



UNIVERSIDAD DE LAS PALMAS DE GRAN CANARIA
Servicio de Informática y Comunicaciones

IV Jornada de Coordinación del SIC

Un plan de seguridad para los servicios
de comunicaciones

Área de Comunicaciones



Manuel Jerez Cárdenes
26 de noviembre de 2004



Índice

- 1. ¿Qué se entiende por Plan de Seguridad?**
- 2. Objetivos del Plan**
- 3. Normativa de Seguridad y Bench-marking**
- 4. Plan de Seguridad para comunicaciones**
 - 4.1. Nivel físico**
 - 4.2. Nivel de enlace**
 - 4.3. Nivel de red**
 - 4.4. Nivel de presentación**
 - 4.5. Nivel de aplicación**
- 5. Estructura**
- 6. Conclusiones**
- 7. Líneas futuras**

1. ¿Qué se entiende por Plan de Seguridad? (i)

- **Plan:** intención, proyecto. Documento escrito.
- **Seguridad:** certeza, conocimiento seguro de algo
seguro: libre y exento de todo peligro, **infallible**
certeza: sin temor a errar
SEGURIDAD \longrightarrow **FIABILIDAD**
- **Fiabilidad:** probabilidad de que un sistema se comporte de la forma esperada.
- **Disponibilidad:** indica la accesibilidad de los datos y la operatividad de los servicios.

1. ¿Qué se entiende por Plan de Seguridad? (ii)

Equipos, sistemas o servicios de alta disponibilidad: sistemas 24x7 o sistemas de cinco nueves (99,999%). Redundancia.

- **El ámbito del Plan será la seguridad entendida en sentido amplio. Contemplará la defensa ante ataques, y además la protección ante aquellos incidentes que supongan una pérdida o merma de servicio. E.g.: catástrofes naturales, problemas eléctricos, errores humanos, etc.**
- **Proyecto que desarrolle los objetivos en materia de seguridad de una organización.**

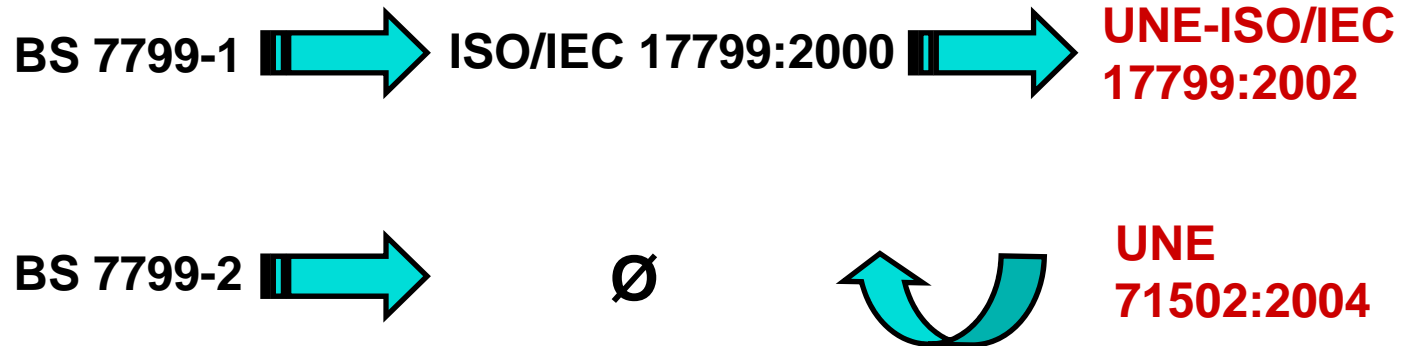
2. Objetivos del Plan (i)

- **Reflejar las deficiencias en materia de seguridad de cada área y proponer acciones correctoras.**
- **Implicar a todas las áreas de tecnologías de la información y comunicaciones (TIC) de la organización:**
 - ✓ **Sistemas**
 - ✓ **Desarrollo**
 - ✓ **Documentación**
 - ✓ **Soporte**
 - ✓ **Comunicaciones**

2. Objetivos del Plan (ii)

- **Conseguir sistemas de cinco nueves (99,999%).**
- **Coordinación entre áreas si es necesaria para implantar una acción.**
- **Planificar un calendario de implantación de las acciones correctoras.**
- **Hacer de la seguridad un hábito en nuestro trabajo diario.**

3. Normativa de seguridad y Bench-marking



3. Normativa de seguridad y Bench-marking

- **Planes de Seguridad de otras Universidades:**
 - **Universidad de Murcia**
 - **Universidad Pablo de Olavide de Sevilla**
 - **Universidad Complutense de Madrid**

Seleccionamos el Plan de la Universidad Pablo de Olavide por ser más completo y detallado.

- **Bibliografía:**
 - **Libro ITIL de Security Management**

4. Plan de Seguridad para comunicaciones

- **Desarrollo según los niveles del modelo OSI:**



4.1. Nivel físico

- **Suministro eléctrico: instalación de SAI en los 93 armarios de comunicaciones de la ULPGC.**
- **Accesibilidad a los edificios fuera del horario de apertura.**
- **Redundancia de la fibra: comprobaciones periódicas de las fibras más críticas en el anillo que forma la red de la ULPGC.**





4.2. Nivel de enlace

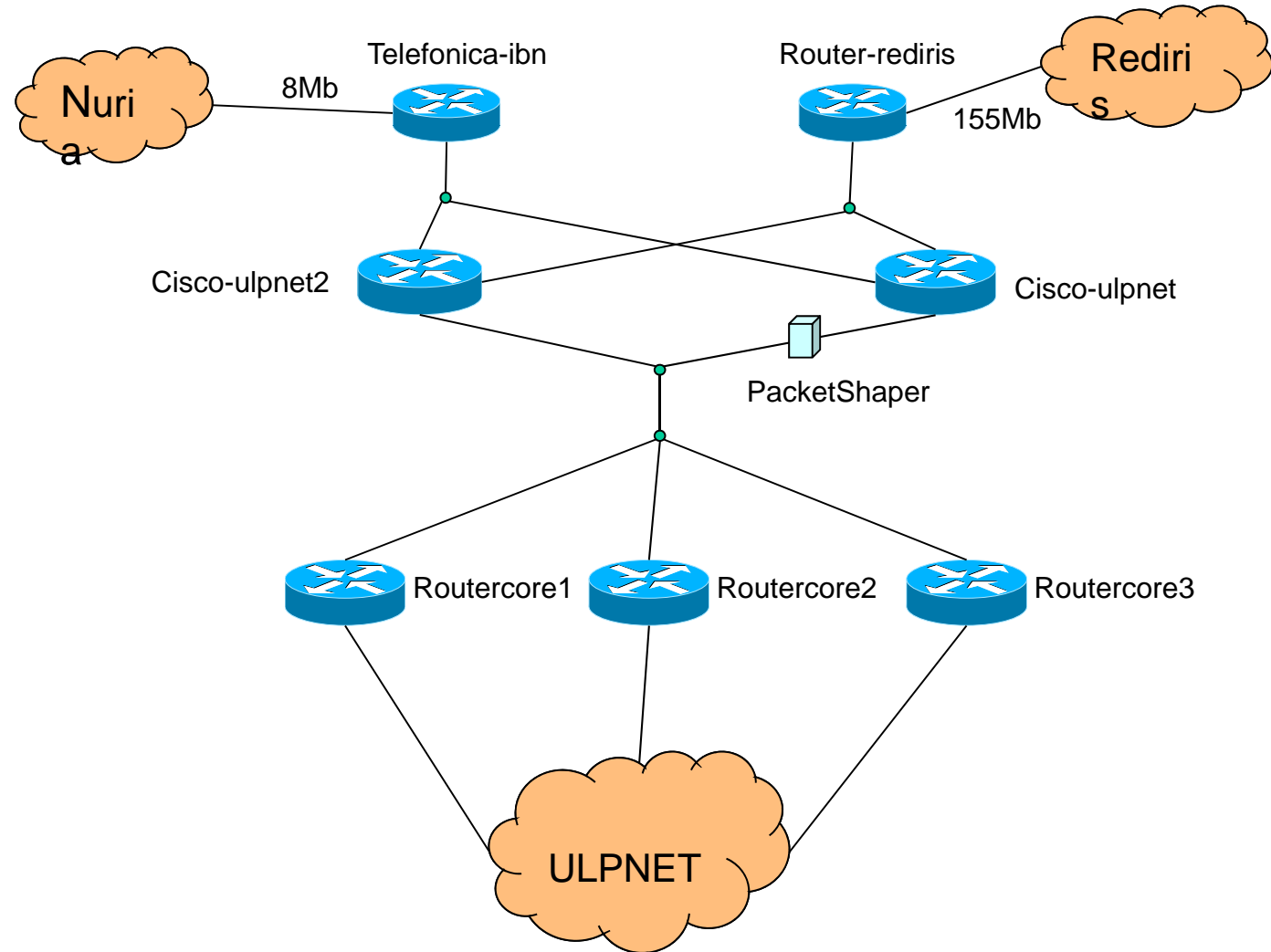
- **Comprobaciones periódicas de recuperación de dispositivos a partir de su copia de seguridad.**
- **Política para la red inalámbrica: conflicto puntos de acceso particulares con puntos de acceso de la ULPGC.**
- **Redundancia del enlace serial de 2Mb que une el nuevo Aulario de Medicina con Ingeniería mediante enlace inalámbrico de 54 Mb entre el Aulario y La Granja.**



4.3. Nivel de red (i)

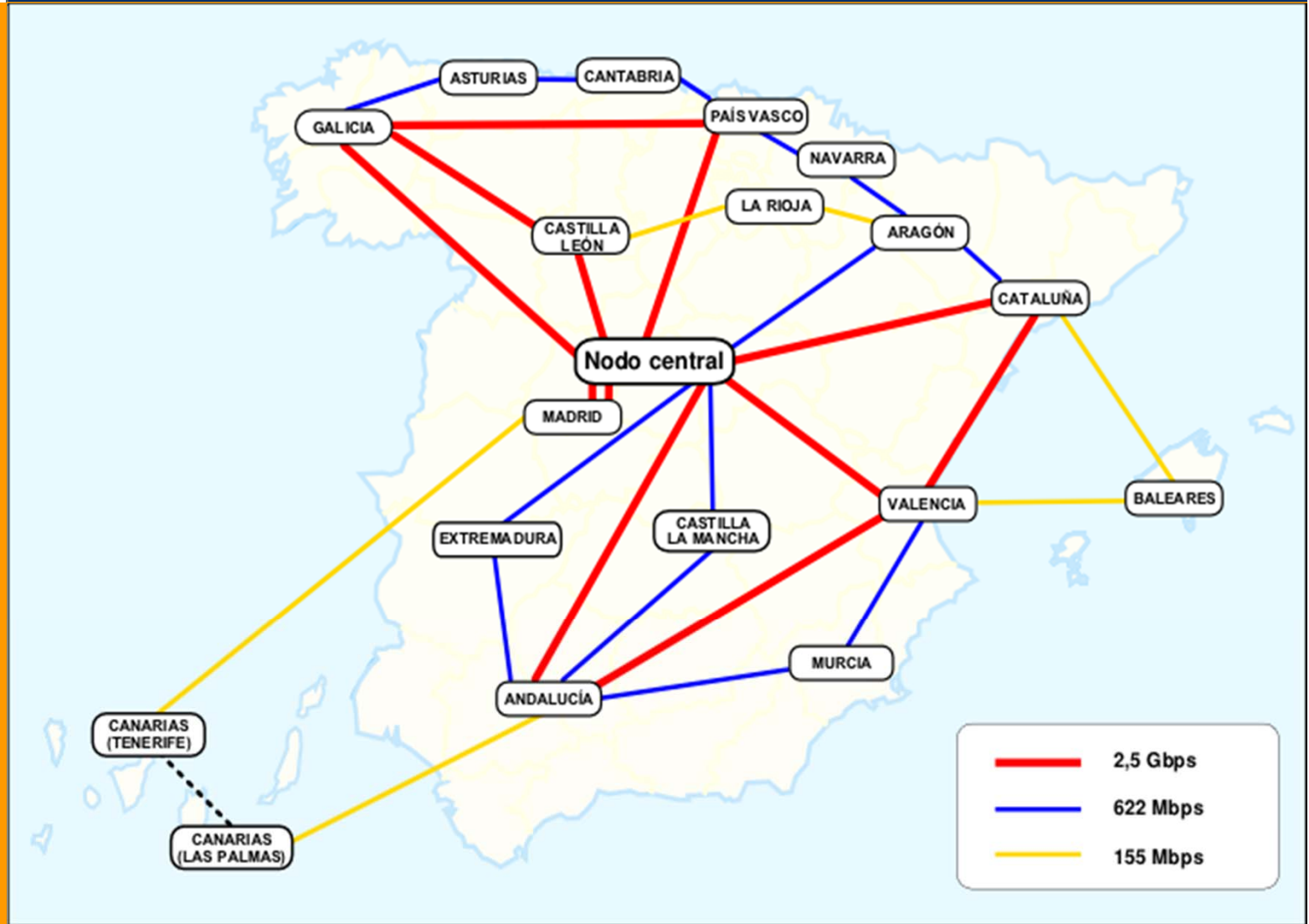
- **Comprobaciones periódicas de la redundancia de los dispositivos con criticidad elevada.**
- **Estrecha colaboración con Rediris para que nos alerten de cualquier anomalía en el tráfico de salida de la ULPGC.**
- **Procedimiento de actuación frente a la caída del enlace principal a internet a través de Rediris. Encaminamiento de todo el tráfico por la red Nuria.**

4.3. Nivel de red (ii)



Un plan de seguridad para los servicios de comunicaciones
Subdirección de Comunicaciones

4.3. Nivel de red (iii)



Un plan de seguridad para los servicios de comunicaciones
Subdirección de Comunicaciones

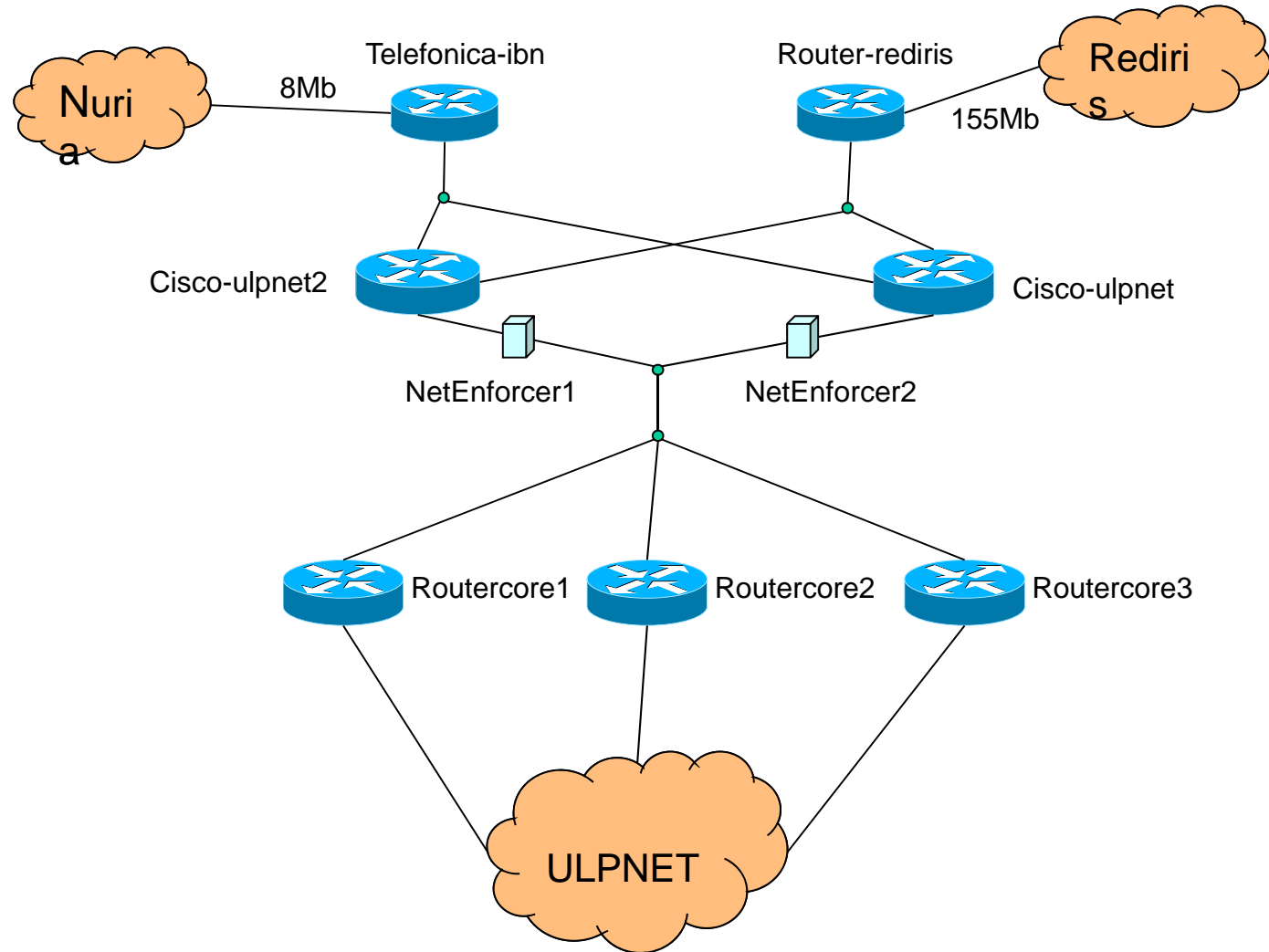
4.4. Nivel de presentación

- **Establecimiento de una política de acceso a través de VPN a la ULPGC, determinando:**
 - **quiénes acceden**
 - **privilegios**
 - **tiempo**
- **Encriptación de tráfico en la red inalámbrica (WEP y WPA).**

4.5. Nivel de aplicación (i)

- **Llevar a cabo la redundancia del servicio de mensajería de voz (UNITY) de Telefonía IP.**
- **Utilización del Sistema de Detección de Intrusos (IDS) Snort para la detección de ataques.**
- **Implementar un sistema de autenticación para la red inalámbrica.**
- **Instalación del segundo gestor de ancho de banda para conseguir redundancia total del enlace de entrada/salida a internet.**

4.5. Nivel de aplicación (ii)



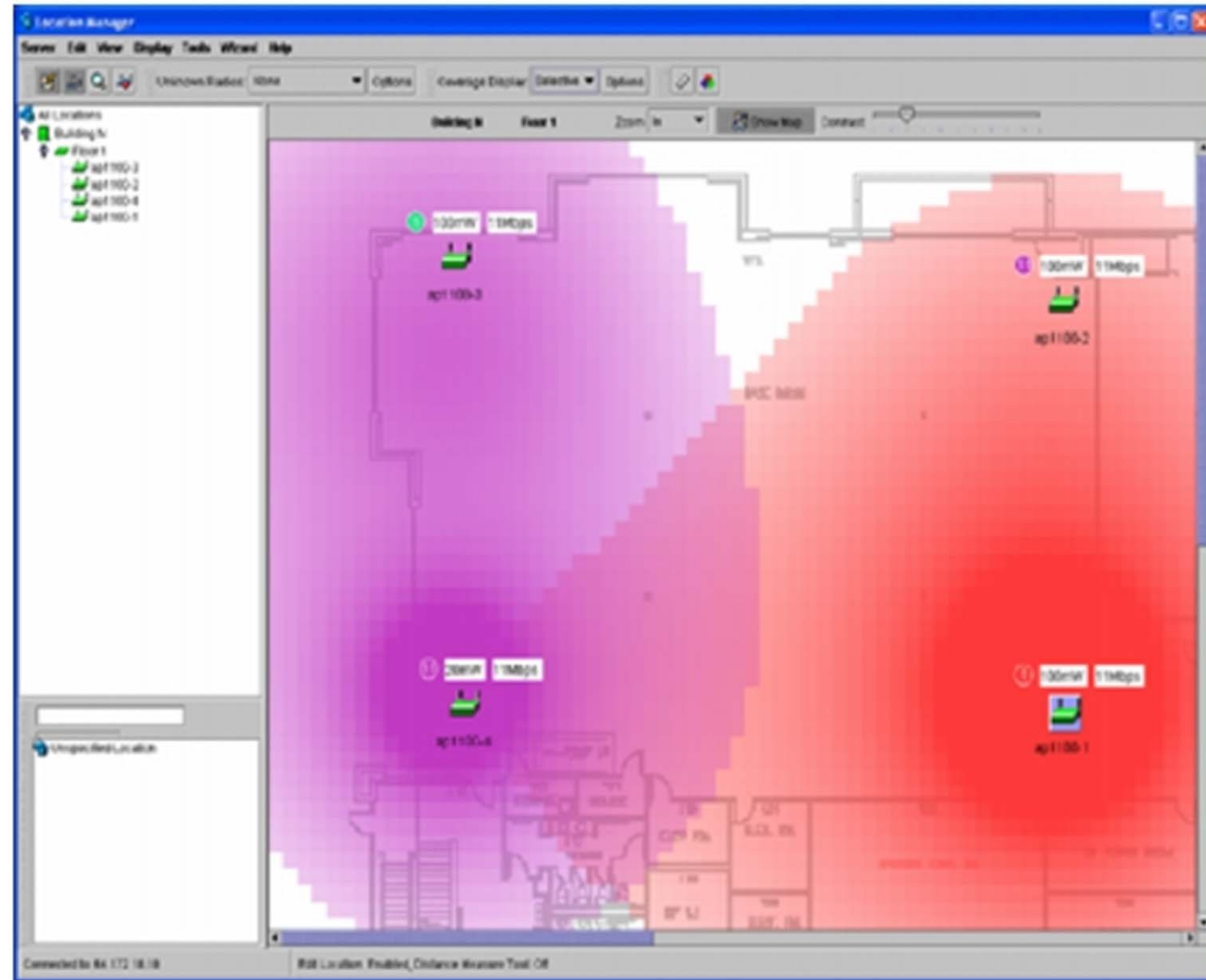
Un plan de seguridad para los servicios de comunicaciones
Subdirección de Comunicaciones

4.5. Nivel de aplicación (iii)



- **Instalación de cortafuegos en redundancia que permitirán proteger los routers de entrada/salida a internet de ataques.**
- **Puesta en funcionamiento de un gestor de la red inalámbrica para los 140 puntos de acceso instalados a día de hoy en la ULPGC.**

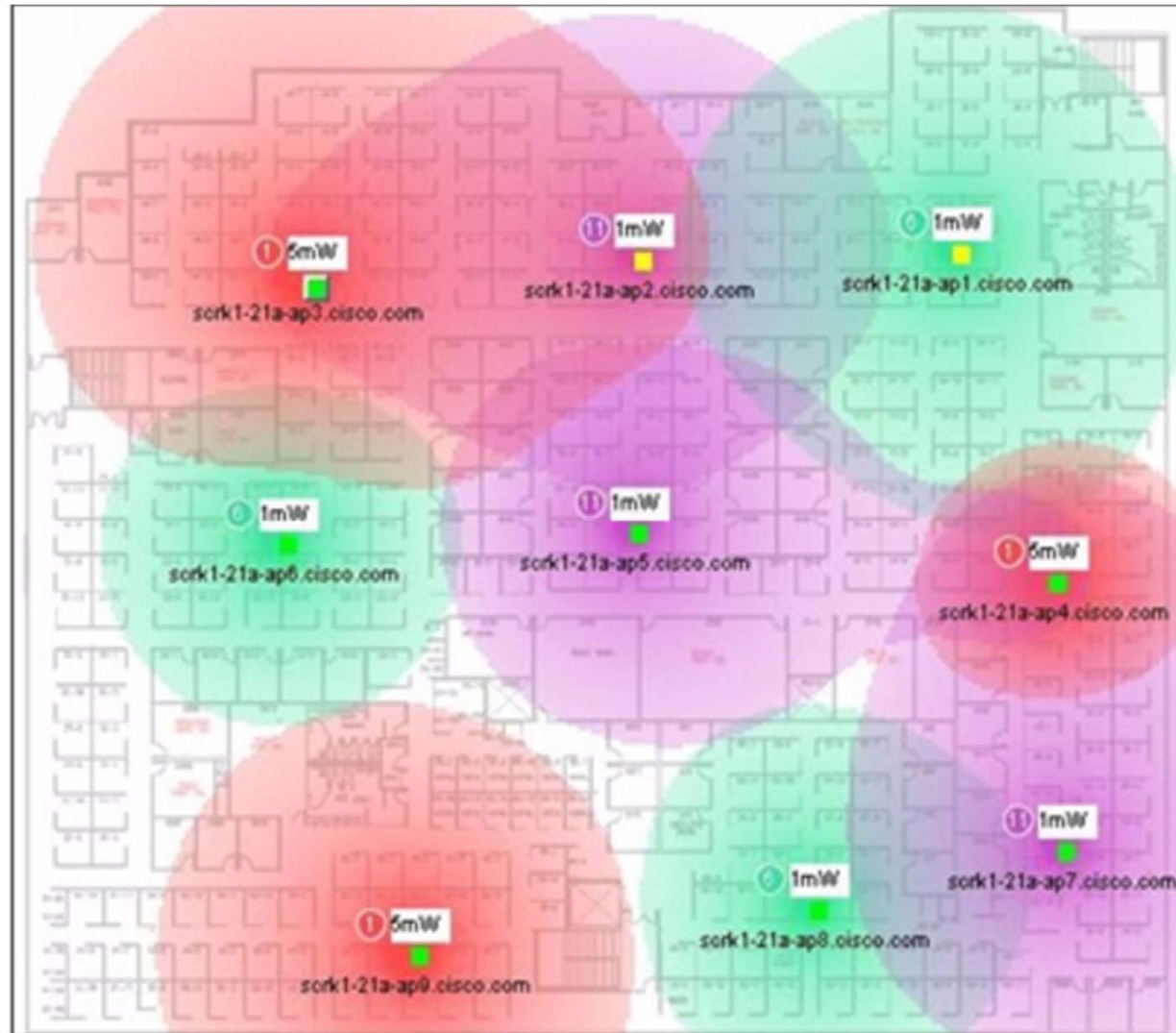
4.5. Nivel de aplicación (iv)



Un plan de seguridad para los servicios de comunicaciones
Subdirección de Comunicaciones



4.5. Nivel de aplicación (v)



Un plan de seguridad para los servicios de comunicaciones
Subdirección de Comunicaciones

6. Estructura

- **Veámos un ejemplo de cómo se documenta una determinada acción dentro del Plan de Seguridad.**



7. Conclusiones

- **Con la implantación de las acciones detalladas en el Plan de Seguridad lograremos entre todos un nivel de seguridad adecuado al momento tecnológico que estamos viviendo.**
- **Una infraestructura de red puntera como la de la ULPGC no se puede ver ensombrecida por problemas de seguridad.**
- **Una meta: conseguir por todos los medios el 99,999% de disponibilidad de los servicios que prestamos a la comunidad universitaria.**



8. Líneas futuras

- **Adecuar anualmente el Plan de Seguridad a las necesidades existentes.**
- **Ser ambiciosos e intentar conseguir objetivos en materia de seguridad que inicialmente puedan parecer imposibles.**
- **Conseguir la certificación ISO 17799.**



MUCHAS GRACIAS



UNIVERSIDAD DE LAS PALMAS DE GRAN CANARIA
Servicio de Informática y Comunicaciones

IV Jornada de Coordinación del SIC

Un plan de seguridad para los servicios
de comunicaciones

Área de Comunicaciones



Manuel Jerez Cárdenes
26 de noviembre de 2004

