de velocidad disimuló las dificultades que presentaba frente a las aplicaciones con requisitos de tiempo real

Evolución


120
100
80
60
40
20
0
1990
1995
2000
2005
2010
centros de control
enlaces de radio
nodos PDH/SDH
enlaces onda portadora

Evolución


3500
3000
2500
2000
1500
1000
500
0
1990
1995
2000
2005
2010
telemedida
RTUs
km de fibras óptica
Routers y switches
otros dispositivos IP (sin contar PCs)

Actores que intervienen en la seguridad

- El personal de Protecciones quiere gestionar sus relés
- El área responsable de controlar los accesos físicos a los locales y salas
- Los responsables de gestionar alarmas
- Los administradores de sistemas SCADA quieren gestionarlos a distancia
- El área comercial quiere leer los medidores de energía, al menos los principales
- Sistemas de Información debe asegurar los sistemas corporativos y los accesos desde fuera de la empresa
- Debe haber personal velando por la estabilidad de la red IP, que pasa a ser algo fundamental, sólo un escalón más abajo que la red eléctrica

Problemas a resolver

Cómo gestionar la seguridad de la información cuando hay tantos actores?

Cada cual organiza su área de responsabilidad (dominio) según sus criterios?

Pasando a algo más práctico: Cómo manejar las claves de usuario de todos estos sistemas?

El Sistema de Gestión de Seguridad de la Información

- Para trabajar de forma metódica, es conveniente partir definiendo los objetivos y el alcance del sistema de gestión de seguridad de la información.

La Política de Seguridad de la Información

- La política debe incluir un marco de referencia y fijar principios de acción en relación a la seguridad de la información. Es recomendable que en su elaboración participen los distintos actores que manejan recursos de información en su dominio
- La Dirección debe aprobar este documento. Esto es necesario para que se asuma el compromiso de apoyar la seguridad, se asignen las responsabilidades y los recursos necesarios y se apruebe el riesgo tolerable para la organización.

Plan de Seguridad

- Es un documento que debe desarrollar cada Dominio. Allí se realiza el análisis de riesgo de los activos específicos del Dominio, y se indica cómo, cuándo y quién va a realizar los controles seleccionados.
- Incluye tareas de concientización y capacitación en seguridad.
- También se indica la forma en que se van a gestionar dentro del Dominio los incidentes de seguridad

Identificar los riesgos

- Identificar los activos más importantes para la organización desde el punto de vista de la información (activos críticos)
- Enumerar las amenazas para cada uno de estos activos
- Indicar las vulnerabilidades que pueden ser explotadas por las amenazas enumeradas

Ejemplo: Amenaza: fuego
Vulnerabilidad: en algunos locales no hay personal permanente ni sistemas de extinción automática

Para cada activo crítico

- Estimar la probabilidad de ocurrencia de las amenazas detectadas

Ej.: Probabilidad de ocurrencia (P)

Valor	Nivel	Probabilidad / Casos al año
0,001	Remoto	Muy baja / Menos de una vez cada 100 años
0,005	Esporádico	Baja / Sucede cada entre 20 y 100 años
0,01	Moderado	Mediana / Sucede cada entre 5 y 20 años
0,05	Frecuente	Significativa / Sucede cada entre 1 y 5 años
0,1	Habitual	Alta / Entre 1 y 12 veces al año
0,5	Constante	Muy alta / Más de 12 veces al año

Para cada activo crítico

- Estimar los impactos que puede ocasionar la pérdida de seguridad sobre los activos críticos

Ej.: Impacto Estratégico (IEs)

Valor	Nivel	Criterio general
1	Insignificante	No afecta / Mínima
2	Marginal	Poco significativa / Pequeña
10	Relativo	Parcial breve / Moderada
100	Importante	Total breve / Significativa
1000	Grave	Parcial extendida / Considerable
10000	Crítico	Total extendida / Gran magnitud

Para cada activo crítico

- Estimar el Impacto Económico (IEc)

  Por ejemplo: pérdidas económicas estimadas expresadas en miles de US$

- Cuantificar el Riesgo de Seguridad sobre cada activo para cada una de las amenazas listadas.

  RS = P x (IEs+IEc)

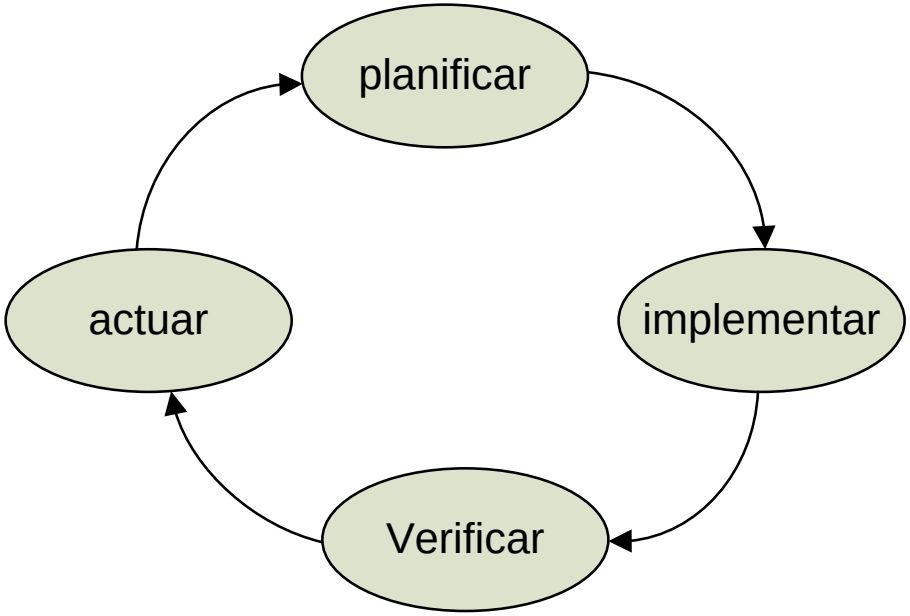
Para cada activo crítico

- Comparar los Riesgos de Seguridad con un Criterio de Aceptabilidad de riesgos predefinido en las Políticas de Seguridad, que normalmente será un valor máximo admisible.
- Los riesgos de seguridad que cumplen el criterio de aceptabilidad se asumen.
- Para aquellos casos que no cumplan el Criterio de Aceptabilidad, fijar objetivos de control y seleccionar los controles correspondientes

Siguientes etapas

El plan es muy importante, pero es solamente el comienzo. Luego deben realizarse estas etapas:

- **Implementar**
- **Verificar**
- **Actuar**



Conclusiones

- Este análisis, si bien no es necesariamente previo a las implementaciones de seguridad, es conveniente para no dejar huecos en nuestro sistema y también para asegurarnos que el gasto en controles se corresponde con el posible perjuicio derivado de fallos de seguridad.