Fomento a la construcción de capacidades en relación a las políticas públicas apoyadas por Contratos de Reforma Sectorial (CRS) en Bolivia

Fortalecimiento de la capacidad institucional en los sectores de desarrollo integral con coca, tráfico ilícito de drogas y seguridad alimentaria para una eficiente gestión del apoyo presupuestario sectorial en Bolivia

LCN 026 Diseño del Sistema Único Integrado de Información sobre Narcotráfico (SUIN)

ANEXO 9: Desarrollo del SUIN

Contrato N° DCI/LA/2017/392-699

N° de identificación: EuropeAid/138320/IH/SER/BO

Proyecto Financiado por la Unión Europea

Implementada por el consorcio:
AGRER — DT GLOBAL— COWATER SA
Bruselas, febrero 2023

Disclaimer:

Este informe ha sido elaborado por el consorcio AGRER/DT Global/Cowater con financiamiento de la Unión Europea. Las opiniones aquí expresadas son del consultor y no expresan necesariamente las de la Comisión Europea.

Fortalecimiento de la capacidad institucional en los sectores de desarrollo integral con coca, tráfico ilícito de drogas y seguridad alimentaria para una eficiente gestión del apoyo presupuestario sectorial en Bolivia (DITISA).

Contrato LA/2017/392-699 DITISA

Misión de Corta Duración Nº. LCN - 026
"Diseño del Sistema Único Integrado de Información sobre Narcotráfico (SUIN)"

ANEXO 9: Desarrollo del SUIN

Consultores:
Jaime Fuentes
Cristian Paucara

La Paz / Bruselas, febrero de 2023

Consorcio AGRER – DT GLOBAL – COWATER

CONTENIDO

1. INTRODUCCIÓN 6
2. ANTECEDENTES 6
3. OBJETIVOS DE LA MISIÓN 7
4. DESARROLLO DEL SUIN 7
4.1. Arquitectura del sistema 7
4.2. Módulos del SUIN 7
4.3. Roles y permisos 8
4.4. Herramientas de desarrollo 9
4.5. Frontend 10
4.6. Backend 11
4.7. Base de datos 12
4.8. Seguridad 12
4.9. Calidad del producto 13
4.10. Ambiente de test 14
5. CONCLUSIONES 14
6. RECOMENDACIONES 15
7. ANEXOS 16
7.1. ANEXO 1: CÓDIGO FUENTE 16
7.2. ANEXO 2: MANUALES DE USUARIO 16
Anexo 7.2.1. Manual Administrador 16
Anexo 7.2.2. Manual de la Entidad 16
Anexo 7.2.3 Manual OBSCD 16
7.3. ANEXO 3: MANUAL DE INSTALACIÓN 16
7.4. ANEXO 4: ACTAS DE REUNIÓN 16

FIGURAS

Figura 1: Arquitectura del SUIN 7
Figura 2: Frontend del SUIN 10
Figura 3: Backend del SUIN 11
Figura 4: Base de datos del SUIN 12
Figura 5: SUIN en ambiente de test 14

TABLAS

Tabla 1: Módulos de SUIN 7
Tabla 2: Roles y permisos para el SUIN 8
Tabla 3: Tecnologías empleadas en el SUIN 9

1. INTRODUCCIÓN

El Sistema Único de Información sobre Narcotráfico (SUIN) tiene el propósito de centralizar información inherente al narcotráfico de diferentes Entidades, mediante la interoperabilidad de sistemas cuya finalidad es el de generar reportes estadísticos.

El diseño y desarrollo del Sistema Único Integrado de Información sobre Narcotráfico (SUIN) están contemplados en el Plan Operativo Anual del Ministerio de Gobierno, y en el Componente 5 del Apoyo Presupuestario Sectorial. La propuesta de diseño se realizó a partir de la información presentada en el diagnóstico, y en coordinación con el equipo técnico del Observatorio Boliviano de Seguridad Ciudadana y Lucha Contra las Drogas (OBSCD) y del Área de Tecnologías y Sistemas del Ministerio de Gobierno.

A partir de las condiciones de las Entidades sobre su infraestructura tecnológica, sistemas informáticos y principalmente en la administración de sus datos, se proyectó una alternativa para la integración inicial al SUIN, siendo este mediante el envío de archivos. Posteriormente, en la medida que las Entidades mejoren sus condiciones, podrán integrarse mediante servicios web, cumpliendo de esta forma con la interoperabilidad entre el SUIN y las Entidades.

El documento contiene la estructura del Sistema Único de Información sobre Narcotráfico – SUIN, que se elaboró a partir de la definición del diseño planteado en el producto 3. Así mismo, contiene el código fuente, manuales de administrador, OBSCD y entidad.

2. ANTECEDENTES

Entre las conclusiones del segundo producto entregable “Diagnóstico SUIN”, se señala que, entre las entidades identificadas que generan información relacionada a narcotráfico, solamente con dos se puede interoperar a corto plazo, la Fiscalía General del Estado y la Dirección General del Régimen Penitenciario. También se señaló que existen seis entidades, que también generan información relevante relacionada a narcotráfico, que no están en condiciones de interoperar en un corto plazo, estas entidades son: Dirección General de la Fuerza Especial de la Lucha Contra el Narcotráfico (DGFELCN), el Viceministerio de Defensa Social y Sustancias Controladas (VDSySC), la Dirección General de Sustancias Controladas (DGSC), la Dirección de Registro, Control y Administración de Bienes Incautados (DIRCABI), el Tribunal Supremo de Justicia y el Ministerio de Salud. En ese sentido, deben buscarse métodos alternativos para que las entidades señaladas reporten información estadística.

A partir del diagnóstico presentado, se realizó el diseño conceptual del SUIN. Entre los módulos contemplados se encontraban: Inicio de sesión, Administración, Datos, Reportes, Ayuda y Logs.

3. OBJETIVOS DE LA MISIÓN

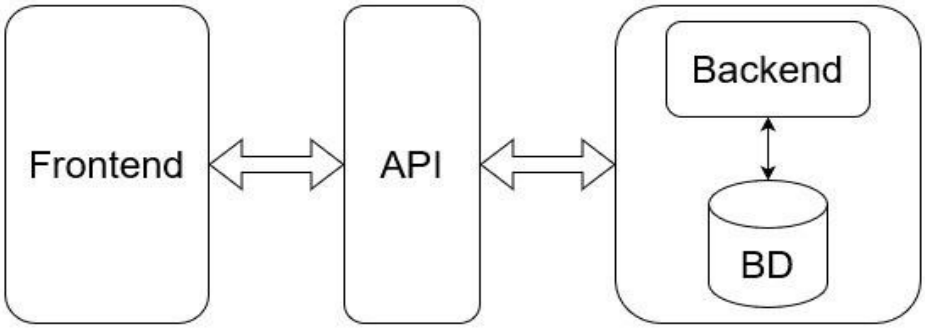
El objetivo del presente documento es presentar el desarrollo del Sistema Único Integrado de Información sobre Narcotráfico (SUIN) para su posterior implementación.

4. DESARROLLO DEL SUIN

4.1. Arquitectura del sistema

La arquitectura del SUIN se basa en una capa de *backend* que se comunica con la base de datos, y que alimenta a la capa de *frontend* a través de servicios API.

Figura 1: Arquitectura del SUIN



Fuente: Elaboración propia

4.2. Módulos del SUIN

Los módulos presentados en el diseño fueron actualizados según las coordinaciones sostenidas con el OBSCD. Entre los cambios más relevantes se dividió el módulo de "Datos" en dos módulos: "Datos de entrada" y "Datos validados" para diferenciar las funcionalidades. Considerando que las entidades dependientes del Ministerio de Gobierno señalaron que están en condiciones de interoperar con el SUIN, o enviar información mediante archivos Excel, se posterga la implementación de un formulario para el envío de información, hasta que alguna entidad así lo requiera. En ese sentido, los módulos actualizados del SUIN se presentan en la siguiente tabla.

Tabla 1: Módulos de SUIN

Módulo	Objetivo	Funcionalidades
Inicio de sesión	Gestionar el acceso al sistema	Iniciar y cerrar sesión
		Recuperar contraseña
		Cambiar contraseña
Administración		Leer, crear, actualizar y eliminar entidades

	Permitir la gestión de entidades y usuarios	Leer, crear, actualizar y eliminar usuarios
Datos de entrada	Gestionar envío, almacenamiento y consulta de información de entrada	Leer, crear, actualizar y eliminar configuración de datos de entrada
		Configurar envío de información por archivo y servicio web
		Enviar datos mediante archivo
		Solicitar datos mediante servicios web
Datos validados	Gestionar envío, almacenamiento y consulta de información validada	Leer, crear, actualizar y eliminar configuración de datos validados
		Leer, crear, actualizar y eliminar datos validados
Reportes	Acceder a reportes	Ver reportes (gráficos, indicadores, entidades)
		Descargar datos
Ayuda	Ayudar al usuario	Ver manual de usuario
Logs	Visualizar los logs del sistema	Crear y ver logs

Fuente: Elaboración propia

4.3. Roles y permisos

Los roles de usuario contemplados para el sistema son: usuario Administrador, usuario OBSCD y usuario Entidad. Cada usuario tiene diferentes funcionalidades

- **Administrador:** El administrador del sistema tiene la finalidad de administrar usuarios, realizar configuraciones sobre datos de archivo e interoperabilidad.
- **OBSCD:** El usuario OBSCD del sistema tiene la finalidad de validar datos, generar reportes y realizar el seguimiento a las Entidades sobre la información.
- **Entidad:** Son Entidades cuya función principal es el de enviar datos al SUIN con el propósito de generar reportes estadísticos de interés.
- **Reportes:** Son usuarios que tiene permisos para ver los reportes.

Los permisos que tiene cada rol en el SUIN se presentan en la siguiente tabla:

Tabla 2: Roles y permisos para el SUIN

Módulo	Funcionalidades	Admin	OBSCD	Entidad	Reportes
Administración	Leer, crear, actualizar y eliminar entidades	CRUD	CRUD	-	-
	Leer, crear, actualizar y eliminar usuarios	CRUD	CRUD	-	-
Datos de entrada	Leer, crear, actualizar y eliminar configuración de datos de entrada	CRUD	R	-	-
	Configurar envío de información por archivo y servicio web	CRUD	R	-	-

	Enviar datos de entrada (archivo y servicio web)	CRUD	CRUD	CR	-
Datos validados	Leer, crear, actualizar y eliminar configuración de datos validados	CRUD	R	-	-
	Leer, crear, actualizar y eliminar datos validados	CRUD	CRUD	-	-
Reportes	Ver reportes (gráficos, indicadores, entidades)	R	R	R	R
	Descargar datos	R	R	R	R
Ayuda	Ver manual de usuario	R	R	R	R
Logs	Crear y ver logs	R	-	-	-

Fuente: Elaboración propia

4.4. Herramientas de desarrollo

Las herramientas que se utilizaron en el desarrollo son:

Tabla 3: Tecnologías empleadas en el SUIN

Tecnología	Lenguaje
Base de datos	PostgreSQL 15
Frontend	Vue.js v3 Vuetify 3 Vue-chartjs Vuex Axios
Backend	Node.js v18 Express.JS Axios Bcrypt Joi Json Web Token Morgan Passport Winston

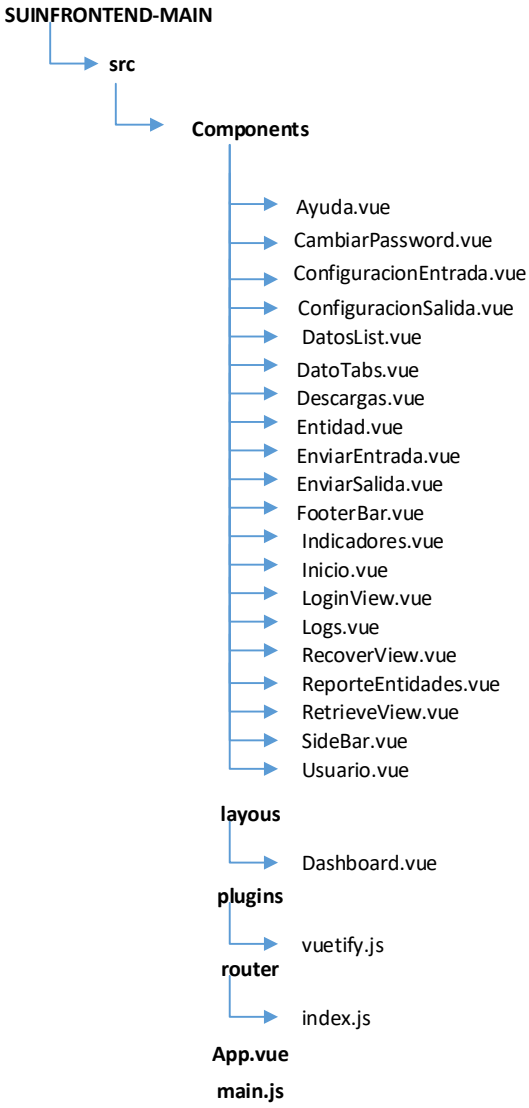
Fuente: Elaboración propia

4.5. Frontend

El SUIN presenta una interfaz amigable e intuitiva que permite acceder a los usuarios para su administración, generación de información y emisión de reportes. Hace referencia a los elementos del SUIN, los cuales pueden interactuar con el usuario

La organización del repositorio del frontend se presenta en la siguiente figura.

Figura 2: Frontend del SUIN

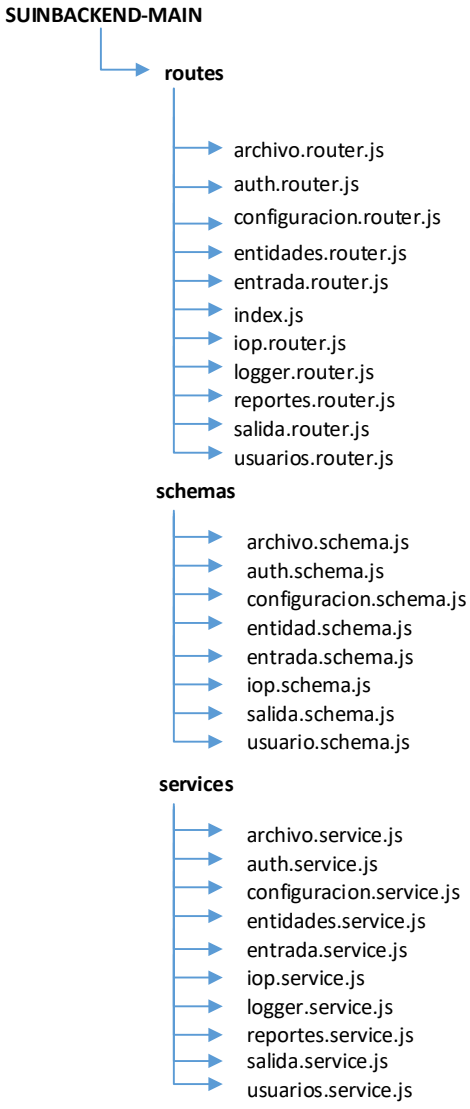


Fuente: Elaboración propia

4.6. Backend

El backend es el encargado de la conexión con la base de datos y contiene la lógica del negocio. El repositorio del backend se estructura de la siguiente manera.

Figura 3: Backend del SUIN

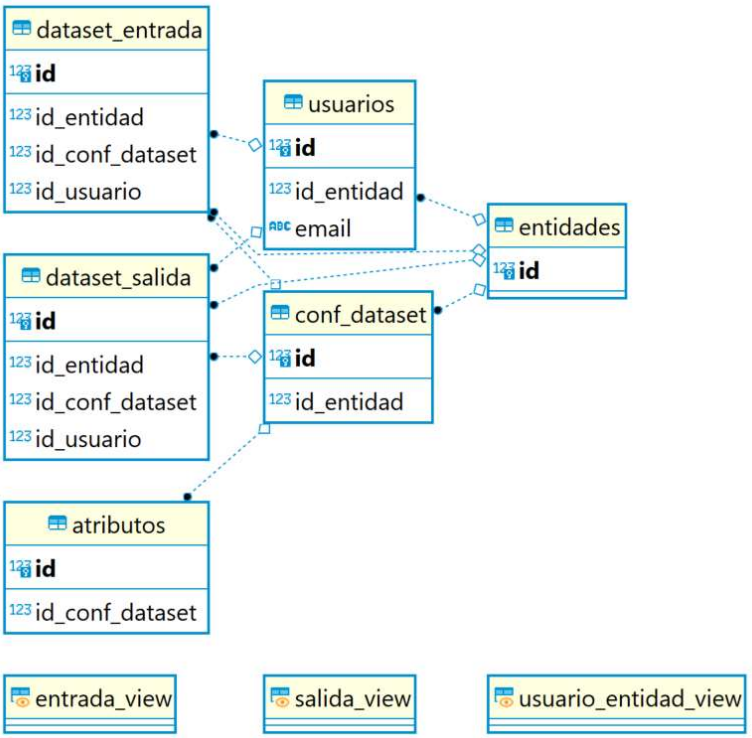


Fuente: Elaboración propia

4.7. Base de datos

Se utiliza una base de datos relacional, guardando la información estadística en formato JSON. El modelo entidad relación de la base de datos utilizado se presenta en la siguiente figura.

Figura 4: Base de datos del SUIN



Fuente: Elaboración propia

4.8. Seguridad

Considerando que el sistema será administrado por una entidad pública, los criterios de seguridad se basan en los "Lineamientos para la elaboración e implementación de los Planes Institucionales de Seguridad de la Información de las entidades del sector público". Los Lineamientos establecen 11 controles de seguridad de información, de estos 11 criterios, los que corresponden al desarrollo de software son dos: control de accesos y criptografía.

a) Control de accesos

Para el control de accesos, el diseño y desarrollo del SUIN contempla que:

- Cada persona cuenta con un usuario y contraseña en el sistema, y así evitar que varias personas compartan el mismo usuario.
- Opción de eliminar cuentas, para evitar su acceso al sistema.
- Registros de inicio de sesión.

- Considerando las especificidades del SUIN, se optó un inicio de sesión mediante cookies.

b) Criptografía

Con el fin de preservar la confidencialidad, autenticidad e integridad de la información, se procede a almacenar las contraseñas encriptadas. Para este fin se hace uso de la librería *bcrypt*.

c) Otros controles

Adicionalmente, se registran otros controles para preservar la seguridad del sistema:

- Registros de logs de todas las peticiones realizadas.
- Registros de acciones realizadas por los usuarios.
- Controles de acceso en *frontend* y *backend*.

Siguiendo los Lineamientos de seguridad, se sugiere que se prevea al momento de la implementación la seguridad en recursos humanos, gestión de activos de información, seguridad física y ambiental, seguridad de las operaciones, seguridad de las comunicaciones, gestión de incidentes de seguridad de la información y plan de contingencias.

4.9. Calidad del producto

la familia de estándares ISO/IEC 25010, permiten determinar la calidad en uso del software a partir de siete características:

- Adecuación funcional: El sistema desarrollado cumple con la funcionalidad principal requerida, que es la centralización de información estadística que generan las entidades públicas.
- Fiabilidad: El sistema desarrollado funciona en condiciones normales, también se prevé que esté disponible las 24 horas del día, y en caso de algún fallo es posible reiniciar el sistema *backend* y *frontend*, sin ninguna consecuencia.
- Eficiencia en el desempeño: El sistema desarrollado tiene tiempos de procesamiento apropiados, y su funcionamiento tampoco demanda muchos recursos, pues la cantidad de usuarios concurrentes es baja.
- Facilidad de uso: El sistema desarrollado tiene funcionalidades bien definidas, se hace uso de íconos para ser más intuitivo, también se proporciona mensajes claros y concisos al usuario para guiar y para mostrar posibles errores.
- Compatibilidad: El sistema desarrollado tiene la capacidad de comunicarse con otros sistemas mediante servicios web.
- Mantenibilidad: El sistema desarrollado puede ser modificado y actualizad, además de estar organizado en módulos para poder incrementar más funcionalidades en el futuro.
- Portabilidad: El sistema desarrollado puede ser instalado en sistemas operativos Linux y Windows, y del lado del cliente, puede ser utilizado en diferentes navegadores web.

4.10. Ambiente de test

El sistema fue instalado en un ambiente de test del ministerio de gobierno, bajo el enlace http://165.172.19.62:8080, como se observa en la siguiente figura.

Figura 5: SUIN en ambiente de test

Fuente: SUIN

El código fuente del sistema, y la base de datos se encuentra en el Anexo 1. Los manuales de instalación y los manuales de usuario se encuentran en los anexos 2 y 3.

5. CONCLUSIONES

Las conclusiones son las siguientes:

- El desarrollo del SUIN se realizó a partir del diagnóstico y diseño conceptual, considerando las condiciones de interoperabilidad de las entidades, y en coordinación con el OBSCD.
- El SUIN desarrollado permite centralizar la información generada por las entidades, y sistematizar la información estadística procesada por el OBSCD.
- Las Entidades relacionadas con información sobre narcotráfico podrán integrarse al SUIN con el propósito de enviar información para generar reportes estadísticos.

6. RECOMENDACIONES

Las recomendaciones son las siguientes:

- Realizar una etapa piloto para encontrar nuevos requerimientos a incorporar en el SUIN.
- Para la implementación, considerar los siguientes controles de seguridad: en recursos humanos, gestión de activos de información, seguridad física y ambiental, seguridad de las operaciones, seguridad de las comunicaciones, gestión de incidentes de seguridad de la información y plan de contingencias
- Realizar una implementación por etapas, iniciando con las entidades dependientes del Ministerio de Gobierno, y con el objetivo de centralizar y sistematizar la información estadística; posteriormente, generar indicadores estadísticos; finalmente, incorporar a otras entidades.

7. ANEXOS

7.1. ANEXO 1: CÓDIGO FUENTE

Entregado a la entidad beneficiaria

7.2. ANEXO 2: MANUALES DE USUARIO

Anexo 7.2.1. Manual Administrador

Anexo 7.2.2. Manual de la Entidad

Anexo 7.2.3 Manual OBSCD

7.3. ANEXO 3: MANUAL DE INSTALACIÓN

7.4. ANEXO 4: ACTAS DE REUNIÓN