ANEXO II

**REQUISITOS PARA LA NORMALIZACIÓN DE LAS REDES Y ENLACES
INALÁMBRICOS EN LA JUNTA DE ANDALUCÍA**

INDICE

INTRODUCCIÓN.....	4
CAPÍTULO 1: REQUISITOS DE DISEÑO E IMPLEMENTACIÓN DE REDES DE ÁREA LOCAL INALÁMBRICA Y ENLACES INALÁMBRICOS.....	6
1 PROYECTO TÉCNICO DE IMPLANTACIÓN DE REDES DE ÁREA LOCAL INALÁMBRICA.....	6
1.1 Antecedentes.....	6
1.1.1 Objetivo del proyecto.....	6
1.1.2 Ubicación.....	6
1.1.3 Requisitos.....	6
1.2 Memoria técnica.....	6
1.2.1 Ubicación de los puntos de acceso (APs).....	6
1.2.2 Estudio de cobertura de los puntos de acceso.....	7
1.2.3 Dimensionamiento de la WLAN.....	7
1.2.4 Equipamiento propuesto.....	8
1.2.5 Requisitos específicos para VoIP.....	9
1.2.6 Esquemas de interconexión con otras Redes de Área Local y/o RCJA.....	10
1.2.7 Etiquetado.....	10
1.3 Cumplimiento de la normativa.....	11
1.3.1 Normativa de la Junta de Andalucía.....	11
1.3.1.1 Cumplimiento de las Políticas de Seguridad para Redes Inalámbricas.....	11
1.3.2 Cumplimiento del Real Decreto 1066/2001.....	11
1.3.3 Cumplimiento de las limitaciones de potencia de los equipos.....	11
1.4 Documentación de fin de instalación.....	11
1.5 Plan de operación.....	12
2 PROYECTO TÉCNICO DE IMPLANTACIÓN DE SOLUCIONES DE CONECTIVIDAD INALÁMBRICA ENTRE EDIFICIOS.....	13
2.1 Antecedentes.....	13
2.1.1 Objetivo del proyecto.....	13
2.1.2 Requisitos.....	13
2.1.3 Justificación de la necesidad.....	13
2.2 Memoria técnica.....	14
2.2.1 Situación del enlace inalámbrico.....	14
2.2.2 Solución Técnica.....	14
2.2.2.1 Cálculos del radioenlace/WLAN propuesto.....	15
2.2.3 Equipamiento.....	15
2.2.4 Esquemas de interconexión con otras Redes de Área Local y/o RCJA.....	16
2.2.5 Etiquetado.....	16
2.3 Cumplimiento de la normativa.....	17
2.3.1 Normativa de la Junta de Andalucía.....	17
2.3.1.1 Cumplimiento de las Políticas de Seguridad para Redes Inalámbricas.....	17
2.3.2 Cumplimiento del Real Decreto 1066/2001.....	17
2.3.3 Cumplimiento de las limitaciones de potencia de los equipos.....	18
2.4 Documentación de fin de instalación.....	18
2.5 Plan de operación.....	18

CAPÍTULO 2: POLÍTICAS DE SEGURIDAD PARA REDES INALÁMBRICAS.....	20
1 MEDIDAS DE SEGURIDAD OBLIGATORIAS.....	20
1.1 Prevenir el acceso físico a los puntos de acceso.....	20
1.2 Restricción del alcance de los puntos de acceso.....	20
1.3 Nombre del ssid aleatorio o sin relación directa con la organización.....	20
1.4 Uso de algoritmos de cifrado.....	20
1.5 Uso de sistemas de autenticación independientes de los puntos de acceso.....	21
1.6 Cambios de configuración en los puntos de acceso para su administración.....	21
1.7 copia de seguridad de la configuración de los puntos de acceso y protección de la misma.....	21
1.8 Protocolo DE ADMINISTRACIÓN en los puntos de acceso.....	22
1.9 Permitir sólo redes de tipo “estructural” y no “AD HOC”.....	22
1.10 Actualización de FIRMWARE sobre los puntos de acceso.....	22
2 MEDIDAS DE SEGURIDAD RECOMENDABLES.....	22
2.1 Recomendaciones de configuración de los puntos de acceso.....	22
2.2 Control de acceso a las zonas de influencia de la red.....	23
2.3 Inhabilitación de los puntos de acceso en horas no laborables.....	23
2.4 Filtrar direcciones MAC en los puntos de acceso.....	23
2.5 Almacenar LOGS generados en los puntos de acceso en un dispositivo externo.....	23
2.6 No activar DHCP en la WLAN.....	23
2.7 Separación entre la red wireless y la red física.....	24
2.8 Instalación de un detector de intrusiones wireless.....	24
3 MEDIDAS RELATIVAS A LA IMPLEMENTACIÓN DE UNA RED ESPECÍFICA PARA INVITADOS.....	24
4 SEGUIMIENTO Y EXPLOTACIÓN DE REDES INALÁMBRICAS.....	25
4.1 Designación de un responsable de explotación local.....	25
5 POLÍTICA DE CONTRASEÑAS.....	25
CAPÍTULO 3: CERTIFICACIÓN Y VERIFICACIÓN DE LA INSTALACIÓN.....	26
CAPÍTULO 4: NORMATIVA APLICABLE Y LISTADO DE ACRÓNIMOS.....	27
6 NORMATIVA APLICABLE.....	27
6.1 Normativa inalámbrica.....	27
6.2 Otra normativa.....	28
7 RELACIÓN DE ACRÓNIMOS Y ABREVIATURAS.....	28

INTRODUCCIÓN

Las **redes de área local inalámbricas** o **wireless LAN** (en adelante WLAN) utilizan ondas electromagnéticas para enlazar los equipos conectados a la red, en lugar de los cables coaxiales o de fibra óptica que se utilizan en redes de área local cableadas convencionales. Las redes inalámbricas fueron creadas inicialmente para sustituir a las anteriores, terminando así con los problemas inherentes del cableado, como sus costes, dificultades de instalación y falta de movilidad.

En primer lugar, las redes inalámbricas proporcionan a los usuarios de una red local acceso a la información en tiempo real en cualquier lugar dentro de la organización o el entorno público en el que están desplegadas. De este modo se proporciona una solución de acceso y conectividad que permite la movilidad de los terminales en los casos en que sea necesario (reorganización departamental, clientes móviles, etc.).

En segundo lugar, la instalación de una red inalámbrica es rápida y fácil y reduce considerablemente o incluso elimina la necesidad de tirar cables a través de paredes y techos. La tecnología inalámbrica permite a la red llegar a puntos de difícil acceso para una red de área local cableada. Por ello, las conexiones inalámbricas pueden ampliar o sustituir a una infraestructura con cables cuando ésta resulta costosa o inabordable. Algunos tipos de construcciones o algunas normativas de construcción pueden prohibir el uso de cableado, lo que convierte a las redes inalámbricas en una importante alternativa.

En tercer lugar, cabe también destacar la escalabilidad de estas soluciones, ya que los sistemas inalámbricos pueden ser configurados en una variedad de topologías para satisfacer las necesidades de las instalaciones y aplicaciones específicas. Las configuraciones son sencillas de modificar y resulta muy fácil la incorporación de nuevos usuarios a la red.

Por último, y como consecuencia de todo lo anterior, cabe mencionar como otra de las ventajas de las soluciones inalámbricas, el reducido costo de propiedad: mientras que la inversión inicial requerida para una red inalámbrica puede ser más alta que el costo en hardware de una red de área local cableada, la inversión de toda la instalación y el costo durante el ciclo de vida puede ser significativamente inferior.

Todos estos factores son los que han contribuido a que la demanda de soluciones de conectividad de naturaleza inalámbrica haya sufrido un gran incremento en los últimos años, aunque no hayan llegado a sustituir totalmente a los sistemas cableados. La sustitución total suele realizarse únicamente en aquellos entornos en los que la movilidad de los equipos es necesaria o el cableado es muy difícil o costoso. En la mayoría de los casos, las redes inalámbricas se despliegan para complementar a la red cableada existente.

Pero junto a estas ventajas, este tipo de redes también presentan importantes inconvenientes como la limitación en el ancho de banda y, fundamentalmente, la falta de seguridad inherente a un modo de transmisión sin posibilidad de control físico en los accesos, como son las ondas radioeléctricas.

Al igual que ocurre con las redes de área local inalámbricas, también la instalación y explotación de **enlaces inalámbricos entre edificios** se están extendiendo cada vez más, sustituyendo a la contratación de accesos de datos a proveedores de servicios de telecomunicaciones. Este tipo de soluciones tienen limitaciones que no las hacen adecuadas para cualquier situación.

En atención a las ventajas e inconvenientes que puedan surgir por el establecimiento de redes de área local y enlaces inalámbricos, y con el fin de garantizar la seguridad y viabilidad de las mismas en el ámbito de la administración pública andaluza, se han recopilado una serie de normas y de recomendaciones para su diseño, instalación y explotación, que se desarrollan en el presente documento. El objeto del documento es por tanto, servir de guía de normalización en el proceso de implantación de redes de área local y enlaces inalámbricos en el ámbito de la Administración de la Junta de Andalucía.

En el primer capítulo se describen los requisitos de diseño e implementación tanto de redes como de enlaces inalámbricos, con el objeto de homogeneizar criterios a la hora de desarrollar los **proyectos técnicos** que se exigen como requisito previo a la autorización de dichas soluciones por parte de la Dirección General de Telecomunicaciones y Sociedad de la Información (DGTSI).

El segundo capítulo de este documento se dedica exclusivamente a describir el conjunto de reglas y recomendaciones que configuran las Políticas de Seguridad para redes inalámbricas.

En el tercer capítulo se indican las pruebas a realizar para la correcta certificación y verificación de las redes y enlaces inalámbricos.

Finalmente, en el cuarto capítulo, se incluye la normativa de aplicación y un listado de acrónimos.

CAPÍTULO 1: REQUISITOS DE DISEÑO E IMPLEMENTACIÓN DE REDES DE ÁREA LOCAL INALÁMBRICA Y ENLACES INALÁMBRICOS

En este capítulo se establecen los requisitos para el diseño y la instalación tanto de las redes de área local inalámbricas como de los enlaces inalámbricos entre edificios, en el ámbito de la Administración de la Junta de Andalucía, de forma que se garantice su correcto funcionamiento y el cumplimiento de las políticas de seguridad establecidas. Para ello, se describe en detalle el **Proyecto Técnico** que debe elaborarse para la implantación de estas soluciones. La presentación de dicho proyecto, acorde a lo establecido en este capítulo, es requisito previo para obtener autorización por parte de la DGTSI para la implantación de la red o enlace inalámbrico.

1 PROYECTO TÉCNICO DE IMPLANTACIÓN DE REDES DE ÁREA LOCAL INALÁMBRICA

A continuación se detallan los apartados que, como mínimo, deberá incluir el **Proyecto Técnico de Implantación de una WLAN**. Para cada apartado de dicho proyecto técnico, se realiza una breve descripción de los aspectos que habrán de tenerse en consideración de forma que se garantice el correcto diseño, dimensionamiento e implantación de la WLAN y todos los elementos que la constituyen. Para ello, se establecen algunos requisitos mínimos de obligado cumplimiento, que deberán aparecer explícitamente mencionados en el proyecto técnico, y también un conjunto de recomendaciones que se dejan a discreción del proyectista.

1.1 ANTECEDENTES

1.1.1 Objetivo del proyecto

Se realizará una descripción del proyecto, explicando el propósito de la red inalámbrica que se desea desplegar, así como la problemática particular existente en el centro donde se pretende instalar dicha red.

1.1.2 Ubicación

Se presentará una descripción de la localización física a la que se desea dotar de cobertura inalámbrica.

1.1.3 Requisitos

Se indicarán todos los requerimientos de la red inalámbrica objeto del proyecto, en términos de coberturas, funcionalidad y servicios, estimación del número de usuarios, tipo de tráfico y carga, etc.

Asimismo, se indicarán en caso de que sean necesarios, otros requisitos del proyecto tales como:

- Necesidad de conexión con redes ya existentes en el edificio.
- Requisitos estéticos necesarios para minimizar el impacto visual de la instalación.
- Necesidades específicas en cuanto a las condiciones de disponibilidad y mantenimiento de la solución.
- Cualesquiera otros requisitos que puedan afectar al diseño de la solución.

1.2 MEMORIA TÉCNICA

1.2.1 Ubicación de los puntos de acceso (APs)

Se aportarán los planos de las instalaciones, indicando la escala utilizada, y especificando de forma clara la ubicación prevista de los puntos de acceso.

Para seleccionar las ubicaciones de los APs se deberán tener en cuenta las siguientes medidas de carácter obligatorio:

- Se instalarán en lugares apropiados, con acceso restringido y controlado, para evitar manipulaciones. Se recomienda que su colocación permita comprobar el estado de los LEDs del equipo.
- Se ubicarán lejos de superficies metálicas (ascensores, armarios metálicos, falso techo metálico, etc), ya que este tipo de superficies pueden afectar a la señal de radiofrecuencia.
- Se colocarán lejos de elementos que generen interferencias RF (motores eléctricos, hornos microondas, etc).

1.2.2 Estudio de cobertura de los puntos de acceso

Se aportará un estudio de los niveles de señal con que se prevé dotar a la instalación, de manera que se cumplan los siguientes objetivos:

1. Disponer de cobertura en las ubicaciones marcadas como requisito.
2. Limitar en la medida de lo posible las emisiones fuera de las instalaciones, para evitar las “escuchas indeseadas” por personas situadas en el exterior del edificio (eavesdropping).
3. Cumplir la normativa vigente sobre emisiones radioeléctricas.

En este estudio se mostrará claramente la ubicación de los APs en las distintas zonas, áreas y plantas. Si se pretende instalar varias redes inalámbricas con distinta cobertura, y/o en varias plantas del edificio, habrá que diferenciar la cobertura de las mismas. Asimismo habrá que indicar el nivel mínimo de señal requerido en cada una de las zonas y el nivel máximo permitido.

Para la realización de este estudio de cobertura se recomienda usar el método del **replanteo previo**, aunque también se podría emplear un **software de planificación de RF** que esté adaptado a despliegues en interior, tenga soporte para los estándares usados y cumpla las recomendaciones que son de aplicación.

En el caso de seleccionar una solución que trabaje en la banda de 2.4 GHz, sería conveniente realizar un **estudio de frecuencia** mediante un analizador de espectro o similar, para averiguar qué **canales tienen menor nivel de interferencia** (de realizarse este estudio, se acompañaría al documento como justificación de los canales elegidos). En el caso de 5 GHz, este estudio no sería necesario ya que esa banda está menos saturada y, por tanto, más libre de interferencias.

1.2.3 Dimensionamiento de la WLAN

En este apartado se aportará el **estudio de la capacidad** que permitirá determinar el número de APs necesarios para poder dar servicio al número de usuarios estimado, en las zonas de interés y con los requisitos de capacidad que se han establecido.

El estudio de capacidad tendrá en cuenta las siguientes consideraciones:

- La necesidad de desplegar más de un punto de acceso dando cobertura a la misma zona, en ubicaciones donde se prevea un gran número de clientes inalámbricos simultáneos, de modo que se produzca un reparto de la carga entre esos puntos de acceso.

- El ancho de banda requerido por las aplicaciones que se van a soportar sobre la red inalámbrica.
- Podrían establecerse, dado el caso, limitaciones del ancho de banda usado por usuario o por perfil, de forma que los usuarios o perfiles con requisitos más exigentes no se vean afectados por el resto de usuarios de la red.
- Dependiendo de la red inalámbrica que se vaya a instalar, puede ser necesario, para su correcto funcionamiento, realizar una **planificación de los canales** adecuada, según los canales disponibles en Europa y el estándar y banda de frecuencia seleccionada. De ser así, se detallará esta planificación, y se mostrará claramente en los planos de cobertura. En este caso, la realización del estudio de frecuencia para averiguar qué canales tienen menos interferencias es aún más recomendable.

Como resultado del estudio de capacidad, y a modo de conclusión, se recomienda incluir en el proyecto las tablas resumen con la información mostrada a continuación:

Denominación del AP (siguiendo la misma nomenclatura que se utilice para identificarlo en los planos que acompañan al proyecto).
Identificación de la WLAN a la que da servicio y número de APs totales que dan servicio a esta WLAN.
Ubicación.
Frecuencia de trabajo y, a ser posible, el canal asignado.
Porcentaje del área de interés cubierta.
Nivel de señal mínimo estimado.
Número máximo estimado de clientes simultáneos.
Capacidad media en carga.
Capacidad media en pico.

1.2.4 Equipamiento propuesto

Los equipos inalámbricos seleccionados deben cumplir los siguientes requisitos mínimos, de carácter obligatorio:

- Deberán soportar estándares inalámbricos con capacidades suficientes para cumplir con los requisitos establecidos (se recomienda el estándar IEEE 802.11g o superior), que no tenga ninguna vulnerabilidad reconocida no solucionada, y que dispongan de certificado de interoperabilidad wifi definido por la W-IFI Alliance.
- Deberán cumplir todas las medidas de seguridad obligatorias incluidas en el capítulo 2 de políticas de seguridad, así como todas las medidas de seguridad recomendables de ese mismo capítulo que sean necesarias para cumplir con los requisitos de seguridad de la solución que se pretenda montar, y de acuerdo con la política de seguridad de la entidad.

Adicionalmente, a la hora de elegir el equipamiento, se tendrán en cuenta, de forma opcional, las siguientes recomendaciones:

- Posibilidad de desactivación de protocolos de administración remota (WEB, FTP y TELNET).
- Permitirán configurar parámetros de calidad de servicio, QoS (IEEE 802.1p).

- Soportarán VLAN (IEEE 802.1q) y asignación dinámica de VLAN's.
- Deberán ser de fabricantes reconocidos como suministradores de soluciones de conectividad inalámbrica.
- Facilidad de gestión, mantenimiento y resolución de problemas.
- La garantía de los equipos será de al menos tres años.
- Permitirán la creación de múltiples SSID en el interfaz inalámbrico.
- En determinadas instalaciones es recomendable emplear 802.3af (Power-Over-Ethernet), para poder alimentar el equipo usando el propio cable Ethernet de datos, ahorrando el tener que alimentar el equipo mediante un transformador de corriente.

En caso de optar por una gestión centralizada, no será necesario que los puntos de acceso tengan todas las funcionalidades individualmente, siempre que el sistema en su conjunto disponga de las mismas.

1.2.5 Requisitos específicos para VoIP

En caso de que la WLAN soporte servicios de VoIP, a lo que generalmente se conoce como VoWLAN, y para cumplir con las especiales características que necesitan este tipo de soluciones (priorización del tráfico de voz, gestión del ancho de banda, transición en la red, seguridad y vida de las baterías), se tendrán en cuenta los siguientes requisitos adicionales a los ya requeridos para los APs, que deberán ser contemplados en el proyecto técnico correspondiente:

- La WLAN deberá proporcionar el ancho de banda suficiente para el transporte de datos, tanto de VoIP como de otras aplicaciones, de forma concurrente y contemplando la simultaneidad de conexiones sobre cada punto de acceso. Habrá que tener en cuenta el codec utilizado y la señalización.
- Los APs deberán disponer de los siguientes certificados de interoperabilidad de la WIFI Alliance:
 - Wi-Fi Protected Access (WPA 2 Enterprise).
 - Wi-Fi Multimedia™ (WMM®)
 - Wi-Fi Multimedia Power Save™ (WMM Ahorro de energía®).
 - Wi-Fi Multimedia Admission Control™ (WMM Control de Admisión®).
 - NOTA: el certificado de interoperabilidad de Voz en WIFI de la WIFI Alliance (Wi-Fi CERTIFIED Voice-Enterprise) ya incluye los certificados indicados anteriormente.
- Otros requisitos que deberán cumplir los APs seleccionados y la WLAN son:
 - Deberán soportar la creación de VLAN, ya que será obligatorio crear una VLAN independiente para la VoIP.
 - Deberán soportar mecanismos de marcado de tráfico y calidad de servicio, al objeto de priorizar el tráfico de VoIP.

En cuanto a la cobertura de radiofrecuencia de la WLAN, las recomendaciones son las siguientes:

- La intensidad de señal mínima será de -70 dB para garantizar la calidad del audio.
- La distancia mínima entre dos zonas de cobertura WLAN con el mismo canal radioeléctrico debe ser -19 dBm.
- Las zonas de cobertura de los APs deberán solaparse entre un 20 y un 30% para garantizar la itinerancia segura.

Por último, se tendrán en cuenta las siguientes consideraciones adicionales:

- Será necesario desactivar el protocolo de asignación dinámica de direcciones IP (DHCP) ya que el servicio de VoIP requiere de direcciones IP estáticas.

- Se recomienda realizar un filtrado de MAC como medida de seguridad adicional.
- Los firewalls deben estar configurados para permitir la VoIP y permitir los paquetes de señalización.
- Para el tráfico de VoIP no deberá aplicarse la traducción de direcciones de red (NAT).

1.2.6 Esquemas de interconexión con otras Redes de Área Local y/o RCJA

Se incluirá el esquema lógico de interconexión con otras redes de área local del edificio y, en su caso, con los accesos de la Red Corporativa de Telecomunicaciones de la Junta de Andalucía (RCJA) y se detallarán las medidas tomadas para su protección.

Se recomienda, de acuerdo con las políticas de seguridad establecidas en el capítulo 2, que la red inalámbrica disponga de una VLAN separada de la red cableada, o varias VLANs dependiendo de las distintas WLANs que se quieran establecer, los perfiles de los usuarios o los recursos a los que se quiera dar acceso.

Adicionalmente, para redes WLAN de grandes dimensiones, se recomienda que la red inalámbrica disponga de un direccionamiento IP diferenciado de la red cableada, de tal forma que a todos los usuarios inalámbricos se les asigne direccionamiento IP dentro del segmento de red seleccionado, independientemente del punto de acceso al que se conecte, de la planta del edificio en que se encuentre, etc. Esto facilitaría la gestión de la/s WLAN/s y la seguridad de la misma.

1.2.7 Etiquetado

Todos los elementos de la instalación estarán convenientemente etiquetados, de forma que se puedan identificar de manera unívoca y permitan una correcta gestión y administración del sistema.

Las etiquetas de identificación cumplirán los siguientes requisitos:

- Se colocarán de modo que se acceda a ellas, se lean y se modifiquen con facilidad.
- Serán resistentes y la identificación deberá permanecer legible toda la vida útil prevista del cableado. No podrán estar escritas a mano.
- No deberán verse afectadas por humedad ni manchas cuando se manipulen.
- Las etiquetas empleadas en el exterior u otros entornos agresivos deberán diseñarse para resistir los rigores de dicho entorno.
- Si se realizan cambios, las etiquetas deberán inspeccionarse para determinar si es necesario actualizar a información recogida en las mismas.

Para la rotulación o etiquetado de los diferentes puntos de acceso de la WLAN, se seguirá la nomenclatura especificada a continuación, sin perjuicio de algún otro sistema de etiquetado unívoco que pudiera tenerse implantado, siempre que se justifique convenientemente que iguala o mejora el propuesto.

Como los APs están conectados a tomas de telecomunicaciones (TT) pertenecientes al sistema de cableado estructurado (SCE) del edificio, habrá que etiquetarlos de tal forma que se identifique fácilmente a qué toma, boca, panel y repartidor a la que van conectados. Y adicionalmente, sería interesante que este etiquetado refleje la red inalámbrica a la que pertenece el AP. Por lo tanto, el etiquetado propuesto es el siguiente: APz.y – x – i.j , donde: “z” identifica el número de AP, “y” la red WLAN a la que da servicio; y la notación “x-i.j” es la misma que la de la TT a la que se conecta, es decir, que identifica el repartidor de planta “x”, el panel “i” y la boca “j”.

Por ejemplo, tenemos en la primera planta una WLAN que la proporcionan dos AP, y en la tercera planta otra WLAN con tres AP. Así, los APs que conforman la WLAN 1 de la primera planta, tendrán el etiquetado AP1.1 – 1 – 4.5 (WLAN 1, AP 1, RP1, panel 4, boca 5) y AP1.2 – 1 – 4.6 (WLAN 1, AP 2, RP1, panel 4, boca 6). Mientras que los APs que conforman la WLAN 2 de la tercera planta se etiquetarían así AP2.1 – 3 – 5.6, AP2.2 – 3 – 5.7 y AP2.3 – 3 – 5.8.

1.3 CUMPLIMIENTO DE LA NORMATIVA

1.3.1 Normativa de la Junta de Andalucía

En este apartado se incluirá una declaración expresa del cumplimiento de la normativa vigente relativa a la instalación de Redes de Área Local Inalámbricas y Enlaces Inalámbricos en el ámbito de la Junta de Andalucía.

1.3.1.1 Cumplimiento de las Políticas de Seguridad para Redes Inalámbricas.

Se deberá justificar de forma detallada el cumplimiento de las medidas incluidas en el capítulo 2 y que constituyen las Políticas de Seguridad en redes inalámbricas, indicando claramente:

- El cumplimiento de las medidas de seguridad obligatorias.
- El listado de las medidas de seguridad recomendables adoptadas, así como cualquier otra medida a implementar para garantizar la seguridad de la instalación.

Se adjuntará una tabla resumen de consulta rápida, donde se indicará, para cada medida dentro de las políticas de seguridad de redes de área local inalámbricas, su nivel de cumplimiento por la presente normativa y si es de aplicación en el presente proyecto.

1.3.2 Cumplimiento del Real Decreto 1066/2001

En este apartado se incluirá la justificación del cumplimiento del Real Decreto 1066/2001 de 28 de septiembre de 2001, por el que se aprueba el Reglamento que establece condiciones de protección del dominio público radioeléctrico, restricciones a las emisiones radioeléctricas y medidas de protección sanitaria frente a emisiones radioeléctricas.

1.3.3 Cumplimiento de las limitaciones de potencia de los equipos

La instalación diseñada en el proyecto técnico debe cumplir las limitaciones de potencia de los equipos establecidas por el Cuadro Nacional de Atribución de Frecuencias (CNAF) o normativa de rango superior.

1.4 DOCUMENTACIÓN DE FIN DE INSTALACIÓN

Este apartado describe la documentación mínima que es necesario generar a la finalización de la ejecución del proyecto técnico, con el objeto de verificar la correcta instalación y funcionamiento de los elementos descritos en el mismo. Se incluirá como apartado dentro del proyecto técnico, para garantizar su cumplimiento por parte de la empresa instaladora.

- Descripción de las tareas llevadas a cabo en la instalación y cumplimiento de las normas generales de la instalación.
- Detalle de la situación definitiva de todos los elementos que conforman la instalación, aportando documentación gráfica de la misma.

- Listado de todo el equipamiento inalámbrico instalado, descripción de sus características técnicas y configuración detallada.
 - Se recomienda incluir una tabla con todos los parámetros, o al menos los más relevantes.
 - Se recomienda adjuntar ficha/hoja técnica del equipamiento, así como documento que acredite normalización del equipo, el marcado CE y la declaración de conformidad que cubra la Directiva europea 1999/5/CE.
- Planificación radioeléctrica definitiva. Medición de los niveles de señal e interferencia obtenidos (mapas de cobertura).
- Verificación de las políticas de seguridad implementada en la red inalámbrica. Se recomienda el uso de checklists donde se pueda comprobar punto por punto que las políticas acordadas en el proyecto técnico de implantación se encuentran correctamente desplegadas.
- Informe de certificación de la red, que recoja las pruebas de conectividad realizadas para la comprobación del correcto funcionamiento de la red. Para llevar a cabo la certificación, se seguirán las recomendaciones especificadas en el capítulo 3 del presente documento.
- Garantía de la instalación realizada y de los distintos fabricantes, condiciones de mantenimiento y ANS contratados.

Se incluirá justificación de cualquier desviación producida con respecto al proyecto inicial, en cualquiera de los apartados de la documentación.

1.5 PLAN DE OPERACIÓN

Sería conveniente incluir un plan de gestión, explotación y seguimiento de la instalación, con el objetivo de garantizar la seguridad de la misma y el cumplimiento continuado de las políticas de seguridad establecidas en el proyecto técnico. Concretamente, se podrían incluir en este apartado medidas como:

- La designación de un responsable de explotación local.
- Un plan de control de acceso a los recursos de red (implementación de una política de contraseñas adecuada, etc).
- Una política de uso de la red, con el objeto de definir el tipo de información/documentación que podrá circular por la infraestructura.
- Procedimientos para la gestión de incidentes.
- Procedimientos y periodicidad de análisis de seguridad y de las vulnerabilidades de la instalación, incluyendo una revisión de la cobertura de los puntos de acceso de la red.
- Plan de formación adecuado para usuarios y personal técnico.

2 PROYECTO TÉCNICO DE IMPLANTACIÓN DE SOLUCIONES DE CONECTIVIDAD INALÁMBRICA ENTRE EDIFICIOS

En este capítulo se detallan los apartados y el contenido que, como mínimo, debe incluir un **Proyecto Técnico de Enlace Inalámbrico** para garantizar el correcto despliegue de este tipo de soluciones. Para cada uno de dichos apartados, se realiza una breve descripción de los aspectos a considerar para garantizar

el correcto diseño, dimensionamiento e implantación del enlace. Para ello, se establecen algunos requisitos mínimos de obligado cumplimiento, que deberán aparecer explícitamente mencionados en el proyecto técnico, y también un conjunto de recomendaciones que se dejan a discreción del organismo.

2.1 ANTECEDENTES

2.1.1 Objetivo del proyecto

Se describirá la problemática que se pretende resolver con la solución de conectividad entre edificios y/o el propósito concreto de la misma.

2.1.2 Requisitos

Se indicarán todos los requisitos de la solución de conectividad entre edificios, adjuntando una tabla resumen con los datos básicos de los radioenlaces que se pretenden instalar. Al menos se aportará la siguiente información:

- Se describirán los extremos del enlace inalámbrico que se pretende montar, la distancia del enlace y la ubicación prevista de los elementos en cada extremo.
- Se indicará también una estimación del número de clientes que harán uso del enlace inalámbrico.
- Se dará una estimación del tipo de tráfico y carga que va a soportar el enlace, así como una estimación de la velocidad o ancho de banda del enlace inalámbrico requerido.
- Se detallarán las necesidades de conexión con redes ya existentes en el edificio, en caso de que sean necesarias.
- Se indicará si existe algún requisito de carácter específico de seguridad, estético, de disponibilidad o mantenimiento del servicio, o cualquier otro que deba ser mencionado.
- Se justificará la necesidad o no de la instalación de Sistemas de Alimentación Ininterrumpida SAI para la protección de los equipos frente a fallos eléctricos.

2.1.3 Justificación de la necesidad

Será necesario justificar la elección del enlace inalámbrico como solución de conectividad frente a las soluciones corporativas existentes en catálogo de servicios de la RCJA, realizando una comparativa tanto a nivel económico como de condiciones de disponibilidad y mantenimiento. Para el cálculo económico, se deberán tener en cuenta los periodos de garantía y mantenimiento de los servicios de RCJA para que sea posible realizar la comparación.

Además, de existir dos o más soluciones que cumplan los requisitos necesarios para constituir el enlace inalámbrico requerido, se indicará el criterio o decisión por el cual se ha elegido la solución incluida en el proyecto técnico.

2.2 MEMORIA TÉCNICA

2.2.1 Situación del enlace inalámbrico

Se adjuntará el plano de planta de la zona, donde figuren tanto el enlace como la ubicación de los extremos del mismo, con sus coordenadas geográficas, e indicación del código de sede RCJA, si es el caso. Es importante indicar la distancia en metros a la que se encuentran los puntos que constituirán el enlace. Si es posible, se incluirá el perfil del enlace donde se muestre la orografía del terreno y donde se aprecie que existe línea de visión directa entre los puntos a enlazar.

Se deberá tener en cuenta que la distancia máxima típica en banda libre es de 500 metros en entornos urbanos y de 3 Km en entornos rurales.

2.2.2 Solución Técnica

En este apartado se especificarán los principales parámetros técnicos de la solución implementada, tanto en el enlace principal como en el de respaldo, si lo hubiera.

Se indicará la banda de frecuencia en la que se pretende que funcione el enlace inalámbrico, con indicación de los canales que se seleccionarán. Se mencionará la nota UN de CNAF que habrá que cumplir:

- En caso de solución en banda libre, es recomendable implementar WiMAX Puro (IEEE 802.16-2009), siendo como mínimo exigible IEEE 802.11h, con Selección Dinámica de Frecuencia DFS (Dynamic Frequency Selection) y Control de Potencia del Transmisor TPC (Transmitter Power Control). Es preferible la banda de los 5GHz (de 5,470 a 5,725 GHz), empleando tecnología WiMAX, para mayor fiabilidad y estabilidad.
- En caso de optar por la solución WiFi, es necesario que los equipos soporten como mínimo prestaciones IEEE 802.11g. En el caso de elegir este tipo de solución, habrá que indicar la banda de frecuencias elegida, la frecuencia a la que trabaja y, dado el caso, el canal seleccionado.

En la realización de radioenlaces en banda de uso común es muy importante la elección de canales que presenten los niveles de interferencias más bajos posibles. Como norma general es más adecuado utilizar soluciones que trabajen en la banda de 5 GHz, ya que hay un mayor número de canales disponibles, un menor uso a nivel residencial y por tanto los niveles de interferencia son mucho menores que en la banda de 2.4 GHz.

En el caso de trabajar en 2,4 GHz, se recomienda realizar un estudio de frecuencia mediante un analizador de espectro o similar, para averiguar qué canales tienen menor nivel de interferencia (en caso de realizarse este estudio, se acompañaría al documento como justificación de los canales elegidos). En el caso de 5 GHz, este estudio no es necesario ya que, además de que la banda está más libre de interferencias, en la única subbanda permitida para exteriores (5,4 a 5,7 GHz) los equipos deben tener activada la Selección Dinámica de Frecuencias (DFS) y el Control Automático de Potencia (TPC), según la normativa europea transpuesta en España en el CNAF mediante la Nota UN-128 (estándar IEEE 802.11h).

En el caso de que haya que establecer varios radioenlaces es necesario elaborar la planificación de frecuencias cuando exista la posibilidad de que interfieran entre ellos.

En lo referente a los elementos radiantes, se recomienda que las antenas sean muy directivas, para reducir la emisión de potencia, evitar en lo posible el multitrayecto, y mitigar desvanecimientos.

Se indicará la capacidad del enlace que finalmente implementa la solución presentada.

En lo referente al cifrado, encriptación y autenticación de las comunicaciones, se deberá garantizar el cumplimiento de los requisitos establecidos en los apartados 1.4. y 1.5 del capítulo 2 del presente anexo.

Si, además del enlace inalámbrico principal, por la importancia de la comunicación establecida, y el requisito de disponibilidad del servicio, fuese necesario disponer de un enlace de respaldo, habría que indicar el protocolo que se configurará para su correcto funcionamiento, siendo deseable la conmutación automática entre principal y reserva, pero siempre con ancho de banda garantizado. Algunas recomendaciones adicionales sobre los enlaces de respaldo se ofrecen a continuación:

- Se recomienda una protección mínima del enlace 1+1 en TX/RX, siendo el respaldo de al menos el 50% del ancho de banda del principal.
- Se recomienda un respaldo mínimo inalámbrico en la banda de 5 Ghz o doble trayecto. Según la criticidad del servicio se requerirán medidas de respaldo adicionales.

Además de la garantía del equipamiento se recomienda que la instalación que se realice tenga una garantía de al menos 3 años.

2.2.2.1 Cálculos del radioenlace/WLAN propuesto

El cálculo del radioenlace es un punto fundamental del proyecto técnico. Gracias a estos cálculos se obtendrá una estimación previa de los niveles de señal que se tendrán en cada uno de los puntos que se quieran interconectar, así como una estimación inicial del throughput que se obtendrá.

Por lo tanto, se incluirá en la memoria técnica el cálculo del radioenlace propuesto, donde deberá apreciarse con claridad que con la potencia de emisión máxima permitida, según la frecuencia elegida, la ganancia de los elementos radiantes y las pérdidas introducidas por los distintos elementos, se recibe en el extremo receptor suficiente señal para el correcto funcionamiento del enlace.

2.2.3 Equipamiento

Los equipos inalámbricos seleccionados deben cumplir los siguientes requisitos mínimos, de carácter obligatorio:

- En caso de optar por una solución en banda libre, los equipos deberán soportar los estándares inalámbricos adecuados (IEEE 802.11 en caso de WIFI, e IEEE 802.16-2009 en caso de optar por WIMAX), con capacidades suficientes para cumplir con los requisitos establecidos, que no tengan ninguna vulnerabilidad reconocida no solucionada, y deberán disponer del certificado de interoperabilidad definido por la entidad certificadora correspondiente (Wi-Fi Alliance o del Wimax Forum).
- En caso de seleccionar otro tipo de soluciones, se detallarán éstas y se justificará convenientemente la elección.
- Los equipos deberán disponer de las siguientes funcionalidades:
 - En caso de tecnología WIFI, los requisitos son los incluidos en el apartado 1.2.4 de este capítulo 1 (con el nivel de cumplimiento indicado en este apartado).
 - En caso de optar por otras tecnologías, los requisitos serán equivalentes a los establecidos para WIFI, debiendo justificarse convenientemente.

Será obligatorio que los equipos vengan protegidos para funcionar en exteriores y ante situaciones climatológicas adversas. Así, se recomienda que el rango de temperatura de operación esté entre 20°C a 50°C.

Adicionalmente, a la hora de elegir el equipamiento se tendrán en cuenta, de forma opcional, las siguientes recomendaciones:

- Que los equipos permitan realizar modulación adaptativa según condiciones del enlace y control automático de potencia.

En cuanto a los niveles de calidad del servicio, se establecen los siguientes requisitos:

- Se recomienda que la garantía de los equipos sea de al menos 3 años.
- La atención al cliente podrá ser un servicio online cuando se trate de un radioenlace de respaldo, pero será necesaria la atención telefónica cuando el radioenlace sirva como acceso principal a RCJA.
- Se dispondrá de un servicio de atención al cliente adecuado a la criticidad de la sede a la que da servicio el radioenlace, siendo como mínimo los mostrados en la siguiente figura. Estos tiempos podrán relajarse siempre y cuando el radioenlace se instale como respaldo de un acceso principal corporativo o no sirva para acceder a RCJA.

	Acceso Ppal.	Acceso de Respaldo
Disponibilidad del Servicio	99,95%	99,95%
Atención al Cliente	24 x 7	8 x 5
Tiempo de Respuesta ante averías	45 min	4 h
Tiempo de Resolución ante averías	4 h	NBD *

2.2.4 Esquemas de interconexión con otras Redes de Área Local y/o RCJA

Se detallará la interconexión que tendrá el enlace inalámbrico con Redes de Área Local (LAN) y accesos a la Red Corporativa de Telecomunicaciones de la Junta de Andalucía (RCJA), en ambos extremos del enlace, así como las medidas concretas que se implementarán para garantizar la seguridad del sistema. Habrá que incluir un esquema lógico de la solución.

2.2.5 Etiquetado

Todos los elementos de la instalación estarán convenientemente etiquetados, de forma que se puedan identificar de manera unívoca y permitan una correcta gestión y administración del sistema.

Las etiquetas de identificación cumplirán los siguientes requisitos:

- Se colocarán de modo que se acceda a ellas, se lean y se modifiquen con facilidad.
- Serán resistentes y la identificación deberá permanecer legible toda la vida útil prevista del cableado. No podrán estar escritas a mano.
- No deberán verse afectadas por humedad ni manchas cuando se manipulen.
- Las etiquetas empleadas en el exterior u otros entornos agresivos deberán diseñarse para resistir los rigores de dicho entorno.

- Si se realizan cambios, las etiquetas deberán inspeccionarse para determinar si es necesario actualizar a información recogida en las mismas.

Para la rotulación o etiquetado de los diferentes equipos, se seguirá la nomenclatura especificada a continuación, sin perjuicio de algún otro sistema de etiquetado unívoco que pudiera tenerse implantado, siempre que se justifique convenientemente que iguala o mejora el propuesto.

Todos los elementos que constituyen los enlaces inalámbricos podrán ir etiquetados con la siguiente notación: $Wz - x - i,j$, donde: “z” identifica en enlace inalámbrico (principal y respaldo); y “x-i,j” se refiere a la de la TT a la que se conecta, es decir, que identifica el repartidor de planta “x”, el panel “i” y la boca “j”.

2.3 CUMPLIMIENTO DE LA NORMATIVA

2.3.1 Normativa de la Junta de Andalucía

En este apartado se incluirá una declaración expresa al cumplimiento de la normativa vigente relativa a la instalación de Redes de Área Local Inalámbricas y Enlaces Inalámbricos en el ámbito de la Junta de Andalucía.

2.3.1.1 Cumplimiento de las Políticas de Seguridad para Redes Inalámbricas.

Se deberá justificar de forma detallada el cumplimiento de las medidas incluidas en el capítulo 2 y que constituyen las Políticas de Seguridad en redes inalámbricas, indicando claramente:

- El cumplimiento de las medidas de seguridad obligatorias.
- El listado de las medidas de seguridad recomendables adoptadas, así como cualquier otra medida a implementar para garantizar la seguridad de la instalación.

Se adjuntará una tabla resumen de consulta rápida, donde se indicará, para cada requisito dentro de las políticas de seguridad de Redes de Área Local Inalámbricas, su nivel de cumplimiento por la presente normativa y si es de aplicación en el presente proyecto. Dado que algunas de las recomendaciones no son aplicables en el caso de interconexión de redes mediante enlaces punto a punto/multipunto, en el análisis detallado de la política de seguridad para la solución de conectividad inalámbrica propuesta, se señalarán aquéllas que no tiene sentido aplicar para dicho enlace.

2.3.2 Cumplimiento del Real Decreto 1066/2001

En este apartado se incluirá la justificación del cumplimiento del Real Decreto 1066/2001 de 28 de septiembre de 2001, por el que se aprueba el Reglamento que establece condiciones de protección del dominio público radioeléctrico, restricciones a las emisiones radioeléctricas y medidas de protección sanitaria frente a emisiones radioeléctricas.

2.3.3 Cumplimiento de las limitaciones de potencia de los equipos

Será necesario justificar el cumplimiento de la limitaciones de potencia de los equipos establecidas por el Cuadro Nacional de Atribución de Frecuencias (CNAF) o normativa de rango superior (haciendo referencia a la nota UN en la que se regula, en función de la frecuencia). Así, se hará referencia a los cálculos realizados y presentados en la memoria técnica para el cálculo de la potencia a la que emitirá el enlace.

2.4 DOCUMENTACIÓN DE FIN DE INSTALACIÓN

Este apartado describe la documentación mínima que es necesario generar a la finalización de la ejecución del proyecto técnico, con el objeto de verificar la correcta instalación y funcionamiento de los elementos descritos en el mismo. Se incluirá como apartado dentro del proyecto técnico, para garantizar su cumplimiento por parte de la empresa instaladora.

- Descripción de las tareas llevadas a cabo en la instalación y cumplimiento de las normas generales de la instalación.
- Detalle de la situación definitiva de todos los elementos que conforman la instalación, aportando documentación gráfica de la misma.
- Listado de todo el equipamiento inalámbrico instalado, descripción de sus características técnicas y configuración detallada.
 - Se recomienda incluir una tabla con todos los parámetros, o al menos los más relevantes.
 - Se recomienda adjuntar ficha/hoja técnica del equipamiento, así como documento que acredite normalización del equipo, el marcado CE y la declaración de conformidad que cubra la Directiva europea 1999/5/CE.
- Planificación radioeléctrica definitiva. Medición de los niveles de señal e interferencia obtenidos (mapas de cobertura).
- Verificación de la política de seguridad implementada. Se recomienda el uso de checklists donde se pueda comprobar punto por punto que las políticas acordadas en el proyecto técnico de implantación se encuentran correctamente desplegadas.
- Informe de certificación del enlace, que recoja las pruebas de conectividad realizadas para la comprobación de su correcto funcionamiento. Para llevar a cabo la certificación, se seguirán las recomendaciones especificadas en el Capítulo 3 del presente documento.
- Garantía de la instalación realizada y de los distintos fabricantes, condiciones de mantenimiento y ANS contratados.

Se incluirá justificación de cualquier desviación producida con respecto al proyecto inicial, en cualquiera de los apartados de la documentación.

2.5 PLAN DE OPERACIÓN

Sería conveniente incluir un plan de explotación y seguimiento de la instalación, con el objetivo de garantizar su correcto funcionamiento, así como el nivel de calidad y seguridad establecidos en el proyecto técnico.

Alguno de los aspectos que podrían incluirse en el plan de gestión, explotación y seguimiento son:

- Política de uso de la red, con el objeto de definir el tipo de información/documentación que podrá circular por la infraestructura.
- Procedimientos para la gestión de incidentes.
- Procedimientos y periodicidad de análisis de seguridad de la infraestructura.
- Plan de formación adecuado para usuarios y personal técnico.

CAPÍTULO 2: POLÍTICAS DE SEGURIDAD PARA REDES INALÁMBRICAS

En este capítulo se muestra un conjunto de reglas a seguir en la implantación de redes inalámbricas, constituyendo éstas las políticas de seguridad de este tipo de redes. Cada regla lleva asociado un determinado nivel de cumplimiento:

- **Obligatorio:** su cumplimiento es requisito indispensable para poner en funcionamiento la red.
- **Recomendable:** su cumplimiento es altamente recomendable, en aras de la seguridad de la red inalámbrica.

1 MEDIDAS DE SEGURIDAD OBLIGATORIAS

1.1 PREVENIR EL ACCESO FÍSICO A LOS PUNTOS DE ACCESO

- El punto de acceso es el lugar por el que pasan todas las comunicaciones. Para evitar la manipulación de los mismos es necesario que sean ubicados en lugares apropiados, con acceso restringido y controlado.
- Nivel de cumplimiento: **Obligatorio.**

1.2 RESTRICCIÓN DEL ALCANCE DE LOS PUNTOS DE ACCESO

- Restringir el alcance de los puntos de acceso a menores distancias es una buena medida de prevención, ya que obliga al atacante a estar físicamente en un lugar controlado por la organización. Para ello se debe comprobar que el límite exterior de la red inalámbrica no quede fuera del perímetro del edificio o de los edificios de la organización, en la medida de lo posible.
- En el caso de enlaces inalámbricos, deberán usarse antenas direccionales, con el objeto de minimizar la dispersión de la radiación.
- Nivel de cumplimiento: **Obligatorio.**

1.3 NOMBRE DEL SSID ALEATORIO O SIN RELACIÓN DIRECTA CON LA ORGANIZACIÓN

- El SSID es el nombre por el que se identifica la red inalámbrica. Sin conocer el SSID ni las claves es difícil acceder a una red inalámbrica. Por ello no se deben utilizar nombres relativos a la organización y no deben contener información útil para un atacante.
- No podrá usarse como SSID de los puntos de acceso el que viene configurado por defecto por los fabricantes.
- Nivel de cumplimiento: **Obligatorio.**

1.4 USO DE ALGORITMOS DE CIFRADO

- En ningún caso se podrá instalar una red inalámbrica sin cifrar las comunicaciones.
- Para cifrar las comunicaciones en el interfaz aéreo se deberá utilizar el algoritmo de cifrado reconocido más avanzado y que proporcione mayor seguridad y garantías, el cual deberá estar recogido o incluido en el estándar de tecnología inalámbrica vigente. Actualmente deberá utilizarse el

algoritmo de cifrado basado en AES (Advanced Encryption Estándar) contemplado en el estándar 802.11i (WPA2), en ningún caso podrá utilizarse WEP.

- Se desactivará todo mecanismo o funcionalidad que tenga alguna vulnerabilidad reconocida y no solucionada. Así, se deberá desactivar el mecanismo WPS (Wi-Fi Protect Setup), dada sus reconocidas vulnerabilidades.
- Nivel de cumplimiento: **Obligatorio.**

1.5 USO DE SISTEMAS DE AUTENTICACIÓN INDEPENDIENTES DE LOS PUNTOS DE ACCESO

- Se deberán utilizar mecanismos de autenticación acordes a las necesidades de seguridad de la entidad o a la política de seguridad, dado el caso, que ésta tenga establecida, o vaya a establecer en el futuro. Deberán seleccionarse mecanismos de autenticación independientes de los puntos de acceso. Los protocolos que actualmente suelen utilizarse son EAP/TLS y EAP/TTLS o EAP/PEAP.
- En caso de que el mecanismo elegido use certificados digitales, deberán utilizarse certificados emitidos por alguna Autoridad de Certificación reconocida y configurar los clientes para validar dichos certificados.
- Nivel de cumplimiento: **Obligatorio.**

1.6 CAMBIOS DE CONFIGURACIÓN EN LOS PUNTOS DE ACCESO PARA SU ADMINISTRACIÓN

- Se deben cambiar de forma obligatoria las contraseñas configuradas por defecto en los puntos de acceso, debiendo utilizar en su lugar otras suficientemente robustas y de acuerdo a la “política de contraseñas”.
- En caso de tener que realizar un cambio de configuración en un AP se requerirá que el dispositivo disponga de un control de acceso de usuarios, sea cual sea su método de administración, y en caso de que sea remoto, deberá hacerse utilizando un canal seguro (como por ejemplo SSL).
- Deberán restringirse las direcciones IP que pueden acceder como administrador a los APs.
- La administración no se realizará nunca a través del medio inalámbrico.
- Nivel de cumplimiento: **Obligatorio.**

1.7 COPIA DE SEGURIDAD DE LA CONFIGURACIÓN DE LOS PUNTOS DE ACCESO Y PROTECCIÓN DE LA MISMA

- En caso de producirse un reseteo de la configuración del punto de acceso, es muy útil disponer de una salvaguarda de toda la configuración. La mayor parte de dispositivos almacenan toda la configuración en archivos que es posible descargar por distintas vías. En estos archivos se almacena información de claves de cifrado y contraseñas de acceso, por lo que es necesario protegerla.
- Será obligatorio realizar copias de seguridad de la configuración de los puntos de acceso, con la periodicidad que se haya establecido, dado el caso, en la política de seguridad de la entidad. De esta forma el procedimiento de contingencia para volver a poner los dispositivos “en producción”, puede realizarse por personal poco especializado y en un breve periodo de tiempo.
- Se deberá deshabilitar la descarga de estos archivos a través de métodos de acceso no seguros, como por ejemplo FTP, HTTP, etc.
- Nivel de cumplimiento: **Obligatorio.**

1.8 PROTOCOLO DE ADMINISTRACIÓN EN LOS PUNTOS DE ACCESO

- Deberá utilizarse un protocolo de administración de puntos de acceso que disponga de mecanismos robustos de autenticación. Actualmente, el más extendido es SNMP, por lo que, en caso de utilizarse éste, deberá emplearse SNMPv3 y ser evitadas las versiones anteriores. En caso de utilizar alguna de las dos primeras versiones, se deben conocer y aceptar en la organización los riesgos que su uso introduce. El control de acceso a la información proporcionada por SNMP debe ser adecuado.
- En caso de no utilizarse un protocolo de administración, se deberá desactivar el mismo de los puntos de acceso.
- En caso de que no sea posible su desactivación, será necesario realizar los cambios en la configuración oportunos para evitar la administración de los puntos de acceso por terceros. Así, si no fuera posible deshabilitar SNMP, será obligatorio cambiar los nombres de las “comunidades” por defecto “Public” y “Private”, por otros más difíciles de obtener (se pueden aplicar las reglas de las políticas de contraseñas para los nombres de las comunidades).
- Nivel de cumplimiento: **Obligatorio**.

1.9 PERMITIR SÓLO REDES DE TIPO “ESTRUCTURAL” Y NO “AD HOC”

- En una red “ad hoc” las comunicaciones se realizan directamente entre los emisores y receptores, sin pasar por un punto central (punto de acceso). Esto facilita la implantación de la red, sin embargo, son extremadamente difíciles de securizar. Sólo se deben permitir redes de tipo “estructural”, en las que todas las comunicaciones pasan a través del punto de acceso y se pueden securizar de forma centralizada.
- Nivel de cumplimiento: **Obligatorio**.

1.10 ACTUALIZACIÓN DE FIRMWARE SOBRE LOS PUNTOS DE ACCESO

- Es necesario actualizar los AP's a sus últimas versiones de firmware, mas aún si las nuevas versiones traen mejoras relativas a la seguridad del protocolo, encriptación de los datos, autenticación de los usuarios o cualquier otra característica relacionada con la seguridad (ver apartado “Seguimiento y explotación de redes inalámbricas”).
- Nivel de cumplimiento: **Obligatorio**.

2 MEDIDAS DE SEGURIDAD RECOMENDABLES

2.1 RECOMENDACIONES DE CONFIGURACIÓN DE LOS PUNTOS DE ACCESO

- Se recomienda deshabilitar todos aquellos protocolos y servicios de los puntos de acceso que no vayan a ser utilizados, siempre que sea posible.
- Nivel de cumplimiento: **Recomendable**.

2.2 CONTROL DE ACCESO A LAS ZONAS DE INFLUENCIA DE LA RED

- A nivel técnico se puede limitar el alcance para tratar de no emitir fuera del perímetro del edificio. Sin embargo, si un atacante puede entrar al edificio libremente con un dispositivo portátil el peligro de intrusión permanece. Por lo tanto, se deberá controlar el acceso a las zonas de influencia dentro del propio edificio.
- Nivel de cumplimiento: **Recomendable**.

2.3 INHABILITACIÓN DE LOS PUNTOS DE ACCESO EN HORAS NO LABORABLES

- Normalmente, los ataques suelen realizarse en horas en las que el atacante sabe que no va a alertar (de inmediato) a los administradores y puede proceder con tranquilidad y tiempo. Por ello, es recomendable el apagado de los puntos de acceso durante las horas en que no son utilizados, especialmente fines de semana, días festivos, etc. Si el *hardware* no permite esta posibilidad se podrán utilizar enchufes con programadores de tiempo. En su defecto, deberá inhabilitarse el sistema inalámbrico de cualquier otra forma que, aunque no implique el apagado de los AP's, impida el acceso vía radio al sistema.
- Nivel de cumplimiento: **Recomendable**.

2.4 FILTRAR DIRECCIONES MAC EN LOS PUNTOS DE ACCESO

- Con esta medida, se permite que sólo las tarjetas inalámbricas autorizadas puedan acceder a la red, y se evita de esta forma el acceso desde puestos cuya dirección MAC no haya sido dada de alta en la lista de acceso. A pesar de que es conocido que un atacante puede cambiar la dirección MAC de su tarjeta, esta medida, combinada con el resto de medidas de seguridad, sí puede resultar efectiva, ya que introduce un grado adicional de dificultad a los posibles atacantes de la red.
- Nivel de cumplimiento: **Recomendable**

2.5 ALMACENAR LOGS GENERADOS EN LOS PUNTOS DE ACCESO EN UN DISPOSITIVO EXTERNO

- En los AP's que dispongan de esta funcionalidad se deberá activar el servicio de "LOG", y enviarlo a un servidor externo, para que en caso de que el AP sea alterado, se disponga de una prueba de cuando se produjo el acceso. También será necesario revisar estos LOG's cada cierto tiempo para comprobar que sólo se ha accedido al AP por el/los administradores.
- Nivel de cumplimiento: **Recomendable**

2.6 NO ACTIVAR DHCP EN LA WLAN

- Se recomienda no activar DHCP, u otro protocolo de asignación dinámica de direcciones IP, para evitar que un atacante obtenga una dirección IP de forma sencilla, obligándole a tener que capturar y analizar el tráfico de la red en busca de los parámetros de red utilizados (rango de direcciones IP utilizado, DNS, Gateway, etc.).
- Nivel de cumplimiento: **Recomendable**

2.7 SEPARACIÓN ENTRE LA RED WIRELESS Y LA RED FÍSICA

- Es recomendable la instalación de un cortafuegos (firewall) entre los AP's y la red local, para separar las redes.
- Asimismo, es recomendable el uso de diferentes VLAN, que distingan entre usuarios inalámbricos y cableados, o bien para poder hacer uso de diferentes perfiles de usuarios inalámbricos.
- Nivel de cumplimiento: **Recomendable**

2.8 INSTALACIÓN DE UN DETECTOR DE INTRUSIONES WIRELESS

- La política de seguridad tiene como objetivo el evitar los accesos no autorizados a la red o al sistema. Sin embargo, es posible que se produzcan violaciones de esta política, siendo recomendable disponer de un sistema que permita detectarlas. Este es el objetivo de un sistema detector de intrusiones (IDS), que no es más que elementos de red que se encuentran escuchando todo el tráfico que circula en su segmento en busca de patrones de ataque preconfigurados, o tráfico no deseado en general.
- Nivel de cumplimiento: **Recomendable**

3 MEDIDAS RELATIVAS A LA IMPLEMENTACIÓN DE UNA RED ESPECÍFICA PARA INVITADOS

En el caso de establecer el uso de una “red de invitados”, red específica para personal externo a la organización, e independientemente de los servicios que se les ofrezca a través de dicha red, se deberán tener en cuenta los siguientes requisitos:

- Se llevará un registro de los usuarios “invitados” que se desean conectar a la red inalámbrica, los recursos o servicios a los que accederían y la temporalidad de la conexión, dependiendo esta última de la política de seguridad de la entidad y de las necesidades del usuario.
- Se establecerán los mecanismos necesarios para permitir el acceso de los usuarios de esta red únicamente a los recursos que se considere conveniente proporcionarles, limitando su acceso al resto de recursos de la red.
- Las conexiones de los clientes inalámbricos externos irán convenientemente cifradas.
- Cuando esta red sea de uso más intensivo, como por ejemplo, acceso público desde una biblioteca o museo, se ofrecerá este servicio a través de una solución específica para tal fin por parte de RCJA (VPN Internet).
- Nivel de cumplimiento: **Obligatorio**

Por otro lado, se recomienda que el tráfico de los clientes inalámbricos externos vaya por una VLAN independiente a la de los empleados.

4 SEGUIMIENTO Y EXPLOTACIÓN DE REDES INALÁMBRICAS

Se recomienda realizar el seguimiento de nuevos desarrollos o estándares de seguridad en redes inalámbricas, así como del tratamiento de vulnerabilidades en este tipo de redes.

También es recomendable establecer una política de actualización del software, firmware y controladores tanto de los puntos de acceso como de los clientes de red, con el objeto de subsanar aquellas vulnerabilidades que puedan aparecer con el tiempo, así como la inclusión de nuevas funcionalidades de seguridad que se puedan desarrollar.

4.1 DESIGNACIÓN DE UN RESPONSABLE DE EXPLOTACIÓN LOCAL

- Se deberá designar un responsable para la explotación local de la red inalámbrica, que será quien realice el seguimiento y explotación de las redes inalámbrica de acuerdo con las recomendaciones indicadas previamente.
- Nivel de cumplimiento: **Obligatorio**

5 POLÍTICA DE CONTRASEÑAS

- En todos los casos en los que haya que configurar una contraseña se deberá cumplir lo establecido en la Resolución de 27 de septiembre de 2004, de la Secretaría General para la Administración Pública, por la que se establece el manual de comportamiento de los empleados públicos en el uso de los sistemas informáticos y redes de comunicaciones de la Administración de la Junta de Andalucía, en las políticas de seguridad concretas establecidas por cada entidad o que éstas puedan establecer en el futuro, así como en las políticas de seguridad que estén establecidas o puedan establecerse en el futuro de forma horizontal para toda la Administración de la Junta de Andalucía.
- Nivel de cumplimiento: **Obligatorio**

CAPÍTULO 3: CERTIFICACIÓN Y VERIFICACIÓN DE LA INSTALACIÓN

Una vez finalizada la instalación, se procederá a realizar la certificación y verificación de la misma para comprobar su correcto funcionamiento. Para ello, se podrán seguir las recomendaciones descritas a continuación.

En el caso de **redes de área local inalámbrica**, habrá que realizar las siguientes pruebas:

- Pruebas de funcionamiento: canal y potencia de emisión de cada punto de acceso. Se comprobará el correcto funcionamiento de las redes inalámbricas y el cumplimiento del CNAF y del RD 1066/2001.
- Pruebas de cobertura, de niveles de potencia, de interferencia, nivel mínimo de la señal en zona de servicio, porcentaje total del área de servicio cubierta, señal mínima fuera de la zona de servicio, etc.
- Pruebas de capacidad (neta por usuario, neta total de la instalación, bruta por usuario), de uso de canales, de velocidad de las distintas redes, etc.
- Pruebas de conectividad, que permitan comprobar que los clientes inalámbricos pueden acceder a los recursos concretados en los requisitos del proyecto, en las distintas zonas de cobertura.
- Pruebas de compatibilidad, si es el caso, entre los equipos existentes y los equipos WIFI, estableciendo las posibles restricciones de potencia y distancia mínima entre ambos.
- Pruebas de seguridad realizadas, en función de los requisitos de seguridad que se hayan implantado. Pruebas de acceso a las distintas VLAN/LAN/WAN.

En el caso de **enlaces inalámbricos**, las pruebas de certificación a realizar serán las siguientes:

- Pruebas de funcionamiento del enlace: canal y potencia de emisión de cada extremo, niveles de señal medidos en cada punto del enlace. Se comprobará el correcto funcionamiento del enlace y el cumplimiento del CNAF y del RD 1066/2001.
- Pruebas de capacidad con objeto de comprobar el caudal del enlace y retardo medio del mismo.
- Pruebas de conectividad, que permitan comprobar que es posible acceder a los recursos necesarios, concretados en los requisitos iniciales del proyecto, a través del enlace inalámbrico.
- Pruebas de compatibilidad, si es el caso, entre los equipos existentes y los equipos que constituyen el enlace inalámbrico, estableciendo las posibles restricciones de potencia y distancia mínima entre ambos.
- Pruebas de seguridad realizadas, en función de los requisitos de seguridad que se hayan implantado. Pruebas de acceso a las distintas VLAN/LAN/WAN, dependiendo de la utilidad que se de al enlace inalámbrico.

CAPÍTULO 4: NORMATIVA APLICABLE Y LISTADO DE ACRÓNIMOS

6 NORMATIVA APLICABLE

A continuación se enumeran las normas del IEEE aplicables a las redes y enlaces inalámbricos, y otra normativa de aplicación.

6.1 NORMATIVA INALÁMBRICA

- IEEE 802.11a: banda de 5 GHz, permitiendo velocidades de hasta 54 Mbps.
- IEEE 802.11b: banda de 2,4 GHz y permite obtener una velocidad de hasta 11 Mbps.
- IEEE 802.11g: banda de los 2,4 GHz y proporciona una velocidad máxima de 54 Mbps.
- IEEE 802.11e: estándar inalámbrico que permite la interoperación entre entornos públicos, de negocios y usuarios residenciales, con la capacidad añadida de resolver las necesidades de cada sector. La especificación añade, respecto de los estándares 802.11b y 802.11a, características QoS y de soporte multimedia, a la vez que mantiene compatibilidad con ellos.
- IEEE 802.11h: extensión del estándar IEEE 802.11a que lo actualiza para conseguir las reglas recomendadas por la ITU. El uso de la banda de 5 GHz en Europa varía de un país a otro. El uso de WLANs a ciertas frecuencias podría causar interferencias con otros dispositivos, como satélites, radares militares, otras WLAN, etc. Así, el estándar 801.11h implementa dos métodos para evitar estos problemas: DFS - Dynamic Frequency Selection (para seleccionar el espectro adecuado para la WLAN) y TPC - Transmission Power Control (para administrar las redes WLANs y las estaciones).
- IEEE 802.11i: Está dirigido a combatir la vulnerabilidad actual en la seguridad para protocolos de autenticación y de codificación. El estándar abarca los protocolos 802.1x, TKIP (Protocolo de Claves Integra – Seguras – Temporales), y AES (Estándar de Cifrado Avanzado). Se implementa en WPA2.
- IEEE 802.11k: Medición de fuente radio.
- IEEE 802.11n: ambas bandas, tanto en 2,4 GHz como en 5 GHz, y proporciona una velocidad máxima de 600 Mbps.
- IEEE 802.11r: Transición rápida de estación base.
- IEEE 802.11u: Interacción con diferentes tecnologías.
- IEEE 802.11v: Gestión de transición de estación base.
- RD- Ley 1/1998, de 27 de febrero, sobre infraestructuras comunes en los edificios para el acceso a los servicios de telecomunicación.
- Real Decreto 346/2011, de 11 de marzo, por el que se aprueba el Reglamento Regulator de las infraestructuras comunes de telecomunicaciones para el acceso a los servicios de telecomunicación en el interior de las edificaciones.
- RD 1066/200, de 28 de septiembre, que establece condiciones de protección del dominio público radioeléctrico, restricciones a las emisiones radioeléctricas y medidas de protección sanitaria frente a emisiones radioeléctricas (BOE)
- RD 1580/2006, de 22 de diciembre, por el que se regula la compatibilidad electromagnética de los equipos eléctricos y electrónicos.

6.2 OTRA NORMATIVA

- IEEE 802.1p: es un estándar que proporciona priorización de tráfico y filtrado multicast dinámico. Esencialmente, proporciona un mecanismo para implementar Calidad de Servicio (QoS) a nivel de MAC (Media Access Control).
- IEEE 802.1q: también conocido como dot1Q, es un mecanismo que permite a múltiples redes compartir de forma transparente el mismo medio físico, sin problemas de interferencia entre ellas (Trunking). VLAN.
- IEEE 802.1x: norma para el control de acceso a red basada en puertos. Permite la autenticación de dispositivos conectados a un puerto LAN, estableciendo una conexión punto a punto o previniendo el acceso por ese puerto si la autenticación falla.
- IEEE 802.3af: permite que la alimentación eléctrica se suministre a un dispositivo de red usando el mismo cable que se utiliza para la conexión de red. PoE Power Over Ethernet.

7 RELACIÓN DE ACRÓNIMOS Y ABREVIATURAS

ANS	Acuerdo de Nivel de Servicio.
AP	Access Point - Punto de Acceso para redes o enlaces inalámbricos.
CNAF	Cuadro Nacional de Atribución de Frecuencias.
DFS	Dynamic Frequency Selection- Selección Dinámica de Frecuencia.
DGTSI	Dirección General de Telecomunicaciones y Sociedad de la Información.
DHCP	Dynamic Host Configuration Protocol.
IP	Internet Protocol.
MAC	Media Access Control.
PoE	Power over Ethernet.
QoS	Quality of Service.
RADIUS	Remote Authentication Dial-In User Server.
RCJA	Red Corporativa de Telecomunicaciones de la Junta de Andalucía.
RP	Repartidor de Planta.
SAI	Sistema de Alimentación Ininterrumpida.
SSID	Service Set Identifier
ToIP	Telephony over IP (Telefonía sobre IP).
TPC	Transmitter Power Control - Control de Potencia del Transmisor.
TT	Toma de Telecomunicaciones.
VLAN	Virtual Local Area Network
VoIP	Voice over IP (Voz sobre IP).
VoWLAN	Voice over WLAN
WLAN	Wireless Local Area Network
WMM	Wifi Multimedia
WPA	Wi-Fi Protected Access