

Activación mundial: trae un teléfono y sal con una capacidad verificada

C0-015-PART-V-6L · 19 original TOC sections · English master frozen for this edition · AI-assisted translations (professional review pending)

Activar una capacidad. Preservar la autoridad humana. Entregar evidencias.

La activación de diez mil millones de teléfonos es una invitación a crear productividad con cosas que la humanidad ya posee, no un censo de diez mil millones de dispositivos aptos. HSIMC plantea un camino desde el móvil, NFC o un acceso compartido hasta una capacidad local cualificada y un resultado aceptado por una persona. Una prueba que falla con una negativa segura también produce conocimiento útil.

Que nadie se quede atrás exige más que una App atractiva. Quien no disponga de NFC, conexión continua, teléfono reciente o siquiera móvil debe tener, cuando exista servicio, opciones de QR, voz y asistencia local. Un modelo de IA y un cliente MCP pueden proponer o llamar a herramientas definidas; no crean derechos de propiedad, señal móvil, seguridad de batería ni consentimiento.

CHAPTER 13 / LOCAL COMMISSIONING & HUMAN REALITY

13. Una red local de puesta en servicio para participar globalmente

Métodos repetibles en todo el mundo, entregados por personas e instalaciones locales responsables

PROPOSITION

El alcance mundial surge de muchas activaciones locales, independientes y autorizadas, no de que HSIMC posea todos los teléfonos. Poner en servicio es un trabajo medible: entender el fin humano, cualificar el equipo, configurar sólo lo acordado, verificar una capacidad limitada y entregar un comprobante comprensible.

13.1 Rutas de activación de autoservicio, asistidas y profesionales

En autoservicio, el propietario puede seguir instrucciones para una App compatible, entrada web segura, permisos mínimos y una prueba de capacidad. La ruta asistida añade profesional formado y accesibilidad para quien no puede usar botones pequeños, formularios largos o Internet constante. Cableado, cambios de OS, calibración, trabajo regulado y recuperación de información requieren expertos competentes.

Las tres rutas comparten lógica de aceptación, con distinto grado de ayuda y seguridad. Quien solicita el servicio elige un fin limitado y puede negarse sin perder información pública. Activar no significa publicar todo el móvil mundialmente. Una persona que sólo trae una tarea puede usar una estación compartida apta, sin contarla como activación de un equipo de su propiedad.

13.2 Estaciones de activación autorizadas y quioscos de puesta en servicio tipo cajero automático

El concepto de estación similar a un cajero ofrece atención accesible, no derecho a tomar teléfonos o reflashearlos. En escuela, taller, reparación o Hub confiable podría explicar opciones, comprobar a quién pertenece el aparato, examinar interfaces y mostrar una aprobación o denegación visible. Cada sesión se vincula con operador y lugar responsables, incluye aviso de privacidad y devuelve el móvil sin gestión permanente no autorizada.

El servicio necesita mantenimiento de seguridad, energía segura, tratamiento confidencial, acceso físico, idiomas y atención humana. QR y NFC abren información, no demuestran propiedad. El aprovisionamiento NFC de Android Enterprise es un proceso distinto con posibles privilegios potentes de administrador [E1]; jamás debe confundirse con tocar una etiqueta URL para leer una explicación.

13.3 Comprobar titularidad y estado; conservar o borrar datos sólo con autorización

Antes de tratar información privada hay que comprobar legítimo dueño o custodio, objetivo y permiso concedido. Inspeccionar batería, carga, golpes, OS, parches, memoria, radios, puertos, accesibilidad y políticas de empresa o escuela. La posesión temporal del teléfono por un técnico no autoriza abrir cuentas, copiar fotos, instalar gestión corporativa ni transferir roles e-Person.

Los datos permanecen por defecto bajo control del titular. Copias, exportaciones, traslados y borrado precisan elección informada y comprobación independiente. Desbloquear bootloader Android puede exigir aceptación y restablecimiento de fábrica, afectando la seguridad [E4]. No prometer flasheo universal sin pérdida de datos ni imponer borrado oculto para ayuda normal. Si es peligroso, está administrado por tercero o no admite soporte, detenerse y ofrecer alternativa.

13.4 Aprovisionar, vincular, probar, explicar controles y emitir recibo de activación

Instalar un paquete no completa la activación. Registrar equipo y compilación, Work permitido, sitio y tiempo, adaptador o MCP realmente usado, Human Supervisor, límites de datos y salida y modo de revocación. Ejecutar la prueba acordada con lectura de vuelta: observación limitada de batería, escritura NFC NDEF seguida de lectura independiente, o entrega accesible de información comprobada.

El comprobante separa DEVICE_INSPECTED, APP_INSTALLED, TOOL_REACHABLE, HUMAN_GRANT_VALID, CAPABILITY_VERIFIED y WORK_ACCEPTED; una etapa no certifica la siguiente. Registrar versión, fecha, consentimiento, entrada, salida observada, fallos, evidencia, coste, operario y contacto sin publicar secretos. Explicar cómo repetir, pausar, revocar o pedir ayuda. Si la prueba falla, entregar un rechazo sincero o requisitos aún no cumplidos.

[Non-executable local commissioning receipt template ↗](#)

13.5 Servicio prestado localmente con métodos de ingeniería reutilizables en todo el mundo

El activo escalable es un método reproducible: lista de aptitud, Capability Contract limitado, guion accesible, comprobante, prueba de reinicio y razones de parada. Operadores independientes de distintas ciudades pueden usar idiomas oficiales, proveedores propios permitidos y entregar resultados comparables. Talleres, universidades y asociaciones pueden contribuir sin ceder marca, clientes ni identidad empresarial a HSIMC.

Los ejemplos públicos describen condiciones y lecciones no sensibles, sin números de serie personales ni credenciales. La federación mundial surge de capacidades verificadas en la Reality correspondiente. Medir comprensión, tiempo, aceptación y replicabilidad en lugar de Apps instaladas. Capacitación, seguro pertinente, ayuda humana y remuneración justa son parte del servicio; la inclusión vale incluso sin ingresos comerciales.

WORK / HUMAN ACCEPTANCE TEST

Capítulo 13 pasa cuando una estación independiente demuestra titularidad, consentimiento, estado medido, permiso limitado, lectura real de capacidad y comprobante comprensible; un equipo incompatible obtiene rechazo seguro documentado o vía asistida.

14. Múltiples rutas de mejora, no un flasheo universal

Elegir una ruta apropiada sin sacrificar datos o seguridad de la persona

PROPOSITION

Un móvil antiguo puede ser útil sin sistema operativo nuevo. HSMC debe comparar instalación mínima, configuración dedicada, flasheo autorizado en pocos equipos aptos, operación mediada por Hub y reutilización de partes. Elegir siempre la opción menos invasiva que satisfaga el Work.

14.1 Instalar una aplicación MCP-ready limitada sobre un sistema ya compatible

Muchas veces conviene mantener el Android u otro OS soportado e instalar, donde permitan las políticas, una App de permisos limitados o servidor MCP local. El dueño conserva los controles del sistema mientras ofrece una función evaluada como estado, NFC o asistencia accesible. Verificar en el modelo real características de OS, permisos, origen del paquete, red y servicios de fondo.

La investigación Sony H4493 confirmó ciertas lecturas MCP limitadas, mientras NFC Writer y gafas USB requieren sus propios ensayos [H2]. No significa que un APK convierta cualquier móvil antiguo en AI Node confiable. El operador indica qué funciona, qué pide interacción y qué está fuera de soporte. Sistema desactualizado o privilegio excesivo exige detenerse, no etiquetar READY.

14.2 Configuración dedicada cuando el sistema operativo la permite

Una institución que posee legítimamente un dispositivo apto puede configurarlo como quiosco supervisado, aula o terminal especializado. Android Enterprise distingue work profile, fully managed y dedicated devices según propiedad, versión y método de alta [E1]. Son funciones de gobierno empresarial, no permiso para gestionar el teléfono personal de un visitante como propiedad de la institución.

El comisionador debe explicar quién define políticas, cómo se aísla el contenido personal, cómo sale el usuario y cómo se recupera o devuelve. El Hub compartido requiere cuentas restringidas, herramientas mínimas, límites de sesión y borrado autorizado. Si el móvil personal no puede matricularse legalmente, utilizar navegador o servicio asistido en Hub.

14.3 Reemplazo de OS o flasheo por el propietario en dispositivos elegibles

Cambiar OS sólo puede justificarse en modelos muy concretos y constituye una intervención de alto riesgo. Se requiere bootloader compatible, imágenes y controladores específicos, aprobación del dueño, plan de recuperación, procedencia firmada y explicación sobre pérdida de datos, garantía y amenazas. Verified Boot y protección anti-rollback defienden contra imágenes maliciosas y versiones vulnerables; no deben desactivarse para una presentación [E4, E5].

Según Android, desbloquear bootloader donde se permite exige confirmación del usuario y borrado de fábrica [E4]. No prometer preservar fotos, banca ni administración empresarial en un flasheo universal; tampoco saltarse restricciones de terceros. Muchos equipos carecen de vía segura o legal. Si falta soporte, plan de vuelta o voluntad del titular, STOP y pasar a App limitada o Hub.

14.4 Participación mediante Hub cuando el teléfono no puede operar solo con seguridad

Un móvil básico o sin soporte quizá sólo pueda mostrar información, aportar voz, cámara consentida, QR/NFC o entrada local, mientras Hub cualificado asume cálculo, red y Work persistente. Si incluso esos usos son inseguros, proporcionar estación compartida o ayuda humana. La cercanía de un Hub no le entrega archivos privados ni permiso universal sobre otros dispositivos.

El contrato Hub precisa quién aporta observaciones, quién recibe datos, qué servicios remotos se usan y quién acepta resultado. Offline sólo se continúa dentro del permiso local vigente; sincronizar después cuando sea lícito. Modelo de nube inaccesible, falta de datos móviles o alimentación insuficiente son limitaciones reales a declarar y no fallos que puedan ocultarse.

14.5 Recuperación, reversión, decisiones de dispositivo incompatible y retirada responsable

Cada mejora necesita desinstalación o parada, revocación de credenciales, restauración, verificación de copia y reinicio tras fallo de energía. Probar instalaciones fallidas, pérdida de red, reinicios, peticiones duplicadas y servicios caídos. Verified Boot y anti-rollback pueden impedir volver a un Android antiguo y vulnerable [E5]; una reversión universal no es una promesa segura.

Sin recuperación responsable, declarar UNSUPPORTED_FOR_THIS_WORK. No mantener viejos equipos sin parches conectados con puertos de control abiertos para inflar activaciones. Reparación certificada, uso desconectado de componente seguro o reciclaje legal pueden ser mejores. El recibo de retirada documenta datos y cadena de custodia para proteger al titular y a próximos usuarios.

14.6 Conservar el equipo, reutilizar subsistema o integrar mediante Hub

El valor puede residir en todo el móvil como pantalla accesible, en cámara o display reutilizados con adaptador probado, en cable o sensor independiente, o en Hub que sustituye al equipo. Seleccionar según interfaz, límites eléctricos, software, seguridad, fijación, costes reales y responsable de mantenimiento, no por atractivo de desmontar un dispositivo.

Manipular componentes puede dañar batería, conectores o carcasa protectora. No improvisar puentes de batería ni adaptadores de alta tensión sin validar. Comparar reutilización con reparación, transporte, repuestos y recuperación de materiales; el ahorro ambiental necesita datos de ciclo de vida comparables. Dar trabajo nuevo a cosas existentes no obliga a reconectar todos los residuos electrónicos.

WORK / HUMAN ACCEPTANCE TEST

Capítulo 14 pasa si se justifica la ruta, se muestra consentimiento y recuperación segura, y se rechaza reflasheo o uso en línea cuando seguridad, compatibilidad o datos no permiten cualificar el aparato.

15. Hacer trabajar activos existentes donde viven y trabajan las personas

El último metro de la Reality física determina la utilidad de la infraestructura global

PROPOSITION

Una capacidad que sólo aparece en laboratorio o vídeo publicitario no es infraestructura humana local. Hay que verificarla en lugar y momento reales con energía, datos, montaje, accesibilidad, seguridad, recuperación y responsables de operación y aceptación.

15.1 Compatibilidad por capacidad probada, configuración y condiciones operativas

La compatibilidad corresponde a una Capability específica en una Reality determinada, no al logo genérico NFC o MCP. Registrar modelo, versión, adaptador, red, interacción, firmware, ambiente y evidencia. Un teléfono puede leer NFC sin escribir cierto tag; abrir una URL quizá requiere otro toque. Android ha modificado la gestión de enlaces web NFC según versión, razón para probar el recorrido con el sistema real [E3].

Construir matriz de comportamiento observado, no catálogo de combinaciones imaginadas. Leer NFC no garantiza producto auténtico, contrato ni permiso de actuar. Cuando tag, lector, navegador o red fallan, mantener QR, URL corta HTTPS, voz y ayuda humana. Una alternativa confiable es también una capacidad que merece prueba.

15.2 Batería, energía, temperatura, soporte y operación prolongada

Un móvil jubilado sometido a carga continua trabaja distinto al uso ocasional. Inspeccionar batería hinchada o dañada, carga, calor sostenido, valores nominales de cable y conector, soporte físico y reinicio tras corte. Usar alimentación aprobada y evaluación eléctrica cuando corresponda. Calor o batería deteriorada nunca justifican desactivar protecciones del fabricante.

Definir ciclo de trabajo, ambiente, tiempo de pantalla, conexión y mantenimiento. Para quioscos públicos o control físico continuo, considerar fuente cualificada, Hub o dispositivo específico y no convertir un móvil viejo en controlador industrial sin vigilancia. Establecer las condiciones de parada antes del primer ensayo no atendido.

15.3 Combinar periféricos, conectividad y energía sin presumir compatibilidad

USB-C no garantiza host USB, webcam, HDMI/DisplayPort Alt Mode, Ethernet ni carga simultánea. Todo depende de OS, controlador, accesorio, presupuesto de energía, drivers y negociación del cable. Las API USB Host de Android ofrecen enumeración y permisos, pero no capacidad automática para operar cualquier periférico [E2].

Separar rutas de alimentación, red, datos y seguridad. Probar cámara o gafas con App, permisos, lectura de fotogramas, conservación de imágenes y recuperación propias; un éxito NFC no demuestra capacidad de vídeo. Un relé de baja tensión requiere comprobación de carga, aislamiento y parada independiente. Un modelo lingüístico nunca debe enviar órdenes de hardware sin límites.

15.4 Red intermitente, reintentos, parada segura y reinicio

El servicio local debe respetar la conectividad real. Work puede comenzar fuera de línea en estación confiable, guardar evidencia autorizada y sincronizar después con el mismo Work ID. Separar reintentos automáticos de nuevas peticiones humanas, guardar sólo lo permitido y dejar estado explícito si faltan autenticación, servicios o supervisor remoto.

Probar cortes de Wi-Fi, datos móviles, alimentación, App, espera de Tool, expiración de token, cancelación y cambio de operario. La recuperación lee el estado actual y no acepta un éxito textual de una sesión pasada. Ante actuación física, control local validado aplica parada segura y una persona nombrada puede intervenir.

15.5 Actualizaciones firmadas, reparación, respuesta a vulnerabilidades y fin de soporte

Un nodo útil puede dejar de ser seguro cuando cesan parches, fallan bibliotecas o componentes o cambia una API del fabricante. Necesita software de origen conocido, verificación de actualizaciones, cuenta limitada, gestión local de credenciales, respuesta a incidentes y responsable de mantenimiento. Verified Boot, firma y anti-rollback reducen riesgos específicos, no garantizan seguridad eterna [E5].

No imponer una política común de actualización a propietarios privados y talleres independientes. Publicar límites de soporte y migración por capacidad, distinguiendo instalación voluntaria de gestión empresarial. Suspender nodo comprometido sin borrar historia Work legítima. Si no puede funcionar conectado de forma segura, usarlo sin red, pasar al Hub o retirarlo.

15.6 Energía y datos estables en el puesto humano, no sólo en la fuente

Las fichas citan potencia nominal de cable o cargador, pero importa tensión y señal medidas en el dispositivo bajo carga. Longitud, resistencia del cobre, conectores, salidas USB-C compartidas, negociación, ruido y desgaste afectan cámara, Hub y móvil. Una etiqueta 100 W no asegura energía estable a dos dispositivos conectados ni datos sin interrupciones.

Medir tensión, temperatura, roles USB, funcionamiento continuo y comunicación en el lugar de uso, no únicamente en el cargador. Para comparar conservar calibración de instrumentos y trazas. La trayectoria de Pannex en productos físicos puede apoyar cables cualificados, pero una relación histórica o una lectura aislada no otorga derechos ajenos ni certificación mundial.

15.7 Ajuste mecánico, interacción accesible, recuperación y salvaguardas independientes

El equipo debe adaptarse a persona, lugar y tarea: alcance, agarre, ayudas visuales o auditivas, legibilidad, respuesta de voz o tacto, altura, cables en el suelo, parada de emergencia, limpieza, vibración y ambiente. Una estación compartida debe permitir comprender permisos, elegir una alternativa y hablar con un humano sin memorizar comandos.

Si se unen IA, mecanismo móvil y usuario con necesidades de apoyo, la seguridad independiente es decisiva. Consentimiento, autorización informática e interbloqueos físicos son tres sistemas distintos; ensayar parada e aislamiento fuera del modelo. Rechazar instalaciones inaccesibles o peligrosas aunque el Demo funcione. La meta es vida autónoma y elección productiva, no obligar a adaptarse a la máquina.

15.8 Fabricación de investigación a escala de oficina: procesos y límites verificados

Una sede de investigación HSMC puede preparar soportes, etiquetas, adaptadores de baja tensión cualificados y piezas de prueba bajo herramientas y supervisión adecuadas. Puede recurrir a especialistas para mecanizado, trabajos eléctricos, óptica, accesibilidad o materiales. Esto no convierte cualquier oficina, biblioteca o escuela en taller autorizado para todos los procesos y residuos peligrosos.

Cada piloto consigna proceso, origen de material, límites de equipo, operario, protección, permisos, salida medida y aceptación. Accessible Product Passport neutral NFC/QR y Human-Guided Circular Work con pieza poco peligrosa son candidatos. Marcas FIFA, contenido licenciado, baterías peligrosas, productos médicos o maquinaria crítica tienen procedimientos independientes. La evidencia repetible posibilita expansión responsable.

WORK / HUMAN ACCEPTANCE TEST

El capítulo 15 pasa cuando un segundo lugar reproduce la capacidad bajo condiciones físicas medidas —energía, datos, montaje, acceso, recuperación, autoridad y seguridad— y sabe explicar un rechazo. La participación global sólo crece a partir de Works locales aceptados.

Evidence register and technical boundary

1. [H0] HSMC C0-009-6L · Immutable 30-chapter Table of Contents — Original Part V chapter and subsection identities.
2. [H1] HSMC C0-014 · e-Person and Work Graph (Part IV) — Persistent Work, bounded Human Authority and actual Reality qualifications.
3. [H2] HSMC Android/Sony/MCP Phone and NFC Writer engineering handoffs — Different bounded research states; no universal read/write or camera execution acceptance.
4. [H3] HSMC Part III · Phone, Capability Contracts, Human Authority — Protocol invocation distinct from local physical and human authorization.
5. [E1] Google · Enroll and provision Android devices — Personal ownership versus company-managed/dedicated provisioning and scope.
6. [E2] Android Developers · USB host overview — Hardware/OS support and explicit USB permissions.
7. [E3] Android Developers · NFC basics — NDEF handling and version-dependent URL dispatch, not identity or Work authorization.
8. [E4] AOSP · Lock and unlock the bootloader — User confirmation, unlocking effects and factory data reset risk.
9. [E5] AOSP · Verified Boot — Integrity and rollback security requirements.
10. [E6] ITU · Facts and Figures 2025 — Global inclusion context; not a measured inventory of reactivatable phones.

Claims and source scope ↗

STATUS / BOUNDARY. La Parte V es un plan de investigación para puesta en servicio local consentida. Diez mil millones es una invitación, no inventario auditado. Quien carece de móvil o Internet quizá necesite estación compartida. Traducciones asistidas por IA pendientes de revisión profesional. Este documento no administra ningún teléfono, SIM, bootloader ni ejecución externa.

NEXT GATE. Congelar el inglés de Part V, alinear los cinco idiomas con sus 19 secciones, validar seis PDF A4 y HTML y publicar nueva versión sólo tras aceptación de SHA/HTTPS/navegador y sin modificar la historia editorial.