

Guía de Seguridad de las TIC CCN-STIC 837

ENS. Seguridad en Bluetooth



Febrero 2018

Edita:



© Centro Criptológico Nacional, 2018

NIPO: 785-18-003-X

Fecha de Edición: febrero de 2018

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

PRÓLOGO

El uso masivo de las tecnologías de la información y las telecomunicaciones (TIC), en todos los ámbitos de la sociedad, ha creado un nuevo espacio, el ciberespacio, donde se producirán conflictos y agresiones, y donde existen ciberamenazas que atentarán contra la seguridad nacional, el estado de derecho, la prosperidad económica, el estado de bienestar y el normal funcionamiento de la sociedad y de las administraciones públicas.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI), encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información en su artículo 4.e), y de protección de la información clasificada en su artículo 4.f), a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN) en su artículo 9.2.f).

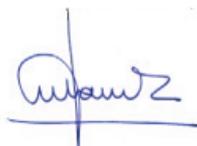
Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través de su Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, a la aplicación de políticas y procedimientos de seguridad, y al empleo de tecnologías de seguridad adecuadas.

El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (ENS, en adelante), al que se refiere el apartado segundo del artículo 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, establece la política de seguridad en la utilización de medios electrónicos que permita una protección adecuada de la información.

Precisamente el Real Decreto 3/2010 de 8 de enero, actualizado por el Real Decreto 951/2015, de 23 de octubre, fija los principios básicos y requisitos mínimos, así como las medidas de protección a implantar en los sistemas de la Administración, y promueve la elaboración y difusión de guías de seguridad de las tecnologías de la información y las comunicaciones (STIC) por parte de CCN para facilitar un mejor cumplimiento de dichos requisitos mínimos.

En definitiva, la serie de documentos CCN-STIC se elabora para dar cumplimiento a los cometidos del Centro Criptológico Nacional y a lo reflejado en el Esquema Nacional de Seguridad, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo su difícil, y en ocasiones, ingrata tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Febrero de 2018



Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ÍNDICE

1 INTRODUCCIÓN	6
2 OBJETO	7
3 ALCANCE.....	7
4 TECNOLOGÍA BLUETOOTH	8
4.1 DEFINICIÓN Y GENERALIDADES.....	8
4.2 CARACTERÍSTICAS TÉCNICAS.....	9
4.2.1 ARQUITECTURA BLUETOOTH	12
4.2.2 PERFILES BLUETOOTH (BLUETOOTH <i>PROFILES</i>)	17
4.2.3 TOPOLOGÍA BLUETOOTH	19
4.3 PROCEDIMIENTOS OPERATIVOS DE BLUETOOTH.....	21
5 SEGURIDAD BLUETOOTH	23
5.1 AMENAZAS A LA TECNOLOGÍA BLUETOOTH.....	23
5.2 ARQUITECTURA DE SEGURIDAD	24
5.2.1 SEGURIDAD EN BLUETOOTH BR/EDR.....	25
5.2.2 SEGURIDAD BLUETOOTH LE (LOW ENERGY).....	33
5.2.3 RESUMEN MECANISMOS DE SEGURIDAD BLUETOOTH	42
6 MEDIDAS DE SEGURIDAD DEL ENS.....	43
6.1 ÁMBITO DE USO DE LA TECNOLOGÍA BLUETOOTH	44
6.2 NORMATIVA DE SEGURIDAD Y GESTIÓN DE RIESGOS	45
6.3 PROTECCIÓN DE LAS COMUNICACIONES BLUETOOTH.....	47
6.4 PROTECCIÓN DE LOS DISPOSITIVOS BLUETOOTH.....	50
6.4.1 AUTENTICACIÓN.....	50
6.4.2 CONFIGURACIÓN DE SEGURIDAD	51
6.4.3 GESTIÓN DE LA CONFIGURACIÓN	53
6.4.4 REGISTROS DE ACTIVIDAD.....	53
6.5 MEDIDAS OPERATIVAS.....	54
6.5.1 MANTENIMIENTO.....	54
6.5.2 AUDITORÍAS DE SEGURIDAD	54
6.6 MEDIDAS APLICABLES AL PERSONAL	55
7 ANEXO A. RESUMEN DE REQUISITOS DEL USO DE BLUETOOTH EN LA ORGANIZACIÓN.....	56
8 ANEXO B. EJEMPLO DE CONFIGURACIÓN BLUETOOTH EN UN EQUIPO WINDOWS61	
9 GLOSARIO DE TÉRMINOS	70
10 REFERENCIAS	72

ÍNDICE DE FIGURAS

Figura 1. Red WPAN.....	6
Figura 2. Combinaciones de Host y Controladores Bluetooth	13
Figura 3. Arquitectura Bluetooth.....	14
Figura 4. Perfiles Bluetooth.	18
Figura 5. Perfiles soportados por Microsoft Windows 10.....	19
Figura 6. Topología Bluetooth BR/EDR.....	20
Figura 7. Topología Bluetooth LE.....	21
Figura 8. Mecanismos de Seguridad Bluetooth BR/EDR.	26
Figura 9. Generación de la clave del enlace LK en BR/EDR.	27
Figura 10. Autenticación SSP (<i>Legacy Authentication</i>).....	29
Figura 11. Autenticación Secure Connections (<i>Secure Authentication</i>).....	30
Figura 12. Generación de clave y cifrado SSP.....	31
Figura 13. Generación de clave y cifrado Secure Connections	32
Figura 14. Mecanismos de Seguridad Bluetooth LE.	35
Figura 15. Fases de pairing en Bluetooth LE.....	36
Figura 16. Comandos SMP Pairing Request / Response.....	37
Figura 17. Generación de la STK en LE Legacy Pairing.	39
Figura 18. Generación de la LTK en LE Secure Connections.....	39
Figura 19. Ejemplo de Adaptador Bluetooth en un equipo Windows 7.	61
Figura 20. Ejemplo de versión Bluetooth empleada en un equipo Windows 7.....	62
Figura 21. Ejemplo de interruptor físico Bluetooth.....	62
Figura 22. Activar / Desactivar el adaptador Bluetooth en Windows 7.....	63
Figura 23. Acceso a la configuración Bluetooth en un equipo Windows 7.....	63
Figura 24. Ventana de opciones de configuración Bluetooth Windows 7.....	64
Figura 25. Ventana de autenticación de dispositivos Windows 7 iPhone 6.	65
Figura 26. Dispositivo iPhone emparejado con el equipo Windows 7.....	66
Figura 27. Servicios ofrecidos por el dispositivo iPhone 6.	66
Figura 28. Ejemplo de transferencia de archivos por Bluetooth Windows 7	67
Figura 29. Ejemplo de transferencia de archivos por Bluetooth Windows 7	68
Figura 30. Configuración de carpetas compartidas en Windows 7.....	69

ÍNDICE DE TABLAS

Tabla 1. Principales versiones y tecnologías Bluetooth y sus características.	12
Tabla 2. Procedimientos operativos Bluetooth BR/EDR, Bluetooth LE.....	22
Tabla 4. Resumen de los mecanismos de seguridad Bluetooth BR/EDR.	42
Tabla 5. Resumen de los mecanismos de seguridad Bluetooth LE.	43
Tabla 6. Mecanismos de autenticación de dispositivos Bluetooth.	47
Tabla 7. Algoritmos empleados por Bluetooth.	48
Tabla 8. Requisitos del ENS aplicables al uso de Bluetooth en la organización.	60

1 INTRODUCCIÓN

1. Las Redes de Área Personal, más conocidas por el acrónimo inglés de PAN (*Personal Area Network*), constituyen uno de los campos de más rápida evolución en el ámbito de las redes de comunicaciones.
2. PAN representa el concepto de redes centradas en el espacio de trabajo de un individuo, en el cual, los dispositivos se conectan entre sí e intercambian datos. Algunos ejemplos de dispositivos que se utilizan en un PAN son los ordenadores personales y sus periféricos (ratón, teclado, impresora), equipos de fax, *smartphones*, *tablets*, auriculares inalámbricos, altavoces, escáneres, consolas de videojuegos, etc.
3. Las Redes inalámbricas de Área Personal WPAN (*Wireless PAN*), son redes PAN sin cables (*wireless*), en las que los dispositivos se comunican entre sí a través de ondas electromagnéticas y sin necesidad, por lo tanto, de cableado.



Figura 1. Red WPAN.

4. Existen varias tecnologías empleadas para las comunicaciones WPAN. Una de las más extendidas es Bluetooth¹, lanzada por Ericsson en 1994.
5. La tecnología Bluetooth está integrada actualmente en más de 8.200.000.000 millones de dispositivos empleados en una gran variedad de sectores del mercado, como la automoción, vivienda, cuidado de la salud, deporte, y especialmente en los sectores de las telecomunicaciones y la informática, como *tablets*, teléfonos móviles, ordenadores portátiles, periféricos, cámaras digitales, etc.
6. El éxito de la tecnología Bluetooth se debe a varias ventajas, como su facilidad de implementación y uso, su bajo consumo energético (fundamental para los dispositivos que utilizan baterías) y su baja latencia².

¹ El origen del término Bluetooth se remonta a 1996 cuando uno de los responsables del desarrollo de esta tecnología, propuso el nombre del rey vikingo Harald "Bluetooth" Gormsson, conocido por unificar Dinamarca y Noruega en el 958, y el cual tenía un diente de un color azul/gris que le hizo ganarse el apodo de "diente azul" (Bluetooth).

² Se denomina latencia a la suma de los retardos temporales en las transmisiones, es decir, al tiempo real que tarda un paquete de datos en llegar desde el emisor al receptor.

7. Siendo evidentes las ventajas que ofrece la tecnología Bluetooth, hay que tener muy en cuenta los riesgos adicionales que añaden a los ya existentes en las redes cableadas. Estos riesgos deben tratarse de forma específica, e implementar las medidas de seguridad apropiadas que proporcionen seguridad de las comunicaciones que se llevan a cabo a través de Bluetooth.

2 OBJETO

8. Este documento forma parte del conjunto de normas desarrolladas por el Centro Criptológico Nacional para la implementación del Esquema Nacional de Seguridad (CCN-STIC-800), siendo de aplicación para la Administración Pública y teniendo como objeto la protección de los servicios prestados a los ciudadanos y entre las diferentes administraciones.
9. El objeto del documento es proporcionar una guía de buenas prácticas que ayude a las organizaciones a mejorar la seguridad de sus implementaciones Bluetooth. Para ello, se indicarán los requisitos más relevantes del ENS que deben tenerse en cuenta en la implantación y uso de esta tecnología.
10. Las pautas que se establecen son de carácter general, de forma que puedan resultar de aplicación a entidades de distinta naturaleza, dimensión y sensibilidad, sin entrar en casuísticas específicas. Por ello, es de esperar que cada organización las particularice para adaptarlas a su entorno singular.

3 ALCANCE

11. El uso de la tecnología Bluetooth dentro de la organización a la que se refiere la presente guía, es aquella en el que a través de conexiones Bluetooth, y empleando dispositivos con capacidades Bluetooth, se accede a sistemas, servicios, recursos y/o se intercambia información propiedad de la organización, y bajo el ámbito de aplicación de su política y normativa de Seguridad.
12. Por lo tanto, no entran dentro del alcance de esta guía aquellas conexiones Bluetooth que puedan establecerse entre los dispositivos personales de los usuarios o en las que la información intercambiada o los recursos accedidos a través de la conexión Bluetooth, no pertenecen a la organización.
13. Por otro lado, a día de hoy existen múltiples tecnologías Bluetooth, cada una de ellas con sus propias características operativas, técnicas, y en especial, de seguridad. Puesto que no todos los dispositivos con capacidades Bluetooth, son capaces de implementar las últimas versiones, se tratarán todas las tecnologías a lo largo de la guía, a excepción de las más antiguas, consideradas ya obsoletas

según Bluetooth SIG³, y que son aquellas versiones de Bluetooth inferiores a la versión 2.1.

14. Las recomendaciones realizadas en la presente guía quedan sometidas a una continua revisión dado el constante avance de la tecnología Bluetooth, así como a la aprobación de nuevos estándares y la aparición de nuevas vulnerabilidades.
15. En esta guía no se referencia ninguna solución Bluetooth de fabricante concreto. Se recomienda consultar otras guías y documentación con información detallada sobre las características, configuración y administración de dispositivos Bluetooth concretos de fabricantes, a la hora de proceder a la selección de una solución Bluetooth.

4 TECNOLOGÍA BLUETOOTH

4.1 DEFINICIÓN Y GENERALIDADES

16. Bluetooth es una tecnología de comunicaciones inalámbrica de corto alcance, empleada para reemplazar las conexiones cableadas entre dispositivos.
17. Es una de las tecnologías más extendidas en la implementación de Redes inalámbricas de Área Personal (WPAN). A través de Bluetooth se pueden crear redes inalámbricas de corto alcance (decenas de metros), que conectan entre sí dispositivos (uno a uno o varios entre sí) con un coste muy bajo y un reducido consumo energético. A estas redes se les da el nombre de *piconets*. Un ejemplo de *piconet* sería un teléfono móvil conectado a unos auriculares inalámbricos.
18. La tecnología Bluetooth posibilita la transmisión de datos entre los dispositivos mediante un enlace por radiofrecuencia. Dicho enlace opera en la banda reservada para uso no comercial en las áreas de instrumentación, ciencia y tecnología (Banda ISM, *Instrumental, Scientific and Medical*), concretamente en la frecuencia de 2.4 GHz, que no requiere licencia para su uso.
19. Además de Bluetooth existen otras muchas tecnologías para redes WPAN, como, por ejemplo, IrDA (Infrared Data Association), que utiliza los infrarrojos como medio de transmisión, o ZigBee y Z-Wave, que al igual que Bluetooth, utilizan ondas de radiofrecuencia en la banda ISM. Cada tecnología cuenta con fortalezas y debilidades, que la hace más apropiada para ciertos escenarios de aplicación. En muchos casos más de una tecnología puede ser adecuada para un escenario, y son factores no técnicos tales como el coste o la disponibilidad, los que determinan qué tecnología es la más apropiada.
20. IEEE (*Institute of Electrical and Electronic Engineers*) ha desarrollado también, dentro del grupo de trabajo IEEE 802.15⁴, un estándar para la definición de redes

³ Bluetooth SIG (Special Interest Group) es una asociación privada sin ánimo de lucro, formada por compañías del ámbito de las telecomunicaciones, informática, automovilismo, música, textil, automatización industrial y tecnologías de red. Los miembros de Bluetooth SIG dirigen el desarrollo de la tecnología Bluetooth.

⁴ En la web de IEEE 802.15 (<http://www.ieee802.org/15/>) se pueden consultar todos los estándares.

WPAN. Las versiones de Bluetooth 1.1 y 1.2 fueron ratificadas por IEEE 802.15.1-2002 y 802.15.1-2005 respectivamente.

21. La tecnología Bluetooth está liderada y gestionada por Bluetooth SIG, que cuenta con más de 30.000 miembros, entre los que se encuentran compañías del sector de las telecomunicaciones, la electrónica y la informática.
22. Cualquier compañía que quiera incorporar la tecnología Bluetooth a sus dispositivos, deberá ser miembro de Bluetooth SIG, superar un proceso de pruebas y certificación del producto que garantizará su compatibilidad con los estándares Bluetooth, y completar un proceso de declaración mediante el cual la compañía acepta los acuerdos de licencias y marca Bluetooth.
23. En la actualidad existen varias versiones de Bluetooth en uso en los dispositivos comerciales. Todas ellas se diseñan siempre con características de compatibilidad hacia atrás, es decir, un dispositivo que implemente la última versión de Bluetooth podrá funcionar también con las versiones anteriores para poder conectarse con dispositivos más antiguos. La versión más actual se puede consultar en la web oficial de Bluetooth.com⁵.

4.2 CARACTERÍSTICAS TÉCNICAS

24. Existen dos tecnologías Bluetooth que han ido cambiando y evolucionando a través de las múltiples versiones de Bluetooth, desde la primera versión (v1.0). Estas dos tecnologías son:
 - **Bluetooth Basic Rate / Enhanced Data Rate/ High Speed (BR/EDR/HS)**, también conocida como *Bluetooth Clásico*.
Basic Rate (BR) ofrece conexiones síncronas y asíncronas con velocidades de transmisión de hasta 1 Mbps, 3 Mbps en EDR y hasta 24 Mbps en HS.
 - **Bluetooth Low Energy (LE)**, también conocido como *Bluetooth de Bajo Consumo*.
25. Low Energy (LE) ofrece conexiones asíncronas con velocidades de hasta 3Mbps. Fue diseñado para hacer posible el uso de Bluetooth en dispositivos que requieren de un bajo consumo y menor complejidad y coste que BR/EDR. LE también fue diseñado para aquellos escenarios en los que la tasa de transferencia de datos es muy baja.
26. Los dispositivos con capacidades Bluetooth pueden implementar una de las dos tecnologías, o ambas.
27. A continuación, se incluye una tabla resumen de las versiones Bluetooth hasta la actualidad (versión 5.0), en la que se describe cómo han ido evolucionando cada una de las dos tecnologías.

⁵ En el momento de redacción de la presente guía, la última versión es Bluetooth 5, disponible desde finales de 2016 e implementada en teléfonos móviles como Iphone 8, Iphone X o Samsung Galaxy S8.

Versión	Características
<p>1.0 (1999) Actualizaciones: 1.1 (2001) 1.2 (2003)</p>	<p>La versión 1.0 fue la primera versión usada para la transmisión de datos y que actualmente se encuentra en desuso. Al ser la primera versión enfrentó muchos problemas de comunicación entre dispositivos.</p> <p>Le sucedieron las actualizaciones 1.1 y 1.2 que incorporaban la tecnología BR (Basic Rate), proporcionando velocidades de transmisión máximas de 1 Mbps. Estas versiones fueron reconocidas como estándar de comunicación IEEE (802.15.1).</p>
<p>2.0 + EDR (2004) Actualizaciones: 2.1 (2007)</p>	<p>La versión 2.0 con EDR supuso la introducción de la tecnología EDR (Enhanced Data Rate), para proporcionar velocidades de transmisión más elevadas que BR, de hasta 3 Mbps.</p> <p>La versión 2.1 con EDR mejora la seguridad del proceso de emparejamiento de dispositivos (llamado <i>pairing</i>), introduciendo la característica SSP (Secure Simple Pairing), que hace uso de mecanismos de clave pública para la generación de la clave del enlace compartida, durante el proceso de <i>pairing</i>.</p> <p>Las tecnologías BR y EDR son conocidas como Bluetooth Clásico.</p>
<p>3.0 + HS (2009)</p>	<p>La versión 3.0 con HS supuso la introducción de la tecnología HS (High Speed), para proporcionar velocidades de transmisión más elevadas que EDR, de hasta 24 Mbps (apto para archivos de música o vídeo).</p> <p>Para lograr esto, el enlace Bluetooth se usa únicamente para el establecimiento y la negociación de la conexión, mientras que, para la transferencia de datos a alta velocidad, se establece un enlace 802.11⁶. A esta nueva característica se le denomina AMP (Alternative MAC/PHY).</p> <p>La tecnología HS se conoce como Bluetooth de Alta Velocidad.</p>

⁶ IEEE 802.11 es un conjunto de especificaciones sobre la capa física (PHY) y la capa de Control de Acceso al Medio (MAC) para implementar comunicaciones Wireless en las bandas de frecuencia de 900 MHz, y 2.4, 3.6, 5 y 60 GHz.

Versión	Características
<p>4.0 + LE (2010) Actualizaciones: 4.1 (2013) 4.2 (2014)</p>	<p>En la versión 4.0 se introdujo la tecnología Bluetooth Low Energy (LE), que permite implementar Bluetooth en dispositivos con baterías pequeñas (también llamadas <i>button</i> o <i>coin cells</i>) y que requieren un tiempo de vida prolongado, por lo que las exigencias de consumo energético requeridas por Bluetooth deben ser bajas.</p> <p>La tecnología LE logra el bajo consumo mejorando la gestión de las conexiones. Se emplea la filosofía de conexiones activas y dormidas, de forma que sólo cuando se requiere un envío de datos es cuando se activa la conexión, permaneciendo el resto del tiempo en estado dormido sin realizar consumo energético.</p> <p>La tecnología LE se conoce como Bluetooth de Bajo Consumo. Dentro de los dispositivos Bluetooth v4, se distinguen los siguientes:</p> <ul style="list-style-type: none"> - Modo único (<i>single-mode devices</i>): sólo implementan LE, no Bluetooth BR/EDR. Se les denomina dispositivos “<i>Bluetooth Smart</i>”. - Modo dual (<i>dual-mode devices</i>): implementan LE y también Bluetooth BR/EDR. Se les denomina dispositivos “<i>Bluetooth Smart Ready</i>”. <p>Las tecnologías de Bluetooth BR/EDR siguen siendo necesarias en ciertos escenarios de aplicación que requieran una tasa alta de transferencia de datos, o una distancia operativa elevada. Es por esto que los dispositivos que ofrecen múltiples funcionalidades, como ordenadores o teléfonos inteligentes (<i>smartphones</i>), son duales (<i>Bluetooth Smart Ready</i>).</p> <p>Respecto a la seguridad, se introduce la característica de seguridad Secure Connections, que mejora los mecanismos de seguridad empleando, entre otras cosas, algoritmos de curva elíptica (ECDH) para la generación de claves, y algoritmos de cifrado AES-CCM. Esta característica se introduce para Bluetooth BR/EDR en la versión 4.1 y para Bluetooth LE en la versión 4.2.</p>

Versión	Características
<p>Bluetooth 5 (2016)</p>	<p>Bluetooth 5 introduce mejoras operativas a la tecnología LE, con objeto de adaptar cada vez más la funcionalidad de Bluetooth para IoT (<i>Internet of Things</i>).</p> <p>Bluetooth 5 ofrece opciones para aumentar significativamente la velocidad de transmisión (duplicarla) reduciendo la distancia operativa, o bien aumentar la distancia operativa (cuadruplicarla) reduciendo la velocidad de transmisión. Por ejemplo, si la distancia operativa de Bluetooth 4 es de 60 m a 1Mbps aproximadamente, con Bluetooth 5 se puede alcanzar 240m a 128 Kbps.</p> <p>También eleva (x8) las capacidades de <i>broadcasting</i> de las conexiones aumentando la longitud de los paquetes.</p>

Tabla 1. Principales versiones y tecnologías Bluetooth y sus características.

28. Los dispositivos Bluetooth pueden tener distintos rangos de operación (alcance) en función de sus potencias de transmisión y en función del tipo y características de sus antenas.
29. Existen principalmente tres clases de dispositivos:
 - **Clase 1.** Tienen un rango de operación máximo de 100 m. Esto implica una potencia de transmisión elevada, alrededor de 100 mW (20 dBm).
 - **Clase 2.** Tienen un rango de operación máximo de 10 m. Esto implica una potencia de transmisión media, alrededor de 2.5 mW (4 dBm).
 - **Clase 3.** Tienen un rango de operación máximo de 1 m. Esto implica una potencia de transmisión baja, alrededor de 1 mW (0 dBm).
30. Son típicamente dispositivos de Clase 2, los teléfonos móviles, auriculares inalámbricos o dispositivos manos libres para automóvil. Los dispositivos Clase 1 suelen ser, por ejemplo, portátiles y dispositivos USB.

4.2.1 Arquitectura Bluetooth

31. La arquitectura de comunicaciones Bluetooth está compuesta por una pila en la que se definen una serie de capas de funcionalidad y protocolos, destinada a asegurar la interoperabilidad entre los dispositivos Bluetooth.
32. La pila de protocolos Bluetooth se puede dividir en dos partes. Una formada por las capas superiores de la pila que forman la entidad lógica denominada **Host** y otra formada por las capas inferiores de la pila que forman la entidad lógica denominada **Controlador (Controller)**.

33. Existen dos tipos de Controladores: primarios y secundarios.
- Controlador primario:
 - Controlador BR/EDR, usado por la tecnología Basic Rate /Enhanced Data Rate.
 - Controlador LE, usado por la tecnología Low Energy.
 - Una combinación de Controlador LE y Controlador BR/EDR.
 - Controlador secundario:
 - Controlador AMP (*Alternate MAC/PHY*), usado por la tecnología HS (High Speed) para el empleo del canal 802.11 en la transferencia de datos de alta velocidad.
34. Host y Controlador pueden estar físicamente juntos o separados (por ejemplo en dos procesadores distintos). Cuando están separados, se requiere la capa HCI (*Host Controller Interface*) que es un interfaz lógico entre el Host y el Controlador.
35. Una implementación Bluetooth está formada por una parte Host, un Controlador primario y ninguno, uno o varios Controladores secundarios tal y como se muestra en la siguiente figura.

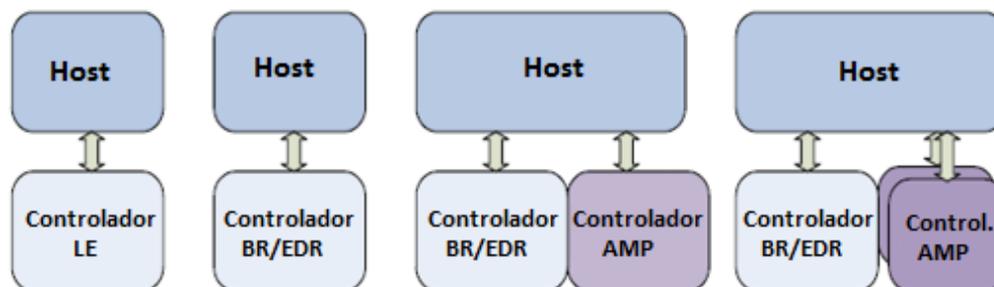


Figura 2. Combinaciones de Host y Controladores Bluetooth
(Figura de BLUETOOTH SPECIFICATION Version 4.2 [Vol 1, Part A]).

36. Como se ha comentado anteriormente, la entidad Host está compuesta por las capas superiores de la pila de protocolos y la entidad Controlador por las inferiores. Algunas de estas capas son las mismas en todas las tecnologías. Otras, son diferentes según la tecnología. La siguiente figura muestra las capas de la pila Bluetooth de las entidades Host y Controlador para las distintas tecnologías.

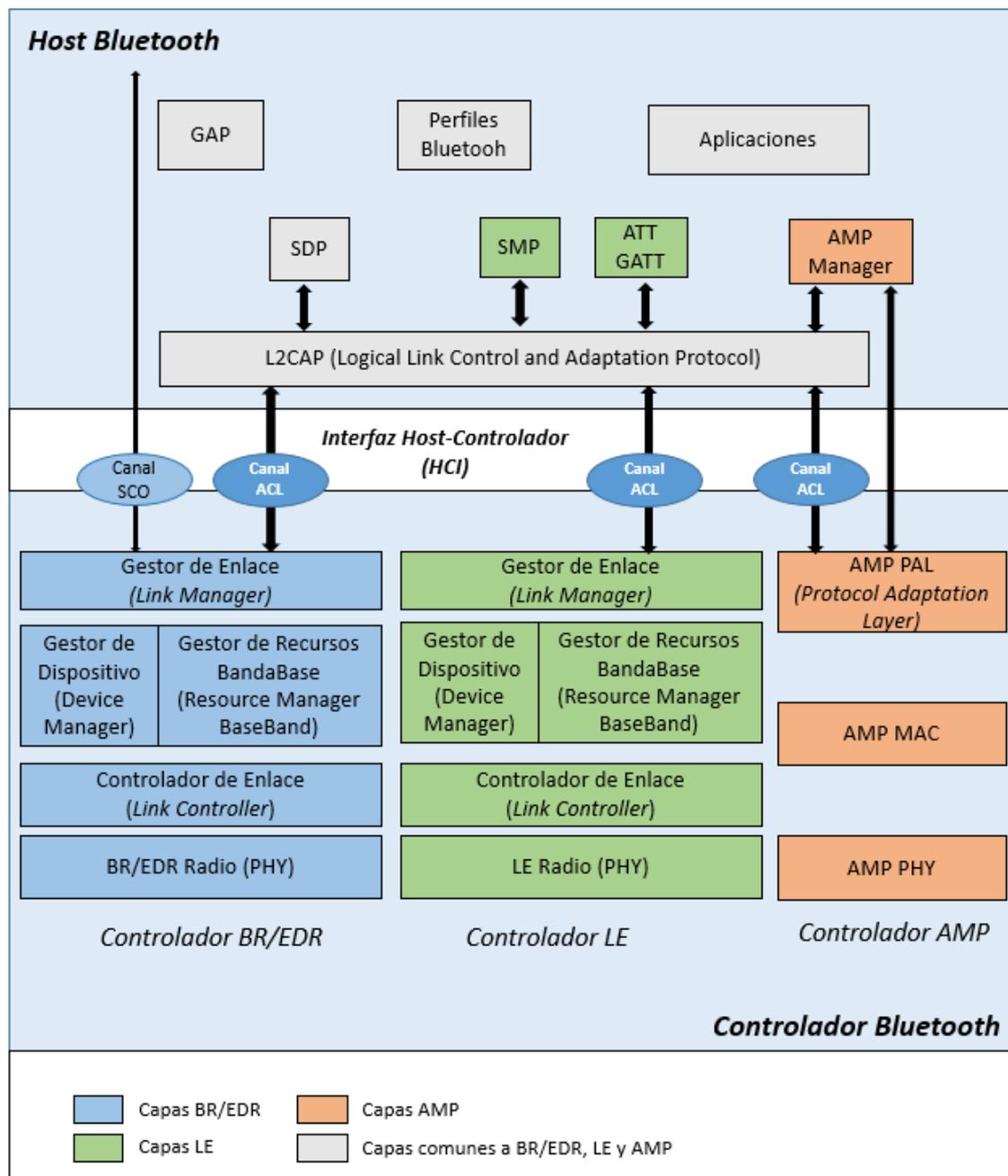


Figura 3. Arquitectura Bluetooth
(Figura a partir de BLUETOOTH SPECIFICATION Version 4.2 [Vol 1, Part A]).

4.2.1.1 Módulo Host

37. **L2CAP** (*Logical Link Control and Adaptation Protocol*), Protocolo de Adaptación y control de enlace lógico, es la capa responsable de las siguientes tareas:
- Establecimiento de conexiones a través de enlaces ACL (Asíncronos) existentes solicitud de un enlace ACL si este no existe.
 - Multiplexación de los datos trasladados por los protocolos superiores para permitir que varias aplicaciones puedan utilizar el mismo enlace ACL.
 - Tareas de calidad de servicio (QoS), fragmentación y re-ensamblado de tramas Bluetooth.
38. L2CAP usa el concepto de *canales* para permitir la transmisión de datos procedentes de múltiples aplicaciones sobre un mismo enlace Bluetooth. Los canales se identifican con un identificador de canal (CID).
39. **SDP** (*Service Discovery Protocol*), Protocolo de descubrimiento de Servicios que permite a un dispositivo descubrir los servicios que otro dispositivo en su área de alcance, ofrece.
40. Un servicio es toda funcionalidad que un dispositivo tiene disponible para su utilización por parte de otro dispositivo Bluetooth remoto. Un mismo dispositivo Bluetooth puede ser a la vez, servidor que ofrece varios servicios y cliente para solicitar el uso de los servicios de otro dispositivo Bluetooth.
41. El módulo SDP define una serie de comportamientos establecidos, tanto para la parte servidor como para la parte cliente de servicios. Un cliente SDP se comunica con un servidor SDP a través de un canal reservado en un enlace L2CAP para localizar qué servicios se encuentran disponibles en el servidor. Posteriormente, cuando el cliente encuentra el servicio buscado, solicita una conexión separada para proceder al uso del servicio.
42. Un servidor SDP dispone de una base de datos propia que contiene el listado de servicios que el servidor ofrece y sus características. Cada servicio está identificado por un UUID (*Universally Unique Identifier*).
43. **GAP** (*Generic Access Profile*), representa la funcionalidad básica común a todos los dispositivos Bluetooth: modos y procedimientos de conexión, descubrimiento de servicios, seguridad, autenticación, modelos de asociación, etc. En el apartado siguiente se proporciona más información sobre los perfiles Bluetooth.
44. **SMP** (*Security Manager Protocol*), Protocolo de Gestión de la Seguridad encargado de la generación y almacenamiento de las claves de la conexión. Opera sobre un canal L2CAP dedicado, y gestiona la funcionalidad de privacidad LE⁷.
45. Esta capa sólo existe en el *Host* de sistemas LE. En BR/EDR, esta funcionalidad la proporciona el Gestor de Enlace (*Link Manager*) de la Controladora BR/EDR.

⁷ La funcionalidad de Privacidad LE se detalla en el apartado 5.2.2 Seguridad Bluetooth LE.

46. **ATT** (*Attribute Protocol*), Protocolo de Atributos que constituye el protocolo extremo a extremo entre un servidor y un cliente de atributos. Un cliente se comunica con un servidor de atributos a través de un canal L2CAP dedicado.
47. **GATT** (*Generic Attribute Profile*), el Perfil de Atributos Genérico representa la funcionalidad del servidor de atributos y, opcionalmente, del cliente de atributos. Describe la jerarquía de servicios, características y atributos empleados por un servidor de atributos. Solo se emplea en los dispositivos LE para el descubrimiento de servicios de perfiles.
48. **Gestor AMP** (*AMP Manager*), es una capa que utiliza canales de señalización L2CAP para comunicarse extremo a extremo con el *AMP Manager* de un dispositivo remoto con objeto de recolectar información para el establecimiento y gestión de los enlaces físicos AMP. También interactúa directamente con el AMP PAL para propósitos de control AMP.

4.2.1.2 Controlador BR/EDR/LE

49. **Gestor de Dispositivos** (*Device Manager*), es un bloque funcional dentro de la capa de Banda Base que controla el comportamiento general del dispositivo. Es el responsable de todas las operaciones que no estén relacionadas con el transporte de datos, como el descubrimiento, conexión, gestión del modo visible / oculto, etc.
50. **Gestor de Enlace** (*Link Manager*), es responsable de la creación, configuración y gestión de los enlaces lógicos. Para ello se comunica con el Gestor de Enlace del dispositivo remoto, utilizando el protocolo LMP (*Link Manager Protocol*) en tecnología BR/EDR, y el protocolo LL (*Link Layer Protocol*) en tecnología LE.
51. Ambos protocolos permiten la creación de nuevos enlaces lógicos entre dispositivos, así como el control general de los enlaces y de la configuración del transporte de datos. Negocian, entre otras cosas, el tamaño de las tramas de Banda Base, los mecanismos de seguridad y los modos de administración de energía o el ajuste de los parámetros de calidad del servicio (QoS).
52. Entre los dispositivos Bluetooth existen dos tipos de enlaces:
 - **SCO** (*Synchronous Connection-Oriented*), Síncronos, Orientados a Conexión para transmisiones de voz.
 - **ACL** (*Asynchronous Connectionless*) Asíncronos, No orientados a conexión para transmisiones de datos.
53. **Gestor de Recursos en Banda Base** (*Baseband Resource Manager*), es responsable de todos los accesos al medio de radio (PHY). Tiene dos funciones principales: una es la de programar *slots* temporales para el uso del canal físico por parte de todas las entidades que hayan contratado el acceso y uso. Otra es la de negociar las características de estos contratos de acceso (aspectos como QoS).
54. **Controlador del Enlace** (*Link Controller*), es responsable de codificar y decodificar los paquetes de datos Bluetooth y sus parámetros relacionados, para su

transmisión en el canal físico (PHY). También lleva a cabo la señalización de los protocolos LMP (en BR/EDR) y LL (en LE), para control de flujo y señales de aceptación y retransmisión de peticiones.

55. **PHY** (*Physical Layer*), capa Física, o es responsable de la transmisión y recepción de paquetes a través del canal físico. Se encarga de la modulación y demodulación de los datos, en señales de radiofrecuencia para su transmisión en el medio aéreo.

4.2.1.3 Controlador AMP

56. **AMP PAL** (*Protocol Adaptation Layer*), es la capa que actúa de interfaz entre la capa de AMP MAC y la parte Host AMP (L2CAP y AMP Manager). Traduce los comandos del Host en primitivas MAC y viceversa. Proporciona soporte para la gestión de los canales AMP, el tráfico de datos y la eficiencia de consumo energético.
57. **AMP MAC** (*Media Access Control*) es la capa MAC tal y como se define en el modelo de referencia IEEE 802. Proporciona servicios como direccionamiento físico y mecanismos de control y acceso a los canales.
58. **AMP PHY** (*Physical Layer*) es la capa física.

4.2.2 Perfiles Bluetooth (Bluetooth Profiles)

59. La interoperabilidad de aplicaciones a través de conexiones Bluetooth, se consigue haciendo uso de lo que se denominan perfiles Bluetooth (*Bluetooth Profiles*). Cuando dos dispositivos implementan un mismo perfil Bluetooth la interoperabilidad de una aplicación en ambos dispositivos está asegurada.
60. Un perfil Bluetooth consiste en la definición del conjunto de funciones y características requeridas en cada una de las capas de la arquitectura Bluetooth, incluyendo cualquier otro protocolo externo necesario fuera de la especificación Bluetooth y especificando, además, comportamientos, configuraciones y formatos de datos que deben emplear las aplicaciones.
61. Como mínimo, la especificación de un perfil contiene:
 - Dependencias con otros perfiles. Cada perfil depende del perfil básico. Algunos pueden depender también de otros perfiles intermedios.
 - Formatos de interfaz de usuario recomendados. Cada perfil describe cómo un usuario debería ver dicho perfil con objeto de mantener una experiencia de usuario uniforme.
 - Partes específicas de la pila de protocolos Bluetooth que utiliza el perfil. Cada perfil usa opciones y parámetros específicos en cada capa de la pila.
62. Los perfiles Bluetooth se agrupan en una jerarquía de grupos. Cada grupo depende de las características proporcionadas por el grupo predecesor.
63. En la raíz de la jerarquía se encuentra el perfil básico **GAP** (*Generic Access Profile*), que todo dispositivo Bluetooth implementa y en el que se basan todos los demás

perfiles. El perfil GAP define los mecanismos básicos para el establecimiento de los enlaces de Banda Base entre dispositivos Bluetooth. Además también define:

- Qué características básicas deben implementarse en todos los dispositivos Bluetooth.
- Procedimientos básicos para el descubrimiento y enlace de dispositivos.
- Aspectos básicos del interfaz de usuario.

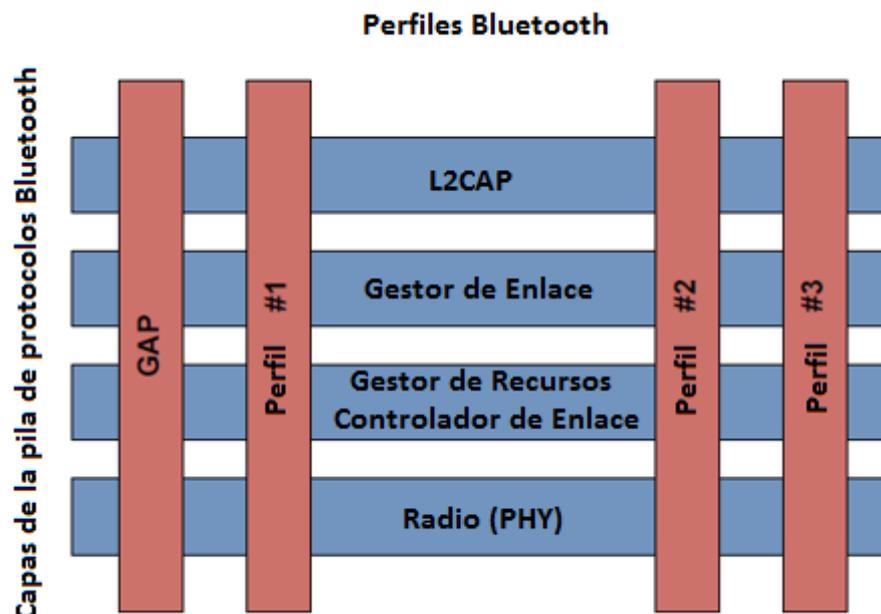
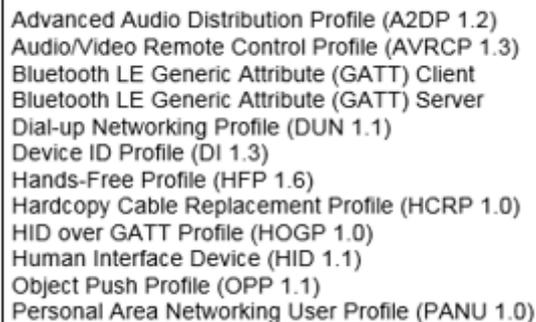


Figura 4. Perfiles Bluetooth.
(Figura de BLUETOOTH SPECIFICATION Version 4.2 [Vol 1, Part A])

64. Bluetooth SIG proporciona las especificaciones de todos los perfiles que han sido adoptados para los dispositivos Bluetooth⁸.
65. Todos los dispositivos indican en sus especificaciones de producto, además de la versión de Bluetooth que implementan los perfiles que soportan. Por ejemplo, Microsoft indica para Windows 10 los siguientes perfiles de Bluetooth soportados⁹:

⁸ Estos perfiles se pueden consultar en <https://www.bluetooth.com/specifications/profiles-overview>.

⁹ Obtenido de la página de soporte Microsoft: <https://support.microsoft.com/en-us/help/10568/windows-10-supported-bluetooth-profiles>.



Advanced Audio Distribution Profile (A2DP 1.2)
Audio/Video Remote Control Profile (AVRCP 1.3)
Bluetooth LE Generic Attribute (GATT) Client
Bluetooth LE Generic Attribute (GATT) Server
Dial-up Networking Profile (DUN 1.1)
Device ID Profile (DI 1.3)
Hands-Free Profile (HFP 1.6)
Hardcopy Cable Replacement Profile (HCRP 1.0)
HID over GATT Profile (HOGP 1.0)
Human Interface Device (HID 1.1)
Object Push Profile (OPP 1.1)
Personal Area Networking User Profile (PANU 1.0)

Figura 5. Perfiles soportados por Microsoft Windows 10.

66. En este ejemplo, el perfil A2DP (*Advanced Audio Distribution Profile*) define el modo en que se propagará un *stream* de audio entre dispositivos a través de la conexión Bluetooth. El perfil PBAP (*Phone Book Access Profile*) define cómo enviar datos de agenda telefónica entre dispositivos. El perfil HFP (*Hands-Free Profile*) se emplea para definir cómo se realiza el transporte de audio empleado en los sistemas manos libres de los automóviles. El perfil SPP (*Serial Port Profile*) indica cómo emular un puerto serie para conexiones RS-232 de aplicaciones a través de Bluetooth. El perfil AVRCP (*Audio/video Remote Control Profile*) permite emplear el dispositivo (por ejemplo, un teléfono móvil) para controlar remotamente a otros dispositivos reproductores de audio y video (como televisores o aparatos de música), etc.

4.2.3 Topología Bluetooth

4.2.3.1 Topología Bluetooth BR/EDR

67. Durante una operativa típica en Bluetooth BR/EDR, un canal físico de radio es compartido por un grupo de dispositivos sincronizados a un reloj común y con un patrón de salto de frecuencias. El dispositivo que proporciona la referencia de sincronización es el dispositivo maestro (*master*) y los demás dispositivos sincronizados al reloj del maestro y a su patrón de salto de frecuencias son los esclavos (*slaves*).
68. Un conjunto de dispositivos sincronizados de esta forma constituye una **Piconet**. Esta es la forma general de operación de la tecnología Bluetooth BR/EDR.
69. Pueden existir varias *piconets* en áreas próximas de forma que un dispositivo puede ser esclavo en más de una *piconet*, pero un dispositivo sólo puede ser maestro en una *piconet* (debido a la sincronización al reloj del maestro). Cuando varias *piconets* están unidas por dispositivos se denomina **Scatternet**.

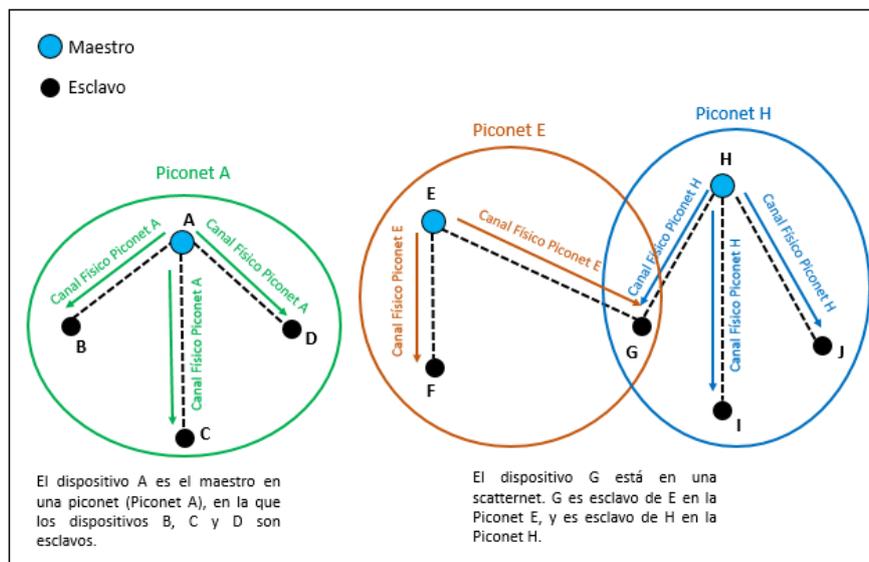


Figura 6. Topología Bluetooth BR/EDR.

4.2.3.2 Topología Bluetooth LE

70. En la tecnología Bluetooth LE el canal físico se subdivide en unidades de tiempo llamadas “eventos”. Los dispositivos LE transmiten datos entre ellos a través de paquetes que son posicionados en estos eventos.
71. Hay dos tipos de eventos: de Publicidad (*Advertising*) y de Conexión (*Connection*).
72. Dentro de los eventos de publicidad, hay un tipo específico de paquetes que los dispositivos emiten para indicar que están disponibles para conexión. Son los llamados “paquetes de publicidad de conexión” (*advertising connectable packets*).
73. Los dispositivos que necesitan establecer una conexión con otro dispositivo, estarán a la escucha de los paquetes de publicidad de conexión emitidos por aquellos dispositivos disponibles para conexión. Estos dispositivos que están a la escucha se llaman “iniciadores” (*initiators*). Los dispositivos que emiten la publicidad de conexión se llaman “publicadores” (*advertisers*).
74. Cuando un iniciador detecta el paquete de publicidad de conexión emitido por un publicador, si desea establecer una conexión con él, le envía una petición de conexión a través del mismo canal físico por el que ha recibido el evento de publicidad (canal físico de publicidad). En caso de que el publicador acepte esta petición de conexión, la conexión podrá iniciarse, para lo cual el evento de publicidad finaliza y comienza un evento de conexión.
75. La conexión entre ambos dispositivos genera una **Piconet** en la que el dispositivo iniciador se convierte en el maestro y el dispositivo publicador pasa a ser esclavo. La transmisión de datos entre maestro y esclavo se realiza a través de eventos de conexión utilizando maestro y esclavo el mismo canal físico.
76. Al contrario que en BR/EDR, en LE los dispositivos esclavos en una *piconet* no comparten el mismo canal físico con el maestro. Cada esclavo se comunica con el maestro a través de un canal físico separado.

77. Dos *piconet* pueden compartir dispositivos formando una **Scatternet**.

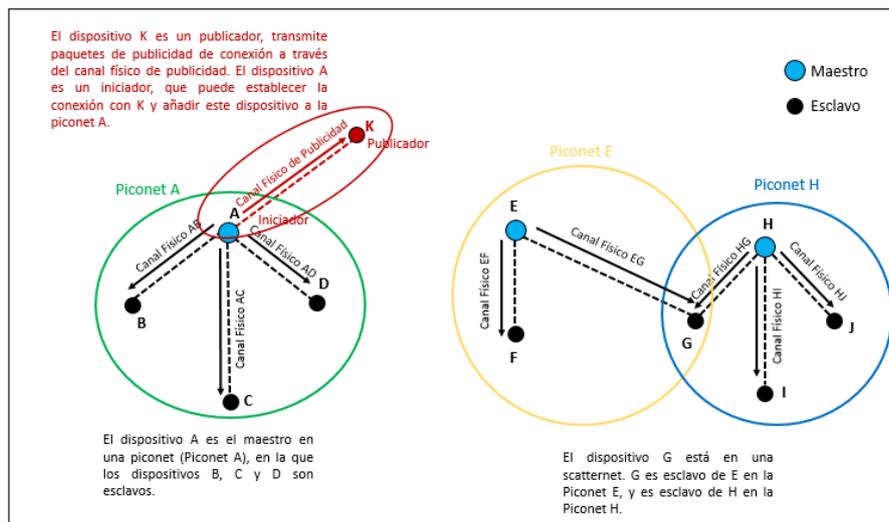


Figura 7. Topología Bluetooth LE.

4.3 PROCEDIMIENTOS OPERATIVOS DE BLUETOOTH

78. El modo de operación habitual de un dispositivo Bluetooth es estar conectado a otros dispositivos Bluetooth (en una *piconet*) e intercambiando datos con ellos. Dado que Bluetooth establece comunicaciones inalámbricas *ad-hoc* (entre dispositivos y sin necesidad de infraestructura), hay una serie de procedimientos operativos que se tienen que llevar a cabo para que se forme la *piconet* de forma que los dispositivos que la integran puedan comunicarse.
79. En la siguiente tabla se indican los principales procedimientos empleados por las distintas tecnologías Bluetooth, para establecer la conexión.

Descubrimiento de Dispositivos visibles, dentro del rango de alcance.	
Bluetooth BR/EDR	<p>Procedimiento de Descubrimiento (<i>Inquiry</i>)</p> <p>El dispositivo que desea descubrir a otros inicia el procedimiento enviando paquetes de solicitud (<i>inquiry_request</i>) de forma activa a un determinado canal físico. Los dispositivos que desean ser descubiertos (modo visible), revisarán este canal cada cierto tiempo y responderán (<i>inquiry_response</i>).</p>

Bluetooth LE	<p>Procedimiento de Publicidad (<i>Advertising</i>) y de Escaneado (<i>Scanning</i>)</p> <p>A través del procedimiento de publicidad, un dispositivo que está en modo visible y desea ser descubierto envía de forma activa paquetes broadcast de eventos de publicidad relativos a descubrimiento a través del canal físico de publicidad broadcast.</p> <p>A través del procedimiento de escaneado, un dispositivo que desea descubrir a otros en su área, escanea (escucha) el canal físico de publicidad broadcast a la espera de detectar paquetes de eventos de publicidad relativos a descubrimiento, enviados por otros dispositivos.</p> <p>Utilizando el procedimiento de filtrado de dispositivos, el dispositivo a la escucha evitará descubrir todos los dispositivos de un área dada cuando sólo busque uno concreto.</p>
Establecimiento de la conexión entre dos dispositivos	
Bluetooth BR/EDR	<p>Procedimiento de Conexión (<i>Paging</i>)</p> <p>Un dispositivo lleva a cabo el procedimiento de conexión (<i>page connection</i>), mientras que el otro dispositivo está a la escucha de solicitudes de conexión (<i>page scanning</i>).</p> <p>El dispositivo objeto de conexión está a la escucha en un canal físico determinado de las solicitudes de conexión. Este canal físico tiene determinados atributos que son específicos del dispositivo objeto de conexión (como su dirección, BD_ADDR) de forma que sólo aquel dispositivo que lo conozca, podrá comunicarse a través de este canal.</p> <p>Una vez finaliza con éxito el proceso de conexión, se establece un canal físico entre los dos dispositivos.</p>
Bluetooth LE	<p>Procedimiento de Publicidad (<i>Advertising</i>) y de Escaneado (<i>Scanning</i>)</p> <p>A través del procedimiento de publicidad, el dispositivo disponible para conexión (publicador) publica paquetes de publicidad de conexión a través del canal físico destinado a publicidad.</p> <p>A través del procedimiento de escaneado, el dispositivo que quiere conectarse escucha estos paquetes y responde por ese mismo canal a estos paquetes con una solicitud de conexión (iniciador).</p> <p>El dispositivo que quiere conectarse, primero habrá descubierto que el dispositivo objeto de conexión está en modo visible en su área y entonces, habrá escaneado sólo los paquetes de publicidad de conexión procedentes de ese dispositivo utilizando el procedimiento de filtrado de dispositivos.</p>

Tabla 2. Procedimientos operativos Bluetooth BR/EDR, Bluetooth LE.

5 SEGURIDAD BLUETOOTH

5.1 AMENAZAS A LA TECNOLOGÍA BLUETOOTH

80. La tecnología Bluetooth y los dispositivos que la emplean están expuestos a las mismas amenazas de toda red inalámbrica y además, a amenazas específicas a la tecnología Bluetooth.
81. Dentro de las amenazas clásicas más importantes en la tecnología inalámbrica se encuentran el **eavesdropping** y los ataques **man-in-the-middle** (MITM).
82. El **eavesdropping**, o escuchas pasivas ocurre cuando un individuo no autorizado captura el tráfico Bluetooth intercambiado entre dos dispositivos.
83. El ataque MITM ocurre cuando a la hora de conectar dos dispositivos, un individuo no autorizado logra introducir un tercer dispositivo que retransmite información entre los dos dispositivos legítimos haciéndoles creer que se están comunicando directamente entre ellos.
84. Durante el proceso de emparejamiento inicial de los dispositivos, proceso llamado **pairing**, es cuando se lleva a cabo la autenticación y la generación y/o intercambio de las claves de cifrado de la conexión. El modo de llevar a cabo el proceso de **pairing**, proporcionará mayor o menor grado de protección frente al **eavesdropping** y los ataques MITM. En los siguientes apartados relativos a la Arquitectura de seguridad se detallan los grados de protección que proporcionan las distintas tecnologías Bluetooth.
85. Los ataques de Denegación del Servicio, DoS, en el caso de los dispositivos Bluetooth pueden impactar dejando inhabilitada la interfaz Bluetooth del dispositivo y drenando su batería. Estos ataques no suelen ser habituales y solo tienen éxito cuando se realizan dentro del rango de alcance del dispositivo.
86. Otros ataques específicos a la tecnología Bluetooth son, entre otros, los siguientes.
 - **Bluesnarfing**. Explota vulnerabilidades en el firmware de algunos dispositivos antiguos. Un individuo no autorizado, a través de la conexión Bluetooth a un dispositivo, logra acceso a los datos almacenados como agenda, calendario, IMEI, etc.
 - **Bluebugging**. Explota vulnerabilidades en el firmware de algunos dispositivos antiguos. Un individuo no autorizado, a través de la conexión Bluetooth a un dispositivo, logra acceso a su sistema operativo y comandos. Usando estos comandos sin que el usuario sea consciente de ello, puede acceder a los datos, escuchar llamadas, enviar mensajes y explotar cualquier servicio que tenga el dispositivo.
 - **Bluejacking**. Se produce cuando un individuo con fines mal intencionados envía mensajes no solicitados a un dispositivo con Bluetooth habilitado. La finalidad es

engañar al usuario para que responda al mensaje o lo guarde en sus contactos. Es similar al *phishing* o *spam* de correo electrónico.

- **Fuzzing.** Consiste en enviar datos no estándar o mal formados al interfaz de radio del dispositivo para ralentizar o paralizar su operación.

87. Dado que la tecnología Bluetooth está en constante evolución y van surgiendo nuevas vulnerabilidades y ataques, el detalle de estos debe consultarse en fuentes actualizadas como puede ser Bluetooth SIG.

5.2 ARQUITECTURA DE SEGURIDAD

88. La arquitectura de seguridad de Bluetooth proporciona los siguientes servicios de seguridad:

- **Generación de claves.** La generación de las claves criptográficas se realiza a través del proceso llamado *pairing*, mediante el cual se lleva a cabo una primera autenticación y el posterior establecimiento de una o más claves secretas compartidas entre los dispositivos.

- **Bonding.** Bluetooth emplea un proceso llamado *bonding*, para almacenar las claves generadas durante el *pairing*, de modo que puedan ser empleadas en conexiones posteriores, creando así una relación de confianza entre dos dispositivos.

- **Autenticación de dispositivos.** Bluetooth dispone de un proceso de autenticación basado en verificar que los dos dispositivos disponen de las mismas claves.

- **Cifrado.** Bluetooth emplea algoritmos de cifrado para proporcionar confidencialidad a los datos.

- **Integridad.** Bluetooth emplea mecanismos de integridad para proporcionar a los mensajes protección frente a alteraciones ilícitas.

- **Privacidad.** Bluetooth dispone de un mecanismo para ocultar las direcciones de los dispositivos, con objeto de que ningún individuo no autorizado pueda realizar un seguimiento al dispositivo y por lo tanto, a su propietario.

- **Firma de Datos.** Bluetooth dispone de un mecanismo que permite autenticar los datos enviados a través de una conexión entre dos dispositivos en escenarios en los que la conexión no implemente cifrado.

89. La implementación de estos servicios de seguridad ha ido evolucionando a lo largo del tiempo y depende por lo tanto, de la tecnología Bluetooth empleada. En los siguientes apartados se describen los servicios de seguridad implementados en cada tecnología.

5.2.1 Seguridad en Bluetooth BR/EDR

90. Los mecanismos de seguridad utilizados en Bluetooth BR/EDR se implementan en la parte del Controlador BR/EDR a nivel del Gestor de Enlace (*Link Manager*)¹⁰.
91. Estos mecanismos han ido evolucionando a lo largo de las versiones de Bluetooth BR/EDR y se agrupan bajo las siguientes nomenclaturas:
 - **BR/EDR Legacy Pairing**: hasta la versión 2.0 (incluida)¹¹.
 - **BR/EDR Secure Simple Pairing (SSP)**: de la versión 2.1 a la 4.0 (incluida).
 - **BR/EDR Secure Connections**: a partir de la versión 4.1.
92. BR/EDR SSP introduce el uso de lo que se llaman “modelos de asociación” que representan distintas formas de llevar a cabo el proceso de *pairing* entre los dispositivos.
93. También introduce el uso de algoritmos basados en ECDH (*Elliptic Curve Diffie-Hellman*) que permiten el acuerdo de clave de forma que las claves son generadas en cada uno de los dispositivos y no son distribuidas a través de la conexión.
94. BR/EDR *Secure Connections* mejora la seguridad de SSP, utilizando algoritmos ECDH más evolucionados y haciendo uso de AES-CCM para el cifrado.
95. En la siguiente figura se muestra un diagrama resumen de los mecanismos de seguridad de BR/EDR SSP y *Secure Connections* que se describen en los siguientes apartados. Se puede consultar un mayor detalle en las especificaciones de Bluetooth *Core Specifications*¹².

¹⁰ Ver apartado 4.2.1. Arquitectura Bluetooth.

¹¹ Las versiones BR/EDR Legacy Pairing son consideradas obsoletas y/o retiradas según Bluetooth SIG, por lo que no se incluye detalle de estos mecanismos en la presente guía.

¹² Las especificaciones de Bluetooth se pueden consultar en: <https://www.bluetooth.com/specifications/bluetooth-core-specification>. Todas las funciones usadas por Bluetooth BR/EDR para autenticación, cifrado, derivación de claves, cálculo de valores de confirmación, etc. se encuentran definidas en Volumen 2- Parte H.

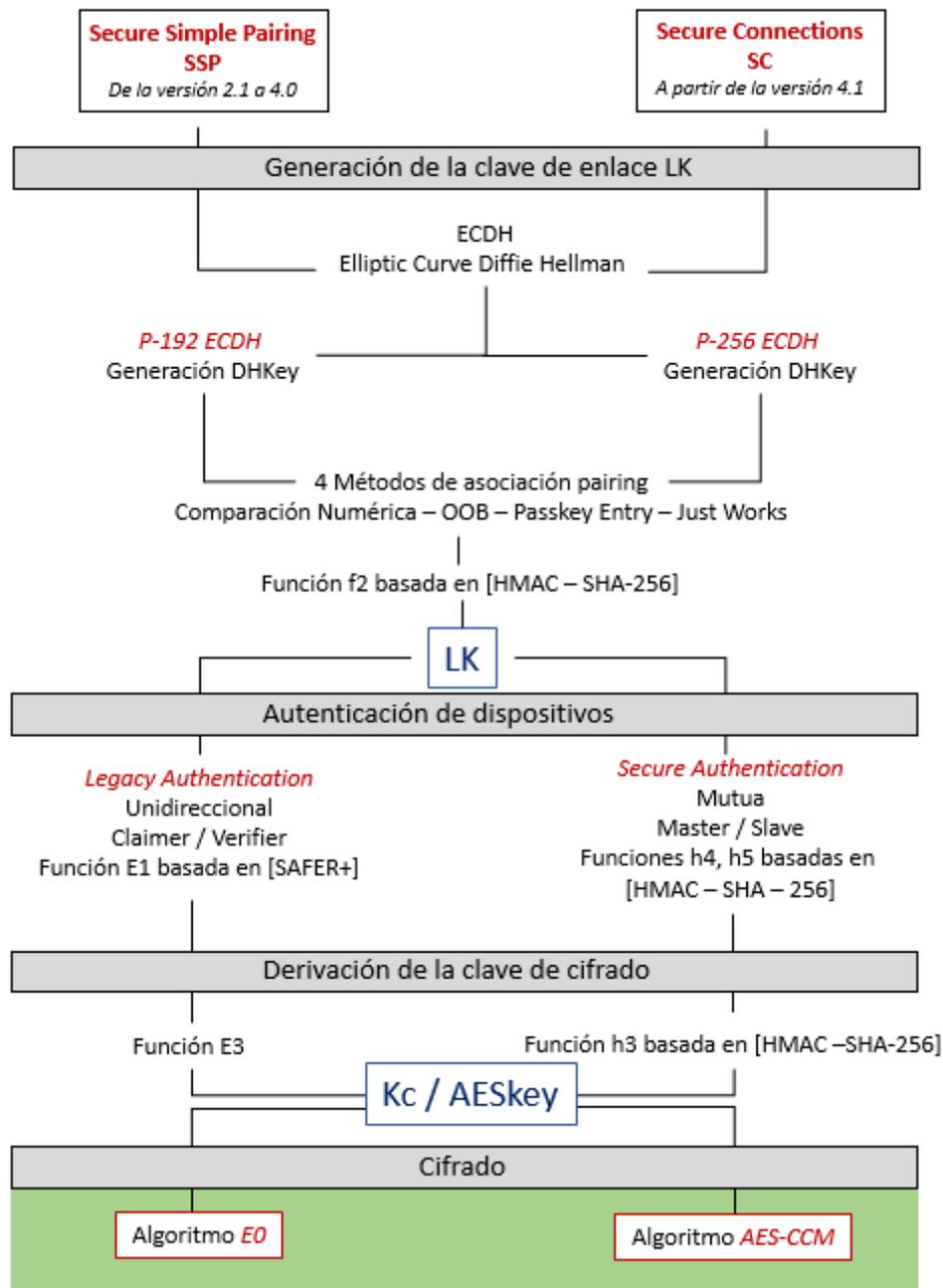


Figura 8. Mecanismos de Seguridad Bluetooth BR/EDR.

5.2.1.1 Generación de la clave del enlace LK (Link Key)

96. Bluetooth BR/EDR utiliza una clave llamada clave del enlace LK (*Link Key*). Esta clave de hasta 128 bits es la que se emplea en los procesos de autenticación de los dispositivos y de generación de las claves de cifrado de la conexión.

97. La LK se obtiene siguiendo los pasos indicados en la siguiente figura.

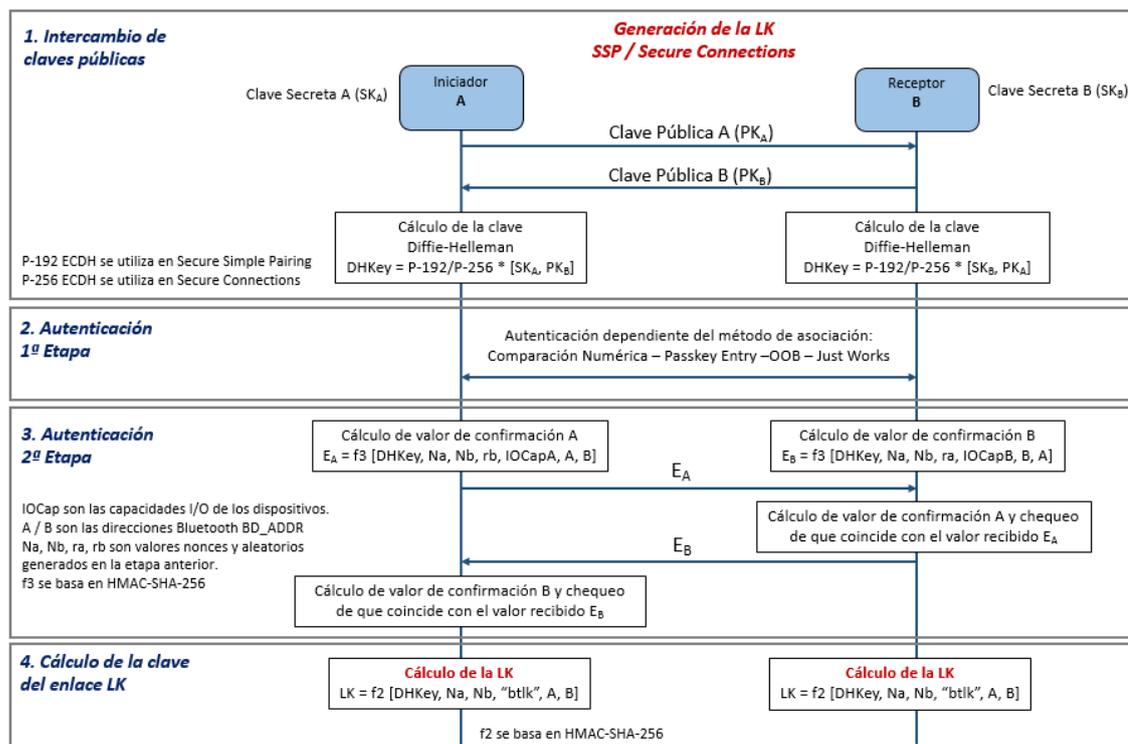


Figura 9. Generación de la clave del enlace LK en BR/EDR.

1. Intercambio de claves públicas. En primer lugar se lleva a cabo el intercambio entre los dispositivos de sus claves públicas y la generación en cada dispositivo de la clave compartida Diffie-Hellman (*DHKey*) a través de un algoritmo ECDH¹³.

Hasta la versión Bluetooth 4.0 se emplea FIPS P-192¹⁴ Elliptic Curve. A partir de la versión 4.1, con *Secure Connections*, se emplea FIPS P-256¹⁴ Elliptic Curve.

2. Autenticación 1ª Etapa. Tras la generación en cada dispositivo del par de claves pública/privada ECDH, se lleva a cabo una primera etapa de autenticación entre los dispositivos que se realizará de distinta forma dependiendo del “modelo de asociación” seleccionado para llevar a cabo el *pairing*.

El modelo de asociación es el mecanismo que van a utilizar los dispositivos para autenticarse entre ellos antes de proceder a la generación / intercambio de las

¹³ ECDH (Elliptic Curve Diffie Hellman) es un protocolo de acuerdo de clave. Permite a dos partes – cada una poseyendo un par de claves públicas privadas de curva elíptica – establecer una clave secreta compartida a través de un canal inseguro. Esta clave secreta se usa posteriormente para mecanismos de seguridad de la conexión.

¹⁴ FIPS P-192 y P-256 son curvas elípticas establecidas como estándar por el gobierno de los Estados Unidos para la utilización por parte de todas las agencias del gobierno no militares y por los contratistas del gobierno. Están definidas en la publicación FIPS PUB 186-4 (<http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf>).

claves. El modelo de asociación seleccionado depende de las capacidades I/O de los dispositivos (referidas a los mecanismos de entrada/salida de datos de los que dispone el dispositivo). Los cuatro modelos que se pueden emplear son:

- **Comparación Numérica.** Se muestra un número, generalmente de 6 dígitos, en la pantalla de cada dispositivo. El usuario debe comprobar que ambos números coinciden e introducir un “Sí” en cada dispositivo para que el proceso continúe. El número generado no se utiliza para el cálculo de la clave del enlace LK.
- **Passkey Entry.** El usuario, o bien introduce un número idéntico generalmente de 6 dígitos en ambos dispositivos (*passkey*), o bien un dispositivo lo muestra y el usuario lo introduce en el otro. El número generado no se utiliza para el cálculo de la clave del enlace LK.
- **Fuera de Banda (OOB, Out-Of-Band).** Diseñado para dispositivos que cuentan con una tecnología adicional de comunicación inalámbrica o cableada como por ejemplo, NFC (*Near Field Communication*). El canal OOB se utiliza para llevar a cabo etapas del proceso de *pairing* y deberá ser un canal seguro para proporcionar protección frente a escuchas ilegales.
- **Just Works.** Cuando ninguno de los dispositivos tiene capacidades I/O. Funciona de forma similar a Comparación Numérica, salvo que no existe pantalla y la conexión es aceptada sin verificar ningún valor calculado en ambos dispositivos.

El detalle de cómo se realiza esta primera autenticación según el modelo de asociación empleado, se puede consultar en las especificaciones de Bluetooth¹⁵.

3. Autenticación 2ª Etapa. La segunda etapa de la autenticación confirma que ambos dispositivos han completado con éxito el intercambio. Cada dispositivo calcula e intercambia un nuevo valor de confirmación empleando la función f_3 basada en HMAC-SHA-256¹⁶ y en los valores aleatorios intercambiados previamente junto con la clave DHKey y las direcciones de los dispositivos. Ambos valores calculados deberán coincidir para continuar el proceso.

4. Cálculo de la clave del enlace LK. Una vez los dispositivos han confirmado el *pairing*, cada uno de ellos calcula la clave del enlace LK derivándola de la clave Diffie-Hellman (DHKey) y de otros valores intercambiados por los dispositivos en las etapas anteriores. La función empleada en la derivación de la LK es f_2 que se basa en HMAC-SHA-256.

¹⁵ En <https://www.bluetooth.com/specifications/bluetooth-core-specification>. [Vol2 – Parte H – Apto 7.2. Secure Simple Pairing – Phase 2: Authentication Stage 1]

¹⁶ HMAC-SHA-256 es un tipo de algoritmo hash con clave, que se crea desde la función hash SHA-256 y se utiliza como HMAC (Código de autenticación de mensajes basado en hash).

5.2.1.2 Autenticación de dispositivos

98. SSP utiliza el método de autenticación que se conoce como “*Legacy Authentication*”. Está basado en el mecanismo de reto-respuesta (*challenge-response*), en el cual uno de los dispositivos representa el papel de solicitante (*claimer*) y el otro el papel de verificador (*verifier*). Dado que los auténticos dispositivos comparten la clave secreta del enlace LK, el objeto del proceso de reto-respuesta es que el verificador compruebe que el solicitante dispone de la misma LK que él.
99. Durante el proceso se utiliza la función de autenticación E_1 ¹⁷ y se obtiene un valor llamado ACO (*Authenticated Ciphering Offset*) necesario para posteriormente derivar la clave de cifrado de la conexión.
100. El verificador no tiene por qué ser el dispositivo maestro en la conexión. Cada aplicación indicará qué dispositivo debe ser autenticado. En caso de que la aplicación requiera de autenticación mutua, se llevarán a cabo dos procesos de autenticación intercambiando roles de solicitante y verificador ambos dispositivos.
101. La siguiente figura muestra el proceso de autenticación en SSP – Legacy Authentication.

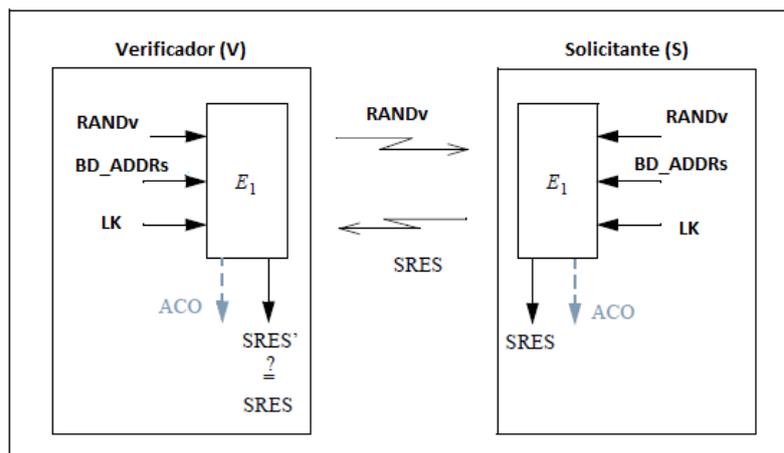


Figura 10. Autenticación SSP (*Legacy Authentication*).
(Figura de BLUETOOTH SPECIFICATION Version 4.2 [Vol 2, Part H])

102. *Secure Connections* utiliza el método de autenticación que se conoce como “*Secure Authentication*”. Está basado también en el mecanismo de reto-respuesta (*challenge-response*), en el cual, los dos dispositivos actuarán como solicitante (*claimer*) y verificador (*verifier*) durante el mismo proceso de autenticación para verificar que ambos disponen de la misma clave secreta del enlace LK. Este método siempre proporciona, por lo tanto, autenticación mutua entre los dispositivos.

¹⁷ La función E_1 empleada por Bluetooth utiliza el algoritmo SAFER+ (cifrador de bloque de 128 bits), el cual es, a su vez, una mejora del cifrador de bloque de 64 bits SAFER-SK128 (Secure And Fast Encryption Routine) diseñado por James Massey, que utiliza claves de 128 bits.

103. Durante el proceso se utilizan las funciones de autenticación h4 y h5 basadas en HMAC-SHA-256 y se obtiene también el valor ACO (*Authenticated Ciphering Offset*) necesario para posteriormente derivar la clave de cifrado de la conexión.
104. La siguiente figura muestra el proceso de autenticación en *Secure Connections – Secure Authentication*.

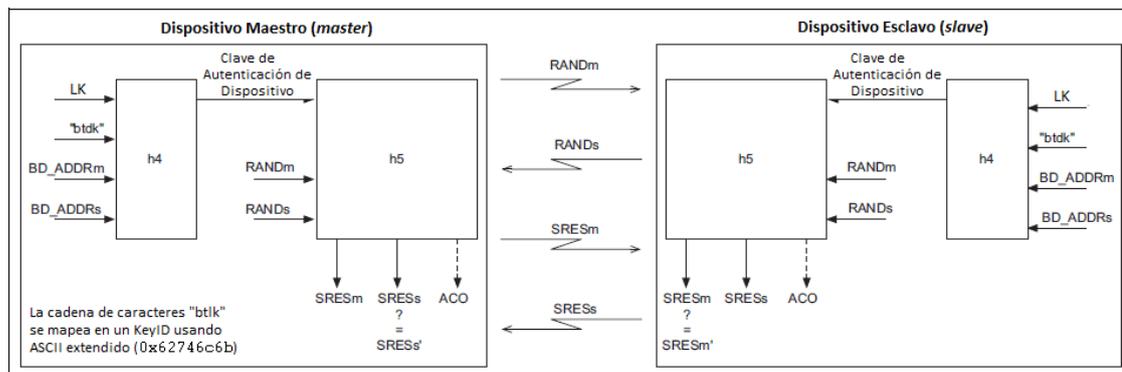


Figura 11. Autenticación Secure Connections (*Secure Authentication*).
(Figura de BLUETOOTH SPECIFICATION Version 4.2 [Vol 2, Part H])

5.2.1.3 Derivación de la clave y cifrado

105. *Secure Simple Pairing* utiliza la función E0 para llevar a cabo el cifrado.
106. La clave de cifrado, Kc, se genera a través de la función E3 y haciendo uso del valor ACO calculado en la fase de autenticación y de la clave del enlace LK.
107. El cifrado a través del cifrador de cadena E0, se realiza de forma que la cadena de clave resultante (*keystream*) es combinada (XOR) con el texto plano para producir el texto cifrado.
108. La siguiente figura muestra el diagrama de generación de la clave Kc y cifrado en SSP.

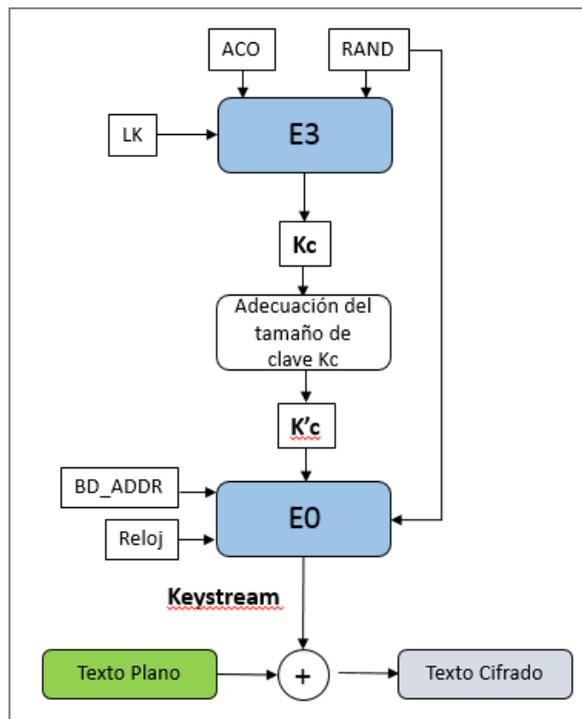


Figura 12. Generación de clave y cifrado SSP.

109. *Secure Connections* utiliza AES-CCM para el cifrado.
110. Las claves de cifrado AES se crean empleando la función h3 basada en el uso de HMAC-SHA-256 y haciendo uso del valor ACO calculado en la fase de autenticación y de la clave del enlace LK.
111. El cifrado es a través de AES-CCM¹⁸. CCM (*Counter Mode with CBC-MAC*) es un modo de operación de un cifrador de bloque simétrico, en este caso AES.
112. Combina dos técnicas: CTR (*Counter Mode*) para la protección de la confidencialidad y CBC-MAC (*Cipher Block Chaining Message Authentication Code*) para la protección de la integridad y autenticidad.
113. La siguiente figura muestra el diagrama de generación de la clave AES y cifrado en *Secure Connections*.

¹⁸ AES-CCM se encuentra definido en las especificaciones de Bluetooth [Vol2 – Parte H – Apdo 9. AES-CCM Encryption for BR/EDR].

CCM está definido en IETF RFC 3610 Counter with CBC-MAC (CCM). También se puede encontrar la descripción de este algoritmo en la publicación especial NIST SP 800-38C <https://csrc.nist.gov/publications/detail/sp/800-38c/final>.

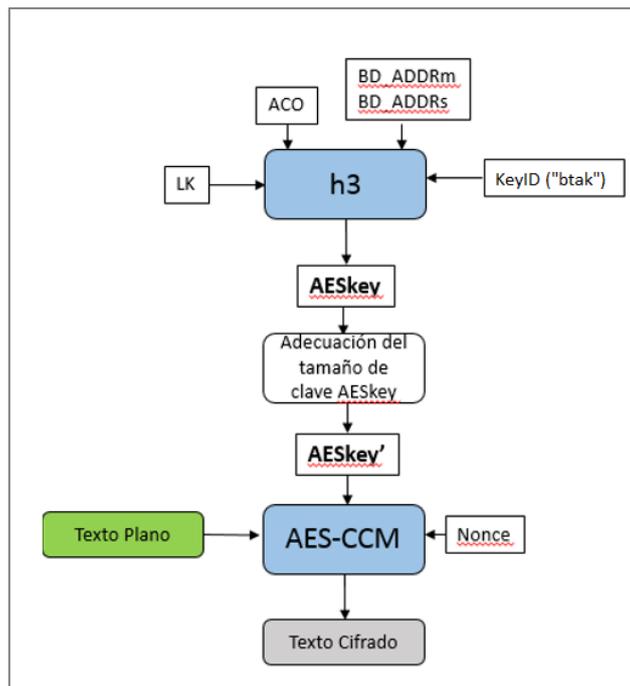


Figura 13. Generación de clave y cifrado Secure Connections

5.2.1.4 Modos de Seguridad

114. Los modos de seguridad en Bluetooth BR/EDR, determinan en qué fase del establecimiento de la conexión entre los dispositivos se inician los mecanismos de seguridad de autenticación y cifrado.
115. Hasta la versión de Bluetooth 2.0 se definen tres modos de seguridad:
- **Modo 1.** No inicia ningún mecanismo de seguridad.
 - **Modo 2.** Los mecanismos de seguridad se inician después del establecimiento del enlace (*service level-enforced*). En este modo de seguridad, un gestor de seguridad local controla el acceso a los servicios a través de políticas de control de acceso e interfaces con otros protocolos y usuarios del dispositivo.
 - **Modo 3.** Los mecanismos de seguridad se inician antes de que el enlace físico esté completamente establecido (*link level-enforced*). Los dispositivos Bluetooth que operan en este modo, establecen como obligatorio la autenticación y el cifrado para todas las conexiones Bluetooth entrantes y salientes del dispositivo
116. A partir de la versión 2.1+EDR, se introduce el **Modo 4**. En el Modo 4, los mecanismos de seguridad se inician después del establecimiento del enlace físico y lógico (*service level-enforced*). Este modo utiliza algoritmos de curva elíptica (ECDH) de acuerdo de clave para la generación de la clave del enlace (LK). Hasta la versión 4.0 se emplea la característica de *Secure Simple Pairing (SSP)*, que usa el algoritmo P-192 Elliptic Curve, y los mismos mecanismos de autenticación y cifrado que los empleados por BR/EDR anterior a la versión 2.1. A partir de la versión 4.1, se emplea el algoritmo P-256 Elliptic Curve y se modifica el modo de autenticación (*Secure Authentication*) y de cifrado (AES-CCM).

117. EL Modo 4 tiene varios niveles de seguridad:
- Nivel 1. No se requiere seguridad.
 - Nivel 2. Clave del enlace (LK) no autenticada, sin protección MITM y con cifrado.
 - Nivel 3. Clave del enlace (LK) autenticada, con protección MITM y con cifrado.
 - Nivel 4. Clave del enlace (LK) autenticada empleando Secure Connections (disponible a partir de la versión 4.1), con protección MITM, y con cifrado.
118. El que la clave de enlace (LK) sea o no autenticada, depende del modelo de asociación empleado durante el *pairing* (todos proporcionan LK autenticada menos *Just Works*).
119. El Modo 4 es obligatorio para todos los dispositivos a partir de la versión 2.1. Los modos 1 a 3 solo se emplean para comunicación con dispositivos anteriores a 2.1 que no soportan el Modo 4 y en esos casos, el Modo 3 será el recomendado.

5.2.2 Seguridad Bluetooth LE (Low Energy)

120. Los mecanismos de seguridad utilizados en Bluetooth LE son gestionados por el *Security Manager (SM)*, Gestor de seguridad de la parte *Host*.
121. SM define el protocolo y el modo de llevar a cabo el proceso de *pairing*, la autenticación y el cifrado entre los dispositivos que sólo disponen de tecnología LE o que disponen de tecnología BR/EDR/LE¹⁹.
122. Bluetooth LE introduce dos características nuevas de seguridad a la tecnología Bluetooth: Privacidad LE y Firma de Datos.

A) Privacidad LE (*LE Privacy*). Es una característica que permite proteger la privacidad. El funcionamiento es el siguiente:

En la fase de descubrimiento, los dispositivos Bluetooth emiten mensajes (llamados “eventos de publicidad”) para anunciar su presencia a otros dispositivos. Estos mensajes contienen, entre otras cosas, la dirección del dispositivo que lo identifica unívocamente. Cualquier individuo no autorizado puede capturar estos mensajes y llevar a cabo el seguimiento de un dispositivo determinado para conocer datos privados sobre su dueño, como lugares donde ha estado, horas, etc.

La función de Privacidad LE, es una característica que salvaguarda la privacidad haciendo que la dirección del dispositivo incluida dentro del mensaje de publicidad, sea reemplazada por un valor aleatorio que va cambiando cada cierto periodo de tiempo. De esta forma un individuo no autorizado, aunque capture estos mensajes de publicidad, al llevar cada uno una dirección “diferente” no será capaz de relacionarlos con un mismo dispositivo.

¹⁹ Dispositivos LE son aquellos que sólo implementan la configuración de Host y Controlador LE. Dispositivos BR/EDR/LE son los que implementan la configuración de Host y Controlador BR/EDR y LE combinados. Ver apartado 4.2.1 Arquitectura Bluetooth.

Esta característica utiliza una clave llamada IRK (*Identity Resolving Key*), que es intercambiada entre los dispositivos durante el proceso de *pairing* y que permite a un dispositivo receptor traducir el valor aleatorio contenido en el mensaje de publicidad del dispositivo emisor.

B) Firma de Datos (*Data Signing*). Es una característica que permite autenticar los datos enviados entre dos dispositivos que ya han finalizado con éxito la fase de *pairing* en escenarios en los que el modo de seguridad de la conexión no implementa la característica de cifrado.

Esta característica utiliza una clave llamada CSRK (*Connection Signature Resolving Key*) que es intercambiada entre los dispositivos durante el proceso de *pairing*. El dispositivo emisor adjunta al mensaje una firma digital compuesta por un contador y un código MAC²⁰ generado con la CSRK. El dispositivo receptor utilizará la CSRK intercambiada con el emisor para verificar la autenticidad del mensaje y el contador para protección contra ataques de reenvío (*replay attacks*).

123. Al igual que en Bluetooth BR/EDR, en Bluetooth LE los mecanismos de seguridad han ido evolucionando y son distintos en función de la tecnología, agrupándose en los siguientes:
- **LE Legacy Pairing**, empleado en las versiones 4.0 y 4.1.
 - **LE Secure Connections**, empleado a partir de la versión 4.2.
124. En la siguiente figura se muestra un diagrama resumen de estos mecanismos de seguridad. En los siguientes apartados se lleva a cabo la descripción de cada mecanismo. Se puede consultar un mayor detalle en las especificaciones de Bluetooth (*Core Specifications*)²¹.

²⁰ MAC (Message Authentication Code) es un valor calculado sobre el mensaje, mediante la aplicación de una función hash criptográfica con una clave secreta, que sólo conocen el remitente y destinatario (en este caso, la CSRK). Se utiliza para autenticar un mensaje, es decir, para confirmar que el mensaje proviene del remitente declarado (su autenticidad) y que no ha sido alterado en tránsito (su integridad).

²¹ Las especificaciones de Bluetooth se pueden consultar en: <https://www.bluetooth.com/specifications/bluetooth-core-specification>. Todas las funciones usadas por Bluetooth LE para autenticación, derivación de claves, cálculo de valores de confirmación, etc. se encuentran definidas en Volumen 3- Parte H.

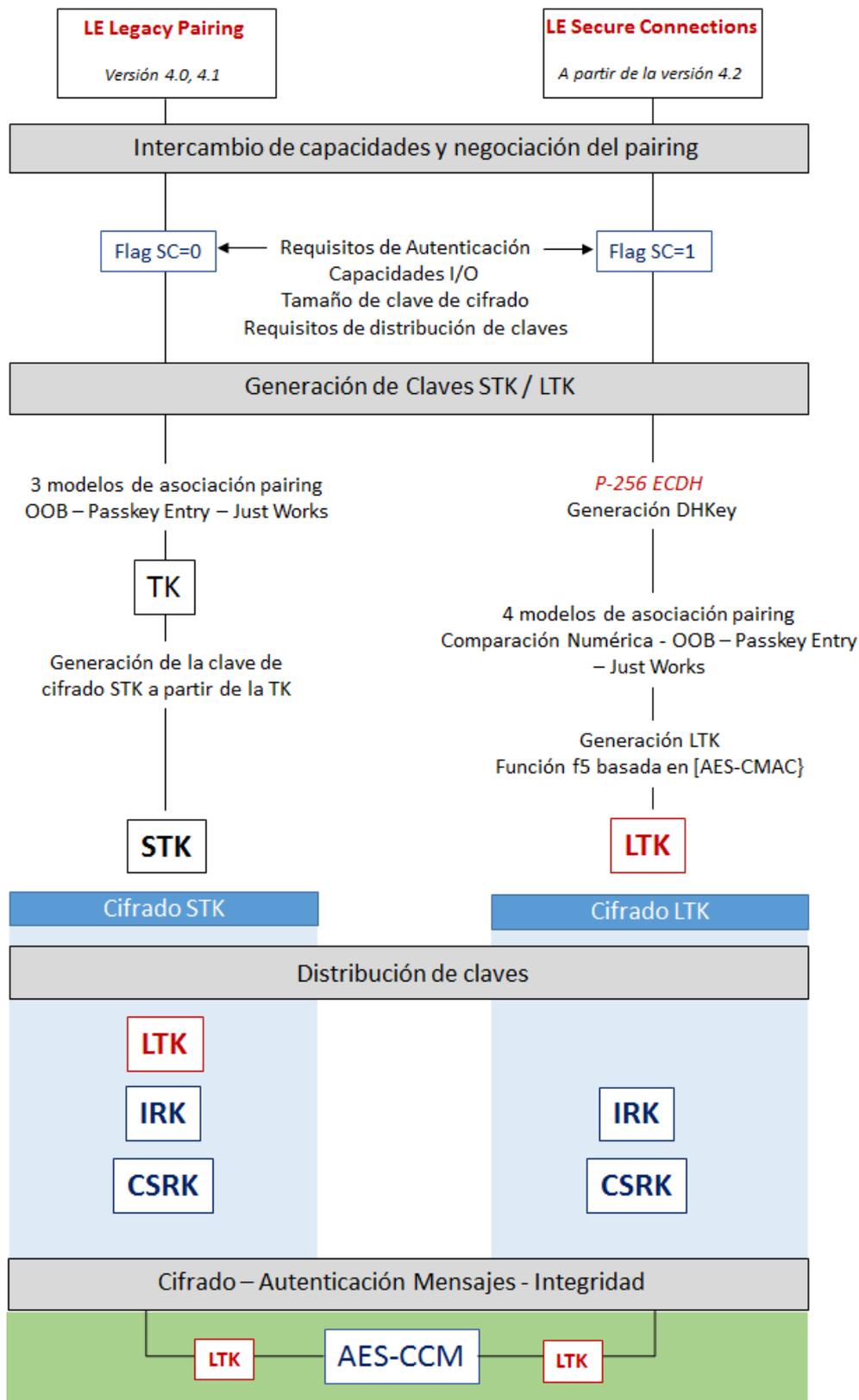


Figura 14. Mecanismos de Seguridad Bluetooth LE.

5.2.2.1 Generación de las claves criptográficas de la conexión

125. La generación de las claves criptográficas de la conexión se realiza por medio del proceso de *pairing*, el cual se lleva a cabo en tres fases:

- **Fase 1.** Intercambio de capacidades y negociación del *pairing*.
- **Fase 2.** Generación de clave:
 - a. Clave de corta duración STK (*Short Term Key*) en LE Legacy Pairing.
 - b. Clave de larga duración LTK (*Long Term Key*) en LE Secure Connections.
- **Fase 3.** Distribución de claves.

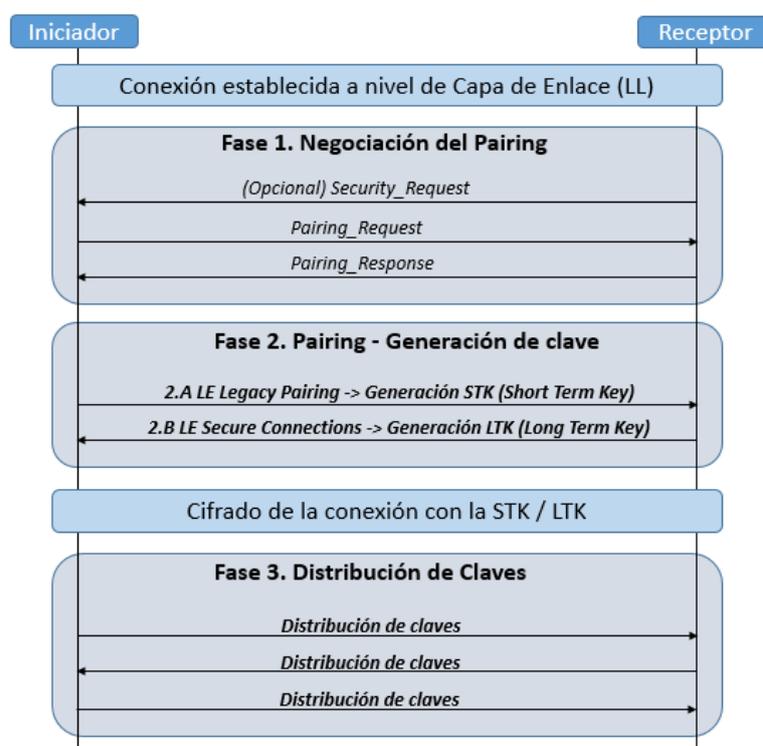


Figura 15. Fases de pairing en Bluetooth LE.
(Figura de BLUETOOTH SPECIFICATION Version 4.2 [Vol 3, Part H])

126. Los mecanismos de seguridad son iniciados por el Gestor de Seguridad (SM) del dispositivo que actúa con el rol de maestro en la conexión (iniciador). Se inician con los comandos SMP (*Security Manager Protocol*) de *Pairing_Request* / *Pairing_Response*. El dispositivo que actúa como esclavo (receptor) responderá a las peticiones del maestro. También cabe la posibilidad de que sea el esclavo quien solicite al maestro el inicio de los mecanismos de seguridad mediante un comando SMP especial (*Security_Request*).

Fase 1. Intercambio de capacidades y negociación del pairing.

Antes de iniciarse el proceso de *pairing*, deben negociarse las características con las que se va a llevar a cabo el mismo. Esto se conoce como negociación del *pairing*. En esta fase previa, los dispositivos intercambian sus capacidades y requisitos y acuerdan los parámetros finales con los que se realizará el *pairing*.

Esto se hace mediante los comandos SMP de *Pairing_Request* y *Pairing_Response* que tienen la sintaxis mostrada en la siguiente figura.

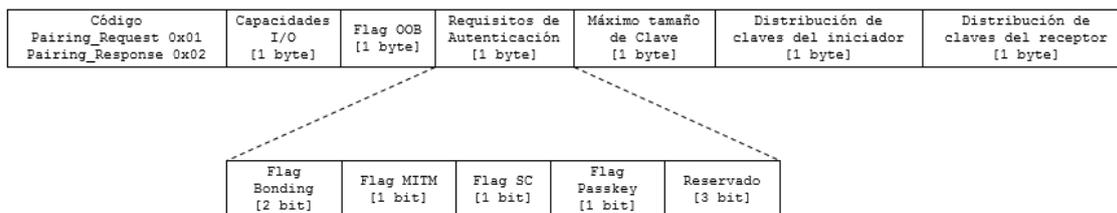


Figura 16. Comandos SMP Pairing Request / Response.

Uno de los aspectos que debe acordarse en la negociación del *pairing* es el tipo de “modelo de asociación”, que es el mecanismo que van a utilizar los dispositivos para autenticarse entre ellos antes de proceder a la generación / intercambio de las claves.

Los modelos de asociación en Bluetooth LE son un total de cuatro: Comparación Numérica, *Passkey Entry*, Fuera de Banda (OOB, *Out-Of-Band*) y *Just Works*. La selección de uno u otro depende además de la tecnología Bluetooth usada, de los siguientes parámetros:

- Protección MITM requerida (Flag MITM Sí / No).
- Capacidades I/O de los dispositivos, referidas a los mecanismos de entrada/salida de datos de los que dispone el dispositivo.
- Disponibilidad en los dispositivos de un canal Fuera de Banda OOB (*Out-Of-Band*). Es decir, de una tecnología adicional de comunicación inalámbrica o cableada como por ejemplo, NFC (*Near Field Communication*).

Fase 2. Generación de clave

Una vez negociado el *pairing*, la siguiente fase tiene por objetivo obtener la clave simétrica que se utilizará para el cifrado de la conexión.

a. LE Legacy Pairing. Generación de la clave de corta duración STK

La clave que se genera en LE Legacy Pairing para el cifrado de la conexión, es una clave de 128 bits llamada clave de corta duración **STK** (*Short Term Key*). Para su generación es necesario que los dispositivos dispongan previamente de una clave temporal llamada TK (*Temporary Key*).

La clave temporal TK es un número aleatorio de 128 bits que se debe generar a través de una función pseudo-aleatoria que cumpla con las especificaciones de Bluetooth.

El modo en que ambos dispositivos obtienen la misma TK, depende del modelo de asociación utilizado en el *pairing* que habrá sido seleccionado en la fase de negociación.

Dado que a partir de la TK se va a generar la clave de cifrado STK, el grado de protección que se logre para la TK determinará el grado de seguridad de la conexión.

En LE Legacy Pairing se pueden utilizar tres modelos de asociación:

- *Just Works*, cuando ninguno de los dispositivos tiene capacidades I/O. La TK se establece a ceros (0x00). No proporciona autenticación por lo que la TK generada es no-autenticada.
- *PassKey Entry*. El usuario o bien introduce un número idéntico, generalmente de 6 dígitos, en ambos dispositivos (*passkey*) o bien un dispositivo lo muestra y el usuario lo introduce en el otro. La TK se forma con esta *passkey*. Proporciona autenticación de dispositivos por lo que la TK generada por este modelo es autenticada.
- Fuera de Banda (*OOB, Out-Of-Band*), que utiliza un canal de comunicación adicional a Bluetooth para la distribución de la TK entre los dispositivos. Ambos dispositivos deberán tener un canal OOB compatible.

Una vez que los dispositivos disponen de la TK, intercambian valores aleatorios y mensajes de confirmación generados con la función *c1* con objeto de verificar que la TK de la que disponen es la misma. La siguiente figura muestra cómo se realiza esta confirmación.

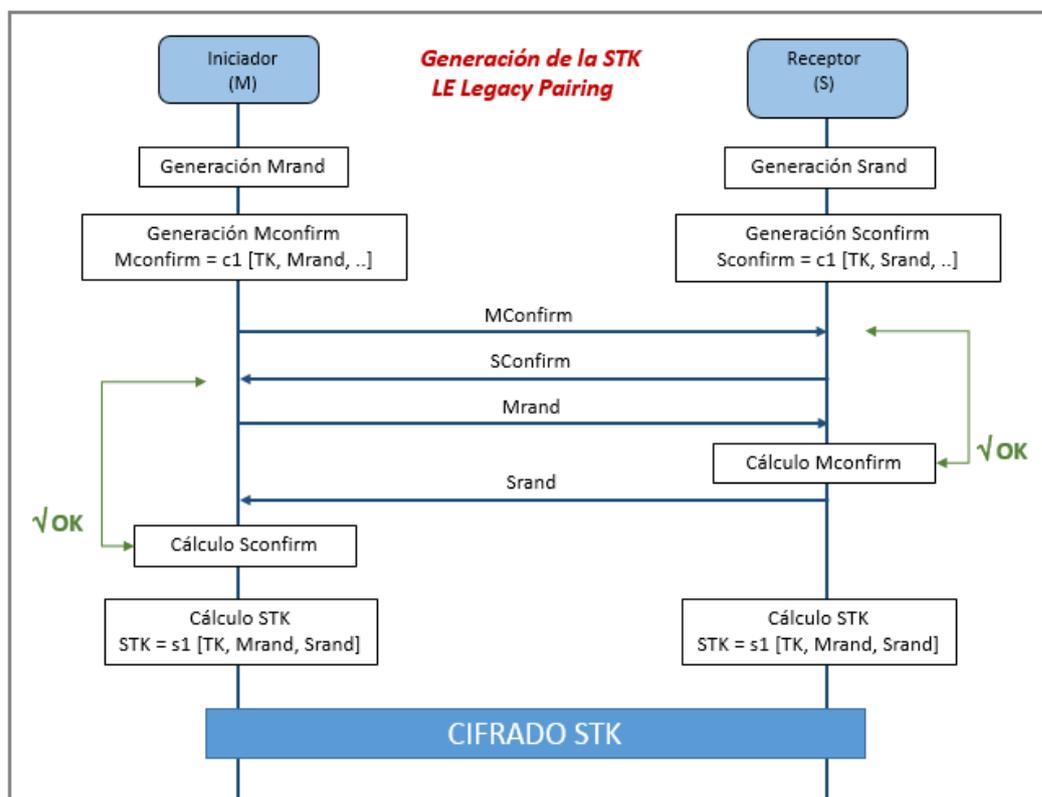


Figura 17. Generación de la STK en LE Legacy Pairing.

A partir de la TK y junto con valores aleatorios intercambiados, se construye la clave de corta duración STK (*Short Term Key*) empleando la función $s1$.

En caso de que la clave STK generada sea superior al máximo tamaño de clave acordado en la fase de negociación del *pairing*, será adaptada al tamaño correcto.

La STK será utilizada para cifrar la conexión actual una vez finaliza el proceso de *pairing*. A través de la conexión cifrada con la STK, se realiza la generación y distribución de otras claves, en especial la clave de larga duración LTK (*Long Term Key*), que será almacenada en los dispositivos y empleada para el cifrado de conexiones futuras entre ambos dispositivos, sin necesidad de llevar a cabo de nuevo el proceso de *pairing*.

b. LE Secure Connections. Generación de la clave de larga duración LTK

La clave que se genera en LE Secure Connections para el cifrado de la conexión, es una clave de hasta 128 bits llamada clave de larga duración LTK.

Para ello, LE Secure Connections emplea algoritmos basados en curva elíptica ECDH (*Elliptic Curve Diffie-Hellman*) que permiten el acuerdo de clave, y añade un nuevo método de *pairing*: Comparación Numérica.

Los pasos que se siguen en la generación de la LTK son los mostrados en la siguiente figura.

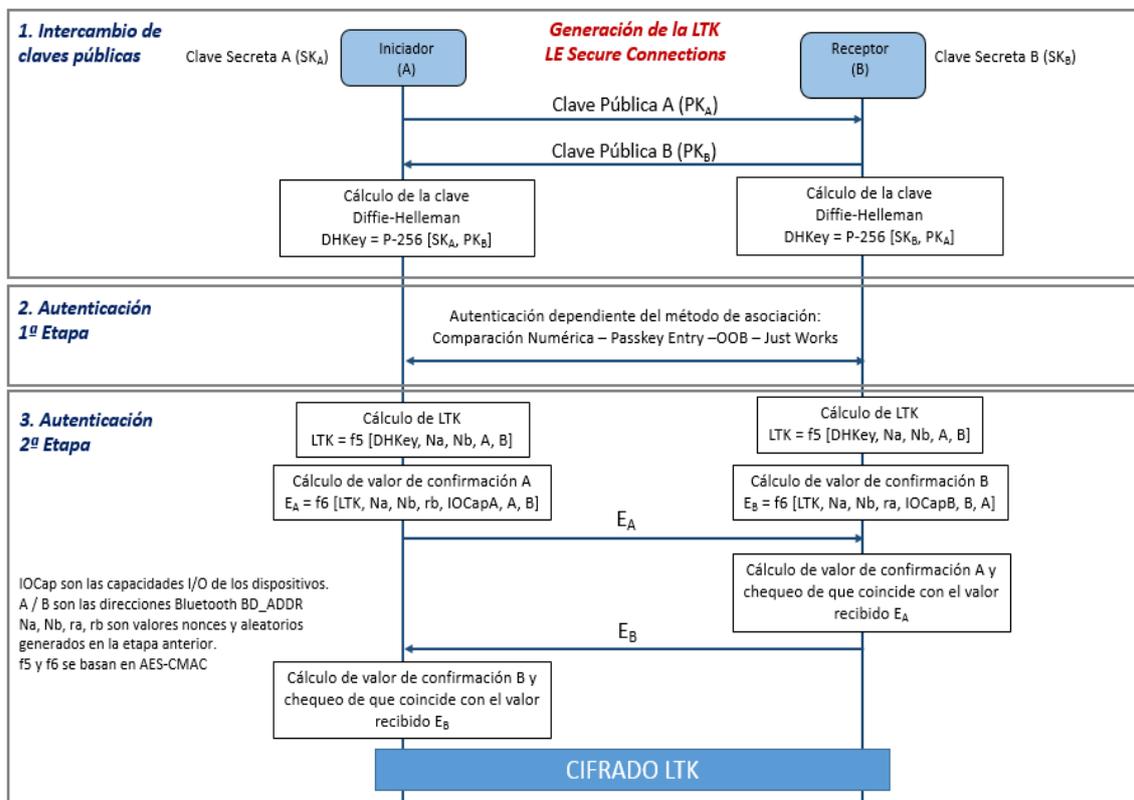


Figura 18. Generación de la LTK en LE Secure Connections.

1. **Intercambio de claves públicas.** En primer lugar se lleva a cabo el intercambio de las claves públicas entre los dispositivos y la generación en cada dispositivo de la clave compartida Diffie-Hellman (DHKey) a través del algoritmo ECDH FIPS P-256.

2. **Autenticación 1ª Etapa.** Tras la generación en cada dispositivo del par de claves pública/privada ECDH, se lleva a cabo una primera etapa de autenticación entre los dispositivos que dependerá del modelo de asociación seleccionado en el *pairing*.

En LE Secure Connections se pueden utilizar cuatro modelos de asociación:

- **Comparación Numérica.** Es el modelo que se utiliza cuando en los requisitos de autenticación se ha acordado la protección MITM y las capacidades I/O de los dispositivos lo permiten.
- **PassKey Entry.** Es el modelo que se utiliza cuando el *flag PassKey* de los requisitos de autenticación está activado y las capacidades I/O de los dispositivos lo permiten.
- **Fuera de Banda (OOB, Out-Of-Band).** En el caso de LE Secure Connections no es necesario que ambos dispositivos dispongan de canal OOB, basta con que uno de ellos lo tenga. Si uno de ellos activa el *flag OOB* en el comando SMP de *Pairing_Request*, este es el modelo de asociación que se empleará en el *pairing*.
- **Just Works,** cuando ninguno de los dispositivos tiene capacidades I/O.

Se puede consultar el detalle de cómo se realiza esta autenticación según el método empleado, en las especificaciones de Bluetooth²².

3. **Autenticación 2ª Etapa – Cálculo de la clave de cifrado LTK.** La segunda etapa de la autenticación, confirma que ambos dispositivos han completado con éxito el intercambio. Cada dispositivo calcula la LTK a través de la función f5 (basada en AES-CMAC) empleando la clave compartida DHKey, junto con los valores aleatorios intercambiados previamente y las direcciones de los dispositivos. A continuación, calculan e intercambian un valor de confirmación, empleando la función f6 (basada también en AES-CMAC), para verificar que ambos dispositivos disponen de la misma LTK.

Fase 3. Distribución de claves.

Las claves adicionales que se van a generar y distribuir se acuerdan entre los dos dispositivos en la fase de negociación del *pairing*, a través de los campos correspondientes a “Distribución de claves” del iniciador y del receptor en los comandos SMP de *Pairing_Request/Response*.

En LE Legacy Pairing, a través de la conexión cifrada con la STK, se generan y distribuyen las siguientes claves:

²² <https://www.bluetooth.com/specifications/bluetooth-core-specification>. [Vol3 – Parte H – Apto 2.3.5.6. LE Secure Connections Pairing Phase 2]

- *Clave de Cifrado de Larga duración LTK (Long Term Key)*. Clave de 128 bits empleada para el cifrado de la conexión a nivel de enlace. Esta clave tiene dos valores asociados que se almacenan en el dispositivo y la identifican de forma que cada vez que se distribuye una nueva LTK, se generan nuevos valores. Estos valores se denominan EDIV (*Encrypted Identifier*, de 16 bit) y Rand (Aleatorio de 64 bit) y habitualmente, son generados por el dispositivo esclavo y enviados al dispositivo maestro para su almacenamiento. Cuando un esclavo inicia una nueva sesión de cifrado con un maestro previamente emparejado, le solicitará la distribución de EDIV y Rand y regenerará la LTK.
- Clave de Privacidad IRK (*Identity Resolving Key*).
- Clave de Firma de Datos CSRK (*Connection Signature Resolving Key*).

En LE Secure Connections, a través de la conexión cifrada con la LTK, se generan y distribuyen las claves IRK y CSRK.

5.2.2.2 Cifrado, Autenticación e Integridad

127. En Bluetooth LE se utiliza AES-CCM para proporcionar los servicios de confidencialidad y autenticación de mensajes e integridad. No existe ninguna etapa separada de autenticación reto-respuesta (*challenge-response*) como en Bluetooth BR/EDR.
128. El éxito del establecimiento del cifrado (usando la clave LTK), de la firma de datos (usando la clave CSRK) y de la resolución de identidades (usando la clave IRK), proporciona una autenticación implícita al significar que ambos dispositivos disponen de las mismas claves.

5.2.2.3 Modos de Seguridad

129. Los modos y niveles de seguridad en Bluetooth LE expresan los requisitos de seguridad de un dispositivo, de un servicio o de una solicitud de servicio. La conexión entre dos dispositivos solo podrá trabajar en un modo y nivel de seguridad.
130. En Bluetooth LE hay dos modos de seguridad: modo 1 y modo 2.
 - A) Modo 1. Tiene los siguientes niveles de seguridad:
 - Nivel 1. Sin seguridad (no hay autenticación ni cifrado).
 - Nivel 2. *Pairing* sin autenticación y uso de cifrado.
 - Nivel 3. *Pairing* con autenticación y uso de cifrado.
 - Nivel 4. *Pairing* con autenticación LE Secure Connections y uso de cifrado (sólo disponible en Bluetooth LE a partir de la versión 4.2).
 - B) Modo 2. Tiene los siguientes niveles de seguridad:
 - Nivel 1. *Pairing* sin autenticación junto con firma de datos.
 - Nivel 2. *Pairing* con autenticación junto con firma de datos.

- 131. El modo de seguridad que se puede considerar más fuerte, es el Modo 1 Nivel 4ya que emplea *Secure Connections* (algoritmo P-256 Elliptic Curve) y cifrado AES-CCM. El Modo 2 no utiliza cifrado.
- 132. A partir de Bluetooth LE 4.2, donde se añade *Secure Connections*, se añade también el modo “Solo *Secure Connections*” que exige que solo se pueda emplear el Modo 1 Nivel 4. Este modo no es por lo tanto compatible con dispositivos LE de versiones 4.1 y 4.2 ya que no disponen de los algoritmos ECDH P-256.

5.2.3 Resumen mecanismos de seguridad Bluetooth

- 133. A continuación, se incluye dos tablas en las que se resumen los mecanismos de seguridad de Bluetooth BR/EDR y de Bluetooth LE.

	Bluetooth BR/EDR	
	Secure Simple Pairing (SSP)	Secure Connections (SC)
Versiones	2.1 a 4.0	A partir de 4.1
Generación de claves (<i>Pairing</i>)	<ul style="list-style-type: none"> ▪ 4 Métodos <i>Pairing</i> (Comparación Numérica, <i>Passkey Entry</i>, OOB, <i>Just Works</i>). ▪ ECDH Acuerdo de clave (Algoritmo P-192 Elliptic Curve). ▪ LK clave de enlace compartida. ▪ Algoritmos de generación de claves basados en HMAC-SHA-256 ▪ Función E3 para generación de la clave de cifrado Kc a partir de la LK. 	<ul style="list-style-type: none"> ▪ 4 Métodos <i>Pairing</i> (Comparación Numérica, <i>Passkey Entry</i>, OOB, <i>Just Works</i>). ▪ ECDH Acuerdo de clave (Algoritmo P-256 Elliptic Curve). ▪ LK clave de enlace compartida. ▪ Algoritmos de generación de claves basados en HMAC-SHA-256 ▪ Función h3 (basada en HMAC-SHA-256) para la generación de la clave de cifrado AES a partir de la LK.
Autenticación de Dispositivos	<p>Legacy Authentication</p> <ul style="list-style-type: none"> ▪ Autenticación unidireccional. Mutua opcional. ▪ Algoritmo E1 basado en SAFER+. 	<p>Secure Authentication</p> <ul style="list-style-type: none"> ▪ Autenticación Mutua. ▪ HMAC-SHA-256.
Cifrado	Algoritmo E0	AES-CCM
Integridad	No	AES-CCM
Protección frente a <i>eavesdropping</i>	<p>Sí. Aunque el tráfico de <i>pairing</i> y de autenticación sea capturado a través de escuchas ilegales (<i>eavesdropping</i>), debe resolverse un problema complejo en criptografía de clave pública (ECDH) para obtener la LK a partir de la información capturada. Esta protección es independiente del modelo de asociación <i>pairing</i> empleado.</p>	

Tabla 4. Resumen de los mecanismos de seguridad Bluetooth BR/EDR.

	Bluetooth LE	
	LE Legacy Pairing	LE Secure Connections
Versiones	4.0 / 4.1	A partir de 4.2
Generación de claves (<i>Pairing</i>)	<ul style="list-style-type: none"> ▪ Generación de STK. ▪ Uso de TK, clave temporal. ▪ 3 Métodos <i>Pairing</i> (Passkey Entry, OOB, Just Works). ▪ Algoritmos de generación de claves AES-128. 	<ul style="list-style-type: none"> ▪ Generación de LTK. ▪ 4 Métodos <i>Pairing</i> (Comparación Numérica, <i>Passkey Entry</i>, OOB, <i>Just Works</i>). ▪ ECDH Acuerdo de clave (P-256 Elliptic Curve). ▪ Algoritmos de generación de claves basados en AES-CMAC.
Autenticación de Dispositivos	AES-CCM	AES-CCM
Cifrado	AES-CCM	AES-CCM
Integridad	AES-CCM	AES-CCM
Protección frente a <i>eavesdropping</i>	<p>No.</p> <p>No usa ECDH para la generación de la clave de cifrado STK. Esta se genera usando una clave temporal TK, que puede ser capturada al ser intercambiada por un enlace no cifrado. Solo cabe la posibilidad de protección para el caso del método de asociación OOB cuando el canal OOB proporciona esta protección.</p>	<p>Sí.</p> <p>Utiliza algoritmos ECDH (P-256) para la generación de la clave DHKey compartida entre los dispositivos. Esta DHKey se utiliza para generar la clave de cifrado LTK. Dado que la DHKey no es distribuida, es muy difícil averiguar la LTK.</p>

Tabla 5. Resumen de los mecanismos de seguridad Bluetooth LE.

6 MEDIDAS DE SEGURIDAD DEL ENS

134. El Real Decreto 3/2010, de 8 de enero, modificado a su vez por el Real Decreto 951/2015, de 23 de octubre, regula el Esquema Nacional de Seguridad (en adelante, ENS) en el ámbito de la Administración Electrónica.
135. El ENS está constituido por los principios básicos y requisitos mínimos requeridos para una protección adecuada de la información. Será aplicado por las Administraciones Públicas para asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos,

- informaciones y servicios utilizados en los medios electrónicos que gestionen el ejercicio de sus competencias.
136. En el ámbito referido al uso de Bluetooth dentro de la organización, el cumplimiento de los principios básicos y requisitos mínimos establecidos en el ENS supone la aplicación de las medidas de seguridad recogidas en su Anexo II que sean aplicables a la protección de las comunicaciones y de los dispositivos Bluetooth.
 137. Para llevar a cabo la selección de estas medidas de seguridad se deberá seguir el procedimiento indicado en el Anexo II del ENS, que consta de los siguientes pasos:
 - a. Identificar los sistemas, servicios, recursos y/o información de la organización a los que se tiene acceso a través de la conexión Bluetooth así como los responsables de los mismos.
 - b. Determinar para dichos sistemas, servicios, recursos y/o información y a través de los responsables, las dimensiones de seguridad relevantes y sus niveles correspondientes, teniendo en cuenta lo indicado en el **Anexo I del ENS**.
 - c. Determinar, en caso de que sea aplicable, la categoría del sistema al que se tiene acceso a través de la conexión Bluetooth, según lo indicado en el **Anexo I del ENS**.
 - d. Seleccionar las medidas de seguridad apropiadas de entre las contenidas en el **Anexo II del ENS**, de acuerdo con las dimensiones de seguridad y sus niveles y en su caso, de acuerdo con la categoría del sistema.
 138. La organización deberá, por lo tanto, llevar a cabo el análisis siguiendo el proceso anteriormente indicado, concluir las medidas que le sean de aplicación en función de las características de sus comunicaciones y dispositivos Bluetooth y establecer el mejor modo de aplicarlas.
 139. La presente guía ofrece en los siguientes apartados, una selección de las medidas de seguridad más relevantes aplicables al uso de Bluetooth dentro de la organización, así como una propuesta para llevar a cabo su implementación a modo orientativo.

6.1 ÁMBITO DE USO DE LA TECNOLOGÍA BLUETOOTH

140. Para establecer el ámbito de uso de la tecnología Bluetooth dentro de la organización se considerarán dos factores: el tipo de dispositivos y el entorno de seguridad, desde los que se permitirá el establecimiento de comunicaciones Bluetooth con sistemas, servicios, recursos y/o información de la organización.
 - a. **Tipo de dispositivos.**
141. Es necesario realizar la distinción entre dispositivos corporativos y dispositivos externos.
142. Los dispositivos no corporativos o externos, representan dispositivos que no se encuentran bajo el control de la organización, correspondiendo generalmente a

dispositivos personales de los usuarios o perteneciendo a personal externo. Estos dispositivos no están sujetos a la política de seguridad de la información de la organización.

143. Los dispositivos corporativos, serán aquellos dispositivos que se encuentran bajo el control de la organización y están, por lo tanto, sometidos a su política de seguridad. Por ejemplo: ordenadores, *tablets* corporativas, impresoras, etc.

b. Entorno de seguridad de la organización.

144. Es necesario realizar la distinción entre entorno de seguridad de la organización y entorno exterior.
145. El entorno de seguridad de la organización, corresponde al interior de sus instalaciones que estarán adecuadamente protegidas con los correspondientes controles, garantizando el acceso solo a personal autorizado.
146. El entorno exterior, corresponde a todo espacio que se encuentre fuera de las instalaciones de la organización, carente por lo tanto, de medidas de protección.
147. Teniendo en cuenta estos dos factores y en base al principio básico de seguridad por defecto y mínima funcionalidad recogido en el **Artículo 19 del ENS**, el ámbito de uso de Bluetooth dentro de la organización deberá comprender únicamente el uso de dispositivos corporativos y preferiblemente, dentro del entorno de seguridad de la organización. En cualquier otro caso, no se recomienda autorizar el uso de Bluetooth para establecer comunicaciones con sistemas, servicios, recursos y/o información de la organización.
148. Como excepción, podrán emplearse dispositivos externos o no corporativos para establecer conexiones Bluetooth con recursos de carácter público, como pueden ser, por ejemplo, servicios web ofrecidos por la organización.
149. El uso de comunicaciones Bluetooth entre dispositivos corporativos fuera del entorno de seguridad de la organización, no es una práctica recomendada y sólo podrá autorizarse cuando, atendiendo al principio de mínima funcionalidad, sea estrictamente necesario y únicamente en el caso de que se implementen las medidas de protección de las comunicaciones apropiadas que se indican en los siguientes apartados.

6.2 NORMATIVA DE SEGURIDAD Y GESTIÓN DE RIESGOS

150. El uso de Bluetooth en la organización, deberá estar perfectamente especificado en su normativa de seguridad y deberá responder a un análisis de riesgos.
151. Al tratarse de una tecnología de comunicaciones inalámbricas, es recomendable que se encuentre integrada dentro de la Normativa, Procedimientos y Procesos relativos al uso y explotación de redes inalámbricas.
152. En esta línea y en cumplimiento de la medida **[org.2]**, *la Política de Seguridad para redes inalámbrica*, que incorporará todas las tecnologías inalámbricas

- implementadas en la organización, deberá establecer claramente si se permite o no el uso de Bluetooth y bajo qué condiciones.
153. Esta Política deberá incluir al menos, los siguientes aspectos:
- Lista de dispositivos Bluetooth autorizados y aceptados en la organización.
 - Uso apropiado e inapropiado de Bluetooth y las medidas disciplinarias correspondientes.
 - Qué se puede hacer a través de conexiones Bluetooth y a qué sistemas, servicios, recursos y/o información se puede acceder.
 - Cuál debe ser la configuración de seguridad mínima de los dispositivos y qué medidas deben establecerse para su protección, especialmente los que sean portátiles y puedan ser objeto de robo fuera de las instalaciones de la organización.
 - Política de almacenamiento de información sensible en los dispositivos Bluetooth, detallando el nivel máximo de la información que puede ser almacenada en este tipo de dispositivos.
154. Atendiendo a lo establecido en la medida **[org.3]**, los Procedimientos correspondientes al uso de la tecnología inalámbrica tendrán en cuenta Bluetooth. Así, deberán indicarse en ellos aspectos como la atención a ataques y vulnerabilidades propios de la tecnología Bluetooth, el alcance y periodicidad de las auditorías sobre el uso de Bluetooth, etc.
155. En función de lo indicado en la medida **[org.4]**, deberá incorporarse también un Proceso de Autorización de usuarios y dispositivos para el uso de Bluetooth.
156. En relación a la gestión de riesgos y en función del **Artículo 13** del ENS y de lo establecido en la medida **[op.pl.1]**, la organización que decide autorizar Bluetooth como medio de acceso a sus sistemas, servicios y/o información, deberá realizar la gestión de los riesgos relacionados con el uso de esta tecnología.
157. Esta gestión debe realizarse por medio del análisis y tratamiento de los riesgos a los que están expuestos este tipo de comunicaciones. Esto permitirá el mantenimiento de un entorno controlado minimizando los riesgos hasta niveles aceptables. La reducción de estos, se realizará mediante el despliegue de las correspondientes medidas de seguridad, manteniendo la proporcionalidad entre ellas y los riesgos.
158. A la hora de planificar y diseñar la seguridad que mitigue los riesgos introducidos por el uso de Bluetooth, se deberán tener en cuenta no sólo los medios técnicos necesarios, sino también humanos, materiales y organizativos. Se deberá prestar máxima atención a la concienciación de las personas que harán uso de la tecnología Bluetooth y a sus responsables jerárquicos, para que ni la ignorancia ni la falta de organización y coordinación ni las instrucciones inadecuadas, sean fuentes de riesgo para la seguridad.

6.3 PROTECCIÓN DE LAS COMUNICACIONES BLUETOOTH

159. Las medidas de protección de las comunicaciones, concretamente [mp.com.2] y [mp.com.3], establecen los requisitos que deben cumplir las tecnologías de comunicaciones para proporcionar la adecuada protección de la confidencialidad [C], autenticidad [A] e integridad [I] de la información transmitida.

Nivel Bajo [I C A]

160. En el caso de que todas las dimensiones de: integridad [I], confidencialidad [C], autenticidad [A] de la información tengan un nivel bajo, [mp.com.3] establece que se debe asegurar la autenticidad de los extremos antes de establecer la comunicación.

161. Bluetooth proporciona autenticación de dispositivos, empleando diferentes mecanismos en función de la tecnología Bluetooth empleada, tal y como se ve en la siguiente tabla.

	Bluetooth BR/EDR			Bluetooth LE	
	Versiones anteriores a 2.1	Versiones 2.1 a 4.0	Versiones a partir de 4.1	Versiones 4.0 y 4.1	Versiones a partir de 4.2
Mecanismo de Pairing	BR/EDR Legacy Pairing	Secure Simple Pairing	BR/EDR Secure Connections	LE Legacy Pairing	LE Secure Connections
Mecanismo Autenticación dispositivos	Legacy Authentication		Secure Authentication	No existe fase explícita de autenticación de dispositivos	
Tipo de Autenticación	Uni-direccional Mutua opcional		Autenticación mutua		
Algoritmo de Autenticación	E1 (SAFER+)		HMAC-SHA-256	AES-CCM	AES-CCM

Tabla 6. Mecanismos de autenticación de dispositivos Bluetooth.

162. Todas las tecnologías Bluetooth proporcionan mecanismos de autenticación mutua de dispositivos.

163. Se recomienda sin embargo, emplear las implementaciones Bluetooth que proporcionan los modos de seguridad más robustos, especialmente si la comunicación se establece fuera del dominio de seguridad de la organización. Esto supone el uso de Bluetooth BR/EDR a partir de la versión 4.1 y de Bluetooth LE a partir de la versión 4.2. No se recomienda en ningún caso el uso de versiones de Bluetooth inferiores a 2.1.

164. En caso de que sea necesario el uso de tecnologías más antiguas, las recomendaciones son las siguientes.

- Debe evitarse el uso del modelo de asociación de *pairing* “Just Works” ya que no proporciona protección MITM. El uso de este tipo de dispositivos debe ser evitado si existen otros que ofrecen las mismas funciones y soportan otros modelos de asociación (comparación numérica, OOB o *passkey entry*).
- Si se utiliza el modelo de asociación *passkey entry*, la *passkey* que se utilice debe ser aleatoria. No debe utilizarse una estática en varios procesos de *pairing*, ya se reduce la protección MITM que proporciona este modelo de asociación.
- Usar el modo de seguridad más robusto permitido por la tecnología (ver apartado 5.2 Arquitectura de Seguridad).

Nivel Medio [I C A]

165. En el caso de que una o varias de las dimensiones de la información alcancen un nivel medio y ninguna de ellas alcance nivel alto, los requisitos de protección de las comunicaciones aplicados a Bluetooth son los siguientes:
- No se recomienda establecer conexiones Bluetooth fuera del entorno de seguridad de la organización. En caso de que estas sean necesarias, atendiendo al principio de mínima funcionalidad deberán emplearse mecanismos de protección equivalentes a una VPN.
 - Los mecanismos de protección de la comunicación deben hacer uso de algoritmos acreditados por el Centro Criptológico Nacional (CCN).
166. A continuación se incluye una tabla resumen con los algoritmos empleados por las tecnologías Bluetooth para generación de claves, cifrado e integridad.

	Bluetooth BR/EDR			Bluetooth LE	
	Versiones anteriores a 2.1	Versiones 2.1 a 4.0	Versiones 4.1 y superiores	Versiones 4.0 y 4.1	Versiones a partir de 4.2
Generación de claves criptográficas (Pairing)	E21/E22 (SAFER+)	P-192 ECDH HMAC-SHA-256	P-256 ECDH HMAC-SHA-256	AES-128	P-256 ECDH AES-CMAC
Cifrado	E0 (Basado en SAFER+)		AES-CCM	AES-CCM	AES-CCM
Integridad	-		AES-CCM	AES-CCM	AES-CCM

Tabla 7. Algoritmos empleados por Bluetooth.

167. La guía *CCN-STIC-807 – Criptografía de empleo en el ENS*, recoge la relación de algoritmos y protocolos criptográficos que se consideran acreditados por el CCN para su uso dentro del ENS, así como las especificaciones que deben seguirse para su correcta implementación.

168. Según la información recogida en dicha guía²³, dentro de los algoritmos empleados por Bluetooth están acreditados AES (*Advanced Encryption Standard*) para cifrado y ECDH para intercambio de clave.
169. Deben usarse, por lo tanto, las tecnologías Bluetooth de *Secure Connections* con los modos de seguridad más elevados:
- En dispositivos Bluetooth BR/EDR, el Modo 4 Nivel 4 que proporciona una clave de enlace autenticada empleando *Secure Connections* y cifrado AES-CCM. Esto supone el uso de dispositivos con versiones Bluetooth BR/EDR a partir de 4.1.
 - En dispositivos Bluetooth LE, el Modo 1 Nivel 4 que proporciona *pairing* con autenticación LE *Secure Connections* y cifrado AES-CCM. Esto supone el uso de dispositivos con versiones Bluetooth LE a partir de 4.2.
170. La guía *CCN-STIC-807* indica también que, cuando se alcance nivel medio en la dimensión de confidencialidad [C], la clave de cifrado simétrico deberá ser, al menos, de 112 bits. La longitud de la clave de cifrado es un parámetro que se acuerda entre los dispositivos Bluetooth en la fase de negociación del *pairing* y en las tecnologías *Secure Connections* puede tener una longitud de entre 7 y 16 octetos. Por lo tanto, la clave deberá tener como mínimo 14 octetos (112 bits) aunque se recomienda que sea de longitud máxima, 16 octetos (128 bits).
171. Respecto a los modelos de asociación de *pairing* que dependen de las capacidades I/O de los dispositivos, se recomienda lo siguiente:
- Evitar el uso del modelo de asociación "*Just Works*" ya que no proporciona protección MITM. El uso de este tipo de dispositivos debe ser evitado si existen otros que ofrecen las mismas funciones y soportan otros modelos de asociación (comparación numérica, OOB o *passkey entry*).
 - Si se utiliza el modelo de asociación *Passkey entry*, la *passkey* que se utilice debe ser aleatoria. No debe utilizarse una estática en varios procesos de *pairing* ya se reduce la protección MITM que proporciona este modelo de asociación.

Nivel Alto [I C A]

172. En el caso de que una o varias de las dimensiones de: integridad [I], confidencialidad [C], autenticidad [A] de la información alcancen un nivel alto, no se deben emplear conexiones Bluetooth ya que Bluetooth es una tecnología para establecer comunicaciones inalámbricas Ad-Hoc (entre dispositivos y sin infraestructura) y por lo tanto, no es posible el uso de dispositivos hardware certificados conforme a lo establecido en la medida [op.pl.5].

²³ Según a la versión de la guía CCN-STIC-807 de abril 2017, vigente en el momento de elaboración de la presente guía.

6.4 PROTECCIÓN DE LOS DISPOSITIVOS BLUETOOTH

173. Los dispositivos Bluetooth que accedan a sistemas, servicios, recursos y/o información de la organización, deberán implementar las medidas de seguridad establecidas en sus políticas y normativas de seguridad.
174. Los dispositivos Bluetooth, ya que en su gran mayoría serán susceptibles de salir de las instalaciones de la organización y no podrán beneficiarse de la protección física correspondiente, estarán expuestos a un riesgo manifiesto de pérdida o robo y deberán ser protegidos también según lo indicado en la medida **[mp.eq.3]**.

6.4.1 Autenticación

a) Autenticación de Dispositivos

175. Bluetooth proporciona únicamente autenticación de dispositivos.
176. El proceso de autenticación forma parte de las etapas del proceso de *pairing* que llevan a cabo los dispositivos para el establecimiento de la comunicación Bluetooth. Este proceso de autenticación, está condicionado por la tecnología Bluetooth utilizada y se recoge en el apartado 6.3 Protección de las comunicaciones.

b) Autenticación de usuarios

177. Además de la autenticación de dispositivos proporcionada de forma nativa por Bluetooth es necesaria la existencia de mecanismos de autenticación de usuario. Esto permite que sólo los usuarios autorizados para hacer uso de una conexión o aplicación Bluetooth, lo hagan y no todos aquellos que puedan tener acceso al dispositivo.
178. La arquitectura de seguridad de Bluetooth permite a las aplicaciones establecer políticas de seguridad más granulares. Por lo tanto, la autenticación basada en usuario y los controles de acceso más granulados dentro del marco de seguridad de Bluetooth pueden y deben ser proporcionados por mecanismos adicionales implementados a través de las capas de aplicación.
179. La medida de seguridad **[op.acc.5]** establece los requisitos para estos mecanismos de autenticación de usuarios.

Nivel Bajo [I C A T]

180. En el caso de que las dimensiones de: integridad [I], confidencialidad [C], autenticidad [A] y trazabilidad [T] de la información alcancen todas ellas un nivel bajo, podrá utilizarse la autenticación de un solo factor.
181. Este factor podrá ser de cualquier tipo: contraseñas o claves concertadas, *tokens*, biometría, etc. En caso de uso de contraseñas o claves concertadas, estas deberán responder a un nivel mínimo de fortaleza (frente a ataques de adivinación, diccionario y fuerza bruta) y deberá existir y aplicarse una Política de contraseñas que indique, además de los requisitos de las contraseñas, el tiempo mínimo de renovación, los intentos máximos permitidos, etc.

Nivel Medio [I C A T]

182. En el caso de que alguna las dimensiones de: integridad [I], confidencialidad [C], autenticidad [A] y trazabilidad [T] de la información o todas ellas, alcancen un nivel medio y ninguna de ellas alcance nivel alto, deberá utilizarse la autenticación de doble factor.
183. Este factor podrá ser de cualquier tipo: contraseñas o claves concertadas, *tokens*, biometría, etc. En caso de uso de contraseñas o claves concertadas, estas deberán responder a un nivel medio de fortaleza (frente a ataques de adivinación, diccionario y fuerza bruta) y deberá existir y aplicarse una Política de contraseñas con exigencias de nivel medio sobre las mismas, su renovación, intentos máximos permitidos, etc.

Nivel Alto [I C A T]

184. En el caso de que alguna de las dimensiones de: integridad [I], confidencialidad [C], autenticidad [A] y trazabilidad [T] de la información alcance un nivel Alto, deberá utilizarse la autenticación de doble factor.
185. Este factor podrá ser de cualquier tipo: contraseñas o claves concertadas, *tokens*, biometría, etc. En caso de uso de contraseñas o claves concertadas, estas deberán responder a un nivel alto de fortaleza (frente a ataques de adivinación, diccionario y fuerza bruta) y deberá existir y aplicarse una Política de contraseñas exigencias de nivel alto sobre las mismas, su renovación, intentos máximos permitidos, etc. En caso de uso de “algo que se tiene”, deberán utilizarse elementos criptográficos hardware que hagan uso de Algoritmos acreditados por el Centro Criptológico Nacional (CCN).

6.4.2 Configuración de Seguridad

186. Los dispositivos Bluetooth deben disponer de una configuración de seguridad tal y como se establece en la medida **[op.exp.2]**.
187. Esta configuración de seguridad debe encontrarse perfectamente definida y documentada y atender a los principios de mínima funcionalidad y seguridad por defecto.
188. La configuración de seguridad de los dispositivos Bluetooth, contemplará las medidas necesarias para el cumplimiento de la política de seguridad de la organización según corresponda al tipo de dispositivo. Por ejemplo, los ordenadores deberán cumplir con actualización del antivirus, parches del sistema operativo, cortafuegos personales, etc²⁴.
189. La Política de seguridad de redes inalámbricas incluirá una configuración de seguridad específica que contemple las medidas de seguridad aplicables a Bluetooth.

²⁴ Se recomienda la consulta de las guías CCN-STIC relacionadas con la implementación del ENS en equipos cliente (por ejemplo, 850 y 899 referidas a equipos cliente con sistema operativo Microsoft Windows).

190. Nunca deberá dejarse en los dispositivos la configuración por defecto ya que generalmente no son seguras. Debe realizarse una revisión minuciosa de todos los parámetros de la configuración Bluetooth y asegurar el cumplimiento de la política de seguridad.
191. La configuración de seguridad para Bluetooth deberá considerar al menos los siguientes aspectos:
- Deshabilitar la capacidad Bluetooth del dispositivo cuando no se estén utilizando comunicaciones basadas en Bluetooth. Sólo deberá ser habilitada expresamente por el usuario para establecer una conexión. Para dispositivos que no permitan esta opción (por ejemplo, unos auriculares), se deberá apagar o desconectar el dispositivo cuando no se utilice.
 - Los dispositivos Bluetooth deberán estar por defecto en modo no visible (*undiscoverable*) y sólo cambiar su configuración a modo visible (*discoverable*) cuando sea absolutamente necesario para conectarse con otros dispositivos. Aunque es posible descubrir dispositivos no visibles mediante el uso de un *sniffer* Bluetooth o técnicas de fuerza bruta sobre la dirección del dispositivo (BD_ADDR), los dispositivos no visibles mitigan la utilización de un gran número de herramientas y técnicas de ataque a través de Bluetooth.
 - Cuando sea posible el dispositivo debe ser configurado de tal forma que cualquier solicitud de conexión Bluetooth entrante, deba ser mostrada al usuario para que éste la autorice antes de proseguir.
 - El nombre del dispositivo no debe ser descriptivo. No debe revelar ninguna característica relacionada con el dispositivo (como marca y modelo), el usuario o la organización. Esta situación podría facilitar la realización de ataques dirigidos y el encontrar vulnerabilidades específicas del dispositivo.
 - El nivel de potencia de los dispositivos debe estar ajustado al mínimo necesario, de forma que las transmisiones Bluetooth permanezcan dentro del perímetro de seguridad de la organización. En este sentido, es recomendable evitar el uso de dispositivos clase 1 que disponen de un rango de alcance muy elevado así como de cualquier tipo de amplificador o antena de alta ganancia.
 - Los servicios y perfiles Bluetooth disponibles en los dispositivos, deben ajustarse al principio de mínima funcionalidad. En caso de que el dispositivo permita deshabilitar perfiles de forma selectiva, sólo deberán estar habilitados aquellos que sean absolutamente necesarios.
 - Configurar contraseñas de acceso en los dispositivos Bluetooth portátiles. Esto ayuda a prevenir accesos no autorizados en caso de que el dispositivo se pierda o sea robado.
 - Instalar software de antivirus en los dispositivos Bluetooth donde esto sea posible (por ejemplo, en ordenadores). Eso ayuda a prevenir que malware desconocido se introduzca en las redes y otros dispositivos Bluetooth.

- Actualizar regularmente el software Bluetooth e instalar las actualizaciones y parches del firmware y sistema operativo en los dispositivos proporcionados por el fabricante. Cada vez que se descubre una nueva vulnerabilidad los fabricantes publican los parches correspondientes. Estos deben ser implementados habiendo pasado previamente por un proceso de pruebas que confirme su efectividad.

6.4.3 Gestión de la Configuración

192. Tal y como se indica en la medida de seguridad **[op.exp.3]**, se debe elaborar y mantener actualizado un inventario completo de todos los dispositivos Bluetooth de la organización recogiendo, al menos sus direcciones (BR_ADDR) y los servicios ofrecidos a través de las conexiones Bluetooth y sus características, especialmente las de seguridad.
193. Esto ayudará, entre otras cosas, a detectar dispositivos Bluetooth no autorizados en las auditorías de seguridad que se lleven a cabo con el objetivo de buscar usos no autorizados de tecnologías inalámbricas.

Categoría Media / Alta

194. La configuración Bluetooth deberá tenerse en cuenta en el proceso de Gestión de la Configuración de los dispositivos de la organización.
195. Se recomienda estandarizar al máximo posible la configuración Bluetooth de los dispositivos. Es recomendable también, que esta configuración se pueda desplegar y mantener de forma automática en todos los dispositivos.
196. Para ello se puede incorporar la configuración Bluetooth en el software de gestión de la configuración general de la organización, en aquellos dispositivos en los que sea posible, por ejemplo, en ordenadores o impresoras.

6.4.4 Registros de actividad

197. Dado que a través de la conexión Bluetooth se lleva a cabo el acceso a sistemas, recursos, servicios y/o información de la organización, la medida **[op.exp.8]** especifica que debe quedar registro de la actividad realizada.
198. Esto posibilita la trazabilidad de acciones y proporciona registros que podrán ser revisados en caso de que ocurra alguna actividad maliciosa.
199. Como Bluetooth no proporciona mecanismos de trazabilidad, la organización debe implementarlos para proporcionar estos registros de actividad que deberán contener:
 - Quién realiza la conexión (dispositivo y usuario)
 - Cuándo se realiza y sobre qué recurso, información o servicio.
 - Registro tanto de conexiones exitosas como fallidas.

Nivel Medio [T]

200. En caso de que la trazabilidad [T] tenga un nivel medio, se deberá realizar una revisión informal de los registros de actividad con objeto de identificar problemas de seguridad y tomar las acciones correctivas cuanto antes.

Nivel Alto [T]

201. En caso de que la trazabilidad [T] tenga un nivel alto, se enviarán los registros en tiempo real a un servidor centralizado para su almacenamiento, correlación y explotación automática. Además, según se indica en la medida **[op.exp.10]** deberán ser protegidos de forma que no puedan ser modificados ni eliminados por personal no autorizado.

6.5 MEDIDAS OPERATIVAS

6.5.1 Mantenimiento

202. La tecnología Bluetooth se encuentra en constante evolución, por lo que además de designar a un responsable encargado de las actividades de mantenimiento recogidas en la medida **[op.exp.4]**, es una buena práctica que la organización designe un responsable encargado de realizar el seguimiento del avance de la tecnología Bluetooth (por ejemplo, a través de Bluetooth SIG).
203. Este responsable además, deberá estar al día de las amenazas y vulnerabilidades que vayan descubriéndose y de esta forma asegurar de manera continuada que se hace un uso seguro de la tecnología Bluetooth en la organización. También realizará un seguimiento en las Web y boletines de seguridad de los fabricantes para conocer las vulnerabilidades asociadas a los dispositivos y obtener las nuevas versiones que solucionan los problemas encontrados.
204. Se deberá tener en cuenta que antes de llevar a cabo el despliegue de nuevas características de seguridad, la organización debe entender completamente los requisitos técnicos, operativos, de seguridad y de personal previo a la implementación.
205. Como parte de las actividades de mantenimiento, es una buena práctica revisar de forma periódica la lista de dispositivos emparejados y de confianza y eliminar aquellos que no son utilizados tan pronto como sea posible.

6.5.2 Auditorías de seguridad

206. Bluetooth deberá ser incluido en las Auditorías de seguridad periódicas que la organización realice sobre sus sistemas e infraestructuras. De esta forma, podrá identificarse el uso y existencia de dispositivos Bluetooth, y especialmente dispositivos no autorizados o mal configurados (*rogue*) que incumplan con las políticas y normativa de seguridad establecidas.

6.6 MEDIDAS APLICABLES AL PERSONAL

207. La organización debe asegurarse de que todos los usuarios y personal relacionado con el uso de la tecnología Bluetooth son plenamente conscientes de sus responsabilidades en relación con la seguridad.
208. Esto se puede lograr mediante la concienciación y la formación del personal, tal y como se establece en las medidas [mp.per.3] y [mp.per.4],
209. Es una buena práctica establecer programas de concienciación sobre la seguridad, que enseñen a los usuarios a seguir prácticas que ayudan a prevenir los incidentes de seguridad.
210. Dentro de las buenas prácticas para el uso de la tecnología Bluetooth, se recomienda incluir las siguientes:
 - Llevar a cabo el proceso de *pairing* (emparejamiento entre dispositivos) con la menor frecuencia posible y siempre en áreas seguras (áreas en el interior de las instalaciones, alejadas de puertas y ventanas y con acceso restringido). Hay que tener en cuenta que el proceso de *pairing* es una función vital de seguridad ya que a través de este proceso se lleva a cabo la generación de las claves criptográficas. Las escuchas ilegales (*eavesdropping*) durante este proceso representan un grave peligro del que los usuarios deben ser conscientes.
 - Los usuarios solo deben establecer conexiones con otros dispositivos de confianza y aceptar contenido solo de estos. No se deben aceptar solicitudes de conexión, ficheros o cualquier otro elemento de orígenes desconocidos.
 - Cuando un dispositivo haya sido robado, perdido o comprometido, el usuario inmediatamente debe proceder a borrarlo de la lista de confianza del resto de sus dispositivos Bluetooth.
 - Es una buena práctica revisar de forma periódica la lista de dispositivos emparejados y de confianza y eliminar aquellos que no son utilizados tan pronto sea posible.
211. Los administradores de la infraestructura inalámbrica de la organización, deben ser plenamente conscientes de las amenazas y los riesgos de seguridad de la tecnología Bluetooth y disponer de la formación y conocimientos adecuados para actuar de forma apropiada cuando se produzca cualquier incidente de seguridad en las conexiones y redes Bluetooth de la organización.
212. Es recomendable que los administradores estén al día sobre nuevas vulnerabilidades y ataques a la tecnología Bluetooth, para lo que pueden consultar la multitud de fuentes que publican este tipo de información.

7 ANEXO A. RESUMEN DE REQUISITOS DEL USO DE BLUETOOTH EN LA ORGANIZACIÓN

ID	Requisito o Recomendación de Seguridad	Medida de Seguridad ENS		Categoría / Dimensiones		
		Descripción	Código	Básica	Media	Alta
1	<p>Ámbito de uso de Bluetooth dentro de la organización:</p> <p>Uso de dispositivos corporativos y, preferiblemente, dentro del entorno de seguridad de la organización.</p> <ul style="list-style-type: none"> - Sólo podrán emplearse dispositivos externos para establecer conexiones Bluetooth con recursos de carácter público. - Sólo podrán establecerse fuera del entorno de seguridad de la organización, cuando lo justifique el principio de mínima funcionalidad y se implementen medidas de protección de las comunicaciones. 	<p>Artículo 19 Principio básico de “<i>Seguridad por defecto</i>”</p>		-	-	-
2	<p>Incorporar la tecnología Bluetooth en la Normativa que rige la organización global de la seguridad de la organización, y en concreto en la relativa al uso y explotación de sus redes inalámbricas.</p> <p>Al menos, deberá incorporarse Bluetooth en:</p> <ul style="list-style-type: none"> - La Política de Seguridad de redes inalámbricas. - Los Procedimientos correspondientes al uso de la tecnología inalámbrica. - Los Procesos de Autorización para el uso de la tecnología inalámbrica. 	<p>Medidas organizativas</p>	<p>[org.2] [org.3] [org.4]</p>	RQ ²⁵	RQ	RQ

²⁵ “RQ” representa un Requisito (requerido por el ENS). “RM” representa una Recomendación, es decir, no requerido explícitamente por el ENS, pero recomendable su implementación.

ID	Requisito o Recomendación de Seguridad	Medida de Seguridad ENS		Categoría / Dimensiones		
		Descripción	Código	Básica	Media	Alta
3	La organización deberá realizar la gestión de los riesgos relacionados con el uso de esta tecnología. Esta gestión debe realizarse por medio del análisis y tratamiento de los riesgos a los que están expuestos este tipo de comunicaciones.	Análisis y Gestión de Riesgos	Artículo 13 [op.pl.1]	RQ	RQ	RQ
4	Utilizar dispositivos Bluetooth que implementen la tecnología de <i>Secure Connections</i> (Bluetooth BR/EDR a partir de la versión 4.1, Bluetooth LE a partir de la versión 4.2).	Protección de las comunicaciones	[mp.com.2] [mp.com.3]	RM [I C A]	RQ [I C A]	NA
5	Evitar el uso del modelo de asociación de <i>pairing "Just Works"</i> , ya que no proporciona protección MITM. Dado que este es el único modelo de asociación que soportan los dispositivos sin capacidades I/O, el uso de este tipo de dispositivos debe ser evitado, si existen otros que ofrecen las mismas funciones, y soportan otros modelos de asociación (<i>comparación numérica, OOB o passkey entry</i>).	Protección de las comunicaciones	[mp.com.2] [mp.com.3]	RM [I C A]	RM [I C A]	NA
6	Si se utiliza el modelo de asociación <i>Passkey entry</i> , la <i>passkey</i> que se utilice debe ser aleatoria. No debe utilizarse una <i>passkey</i> estática en varios procesos de <i>pairing</i> , ya que eso reduce la protección MITM que proporciona este modelo de asociación.	Protección de las comunicaciones	[mp.com.2] [mp.com.3]	RM [I C A]	RM [I C A]	NA
7	Longitud de la clave de cifrado (negociada en el <i>pairing</i>) de, al menos, 112 bits. Recomendable 128 bits	Protección de las comunicaciones	[mp.com.2] [mp.com.3]	RM [I C A]	RQ [I C A]	NA
8	No emplear conexiones Bluetooth dado que no existe posibilidad de establecerlas a través de dispositivos hardware certificados conforme a lo establecido en la medida [op.pl.5].	Protección de las comunicaciones	[mp.com.2] [mp.com.3]	NA	NA	RQ [I C A]
9	Implementar mecanismos de autenticación de usuarios a través de las capas de aplicación, que cumplan con las especificaciones de autenticación recogidas en la medida [op.acc.5].	Mecanismo de Autenticación	[op.acc.5]	RQ [I C A T]	RQ [I C A T]	RQ [I C A T]

ID	Requisito o Recomendación de Seguridad	Medida de Seguridad ENS		Categoría / Dimensiones		
		Descripción	Código	Básica	Media	Alta
10	Los dispositivos Bluetooth que accedan a sistemas, servicios, recursos y/o información de la organización, deberán implementar las medidas de seguridad establecidas en sus políticas y normativas de seguridad. Los dispositivos que, además, sean susceptibles de salir de las instalaciones de la organización, y estar expuestos a un riesgo de pérdida o robo, y deberán ser especialmente protegidos.	Protección de equipos	[mp.eq.3]	RQ	RQ	RQ
11	Nunca deberá dejarse en los dispositivos la configuración por defecto. Debe realizarse una revisión minuciosa de todos los parámetros de la configuración Bluetooth, y asegurar el cumplimiento de la política de seguridad.	Configuración de Seguridad	[op.exp.2]	RQ	RQ	RQ
12	Deshabilitar las capacidades Bluetooth del dispositivo cuando no se estén utilizando.	Configuración de Seguridad	[op.exp.2]	RQ	RQ	RQ
13	Los dispositivos Bluetooth deberán estar por defecto, en modo no visible (<i>undiscoverable</i>) y sólo cambiar su configuración a modo visible (<i>discoverable</i>) cuando sea absolutamente necesario, para conectarse con otros dispositivos.	Configuración de Seguridad	[op.exp.2]	RQ	RQ	RQ
14	El nombre del dispositivo no debe ser descriptivo (no debe revelar ninguna característica relacionada con el dispositivo, el usuario, la organización, etc.).	Configuración de Seguridad	[op.exp.2]	RQ	RQ	RQ
15	El nivel de potencia de los dispositivos debe estar ajustado al mínimo necesario, de forma que las transmisiones Bluetooth permanezcan dentro del perímetro de seguridad de la organización.	Configuración de Seguridad	[op.exp.2]	RM	RM	RM
16	Cuando sea posible, sólo los servicios y perfiles Bluetooth que sean absolutamente necesarios, deberán estar habilitados.	Configuración de Seguridad	[op.exp.2]	RM	RM	RM
17	Configurar contraseñas de acceso en los dispositivos Bluetooth portátiles.	Configuración de Seguridad	[op.exp.2]	RQ	RQ	RQ

ID	Requisito o Recomendación de Seguridad	Medida de Seguridad ENS		Categoría / Dimensiones		
		Descripción	Código	Básica	Media	Alta
18	Instalar software de antivirus en los dispositivos Bluetooth donde esto sea posible.	Configuración de Seguridad	[op.exp.2]	RM	RM	RM
19	Actualizar regularmente el software Bluetooth e instalar las actualizaciones y parches del firmware y sistema operativo en los dispositivos.	Configuración de Seguridad	[op.exp.2]	RQ	RQ	RQ
20	Inventario completo de todos los dispositivos Bluetooth de la organización recogiendo, al menos, sus direcciones (BR_ADDR) y los servicios ofrecidos a través de la conexión Bluetooth.	Gestión de la Configuración	[op.exp.3]	RQ	RQ	RQ
21	Configuración Bluetooth incluida en los procedimientos de Gestión de la Configuración de los dispositivos y equipos de la organización.	Gestión de la Configuración	[op.exp.3]	NA	RQ	RQ
22	Se deben implementar mecanismos adicionales a Bluetooth, que proporcionen registros de actividad que, al menos, contengan: Quién realiza la conexión (dispositivo y usuario), cuándo se realiza y sobre qué recurso, información o servicio. Registro tanto de conexiones exitosas, como fallidas.	Registro de Actividad	[op.exp.8]	RQ	RQ	RQ
23	Se deberá realizar una revisión informal de los registros de actividad.	Registro de Actividad	[op.exp.8]	NA	RQ [T]	RQ [T]
24	Se enviarán los registros en tiempo real a un servidor centralizado para su almacenamiento, correlación y explotación automática. Estos registros deberán ser protegidos de forma que no puedan ser modificados ni eliminados por personal no autorizado.	Registro de Actividad Protección de los registros de actividad	[op.exp.8] [op.exp.10]	NA	NA	RQ [T]
25	Designar un responsable de mantenimiento, que realice el seguimiento del avance de la tecnología Bluetooth, de las amenazas y vulnerabilidades que vayan descubriéndose, y de los boletines de seguridad de los fabricantes.	Mantenimiento	[op.exp.4]	RM	RM	RM

ID	Requisito o Recomendación de Seguridad	Medida de Seguridad ENS		Categoría / Dimensiones		
		Descripción	Código	Básica	Media	Alta
26	Incluir Bluetooth en las Auditorías de seguridad periódicas que la organización realice sobre sus sistemas e infraestructura, para identificar el uso y existencia de dispositivos Bluetooth que incumplan con las políticas y normativa de seguridad establecidas.	Auditorías de Seguridad	[op.mon]	RQ	RQ	RQ
27	Revisar de forma periódica la lista de dispositivos emparejados y de confianza y eliminar aquellos que no son utilizados, tan pronto sea posible.	Mantenimiento	[op.exp.4]	RM	RM	RM
28	Programas regulares de concienciación a los usuarios acerca de su responsabilidad en el uso de la tecnología Bluetooth.	Concienciación	[mp.per.3]	RQ	RQ	RQ
29	Llevar a cabo el proceso de <i>pairing</i> (emparejamiento entre dispositivos) con la menor frecuencia posible, y siempre en áreas seguras.	Concienciación	[mp.per.3]	RM	RM	RM
30	Establecer conexiones solo con otros dispositivos de confianza. No aceptar solicitudes de conexión, ficheros o cualquier otro elemento de orígenes desconocidos.	Concienciación	[mp.per.3]	RM	RM	RM
31	Cuando un dispositivo haya sido robado, perdido o comprometido, proceder cuanto antes, a borrarlo de la lista de confianza del resto de sus dispositivos Bluetooth	Concienciación	[mp.per.3]	RM	RM	RM
32	Los administradores de la infraestructura inalámbrica deberán estar correctamente formados y al día de las amenazas y vulnerabilidades de la tecnología Bluetooth.	Formación	[mp.per.4]	RQ	RQ	RQ

Tabla 8. Requisitos del ENS aplicables al uso de Bluetooth en la organización.

8 ANEXO B. EJEMPLO DE CONFIGURACIÓN BLUETOOTH EN UN EQUIPO WINDOWS

A) Versión Bluetooth del dispositivo

El método para averiguar la versión Bluetooth que utiliza un dispositivo depende del tipo de dispositivo y de su firmware o de su sistema operativo. Se recomienda consultar la página web del fabricante para conocer el procedimiento para averiguarla.

1. Acceder al Administrador de dispositivos (desde el Panel de Control hacer clic en “Administrador de Dispositivos” o ejecutar “*devmgmt.msc*” desde una ventana de ejecución de Windows).

2. Buscar de entre la lista de dispositivos el adaptador Bluetooth. Su nombre varía dependiendo del hardware del equipo, pero suele llamarse algo similar a “Radio Bluetooth”. Dentro de la lista del adaptador, el ítem a revisar es el que no contenga la palabra “Enumerador”. En el caso de este ejemplo es el que se denomina “Intel (R) Wireless Bluetooth”:

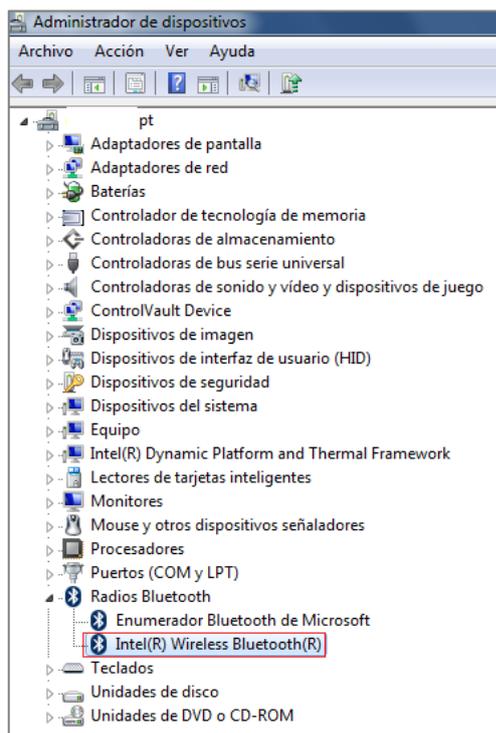
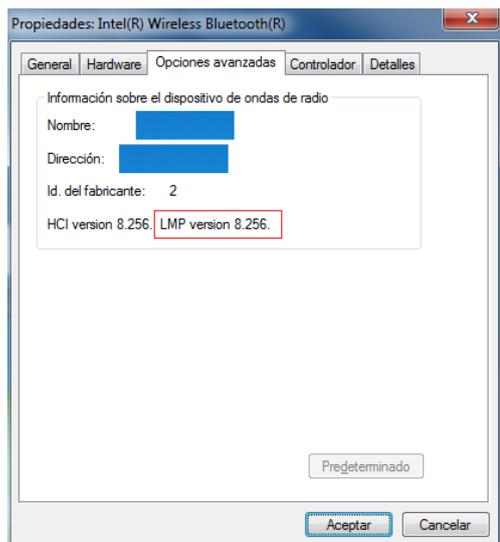


Figura 19. Ejemplo de Adaptador Bluetooth en un equipo Windows 7.

3. El adaptador puede mostrar directamente la versión de Bluetooth o no. En caso negativo, hacer clic con el botón derecho del ratón en el adaptador, seleccionar “Propiedades” e ir a la pestaña de “Opciones avanzadas”. Localizar en la ventana la versión del Protocolo LMP (*Link Manager Protocol*) ya que esta se corresponde con una determinada versión de Bluetooth:



LMP	Versión Bluetooth
0.x	Bluetooth 1.0b
1.x	Bluetooth 1.1
2.x	Bluetooth 1.2
3.x	Bluetooth 2.0 + EDR
4.x	Bluetooth 2.1 + EDR
5.x	Bluetooth 3.0 + HS
6.x	Bluetooth 4.0
7.x	Bluetooth 4.1
8.x	Bluetooth 4.2
9.x	Bluetooth 5

Figura 20. Ejemplo de versión Bluetooth empleada en un equipo Windows 7.

B) Gestión de la configuración Bluetooth del dispositivo

La configuración Bluetooth es propia de cada tipo de dispositivo. A continuación se muestra un ejemplo de la gestión de la configuración Bluetooth para un equipo Windows 7 Enterprise.

Encendido y Apagado de Bluetooth

Para desactivar Bluetooth puede haber varias opciones:

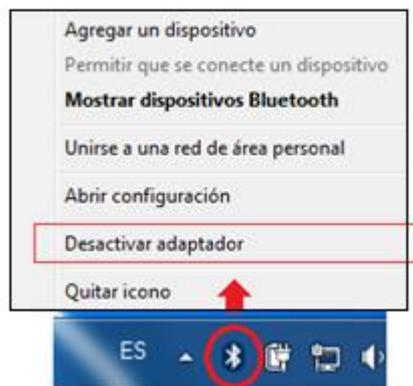
- Algunos equipos disponen de un interruptor físico en el equipo que proporciona el apagado o encendido de la capacidad Bluetooth. La siguiente figura muestra un ejemplo.



Figura 21. Ejemplo de interruptor físico Bluetooth.

- Activar o desactivar el adaptador Bluetooth a través de software. Esta opción se despliega al hacer clic en el icono de Bluetooth de la bandeja (1) o desde la ventana de Configuración de Bluetooth (2). Esta es la opción recomendada por Microsoft en caso de que el equipo disponga de ella. Si el equipo dispone de esta opción y también del interruptor físico, no se deben usar a la vez (desactivar de una forma y activar de otra).

(1)



(2)

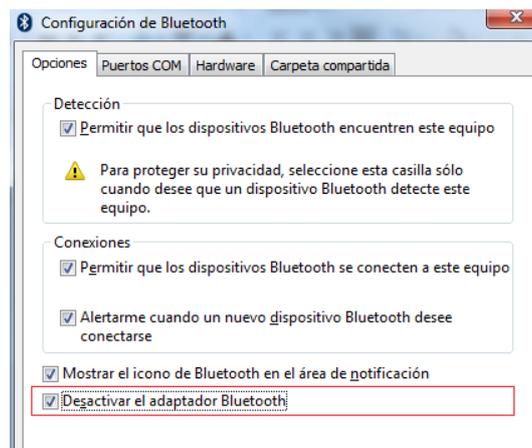


Figura 22. Activar / Desactivar el adaptador Bluetooth a través de software en un equipo Windows 7.

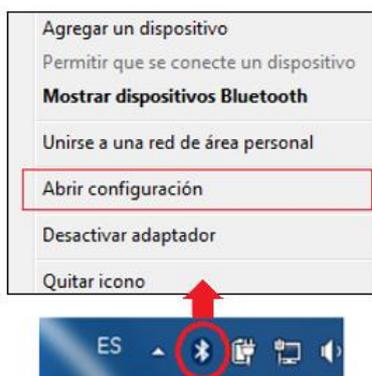
- Existe una tercera opción, que es la de activar o desactivar el adaptador Bluetooth a través del Administrador de Dispositivos, pero esta opción no está recomendada por Microsoft.

Estas opciones representan el [Requisito 12 de la tabla del Anexo A].

Opciones de Configuración Bluetooth

Existen varias formas para acceder a la configuración Bluetooth del equipo. Una de ellas es hacer clic en el icono Bluetooth de la bandeja y seleccionar la opción “Abrir configuración” (1). Otra es hacer la búsqueda de Bluetooth en la ventana de inicio de Windows (2).

(1)



(2)

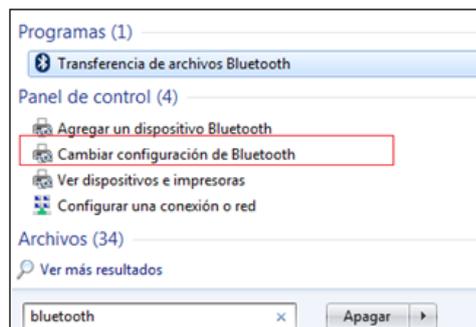


Figura 23. Acceso a la configuración Bluetooth en un equipo Windows 7.

La ventana de configuración Bluetooth muestra las opciones disponibles.

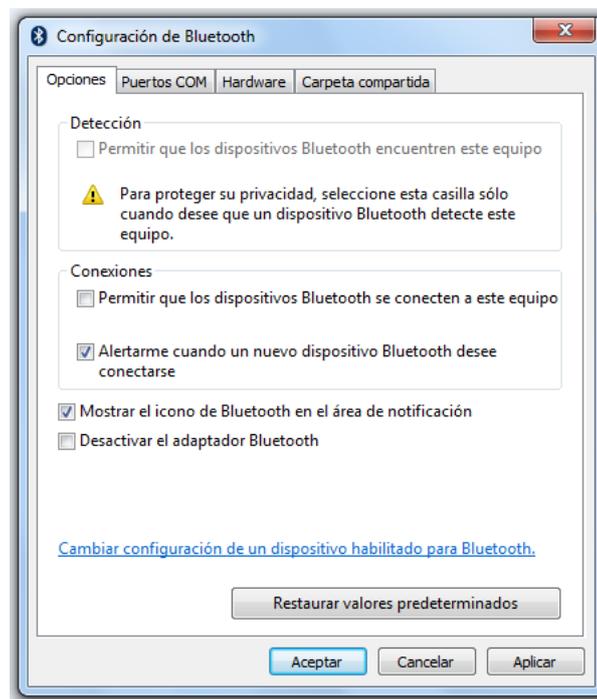


Figura 24. Ventana de opciones de configuración Bluetooth en un equipo Windows 7.

La opción de “Permitir que los dispositivos Bluetooth encuentren este equipo” es lo que hace que el equipo esté en modo visible (*discoverable*) o en modo no visible u oculto (*non discoverable*). Esta opción es la que se activa para permitir que el equipo sea detectable para otros dispositivos Bluetooth. Si se desactiva esta casilla, el equipo podrá detectar otros dispositivos Bluetooth que se encuentren en modo de detección pero los dispositivos no podrán detectar el equipo.

La opción de “Permitir que los dispositivos Bluetooth se conecten a este equipo”, permite agregar dispositivos Bluetooth al equipo, es decir, realizar con ellos el proceso de emparejamiento (*pairing*) para poder establecer una conexión.

Estas dos opciones anteriores representan el [Requisito 13 de la tabla del Anexo A].

La opción de “Alertarme cuando un nuevo dispositivo Bluetooth desee conectarse”, se utiliza para recibir una notificación cuando un dispositivo Bluetooth esté intentando conectarse al equipo.

La opción “Mostrar el icono de Bluetooth en el área de notificación” permite visualizar el icono de Bluetooth en la bandeja del equipo.

C) Conexión de dispositivos Bluetooth

A continuación, se muestra un ejemplo del establecimiento de la conexión Bluetooth entre un equipo Windows 7 y dispositivo iPhone 6.

El procedimiento para agregar en el equipo Windows el dispositivo Bluetooth y establecer la conexión con él consta de tres pasos:

1. Detección del dispositivo.

El dispositivo (iPhone) debe estar con Bluetooth activado y en modo visible.

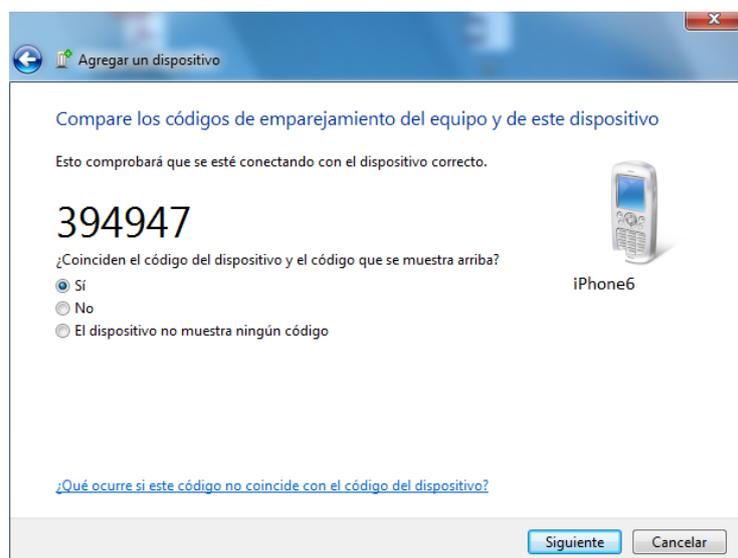
En el equipo Windows se debe hacer clic en el icono Bluetooth de la bandeja y seleccionar "Agregar un dispositivo". Esto realizará una búsqueda y mostrará todos los dispositivos Bluetooth situados dentro del alcance del equipo.

2. Emparejar y establecer un enlace seguro entre el equipo y el dispositivo.

Cuando aparece el dispositivo Bluetooth (iPhone) en la ventana de "Agregar un dispositivo", seleccionar su icono y hacer clic en Siguiente

Esto inicia el proceso de *pairing* (emparejamiento) una de cuyas etapas es la autenticación de dispositivos. Esta autenticación, en este caso, se realiza verificando un código de 6 dígitos generado en ambos dispositivos (modelo de asociación de *pairing* de comparación numérica).

En el equipo:



En el iPhone:



Figura 25. Ventana de autenticación de dispositivos durante el emparejamiento entre un equipo Windows 7 y un iPhone 6.

Una vez están emparejados los dispositivos en el iPhone aparece el equipo Windows dentro de la lista de "mis dispositivos Bluetooth" en estado conectado. En el equipo Windows aparece el dispositivo iPhone en la lista de Dispositivos Bluetooth, a la cual se accede haciendo clic en el icono Bluetooth de la bandeja, y seleccionando la opción de "Mostrar dispositivos Bluetooth":



Figura 26. Dispositivo iPhone emparejado con el equipo Windows 7.

3. Conectar el equipo Windows al servicio del dispositivo Bluetooth.

Para acceder a los servicios ofrecidos por el dispositivo, se realizará doble clic en el icono del dispositivo agregado para abrir la ventana Servicios correspondiente. Esto muestra lo que se puede hacer con el dispositivo Bluetooth agregado a partir de los servicios que este ofrece. En este ejemplo, es la reproducción de música.



Figura 27. Servicios ofrecidos por el dispositivo iPhone 6.

Una vez que el dispositivo está emparejado con el ordenador, podemos desconectarlo cuando la conexión no se esté utilizando y volver a conectarlo cuando se quiera usar sin repetir de nuevo el proceso de emparejamiento. Para Desemparejarlo debemos utilizar la opción de “quitar dispositivo” que lo desagrega de la lista de dispositivos del equipo. Esto representa el [Requisito 27 de la Tabla del Anexo A].

Cuando queramos volver a conectarnos al dispositivo se deberá realizar de nuevo el proceso de emparejamiento y por lo tanto de autenticación.

D) Servicio de transferencia de archivos a través de Bluetooth de Microsoft

Microsoft Windows dispone de un servicio de transferencia de archivos entre dispositivos compatibles con Bluetooth habilitado. Este servicio hace uso de los perfiles de Bluetooth BIP (*Basic Imaging Profile*) y OPP (*Object Push Profile*)²⁶.

Esta transferencia se puede llevar a cabo de varias maneras. A continuación se muestra un ejemplo de transferencia de archivos entre dos equipos Windows: Windows 7 y Windows 10.

a. En el equipo Windows 7 desde el menú de inicio, seleccionar “Transferencia de archivos Bluetooth”, seleccionar “Enviar archivos”, seleccionar el equipo con Bluetooth habilitado, seleccionar el archivo a enviar y hacer clic en “siguiente”.

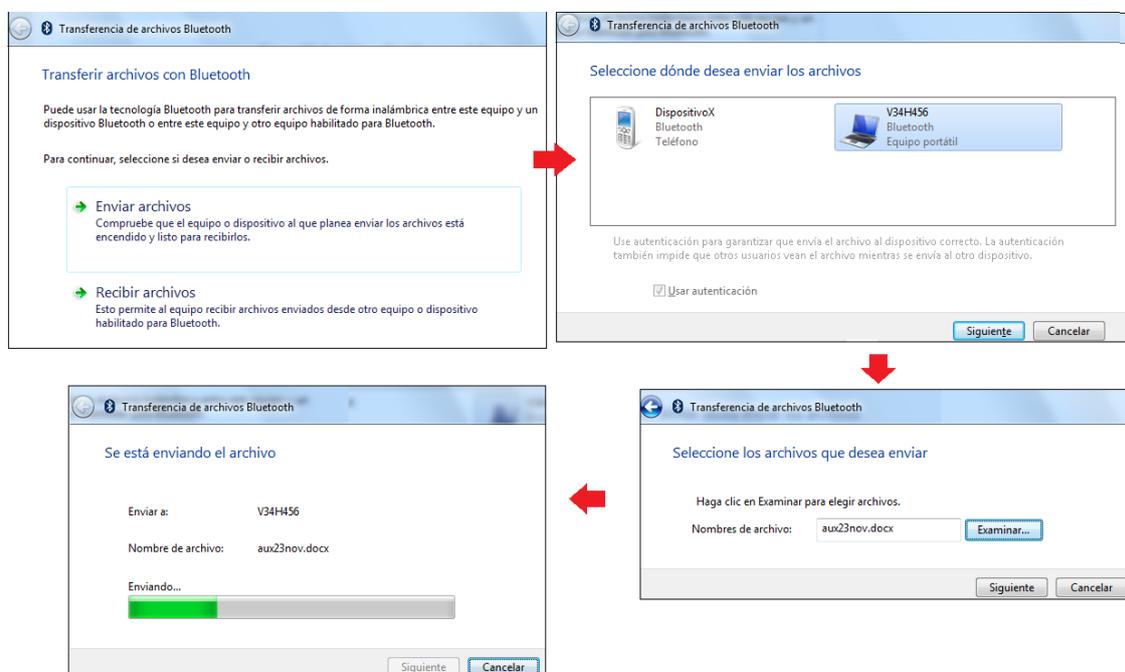


Figura 28. Ejemplo de transferencia de archivos por Bluetooth desde un equipo Windows 7 empleando la opción de “Transferencia de archivos Bluetooth”.

b. Otra opción es seleccionar el archivo, hacer clic con el botón derecho del ratón y seleccionar la opción de “Enviar a Bluetooth”. En este caso se abre el asistente para enviar archivos a un dispositivo Bluetooth que funciona de forma similar a la opción anterior.

²⁶ OPP (Object Push Profile) es un perfil Bluetooth cuya finalidad es el envío de “objetos” genéricos. Sigue el modelo “push”, ya que es el emisor el que inicia siempre la comunicación. BIP (Basic Imaging Profile) es un perfil Bluetooth diseñado para enviar imágenes, e incluye capacidades de ajuste de tamaño y conversión de formatos.

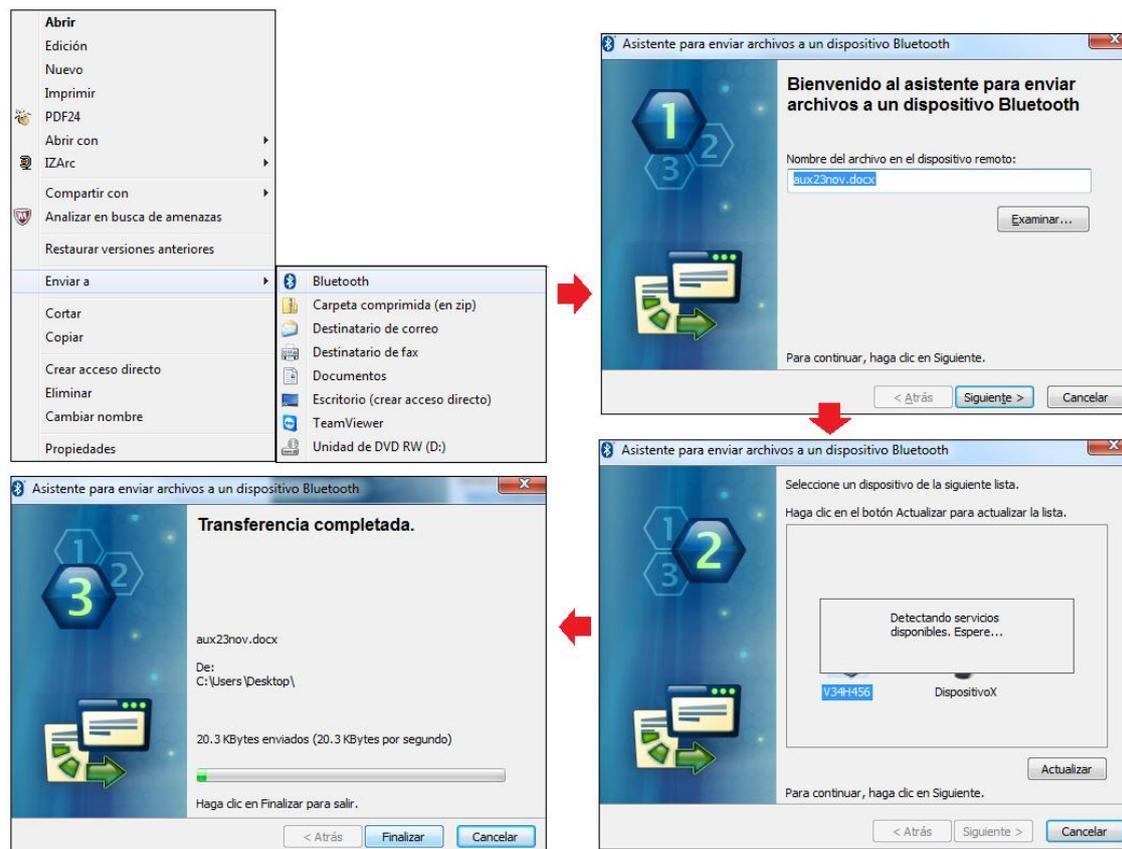


Figura 29. Ejemplo de transferencia de archivos por Bluetooth desde un equipo Windows 7 empleando el “Asistente para enviar archivos a un dispositivo Bluetooth”.

En ambos casos, el equipo Windows 10 debe estar a la espera de una conexión Bluetooth para recibir archivos. Para ello, desde el panel de Configuración Windows se debe seleccionar “Dispositivos Bluetooth”, clic en la opción de “Enviar o recibir archivos a través de Bluetooth” y seleccionar “Recibir archivos”.

El servicio de transferencia de archivos a través de Bluetooth se puede utilizar entre dispositivos previamente emparejados o no. Si no están previamente emparejados, al intentar transferir archivos de uno al otro se iniciará el emparejamiento y la consiguiente autenticación entre los dispositivos.

E) Servicio de Carpetas compartidas de Microsoft

Microsoft Windows proporciona un servicio para compartir archivos y carpetas locales del equipo Windows con otros dispositivos Bluetooth. La carpeta compartida se utiliza como la carpeta raíz para la transferencia de archivos a través de FTP y como carpeta predeterminada para recibir archivos mediante OPP y BIP.

Para acceder a la configuración de la carpeta compartida, se debe abrir la configuración de Bluetooth e ir a la pestaña de “Carpeta Compartida”:

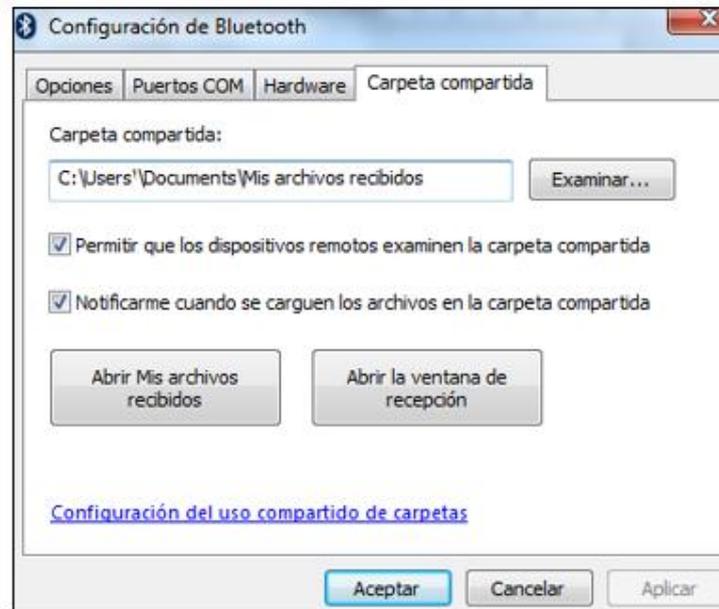


Figura 30. Configuración de carpetas compartidas en Windows 7.

Para habilitar el uso compartido de carpetas se debe activar la opción “Permitir que los dispositivos remotos examinen la carpeta compartida” que será la carpeta local seleccionada a través de “Examinar”.

9 GLOSARIO DE TÉRMINOS

Ad Hoc. Es un tipo de conexión que permite a dispositivos que se encuentran en la misma área física, establecer conexiones entre ellos de forma sencilla y sin necesidad de infraestructura (como podría ser un punto de acceso o una estación base).

Autenticación. Es el proceso de confirmar que algo (o alguien) es quien dice ser. A la parte que se identifica se le llama *probador*. A la parte que verifica la identidad se la llama *verificador*. Cuando los dos participantes en una comunicación se autentican entre sí, se llama autenticación mutua.

Autenticación de origen (*data origin Authentication*). Propiedad que permite al receptor verificar que el mensaje no ha sido alterado en el tránsito (integridad de datos) y que ha sido originado del emisor legítimo (autenticidad).

Autenticidad. Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.

CCM (Counter with CBC-MAC). Es un modo de operación de un cifrador de bloque, normalmente AES (AES-CCM). Combina dos técnicas: CTR para la protección de confidencialidad y CBC-MAC para la protección de la integridad y autenticidad.

Confidencialidad. Propiedad o característica consistente en que la información ni se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.

Disponibilidad. Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.

Eavesdropping. El *eavesdropping* o escucha pasiva, es un tipo de ataque a las comunicaciones inalámbricas, mediante el cual un individuo no autorizado, mediante el uso de un receptor adecuado, captura la comunicación con fines malintencionados.

Integridad. Propiedad o característica consistente en que la información no ha sido alterada de manera no autorizada.

MITM (Man-In-The-Middle). El ataque de “Hombre en el medio” ocurre cuando un usuario quiere conectar dos dispositivos, pero en lugar de conectar directamente uno con el otro, estos sin saberlo se están conectando a un tercero (dispositivo ilícito) que engañosamente representa el papel del dispositivo con el que ellos quieren emparejarse. El tercer dispositivo retransmite la información entre los dos dispositivos haciéndoles creer que se están comunicando directamente entre ellos.

Nonces. Es un valor arbitrario de un solo uso utilizado en criptografía. Normalmente es un número aleatorio o pseudo-aleatorio que se utiliza en los protocolos de autenticación para evitar el empleo de paquetes antiguos de la comunicación en ataques de reenvío (*replay attacks*). También se utilizan como vectores de inicialización (IV) en funciones hash criptográficas.

Pairing. El proceso de *pairing* o emparejamiento es el que tiene lugar tras el descubrimiento de los dispositivos y para el establecimiento de la conexión. Durante este proceso se lleva a cabo la autenticación y la generación y/o intercambio de las claves de cifrado de la conexión.

Piconet. Una red Bluetooth creada sobre la base de conexiones Ad Hoc que incluye dos o más dispositivos.

Rango o Alcance. La máxima distancia posible a la que se puede establecer una comunicación inalámbrica.

Scatternet. Una cadena de *piconets* creadas a base de dispositivos que actúan como esclavos en una piconet y como maestros de otras *piconet* simultáneamente.

Solicitante (claimant). Es el dispositivo Bluetooth que intenta probar su identidad a un verificador (*verifier*) durante el proceso de conexión Bluetooth.

Verificador (verifier). Es el dispositivo Bluetooth que valida la identidad del solicitante (*claimant*) durante el proceso de conexión Bluetooth.

WLAN (Wireless Local Area Network). Red de Área Local inalámbrica, es un grupo de puntos de acceso inalámbricos (AP) y su infraestructura asociada dentro de un área geográfica limitada, como un edificio o un campus universitario que permite el establecimiento de comunicaciones a través de radio.

WPAN (Wireless Personal Area Network). Red de Área Personal inalámbrica, es una red inalámbrica de pequeña escala que no requiere infraestructura y opera en el corto alcance. Un uso típico de una WPAN es para la conexión de unos pocos dispositivos en una habitación evitando el uso de cableado.

10 REFERENCIAS

- Real Decreto 3/2010, de 8 de enero, modificado a su vez por el Real Decreto 951/2015, de 23 de octubre, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Guía CCN-STIC-808 - Verificación del cumplimiento de las medidas en el ENS. Junio. 2017.
- Guía CCN-STIC-807 - Criptografía de empleo en el Esquema Nacional de Seguridad Abril 2017.
- CCN-STIC-418: Guía de Seguridad de las TIC. Seguridad en Bluetooth. Enero 2009.
- CCN-STIC-804: Guía de Implantación Esquema Nacional de Seguridad. Junio 2017.
- Draft SP800-121 Rev2 (Draft): Guide to Bluetooth Security. National Institute of Standards and Technology (NIST). Dic 2016.
- Bluetooth Technology Website [www.bluetooth.com].
- RFC 3748 “3610 Counter with CBC-MAC (CCM)” <https://tools.ietf.org/html/rfc3610>