



COORDENADAS 126.

Año XXXVIII | N°126 | Agosto-Septiembre/2026



artículo técnico

8 Trilogía de agentes de IA en la era GPT-5: guía práctica del prototipo al impacto (III)

3 editorial
**La postura del COPITEC
frente a la Resolución 57
de ENACOM**

6 noticias
**Nuevos matriculados...
¡Bienvenidos!**

26 artículo técnico
**Ecuación de Friis
en Radioenlaces**

NOSOTROS



Autoridades

Presidente:

Ing. Enrique Luciano Larrieu-Let

Vicepresidente:

Ing. Roberto Osvaldo Mayer

Secretario:

Ing. Luis Alberto Chavarría

Tesorero:

Téc. Javier Bernardo Gratz

Consejeros titulares:

Ing. Juan Manuel Beltrán

Ing. Luis Alberto Bibini

Ing. Fabián Salvador Piscitelli

Consejeros suplentes:

Ing. Hernán Martín Anté

Ing. Marcelo Alberto Crivelli

Ing. Martín Carlos Letier

Ing. Norberto Jesús Solís

Téc. Juan Antonio Vrana

Comisión revisora de cuentas:

Ing. Eduardo Manuel Caparrós

Ing. Pablo Bernabé Ramón Crivello

Téc. Martín Alejandro Durand



COORDENADAS 126.

Es la única publicación oficial



COPITEC

Consejo Profesional de Ingeniería de
Telecomunicaciones, Electrónica y Computación

Contenidos

▶	editorial	3	La postura del COPITEC frente a la Resolución 57 de ENACOM
▶	noticia	6	Nuevos matriculados... ¡Bienvenidos!
▶	artículo técnico	8	Trilogía de agentes de IA en la era GPT-5: guía práctica del prototipo al impacto (III)
▶	libro	16	Capítulo 4: Redes PAN basadas en Bluetooth
▶	artículo técnico	26	Ecuación de Friis en Radioenlaces

COPITEC | Perú 562, CABA, Argentina | www.copitec.org.ar

Contacto: secretaria@copitec.org.ar

matricula@copitec.org.ar | consultas@copitec.org.ar

Realización integral Revista Coordinadas:

COPITEC

1. COORDENADAS es una publicación de EL CONSEJO, según registro de propiedad intelectual n°1.904.071

2. Los artículos técnicos y opiniones vertidas son responsabilidad de sus respectivos autores y no reflejan necesariamente la opinión de las autoridades de EL CONSEJO.

3. La propiedad intelectual de la publicación coordinadas, será exclusivamente de EL CONSEJO y se permite su producción total o parcial citando a la fuente

La postura del COPITEC frente a la Resolución 57 de ENACOM



Enrique Larrieu-Let
Presidente COPITEC

Resguardar la infraestructura crítica nacional y la soberanía tecnológica

Desde el comienzo de esta gestión del COPITEC, se llevaron a cabo varios intentos de acercamiento al ENACOM, tanto de manera informal como formal, para ofrecernos como asesores y colaboradores y poner a disposición nuestra estructura profesional en la materia y ser considerados como elemento de consulta permanente en temas de incumbencia en común con el ENACOM, y de esa manera tener la posibilidad de brindar nuestras propuestas a fin de optimizar trámites y actividades que colaboren en mejorar la gestión de dicho ente y promoviendo, que en un organismo público nacional, **se tomen decisiones que beneficien a una infraestructura estratégica para la seguridad nacional y la soberanía tecnológica como son las Telecomunicaciones.**

El 26 de febrero de 2026 fuimos sorprendidos por la publicación de la **Resolución 57/2026** - ENACOM (RESOL-2026-57-APN-ENACOM#JGM), y nos vimos en la urgente necesidad de advertir a las autoridades del ente, a modo de aporte del ámbito profesional de la ingeniería, por considerar que dicha normativa **introduce cambios que podrían afectar la transparencia, incrementar regulaciones y costos y debilitar el control técnico en un área crítica y estratégica** como ya se mencionó.

Consideramos que cualquier modificación en los mecanismos de control del Estado, debe fortalecer, y no debilitar las garantías técnicas existentes, que puedan afectar la seguridad de la sociedad, desprotegiendo a los ciudadanos al eliminar de ciertos trámites la participación de los **profesionales de la ingeniería**

matriculados por el COPITEC, quienes *durante más de cuatro décadas han garantizado con su responsabilidad técnica los procesos de homologación de equipos.*

CRONOLOGÍA de los acontecimientos

- » 2023_Octubre – Inicio nueva gestión y autoridades en COPITEC
- » 2024_Enero - Intervención de ENACOM por 180 días (Decreto 89/2024)
- » 2024 (marzo- agosto) intentos informales de acercamiento por parte del COPITEC.
- » 2024_Julio – Primera Prórroga de la intervención hasta el 7 de julio de 2025 (Decreto 675/2024)
- » **2024_Septiembre - PD-2024-98667380-APN-DGDYD#JGM: COPITEC realiza una solicitud formal de pedido de audiencia-Resultado ignorado hasta la fecha.**
- » 2025_Julio – Segunda Prórroga de la intervención por seis meses hasta el 4/1/2026. (Decreto 448/2025)
- » 2026_Enero – Tercera Prórroga de la intervención por un año hasta el 4/1/2027. (Decreto 938/2025)
- » 2026_26 de Febrero - RESOL-2026-57-APN-ENACOM#JGM: publicación en el Boletín Oficial.
- » **2026_Marzo – COPITEC INTERPONE RECLAMO ADMINISTRATIVO IMPROPIO EN LOS TÉRMINOS DEL ART. 24 INC. A) DE LA LEY DE PROCEDIMIENTO ADMINISTRATIVO N° 19.549.**
- » 2026_Mayo_20 – ENACOM rechaza el Reclamo Administrativo mediante la Resolución 362/2026.
- » **2026_Julio - COPITEC recurre a la instancia judicial y promueve una DEMANDA CONTENCIOSO ADMINISTRATIVA DE NULIDAD, CON PEDIDO DE MEDIDA CAUTELAR PARA LA SUSPENSIÓN DE LOS EFECTOS DE LA RESOLUCIÓN 57/2026.**
- » 2026_Agosto_28 – ENACOM publica en el Boletín Oficial la Resolución N° 843/2026, prorrogando la entrada en vigor del nuevo sistema de homologación de equipos de telecomunicaciones del 1° de septiembre al 1° de diciembre de 2026, reconociendo en sus propios considerandos: *“...se ha verificado que no se encuentran dadas las condiciones indispensables para su correcta ejecución dentro de los plazos originalmente establecidos.”*

introduce cambios que podrían afectar la transparencia, incrementar regulaciones y costos y debilitar el control técnico en un área crítica y estratégica

EL COPITEC celebra esta última decisión de ENACOM ya que permite la posibilidad de revisar la implementación de la normativa y de ser convocados a colaborar.

La *acción judicial de NULIDAD iniciada por COPITEC ante la Justicia Federal, necesaria para obtener tutela efectiva de los derechos de los matriculados, continúa su curso. Confiamos en que la justicia, como poder independiente, comprenderá la importancia del tema y los riesgos de su impacto para la sociedad, y por lo tanto resolverá la medida cautelar solicitada con la urgencia que el caso requiere.*

La importancia de la cooperación entre instituciones

Entendemos que estas **situaciones no se presentarían** si se destinaran recursos y tiempo a vincular y potenciar las instituciones **mediante un trabajo mancomunado** entre las mismas.

Consideramos que la conjunción de varios puntos de vista, proporcionados por **profesionales matriculados con incumbencia** en el tema, que sugieran mejoras a las iniciativas del Estado, puede permitir al mismo brindar **mejores servicios y protección** a la infraestructura y patrimonio de comunicaciones, como lo es el espectro radioeléctrico de jurisdicción nacional.

Una gestión se compone de **estrategias** que marcan rumbos y **tácticas** que conducen a cumplir objetivos.

El **COPITEC** está siempre a disposición de los estamentos de estado para sugerirle propuestas, en ambos aspectos, en términos de **calidad y seguridad**, garantizando que **se cumplan estándares** en la materia, **para el beneficio de toda la sociedad**.

*Consideramos que la **conducción estratégica de un organismo público nacional de carácter técnico, en su directorio, debe contener profesionales ingenieros matriculados en la jurisdicción nacional, sin desmedro de otras profesiones también necesarias, y asimismo para la conducción operativa y la toma de decisiones tácticas debe incorporar en las áreas técnicas al mismo tipo de profesionales especialistas.***

Por lo expresado

Es necesario que existan ingenieros matriculados en la jurisdicción nacional para integrar los cuadros de máximo nivel de conducción estratégica de organismos públicos nacionales vinculados a temas tecnológicos y de infraestructuras críticas.

Nuevos matriculados...

¡Bienvenidos!

Damos la bienvenida a nuestros nuevos y nuevas matriculadas. Celebramos su llegada a nuestra institución.

INGENIEROS

MATR.	APELLIDO Y NOMBRE	TITULO	ESTABLECIMIENTO EDUCATIVO
I07015	CAMURATI SEBASTIÁN ANÍBAL	ELECTRÓNICO	UBA
I07016	FAUST OMAR ALEJANDRO	BIOINGENIERO	UNER
I07017	MONTENEGRO GUILLERMO AGUEDO	ELECTRÓNICO	UBA
I07018	ESCOBAR FERNANDO GABRIEL	ELECTRÓNICO	UdeMM
I07019	AMARO MÓNACO NICOLÁS	ELECTRÓNICO	UTN
I07020	BASGALL MARÍA DEL ROSARIO	BIOINGENIERA	UNER
I07021	FERNÁNDEZ MATÍAS AGUSTÍN	ELECTRÓNICO	UNLP
I07022	NEME JOSÉ MAXIMILIANO	BIOINGENIERO	UNER
I07023	CORBALÁN MAXIMILIANO ADOLFO	BIOINGENIERO	UNER
I07024	PASZTOR MATÍAS	ELECTRÓNICO	UBA
I07025	MARTÍNEZ ADRIANA SILVIA	EN SISTEMAS DE INFORMACIÓN	UTN

LICENCIADOS

MATR.	APELLIDO Y NOMBRE	TITULO	ESTABLECIMIENTO EDUCATIVO
L00457	ROMEO DIEGO MARTÍN	EN SISTEMAS	UK
L00458	DI CARLO JAVIER ROBERTO	EN INFORMÁTICA	UP





CONSEJO PROFESIONAL DE INGENIERÍA DE TELECOMUNICACIONES, ELECTRÓNICA Y COMPUTACIÓN

Bioingeniería, informática, higiene y seguridad,
y otras actividades afines.

TÉCNICOS

MATR.	APELLIDO Y NOMBRE	TÍTULO	ESTABLECIMIENTO EDUCATIVO
T03704	MENDOZA CASTILLO AARÓN B.	ELECTRÓNICO	ET N°1
T03705	RIZZO OSVALDO LEANDRO	EN COMPUTACIÓN	ET N° 37
T03706	CASOLINO EMANUEL GASTÓN	ELECTRÓNICO	EEST N° 9
T03707	MOYANO URIEL ALEJANDRO	EN ELECTRÓNICA	EEST N° 9
T03708	ARAGÓN ALEJO DANIEL	EN ELECTRÓNICA	EEST N° 8
T03709	SERVIÁN ZOTELO DORA MARILÍN	SUP EN HIG. Y SEG. TRABAJO	ISFT N° 184
T03710	GALLO ÓSCAR ALFREDO	ELECTRÓNICO	ET N°1
T03711	MORÁN GONZALO RODOLFO	ELECTRO OR. ELECT. IND.	EET N° 17
T03712	DE FEO ALEJANDRO GUSTAVO	EN ELECTRÓNICA	ENET N° 25
T03713	MARTÍNEZ FERNANDO GABRIEL	EN ELECTRÓNICA	ESCUELA TEC. PHILIPS ARGENTINA
T03714	LÓPEZ HUGUETTI GASTÓN A.	EN ELECTRÓNICA	INSTITUTO SAN LEONARDO MURIALDO
T03715	SORIANO MARTÍN GABRIEL	EN ELECTRÓNICA	EEST N°8
T03716	JALLE EMANUEL	EN ELECTRÓNICA	ESCUELA PIO IX
T03717	MURÚA NAZARENO NICOLÁS	EN ELECTRÓNICA	INSTITUTO SAN JOSE
T03718	GJINOVICH IGNACIO JAVIER	EN ELECTRÓNICA OR. TELEC.	INSTITUTO LUIS A HUERGO
T03719	PALACIO MARCOS DAMIÁN	EN ELECTRÓNICA	EET N°5
T03720	GUTIÉRREZ ALBERTO RICARDO	EN ELECTRÓNICA	COLEGIO PIO IX
T03721	WILSON LUCAS MAXIMILIANO	EN ELECTRÓNICA	INSTITUTO LUIS A HUERGO
T03722	SALINA VARGAS LUISA BELÉN	ELECTRÓNICO	ET N° 12
T03723	CORRALES RODRIGO	ELECTRÓNICO	ET N° 12
T03724	COSTENARO HORACIO GABRIEL	ELECTRÓNICO	ET N° 28
T03725	GARCÍA MARTÍN EZEQUIEL S.	EN ELECTRÓNICA	EET N° 28
T03726	ESCOBAR LEIVA LUCAS MARIANO	EN ELECTRÓNICA	EET N° 17
T03727	PITASHNY VALENTÍN IGNACIO	EN ELECTRÓNICA	ESCUELA ORT
T03728	LOBOS SEBASTIÁN RAÚL	EN ELECTRÓNICA	ENET N° 28
T03729	CÁCERES MATÍAS LIONEL	EN ELECTRÓNICA	ET N° 1
T03730	MONTERO IVÁN GUSTAVO	EN ELECTRÓNICA	ENET N° 28
T03731	REDONDO NICOLÁS	EN ELECTRÓNICA	ENET N° 28
T03732	FERRONI ROLANDO LUIS	EN ELECTRÓNICA	ENET N° 28
T03733	ALBARELLOS BRUNO MARTÍN	ELECTRÓNICO	ESCUELA CRISTIANA EVANGELICA ARG.
T03734	COLOMBO FEDERICO SEBASTIÁN	EN ELECTRÓNICA	ESCUELA CRISTIANA EVANGELICA ARG.

Trilogía de agentes de IA en la era GPT-5: guía práctica del prototipo al impacto (III)

Leonardo López

Ingeniero en Telecomunicaciones

Mat. I-06913 COPITEC

Máster en Ciencias de Datos (ORCID: 0009-0000-4024-3427)

Coordinador responsable de la Comisión de Inteligencia Artificial de COPITEC

Diego Javier Romero

Ingeniero en Informática | Ingeniero Electrónico | Licenciado en Redes y Comunicación de Datos

Mat. I-06597 COPITEC

Especialista en Informática Forense | Magíster en Informática

Miembro de la Comisión de Inteligencia Artificial de COPITEC

8

La primera entrega de esta trilogía presentó cinco tipologías prácticas de agentes de IA y un mapa para elegir el diseño adecuado según el objetivo y el riesgo del proyecto. La segunda entrega abordó su despliegue responsable: marcos éticos y normativos, evaluación de sesgos y casos de aplicación institucional en COPITEC. Esta tercera y última entrega cierra la serie analizando cómo los agentes de IA convergen con cinco tecnologías emergentes (Edge AI, criptografía post-cuántica, blockchain, orquestación multiagente y computación cuántica) para evolucionar de herramientas puntuales a orquestadores de ecosistemas inteligentes.

Del agente responsable al agente integrado

La entrega anterior de esta trilogía habló de gobernanza antes que de expansión. Repasó los riesgos de la autonomía operativa, la toma de decisiones automatizada, el marco de referencia del AI Risk Management Framework del NIST y del AI Act europeo, y dos casos concretos ya implementados en COPITEC: un asistente de ética y normativa en IA, y COPI, el asistente institucional de atención a matriculados. Ambos contruidos

bajo la misma idea: orientar, no decidir por la persona.

Esa entrega cerraba anticipando justamente el tema de esta tercera parte: cómo los agentes de IA evolucionan al integrarse con tecnologías emergentes, y qué implica eso para sistemas cada vez más autónomos. No es un giro hacia la especulación. Es la continuación del mismo problema: un agente bien gobernado que opera aislado tiene un techo bajo. Ese techo se levanta, para bien y

para mal, cuando el agente empieza a coordinarse con otros, a operar en el borde de la red en lugar de depender de la nube, a dejar registro verificable de lo que hizo, y a proteger sus comunicaciones frente a amenazas que hoy son en gran parte teóricas pero que ya exigen decisiones de diseño.

Esta entrega recorre cinco ejes: Edge AI, criptografía post-cuántica, blockchain, orquestación multiagente y computación cuántica. No están to-

dos en el mismo punto de madurez, y conviene decirlo de entrada para no venderlos como si lo estuvieran. Edge AI y la orquestación multiagente ya se usan en producción. Criptografía post-cuántica y blockchain están en adopción temprana, con base técnica sólida pero todavía poca experiencia acumulada. La computación cuántica aplicada a agentes de IA, en cambio, sigue siendo investigación: no hay casos productivos que la respalden todavía. Un ingeniero que diseña con estos cinco ejes en mente necesita saber en cuál de esos tres estadios está parado cada uno.

Hay además un hilo que atraviesa los cinco: la ciberseguridad. Un agente que opera en el borde de la red,

que habla con otros agentes, que deja registro en una estructura auditable, es un activo más que puede ser atacado. El mismo agente que hoy ayuda a detectar una intrusión puede terminar siendo, si accede a credenciales o sistemas productivos sin los límites adecuados, la puerta de entrada de un ataque nuevo. Esa doble cara (herramienta de defensa y blanco potencial) aparece en cada uno de los ejes que siguen.

Edge AI: autonomía con latencia mínima

Un agente de IA que depende de una consulta a un modelo en la nube para cada decisión hereda las limitaciones de esa dependencia: latencia de red, costo de transmisión de datos, y un punto único de falla si

la conectividad se interrumpe. Edge AI desplaza parte del procesamiento (inferencia, y en algunos casos entrenamiento incremental liviano) al dispositivo o al nodo donde se genera el dato: un sensor industrial, una cámara de videovigilancia, una estación base de telecomunicaciones, un equipo médico, un vehículo.

Para un agente de IA, operar en el borde cambia algo más que el rendimiento: cambia su perfil de riesgo. Un agente que decide localmente puede reaccionar en milisegundos ante un corte de energía, una anomalía en una línea de producción o una falla en un enlace, sin esperar el viaje de ida y vuelta a un servidor remoto. Pensemos en una planta industrial: un agente que analiza sen-



Imagen 1: Nodos.

sores de temperatura o vibración puede disparar una alerta ni bien detecta algo raro, sin depender de la nube. A veces esa rapidez es la diferencia entre una parada programada y una falla que rompe la línea entera.

La contracara de esa cercanía al dato es que cada dispositivo de borde es también una puerta de entrada. Un agente que vive ahí puede ayudar a detectar tráfico anómalo o accesos no autorizados cerca del origen del incidente, pero el dispositivo que lo aloja es, al mismo tiempo, un blanco. Por eso no alcanza con diseñarlo para que rinda bien: necesita autenticación fuerte, cifrado, forma segura de actualizar el modelo que corre ahí, monitoreo, y la posibilidad de revocarlo de forma remota si se ve comprometido.

- » Menor latencia: decisiones en el punto donde ocurre el evento, relevante en infraestructura crítica y control industrial.
- » Mayor autonomía operativa ante interrupciones de conectividad, particularmente relevante en redes de telecomunicaciones y zonas de cobertura limitada.
- » Menor dependencia de la nube y del ancho de banda disponible para transmitir datos crudos.
- » Procesamiento local de datos sensibles, con impacto directo en privacidad y en el perímetro de seguridad que debe protegerse.
- » Requiere redefinir cómo se auditan y actualizan modelos distribuidos en cientos o mi-

les de dispositivos, un desafío operativo que no existe en arquitecturas centralizadas.

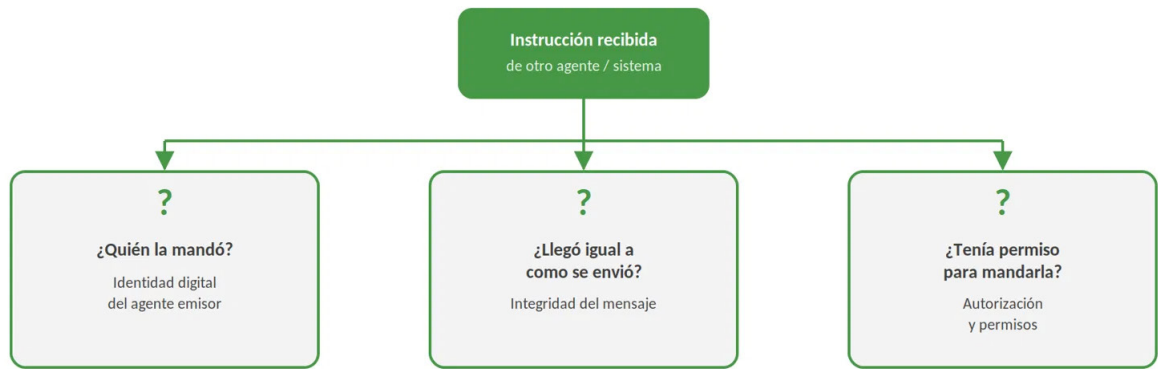
Un agente que decide en el borde no elimina la necesidad de supervisión: la traslada al dispositivo, y con ella, la exigencia de trazabilidad.

Criptografía post-cuántica: seguridad por diseño para decisiones autónomas

Imagen 2: Sensores.



Imagen 3: Identidad.



Cuando dos sistemas se comunican de forma segura, usan un tipo de matemática que a una computadora convencional le llevaría un tiempo enorme romper. Ese es, en el fondo, el candado que protege casi todo internet hoy: RSA, curvas elípticas. Una computadora cuántica lo suficientemente potente podría, en teoría, forzar ese candado en un tiempo mucho más corto. Esa máquina todavía no existe a la escala necesaria.

Pero el riesgo no es solo cosa del futuro. Hay un patrón ya conocido en ciberseguridad que se llama, en la jerga del sector, *store now, decrypt later*: guardar hoy el tráfico cifrado que se intercepta, para abrirlo el día que exista una computadora cuántica capaz de hacerlo. Para un dato que necesita quedar protegido por años, como una identidad digital, un contrato o un registro institucional, ese riesgo ya empieza a importar ahora, aunque la máquina que lo explotaría no exista todavía.

La buena noticia es que ya hay un camino de salida. En 2024 el NIST (el organismo de Estados Unidos que fija estándares de seguridad) aprobó los primeros algoritmos pensados específicamente para resistir ese escenario: se conocen como ML-KEM, para intercambiar claves, y ML-DSA y SLH-DSA, para firmar digitalmente. Que existan estándares aprobados

cambia la naturaleza del problema: deja de ser una discusión teórica y pasa a ser una decisión de arquitectura que ya se puede tomar.

Para un agente de IA que actúa por su cuenta, esto le toca de cerca en tres lugares. Uno: cómo se comunica con otros agentes y con los sistemas que orchestra. Dos: cómo demuestra que es quien dice ser, si opera con credenciales o certificados propios. Tres: cómo se garantiza que sus registros de auditoría (lo que decidió, cuándo y por qué) no puedan falsificarse más adelante. Si cualquiera de esos tres puntos queda sin proteger, toda la arquitectura de confianza se cae, sin importar qué tan bien razone el agente.

Dicho de otra forma: toda esta capa de seguridad existe para responder a tres preguntas simples, cada vez que un agente recibe una orden de otro sistema. ¿Quién la mandó? ¿Llegó igual a como se envió? ¿Tenía permiso para mandarla? Un sistema de agentes que no puede contestar esas tres preguntas con certeza técnica no está listo para actuar solo, por más sofisticado que sea.

» La amenaza es sobre datos que se capturan hoy y podrían descifrarse en el futuro, no sobre computadoras cuánticas operando en la actualidad.

- » Ya existen estándares del NIST (ML-KEM, ML-DSA, SLH-DSA) para empezar a migrar sin esperar a que el riesgo se materialice.
- » Un agente con credenciales propias necesita el mismo nivel de protección que la identidad digital de una persona.
- » Los registros de auditoría necesitan firmas que sigan siendo válidas durante toda su vida útil, no solo en el momento en que se generan.

Blockchain: la caja negra auditable de los agentes de IA

La entrega anterior de esta trilogía comparó la trazabilidad de un agente de IA con la caja negra de un avión: todo lo que hace debe quedar registrado, entradas, salidas, contexto, acciones ejecutadas. Blockchain (entendido acá no como criptomoneda, sino como estructura de datos distribuida e inmutable) es una tecnología candidata para esa capa de registro, cuando el requisito no es solo guardar el log sino garantizar que nadie pudo tocarlo después.

Esa distinción importa. Un log tradicional en una base de datos centralizada puede editarlo cualquiera con privilegios de administrador, y eso lo vuelve insuficiente como evidencia frente a un regulador o en una

disputa. Un registro anclado en una estructura blockchain, en cambio, ofrece evidencia verificable de que algo ocurrió en un momento determinado y no se modificó después. Sirve, sobre todo, para eventos críticos del ciclo de vida de un agente: autorizaciones de despliegue, cambios de configuración, versiones de modelo puestas en producción, intervenciones humanas en procesos de supervisión.

Ahora bien, hay que ser claros sobre lo que blockchain no hace: no valida que la decisión del agente haya sido correcta, ni reemplaza la evaluación de sesgos ni la supervisión humana de las que hablamos en la entrega anterior. Su aporte es más chico, y por eso mismo más sólido: garantiza que el registro de lo que pasó es confiable. Qué tan sólida sea esa garantía depende de cómo se diseñe la solución (quién opera los nodos, qué tan pública o permissionada es la red, qué costo de latencia agrega cada escritura), y eso se define caso por caso, no de una vez para siempre.

En la práctica, no hace falta guardar toda la información sensible adentro de la cadena de bloques. Alcanza con registrar ahí una huella criptográfica del evento (un hash, algunos metadatos, un sello de tiempo) junto con el identificador del agente y la autorización correspondiente, mientras los datos completos quedan en repositorios seguros con control de acceso convencional. Así se logra evidencia verificable sin exponer información sensible en una estructura

que, por diseño, es casi imposible de borrar.

**Blockchain no
certifica que una
decisión del agente
fue correcta.
Certifica que el
registro de esa
decisión no fue
alterado.**

Orquestación multi-agente: de agentes aislados a ecosistemas colaborativos

Este es, para nosotros, el eje más determinante de la entrega, y el que mejor conecta con la gobernanza de la que hablamos en la parte II: el paso de un agente individual a un ecosistema de agentes especializados que colaboran bajo reglas explícitas. La primera entrega ya adelantaba una arquitectura de este tipo (swarm o graph agents), donde un agente principal identifica la necesidad y distribuye tareas: uno extrae datos, otro los valida, otro redacta, otro verifica. Acá la retomamos no como una tipología más entre otras, sino como la dirección hacia la que va el campo.

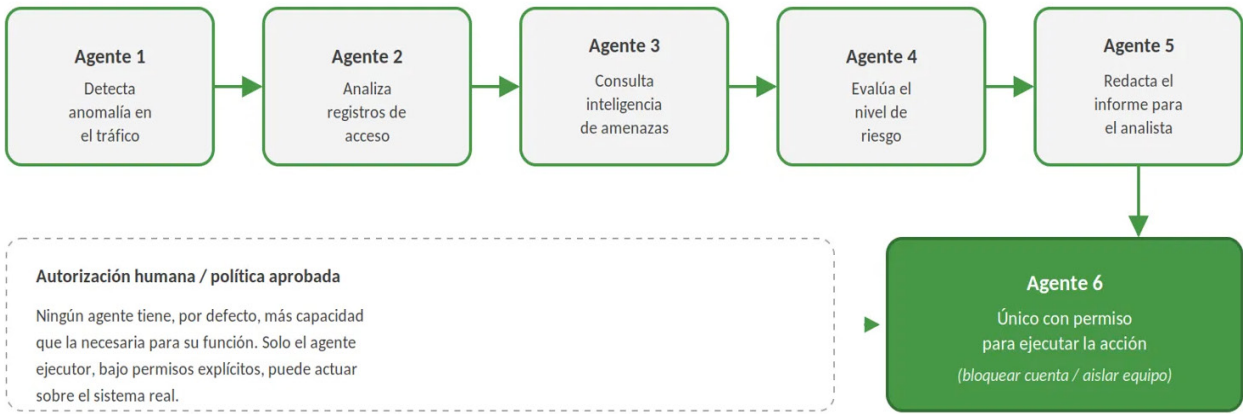
La razón es sencilla. Un agente generalista que intenta hacer de todo termina siendo mediocre en cada tarea puntual, y encima concentra en un solo punto todo el riesgo operativo.

Un ecosistema con roles diferenciados (análisis, ejecución, auditoría, supervisión) permite que cada pieza se especialice, se valide por separado, y se reemplace o actualice sin tener que rediseñar todo el sistema. Ahí aparece la hiperautomatización de punta a punta: ya no es un agente que reemplaza una tarea, sino una cadena de agentes que reemplaza un proceso entero, con puntos de control humano en las etapas donde el riesgo lo pide.

El costo va de la mano del beneficio. Cuantos más agentes coordinados, más grande la superficie de falla: un error de interpretación en el agente de análisis puede propagarse al de ejecución antes de que nadie tenga chance de corregirlo, a menos que el diseño incluya jerarquías de decisión, límites claros de actuación por agente, y mecanismos de corte cuando algún subproceso entra en bucle o se desvía. Acá la gobernanza no es un agregado que se pone después: tiene que estar en el diseño desde el arranque, porque el sistema ya funciona mal sin ella.

Un ejemplo aplicado a un incidente de ciberseguridad ayuda a verlo concreto: un agente detecta una anomalía en el tráfico de red, otro analiza los registros de acceso, otro consulta fuentes de inteligencia de amenazas para contrastar IPs o dominios, otro evalúa el nivel de riesgo, otro redacta el informe para el analista humano. Y solo uno, con permisos explícitos y bajo una política ya aprobada, puede ejecutar una acción como bloquear una cuenta o aislar un equipo. Cada

Imagen 4: Cadena de agentes.



eslabón hace una sola cosa, y ninguno tiene por defecto más capacidad que la que necesita para su función. Es el mismo principio de mínimo privilegio que se aplica a usuarios, trasladado a agentes.

Esa lógica se puede resumir en tres preguntas por agente: qué puede conocer, qué puede decidir y qué puede ejecutar. Un agente que solo analiza no necesita, por diseño, permisos para modificar sistemas reales. Y no toda acción pesa lo mismo: generar un informe no es lo mismo que modificar una configuración de red, ni clasificar una alerta es lo mismo que bloquear una cuenta de usuario. Graduar la autonomía en niveles (observar y recomendar, ejecutar tareas de bajo impacto, y recién después actuar sobre procesos críticos, bajo política estricta y con forma de revertir lo hecho) permite que la autonomía sea proporcional al riesgo de cada acción, en vez de una propiedad pareja para todo el sistema.

- » Agentes con roles diferenciados: análisis, ejecución, auditoría y supervisión, cada uno con permisos y límites de actuación propios.
- » Coordinación mediante un agente orquestador (o mediante protocolos de coordinación entre pares) que

distribuye tareas y consolida resultados.

- » Hiperautomatización de procesos completos, no de tareas aisladas, con puntos de control humano definidos según el nivel de riesgo de cada etapa.
- » Necesidad de jerarquías, límites de tiempo y costo, y mecanismos de corte para evitar la propagación de errores entre agentes.
- » El riesgo no es técnico únicamente: sin gobernanza explícita, un error local se convierte en un error sistémico en el tiempo que tarda un mensaje en pasar de un agente a otro.

Computación cuántica: optimización avanzada, con prudencia

De los cinco ejes de esta entrega, este es el que pide más cuidado a la hora de escribirlo. La computación cuántica promete, en teoría, ventajas fuertes para ciertos problemas de optimización: asignación de recursos, planificación de rutas o de infraestructura, simulación de escenarios donde el número de variables crece tan rápido que a una computadora clásica se le hace cuesta arriba. Gestionar infraestructura de telecomunicaciones a gran escala, con miles de nodos y demanda variable, es justo el tipo de problema donde esa ventaja, si se confirma, importaría.

Ahora, hoy no hay evidencia de agentes de IA funcionando en producción con hardware cuántico integrado para resolver nada de esto. Los enfoques híbridos, con algoritmos como QAOA o VQE que combinan procesamiento cuántico y clásico, siguen en investigación activa: dan resultados en problemas chicos, pero todavía no muestran una ventaja consistente frente a los mejores algoritmos clásicos que ya tenemos. Decir que esta convergencia ya está disponible sería mentir. Decir que no tiene ningún fundamento también sería exagerar.

El criterio que nos parece razonable para un ingeniero que evalúa esta tecnología es el mismo de siempre: no atarse a una capacidad que todavía no es estable ni accesible, pero sí seguirle el rastro, porque el problema que resolvería (optimizar infraestructura a escala masiva) es un problema real que la disciplina ya enfrenta con métodos clásicos, y cualquier mejora ahí tiene impacto directo en cómo se operan redes y servicios.

- » Optimización de redes y asignación de recursos: el tipo de problema combinatorio donde la computación cuántica ofrece ventaja teórica.
- » Simulación de escenarios complejos y planificación de infraestructura a gran escala.

- » Sin evidencia, a la fecha, de despliegues productivos que integren agentes de IA con hardware cuántico.
- » Horizonte de investigación activa (algoritmos híbridos cuántico-clásicos), no de adopción inmediata.

El ingeniero matriculado como garante de resiliencia tecnológica inteligente

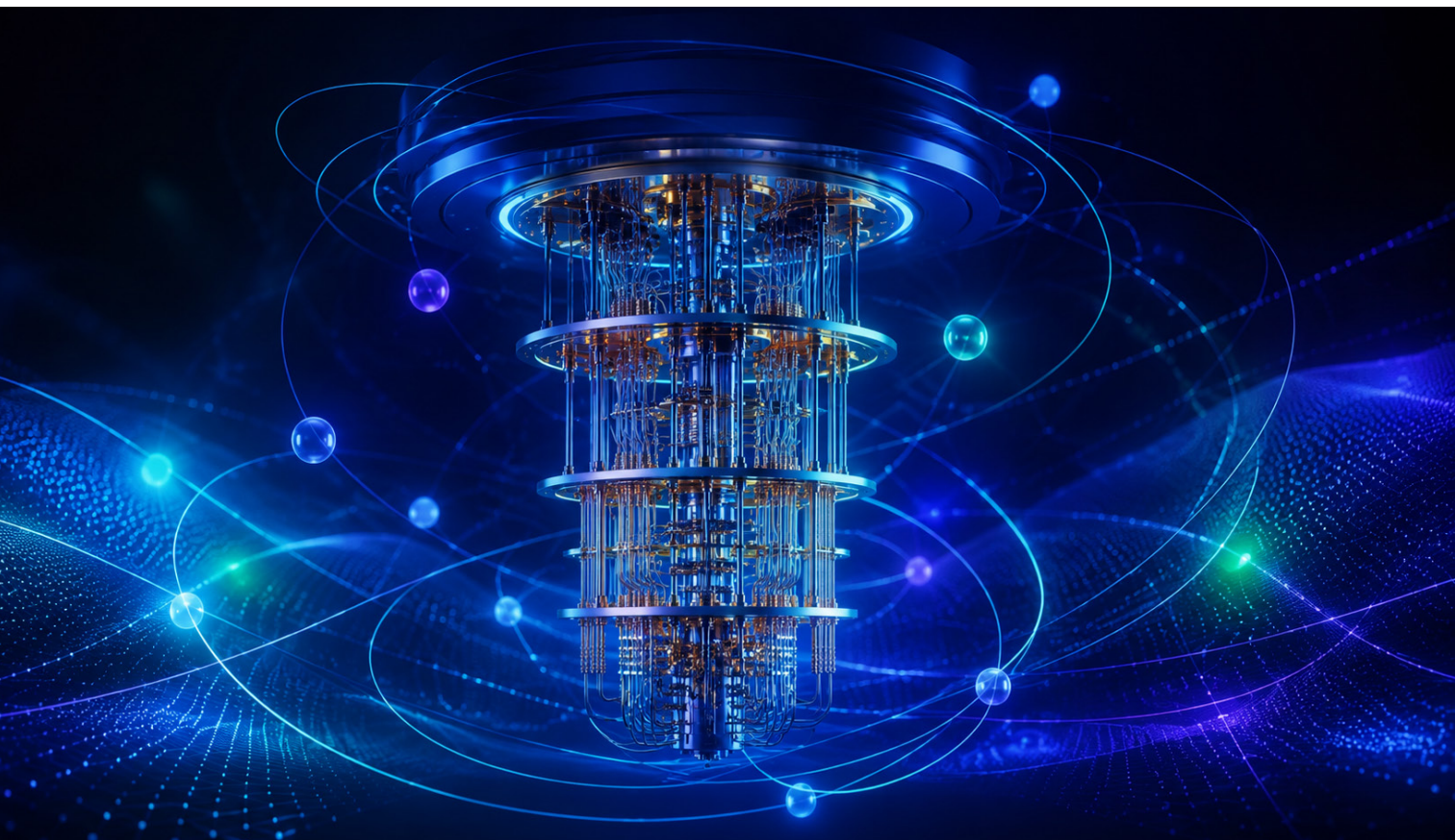
Los cinco ejes de esta entrega no encajan por casualidad. Edge AI decide dónde se ejecuta la acción. Criptografía post-cuántica y blockchain se ocupan de cómo se protege y se audita esa acción. La orquestación multiagente resuelve cómo se coordinan varias decisiones especializadas entre sí. Y la computación cuántica,

todavía en investigación, apunta a resolver optimizaciones que hoy son casi imposibles a la escala que pide la infraestructura crítica. Ninguno de estos ejes reemplaza a los otros. Y ninguno reemplaza la gobernanza de la que hablamos en la entrega anterior: la potencia, para bien o para mal, según qué tan en serio se la tome quien la implemente.

Esta trilogía arrancó siendo técnica y terminó siendo, sobre todo, institucional. Del prototipo funcional (parte I) pasamos al despliegue responsable (parte II) y llegamos a la convergencia con tecnologías emergentes (esta parte III). Lo que se mantiene igual en las tres entregas es una idea simple: un agente de IA no es algo que se instala y se olvida. Es un siste-

ma que necesita diseño deliberado, supervisión continua y responsabilidad profesional en cada capa, técnica, ética y regulatoria.

Desde la Comisión de Inteligencia Artificial de COPITEC, que coordinamos y en la que participan matriculados y profesionales de varias disciplinas activos en el tema, tratamos de sostener esto en la práctica y no solo en el papel. Nos reunimos todos los meses. Desde ahí impulsamos actividades de vinculación con otros organismos, aplicamos algunas implementaciones internas para el Consejo, trabajamos en una normativa interna de ética en IA todavía en elaboración, y organizamos capacitaciones mensuales abiertas a quien se quiera sumar.



Esa es, para nosotros, la función que le cabe al ingeniero matriculado frente a todo lo que describimos en este artículo: no la de mirar desde afuera una evolución que pasa en otro lado, sino la de diseñar, validar, auditar y supervisar estos sistemas con el mismo estándar de responsabilidad que rige el resto del ejercicio de la ingeniería. La tecnología pone las piezas sobre la mesa. La arquitectura, los controles y la idoneidad profesional son los que definen si esas piezas terminan siendo un sistema seguro, o un riesgo distribuido a gran escala.

La próxima etapa de los agentes de IA no estará definida únicamente por su capacidad de razonar o actuar, sino por la calidad de las arquitecturas que los integren, los controles que los gobiernen y los profesionales que garanticen su uso seguro, trazable y responsable.

Los profesionales interesados en participar de la Comisión de Inteligencia Artificial de COPITEC pueden contactarse a través del correo institucional:
comision-ia@copitec.org.ar

Referencias

1. National Institute of Standards and Technology (2023). AI Risk Management Framework (AI RMF 1.0).
2. National Institute of Standards and Technology (2024). The NIST Cybersecurity Framework (CSF) 2.0.
3. National Institute of Standards and Technology (2024). Módulos de estandarización de criptografía post-cuántica: FIPS 203 (ML-KEM), FIPS 204 (ML-DSA) y FIPS 205 (SLH-DSA).
4. International Organization for Standardization (2022). ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection.
5. International Organization for Standardization (2023). ISO/IEC 42001:2023. Information technology. Artificial intelligence management system.
6. OWASP Foundation (2026). OWASP Top 10 for LLM and Generative AI Applications, edición 2026.
7. Unión Europea (2024). Reglamento de Inteligencia Artificial (AI Act).

Capítulo 4: Redes PAN basadas en Bluetooth

Bluetooth es una tecnología de comunicación inalámbrica de corto alcance diseñada para conectar y transferir datos entre dispositivos de forma rápida y sin necesidad de cables. Desde su creación, ha evolucionado y es ampliamente utilizada en múltiples sectores, incluyendo el de consumo, industrial, médico y automotriz. Este capítulo examina los usos actuales de Bluetooth, sus ventajas y desventajas, así como sus características técnicas y funcionales.

16

Marcelo Romeo

Ingeniero en Electrónica

Mat. I-01333 COPITEC

Universidad Tecnológica Nacional

Nota del editor

Coordenadas continúa con la publicación del libro **Comunicaciones inalámbricas**, sobre el estado del arte de tecnologías vinculadas a la matrícula del COPITEC. Los capítulos anteriores pueden encontrarse en las ediciones 121, 122, 123 y 125 de esta revista.

3 Perfiles de Comunicación

Los **perfiles de comunicación en Bluetooth** son conjuntos de especificaciones que definen cómo se deben comunicar los dispositivos Bluetooth para realizar tareas específicas.

Un perfil en Bluetooth define las funciones, los comandos, y las configuraciones necesarias para que dos dispositivos puedan interactuar en una aplicación específica. Cada perfil actúa como una **capa de software** que utiliza las capacidades de hardware de Bluetooth para realizar tareas específicas. Esto permite que los dispositivos puedan, por ejemplo, transferir audio, enviar datos de sensores o actuar como un control remoto.

En definitiva, cada perfil contiene **reglas y protocolos** que estandarizan las funciones de comunicación, asegurando la **compatibilidad** entre dispositivos de

diferentes fabricantes y permitiendo que puedan trabajar juntos en distintas aplicaciones.

3.1 Ejemplos de Perfiles Comunes de Bluetooth

- » **HSP (Headset Profile):** Este perfil permite la conexión de auriculares y micrófonos Bluetooth. Es uno de los perfiles básicos que permite realizar y recibir llamadas de voz desde un teléfono a través de un auricular inalámbrico.
- » **HFP (Hands-Free Profile):** Similar al HSP, este perfil extiende las capacidades de manos libres para vehículos, permitiendo funciones adicionales como la activación de comandos de voz, la transferencia de contactos y la marcación de números.

- » **A2DP (Advanced Audio Distribution Profile):** Este perfil permite la transmisión de audio estéreo de alta calidad desde un dispositivo, como un teléfono móvil, a un altavoz o auricular. Es ideal para reproducir música y otros archivos de audio.
- » **AVRCP (Audio/Video Remote Control Profile):** Utilizado para controlar dispositivos de audio y video de forma remota. Por ejemplo, permite a un teléfono móvil controlar el volumen, la reproducción y el cambio de pista en un altavoz o reproductor multimedia Bluetooth.
- » **SPP (Serial Port Profile):** Emula un puerto serie, permitiendo una comunicación bidireccional de datos entre dispositivos. Es usado en aplicaciones de baja velocidad de datos, como dispositivos de navegación GPS o impresoras.
- » **PAN (Personal Area Networking Profile):** Permite la creación de redes personales entre dispositivos Bluetooth. Este perfil es ideal para compartir una conexión a Internet entre un teléfono móvil y una computadora.
- » **GATT (Generic Attribute Profile):** Específico de Bluetooth Low Energy (BLE), este perfil define la manera en que los dispositivos BLE descubren y organizan servicios. GATT es esencial para el Internet de las Cosas (IoT), permitiendo que sensores y otros dispositivos de baja potencia se comuniquen.
- » **MAP (Message Access Profile):** Permite el acceso y la transferencia de mensajes (como SMS o correos electrónicos) desde un dispositivo, como un teléfono móvil, a otro dispositivo, como un sistema de infoentretenimiento en el automóvil.

3.2 Perfiles de Comunicación y Compatibilidad

Cada perfil de comunicación está diseñado para una aplicación específica, lo que asegura que cualquier

dispositivo compatible con el mismo perfil podrá trabajar sin problemas. Por ejemplo, cualquier auricular que soporte el perfil A2DP puede conectarse y recibir audio estéreo desde cualquier dispositivo Bluetooth compatible con A2DP, sin importar el fabricante.

3.3 Importancia de los Perfiles en Bluetooth

- » **Estandarización:** Los perfiles aseguran que los dispositivos Bluetooth puedan conectarse y comunicarse de forma compatible y uniforme.
- » **Compatibilidad Multiplataforma:** Los perfiles de comunicación permiten que dispositivos de diferentes fabricantes funcionen juntos, eliminando la necesidad de configuraciones complicadas.
- » **Variedad de Aplicaciones:** Con distintos perfiles, Bluetooth soporta una amplia gama de aplicaciones, desde el streaming de audio hasta el monitoreo de salud en dispositivos de bajo consumo.

En resumen, los perfiles de comunicación en Bluetooth son el núcleo que permite que los dispositivos Bluetooth trabajen juntos para cumplir tareas específicas, facilitando aplicaciones en audio, video, datos, y muchas otras áreas. Cada perfil garantiza que los dispositivos cumplan con un estándar de interoperabilidad, asegurando una experiencia de usuario coherente y confiable.

4 Características Físicas

Las **características físicas de Bluetooth** abarcan aspectos como la frecuencia de operación, el tipo de modulación, el rango de alcance, el diseño de la antena y el salto de frecuencia. Estos elementos permiten que Bluetooth mantenga una conexión estable y eficiente en aplicaciones de corto alcance.

4.1 Frecuencia de Operación

Bluetooth opera en la **banda de frecuencia ISM de 2.4 GHz** (Industrial, Scientific, and Medical), una fre-

cuencia globalmente accesible y libre de licencia. Esta banda es compartida con otras tecnologías como Wi-Fi y microondas, lo que requiere mecanismos de control de interferencia, como el salto de frecuencia.

4.2 Salto de Frecuencia (Frequency Hopping)

Bluetooth emplea una técnica llamada **salto de frecuencia (frequency hopping)** para evitar interferencias con otros dispositivos en la misma banda. En Bluetooth clásico, se dividen 79 canales de 1 MHz cada uno, y la tecnología salta entre estos canales hasta 1600 veces por segundo. Esto permite que la señal Bluetooth "salte" a diferentes frecuencias, minimizando la interferencia y mejorando la estabilidad de la conexión.

En **Bluetooth Low Energy (BLE)**, el salto de frecuencia usa solo 40 canales de 2 MHz, lo cual optimiza el ancho de banda y reduce el consumo de energía.

4.3 Modulación

Bluetooth clásico utiliza **GFSK (Gaussian Frequency-Shift Keying)** como método de modulación, que codifica los datos mediante cambios en la frecuencia de la señal portadora. Las versiones más recientes de Bluetooth, como Enhanced Data Rate (EDR), también emplean **$\pi/4$ -DQPSK** y **8DPSK**, permitiendo mayores velocidades de transmisión en ciertos perfiles y aplicaciones.

4.4 Alcance y Clases de Dispositivos

Bluetooth está diseñado principalmente para comunicaciones de corto alcance, aunque el alcance exacto depende de la clase de potencia del dispositivo:

- » **Clase 1:** Alcance de hasta 100 metros, utilizado en aplicaciones industriales.
- » **Clase 2:** Alcance de hasta 10 metros, común en dispositivos de consumo como auriculares y teléfonos móviles.

- » **Clase 3:** Alcance de hasta 1 metro, usado en dispositivos de muy corto alcance (aunque menos común).

El alcance real puede variar según factores como obstáculos físicos, interferencias y la sensibilidad del receptor.

4.5 Antena y Diseño de Hardware

Bluetooth generalmente utiliza antenas de corto alcance que pueden estar integradas en el circuito del dispositivo o conectarse de forma externa. Las antenas están diseñadas para la banda de 2.4 GHz y pueden ser de diferentes tipos, como:

- » **Antenas de chip:** Integradas en el chip Bluetooth, comunes en dispositivos compactos.
- » **Antenas de cerámica:** Ofrecen una mayor resistencia a la interferencia, usadas en dispositivos industriales.
- » **Antenas de PCB:** Impresas en la placa de circuito y son compactas, adecuadas para dispositivos portátiles.

4.6 Topología de Red: Piconet y Scatternet

En **Bluetooth**, la topología de red está basada en estructuras denominadas **piconet** y **scatternet**, las cuales organizan cómo se conectan y comunican los dispositivos dentro de la red. Estas topologías permiten que varios dispositivos se conecten de manera eficiente, optimizando el uso de ancho de banda y gestionando las conexiones en aplicaciones de corto alcance.

4.6.1 Piconet.

Una **piconet** es la unidad básica de la red Bluetooth y consiste en un grupo de dispositivos conectados de forma temporal.



Figura 3. Topología Bluetooth

En una piconet:

- » **Estructura Maestro-Eslavo:** Un dispositivo actúa como **maestro**, y puede conectarse con hasta **siete** dispositivos esclavos activos simultáneamente. Además, se pueden conectar hasta 255 dispositivos como **esclavos** en modo inactivo o en espera, aunque solo los siete esclavos activos pueden intercambiar datos en un momento dado.
- » **Sincronización:** El dispositivo maestro controla la frecuencia y el tiempo en la piconet, sincronizando los intervalos de comunicación con los esclavos. Esto permite que cada dispositivo esclavo sepa cuándo puede transmitir y recibir datos, evitando conflictos y optimizando el uso de la conexión.
- » **Canal de Comunicación Compartido:** Todos los dispositivos en la piconet comparten un solo canal de comunicación, usando técnicas de **salto de frecuencia** para minimizar la inter-

ferencia con otras señales de Bluetooth u otras redes en la misma banda.

- » **Ejemplo de Uso de Piconet:** Un teléfono móvil conectado a varios dispositivos Bluetooth, como auriculares, un reloj inteligente y un sistema de infoentretenimiento de un automóvil, puede formar una piconet. El teléfono actúa como maestro, mientras que los otros dispositivos funcionan como esclavos sincronizados.

4.6.2 Scatternet.

Una **scatternet** es una red más compleja que conecta varias piconets, permitiendo que un dispositivo participe en múltiples piconets al mismo tiempo.

Esto permite una mayor interconexión de dispositivos, con los siguientes elementos clave:

- » **Dispositivo Puente:** En una scatternet, uno o varios dispositivos actúan como puentes entre diferentes piconets. Un dispositivo puente puede funcionar como esclavo en una piconet y como maestro o esclavo en otra, permitiendo el paso de datos entre ellas.

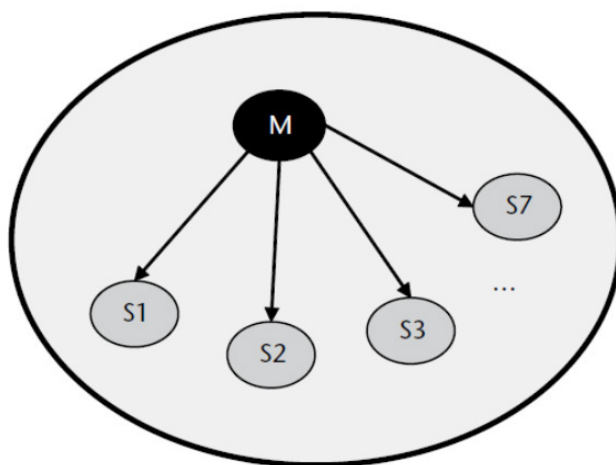


Figura 4. Esquema de una piconet

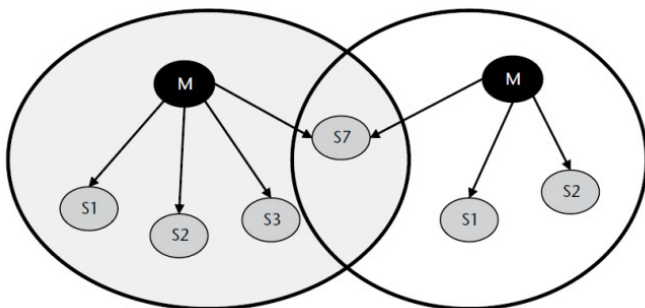


Figura 5. Estructura de una scatternet

20

- » **Interoperabilidad:** Cada piconet mantiene su propia estructura de maestro-esclavo y frecuencia, pero el dispositivo puente gestiona la sincronización para facilitar la comunicación entre ellas.
- » **Flexibilidad y Expansión:** Las scatternets permiten a una red Bluetooth conectar muchos más dispositivos que una sola piconet, expandiendo el alcance y la funcionalidad de la red sin sobrecargar el canal de comunicación.
- » **Ejemplo de Uso de Scatternet:** En un entorno de IoT en una fábrica, un sensor ambiental conectado a una piconet puede actuar como puente con otra piconet donde se encuentran

dispositivos de monitoreo de maquinaria. Esto permite que los datos fluyan entre piconets, centralizándolos en una red más amplia de monitoreo.

4.6.4 Ventajas y Desventajas

Piconet:

- » Ventajas: Baja complejidad y adecuado para conexiones sencillas y de corto alcance.
- » Desventajas: Limitada a un máximo de 7 dispositivos activos y no puede interconectarse con otras piconets sin un puente.

Scatternet:

- » Ventajas: Mayor flexibilidad y capacidad de expandir la red al interconectar varias piconets.
- » Desventajas: Mayor complejidad en la sincronización y posible latencia en el paso de datos entre piconets.

4.7 Resumen de las Características Físicas de Bluetooth

- » **Frecuencia de Operación:** 2.4 GHz, banda ISM.

Característica	Piconet	Scatternet
Estructura	Maestro y varios esclavos	Varias piconets interconectadas
Número de Dispositivos Activos	Hasta 7 esclavos activos	Muchos dispositivos, dependiendo de la cantidad de piconets
Dispositivos Puente	No requiere dispositivos puente	Requiere dispositivos puente para conectar piconets
Complejidad	Simple y de corto alcance	Compleja y de mayor alcance
Aplicación	Conexión entre pocos dispositivos cercanos	Redes expandidas, como en aplicaciones IoT

Figura 6.- 4.6.3 Comparación entre Piconet y Scatternet

- » **Salto de Frecuencia:** Hasta 1600 saltos por segundo en Bluetooth clásico (79 canales de 1 MHz) y 40 canales en BLE.
- » **Modulación:** GFSK en Bluetooth clásico; $\pi/4$ -DQPSK y 8DPSK en versiones con Enhanced Data Rate.
- » **Alcance:** De 1 a 100 metros, dependiendo de la clase de potencia del dispositivo.
- » **Antenas:** Diferentes tipos según la aplicación, como chip, cerámica y PCB.
- » **Topología de Red:** Piconets y scatternets para organizar y conectar múltiples dispositivos.
- » **Portabilidad de los Chips:** Los chips Bluetooth modernos son extremadamente pequeños, lo cual facilita su integración en una gran variedad de dispositivos. Esto permite que Bluetooth se encuentre en dispositivos como teléfonos móviles, relojes inteligentes, auriculares, sensores de salud y más.
- » Los chips Bluetooth de bajo consumo (BLE) son particularmente compactos y están optimizados para dispositivos de bajo costo y aplicaciones de IoT.

Estas características físicas permiten que Bluetooth sea ampliamente compatible y adaptable, adecuado para aplicaciones de corto alcance que requieren bajo consumo de energía y estabilidad en la conexión.

5 Características Eléctricas

Las **características eléctricas de Bluetooth** se relacionan con la potencia de transmisión, el consumo de energía, las clases de potencia, y el rango de alcance. Estas características han sido optimizadas para asegurar una conectividad inalámbrica eficiente y de bajo consumo, adecuada tanto para dispositivos móviles de corto alcance como para aplicaciones de bajo consumo en el Internet de las Cosas (IoT).

5.1 Clases de Potencia y Alcance

Los dispositivos Bluetooth están clasificados en clases de potencia según su alcance y potencia de

transmisión:

- » **Clase 1:**
 - **Potencia de Transmisión:** Hasta 100 mW (20 dBm).
 - **Alcance:** Hasta 100 metros (en condiciones ideales).
 - **Uso Típico:** Dispositivos industriales y comerciales donde se requiere mayor cobertura.
- » **Clase 2:**
 - **Potencia de Transmisión:** Hasta 2.5 mW (4 dBm).
 - **Alcance:** Aproximadamente 10 metros.
 - **Uso Típico:** Dispositivos de consumo, como auriculares y teléfonos móviles.
- » **Clase 3:**
 - **Potencia de Transmisión:** Hasta 1 mW (0 dBm).
 - **Alcance:** Aproximadamente 1 metro.
 - **Uso Típico:** Dispositivos de muy corto alcance, aunque esta clase es menos común hoy en día.

El alcance real de los dispositivos Bluetooth puede verse afectado por factores como interferencias ambientales, obstáculos físicos y la sensibilidad de los dispositivos conectados.

5.2 Consumo de Energía

Bluetooth está diseñado para ser eficiente en términos de consumo de energía, lo cual es crucial en dispositivos portátiles y de bajo consumo.

- » **Bluetooth Clásico:** Consume más energía que Bluetooth Low Energy y está diseñado para aplicaciones que requieren un enlace de datos continuo, como auriculares y dispositivos de audio.
- » **Bluetooth Low Energy (BLE):** Diseñado para aplicaciones de IoT, como sensores de salud y dispositivos de monitoreo. BLE tiene modos de operación que permiten que los dispositivos mantengan una conexión sin consumir

mucha energía, ideal para dispositivos de baja potencia.

5.3 Modulación y Espectro de Frecuencia

Bluetooth utiliza la banda de frecuencia **ISM de 2.4 GHz** (Industrial, Scientific, and Medical), la cual es una frecuencia libre de licencia disponible en todo el mundo. La modulación típica en Bluetooth clásico es **GFSK (Gaussian Frequency-Shift Keying)**, mientras que en versiones recientes, especialmente BLE, se emplean otras formas de modulación, como **DPSK** y **8DPSK** para mejorar la velocidad de transmisión en aplicaciones específicas.

5.4 Tensión de Operación

El voltaje de operación de los chips Bluetooth varía según el fabricante, pero la mayoría de los dispositivos Bluetooth modernos operan a un **voltaje bajo, entre 1.8 y 3.6 V**. Esto permite que Bluetooth sea integrado en dispositivos de bajo consumo de batería, como relojes inteligentes y sensores portátiles.

5.5 Control de Potencia de Transmisión

Bluetooth incluye un mecanismo de **control de potencia** para ajustar la intensidad de la señal de acuerdo a la distancia entre los dispositivos. Si los dispositivos están cerca, la potencia de transmisión se reduce para ahorrar energía, mientras que, si están más alejados, se incrementa para mantener la conexión.

5.6 Ciclos de Trabajo y Ahorro de Energía

Los dispositivos Bluetooth, especialmente los de BLE, alternan entre **ciclos de trabajo activos y en reposo** para reducir el consumo energético. BLE permite el escaneo y la transmisión en intervalos, de modo que los dispositivos pasan la mayor parte del tiempo en estado de reposo, despertándose solo en momentos predeterminados para transmitir o recibir datos.

Resumen de las Características Eléctricas de Bluetooth

- » **Clases de potencia:** Definen el alcance y la potencia de transmisión en función del tipo de aplicación.
- » **Consumo de energía:** Optimizado en BLE para aplicaciones de bajo consumo, permitiendo que los dispositivos funcionen por largos periodos con baterías pequeñas.
- » **Modulación y frecuencia:** Uso de GFSK y salto de frecuencia en la banda ISM de 2.4 GHz para minimizar interferencias.
- » **Voltaje de operación:** Generalmente entre 1.8 y 3.6 V.
- » **Control de potencia:** Ajuste dinámico de la potencia de transmisión para optimizar el consumo y mantener la conexión.
- » **Ciclos de trabajo:** Especialmente en BLE, para reducir el consumo en dispositivos que requieren conexiones de larga duración.

Estas características permiten que Bluetooth sea eficiente y práctico para dispositivos de uso cotidiano y aplicaciones de IoT, asegurando una comunicación estable y de bajo consumo energético.

Bluetooth está diseñado para ser eficiente en el consumo de energía. Sus características eléctricas dependen del tipo de dispositivo y la versión del protocolo. En general, Bluetooth clasifica sus dispositivos según la potencia de transmisión:

- » **Clase 1:** Hasta 100 mW (20 dBm), con un alcance de hasta 100 metros.
- » **Clase 2:** Hasta 2.5 mW (4 dBm), con un alcance de unos 10 metros.
- » **Clase 3:** Hasta 1 mW (0 dBm), con un alcance de 1 metro.

Bluetooth Low Energy (BLE) es una versión optimizada para aplicaciones que requieren poco consumo de energía, lo que permite su uso en dispositivos pequeños con baterías de larga duración.

6 Análisis de Comandos

Bluetooth utiliza comandos específicos para controlar la conexión y transmisión de datos.

Algunos de los comandos más comunes son:

- » **AT Commands:** Utilizados en módulos Bluetooth para iniciar y gestionar la conexión
- » **Comandos HCI (Host Controller Interface):** Controlan la interfaz de hardware de Bluetooth.

6.1 Comandos AT

Los **comandos AT** son una serie de instrucciones de alto nivel desarrolladas originalmente para controlar módems y que se han adaptado para gestionar módulos Bluetooth. Estos comandos son fáciles de usar y permiten realizar configuraciones básicas de Bluetooth sin necesidad de un control directo del hardware.

Ejemplos de Comandos AT Comunes

- » **AT+NAME:** Configura o muestra el nombre del dispositivo Bluetooth.
 - **Ejemplo:** AT+NAME=MiDispositivo cambia el nombre del dispositivo a "MiDispositivo".
- » **AT+PIN:** Configura o muestra el PIN utilizado para el emparejamiento.
 - **Ejemplo:** AT+PIN=1234 establece el PIN como "1234".
- » **AT+ROLE:** Establece el rol del dispositivo (maestro o esclavo).
 - **Ejemplo:** AT+ROLE=1 asigna al dispositivo el rol de maestro.
- » **AT+UART:** Configura los parámetros de comunicación UART, como la velocidad de transmisión.
 - **Ejemplo:** AT+UART=9600,1,0 establece una velocidad de 9600 bps, con 1 bit de parada y sin paridad.
- » **AT+RESET:** Reinicia el módulo Bluetooth para aplicar cambios.
- » **Ejemplo:** AT+RESET reinicia el dispositivo.

Ventajas de los Comandos AT

- » **Facilidad de Uso:** Los comandos AT son fáciles de implementar y utilizar, especialmente para aplicaciones sencillas.

- » **Configuración Rápida:** Permiten configurar parámetros de conexión de manera rápida y eficiente.
- » **Compatibilidad:** Son compatibles con la mayoría de los módulos Bluetooth estándar del mercado.

Limitaciones

- » **Control Limitado:** No ofrecen control profundo del hardware del dispositivo.
- » **Menos Opciones de Configuración Avanzada:** Son adecuados para configuraciones básicas, pero no para aplicaciones avanzadas.

6.2 Comandos HCI (Host Controller Interface)

Los comandos HCI son instrucciones a nivel de hardware que permiten la comunicación entre el host (como una computadora o un teléfono) y el controlador Bluetooth. Estos comandos son parte del protocolo HCI (Host Controller Interface), que define cómo interactúa el software con el hardware Bluetooth para gestionar las funciones de bajo nivel.

Ejemplos de Comandos HCI Comunes

- » **HCI_Reset:** Restablece el controlador Bluetooth, similar al comando AT+RESET. Este comando inicializa el controlador, borrando configuraciones temporales y reconfigurándolo a los valores predeterminados.
- » **HCI_Inquiry:** Inicia una búsqueda de dispositivos Bluetooth cercanos. Este comando permite al dispositivo buscar y obtener información de los dispositivos Bluetooth dentro de su rango.
- » **HCI_Create_Connection:** Establece una conexión con un dispositivo Bluetooth específico. A través de este comando, el host puede establecer una conexión con un dispositivo detectado en la búsqueda.

- » **HCI_Disconnect:** Finaliza la conexión activa con un dispositivo. Permite al host desconectar un dispositivo específico, liberando recursos de conexión
- » **HCI_Read_Remote_Supported_Features:** Consulta las características del dispositivo remoto. Permite conocer las capacidades del dispositivo al que se está conectando, como el soporte para perfiles específicos o compatibilidad de cifrado.
- » **HCI_Set_Event_Filter:** Configura un filtro para los eventos que el controlador notificará al host. Este comando permite filtrar ciertos eventos o notificaciones, optimizando el rendimiento al solo escuchar eventos relevantes.

Ventajas de los Comandos HCI

24

- » **Control Profundo:** Proporcionan un control detallado de las funciones de hardware, ideales para aplicaciones avanzadas.
- » **Flexibilidad en la Configuración:** Permiten personalizar la comunicación y las conexiones Bluetooth de manera avanzada.
- » **Compatibilidad con Sistemas Embebidos:** Utilizados en entornos que requieren un control específico sobre las conexiones y los eventos de Bluetooth.
- » **Limitaciones**
 - **Complejidad:** Requieren conocimientos avanzados para implementar y manejar correctamente.
 - **Mayor Carga de Trabajo:** Pueden ser más lentos de implementar debido a su complejidad y a las configuraciones detalladas.

7 Apéndice 1- Reconocimiento y Configuración de Puerto COM

Los puertos **COM** (Communications Port) son interfaces de comunicación serial que permiten la transmisión de datos entre dispositivos periféricos y una computadora. Aunque los puertos COM físicos (como el RS-232) son menos comunes en computadoras

modernas, muchos dispositivos utilizan **puertos COM virtuales** a través de conexiones USB, especialmente en programación y electrónica.

Para utilizar Bluetooth en dispositivos que requieren comunicación serial, se configura un puerto COM virtual. El sistema operativo asigna un puerto COM para que la aplicación lo use como si estuviera conectado físicamente a través de un cable serial.

A continuación veremos como interactuar con puertos COM en distintos sistemas operativos:

7.1 Reconocimiento de Puertos COM en Windows

7.1.1 1. Acceder al Administrador de Dispositivos:

- » Presione **Windows + R** para abrir el cuadro de diálogo Ejecutar.
- » Escriba **devmgmt.msc** y presione **Enter**. Esto abrirá el **Administrador de dispositivos**.

7.1.2 Ubicar los Puertos COM:

- » En el Administrador de dispositivos, busque y expanda la sección "**Puertos (COM y LPT)**".
- » Aquí verá una lista de los puertos COM y LPT disponibles en su sistema, por ejemplo:
 - "**Puerto de comunicaciones (COM1)**"
 - "**USB Serial Port (COM3)**"

7.1.3 Identificar el Puerto Correcto:

- » Si ha conectado un dispositivo recientemente (como un adaptador USB-Serial, un módulo Bluetooth, un Arduino, etc.), debería aparecer en esta lista.
- » Anote el número de puerto COM asignado (por ejemplo, **COM3**).

7.1.4 Configuración del Puerto COM Acceder a las Propiedades del Puerto:

- » En el **Administrador de dispositivos**, haga clic derecho sobre el puerto COM que desea configurar.
- » Seleccione "**Propiedades**" en el menú contextual.

7.1.5 Configurar los Parámetros del Puerto:

- » Vaya a la pestaña **"Configuración del puerto"**.
- » Ajuste los siguientes parámetros según las necesidades de su dispositivo o aplicación:
 - **Bits por segundo (Baud Rate):** Velocidad de transmisión (por ejemplo, 9600, 19200, 115200).
 - **Bits de datos:** Usualmente 8.
 - **Paridad:** Ninguno, Par, Impar.
 - **Bits de parada:** Normalmente 1.
 - **Control de flujo:** Ninguno, Hardware (RTS/CTS), Software (XON/XOFF).

7.1.6 Aplicar los Cambios:

- » Después de ajustar los parámetros, haga clic en **"Aceptar"** para guardar la configuración.

7.1.7 Asignación de Número de Puerto COM

En algunos casos, es posible que necesites cambiar el número asignado al puerto COM, especialmente si un software específico requiere un número determinado.

7.1.8 Cambiar el Número de Puerto COM:

- » En la ventana de **Propiedades** del puerto COM, ve a la pestaña **"Configuración del puerto"**.
- » Haz clic en **"Opciones avanzadas..."**.
- » En la sección **"Número de puerto COM"**, selecciona el número deseado de la lista desplegable.
- » **Nota:** Asegúrate de elegir un número que no esté en uso por otro dispositivo.
 - **2. Confirmar y Reiniciar:**
 - Haz clic en "Aceptar" en todas las ventanas para aplicar los cambios
 - Es posible que debas reiniciar el sistema o desconectar y volver a conectar el dispositivo para que los cambios surtan efecto.

8 Solución de Problemas Comunes

» El Puerto COM No Aparece:

- Verifica que el dispositivo esté correctamente conectado y funcionando.
- Asegúrate de que los controladores (drivers) del dispositivo estén instalados correctamente.
- Puedes buscar actualizaciones de controladores en el sitio web del fabricante.

» Conflicto de Puertos:

- Si recibes un mensaje de error indicando que el puerto está en uso, cierra cualquier aplicación que pueda estar utilizando el puerto.
- Verifica en el Administrador de dispositivos si hay conflictos o dispositivos marcados con un símbolo de advertencia.

» El Dispositivo No Funciona Correctamente:

- Revisa que los parámetros de configuración (baudios, paridad, etc.) coincidan entre el dispositivo y la configuración del puerto.
- Prueba con diferentes cables o puertos USB si es un dispositivo USB-Serial.

25

9 Uso del Puerto COM en Aplicaciones

Una vez que el puerto COM está correctamente configurado, puedes utilizarlo en diversas aplicaciones:

1. Programas de Terminal Serial:

- **PuTTY, TeraTerm, RealTerm, o HyperTerminal** pueden conectarse al puerto COM para enviar y recibir datos.
- Configura los parámetros de conexión (velocidad, paridad, bits de datos, bits de parada, control de flujo) para que coincidan con los del dispositivo.

2. Desarrollo de Software:

- Lenguajes como **Python, C#, Java, y C++** ofrecen bibliotecas para comunicación serial.
- Por ejemplo, en Python puedes usar la biblioteca **pySerial**:

Bibliografía

1. Bluetooth Low Energy: The Developer's Handbook Nov 7, 2012 - Robin Heydon - Prentice Hall - ISBN-13: 978-0132888363 ISBN-10: 013288836X.
2. Bluetooth Essentials for Programmers* - Albert S. Huang y Larry Rudolph. ISBN: 978-0521687995.
3. Bluetooth Low Energy: The Developer's Handbook - Robin Heydon. ISBN: 9780132888363.
4. Bluetooth Technology and Its Applications with Java and J2ME* - C. Bala Kumar, Paul J. Kline y Timothy J. Thompson. ISBN: 978-0131433519.
5. Bluetooth Core Specification - Bluetooth Special Interest Group (SIG). Disponible en: Bluetooth SIG.
6. Bluetooth Low Energy: A Survey - Mohammad S. R. Ayyash et al.
7. Enabling the Internet of Things: Bluetooth Low Energy (BLE) - David Boswarthick

Ecuación de Friis en Radioenlaces

Diseñada para escenarios sin obstáculos ni reflexiones, la fórmula de Harald T. Friis se utiliza masivamente en el diseño de radioenlaces. Sin embargo, sus limitaciones frente a la realidad del entorno radioeléctrico han abierto fuertes controversias sobre la precisión de sus resultados en la práctica profesional.

Homero Corbo

Ingeniero en Telecomunicaciones

Mat. I-01698 COPITEC

26

1.- Introducción

La **Ecuación de Transmisión de Friis** se utiliza para calcular la potencia recibida de una señal propagada en un enlace de radiofrecuencia, válida únicamente bajo condiciones ideales de espacio libre y sin obstáculos.

La fórmula fue presentada por primera vez en 1946 por el Ingeniero de Radio danés-estadounidense **Harald T. Friis** (*ref. al pie*) y **se utiliza de manera universal en Ingeniería de RF** para calcular enlaces radioeléctricos, pero **adolece de varias y severas limitaciones técnicas para la mayoría de las aplicaciones** y que serán tratadas

posteriormente, pues su utilización generalizada genera inconvenientes en Ingeniería.

2.- Ecuación de Friis

En ANEXO I se expone el procedimiento de obtención de la ecuación y considerando una fuente isotrópica emisora que sirve a los fines Físicos/Matemáticos para establecer un enlace radioeléctrico e irradia un frente de onda esférica con la misma intensidad en todas las direcciones, para una antena ideal y puntual de ganancia unitaria; se define una densidad esférica de potencia irradiada y el área de apertura de un dipolo receptor de media onda que detecta la señal propagada a una cierta dis-

tancia y cubriendo un casco esférico; luego se relaciona con las ganancias para cualquier antena transmisora y receptora respecto a un dipolo de media onda.

La **Ecuación de Friis** expresada en [dbm], aplicando logaritmos y refiriendo las potencias a [1 mWatt] se obtiene la relación normalmente utilizada:

$$PRX = 32,45 + 20\log D + 20\log Frec + 10\log PTX + GantRX + GantTX \\ (Ec 2.1)$$

donde:

PRX: potencia recibida [dbm]

D: distancia entre Tx y Rx [Km]

Frec: frecuencia de operación [MHz]

PTX: potencia transmisor [dbm]

GantRX/GantTX: ganancias de an-

1.-Friis, HT (mayo de 1946). "Una nota sobre una fórmula de transmisión simple". IRE Proc . 34 (5): pag (254– 256)

tenas referidas a dipolo de media onda $[db\lambda/2]$

Corresponde destacar que la potencia recibida en un enlace está relacionada cuadráticamente con la inversa de la distancia, pues se considera una fuente emisora que propaga un frente de onda esférico y también una relación cuadrática con la inversa de la frecuencia de operación.

3.- Limitaciones de Friis

La utilización de la **Ecuación de Friis** no solo se limita a que el enlace sea óptico pues en los últimos tiempos hubo infinidad de aportes técnicos en sistemas de comunicaciones y de propagación; observándose las siguientes limitaciones y controversias que restringen su utilización de manera tan general y universal para considerar el cálculo de un enlace radioeléctrico, según:

- » 01) **Enlace óptico y libre de obstáculos:** Las condiciones ideales casi nunca se alcanzan en comunicaciones terrestres ordinarias; debido a obstrucciones, reflexiones de edificios y fundamentalmente con reflexiones del suelo. Una situación razonablemente precisa de la ecuación es en enlaces

satelitales y cuando la absorción atmosférica es despreciable (también espaciales); otra situación es en cámaras anecoicas para minimizar las reflexiones.

- » 02) **Ancho de Banda:** El ancho de banda deberá ser lo suficientemente estrecho como para que se pueda utilizar un único valor para la longitud de onda y representar todas las características de transmisión.
- » 03) **Alineación de Antenas:** no solo deberán estar alineadas las antenas transmisoras y receptoras, sino fundamentalmente con la misma polarización.
- » 04) **Pérdidas por Polarización:** la ecuación no considera la diferencia de pérdidas en una propagación debido a diferentes polarizaciones (vertical, horizontal o circular) por ionización del suelo. La ecuación tampoco contempla las pérdidas por rebotes en diferentes polarizaciones con obstáculos circundantes (edificios, suelo, colinas, etc) y su efecto en el filtrado de polarizaciones.
- » 05) **Polarización Cruzada:** Friis no considera que las an-

tenas transmisora y receptora estén en polarización cruzada: (vertical vs horizontal) ó (circular giro dextrógiro vs levógiro) y las pérdidas consecuentes que pueden rondar en (20-30 db) ó mayor.

- » 06) **Polarización Circular:** el método Friis tampoco considera que en polarización circular (o elíptica), la potencia emitida se reparte en horizontal y vertical.
- » 07) **Campo Lejano:** la ecuación es válida cuando las antenas estén en el campo lejano de la otra y a una distancia mayor a (5λ) ; vale destacar, que la distancia entre las antenas debe ser mucho mayor que la dimensión máxima de los dipolos; para **dipolos largos $(> 1 \lambda)$, el campo lejano aumenta de manera notable frente a la considerada para dipolos de media onda.**
- » 08) **Área de Apertura Receptora:** la apertura efectiva de la antena receptora puede ser igual, mayor o menor al área física enfrentada y contradice a muchos autores de bibliografía técnica.

- » **09) Acoplamiento:** la ecuación es válida si las antenas transmisora y receptora estén perfectamente acopladas a las líneas de transmisión, de tal manera que la potencia irradiada sea idéntica a la emitida por el transmisor y consecuentemente, que la potencia inducida en la antena receptora sea la misma que la propagada; sin considerar las pérdidas por aisladores, materiales constructivos, etc.
- » **10) Dipolos cortos:** No es válido Friis para utilizar con dipolos cortos ($< 0,1 \lambda$) pues obtendremos resultados analíticos menores a los hallados prácticamente.
- » **11) Dipolos largos:** La impedancia de entrada de un dipolo varía drásticamente según su longitud total en relación con la longitud de onda, mientras que un dipolo clásico de media onda tiene una impedancia resistiva cercana a los 73Ω ; un dipolo largo (que supera esa medida) experimenta grandes fluctuaciones en su valor de impedancia y componentes reactivos. El caso mas relevante es para un dipolo de una onda completa, la distribución de corriente en los terminales de alimentación se vuelve cero y eleva la impedancia de entrada a valores teóricamente infinitos. Para el caso de dipolos de 1 ó $1,5 \lambda$, tiene un patrón de

radiación diferente al de un dipolo clásico de media onda y mayor cantidad de lóbulos secundarios. Por tanto se debe considerar la ganancia directiva real y exacta correspondiente a la longitud física del dipolo utilizado.

- » **12) Frente de onda esférica:** Friis solo es válida para antenas con frente de radiación de tipo esférica, no así para **antenas de muy alta frecuencia y directivas, donde está controlada la emisión de lóbulos secundarios para generar un frente de radiación tipo planar.** Al respecto es importante destacar que la atenuación de un frente de emisión esférico se atenúa con la inversa de la distancia al cuadrado; para un frente plano es con la inversa de la distancia; por ende y con la planar, la propagación se atenuará en un grado mucho menor.
- » **13) Frente de onda planar:** De acuerdo a la teoría de antenas, los lóbulos primario y secundarios conformados en su diagrama de irradiación están cambiados de fase en (180°) y entre ellos alternativamente; **el aporte de los secundarios conformarán un frente de emisión de tipo esférico.** Vale destacar y como sucede con algunas

antenas altamente directivas y con el uso de reflectores y colimadores, **se irradiarán muy pocos lóbulos secundarios y además linealizadas las fases entre ellos con el uso de colimadores**, produciendo un frente onda propagada del tipo plana; sumamente utilizadas en comunicaciones satelitales y espaciales pues **la atenuación con la distancia se mejora notablemente al depender de la inversa con la distancia** (no con su cuadrado).

- » **14) Condiciones climáticas y ambientales:** Friis no considera pérdidas en el trayecto por nieve, humedad ambiente, lluvia, neblina, granizo, tipo de terreno, climas desérticos, espejos de agua, etc.
- » **15) Multitrayectorias:** la ecuación no contempla la acción de múltiples rebotes en el fenómeno de propagación de una onda.
- » **16) Efecto Doppler:** la ecuación de Friis solo considera que el enlace es de tipo estático sin contemplar desplazamiento de frecuencias por movimientos relativos entre transmisor y receptor, más aún en sistemas de banda ancha o para el caso de naves espaciales que pueden moverse relativamente a decenas de miles de Km/h y que afectarán gravemente la confiabilidad de enlaces.

» **17) Margen Desvanecimiento: (M_{fade})** es un nivel de potencia incremental que se considera en un enlace de telecomunicaciones, sirve para garantizar que la señal sea la correcta aunque ocurran problemas temporales que reduzcan su intensidad y que afectará la confiabilidad pretendida del enlace. El Margen de Desvanecimiento es el factor menos predecible de todos los fenómenos puestos en juego en una propagación, por tanto es recomendable considerarlo siempre en exceso. Vale destacar y para sistemas de banda ancha, que el desvanecimiento puede ser selectivo para componentes de frecuencias dentro de esa misma banda. La **Confiabilidad** de un enlace normalmente se fija para el 99,99 % del tiempo; por tanto, solo el 0,01 % del tiempo la señal será inferior que la pretendida para un enlace. Fijar un valor diferente en la Confiabilidad puede generar ciertos inconvenientes: a) Si fuese menor, por ej. 99,9 %, el resultado sería un enlace de muy pobre Confiabilidad y b) Si fuese mayor, por ej. 99,999 %, encarecería ostensiblemente al sistema completo de enlace. El Margen de Desvanecimiento depende de la distancia del enlace, frecuencia de operación, condiciones climáticas/

terreno del trayecto, confiabilidad pretendida e inclusive para algunos métodos de obtención, de la cantidad de multitrayectorias o rebotes; en el ANEXO II se muestra un método simple de obtención. El **Margen Desvanecimiento (M_{fade})** valdrá aproximadamente (5/10 db), un valor cercano a (20 db) es sumamente crítico para un enlace. Dicho margen afectará la Ecuación de Friis, según:

$$PRX = 32,45 + \dots + G_{antRX} + G_{antTX} - M_{fade} \quad (Ec. 3.1)$$

Por tanto, la potencia recibida deberá igualar como mínimo la sensibilidad del receptor, considerando las pérdidas de coaxil y conectores; de ser menor, necesariamente habría que aumentar las ganancias de antenas y/o potencia del transmisor.

» **18) "Diversity" de Espacio o Frecuencia:** la ecuación no

contempla la posibilidad de utilizar diversidad de espacio con varias antenas receptoras o de múltiples frecuencias para evitar desvanecimientos de la señal propagada.

» **19) Técnicas "MIMO":** la ecuación tampoco contempla las técnicas MIMO (Múltiples Entradas y Múltiples Salidas) usando varias antenas en el transmisor y el receptor, pues **mejora el alcance de un enlace inalámbrico** y aprovechando el rebote de las señales propagadas.

» **20) Pérdida de obstáculo:** Friis tampoco considera la pérdida por difracción por un obstáculo de tipo "filo de cuchillo" y que además la onda se difracta en la zona de sombra, íntimamente relacionado con las Zonas de Fresnel.

» **21) Ganancia de altura:** Friis no considera el Factor correctivo en modelos de propagación (como el de

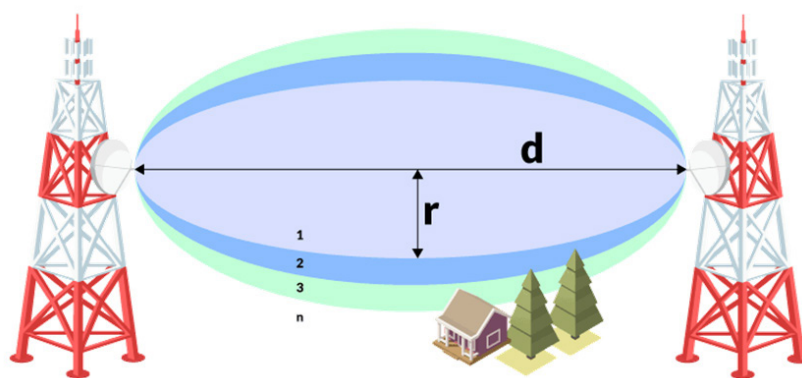


Figura 3.1 – Zonas de Fresnel

» **22) Zonas de Fresnel:** La primera zona de Fresnel transporta y concentra aproximadamente el 90% de la energía total de la señal de radio que se transmite entre dos antenas y es el volumen elipsoidal más importante para asegurar un buen enlace inalámbrico, donde las antenas coinciden con sus focos elipsoidales.

Las ondas que pasan por esta primera zona de Fresnel llegan al receptor en una fase que suma potencia a la señal principal y de manera constructiva; una obstrucción en su trayecto y superior al 40% genera una pérdida notable de la potencia recibida. La obstrucción de la primera zona de Fresnel en un enlace de radiofrecuencia provoca pérdidas por difrac-

ción y desfases de las ondas. Si un **obstáculo bloquea más del 40% de esta zona elipsoidal, la señal directa sufre una atenuación severa aunque exista línea de visión directa;** la zona mas riesgosa de obstrucción normalmente se ubica a mitad de camino del enlace donde el radio de la elipsoide de la primera zona de Fresnel es mayor. Respecto de este punto, se genera normalmente una confusión ingenieril si se refiere al ensombrecimiento de un obstáculo referida a la superficie del 40% de la sección circular (transversal) de la elipsoide o solo referido a la altura invasiva del obstáculo. Por tanto, es para **una obstrucción que apantalle el enlace al 40% de su radio (no de su diámetro ni al área) y a cualquier distancia entre antenas, independiente del grosor o forma del obs-**

táculo.

La 1° Zona de Fresnel será libre de obstáculos si se cumple $(r_2 > 60\% \cdot r_1)$ (ver-Figura 3.2).

Atenuación crítica: Una obstrucción superior al 60% añade pérdidas adicionales importantes (de 6 dB o mayor) y que degradarán gravemente la confiabilidad del enlace.

4.- Conclusiones

En el presente artículo se expusieron agudas limitaciones con la utilización de la Ecuación de Friis para el cálculo de radioenlaces y universalmente empleada desde mediados del siglo XX; además es el único método ingenieril disponible hasta el presente y restringida su utilización en condiciones ópticas ideales entre antenas y libres de obstáculos; vale considerar infinidad de factores reales que afectan el fenómeno de propagación como: tipos de antenas, polarizaciones, anchos de banda, Zona de Fresnel, reflexiones indeseadas, etc.

Por tanto, es recomendable que el ingeniero proyectista considere todas las limitaciones técnicas al utilizar el método de Friis y sus posibles implicancias en desmedro de la calidad pretendida de un radioenlace.

ANEXO I Ecuación de Friis

En este ítem se dará una explicación sucinta del procedimiento para obtener de la ecuación y considerando una fuente isotrópica emisora que sirve a los fines y que

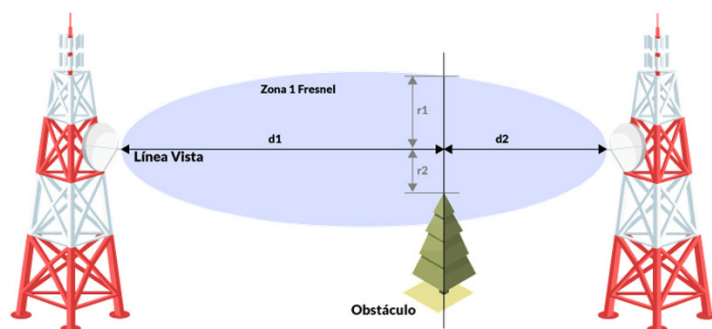


Figura 3.2 – Obstáculo en 1° Zona de Fresnel



Consejo Profesional de Ingeniería de Telecomunicaciones, Electrónica y Computación

Bioingeniería, informática, higiene y seguridad, y otras actividades afines.

“Desde 1959, asumiendo el control del ejercicio profesional en la materia, otorgando matrículas y cumpliendo así con las funciones específicas delegadas por el estado nacional”

Decreto Ley 6070/58 - Jurisdicción Nacional
Ley 6908/25 (CABA).

