

UNIVERSIDAD NACIONAL DE INGENIERÍA



Manual de Usuario: EUDR-Blockchain (v1.0)

Blockchain y Validación Geoespacial para la Trazabilidad Agrícola en
Cumplimiento Normativo EUDR

PROYECTO: PROCICIENCIA – PE501093703-2024

2026

Contenido

1. Introducción	3
2. ¿Qué hace el sistema?	3
3. Requisitos básicos para el usuario	4
3.1. Requisitos del cliente (Navegadores y dispositivos)	4
3.2. Requisitos de red	4
3.3. Prerrequisitos técnicos	4
4. Acceso y Autenticación (Paso a paso)	4
4.1. Paso 1: Registro de un nuevo usuario	4
4.2. Paso 2: Inicio de sesión en la plataforma	6
4.3. Paso 3: El Dashboard principal	6
5. Cómo utilizar el sistema (Por Perfiles)	8
5.1. Perfil de Producción (Productores)	8
5.1.1. Registro de Finca (Creación de Origen)	8
5.1.2. Registro de Cosecha	10
5.2. Perfil de Poscosecha centro de beneficio o acopio (asociaciones, cooperativas, empresas o acopiadores independientes)	11
5.2.1. Recepción de Cosecha (Validación y Pesaje)	11
5.2.2. Mantenimiento de Grupos (Batching/Mezcla)	14
5.3. Perfil de planta de proceso y exportación (cooperativas o empresas)	16
5.3.1. Gestión de Datos Empresariales (Configuración)	16
5.3.2. Recepción de embarque y Declaración de diligencia debida EUDR	18
6. Productos y Certificados que genera el sistema	20
6.1. NFT (Token No Fungible) de Parcela	20
6.2. Bloques Criptográficos (Cosecha, Ticket, paquete de embarque, exportación)	20
6.3. Reporte de Producción (Declaración EUDR)	20
7. Buenas prácticas para el usuario	20
8. ¿Para qué sirve este sistema en la práctica?	21
9. Solución de Problemas Comunes (Troubleshooting)	21
9.1. Problemas de acceso y registro	21
9.2. Errores al registrar polígonos o parcelas	22
9.3. Hashes o códigos QR no reconocidos	22
10. Checklist de Uso Rápido por Perfil	22

1. Introducción

El **Sistema de Trazabilidad Blockchain EUDR** es una plataforma web y móvil diseñada para registrar, asegurar y certificar toda la cadena de suministro de productos de exportación (como café y cacao), garantizando el cumplimiento de la normativa europea de cero deforestación (EUDR).

El sistema utiliza tecnología Blockchain para crear registros inmutables, lo que significa que una vez ingresada la información (pesos, fechas, ubicaciones geográficas), esta no puede ser alterada ni falsificada.

Público objetivo:

Este manual está dirigido a todas las partes interesadas de las cooperativas cafetaleras y cacaoteras peruanas:

- **Productores:** Encargados de registrar sus fincas y reportar sus cosechas.
- **Acopiadores:** Encargados de recepcionar las cosechas, validar los pesos y agrupar los lotes.
- **Exportadores:** Encargados de consolidar los lotes de acopio y generar el reporte final de debida diligencia EUDR.

2. ¿Qué hace el sistema?

El sistema digitaliza y asegura el viaje del producto desde la tierra hasta el puerto, ejecutando los siguientes pasos:

- **Generación de Identidad Digital (NFT):** Crea una "huella digital" única para cada finca agrícola basada en sus coordenadas GPS, validando automáticamente que esté libre de deforestación.
- **Trazabilidad de Cosecha:** Registra el origen exacto y el peso inicial de los productos recolectados en campo.
- **Consolidación y Empaquetado (Merkle Tree):** Permite a los centros de acopio agrupar múltiples entregas pequeñas en grandes lotes de exportación sin perder el rastro de qué productor aportó qué cantidad.
- **Emisión de Reportes EUDR:** Genera automáticamente la documentación oficial y los códigos QR necesarios para exportar el producto hacia la Unión Europea.

3. Requisitos básicos para el usuario

3.1. Requisitos del cliente (Navegadores y dispositivos)

Para que la plataforma web funcione correctamente, su equipo debe cumplir con lo siguiente:

- **Dispositivo:** Computadora de escritorio, laptop o tableta. (Para el registro en campo sin internet, se utilizará la Aplicación Móvil complementaria).
- **Navegador Web:** Se recomienda usar las versiones más recientes de **Google Chrome**, **Mozilla Firefox**, **Microsoft Edge** o **Safari**.
- **Resolución:** Pantalla estándar (optimizada para resoluciones de 1024x768 o superiores).

3.2. Requisitos de red

- **Conectividad:** Es indispensable contar con conexión a Internet estable (WiFi o red de datos móviles) para acceder al portal web y sincronizar la información con la Blockchain.

3.3. Prerrequisitos técnicos

- No se requiere instalación de software adicional para usar la versión web. El acceso se realiza netamente a través de un enlace web (URL) proporcionado por el administrador.

(Nota: Si el usuario administrador requiere hacer pruebas de API a través de terminal, necesitará herramientas como Bash, CMD o PowerShell instaladas).

4. Acceso y Autenticación (Paso a paso)

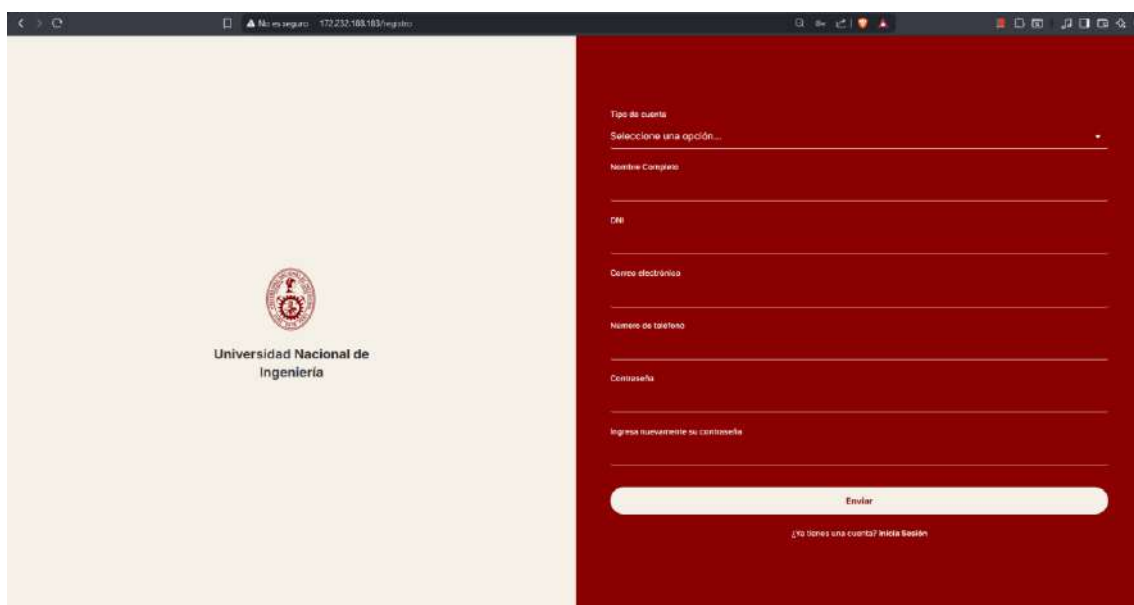
Para garantizar la seguridad de la cadena de bloques, cada actor debe tener una cuenta personal e intransferible.

4.1. Paso 1: Registro de un nuevo usuario

Si es su primera vez en el sistema, debe crear una cuenta:

1. Abra su navegador web e ingrese a la ruta proporcionada por su cooperativa:
[IP_del_Servidor]/registro.

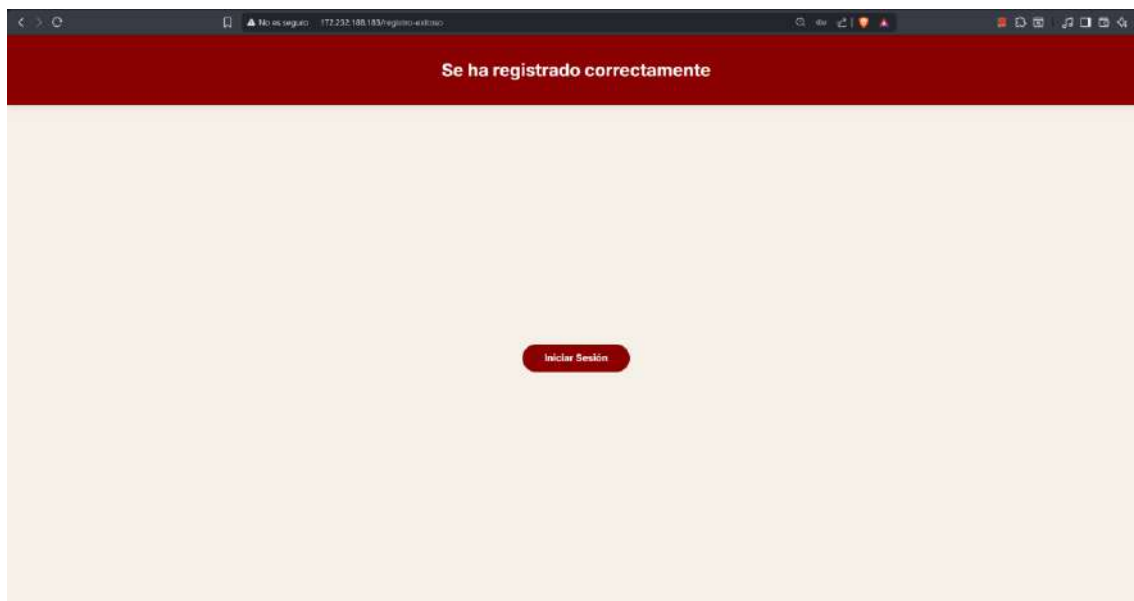
2. Complete el formulario con sus datos reales (Nombre completo, DNI, Correo electrónico y Número de teléfono).
3. **Seleccione su Tipo de Cuenta (Rol):** Es vital elegir correctamente si usted es Productor, Acopiador o Exportador, ya que esto definirá a qué pantallas tendrá acceso.
4. Cree una contraseña segura y presione el botón **Enviar**.
5. El sistema lo redirigirá a la pantalla de "Registro Exitoso" (/registro-exitoso). Haga clic en **Iniciar Sesión**.



The screenshot shows a web browser window with the URL "No es seguro 172.232.188.183/registro". The page is split into two main sections. On the left, there is a light beige background with the logo of the Universidad Nacional de Ingeniería (UNI) and the text "Universidad Nacional de Ingeniería" below it. On the right, there is a dark red background containing a registration form. The form fields are as follows:

- Tipo de cuenta:** A dropdown menu with the text "Seleccione una opción..."
- Nombre Completo:** A text input field.
- DNI:** A text input field.
- Correo electrónico:** A text input field.
- Número de teléfono:** A text input field.
- Contraseña:** A text input field.
- Ingrese nuevamente su contraseña:** A text input field.

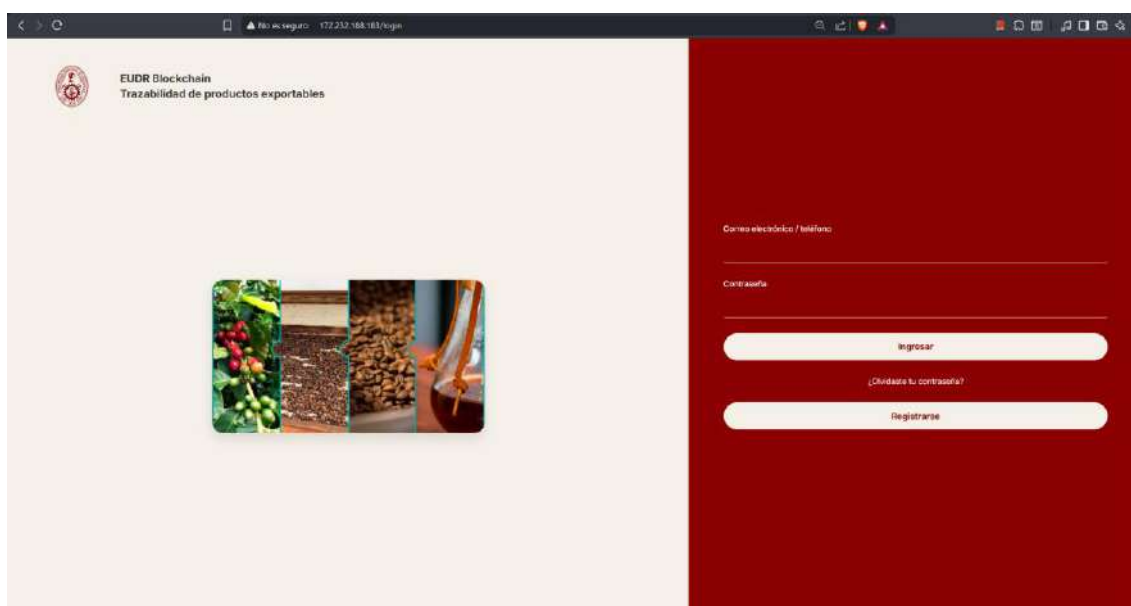
Below the form fields is a white button with the text "Enviar". At the bottom of the red section, there is a small link that says "¿Ya tienes una cuenta? Inicia sesión".



4.2. Paso 2: Inicio de sesión en la plataforma

Una vez registrado, siga estos pasos para entrar al sistema:

1. Ingrese a la ruta principal de acceso: [IP_del_Servidor]/login.
2. Introduzca su **Correo electrónico o teléfono** y su **Contraseña**.
3. Haga clic en el botón **Ingresar**. *(Nota: Actualmente el sistema no cuenta con recuperación automática de contraseña. Si olvida su clave, deberá contactar al administrador del sistema).*



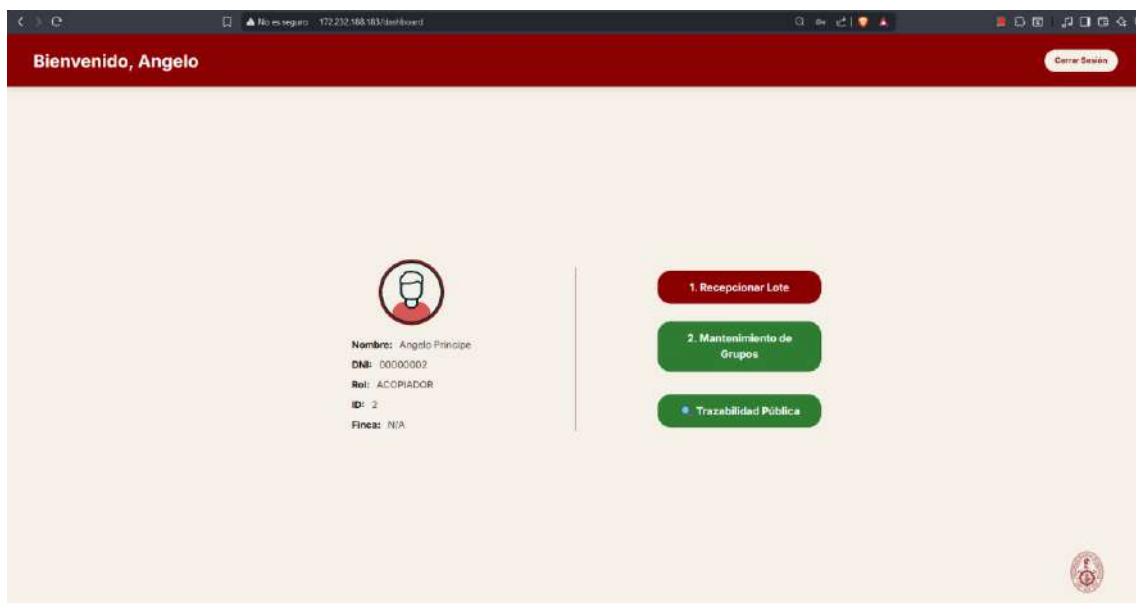
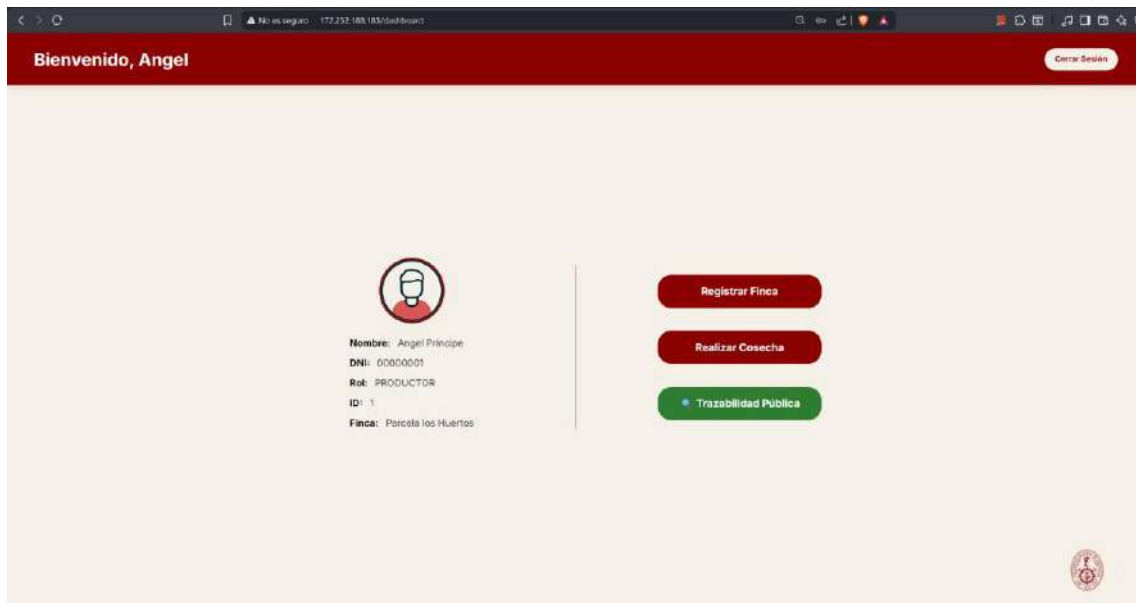
4.3. Paso 3: El Dashboard principal

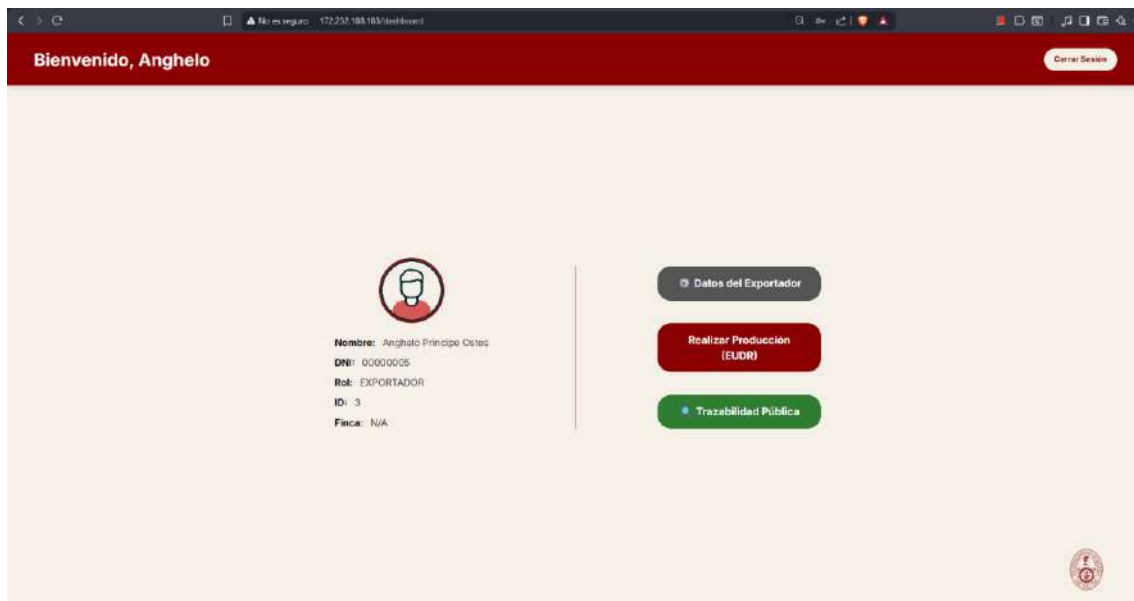
Al ingresar exitosamente, el sistema lo llevará automáticamente a su panel de control o **Dashboard** ([IP_del_Servidor]/dashboard).

El sistema es inteligente y adaptará su interfaz según el rol que usted haya elegido:

- **Si es Productor:** Verá botones de color rojo para "Registrar Finca" y "Realizar Cosecha".
- **Si es Acopiador:** Verá botones para "Recepcionar Lote" y "Mantenimiento de Grupos".
- **Si es Exportador:** Verá opciones para "Datos del Exportador" y "Realizar Producción (EUDR)".

- *Todos los perfiles* tendrán acceso a un botón verde denominado **"Trazabilidad Pública"** para explorar la cadena de bloques.





5. Cómo utilizar el sistema (Por Perfiles)

El sistema adapta sus herramientas de manera automática dependiendo del tipo de usuario con el que haya iniciado sesión. A continuación, se detallan los flujos de trabajo para cada perfil operativo de la cadena.

5.1. Perfil de Producción (Productores)

El perfil de producción es el encargado de iniciar la cadena de trazabilidad de forma segura. Al ingresar a su Dashboard, verá las opciones en color rojo.

5.1.1. Registro de Finca (Creación de Origen)

Descripción: Permite dar de alta una unidad productiva o parcela en el sistema. Es el paso fundamental para la validación de cero deforestación.

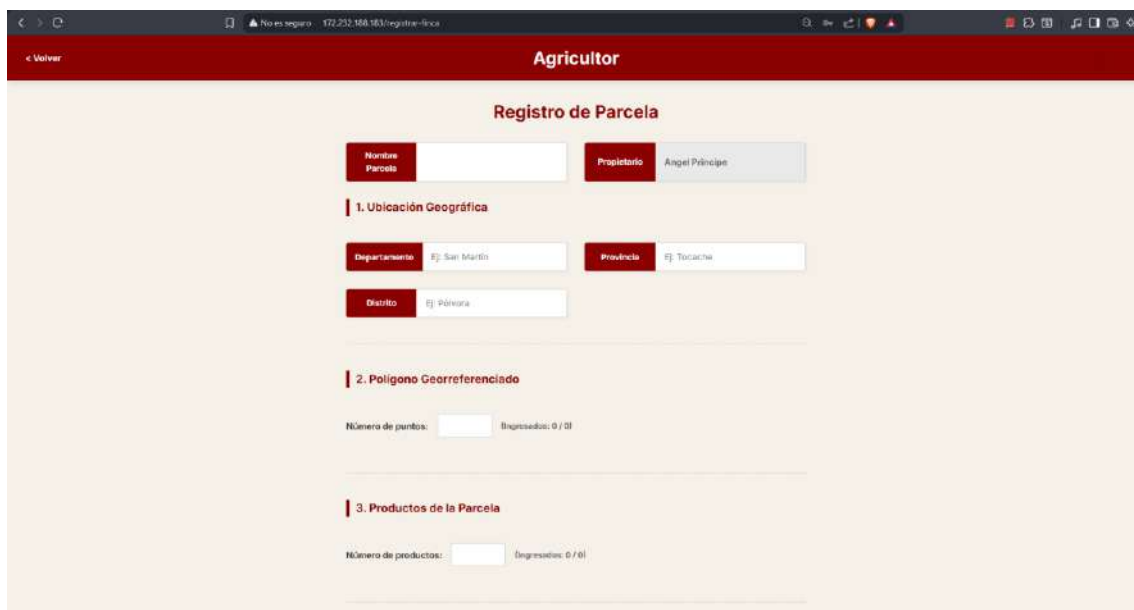
Ruta: [IP_del_Servidor]/registrar-finca

Pasos a seguir:

1. En el Dashboard, haga clic en el botón **Registrar Finca**.
2. Complete el formulario ingresando el Nombre de la Parcela, el Propietario y la Ubicación Geográfica (Departamento, Provincia, Distrito).
3. **Paso crítico:** Ingrese el número de puntos del **Polígono Georreferenciado** y cargue las coordenadas exactas de su terreno.

- Ingrese el número y nombre de los productos cultivados en esa parcela (ej. Café, Cacao).
- Guarde la información.

Resultado del Sistema: El motor de IA evaluará las coordenadas en tiempo real. Si está libre de deforestación, el sistema generará automáticamente un **NFT (Token No Fungible)** único asociado a la finca.



Agricultor

Registro de Parcela

Nombre Parcela: Propietario: Angel Príncipe

1. Ubicación Geográfica

Departamento: Ej. San Martín Provincia: Ej. Tocache

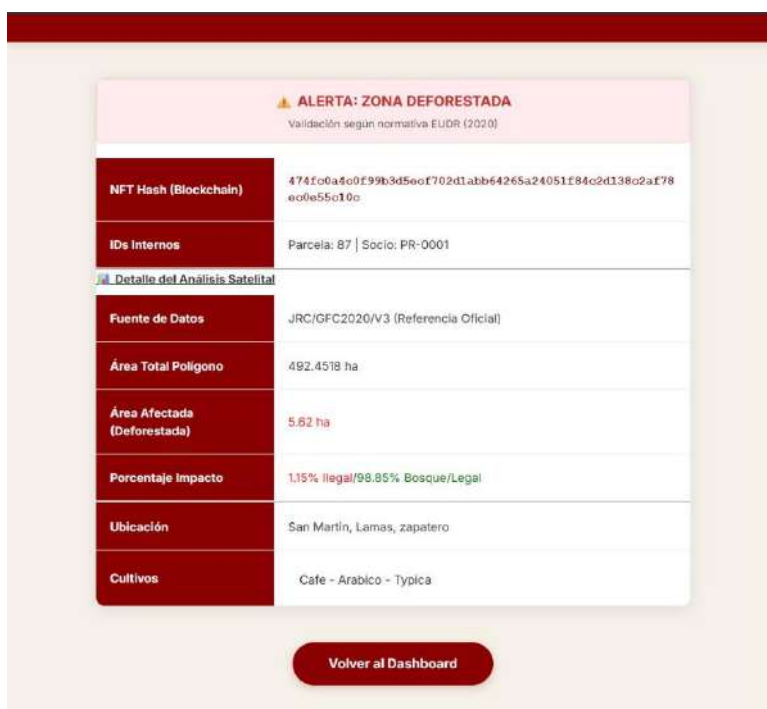
Distrito: Ej. Pálvora

2. Polígono Georreferenciado

Número de puntos: Ingresados: 0 / 50

3. Productos de la Parcela

Número de productos: Ingresados: 0 / 50



ALERTA: ZONA DEFORESTADA
Validación según normativa EUDR (2020)

NFT Hash (Blockchain)	474fo0a40f99b3d5e0f702d1abb64265a24051f84c2d138c2aef8e0fe55c10c
IDs Internos	Parcela: 87 Socio: PR-0001
Detalle del Análisis Satelital	
Fuente de Datos	JRC/GFC2020/V3 (Referencia Oficial)
Área Total Polígono	492.4518 ha
Área Afectada (Deforestada)	5.62 ha
Porcentaje Impacto	1.15% ilegal/98.85% Bosque/Legal
Ubicación	San Martín, Lamas, zapatero
Cultivos	Café - Arabico - Typica

[Volver al Dashboard](#)

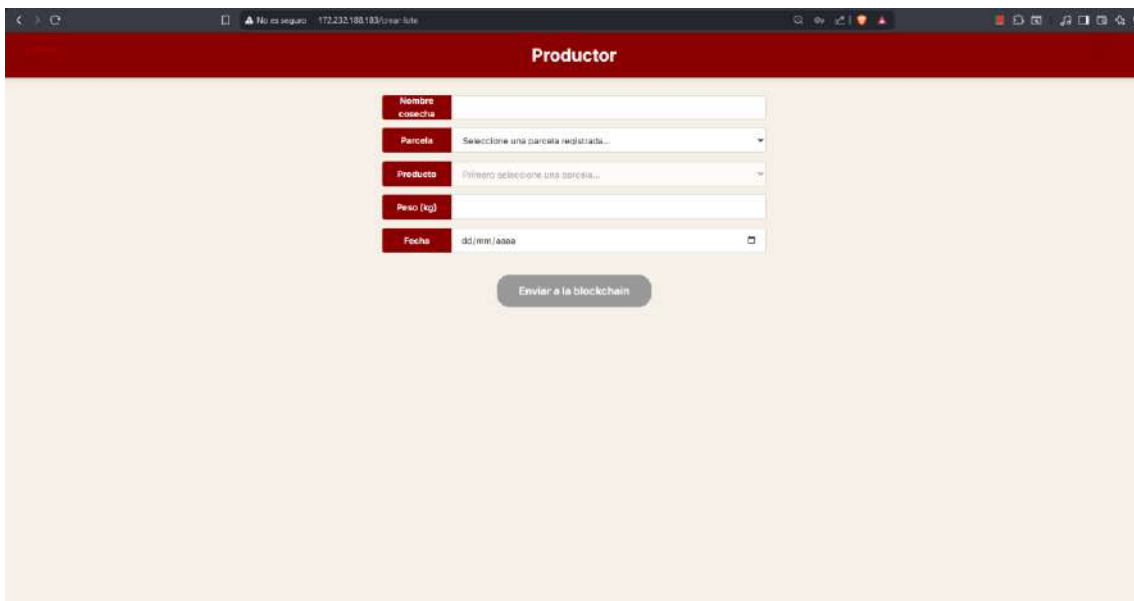
5.1.2. Registro de Cosecha

Descripción: Documenta la recolección física de productos de una finca que ya cuenta con su NFT. **Ruta:** [IP_del_Servidor]/crear-lote

Pasos a seguir:

1. En el Dashboard, haga clic en **Realizar Cosecha**.
2. Seleccione una parcela previamente registrada en el menú desplegable.
3. Llene los detalles de la recolección: Producto, Peso estimado (kg) y Fecha.
4. Haga clic en **Enviar a la blockchain**.

Resultado del Sistema: Se crea el **Bloque de Cosecha (Génesis)**. Este bloque es inmutable y servirá como "padre" para los siguientes procesos, emitiendo un código QR que acompañará físicamente a los sacos.



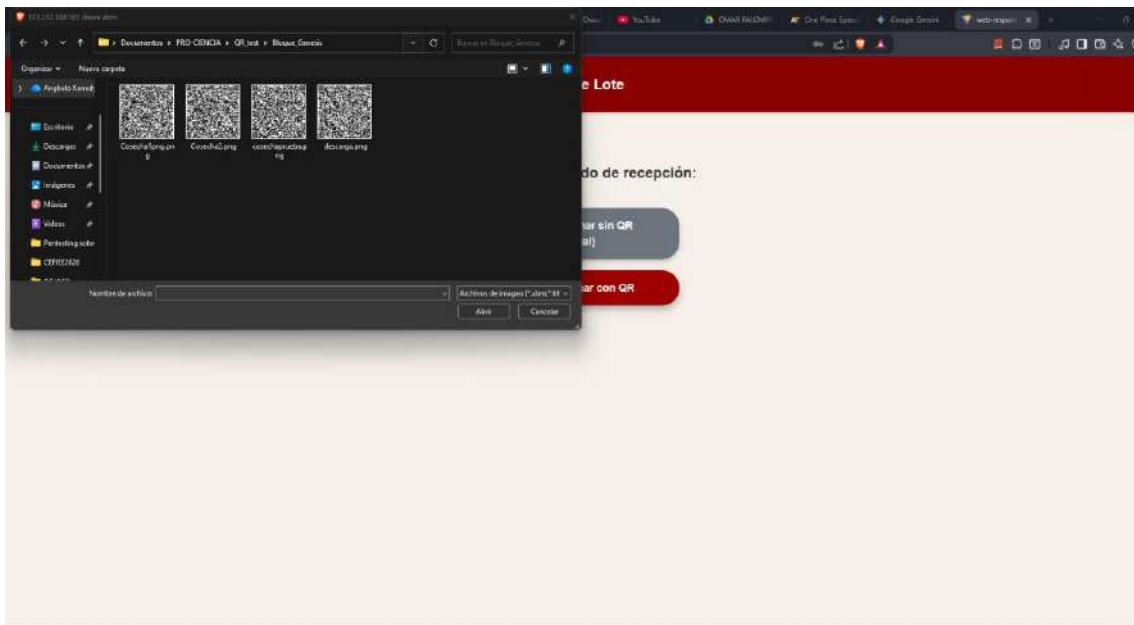
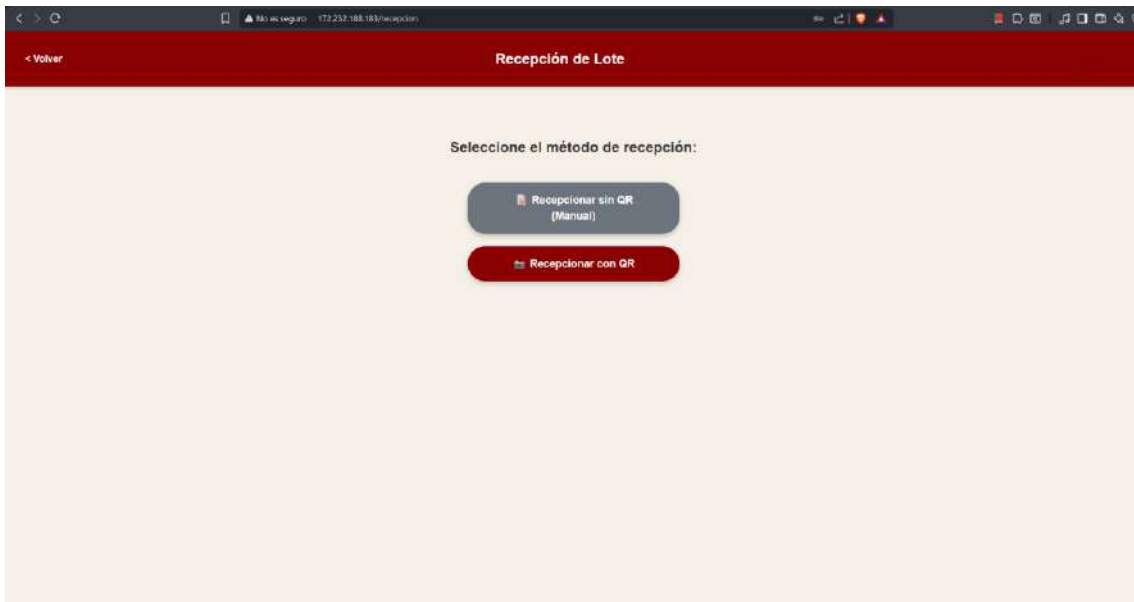
The screenshot shows a web browser window with the address bar displaying 'No se registro - 172.232.100.103/crear-lote'. The page title is 'Productor'. The main content area features a form with the following fields:

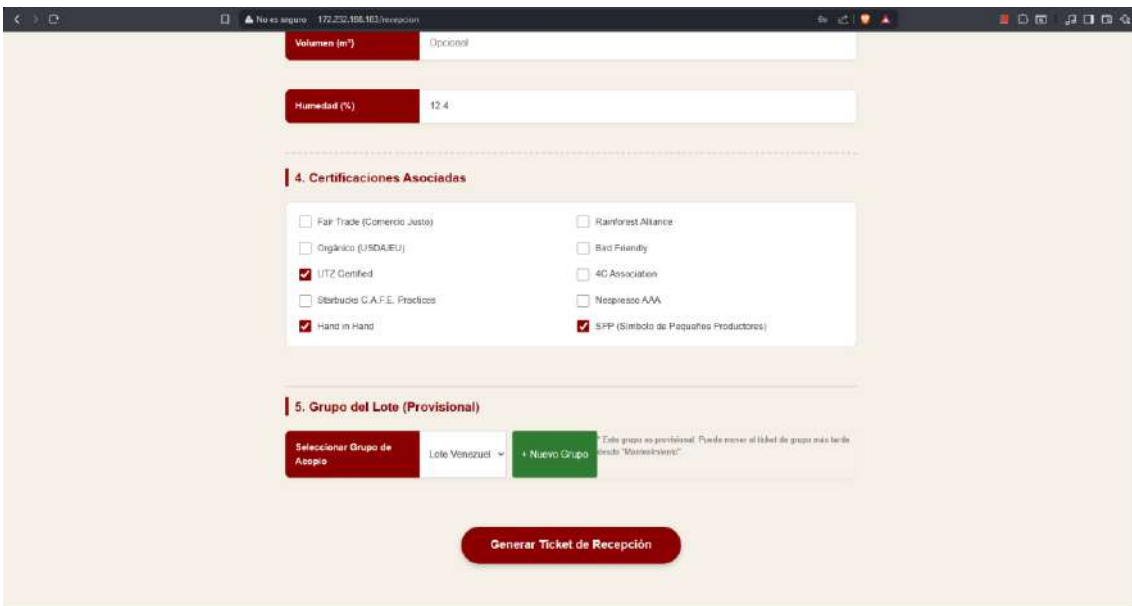
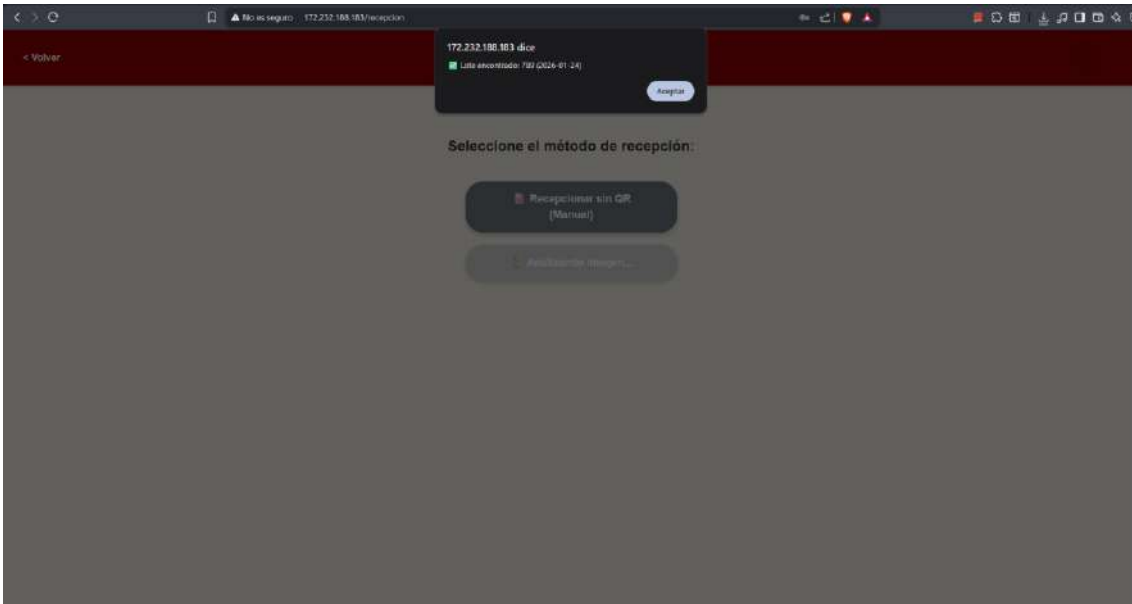
- Nombre cosecha:** A text input field.
- Parcela:** A dropdown menu with the placeholder text 'Seleccione una parcela registrada...'
- Producto:** A dropdown menu with the placeholder text 'Primero seleccione una parcela...'
- Peso (kg):** A text input field.
- Fecha:** A date picker field showing 'dd/mm/aaaa'.

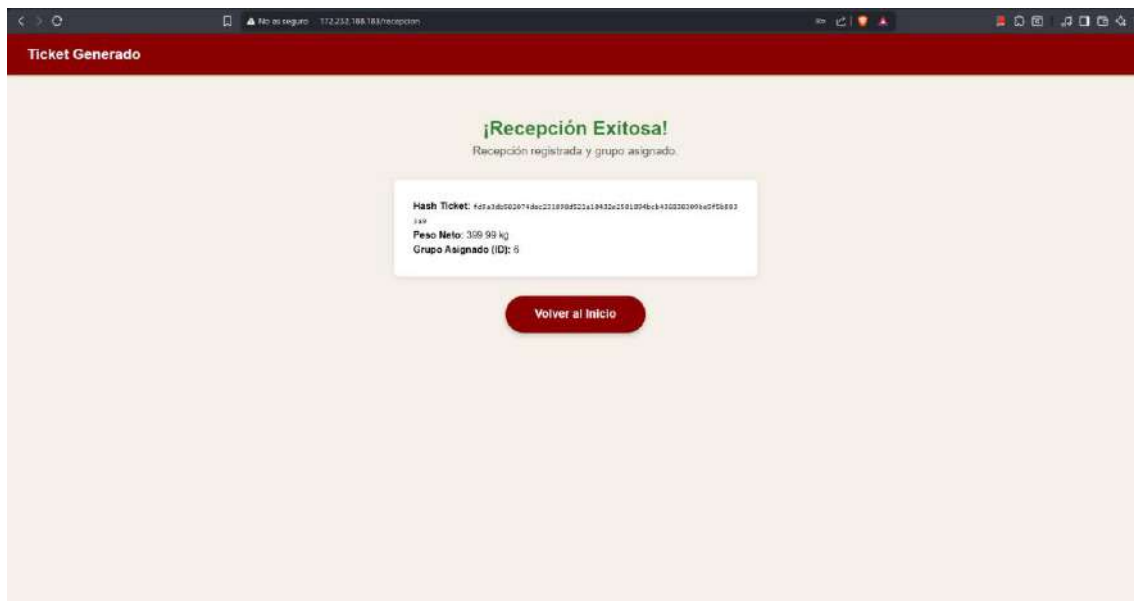
Below the form is a button labeled 'Enviar a la blockchain'.

5. Marque las certificaciones asociadas (ej. Comercio Justo, UTZ, Orgánico) y asigne el ingreso a un "Grupo de Acopio" provisional.
6. Haga clic en **Generar Ticket de Recepción**.

Resultado del Sistema: Se genera un **Bloque Ticket de Pesada**. Este ticket queda enlazado criptográficamente al Bloque de Cosecha original, asegurando que el peso corresponde estrictamente a ese origen.







5.2.2. Mantenimiento de Grupos (Batching/Mezcla)

Descripción: Permite consolidar varios ingresos (tickets) de distintos agricultores para crear un lote final de exportación en un contenedor.

Ruta: [IP_del_Servidor]/mantenimiento

Pasos a seguir:

1. Ingrese a **Mantenimiento de Grupos**.
2. En el panel izquierdo ("Área de Trabajo"), visualizará los tickets pendientes.
3. Seleccione los múltiples *Tickets de Pesada* disponibles y asígneles al lote de destino (ej. "Lote Venezuela-EEUU").
4. Una vez que el lote tenga el peso deseado, haga clic en **Cerrar y Generar Bloque**. Confirme la acción, recordando que es irreversible.

Resultado del Sistema: Se genera el **Bloque de Acopio**. El sistema calcula automáticamente un **Hash Merkle (Merkle Root)**. Esta es una "huella digital maestra" que condensa la información de todos los tickets seleccionados, garantizando de por vida que ninguno fue alterado individualmente.

172.232.168.183/mantenimiento

Mantenimiento de Grupos

Actualizar + Nuevo Grupo

Area de Trabajo (Grupos Activos)

Sin Asignar
No hay tickets.

Lote Venezuela-EEUU
1 tickets | 399.99 kg

ID: 00
2026-01-24T11:55
Mover a:
Lote Venezuela-EEUU

(Máximo 2 tickets)

Histórico (Grupos Cerrados)

Lote Colombia-Peru	Lote Bolivia-Argentina	Lote Uruguay-Brasil	Lote Argentina-Peru	Lote Peru-Chile
Canada 2 tickets 180.00 kg	Canada 2 tickets 20.99 kg	Canada 2 tickets 225.00 kg	Canada 2 tickets 250.00 kg	Canada 2 tickets 264.96 kg
ID: 4 2026-01-19T18:07	ID: 9 2026-01-19T19:11	ID: 14 2026-01-19T19:33	ID: 20 2026-01-19T19:53	ID: 26 2026-01-20T09:31
ID: 5 2026-01-19T18:06	ID: 10 2026-01-19T19:12	ID: 15 2026-01-19T19:34	ID: 21 2026-01-19T19:53	ID: 24 2026-01-20T09:30
100 kg	13.99 kg	100 kg	145 kg	88.99 kg
80 kg	15 kg	120 kg	145 kg	114.99 kg

172.232.168.183/mantenimiento

Mantenimiento de Grupos

Actualizar + Nuevo Grupo

Area de Trabajo (Grupos Activos)

Sin Asignar
No hay tickets.

Lote Venezuela-EEUU
2 tickets | 603.99 kg

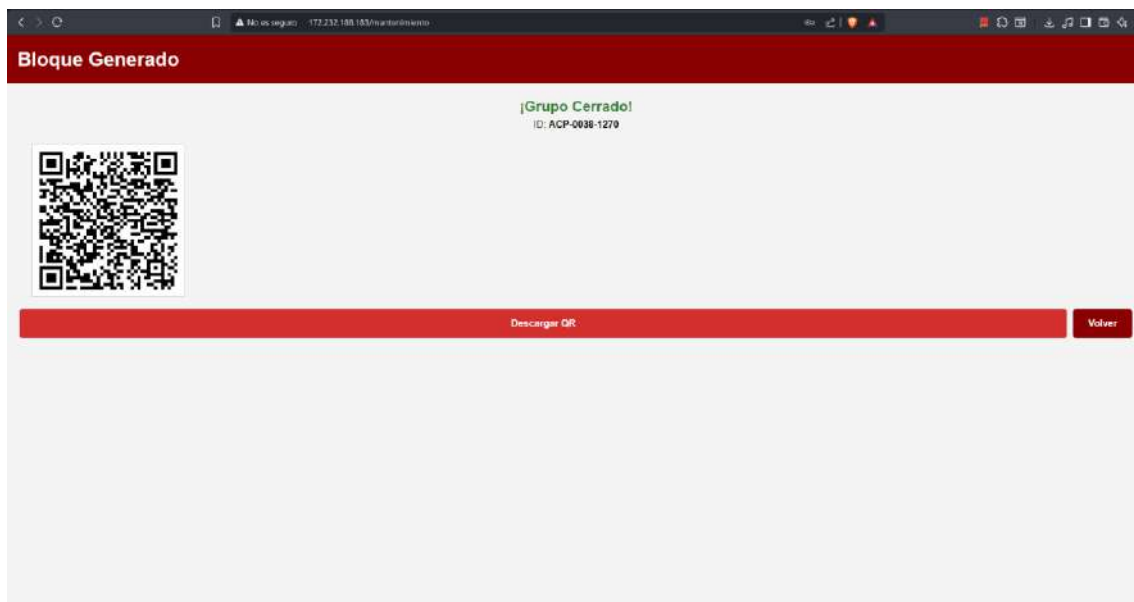
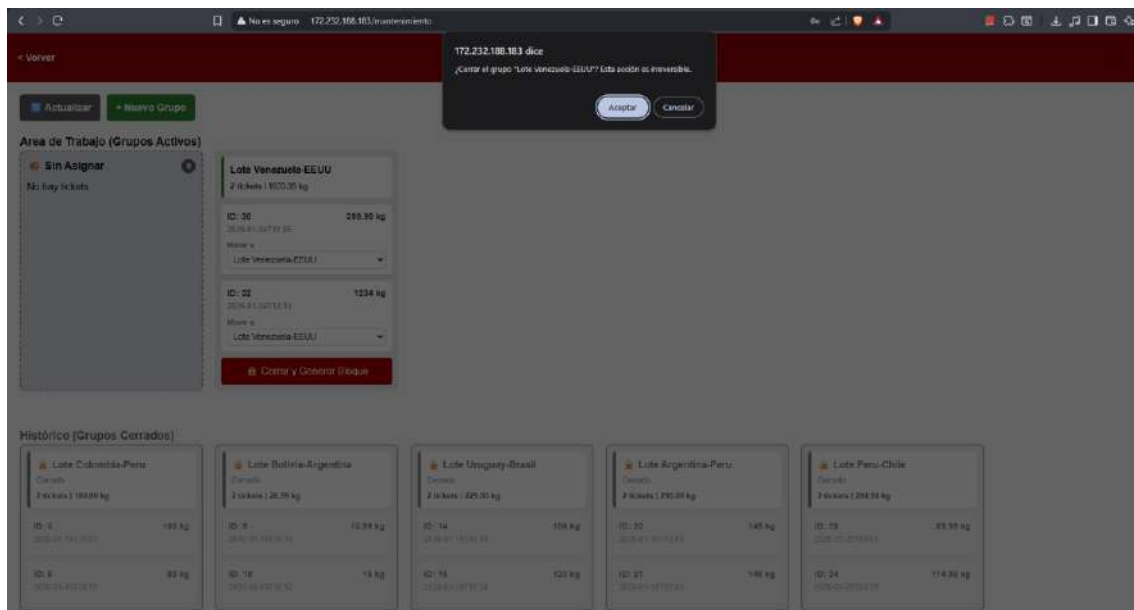
ID: 00
2026-01-24T11:55
Mover a:
Lote Venezuela-EEUU

ID: 02
2026-01-24T12:01
Mover a:
Lote Venezuela-EEUU

Cerrar y Generar Bloqueo

Histórico (Grupos Cerrados)

Lote Colombia-Peru	Lote Bolivia-Argentina	Lote Uruguay-Brasil	Lote Argentina-Peru	Lote Peru-Chile
Canada 2 tickets 180.00 kg	Canada 2 tickets 20.99 kg	Canada 2 tickets 225.00 kg	Canada 2 tickets 250.00 kg	Canada 2 tickets 264.96 kg
ID: 4 2026-01-19T18:07	ID: 9 2026-01-19T19:11	ID: 14 2026-01-19T19:33	ID: 20 2026-01-19T19:53	ID: 26 2026-01-20T09:31
ID: 5 2026-01-19T18:06	ID: 10 2026-01-19T19:12	ID: 15 2026-01-19T19:34	ID: 21 2026-01-19T19:53	ID: 24 2026-01-20T09:30
100 kg	12.99 kg	100 kg	148 kg	89.99 kg
80 kg	15 kg	120 kg	145 kg	114.99 kg



5.3. Perfil de planta de proceso y exportación (cooperativas o empresas)

El perfil de planta de proceso y exportación finaliza la cadena logística en territorio nacional y genera la documentación legal y aduanera exigida por la normativa EUDR.

5.3.1. Gestión de Datos Empresariales (Configuración)

Descripción: Configuración previa y obligatoria para emitir documentación legal.

Ruta: [IP_del_Servidor]/datos-exportador

Pasos a seguir:

1. Haga clic en **Datos del Exportador**.
2. Complete la "Identificación del Operador Responsable" (Razón Social, Dirección, Número EORI, País de Origen y Destino UE).
3. Defina los datos de la Persona de Contacto y el Firmante.
4. Haga clic en **Guardando....** (Nota: Estos parámetros son obligatorios antes de intentar generar cualquier reporte de producción).

Complete esta información para que aparezca automáticamente en sus reportes de producción EUMR.

1. Identificación del Operador Responsable

Nombre o Razón Social
Ej: Exportadora Café del Norte S.A.C.

Dirección completa
Av. Principal 123, Lima

Número EORI
Ej: PE123456789012

País de Origen: Perú País de Destino (UE): Seleccione destino...

2. Persona de Contacto

Nombre: _____ Cargo: _____
Correo: _____ Teléfono: _____

3. Firmante (Configuración por Defecto)

Firmado en nombre de (Entidad): _____

172.232.188.183 dice: Datos actualizados correctamente

123456

País de Origen: Perú

2. Persona de Contacto

Nombre: Angelo Cargo: Jefe
Correo: angelo@una.pe Teléfono: 996088777

3. Firmante (Configuración por Defecto)

Firmado en nombre de (Entidad): UNA

Nombre y Apellidos: Angelo Cargo: Jefe

Fecha (Default): 24/01/2025

Firma
(La línea digital no generará el reporte)

Guardando...

5.3.2. Recepción de embarque y Declaración de diligencia debida EUDR

Descripción: Aceptación formal del lote consolidado en puerto o planta final y emisión del documento de debida diligencia. **Ruta:** [IP_del_Servidor]/produccion

Pasos a seguir:

1. Seleccione **Realizar Producción (EUDR)**.
2. Escanee el código QR del **Bloque de Acopio** proporcionado por el Acopiador. El sistema validará la integridad del *Hash Merkle*.
3. El sistema autocompletará el formulario de Declaración EUDR con los datos de la empresa, el producto, el peso final y listará las coordenadas geográficas de **todas las fincas** que aportaron a este lote, indicando el estado de riesgo (ej. OK o Alerta).
4. Haga clic en **Generar Declaración**.

Resultado del Sistema: Se forja el Bloque Final y se genera el **Reporte de Producción (PDF/QR)**. Este documento estampa los datos de la empresa junto con toda la traza inmutable de la Blockchain (Finca -> Cosecha -> Tickets -> Acopio -> Exportación), listo para presentar en aduanas europeas.



1. Identificación del Operador

Nombre / Razón Social	Asoc. Villa Florida Mz B L16 19 - Puente Piedra
123456	País de Origen: Perú
País de Destino (UE)	Alemania
Jefe	angelo@uni.pe
99988777	

2. Producto

Producto (BC)	Cacao (Trinitario), Cafe (Arabico)	Nombre Comercial
Código HS/A		
Descripción		
Peso (BC)	213.97	Unidad: Kg

3. Origen y Geolocalización

Produtor / Finca	Ubicación	Coordenadas Geográficas	Área (ha)	Estado
Angel Príncipe Finca Los Hornos 123	Lima / Lima / Miraflores	(-6.9192, -76.9899)(-8.4193, -76.9800)(-6.9192, -76.9898)	0.00	OK
Angel Príncipe Finca Los Hornos	Lima / Lima / Puente Piedra	(-3.0096, -3.0000)(2.9999, 2.9999)(-1.0000, -1.9998)	0.00	Alerta

Las parcelas no han sido deforestadas (verificar)
Cumple legislación ambiental vigente.

4. Riesgo

No se ha detectado riesgo.
Riesgo despreciable (ninguno).

7. Firma

UNI	24/01/2020
Angelo	Jefe

Generar Declaración

¡Producción Registrada!

Bloque EXP-0039-26A8

35a623618547c849202e403399354735496751e0e3887f5328614A803838



Descargar PDF

Descargar QR

Volver al Dashboard

6. Productos y Certificados que genera el sistema

Al utilizar correctamente la plataforma, el sistema generará de forma automática activos digitales y documentos con valor probatorio.

6.1. NFT (Token No Fungible) de Parcela

Es el primer producto que genera el sistema. Al registrar una finca y verificar mediante Inteligencia Artificial que no existe deforestación, se emite un **NFT Hash**. Este código alfanumérico es la "identidad digital" inalterable de la parcela y avala su cumplimiento normativo.

6.2. Bloques Criptográficos (Cosecha, Ticket, paquete de embarque, exportación)

A lo largo del proceso, la Blockchain forja distintos "Bloques" que representan las etapas de la cadena de suministro:

- **Bloque de Cosecha:** Genera un Código QR que el productor debe entregar (física o digitalmente) junto con sus sacos de café/cacao.
- **Bloque Ticket de Pesada:** Un registro inmutable del peso exacto entregado en el acopio, protegiendo tanto al productor como al comprador.
- **Bloque de Acopio (Merkle Root):** Genera un Código QR final que agrupa criptográficamente decenas de tickets individuales en un solo contenedor.

6.3. Reporte de Producción (Declaración EUDR)

Es el documento final (exportable en PDF). Contiene la declaración oficial de debida diligencia exigida por la Unión Europea, detallando el exportador, el peso final, y un listado con todas las coordenadas GPS de las fincas de origen.

7. Buenas prácticas para el usuario

Para asegurar una operación fluida y sin errores, recomendamos seguir estas pautas:

- **Cuidado de Credenciales:** Su usuario y contraseña son firmas digitales. Nunca comparta estos datos; cualquier acción realizada con su cuenta es su responsabilidad legal.

- **Verificación de Coordenadas:** Al registrar una finca, asegúrese de ingresar correctamente la latitud y longitud. Un error numérico podría ubicar su parcela fuera del mapa y generar un falso positivo de deforestación.
- **Protección de los QR:** Si imprime los códigos QR de los Lotes de Cosecha, evite que el papel se manche, doble o humedezca para asegurar una lectura rápida en el centro de acopio.
- **Cierre de Sesión:** Siempre cierre su sesión (botón superior derecho) al terminar de usar el sistema, especialmente en computadoras compartidas en la cooperativa.

8. ¿Para qué sirve este sistema en la práctica?

Este sistema no es solo una base de datos; es una herramienta de confianza criptográfica utilizada para:

- **Garantizar Exportaciones a la UE:** Permite demostrar matemáticamente que el café o cacao no proviene de zonas deforestadas (Cumplimiento EUDR).
- **Evitar Fraudes:** Al estar en una Blockchain, nadie puede alterar los pesos de las básculas registrados en el acopio ni cambiar fechas de forma maliciosa.
- **Auditorías Inmediatas:** Un auditor o comprador extranjero puede escanear el QR final y ver instantáneamente todo el linaje del producto hasta llegar al agricultor.

9. Solución de Problemas Comunes (Troubleshooting)

9.1. Problemas de acceso y registro

- **Error:** *"Credenciales incorrectas" o "No puedo iniciar sesión"*. **Solución:** Verifique que no haya espacios en blanco al inicio o final de su correo. Si olvidó su contraseña, debe comunicarse con el Administrador de la Cooperativa, ya que por seguridad en la Blockchain no hay reseteo automático.
- **Error:** *"Sesión Expirada" o el sistema lo devuelve al inicio.* **Solución:** Por seguridad, las sesiones caducan tras horas de inactividad. Vuelva a iniciar sesión en [IP_del_Servidor]/login.

9.2. Errores al registrar polígonos o parcelas

- **Problema:** *"La parcela figura con Estado de Alerta roja por deforestación".*
Solución: El motor de Inteligencia Artificial detectó pérdida de bosque. Revise que las coordenadas GPS ingresadas correspondan exactamente a su parcela de cultivo y no a una zona boscosa adyacente.
- **Problema:** *"No aparece mi parcela en la lista al intentar hacer una cosecha".*
Solución: Asegúrese de haber finalizado y guardado correctamente el "Registro de Finca" en el paso anterior.

9.3. Hashes o códigos QR no reconocidos

Error: *"El lector QR no reconoce el código del agricultor".*

Solución: Asegúrese de tener buena iluminación. Si el QR físico está dañado, utilice la opción "**Recepcionar sin QR (Manual)**" ingresando el código del lote.

10. Checklist de Uso Rápido por Perfil

Para el Productor:

1. Inicie sesión correctamente.
2. Registré mi Finca y obtuve mi NFT.
3. Registré mi Cosecha con el peso estimado.
4. Descargué o imprimí mi Código QR para llevarlo al acopio.

Para el Acopiador:

1. Inicie sesión en mi estación de pesaje.
2. Escaneé el QR del productor al recibir los sacos.
3. Ingresé el peso neto real en la báscula y generé el Ticket.
4. Fui a "Mantenimiento", agrupé los tickets y "Cerré el Grupo" para generar el Merkle Root.

Para el Exportador:

1. Llené los "Datos del Exportador" en configuración (Una sola vez).

2. Escaneé el QR del Lote de Acopio final.
3. Verifiqué el país de destino.
4. Generé y descargué el PDF de la "Declaración EUDR".

UNIVERSIDAD NACIONAL DE INGENIERÍA



Manual API de Integración Técnica: EUDR-BlockChain (v1.0)

**Blockchain y Validación Geoespacial para la Trazabilidad Agrícola en
Cumplimiento Normativo EUDR**

PROYECTO: PROCIENCIA – PE501093703-2024

2026

Contenido

1. Introducción	3
2. Arquitectura Offline-First y Flujo de Trabajo	3
3. Autenticación y Seguridad	3
3.1. Uso de API Key (x-api-key)	4
3.2. Uso de JWT Token (Authorization: Bearer)	4
4. Algoritmo de Hashing Criptográfico (SECCIÓN CRÍTICA)	4
4.1. Reglas estrictas de limpieza (Sanitización del Payload)	4
4.2. Fórmula Final de Hashing (SHA-256)	5
5. Referencia de Endpoints (API REST)	5
5.1. Endpoints de Inicialización	5
5.1.1. Obtener Catálogos Base (GET /mobile/catalogs)	5
5.1.2. Registro de Usuario Offline (POST /mobile/sync-user)	6
5.1.3. Login Móvil (POST /mobile/login)	6
5.2. Endpoints Transaccionales (Blockchain)	7
5.2.1. Sincronización de Parcela / NFT (POST /mobile/sync-parcela)	7
5.2.2. Sincronización de Cosechas / Lotes (POST /mobile/sync-lotes)	7
5.2.3. Sincronización de Acopio / Merkle Root (POST /mobile/sync-acopio)	8
6. Guía de Depuración de Hashes (Troubleshooting)	9
6.1. ¿Qué hacer si obtiene "hash_match": false?	9
6.2. Uso del parámetro debug_string_server	9
6.3. Errores comunes de serialización	9
7. Checklist de Integración Rápida	10

1. Introducción

El presente documento establece las directrices, reglas criptográficas y la referencia de *endpoints* necesarios para integrar aplicaciones móviles (Android/iOS) con el **Backend Blockchain EUDR**.

El objetivo de esta API no es solo recibir datos, sino garantizar que la información recolectada en zonas rurales mantenga su integridad criptográfica desde el dispositivo del usuario hasta su inserción en la cadena de bloques.

2. Arquitectura Offline-First y Flujo de Trabajo

La API Móvil está diseñada bajo una arquitectura estrictamente **Offline-First**. Esto significa que la aplicación móvil debe estar preparada para operar en zonas agrícolas sin conexión a internet.

El flujo de trabajo obligatorio para la App Móvil es el siguiente:

1. **Captura Local:** Almacenar todos los datos transaccionales (parcelas, cosechas, acopios) en la base de datos local del dispositivo (ej. SQLite / Room).
2. **Firma Criptográfica Local:** La aplicación móvil es la única encargada de generar los **Hashes criptográficos** en el momento exacto de la operación en campo.
3. **Sincronización Asíncrona (Lotes):** Cuando el dispositivo detecte una conexión a internet estable, enviará los paquetes de datos al servidor. El servidor recalculará los hashes recibidos; si coinciden, el bloque se considerará válido y se guardará en la Blockchain.

3. Autenticación y Seguridad

La API utiliza dos capas de seguridad distintas dependiendo del nivel de criticidad del *endpoint*:

3.1. Uso de API Key (x-api-key)

Utilizada para autorizar a la aplicación móvil en sí misma para consumir recursos base. Es requerida para operaciones de inicialización o donde el usuario aún no tiene una sesión activa (ej. Login, Registro Offline de usuarios, Descarga de Catálogos).

- **Implementación:** Debe enviarse obligatoriamente en las cabeceras (*Headers*) de la petición HTTP.
- **Formato:** x-api-key: <tu_api_key_proporcionada>

3.2. Uso de JWT Token (Authorization: Bearer)

Utilizada para identificar al usuario final que está realizando una transacción. Es requerida para todas las operaciones de escritura en la Blockchain (Sincronización de parcelas, lotes y acopios).

- **Implementación:** Se obtiene tras consumir exitosamente el *endpoint* de Login.
- **Formato:** Debe enviarse en el Header como Authorization: Bearer <token_jwt>.

4. Algoritmo de Hashing Criptográfico (SECCIÓN CRÍTICA)

Para que el servidor acepte y mine los bloques enviados por la aplicación móvil, **el Hash SHA-256 generado en el celular (ya sea en Kotlin, Swift o Flutter) debe ser matemáticamente idéntico al que calculará el servidor.**

Dado que ambos sistemas operan en lenguajes distintos, es **obligatorio** que el móvil sanitice (limpie) el JSON antes de encriptarlo.

4.1. Reglas estrictas de limpieza (Sanitización del Payload)

Antes de aplicar la función de Hash, el diccionario de datos (JSON) debe pasar por el siguiente filtro exacto:

- **Regla 1 (Sin IDs Locales):** Elimine cualquier clave que se llame exactamente id o que termine en los sufijos `_id` o `_ids` (ej. `parcela_id`, `producto_id`). Los IDs de SQLite del celular no existen en la nube y romperán la Blockchain.
- **Regla 2 (Sin Hashes):** Elimine las claves `hash` o `nft_hash`, ya que son el resultado del cálculo y no pueden ser parte del input.

- **Regla 3 (Sin Nulos ni Vacíos):** Elimine cualquier clave cuyo valor sea null o un *string* vacío "".
- **Regla 4 (Normalización de Números):** Si su lenguaje móvil tipa un número entero como flotante añadiendo un decimal cero (ej. 68.0), debe serializarlo estrictamente como entero (68).

4.2. Fórmula Final de Hashing (SHA-256)

Una vez aplicado el filtro anterior, convierta el diccionario a un *String* JSON aplicando la **Regla 5 (Orden y Espacios)**:

- Las llaves del JSON deben estar ordenadas alfabéticamente.
- **No deben existir espacios** después de las comas o los dos puntos (Formato: {"a":1,"b":"texto"}).
- No escape los caracteres Unicode (tildes, letras ñ). Deben enviarse crudos (UTF-8).

Finalmente, aplique la siguiente fórmula para obtener el Hash de 64 caracteres:

Hash = SHA256 (JSON_LIMPIO_STRING_ORDENADO + PREVIOUS_HASH)

(Nota: El valor del PREVIOUS_HASH dependerá del endpoint que esté consumiendo y se especificará en la Referencia de la API).

5. Referencia de Endpoints (API REST)

Todas las peticiones deben enviarse con el encabezado Content-Type: application/json.

5.1. Endpoints de Inicialización

5.1.1. Obtener Catálogos Base (GET /mobile/catalogs)

Descarga la lista maestra de productos (ej. Café, Cacao) para poblar la base de datos local (SQLite/Room) del dispositivo móvil.

- **Método y Ruta:** GET /mobile/catalogs
- **Headers requeridos:** x-api-key: <tu_api_key>
- **Respuesta Exitosa (200 OK):**

```
{
  "productos": [
    { "id": 1, "nombre": "CACAO" },
    { "id": 2, "nombre": "CAFE" }
  ]
}
```

5.1.2. Registro de Usuario Offline (POST /mobile/sync-user)

Sincroniza un usuario (Productor o Acopiador) que fue creado en el campo sin conexión a internet.

- **Método y Ruta:** POST /mobile/sync-user
- **Headers requeridos:** x-api-key: <tu_api_key>
- **Payload (Cuerpo):**

```
{
  "nombre": "Juan Perez",
  "email": "juan@test.com",
  "password": "123",
  "dni": "70123456",
  "rol": "productor"
}
```

- **Respuesta Exitosa (201 Created):** Retorna status, server_id y el codigo_generado (ej. PR-0001).

5.1.3. Login Móvil (POST /mobile/login)

Autentica al usuario contra el servidor y devuelve el Token JWT necesario para transacciones Blockchain.

- **Método y Ruta:** POST /mobile/login
- **Headers requeridos:** x-api-key: <tu_api_key>
- **Payload (Cuerpo):**

```
{
  "credential": "juan@test.com",
  "password": "123"
}
```

- **Respuesta Exitosa (200 OK):** Retorna el objeto user y el string token.

5.2. Endpoints Transaccionales (Blockchain)

5.2.1. Sincronización de Parcela / NFT (POST /mobile/sync-parcela)

Registra el polígono geográfico. El servidor evaluará la deforestación y validará el Hash NFT.

- **Método y Ruta:** POST /mobile/sync-parcela
- **Headers requeridos:** Authorization: Bearer <token>
- **Previous Hash para cálculo local:** String vacío "".
- **Payload (Cuerpo):**

```
{
  "nombre_parcela": "Mi Finca",
  "departamento": "San Martín",
  "provincia": "Tocache",
  "distrito": "Zapatero",
  "poligono": [[-6.55, -76.50], [-6.56, -76.51], [-6.54, -76.51]],
  "productos_nombres": ["CACAO"],
  "nft_hash": "hash_calculado_localmente"
}
```

- **Respuesta Exitosa (201 Created):** Retorna deforestacion_status (booleano indicando si es legal) y match (booleano validando si su hash coincide con el del servidor).

5.2.2. Sincronización de Cosechas / Lotes (POST /mobile/sync-lotes)

Sincroniza uno o múltiples bloques génesis de cosecha. **Este endpoint es idempotente:** soporta reintentos seguros si se cae la red.

- **Método y Ruta:** POST /mobile/sync-lotes
- **Headers requeridos:** Authorization: Bearer <token>

- **Previous Hash para cálculo local:** 64 ceros ("00").
- **Payload (Cuerpo):**

```

{
  "lotes": [
    {
      "nombreCosecha": "Lote 01",
      "fecha": "2026-02-24",
      "hora": "14:30:00",
      "pesoKg": 55.5,
      "producto_nombre": "CACAO",
      "parcela_id": 12,
      "hash": "hash_calculado_localmente"
    }
  ]
}

```

- **Respuesta Exitosa (201 Created):** Devuelve un array de detalles. Si el status es "already_synced" o "ok", usted debe marcar ese registro como "subido" en su BD local.

5.2.3. Sincronización de Acopio / Merkle Root (POST /mobile/sync-acopio)

Sincroniza el bloque contenedor que agrupa múltiples tickets escaneados mediante el Árbol de Merkle.

- **Método y Ruta:** POST /mobile/sync-acopio
- **Headers requeridos:** Authorization: Bearer <token>
- **Previous Hash para cálculo local:** 64 ceros ("00").
- **Payload (Cuerpo):**

```
{
  "acopios": [
    {
      "merkle_root": "raiz_merkle_escaneada_qr",
      "cantidad_exportable": 1500.0,
      "fecha_actual": "2026-02-24 18:00:00",
      "hash": "hash_calculado_localmente"
    }
  ]
}
```

6. Guía de Depuración de Hashes (Troubleshooting)

6.1. ¿Qué hacer si obtiene "hash_match": false?

Si el servidor responde con un estado HTTP 201 pero el campo "hash_match" es false, significa que los datos se guardaron, pero **la firma criptográfica de su aplicación móvil es distinta a la del servidor.**

6.2. Uso del parámetro debug_string_server

Para solucionar esto inmediatamente, el servidor le enviará una variable de ayuda llamada "debug_string_server" dentro del detalle del error.

1. Ese campo contiene el **String exacto (letra por letra)** que el servidor de Python utilizó antes de pasarlo por la función SHA-256.
2. Imprima en la consola de su entorno móvil (LogCat / Xcode Console) el String que usted generó.
3. Compare ambos textos frente a frente.

6.3. Errores comunes de serialización

Generalmente, la discrepancia entre el texto del móvil y del servidor radica en:

- **Espacios residuales:** Un espacio extra después de una coma o dos puntos generados por su librería JSON.
- **IDs Locales infiltrados:** Olvidó excluir un campo `_id` (ej. `parcela_id`) de su objeto antes de convertirlo a texto.

- **Tipos de datos:** Un número con punto decimal (.0) que no fue normalizado a entero antes de hashear.

7. Checklist de Integración Rápida

- Tengo la x-api-key configurada en las constantes de mi App.
- Desarrollé una función cleanPayload() que elimina IDs locales, nulos y la propia llave hash antes de encriptar.
- Mi función convierte campos Float como 68.0 a Int 68.
- Mi serializador JSON ordena las llaves alfabéticamente y no deja espacios en blanco.
- Almaceno el Token JWT y lo envío como Bearer en los endpoints de Sincronización.
- Implementé lógica para marcar como "Sincronizado" un lote si el servidor me devuelve "status": "already_synced".