Gobernación de Cundinamarca

DOCUMENTO DE ARQUITECTURA DE SOFTWARE

Kiosco de Impuestos Bogotá y Cundinamarca

Consulta · pago en portales oficiales · impresión segura · aislamiento de sesiones

Versión	1.0
Estado	Arquitectura base para construcción
Fecha	29 de septiembre de 2026
Plataforma objetivo	Windows 11 · pantalla táctil · HP LaserJet M111w USB
Tecnología base	C# · .NET 10 LTS · WPF · Microsoft Edge WebView2

> Decisión arquitectónica principal: el kiosco NO procesa directamente datos financieros ni reemplaza los portales tributarios. Controla la experiencia local, la sesión, la navegación, la impresión y el bloqueo del sistema operativo; el cálculo del impuesto, CAPTCHA, pago y confirmación permanecen en los sistemas oficiales.

Calle 26 #51-53 Bogotá D.C.
Sede Administrativa - Torre Beneficencia Piso 4.
Código Postal: 111321 – Teléfono: 749 1692
/CundiGob @CundinamarcaGob
www.cundinamarca.gov.co

0. Decisiones ejecutivas y puntos de control

Decisión	Definición
Runtime	Adoptar .NET 10 LTS para iniciar el desarrollo en 2026. .NET 10 tiene soporte LTS hasta noviembre de 2028; .NET 8 finaliza soporte en noviembre de 2026.
UI de escritorio	WPF sobre .NET 10 por estabilidad, madurez, interoperabilidad con Windows y menor complejidad operacional para un kiosco dedicado.
Navegación web	Microsoft Edge WebView2 embebido, sin automatizar ni modificar el DOM de los portales oficiales salvo necesidades técnicas expresamente aprobadas.
Lockdown de producción	Windows Shell Launcher + Keyboard Filter + cuenta estándar dedicada. Para este nivel de bloqueo se requiere Windows 11 Enterprise/Education/IoT Enterprise o equivalente compatible.
Sesión	Sesión efímera: limpieza completa de datos de navegación, descargas temporales y contexto del usuario al finalizar o por inactividad.
Pago	La aplicación nunca reenvía automáticamente un pago ni deduce el resultado de una transacción ante pérdida de conectividad; el estado válido lo determina el portal/pasarela.
Impresión	HP LaserJet M111w por USB; impresión silenciosa desde WebView2/Windows Print Spooler y manejo de estados disponibles por el driver.
Backend	No se requiere backend propio para el alcance inicial. La solución es local y parametrizable. Monitoreo centralizado de flota queda como evolución futura.

Punto bloqueante antes de producción: confirmar la edición exacta de Windows 11 instalada en los StarPOS. Assigned Access está disponible en Pro, pero Shell Launcher y Keyboard Filter —necesarios para el hardening planteado— tienen requisitos de edición más altos. Si el equipo trae Windows 11 Pro, se debe validar licenciamiento/upgrade o aceptar un perfil de seguridad inferior.

0.1 Alcance cubierto por esta arquitectura

- Pantalla Home táctil y parametrizable por ubicación.
- Bogotá: acceso a flujos Vehicular y Predial en la Oficina Virtual SHD.
- Cundinamarca: acceso al portal de impuesto vehicular entregado como alcance base.
- Navegación hacia pasarelas/bancos existentes iniciada por los portales oficiales.
- Impresión de factura para pago en banco y/o comprobante/recibo posterior al pago.
- Manejo de impresora no disponible, reintento y mensajes de mantenimiento.
- Teclado táctil de Windows; no se consideran periféricos adicionales.
- Reset por inactividad, aislamiento entre ciudadanos y limpieza de datos.
- Arranque automático, recuperación ante cierre y bloqueo de acceso al sistema operativo.

Calle 26 #51-53 Bogotá D.C.
Sede Administrativa - Torre Beneficencia Piso 4.
Código Postal: 111321 – Teléfono: 749 1692
/CundiGob @CundinamarcaGob
www.cundinamarca.gov.co

- Manejo controlado de pérdida de Internet; no existe modo offline para consulta/pago.
- Logging técnico sin PII, configuración local protegida y paquete de instalación.

1. Contexto, objetivos y alcance funcional

1.1 Objetivo

Construir una aplicación de kiosco para Windows que simplifique y asegure el acceso de ciudadanos a los portales tributarios oficiales, permita completar consultas y pagos ofrecidos por dichos portales, e imprima facturas o comprobantes sin exponer el sistema operativo ni información de una sesión a la siguiente.

1.2 Usuarios objetivo

El diseño prioriza personas con baja familiaridad digital, adultos mayores y población rural. La aplicación propia debe reducir decisiones, evitar lenguaje técnico y ofrecer acciones grandes, inequívocas y recuperables. Los formularios internos de los portales externos no son controlados por este proyecto.

1.3 Flujos funcionales

ID	Flujo	Resultado
F-01	Inicio / selección	El ciudadano ve solo los trámites habilitados para el perfil del kiosco.
F-02	Consulta de impuesto	El kiosco abre el portal oficial correspondiente en un WebView2 controlado.
F-03	Pago en línea	El portal redirige a su pasarela/banco; el kiosco conserva el aislamiento y las políticas de navegación.
F-04	Imprimir para banco	Se imprime la factura/recibo generado por el portal para pago presencial.
F-05	Imprimir comprobante	Se imprime el documento disponible después del pago cuando el portal lo ofrezca.
F-06	Finalizar sesión	Se cierra la navegación, se eliminan datos temporales y se retorna a Home.
F-07	Inactividad	Se muestra advertencia y, si no hay respuesta, se finaliza y limpia la sesión.
F-08	Falla de red	Se muestra mensaje; se permite reintentar o finalizar. No se reenvían pagos automáticamente.
F-09	Falla de impresora	Se informa indisponibilidad y se permite reintentar. La reparación física queda en mantenimiento.
F-10	Reinicio / crash	El kiosco recupera el Home automáticamente al reiniciar Windows o al terminar inesperadamente la app.

1.4 Fuera de alcance

- Desarrollo o modificación de los portales de Bogotá, Cundinamarca, bancos o pasarelas.

Calle 26 #51-53 Bogotá D.C.
Sede Administrativa - Torre Beneficencia Piso 4.
Código Postal: 111321 – Teléfono: 749 1692
/CundiGob @CundinamarcaGob
www.cundinamarca.gov.co

- Implementación de una nueva pasarela, adquirencia, conciliación o reglas tributarias.
- Captura, almacenamiento o analítica de datos de tarjeta/cuenta bancaria.
- Operación offline del impuesto o del pago.
- Mantenimiento físico de kiosco, impresora, papel, tóner o conectividad.
- Corrección del responsive o accesibilidad interna de portales externos.
- MDM, monitoreo centralizado de flota y despliegue masivo; quedan previstos como evolución.

2. Drivers y atributos de calidad

2.1 Prioridades

Prioridad	Atributo	Objetivo arquitectónico
1	Seguridad	Aislar ciudadanos, limitar navegación, impedir acceso al SO, no almacenar información financiera y minimizar PII.
2	Usabilidad y accesibilidad	Flujo simple, táctil, legible y recuperable para usuarios de baja alfabetización digital.
3	Resiliencia / disponibilidad	Autorecuperación, degradación controlada ante Internet/impresora y retorno consistente a Home.
4	Mantenibilidad	Configuración por perfiles, separación por componentes y pruebas automatizadas de reglas críticas.
5	Observabilidad	Logs técnicos útiles para soporte, sin capturar datos tributarios o financieros.
6	Rendimiento	Interacción local inmediata; el tiempo de portales externos se reporta sin bloquear la app.

2.2 Escenarios de calidad medibles

ID	Escenario	Criterio
QA-SEC-01	Un ciudadano termina la sesión.	Antes de mostrar Home se limpian cookies, DOM storage, caché, autofill, historial, permisos y archivos temporales de esa sesión.
QA-SEC-02	Se intenta abrir una URL no autorizada o un popup.	La navegación se bloquea; no se abre navegador externo ni aplicación asociada.
QA-SEC-03	El usuario intenta Alt+Tab, Win, F12, Ctrl+P u otros accesos.	En producción, las combinaciones definidas no permiten escapar del kiosco ni abrir herramientas.
QA-USE-01	Usuario en Home.	Cada trámite se identifica con texto claro y un control táctil de al menos 64×64 px equivalentes; sin doble clic, hover o gestos obligatorios.
QA-USE-02	Usuario queda inactivo.	Se avisa antes del cierre y se ofrece una única acción “Continuar”.

Calle 26 #51-53 Bogotá D.C.
Sede Administrativa - Torre Beneficencia Piso 4.
Código Postal: 111321 – Teléfono: 749 1692
/CundiGob @CundinamarcaGob
www.cundinamarca.gov.co

ID	Escenario	Criterio
QA-RES-01	Kiosk.App termina inesperadamente.	El shell la relanza automáticamente y vuelve a Home sin reutilizar la sesión anterior.
QA-RES-02	Se pierde Internet durante navegación/pago.	No se repite automáticamente ninguna solicitud de pago; se informa que el estado debe confirmarse con el portal al recuperar conexión.
QA-RES-03	Impresora no disponible.	La app no reinicia el flujo de pago; ofrece reintento de impresión y registra el error técnico.
QA-PERF-01	App iniciada.	Home visible ≤ 5 s en hardware objetivo, excluyendo arranque de Windows.
QA-PERF-02	Finalización de sesión.	Retorno a Home con limpieza completada ≤ 10 s en condiciones normales.

3. Arquitectura de alto nivel

3.1 Diagrama de contexto

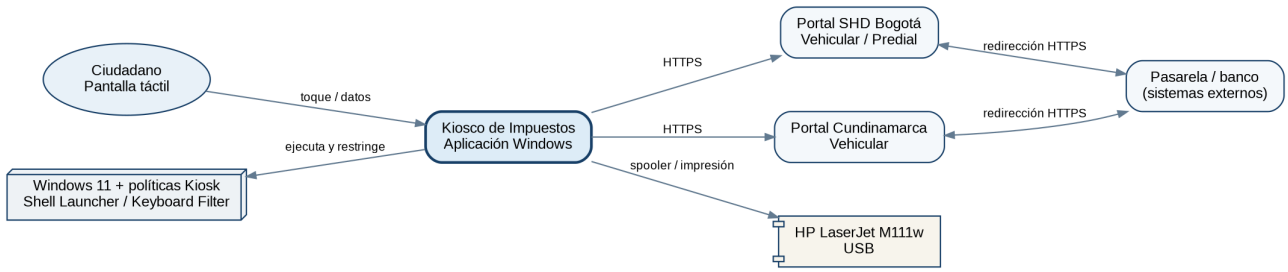


Figura 1. Contexto del sistema y dependencias externas.

La aplicación actúa como mediador local. Los portales oficiales y sus pasarelas continúan siendo los sistemas de registro para obligaciones, pagos y comprobantes. La impresora y Windows son dependencias locales controladas por la solución.

Calle 26 #51-53 Bogotá D.C.
Sede Administrativa - Torre Beneficencia Piso 4.
Código Postal: 111321 – Teléfono: 749 1692
/CundiGob @CundinamarcaGob
www.cundinamarca.gov.co

3.2 Arquitectura lógica

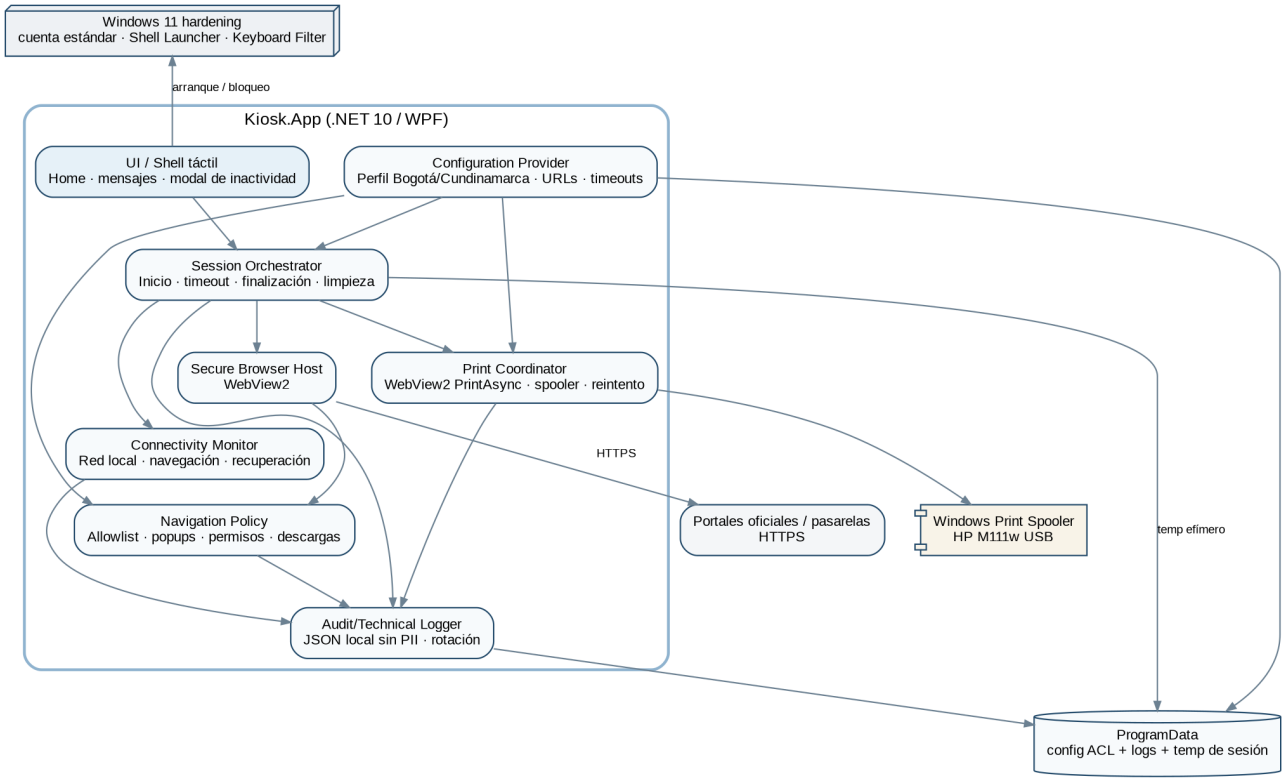


Figura 2. Componentes lógicos dentro del equipo kiosco.

3.3 Componentes

Componente	Responsabilidad principal
Kiosk.UI	Home, marco de navegación, mensajes, diálogos de confirmación, accesibilidad y feedback.
Session Orchestrator	Máquina de estados, inicio/fin de sesión, timeout, cleanup y coordinación de errores.
Secure Browser Host	Inicialización y operación de WebView2 con perfil controlado.
Navigation Policy	Valida scheme/host, controla popups, descargas, permisos y navegación a destinos permitidos.
Print Coordinator	Detecta impresora configurada, envía a impresión silenciosa, serializa trabajos y maneja reintentos.
Connectivity Monitor	Diferencia falta de red local de error de navegación y aporta estado a la UX.
Configuration Provider	Carga y valida perfil del kiosco, URLs, dominios, impresora, timeouts y políticas.
Technical Logger	Eventos estructurados locales, correlación por sesión y sanitización de PII.

Calle 26 #51-53 Bogotá D.C.
Sede Administrativa - Torre Beneficencia Piso 4.
Código Postal: 111321 – Teléfono: 749 1692
/CundiGob @CundinamarcaGob
www.cundinamarca.gov.co

Componente	Responsabilidad principal
Windows Kiosk Hardening	Cuenta estándar, auto logon, shell dedicado, filtro de teclado, ACL y políticas del equipo.

4. Decisiones de arquitectura (ADR)

ADR	Decisión	Justificación
ADR-001	C# + .NET 10 LTS	Versión LTS vigente para un desarrollo nuevo en 2026; evita iniciar con .NET 8 próximo a fin de soporte.
ADR-002	WPF como shell UI	Madurez, estabilidad y compatibilidad directa con Windows/WebView2/impresión; reduce riesgo frente a alternativas más nuevas.
ADR-003	WebView2 Evergreen	Motor Edge actualizable y soporte oficial de impresión programática, control de navegación y perfiles.
ADR-004	Sin backend propio	El alcance no requiere persistir negocio. Menor superficie de ataque, costo operativo y dependencia de infraestructura.
ADR-005	Configuración por perfil	Un mismo binario sirve para Bogotá/Cundinamarca; cambian opciones y allowlists mediante configuración protegida.
ADR-006	Sesión efímera y limpieza completa	Reduce el riesgo de que cookies, autocompletado, storage o documentos queden visibles al siguiente usuario.
ADR-007	Shell Launcher + Keyboard Filter en producción	Bloqueo más fuerte para aplicación Win32/WPF y combinaciones de teclas; requiere edición Windows compatible.
ADR-008	Impresión sin visor externo	Evita abrir Acrobat/Edge/Explorer fuera del shell. Se imprime con WebView2 y Windows Print Spooler.
ADR-009	No automatizar pagos	No hacer scraping, auto-submit ni reintentos de POST de pago. Reduce riesgo de duplicidad y alcance de seguridad.
ADR-010	Logs sin PII por diseño	URLs se registran sin query/fragment y no se capturan campos, documento, placa, CHIP ni datos financieros.

Calle 26 #51-53 Bogotá D.C.
Sede Administrativa - Torre Beneficencia Piso 4.
Código Postal: 111321 – Teléfono: 749 1692
/CundiGob @CundinamarcaGob
www.cundinamarca.gov.co

5. Diseño de sesión y navegador seguro

5.1 Máquina de estados

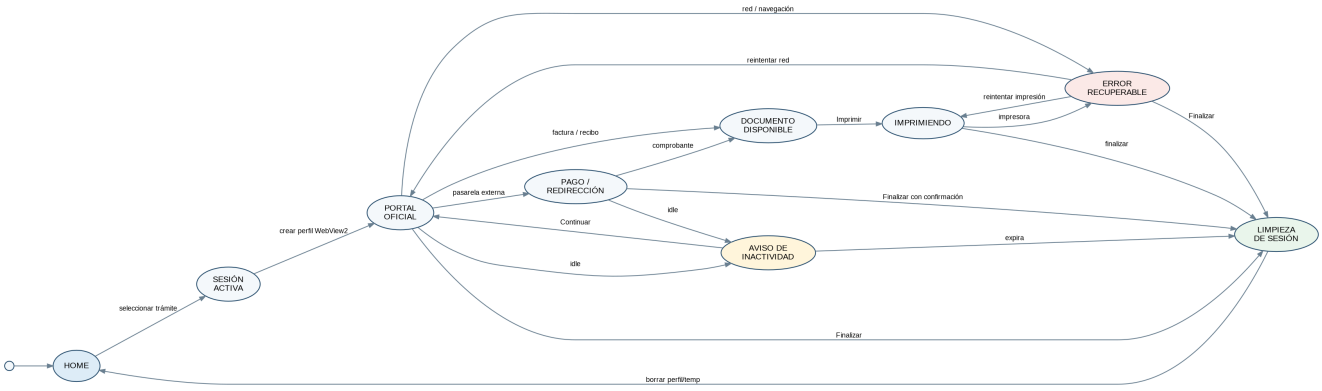


Figura 3. Máquina de estados simplificada de una sesión ciudadana.

5.2 Ciclo de una sesión

1. Al seleccionar un trámite se crea un identificador de sesión aleatorio solo para correlación técnica.
2. Se inicializa WebView2 con las políticas de seguridad y navegación del perfil del kiosco.
3. La interacción permanece dentro del WebView; popups permitidos se redirigen al mismo contenedor o a un WebView controlado.
4. Las descargas se interceptan. Solo se admiten tipos explícitamente necesarios (principalmente PDF) desde hosts autorizados.
5. Al finalizar o por timeout, se navega fuera del contenido, se limpia el perfil WebView2 y se eliminan temporales.
6. Solo después de confirmar la limpieza se muestra Home para el siguiente ciudadano.

5.3 Datos a limpiar

Tipo	Tratamiento
Cookies / sesión web	Eliminar al finalizar cada sesión.
DOM storage	Eliminar LocalStorage, IndexedDB, CacheStorage y demás AllSite/AllDomStorage.
Cache / historial	Eliminar disco, navegación y descargas.
Autofill / password save	Deshabilitados y limpiados.
Permisos web	No persistir concesiones entre ciudadanos.
Archivos descargados	Guardar solo en carpeta temporal de la sesión; eliminar al finalizar.

Calle 26 #51-53 Bogotá D.C.
Sede Administrativa - Torre Beneficencia Piso 4.
Código Postal: 111321 – Teléfono: 749 1692
/CundiGob @CundinamarcaGob
www.cundinamarca.gov.co

Tipo	Tratamiento
Portapapeles	No usar para lógica interna; denegar permisos web si no son requeridos.
Logs	Conservar solo metadatos técnicos sanitizados; nunca valores de formularios.

5.4 Hardening de WebView2

- Permitir únicamente HTTPS para portales externos; file:// solo para recursos internos controlados cuando sea estrictamente necesario.
- Validar host por coincidencia exacta o subdominio delimitado; nunca usar “contains” sobre la URL.
- Deshabilitar DevTools, menús contextuales, guardado de contraseñas, autofill y aceleradores de navegador no necesarios.
- Interceptar NavigationStarting y NewWindowRequested; ningún popup debe escapar al navegador del sistema.
- Bloquear esquemas externos (file, shell, ms-settings, mailto, custom protocols) salvo aprobación explícita.
- No ignorar errores de certificado TLS y no instalar certificados de confianza ad hoc desde la aplicación.
- No usar ExecuteScriptAsync con datos del usuario ni inyectar JavaScript en formularios de pago.
- No usar WebMessage/host objects si no son necesarios. Si se habilitan en el futuro, deben validar origen y esquema de mensaje.
- Bloquear ejecutables, instaladores, scripts y archivos no requeridos en DownloadStarting.

5.5 Política de dominios

La allowlist se mantiene por perfil y por fase del flujo. El conjunto inicial debe levantarse en PoC observando redirecciones reales de los portales y pasarelas. La configuración de producción no debe permitir “cualquier dominio HTTPS”.

```
{
  "profile": "BOGOTA",
  "services": [
    {
      "id": "vehicular",
      "startUrl": "https://nuevaoficinavirtual.shd.gov.co/bogota/es/descargaFacturaVA?impuesto=0002",
      "allowedHosts": ["nuevaoficinavirtual.shd.gov.co"],
      "paymentHosts": ["<definidos-en-PoC>"]
    }
  ]
}
```


Calle 26 #51-53 Bogotá D.C.
Sede Administrativa - Torre Beneficencia Piso 4.
Código Postal: 111321 – Teléfono: 749 1692
/CundiGob @CundinamarcaGob
www.cundinamarca.gov.co

6. Seguridad del sistema operativo y del dispositivo

6.1 Perfil recomendado de producción

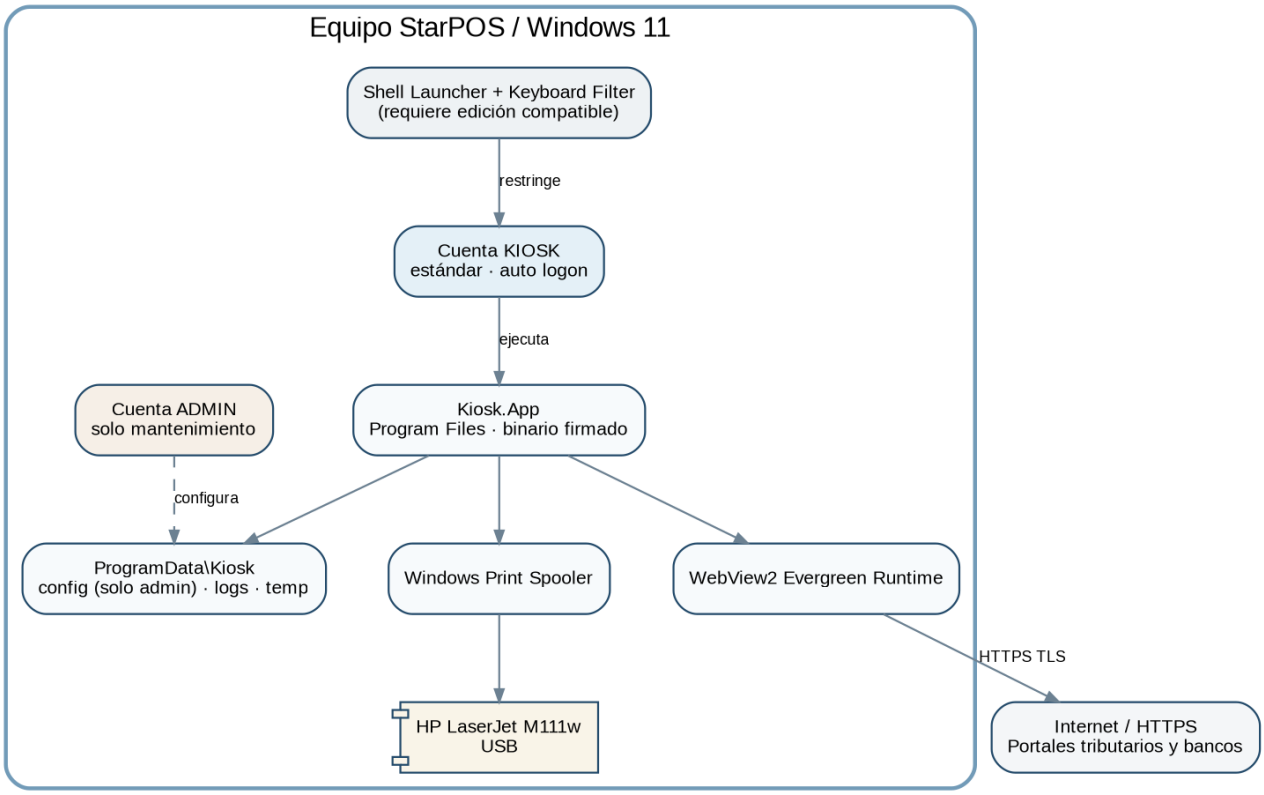


Figura 4. Despliegue recomendado sobre el dispositivo Windows.

- Windows 11 Enterprise, Education o IoT Enterprise para habilitar Shell Launcher y Keyboard Filter conforme a la documentación de Microsoft.
- Cuenta local estándar “KioskUser”, sin privilegios administrativos y usada únicamente por el kiosco.
- Cuenta administrativa separada para mantenimiento, protegida con credenciales gestionadas por el cliente.
- Shell Launcher configura Kiosk.App como shell; Explorer no queda disponible al ciudadano.
- Keyboard Filter bloquea secuencias definidas (Alt+Tab, tecla Windows, Ctrl+Alt+Del según política, etc.) y mantiene un procedimiento de breakout para soporte.
- Binarios en Program Files con permisos de escritura solo para administradores; configuración en ProgramData con ACL restrictiva.
- Auto logon del usuario kiosco según política del cliente, seguido de arranque automático del shell.
- Firma Authenticode del instalador/binario recomendada para producción y allowlisting del ejecutable.
- Actualizaciones Windows/WebView2 se ejecutan en ventana de mantenimiento; después se ejecuta smoke test del portal e impresión.

Calle 26 #51-53 Bogotá D.C.
Sede Administrativa - Torre Beneficencia Piso 4.
Código Postal: 111321 – Teléfono: 749 1692
/CundiGob @CundinamarcaGob
www.cundinamarca.gov.co

No se debe intentar "bloquear Alt+Tab" únicamente desde código WPF. Ese control debe residir en capacidades de Windows diseñadas para dispositivos dedicados. El código de la aplicación complementa, pero no reemplaza, el hardening del sistema operativo.

6.2 Acceso de mantenimiento

El personal de soporte podrá conectar teclado si es necesario, ejecutar la secuencia de breakout definida y autenticarse con la cuenta administrativa. La secuencia no es un secreto suficiente por sí sola: el control real es la autenticación del administrador y la separación de privilegios.

7. Navegación de pago y manejo de conectividad

7.1 Principios

- El kiosco no captura ni interpreta campos financieros.
- El motor WebView2 muestra el contenido HTTPS del proveedor tal como fue entregado.
- No se reenvían automáticamente formularios ni se usa refresh automático en páginas de pago.
- Si la red cae después de que el usuario confirmó un pago, la app no muestra "pago fallido" ni "pago exitoso" por inferencia.
- Al recuperar conexión, el usuario debe continuar con el mecanismo que el portal/pasarela soporte para confirmar el estado; si no existe, se debe finalizar con un mensaje prudente y canal de verificación del tercero.

7.2 Tipos de falla

Falla	Comportamiento
Sin interfaz de red	Bloquear inicio del trámite y mostrar mensaje simple "Sin conexión".
DNS / Internet no disponible	Mostrar indisponibilidad; reintentar con backoff manual/limitado.
Portal responde 4xx/5xx	No atribuir a la red local; mostrar que el servicio externo no está disponible.
Timeout de navegación	Ofrecer Reintentar o Finalizar.
Caída durante pago	No refrescar ni duplicar; preservar la pantalla si es posible y mostrar instrucción al recuperar conexión.
Certificado TLS inválido	Bloquear navegación; registrar evento técnico sin permitir bypass.

Calle 26 #51-53 Bogotá D.C.
Sede Administrativa - Torre Beneficencia Piso 4.
Código Postal: 111321 – Teléfono: 749 1692
/CundiGob @CundinamarcaGob
www.cundinamarca.gov.co

8. Arquitectura de impresión

8.1 Hardware objetivo

Impresora HP LaserJet M111w conectada por USB 2.0 al kiosco. HP declara compatibilidad con Windows 11. La configuración de producción debe usar un nombre lógico de impresora validado durante instalación y prueba.

8.2 Estrategias de impresión soportadas

Caso	Estrategia
Página HTML imprimible	CoreWebView2.PrintAsync con PrintSettings y nombre de impresora configurado.
PDF mostrado dentro de WebView2	Impresión silenciosa del documento activo mediante WebView2.
PDF descargado por el portal	Interceptar descarga, guardar en temp de sesión, abrir en WebView2 controlado/oculto y enviar a impresión; eliminar luego.
window.print() del portal	Evitar cuadro de diálogo del sistema; validar en PoC el patrón del portal y sustituir por flujo controlado si es necesario.
Tipo no permitido	Cancelar descarga y mostrar mensaje; nunca abrir ejecutables o archivos con aplicación externa.

8.3 Semántica de éxito

> **"Impresión exitosa" significa que WebView2/Windows aceptó el trabajo de impresión. No equivale necesariamente a "papel físicamente entregado". La detección de sin papel, atasco, tóner u otros estados depende de lo que expongan Windows y el driver HP.**

8.4 Fallas y reintentos

- Antes de imprimir se valida que la impresora configurada exista y no esté reportada como indisponible.
- Solo se permite un trabajo de impresión en curso por instancia para evitar colisiones.
- Ante PrinterUnavailable/Error, se muestra "No pudimos imprimir. Verifica la impresora o solicita ayuda" y botón Reintentar.
- Reintentar impresión NO vuelve a ejecutar la consulta ni el pago.
- El documento temporal se conserva únicamente mientras la sesión siga activa y solo si es necesario para reimpresión.
- Atascos, papel y tóner se resuelven por mantenimiento físico; la app solo muestra estados disponibles.

Calle 26 #51-53 Bogotá D.C.
Sede Administrativa - Torre Beneficencia Piso 4.
Código Postal: 111321 – Teléfono: 749 1692
/CundiGob @CundinamarcaGob
www.cundinamarca.gov.co

9. Diseño de experiencia, usabilidad y accesibilidad

9.1 Principios para población objetivo

Principio	Aplicación
Una decisión por pantalla	Home con máximo dos trámites visibles; errores con una acción primaria.
Lenguaje ciudadano	“Imprimir recibo”, “Volver al inicio”, “Intentar de nuevo”; evitar “spooler”, “timeout” o “HTTP”.
Controles grandes	Objetivo táctil ≥ 64×64 px equivalentes; separación amplia para evitar toques accidentales.
Tipografía legible	Texto base propio 20–24 px; títulos 36–44 px; alto contraste; no depender solo del color.
Sin gestos complejos	No exigir hover, drag, doble clic o combinaciones de teclado.
Confirmación de acciones destructivas	“Finalizar” pide confirmación si existe una sesión activa.
Tiempo suficiente	Timeout configurable; aviso visible al menos 30–60 s antes del cierre.
Recuperación	Errores indican qué ocurrió y qué puede hacer el usuario; siempre existe retorno seguro a Home.
Accesibilidad	UI propia alineada a WCAG 2.2 AA en contraste, foco, texto, etiquetas y no dependencia de color; portales externos son responsabilidad de sus dueños.

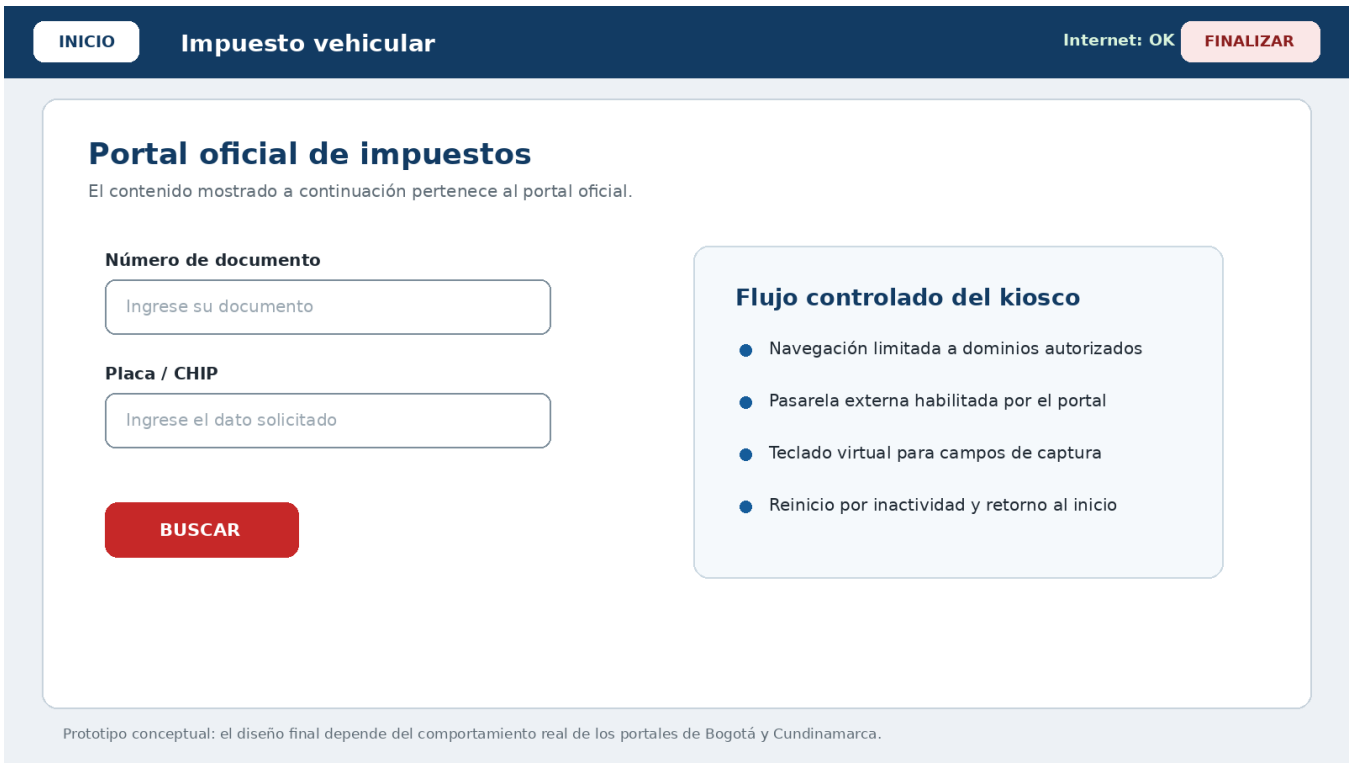
9.2 Pantallas propias

Pantalla	Elementos
Home	Título, ubicación, Vehicular, Predial según perfil, estado de servicio discreto.
Marco de portal	Contenido WebView2, Inicio, Finalizar, ayuda/estado, sin barra de direcciones.
Confirmación de impresión	Documento listo, botón grande Imprimir y opción Finalizar.
Impresora no disponible	Mensaje simple, Reintentar y Finalizar.
Sin conexión	Mensaje, Reintentar y Volver al inicio.
Aviso de inactividad	Cuenta regresiva y botón Continuar.
Limpieza	Pantalla transitoria “Preparando el kiosco para el siguiente usuario...”.

Calle 26 #51-53 Bogotá D.C.
Sede Administrativa - Torre Beneficencia Piso 4.
Código Postal: 111321 – Teléfono: 749 1692
/CundiGob @CundinamarcaGob
www.cundinamarca.gov.co



Figura 5. Prototipo conceptual de Home.



Calle 26 #51-53 Bogotá D.C.
Sede Administrativa - Torre Beneficencia Piso 4.
Código Postal: 111321 – Teléfono: 749 1692
/CundiGob @CundinamarcaGob
www.cundinamarca.gov.co

Figura 6. Prototipo conceptual del marco de navegación.

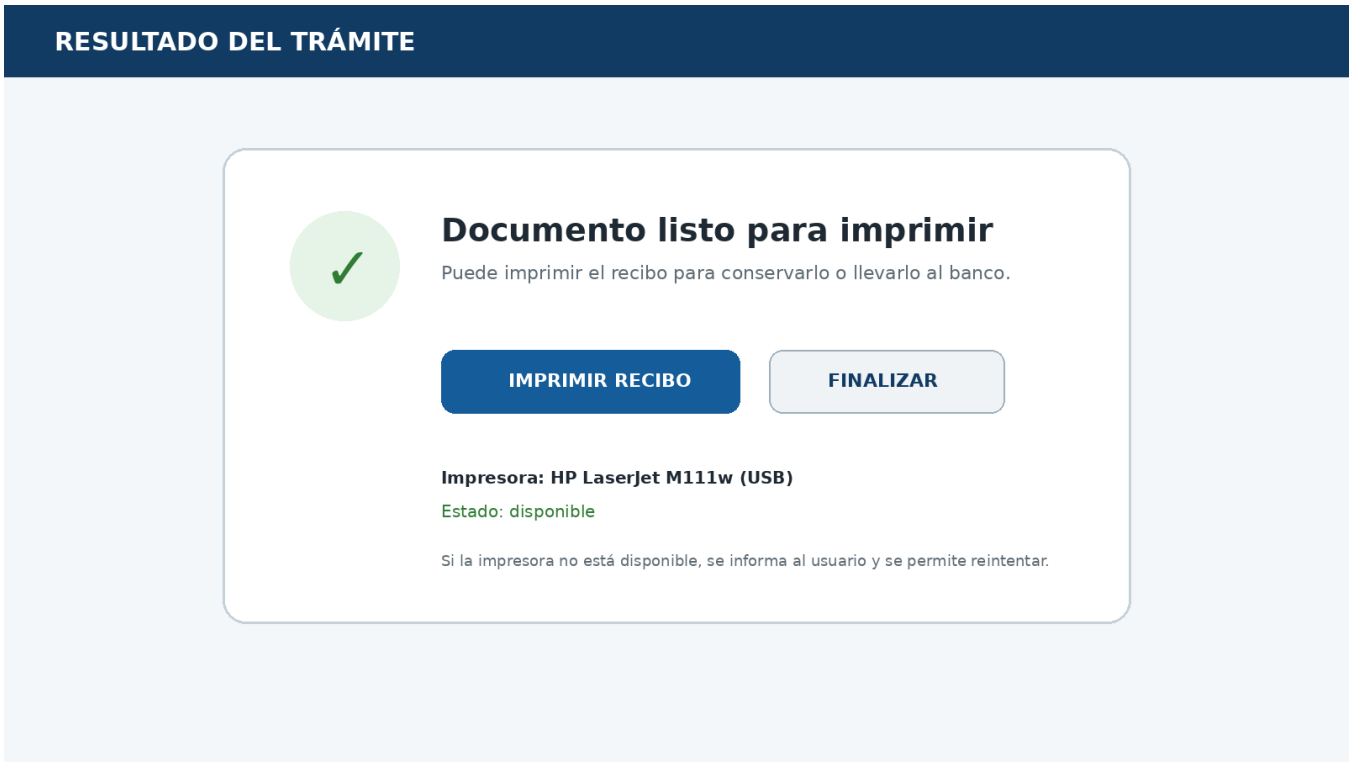


Figura 7. Prototipo conceptual de impresión.

Calle 26 #51-53 Bogotá D.C.
Sede Administrativa - Torre Beneficencia Piso 4.
Código Postal: 111321 – Teléfono: 749 1692
/CundiGob @CundinamarcaGob
www.cundinamarca.gov.co

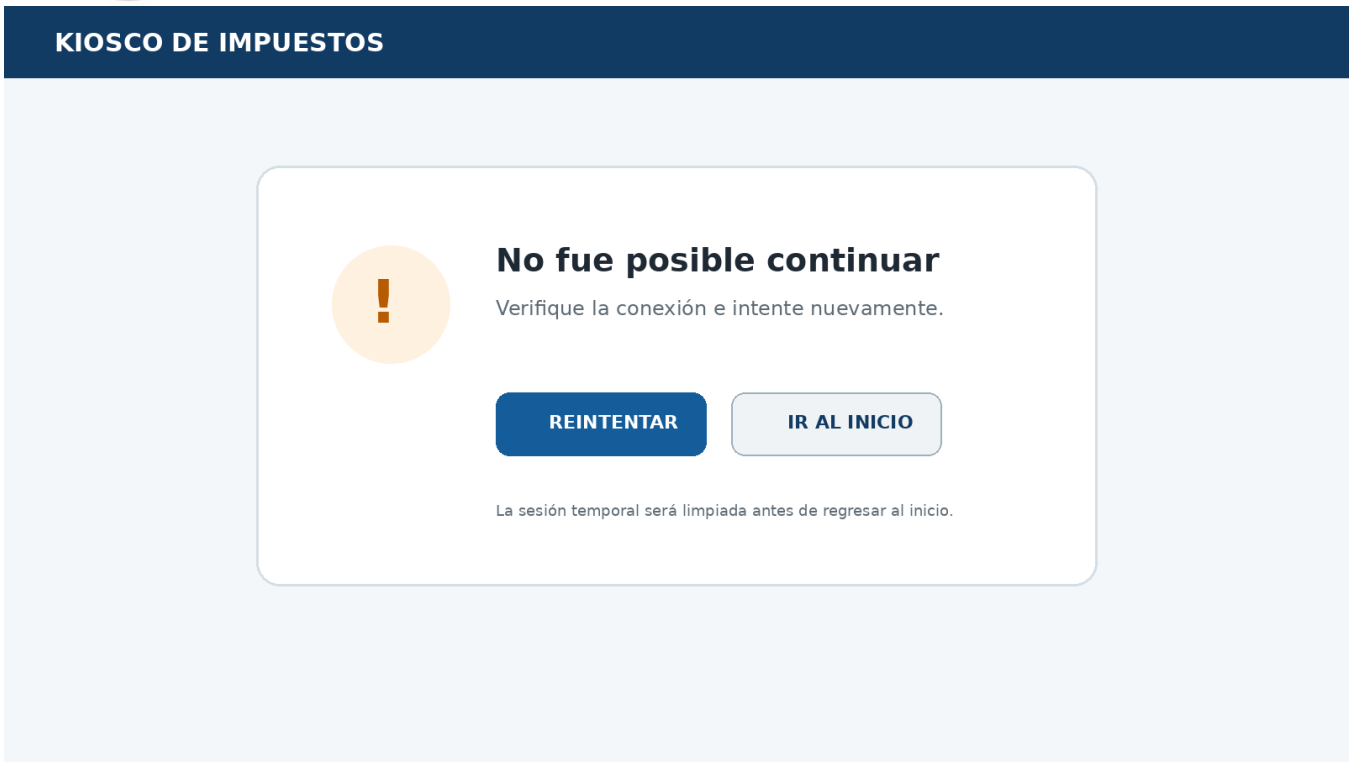


Figura 8. Prototipo conceptual de indisponibilidad.

Calle 26 #51-53 Bogotá D.C.
Sede Administrativa - Torre Beneficencia Piso 4.
Código Postal: 111321 – Teléfono: 749 1692
/CundiGob @CundinamarcaGob
www.cundinamarca.gov.co

10. Resiliencia y disponibilidad

10.1 Estrategia de autorrecuperación

Evento	Respuesta
Cierre normal de Kiosk.App	Shell Launcher reinicia el shell para el usuario kiosco.
Crash no controlado	Proceso termina; Shell Launcher lo relanza. Al iniciar, la app elimina temporales huérfanos y muestra Home.
Reinicio del PC	Auto logon + shell de kiosco + Home.
Impresora reiniciada físicamente	La app vuelve a consultar disponibilidad cuando el usuario reintenta.
Internet regresa	La navegación puede reintentarse manualmente sin reenvío automático del pago.
Portal externo caído	La app sigue operativa, pero informa indisponibilidad del servicio específico.
Configuración inválida	Fail closed: no abrir URLs desconocidas; mostrar pantalla de servicio no disponible y registrar evento.

10.2 Límites de alta disponibilidad

Un kiosco físico es un único nodo: no existe alta disponibilidad de hardware dentro del mismo equipo. La arquitectura maximiza disponibilidad mediante recuperación automática y degradación controlada. La continuidad del servicio ante daño de hardware, pérdida prolongada de Internet o caída del portal requiere redundancia externa (otro kiosco, conectividad alternativa o disponibilidad del tercero).

10.3 Objetivos operativos sugeridos

- Home ≤ 5 s desde que Kiosk.App inicia.
- Recuperación de crash ≤ 15 s después de la terminación del proceso, sujeto a Windows.
- Cleanup de sesión ≤ 10 s en condiciones normales.
- Rotación de logs: 14 días o límite de tamaño configurable.
- 0 datos de formularios ciudadanos en logs de aplicación.
- 0 navegación permitida fuera de hosts aprobados en pruebas de seguridad.

11. Configuración, logging y datos locales

11.1 Configuración

La configuración se almacena bajo ProgramData con ACL de solo lectura para KioskUser y escritura exclusiva de administradores. No contiene secretos. Se valida contra un esquema al iniciar y puede incluir hash/firma de integridad si el cliente requiere control adicional.

Calle 26 #51-53 Bogotá D.C.
Sede Administrativa - Torre Beneficencia Piso 4.
Código Postal: 111321 – Teléfono: 749 1692
/CundiGob @CundinamarcaGob
www.cundinamarca.gov.co

Parámetro	Ejemplo / regla
KioskId	Identificador técnico sin datos de persona.
Profile	BOGOTA / CUNDINAMARCA.
Services	Lista de trámites visibles y startUrl.
AllowedHosts	Hosts del portal y navegación aprobada.
PaymentHosts	Hosts de pasarela/bancos validados en PoC.
PrinterName	Nombre exacto de la HP M111w instalada.
InactivityTimeout	Ej. 300 s, configurable.
WarningBeforeTimeout	Ej. 60 s.
NetworkProbe	Hosts del propio servicio; no usar un tercero ajeno como único indicador.
LogRetention	Días y tamaño máximo.

11.2 Logging

Los eventos se registran como JSON estructurado, con timestamp UTC/local, EventId, nivel, componente, KioskId, SessionCorrelationId y detalle sanitizado. Las URLs se guardan sin query string ni fragmento. No se registran documento, placa, CHIP, nombres, cookies, tokens, cuerpos HTTP, campos financieros ni screenshots.

12. Modelo de amenazas resumido

Amenaza	Ejemplo	Mitigación
Spoofing	Sitio falso o redirección inesperada.	HTTPS + validación estricta de host + no bypass TLS.
Tampering	Usuario modifica config o ejecutable.	ACL, cuenta estándar, Program Files, firma de binario, fail closed.
Repudiation	No hay trazabilidad de un fallo técnico.	Eventos técnicos correlacionados sin PII; reloj del sistema protegido.
Information Disclosure	Siguiente ciudadano ve cookies, PDF o autofill.	Perfil efímero/cleanup AllProfile + temp por sesión + autofill/password off.
Denial of Service	Portal, red o impresora no disponible.	Mensajes recuperables, reintento limitado/manual, shell autorestart.
Elevation of Privilege	Escape a escritorio/Task Manager/DevTools.	Shell Launcher, Keyboard Filter, cuenta estándar, DevTools/context menu off.

Calle 26 #51-53 Bogotá D.C.
Sede Administrativa - Torre Beneficencia Piso 4.
Código Postal: 111321 – Teléfono: 749 1692
/CundiGob @CundinamarcaGob
www.cundinamarca.gov.co

Amenaza	Ejemplo	Mitigación
Malicious Download	Portal comprometido intenta descargar EXE.	DownloadStarting allowlist por MIME/extensión/host, temp controlado, no ShellExecute.
Duplicate Payment	Refresh/reintento automático después de pérdida de red.	Nunca re-submit automático; resultado lo determina el tercero.
Sensitive Logging	Query URL contiene identificación.	Sanitizar query/fragment y prohibir payloads/campos en logs.

13. Despliegue, instalación y operación

13.1 Paquete

- Publicación x64 self-contained de .NET 10 para reducir dependencia del runtime global.
- Instalador MSI/EXE corporativo que copia binarios a Program Files y configuración a ProgramData.
- Validación de presencia/versión del WebView2 Evergreen Runtime.
- Creación/verificación del usuario kiosco y políticas mediante script PowerShell ejecutado como administrador/SYSTEM.
- Instalación y prueba del driver HP M111w por USB.
- Aplicación del perfil de kiosco y smoke test posterior.

13.2 Orden de instalación

1. Confirmar edición de Windows y actualizar parches.
2. Instalar/validar driver HP y realizar página de prueba.
3. Instalar Kiosk.App y WebView2 Runtime si aplica.
4. Copiar configuración firmada/aprobada del perfil.
5. Crear/configurar KioskUser y políticas de Shell Launcher/Keyboard Filter.
6. Reiniciar, validar auto logon y Home.
7. Ejecutar casos E2E de portal, pago de prueba cuando exista ambiente controlado, impresión y cleanup.
8. Entregar procedimiento de breakout/mantenimiento al responsable autorizado.

14. Estructura del proyecto de software

La solución se organizará para que reglas críticas sean testeables sin depender de WPF/WebView2. El UI queda delgado y la lógica se concentra en servicios e interfaces.

```
KioskTaxes.sln
src/
  KioskTaxes.App/                # WPF, composición y UI
  KioskTaxes.Application/        # casos de uso y orquestación
  KioskTaxes.Domain/             # modelos, estados, políticas puras
  KioskTaxes.Infrastructure/     # WebView2, impresión, red, archivos, logging
tests/
  KioskTaxes.Domain.Tests/
```


Calle 26 #51-53 Bogotá D.C.
Sede Administrativa - Torre Beneficencia Piso 4.
Código Postal: 111321 – Teléfono: 749 1692
/CundiGob @CundinamarcaGob
www.cundinamarca.gov.co

```
  KioskTaxes.Application.Tests/
  KioskTaxes.Infrastructure.Tests/
  KioskTaxes.AcceptanceTests/     # pruebas sobre adaptadores/fakes y smoke scripts
deploy/
  powershell/                     # hardening, install, validate, rollback
config/
  schema/                         # JSON schema
  examples/
docs/
  architecture/
  operations/
```

14.1 Interfaces principales

Interfaz	Propósito
ISessionOrchestrator	Iniciar/finalizar sesión, timeout y transiciones.
IBrowserSession	Crear WebView, navegar, limpiar perfil y cerrar.
INavigationPolicy	Decidir permit/block para Uri, popup, permiso y descarga.
IPrintService	Disponibilidad, impresión y resultado.
IConnectivityService	Estado de red y diagnóstico no intrusivo.
IKioskConfiguration	Perfil validado y solo lectura.
ITechnicalLogger	Eventos sanitizados.
IClock / IIdleDetector	Tiempo testeable y detección de inactividad.

15. Estrategia de pruebas

15.1 Pirámide de pruebas

Nivel	Cobertura
Unitarias	Policy de URLs, sanitizer de logs, máquina de estados, timeout, validación de configuración, reintentos de impresión.
Componentes	Adapters WebView2/print/network con fakes y pruebas Windows donde aplique.
Integración	WebView2 real contra sitios de prueba/controlados; generación PDF; spooler con impresora o cola controlada.
E2E	Kiosco físico: Home → portal → factura/pago de prueba → impresión → finalizar → verificar limpieza.
Seguridad	Escape de kiosk, atajos, DevTools, URL tampering, popups, downloads, TLS, PII en logs.
Resiliencia	Kill process, reinicio PC/impresora, desconexión de red, portal 5xx, impresora offline.

Calle 26 #51-53 Bogotá D.C.
Sede Administrativa - Torre Beneficencia Piso 4.
Código Postal: 111321 – Teléfono: 749 1692
/CundiGob @CundinamarcaGob
www.cundinamarca.gov.co

Nivel	Cobertura
Usabilidad	Pruebas con usuarios representativos: tiempo, errores, comprensión de botones y recuperación.

15.2 Casos críticos de aceptación

ID	Prueba	Esperado
T-SEC-01	Cerrar sesión A y empezar B.	B no ve cookies, datos, PDFs, historial ni autocompletado de A.
T-SEC-02	Intentar URL no permitida.	Bloqueada y registrada sin query.
T-SEC-03	F12 / Ctrl+P / Alt+Tab / Win / secuencias definidas.	No permite escapar ni abrir herramientas en perfil de producción.
T-PAY-01	Desconectar Internet después de iniciar pago.	No se reenvía automáticamente; mensaje neutral de estado.
T-PRN-01	Impresora apagada.	Mensaje + Reintentar; no reinicia pago.
T-PRN-02	Factura PDF.	Se imprime sin abrir visor externo y se elimina temp al cerrar sesión.
T-RES-01	Matar Kiosk.App.	Se relanza y regresa a Home.
T-USE-01	Usuario solo con pantalla táctil.	Puede completar navegación y entrada de datos con teclado táctil.
T-IDLE-01	Inactividad hasta timeout.	Aviso, expiración, cleanup y Home.
T-LOG-01	Ejecutar flujo con datos reales de prueba.	Logs no contienen documento, placa, CHIP, cookies ni query sensible.

16. Trazabilidad alcance → componente → prueba

Requisito	Componente	Pruebas
Dos accesos / perfiles por ubicación	Kiosk.UI + Configuration Provider	T-USE-01 + unit de config
Portales oficiales	Secure Browser + Navigation Policy	T-SEC-02 + E2E por portal
Pasarela existente	Secure Browser + allowlist	T-PAY-01 + E2E de redirección
Imprimir factura / comprobante	Print Coordinator	T-PRN-01/02
No cruzar sesiones	Session Orchestrator + Browser cleanup	T-SEC-01

Calle 26 #51-53 Bogotá D.C.
Sede Administrativa - Torre Beneficencia Piso 4.
Código Postal: 111321 – Teléfono: 749 1692
/CundiGob @CundinamarcaGob
www.cundinamarca.gov.co

Requisito	Componente	Pruebas
No acceder al SO	Windows Kiosk Hardening + WebView settings	T-SEC-03
Sin Internet	Connectivity + Session Orchestrator	T-PAY-01 + resiliencia
Autoarranque / reinicio	Shell Launcher + deployment	T-RES-01 + reboot test
Usabilidad tercera edad/campo	Kiosk.UI	T-USE-01 + prueba de usuario
Logs para soporte	Technical Logger	T-LOG-01

17. Plan de construcción con Codex

Codex se usará como agente de implementación dentro del repositorio local. La arquitectura y los criterios de aceptación de este documento son la fuente de verdad. Cada iteración debe terminar con build limpio, pruebas automatizadas y revisión de diff antes de continuar.

Iteración	Objetivo	Gate
0 · PoC	WPF + WebView2, portal Bogotá/Cundinamarca, touch keyboard, descarga/impresión HP, redirecciones.	Demostrar viabilidad en hardware real y levantar hosts/print patterns.
1 · Foundation	Solution, DI, configuración validada, logging sanitizado, Home y state machine.	Unit tests verdes; config inválida falla cerrada.
2 · Secure Browser	Allowlist, popups, permisos, downloads, cleanup, timeout.	Security tests + no fuga entre sesiones.
3 · Printing	HTML/PDF, status, retry, temp lifecycle.	Pruebas con HP M111w física.
4 · Resilience/Hardening	Connectivity, recovery, installer, Shell Launcher, Keyboard Filter.	Kill/reboot/network/printer tests.
5 · UAT/Pilot	UX final, E2E, documentación operación y rollback.	Criterios de aceptación firmados.

17.1 Reglas para Codex

- No modificar el alcance ni “simplificar” controles de seguridad sin un ADR aprobado.
- No introducir scraping o automatización de campos de portales/pagos.
- No almacenar ni loguear PII o datos financieros, incluso en Debug.
- Toda regla de URL debe tener pruebas positivas y negativas.
- Toda transición de sesión debe tener pruebas; cleanup es obligatorio en finally/error paths.
- No abrir archivos descargados mediante ShellExecute ni visor externo.

Calle 26 #51-53 Bogotá D.C.
Sede Administrativa - Torre Beneficencia Piso 4.
Código Postal: 111321 – Teléfono: 749 1692
/CundiGob @CundinamarcaGob
www.cundinamarca.gov.co

- Pin de paquetes y Package Lock; dependencias externas mínimas y justificadas.
- Warnings as errors en CI para proyectos propios; analizadores .NET habilitados.
- No hacer merge si dotnet test falla o si un test de seguridad crítico está omitido.

18. Decisiones pendientes antes de congelar implementación

Prioridad	Decisión / dato requerido	Impacto si no se confirma
BLOQUEANTE	Edición exacta de Windows 11 del StarPOS.	Define si podemos aplicar Shell Launcher/Keyboard Filter o si se requiere upgrade.
ALTA	Hosts reales de pasarela/bancos en cada portal.	Necesarios para una allowlist segura sin bloquear el pago.
ALTA	Patrón de documento en cada portal: HTML, PDF embebido o descarga.	Define adapter de impresión y pruebas.
ALTA	Nombre exacto de la impresora instalada/driver HP en Windows.	Necesario para PrintSettings y health check.
MEDIA	Timeout de inactividad aprobado por negocio.	Afecta UX y seguridad; propuesto 5 min + aviso 60 s.
MEDIA	Mecanismo de actualización y soporte en campo.	Sin MDM, se requiere procedimiento manual/ventana de mantenimiento.
MEDIA	Si Cundinamarca incluirá Predial por municipio.	Puede agregar múltiples portales, allowlists y pruebas.
BAJA	Branding final y textos ciudadanos.	No cambia arquitectura; sí UI/aceptación.

19. Referencias técnicas

[R1] Microsoft .NET releases and support — Consultado 29-09-2026. .NET 10 LTS hasta noviembre de 2028.
https://learn.microsoft.com/dotnet/core/releases-and-support

[R2] Microsoft Shell Launcher — Ediciones compatibles y uso como shell dedicado.
https://learn.microsoft.com/windows/configuration/shell-launcher/

[R3] Microsoft Assigned Access — Kiosk/restricted user experience y requisitos de edición.
https://learn.microsoft.com/windows/configuration/assigned-access/

[R4] Microsoft Keyboard Filter — Bloqueo de combinaciones de teclas en dispositivos dedicados.
https://learn.microsoft.com/windows/configuration/keyboard-filter/

[R5] WebView2 printing — PrintAsync y configuración de impresión programática.
https://learn.microsoft.com/microsoft-edge/webview2/how-to/print

[R6] WebView2 user data folders / browsing data — Datos del perfil y estrategia de limpieza.
https://learn.microsoft.com/microsoft-edge/webview2/concepts/user-data-folder

[R7] HP LaserJet M111w specifications — USB 2.0 y compatibilidad con Windows 11.
https://support.hp.com/co-es/product/product-specs/hp-laserjet-m109-m112-printer-series/34443749

Calle 26 #51-53 Bogotá D.C.
Sede Administrativa - Torre Beneficencia Piso 4.
Código Postal: 111321 – Teléfono: 749 1692
/CundiGob @CundinamarcaGob
www.cundinamarca.gov.co

20. Criterio para iniciar construcción

> Baseline para construcción: antes de cerrar la Iteración 0 deben confirmarse la edición de Windows, las redirecciones/hosts de pago, el patrón real de descarga/impresión en ambos portales y la HP M111w física. Cambios posteriores que alteren seguridad, sesión, impresión o navegación requieren un ADR aprobado.

Calle 26 #51-53 Bogotá D.C.
Sede Administrativa - Torre Beneficencia Piso 4.
Código Postal: 111321 – Teléfono: 749 1692
/CundiGob @CundinamarcaGob
www.cundinamarca.gov.co