

CHAPTER 1 / HSIMC BLUEPRINT

La oportunidad de los diez mil millones de teléfonos

De una ambición movilizadora a una capacidad útil y verificable

PROPOSITION

Activar diez mil millones de teléfonos es una invitación estratégica y una hipótesis de investigación, no un recuento auditado de teléfonos inactivos, seguros, accesibles o desplegables. El resultado importante es un Work útil aceptado por una persona, no un aparato meramente contado o conectado.

1.1 Obsolescencia de consumo frente a capacidad productiva restante

Un teléfono retirado del uso personal cotidiano puede conservar cámara, pantalla, micrófono, sensores, almacenamiento, conectividad o una interfaz accesible. Sustituir un producto de consumo no equivale a que haya perdido toda utilidad técnica. Sin ejecutar un gran modelo de lenguaje, puede recoger pruebas, mostrar una solicitud de consentimiento, servir como terminal supervisado o conectar una capacidad local apta a un Work autorizado.

Las funciones restantes no demuestran preparación. Hay que evaluar batería, seguridad eléctrica, soporte del sistema operativo, aislamiento de red, datos personales residuales, permisos y accesibilidad para la función concreta. Un dispositivo inseguro o imposible de proteger puede requerir reparación o reciclaje responsable. La utilidad económica o ambiental de reutilizarlo debe medirse, no darse por supuesta.

1.2 Teléfonos inactivos como puntos de partida distribuidos, no inventario centralizado

Los posibles dispositivos pertenecen a hogares, empresas, escuelas, talleres, organizaciones benéficas y otros titulares independientes. La propiedad, posesión y autorización siguen siendo suyas; HSIMC no puede considerarlos existencias bajo su control. Que un teléfono esté inactivo no significa que esté abandonado, disponible, sea transferible o seguro para registrarlo. La participación comienza con un titular identificado y voluntario y una finalidad delimitada.

Un registro de activación fiable incluye permiso del titular, descripción mínima del equipo, resultado de revisión, función propuesta y una vía clara de suspensión o revocación. Una URL o un QR pueden ser la entrada; NFC o adaptadores locales cualificados son opciones, no requisitos. No se presuponen restablecimientos universales de fábrica, acceso root, instalaciones laterales ni privilegios administrativos.

1.3 Existencias, futuras retiradas y escenarios alternativos de adopción de IA

Los indicadores de escala muestran relevancia, pero no inventario ejecutable. La UIT estimó 6.000 millones de usuarios de Internet y 2.200 millones de personas desconectadas en 2025 [E1]. GSMA registró 4.800 millones de usuarios de Internet móvil a fines de 2025 [E2]. Esas cifras miden personas con definiciones diferentes, no teléfonos disponibles para un Work. La UIT y UNITAR estimaron 62 millones de toneladas de residuos electrónicos de todas las categorías en 2022, de los que un 22,3 % constaba oficialmente como recogido y reciclado [E3]; esa masa no permite calcular teléfonos reutilizables.

El lema de los diez mil millones debe probarse como hipótesis de participación a largo plazo, nunca presentarse como diez mil millones de nodos elegibles hoy. Deben distinguirse aparatos ya guardados, próximas retiradas del uso principal, pérdidas, reciclaje y registros repetidos. Escenarios bajo, de referencia y alto necesitan cohortes observadas, deduplicación, supuestos transparentes de elegibilidad y revisión fechada, no extrapolaciones de suposiciones.

1.4 De dispositivos estimados a nodos elegibles, contribuciones activas y Work aceptado

La cadena de medida es explícita: **candidato observado** → **permiso del titular** → **equipo operable y seguro** → **interfaz accesible** → **capacidad cualificada** → **acción realizada** → **Work aceptado por una persona**. Cada paso requiere numerador, denominador, pruebas y razones de rechazo. Tener Wi-Fi no convierte el teléfono en servidor MCP; llamar bien una herramienta no equivale a entregar un servicio; terminar una acción tampoco garantiza su aceptación.

HSIMC debe medir tiempo hasta una primera prueba útil, éxito de operadores independientes, esfuerzo de supervisión, aceptaciones repetidas, coste total y tasas de fallo o retirada. Dispositivos únicos, operadores, solicitudes de Work y resultados aceptados son entidades distintas. Una cohorte pequeña con resultados replicables es evi-

dencia más sólida que muchos iconos no verificados en un mapa. Un auditor debe poder recorrer Intent, Authority, Reality, Action, Evidence, Acceptance y Continue.

En un piloto comparable, el registro separará equipo, operador, petición y decisión de aceptación. Los datos personales e identificadores se mantienen privados por defecto, y solo se conserva lo necesario y legítimo para ese Work limitado. Publicar agregados también requiere permiso. Un Work verificable posee evidencias revisables, pero no presupone que el teléfono permanezca conectado siempre.

1.5 La invitación a comenzar con el teléfono y la oportunidad de otros activos existentes

La primera invitación puede ser concreta: traer un teléfono existente, revisarlo sin acceso innecesario a datos, elegir una tarea acotada, explicar permisos y producir un resultado verificable. Un operador autorizado, por ejemplo, podría fotografiar el estado visible de un producto y remitir evidencia fechada para revisión humana. Debe poder aceptarse, rechazarse, borrarse o retirarse. Es un Work propuesto, no un despliegue acreditado.

El teléfono es la entrada, no el límite. Cables de carga y datos cualificados, identificadores NFC, soportes, sensores, informática local y servicios humanos pueden aportar condiciones que falten. Algunos casos no necesitarán ningún producto adicional; otros no deben continuar. La oportunidad de infraestructura consiste en encontrar la condición mínima que falta para un Work valioso y autorizado, y verificar allí el resultado.

La primera plantilla también necesita una auténtica barrera de rechazo: alimentación peligrosa, software sin soporte, pruebas ambiguas o retirada del consentimiento deben detener el intento y conservar solo lo permitido. Negarse correctamente forma parte de un servicio confiable. El método debería poder replicarse en idiomas, instalaciones y jurisdicciones sin traspasar propiedad, datos personales ni control empresarial a HSIMC.

WORK / DECISION TEST

Este capítulo solo avanza si un piloto real registra por separado candidatos, dispositivos autorizados, equipos seguros, capacidades utilizables y Works aceptados independientemente. Si coste, riesgo o permisos hacen peor esta vía, corresponde revisarla o rechazarla, no inflar las cifras.

PUBLIC EVIDENCE · SOURCE LINKS

[E1] International Telecommunication Union (ITU) · [Measuring digital development: Facts and Figures 2025](#) (2025)

[E2] GSMA · [The State of Mobile Internet Connectivity 2026](#) (2026)

[E3] ITU / UNITAR · [The Global E-waste Monitor 2024 \(UNITAR release\)](#) (2024)

STATUS / BOUNDARY. Propuesta de infraestructura HSIMC; no hay prueba de diez mil millones de teléfonos elegibles, aval de terceros ni permiso de despliegue.

NEXT GATE. Tras congelar el Part I inglés, alinear las seis lenguas y preparar criterios de aceptación para un Work concreto en campo.

CHAPTER 2 / HSIMC BLUEPRINT

Del uso centrado en aplicaciones a herramientas físicas guiadas por intención

Conservar la interfaz humana y hacer calculable un resultado real delimitado

PROPOSITION

Una herramienta física GenAI útil no se define por controlar una pantalla, sino por una capacidad declarada que ayuda a cumplir una intención humana específica en una Reality conocida, con autorización, evidencia y aceptación responsables.

2.1 Del manejo de una aplicación a pedir un resultado del mundo real

El modelo centrado en aplicaciones exige encontrar una app, navegar menús e interpretar resultados. Un Work guiado por intención empieza por un resultado humano: documentar una muestra, comprobar una condición, solicitar orientación accesible o conseguir una pieza útil localmente. La intención por sí misma no ordena actuar: resultado esperado, alcance permitido, responsables, entorno y criterios de aceptación deben estar definidos.

Por ejemplo, «identificar este conector» puede descomponerse en una imagen autorizada, una herramienta cualificada de identificación, evidencia de incertidumbre y una decisión que un técnico pueda confirmar. Debe poder rechazarse una identificación equivocada. La infraestructura mantiene la relación entre pedido y pruebas; una respuesta elegante no completa el Work.

2.2 Mantener interfaces humanas y exponer funciones limitadas a la IA

Las personas siguen necesitando pantallas, controles accesibles, explicaciones multilingües, consentimiento y un botón de parada visible. Diseñar desde la intención no elimina las apps ni sustituye al usuario. Una web o aplicación local puede seguir como Host que explica consecuencias, pide permiso y presenta resultados; el Client asistido por modelo elige solo herramientas calificadas.

HSIMC separa interfaz, capacidad y autoridad. Ver una cámara no es igual que modificar el sistema, borrar datos o comprar. Los actos sensibles exigen permisos explícitos, limitados y a veces otra comprobación humana. Que exista una API de automatización o un servicio de accesibilidad no autoriza a gobernar todo el teléfono.

2.3 Teléfono como sensor, interfaz, recurso de cómputo y pasarela física

Un teléfono existente puede observar, mostrar tareas, enlazar redes, ejecutar cálculo limitado o alimentar a un equipo cercano cualificado. Son papeles posibles, no promesas para cada dispositivo. Cada papel requiere revisar versiones y parches del sistema, batería y energía, conexión, sensores y cámara, permisos, protección de almacenamiento y accesibilidad.

Cuando falta alguna condición, un cable, soporte, etiqueta NFC, equipo Edge o lugar supervisado puede aportarla. Estas piezas no son automáticamente herramientas inteligentes; un cable pasivo puede ser una dependencia material sin ser servidor MCP. El Work Graph identifica contribuciones y separa compra, inspección física y prestación.

2.4 Participar en GenAI sin ejecutar un gran modelo en el teléfono

Un dispositivo puede aportar observaciones estructuradas o invocar un modelo remoto permitido sin alojarlo. No hay que descartar hardware solo porque no ejecute el modelo más nuevo. Pero la inferencia en línea implica latencia, transmisión, condiciones de cuenta, seguridad, energía y dependencias de disponibilidad. Las vías locales, híbridas y remotas se comparan con los mismos criterios de Work.

Cuando falla la conexión, la tarea puede detenerse, guardar temporalmente evidencia no sensible con permiso o emplear una vía offline probada. No debe enviar imágenes privadas sin informar ni repetir indefinidamente una acción con consecuencias. La elección depende del objetivo, sensibilidad de los datos, capacidades locales y ventana temporal humana, no de la etiqueta «IA».

2.5 Más allá de controlar apps: autorizar capacidades

Atajos de pantalla, puentes de depuración y APIs privilegiadas sirven en laboratorios autorizados, pero son malos contratos universales: permisos y conducta varían según dispositivo y sistema y pueden dar excesiva agencia.

OWASP distingue el exceso de funciones, permisos y autonomía como causas de riesgo [E4]. Se prefieren capacidades con entradas tipadas, efectos limitados y registros visibles.

Un contrato declara quién puede solicitar, qué datos se exponen, cuándo confirmar y cómo medir o revocar. Ejecutar pertenece a un Work supervisado en su Reality concreta. El cambio es pasar de «la IA puede tocar una app» a «una persona autorizada puede obtener y revisar un resultado útil mediante una capacidad declarada».

WORK / DECISION TEST

El piloto debe mostrar un Work completo: intención humana, acceso delimitado, capacidad de rechazar una llamada peligrosa, evidencia y aceptación o rechazo. Deben verse Host, herramienta, papel real del dispositivo y vía de revocación; no se contabilizan toques de pantalla como valor.

PUBLIC EVIDENCE · SOURCE LINKS

[E4] OWASP GenAI Security Project · LLM06:2025 Excessive Agency (2025)

STATUS / BOUNDARY. Propuesta arquitectónica HSIMC sin permisos universales de dispositivos, aval de apps ajenas, despliegue masivo ni Work ya aceptado.

NEXT GATE. Congelar contrato Work y prueba de consentimiento visible con Part I; evaluar un flujo local de objeto a evidencia solo con nueva autorización.

CHAPTER 3 / HSIMC BLUEPRINT

MCP como facilitador, no como sistema de producción completo

La interoperabilidad del protocolo no es preparación operativa ni entrega aceptada

PROPOSITION

MCP permite descubrir e invocar herramientas y recursos de contexto entre implementaciones, pero no establece por sí mismo el derecho de actuar, las condiciones físicas para ejecutar con seguridad ni la aceptación humana del resultado.

3.1 El cambio de protocolo del 28 de julio de 2026 y las capacidades distribuidas

La revisión MCP 2026-07-28 publicada elimina el intercambio initialize y la cabecera de sesión Mcp-Session-Id a nivel del protocolo. Cada solicitud incluye metadatos de versión y capacidades; existe descubrimiento de servidor cuando hace falta y se simplifica el enrutamiento HTTP. Es un cambio concreto, no prueba que todos los Client, Server heredados o teléfonos ya implementen esta versión [E5].

Una capacidad física cualificada puede exponerse mediante un Server autorizado sin tratar una sesión persistente de transporte como identidad. El equipo aún puede requerir calibración, operador, electricidad, permisos legales y evidencias duraderas. Para HSIMC, MCP es una capa de interoperabilidad dentro de una infraestructura más amplia de Reality y Work; las pruebas de compatibilidad deben indicar la versión real.

3.2 Descubrimiento, invocación e interoperabilidad independiente

MCP distingue herramientas invocables de recursos que aportan contexto. Un Host presenta funciones disponibles a un Client asistido por modelo, que llama una herramienta con parámetros acotados por esquema. Distintos proveedores pueden ofrecer resultados equivalentes mediante implementaciones independientes. El esquema ayuda a interoperar, pero no valida proveedores, no garantiza datos verdaderos ni concede permisos físicos [E6].

El registro de capacidad identifica herramienta y versión, proveedor, entradas, salidas, errores, límites, permisos, entorno y pruebas. Descubrir, invocar con éxito y operar de forma segura son barreras distintas. El Client valida datos recibidos y trata descripciones, anotaciones y textos no fiables como datos, no autoridad nueva; las operaciones importantes conservan aprobación humana.

3.3 Interacciones sin sesión de protocolo, identidad de Work persistente y estado físico

La comunicación sin estado implica que el protocolo no necesita una conversación oculta en el servidor entre solicitudes. No implica aplicaciones sin memoria ni tareas físicas sin estado. Un Work puede persistir mediante ID explícito, pruebas verificables, almacenamiento duradero bajo control del responsable y una referencia declarada de continuación, no porque una conexión equivalga a permiso.

El estado físico existe por separado: una batería carga, un soporte se mueve, llega un paquete o se retira el consentimiento. Antes de actuar hay que reconciliar la Reality. Perder una respuesta no debe repetir automáticamente una acción irreversible. Idempotencia, reintentos, parada, lectura independiente y control humano pertenecen al contrato de Work, con o sin sesiones de transporte.

3.4 Conformidad de protocolo, preparación del equipo y entrega aceptada son hitos distintos

Se requieren tres pruebas. **Conformidad:** Client y Server intercambian mensajes válidos en una versión indicada.

Preparación de Reality: equipo, lugar, entrada, adaptador, seguridad y autorización sirven ahora para la tarea.

Entrega aceptada: la evidencia satisface reglas humanas u organizativas específicas de aceptación.

Pasar una no permite suponer las otras. Wi-Fi o tools/list no demuestran permiso de cámara, energía segura ni derechos comerciales. Y una demostración manual puede aportar pruebas reales sin constituir un producto MCP conforme. Fallos y negativas correctas son resultados valiosos que deben registrarse, no ocultarse para inflar nodos.

3.5 Conformidad fechada y antigua base del piloto Sony

El recorrido Sony de referencia de HSIMC es una investigación histórica, no una prueba automática de conformidad posterior. Hay que conservar fecha, hardware, transporte, revisión de software, alcance y justificante original

de cada experimento. Si un prototipo empleaba handshake MCP anterior o un adaptador propio de app, debe etiquetarse así. MCP 2026-07-28 contiene cambios incompatibles; migrar exige otro Work verificable, no cambiar etiquetas retrospectivamente [E5].

El nuevo piloto informa la versión declarada o acordada, identidad autenticada, conjunto mínimo de herramientas, decisión de consentimiento, acción visible, huella digital de evidencia, conducta ante fallos y aceptación independiente. «MCP-ready» solo vale para la configuración probada. La meta es cooperar según contratos inspeccionables, no prometer compatibilidad universal por usar un término.

WORK / DECISION TEST

En una configuración expresamente autorizada, demostrar separadamente intercambio MCP de versión indicada, preparación física segura y Work revisado por otra persona. Un éxito parcial no acredita un despliegue productivo.

PUBLIC EVIDENCE · SOURCE LINKS

- [E5] [Model Context Protocol Core Maintainers · The 2026-07-28 Specification](#) (2026)
- [E6] [Model Context Protocol specification · 2026-07-28 Tools](#) (2026)

STATUS / BOUNDARY. Afirmaciones de protocolo fechadas en MCP 2026-07-28; no se presume conformidad de Sony u otros equipos ni aval de socios o ampliación de permisos.

NEXT GATE. Aplicar las tres barreras en los capítulos 11, 16–18 y 30; abrir un registro de aceptación específico antes de ejecución física.