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

Informe Final de Misión de Corta Duración ATI

Validación y análisis a los módulos desarrollados del SISCOCA, para su posterior implementación

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 — AECOM — TRANSTEC

La Paz / Bruselas, septiembre 2020

Disclaimer:

Este informe ha sido elaborado por el consorcio AGRER/AECOM/TRANSTEC 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 Nº DCI/LA/2017/392-699

Misión DI-023-1: Validación y análisis a los módulos desarrollados del SISCOCA, para su posterior implementación

Informe final

Autor:

Ricardo Laredo – Experto en Sistemas y Jefe de Equipo

Rinna Chipana – Experto en Control de Calidad

Bruselas, septiembre 2020

Consorcio AGRER – AECOM – TRANSTEC

Contenido

ANEXOS

Anexo 1 _ TdR de la misión
Anexo 2_ Comité Selección
Anexo 3_Hojas de presencia
Anexo 4_ReporteOwasp

1. Resumen Ejecutivo

El presente trabajo de consultoría presenta el análisis y evaluación general del Sistema Único de la Coca – SISCOCA, sistema desarrollado por el Ministerio de Desarrollo Rural y Tierras del Gobierno del Estado Plurinacional de Bolivia. Dicho sistema ha sido cuidadosamente analizado en el ámbito técnico y se lo ha sometido a test's con diferentes herramientas de software, encontrándose que posee diversos problemas de rendimiento, tratamiento de procesos transaccionales, validación de datos en la capa de servicios, formularios de la aplicación web y una arquitectura monolítica que carece de características empresariales, tales como, manejo de transacciones para garantizar la unicidad de la base de datos, soporte para procesos concurrentes y otros especificados en la sección Análisis de arquitectura.

El estado actual del sistema "Siscoca" en el ambiente de desarrollo es inoperable, producto de las pruebas realizadas.

A continuación, se encuentran descritos detalladamente los tipos de problemas encontrados:

TIPO DE PROBLEMA	RESULTADO	CLASIFICACIÓN
Pruebas de estrés	En una prueba de estrés de 30 peticiones con una frecuencia de una petición por segundo, se logró dejar el sistema fuera de servicio. El sistema no implementa ninguna técnica de paginación en los API REST de recuperación de datos; por consiguiente, los tiempos de respuesta de las interfaces web que visualizan los datos toman entre 30 segundos y 2 minutos en las interfaces más usadas. El sistema implementa algoritmos de generación de código único (código de productor, comercializador, etc.) que son inadecuados para procesos concurrentes y de alto tráfico. El sistema extrae datos innecesarios que causan lentitud al momento de cargar los datos en las interfaces web.	Crítico
Análisis de manejo de transacciones en procesos críticos	El sistema no implementa validaciones de datos en los formularios de las interfaces web ni en ninguna interfaz de la capa de servicios.	Crítico

	El sistema no implementa ningún concepto de manejo de transacciones para asegurar la unicidad y consistencia de la base de datos.	
Divulgación de datos sensibles del servidor	El sistema no maneja correctamente las excepciones que se generan en los procesos de la capa de servicios; por ende, cuando se genera alguna excepción a nivel de código o a nivel de base de datos se envía hasta la aplicación web los errores con información sensible del servidor y de la base de datos, mismos que podría ser utilizados por un atacante para explotar vulnerabilidades a nivel de Sistema Operativo o Base de Datos.	Crítico
Pruebas funcionales	El sistema no contempla control sobre duplicidad de registros, longitudes máximas, obligatoriedad de campos, tipos de datos ni excepciones, lo que provoca que el usuario final manipule de forma incorrecta el sistema y genere inconsistencia a nivel de Base de Datos. Los componentes de carga de archivo y hora no funcionan correctamente. Para el primer caso, el sistema ofrece información errónea al usuario. El componente hora no recupera la información ingresada. La funcionalidad de reconocimiento facial demora varios minutos en ejecutarse y en la mayoría de los casos el proceso no es exitoso, por lo que no es posible finalizar el respectivo flujo. Algunos flujos no lograron ser finalizados debido a problemas de generación de código correlativo o funcionalidad de componentes.	Crítico
Pruebas de diseño	Al realizar pruebas de compatibilidad, se verificó que el sistema no carga en el navegador Internet Explorer, pero si lo hace desde Microsoft Edge. Al realizar pruebas de navegabilidad y usabilidad al sistema, se identificó que al contraer el menú de opciones no es posible navegar con normalidad por la aplicación. Los roles DIGCOIN/OII/CLIENTE presentan	Crítico

	acceso denegado al navegar por las diferentes opciones de menú disponibles. El sistema contempla errores ortográficos y de acentuación. Por otro lado, algunos componentes y mensajes de éxito/error se muestran en idioma inglés.	
Análisis de código fuente de lado del servidor (Backend)	Los resultados del análisis estático del código fuente, muestran que no existen errores de programación.	Crítico
Análisis de código fuente de la aplicación web (Frontend)	Los resultados de análisis estático del código fuente, muestran que existen 14 errores en la programación de la aplicación web	Crítico
Análisis de vulnerabilidades del sistema	En el escaneo de seguridad realizado con la herramienta **Owasp ZAP**, se han detectado las siguientes vulnerabilidades críticas: • Dos observaciones de “Inyección SQL”. • 165 observaciones de “Sobrecarga de Memoria” que causan la caída del servidor.	Crítico
Análisis de arquitectura	Se realizó el análisis de arquitectura en base a seis criterios básicos y se concluye que la arquitectura implementada no es la adecuada para un sistema empresarial concurrente, transaccional y de alto tráfico.	Crítico

2. Marco Normativo

El Decreto Supremo N° 3318 que reglamenta la Ley 906 “Ley General de la Coca”, establece en su Artículo 49 inciso I) que el Sistema Único de la Coca – SISCOCA, es el registro informático digitalizado de todas actividades vinculadas a la Coca y determina en su inciso II) que el Viceministerio de Coca y Desarrollo Integral es la instancia competente de la administración del SISCOCA, debiendo registrar como mínimo los siguientes datos:

a. Detalle de Productores y comerciantes al detalle.
b. Empresas de industrialización, instituciones de investigación públicas y privadas u otras de similar naturaleza, autorizadas para la adquisición y transporte de hoja coca en su estado natural.
c. Emisión, renovación, duplicado o sustitución del carnet del productor y del comercializador.
d. Cambio de área y/o puesto de venta de productores al detalle y de comerciantes al detalle.
e. Sustitución del registro del productor y del comercializador de la hoja de coca en su estado natural.
f. Productores que realicen trueque.

g. Resoluciones administrativas sancionatorias ejecutoriadas con especificaciones de las infracciones y sanciones.
h. Otros datos que el Viceministerio de Coca y Desarrollo Integral considere necesario.

Además, señala en el inciso III que el Viceministerio de Defensa Social y Sustancias Controladas dependiente del Ministerio de Gobierno, será quien acceda a la consulta de todos los datos registrados en SISCOCA, en línea y tiempo real; asimismo, proporcionará al Viceministerio de Coca y Desarrollo Integral dependiente del Ministerio de Desarrollo Rural y Tierras, copia de todos los registros de productores de coca.

3. Marco de Referencia

El Sistema Único de la COCA (SISCOCA) conceptualmente constituye una herramienta fundamental dentro la ejecución de la nueva Estrategia de Desarrollo Integral Sostenible para los Yungas de La Paz y el Trópico de Cochabamba (EDIS YLP-TC). En la Estrategia se postula que una mejora en los sistemas de control de la producción y comercialización de la coca, es indispensable para estabilizar la superficie cultivada con hoja de coca en Bolivia o para reducirla. En virtud a lo establecido, el SISCOCA constituye la herramienta principal para organizar y monitorear la producción y comercialización de hoja de coca.

Su desarrollo se ejecuta en el marco del apoyo que brinda la Unión Europea representada por la Comisión Europea, encargada del financiamiento del sistema SISCOCA y por cuenta del Ministerio de Desarrollo Rural y Tierras del Gobierno del Estado Plurinacional de Bolivia, contexto bajo el que se requiere el servicio de consultoría en su primera fase a cargo de la empresa MC4 S.R.L., para evaluar, probar e informar sobre el estado actual del sistema.

4. Introducción

En el marco del objetivo general determinado para la consultoría, el cuales es contribuir a la mejora de los sistemas de control de la producción y comercialización de la hoja de coca y de los objetivos específicos establecidos en los Términos de Referencia para la misión de corta duración referidos al control de calidad de los módulos desarrollados de SISCOCA por parte de MDRyT, la identificación de puntos débiles y la emisión de recomendaciones para resolver los puntos débiles detectados.

El trabajo realizado se realizó a partir del análisis de la documentación recibida, de artefactos de software provistos y la revisión de los trece módulos, en el marco de la metodología de trabajo detallada en el punto 6 del presente documento y la aplicación de las herramientas informáticas más adecuadas para el análisis.

4.1. Alcance de la misión

Los trabajos de análisis se iniciaron sobre la base de los siguientes documentos y artefactos de software provistos por sus respectivos responsables:

NOMBRE	RESPONSABLE	RUTA	HASH
TdR Validación SISCOCA 0706.docx	Marko Lehto, Jefe de Equipo de DITISA-UE.	Enviado mediante correo electrónico.	
Código Fuente "siscoca-02072020.tar.gz"	Mario Adolfo Valverde Suarez, Responsable Área de Sistema del Ministerio de Desarrollo Rural y Tierras. Gonzalo Poma, Técnico en Sistema del Ministerio de Desarrollo Rural y Tierras	SISCOCA-02072020/INFORMACION SISCOCA/SISCOCA BK DE SERVIDORES DE PRUEBA Compartido mediante Google Drive	d08f41aad89b5386171d4fb47119ff11
Script "siscoca02072020.sql"	Mario Adolfo Valverde Suarez, Responsable Área de Sistema del Ministerio de Desarrollo Rural y Tierras. Gonzalo Poma, Técnico en Sistema del Ministerio de Desarrollo Rural y Tierras	SISCOCA-02072020/INFORMACION SISCOCA/SISCOCA BK DE SERVIDORES DE PRUEBA	eb27e53df0bcb3d0d349dfdae82cf59e
siscoca_schema.sql	Gonzalo Poma, Técnico en Sistema del Ministerio de Desarrollo Rural y Tierras	Enviado mediante correo electrónico.	
Manual de Usuario	Mario Adolfo Valverde Suarez, Responsable Área de Sistema del Ministerio de Desarrollo Rural y Tierras. Gonzalo Poma, Técnico en Sistema del Ministerio de Desarrollo Rural y Tierras	SISCOCA-02072020/INFORMACION SISCOCA/siscoca final entregado por consultores/M	65d2e6204ed2d12226b29dafb74c3d04

		anual de usuario	
Manual Técnico	Mario Adolfo Valverde Suarez, Responsable Área de Sistema del Ministerio de Desarrollo Rural y Tierras. Gonzalo Poma, Técnico en Sistema del Ministerio de Desarrollo Rural y Tierras	SISCOCA-02072020/INFORMACION SISCOCA/siscoca final entregado por consultores/Manual Técnico	d6d754b1ee430ec28a73d6511eebbcca
INFORME FINAL: DISEÑO SISTEMA SISCOCA	Mario Adolfo Valverde Suarez, Responsable Área de Sistema del Ministerio de Desarrollo Rural y Tierras. Gonzalo Poma, Técnico en Sistema del Ministerio de Desarrollo Rural y Tierras	SISCOCA-02072020/INFORMACION SISCOCA/siscoca final entregado por consultores/Documento MC-4/FINAL SISCOCA 2019-06-16.pdf	7c8df30465c016bbc654a27a974026a9
Ruta de aplicación https://siscoca.ruralytierras.gob.bo/index	Gonzalo Poma, Técnico en Sistema del Ministerio de Desarrollo Rural y Tierras	Acceso de la Aplicación IP Pública: 181.115.188.149 usuario: admin@admin.com password: admin	

5. Metodología de Trabajo

El trabajo de análisis se centró en cuatro puntos específicos descritos en la siguiente tabla:

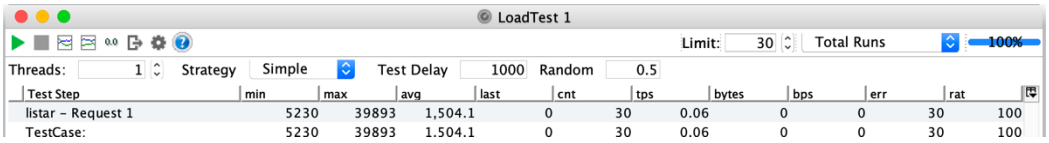
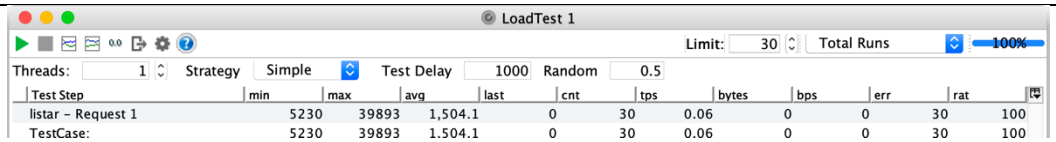
TRABAJO	DESCRIPCIÓN
Análisis de rendimiento del sistema.	Para este análisis se revisó el código fuente con el fin de determinar si las técnicas de paginación, manejo de transacciones y procesos concurrentes fueron implementados. Se realizaron pruebas de concepto para evidenciar las fallas a nivel de transacciones y los procesos concurrentes. Se utilizaron las herramientas SOAP UI, OWASP ZAP y el navegador Chrome para simular y evidenciar escenarios de alto tráfico (estrés) con el objetivo de determinar si el sistema está desarrollado para trabajar en escenarios de alto tráfico con procesos concurrentes y si garantiza la unicidad y confiabilidad de los datos.
Análisis funcional del sistema.	Para este análisis se utilizó la técnica de caja negra, en la que se analiza la funcionalidad el sistema sin tomar en cuenta la estructura interna del código fuente, con el objetivo de revisar manualmente las funcionalidades del sistema y determinar si: • Las funcionalidades del sistema realizan sus operaciones de manera apropiada y correcta. • Las interfaces web aplican validaciones a los datos de entrada. • Si se logra completar los flujos de negocio, es decir, registrar productores, comercializadores, industrializadores; generación de los respectivos carnets, registro y control de las rutas de internación y hojas de ruta. • Los mensajes emitidos por el sistema son adecuados.
Análisis estático de código fuente.	Para el análisis estático de código fuente se utilizó la herramienta "SonarQube" con el objetivo de determinar si existen errores de programación a nivel de código fuente.
Análisis de seguridad de la aplicación.	Para el análisis de seguridad se utilizó la herramienta OWASP ZAP. OWASP ZAP, ejecuta diferentes pruebas con el propósito de determinar vulnerabilidades de seguridad, de rendimiento, errores no controlados que

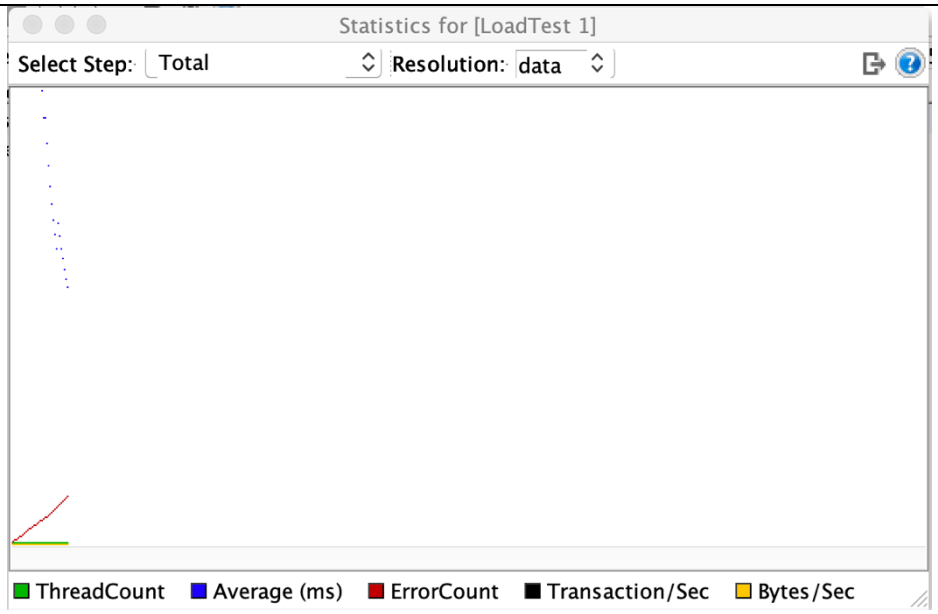
	permitan divulgar información sensible del servidor y uso de cabeceras de seguridad.

6. Resultados de Análisis

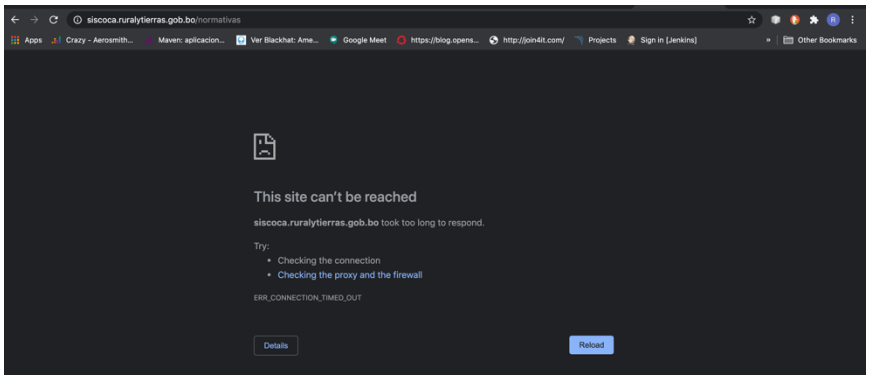
6.1. Análisis de rendimiento del sistema

6.1.1. Pruebas de estrés

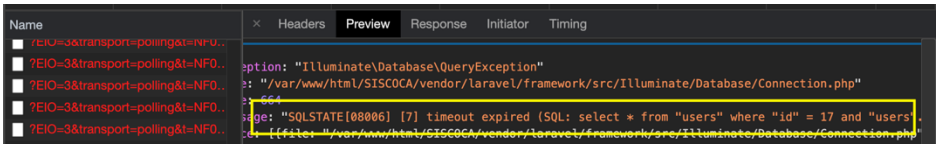
Paginación en la recuperación de datos	
Gravedad	Alto
URL	https://siscoca.ruralytierras.gob.bo/lista_eventos https://siscoca.ruralytierras.gob.bo/reclamos_portal_info https://siscoca.ruralytierras.gob.bo/productores https://siscoca.ruralytierras.gob.bo/comercializadores https://siscoca.ruralytierras.gob.bo/productores-al-detalle https://siscoca.ruralytierras.gob.bo/api/persona
Módulo	Módulo de Registro
Riesgo	Caída del servicio
Causa	Usando la herramienta SOAP UI, se programó 30 solicitudes con frecuencia de una solicitud por segundo.  Con esta prueba de estrés, el servidor dejó de responder 10 segundos después de haber iniciado la prueba.
Posible Solución	Se realizaron pruebas de estrés a la url https://siscoca.ruralytierras.gob.bo/api/persona que obtiene la lista de personas registradas en la base de datos. Revisar que los servicios web, implementen técnicas de paginación y que no retornen entidades con todas sus relaciones.
Evidencia	 Programación de las pruebas de estrés. De las 30 peticiones enviadas ninguna fue exitosa, los tiempos de respuesta y el promedio de los tiempos de respuesta fue aproximadamente 15 segundos.



Estadística de las pruebas de estrés realizadas.

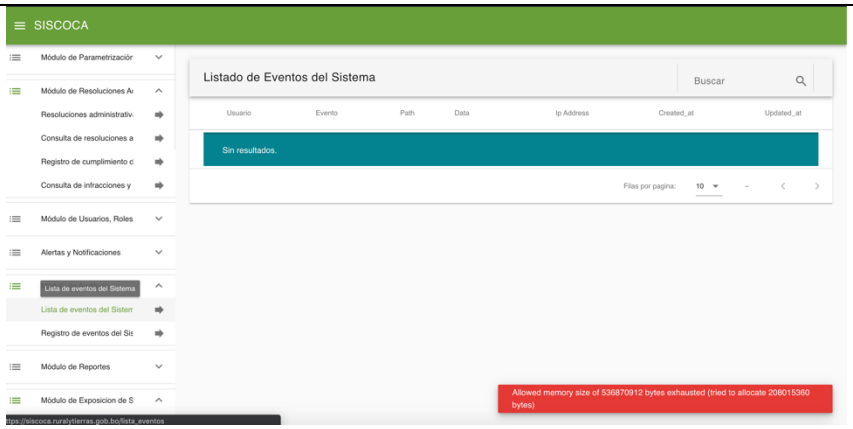


El servidor no responde por aproximadamente una hora.



Después de recuperado el servicio, algunas funcionalidades presentaron problemas de acceso a la base de datos y solo se solucionó reiniciando el servidor de base de dados.

Paginación en la recuperación de datos	
Gravedad	Alto
URL	https://siscoca.ruralytierras.gob.bo/lista_eventos https://siscoca.ruralytierras.gob.bo/reclamos_portal_info https://siscoca.ruralytierras.gob.bo/productores https://siscoca.ruralytierras.gob.bo/comercializadores https://siscoca.ruralytierras.gob.bo/productores-al-detalle https://siscoca.ruralytierras.gob.bo/caracteristicas_produccion
Módulo	-Módulo de Registro -Módulo de Portal Informativo -Módulo de Gestión de Actividades de Producción -Módulo de Actividades de Comercialización e Industrialización -Módulo de Parametrización -Módulo de Usuarios, Roles y Permisos -Módulo de Auditoria
Riesgo	Se revisaron todos los controladores que exponen interfaces de servicios web del sistema y se evidenció que ninguno implementa la técnica de paginación en la recuperación de datos, lo cual repercute significativamente en el tiempo respuesta de las interfaces web que recuperan datos.
Causa	El hecho de no implementar paginación en la recuperación de datos repercute necesariamente en mayor tráfico en la red, mayor procesamiento del motor de base de datos, mayor consumo de la memoria del servidor y sobre todo, en la experiencia de usuario, puesto que las interfaces que visualizan los datos toman mayor tiempo en la obtención de los datos.
Posible Solución	Se debe implementar la técnica de paginación en la recuperación de datos en las interfaces y servicios web que manejen gran volumen de datos.
Evidencia	En el “Módulo de Auditoria” la funcionalidad “Listado de Eventos del Sistema” es el principal afectado al momento del presente análisis por no implementar la paginación en la recuperación de datos. Esta funcionalidad lista los diferentes eventos que se registran en el sistema, cuando se intenta acceder a la mencionada funcionalidad se genera el error “Allowed memory size of 536870912 bytes exhausted (tried to allocate 155488256 bytes)”, esto indica que el límite establecido en memoria RAM para ejecutar PHP ha sido sobrepasado.



Interfaz de “Lista de Eventos del Sistema”

Esto sucede porque el API REST https://siscoca.ruralytierras.gob.bo/api/action/index intenta recuperar todo el contenido de la tabla “Action”.

```php
/**
 * Display a listing of the resource.
 *
 * @return \Illuminate\Http\Response
 */
public function index()
{
    return Action::with('user')->whereNotNull('user_id')->get();
}
```

Consulta para obtener el resultado.

Generación códigos únicos	
Gravedad	Medio
URL	https://siscoca.ruralytierras.gob.bo/productores https://siscoca.ruralytierras.gob.bo/productores-al-detalle https://siscoca.ruralytierras.gob.bo/comercializadores https://siscoca.ruralytierras.gob.bo/empresas https://siscoca.ruralytierras.gob.bo/entidad-de-investigacion https://siscoca.ruralytierras.gob.bo/beneficiarios-de-donaciones https://siscoca.ruralytierras.gob.bo/beneficiarios-de-desarrollo https://siscoca.ruralytierras.gob.bo/guias_internacion https://siscoca.ruralytierras.gob.bo/hojas_de_ruta https://siscoca.ruralytierras.gob.bo/api/persona POST
Módulo	-Módulo de Registro -Módulo de Actividades de Comercialización e Industrialización
Riesgo	Es posible generar códigos de productores, comercializadores, etc. Duplicados.

Causa	Se ha implementado un algoritmo inadecuado para generación de códigos; el mismo consiste en obtener el último registro y sumarle una unidad. Este algoritmo funciona de manera errónea en sistemas altamente transaccionales y no es recomendado para procesos concurrentes, puesto que dos procesos podrían a la misma vez obtener el mismo registro y sumarle una unidad con lo que se podría generar códigos repetidos.

Posible Solución	En el algoritmo de generación de códigos se debe considerar usar la ***secuencia*** proporcionados por el motor de base de datos, el mismo garantiza que todo número que genere siempre será único; utilizar esta técnica optimiza y da mayor seguridad.
	Ejemplo.
	//Comando para crear secuencia
	create sequence seq_codigo_productor
	
	//Comando para recuperar una secuencia
	select *nextval*('seq_codigo_productor');

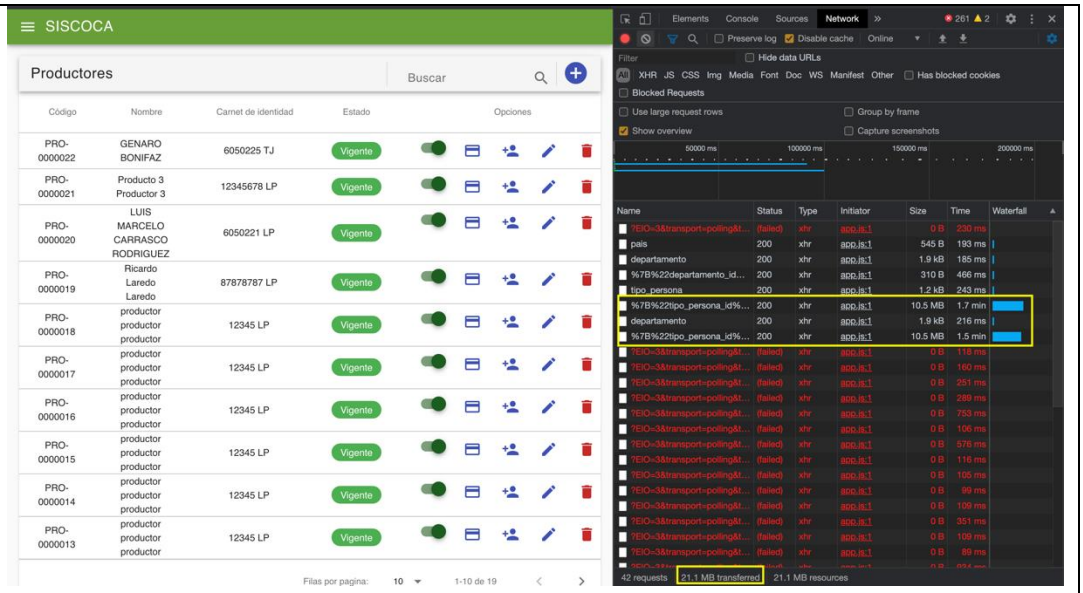
Evidencia	El sistema utiliza un algoritmo inadecuado para generar el código de los productores, comercializadores, etc.

PersonaController.php

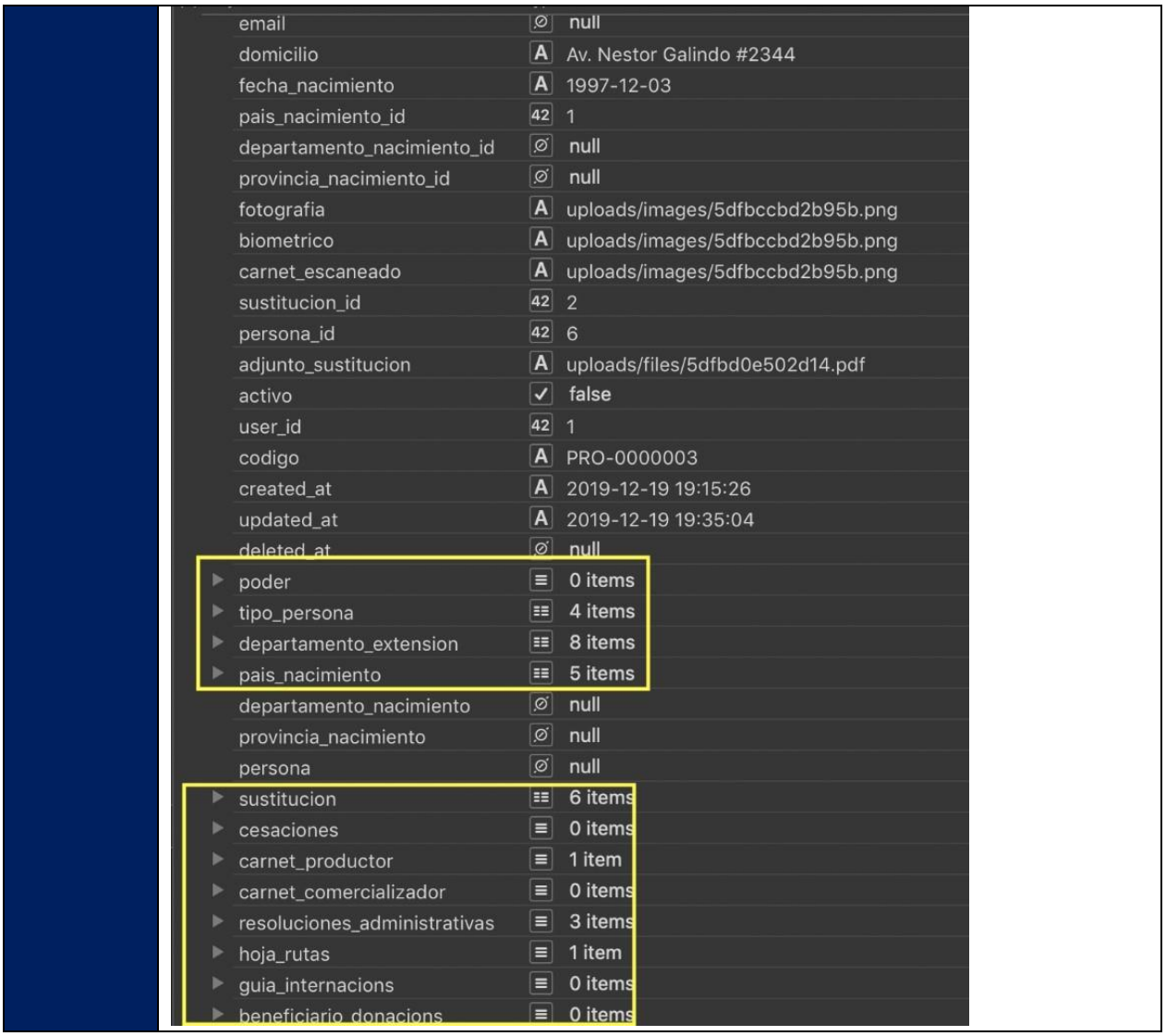
```
101
102     public function setMax($request){
103         $correlativo = '';
104         switch ($request->tipo_persona_id) {
105             case 1:
106                 $correlativo = 'PRO';
107                 break;
108             case 2:
109                 $correlativo = 'PRD';
110                 break;
111             case 3:
112                 $correlativo = 'COM';
113                 break;
114             case 4:
115                 $correlativo = 'IND';
116                 break;
117             case 5:
118                 $correlativo = 'INV';
119                 break;
120             case 6:
121                 $correlativo = 'DON';
122                 break;
123             case 7:
124                 $correlativo = 'DEI';
125                 break;
126         }
127         if(Persona::where('tipo_persona_id', $request->tipo_persona_id)->count() > 0){
128             $latest = Persona::orderBy('created_at', 'DESC')->take(1)->where('tipo_persona_id', $request->tipo_persona_id)->get();
129             $max = explode('-', $latest[0]->codigo);
130             $correlativo = $correlativo.'-'.str_pad($max[1] + 1, 7, "0", STR_PAD_LEFT);
131             return $correlativo;
132         }
133         else{
134             $correlativo = $correlativo.'-'.str_pad('1', 7, "0", STR_PAD_LEFT);
135             return $correlativo;
136         }
137     }
```

Algoritmo de generación de códigos.

Cargado de datos Innecesarios	
Gravedad	Medio
URL	https://siscoca.ruralytierras.gob.bo/productores https://siscoca.ruralytierras.gob.bo/productores-al-detalle https://siscoca.ruralytierras.gob.bo/comercializadores https://siscoca.ruralytierras.gob.bo/empresas https://siscoca.ruralytierras.gob.bo/entidad-de-investigacion https://siscoca.ruralytierras.gob.bo/beneficiarios-de-donaciones https://siscoca.ruralytierras.gob.bo/beneficiarios-de-desarrollo https://siscoca.ruralytierras.gob.bo/guias_internacion https://siscoca.ruralytierras.gob.bo/hojas_de_ruta https://siscoca.ruralytierras.gob.bo/api/persona POST
Módulo	-Módulo de Registro -Módulo de Actividades de Comercialización e Industrialización
Riesgo	Posible sobrecarga de la memoria del servidor y del navegador
Causa	Los servicios web retornan los registros con todas sus relaciones, esto provoca que la recuperación de datos sea muy lenta aunque la cantidad de los datos sea mínima.
Posible Solución	Se debe realizar una refactorización de los siguientes puntos: • Mapeo de tablas a entidades. • Implementación de los servicios web para que no retornen los Objetos entidad con todas sus relaciones. • Implementación de paginación al recuperar los datos.
Evidencia	Al momento de la elaboración del presente informe, existen 19 registros de productores, cargar los datos demora 8.3 segundos aproximadamente y descarga 10.3 MB de datos. Considerando los 19 registros, el tiempo que toma y los datos que descarga, el servicio que recupere los datos, es **extremadamente ineficiente.**

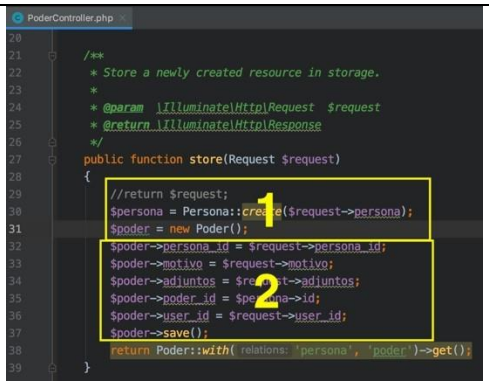


A continuación, se presenta un objeto “Persona” recuperado con varias de sus relaciones; se puede observar al cargar a un objeto “Persona”.



6.1.2. Análisis de manejo de transacciones en procesos críticos

Manejo de Transacciones	
Gravedad	Alto
URL	https://siscoca.ruralytierras.gob.bo/poderes
Módulo	-Módulo de Registro -Módulo de Actividades de Comercialización e Industrialización
Riesgo	Es posible que se registren datos inconsistentes por errores dentro de una transacción.
Causa	En los procesos de registro no se manejan transacciones a nivel de base de datos ni a nivel de la aplicación.



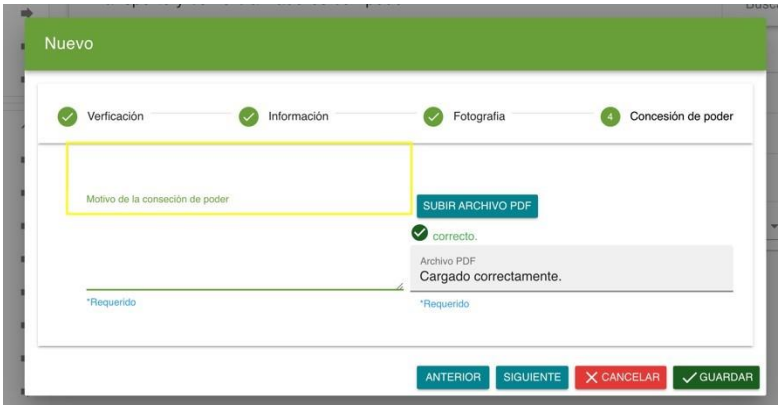
En la anterior imagen se muestra el método (proceso) de registro de poderes, en el cual, primero registra a la persona que va a tener el poder en la tabla "Persona" y luego registra la relación en la tabla "Poder".
Cualquier error que se produzca dentro de este proceso debiera generarse "rollback", para garantizar que no exista inconsistencia de datos, pero al no implementar manejo de transacciones, si se genera un error al registrar en la tabla "Poder" se registrará datos en la tabla "Persona" y no en la tabla "Poder".

Posible Solución

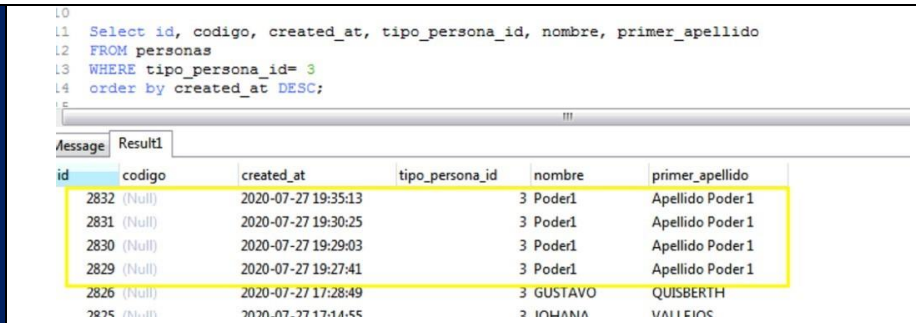
Se debe manejar transacciones a nivel de la aplicación o a nivel de la base de datos.

Evidencia

Se ha intentado crear un poder para transporte y comercialización, se ha registrado los datos correctos de la persona, pero en el campo "Motivo" se ha rellenado con "espacios en blanco" como se logra visualizar en la siguiente imagen.



El campo motivo se registra en la tabla "Poder" por cual, como no se realiza ninguna validación de datos correctos ni en el formulario ni a nivel de servicios web, el proceso intentará registrar en el campo "motivo" un texto vació y el motor de base de datos retorna error porque el campo no permite nulo. Por consiguiente, se ha registrado en la tabla persona, pero no se ha registrado la relación en la tabla "Poder", por consiguiente, los datos quedan inconsistentes.



Registros de la tabla “Personas”

No Existe el registro en la tabla “Poder” del id_persona 2832.

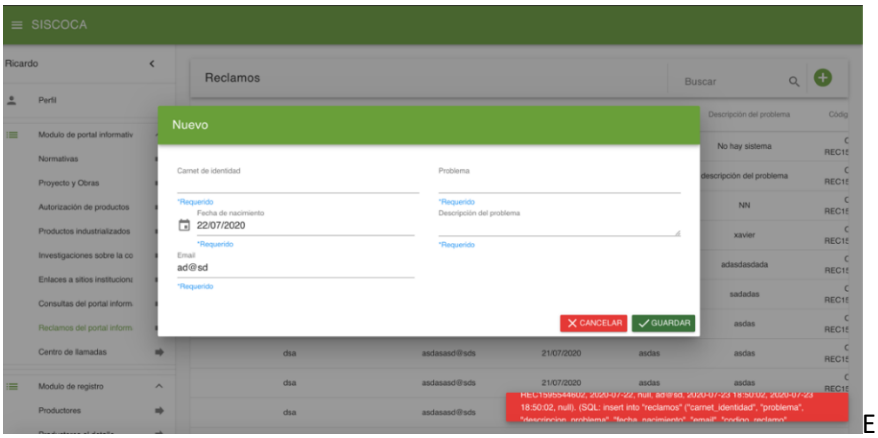
6.2. Análisis de seguridad del sistema

6.2.1. Divulgación de datos sensibles del servidor

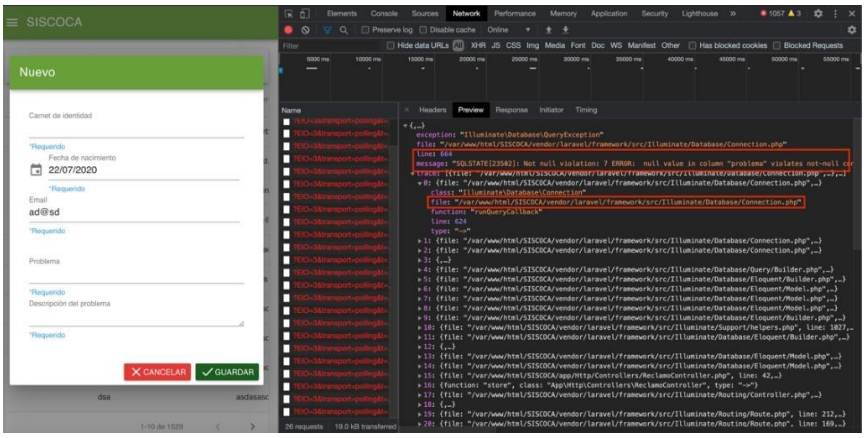
Divulgación de datos sensibles del servidor	
Gravedad	Alto
URL	https://siscoca.ruralytierras.gob.bo/reclamos_portal_info https://siscoca.ruralytierras.gob.bo/productores Todas las funcionalidades tienen el mismo inconveniente.
Módulo	Todos los módulos
Riesgo	El sistema divulga información sensible del servidor, como rutas de la ubicación la aplicación, la tecnología utilizada para el desarrollo. Información que puede ser usada por un atacante para vulnerar la seguridad del sistema o robar datos.
Causa	Todos los controladores de API REST analizados no implementan ninguna validación de los datos que recibe y no implementan ninguna estrategia para capturar los errores que se generan en los procesos internos del sistema.
Posible Solución	Los API REST deben realizar validación de tipo de dato, longitud cadena, dígitos y existencia de registros, antes de iniciar las transacciones para evitar generar errores a nivel de base de datos. En todas las transacciones u operaciones que se ejecuten en la lógica de los API REST, se debe capturar las excepciones y retornar hacia el cliente una descripción entendible de los mismos. Ejemplo: Número de documento inválido. Longitud del campo ‘Nombre’ debe ser menor a 100 caracteres.

Evidencia

La evidencia se basa en la funcionalidad de registrar un “Nuevo Reclamo”, donde se evidencia que no se realizan las validaciones necesarias en el formulario ni a nivel del API REST, puesto que es posible registrar en todos los campos el carácter espacio “ ” lo cual genera error al momento de registrar en la base de datos y divulga información sensible del servidor.



Error a nivel de Interfaz



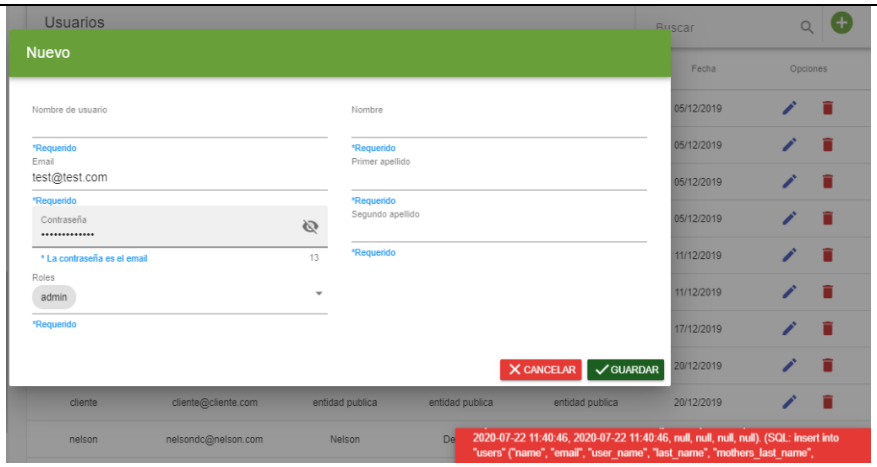
Información sensible del servidor.

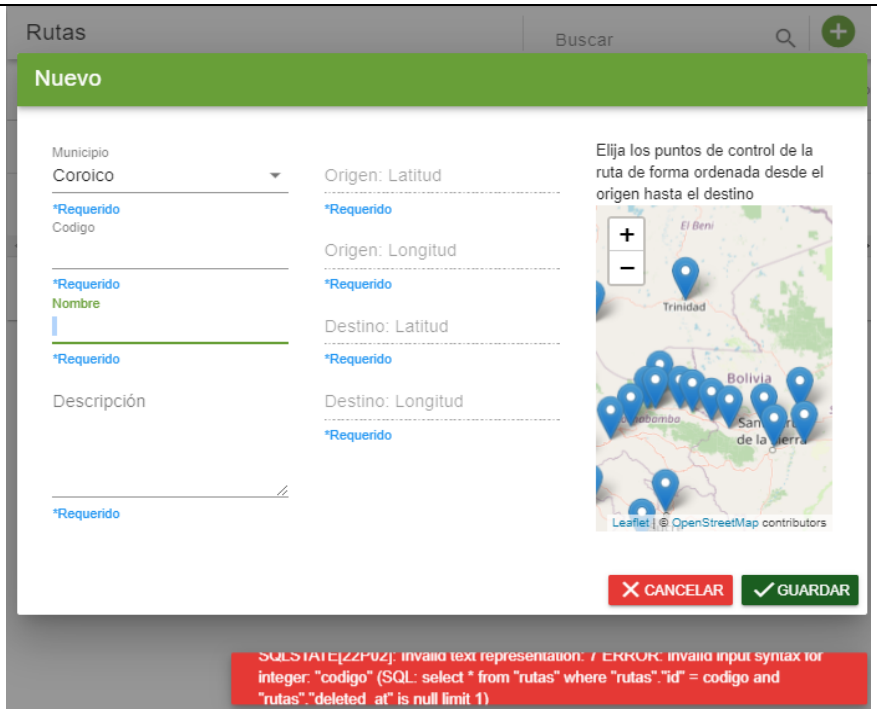
```php
/**
 * Store a newly Item if no one found in the database.
 *
 * @param  \Illuminate\Http\Request  $request
 * @return \Illuminate\Http\Response
 */
public function store(Request $request)
{
    $now = now();
    $codigo_reclamo = "COD-REC".$now->timestamp;
    $request->request->add(['codigo_reclamo' => $codigo_reclamo]);
    return Reclamo::create($request->all());
}
```

Controlador del API REST de reclamos, donde se observa que no se realiza ninguna validación ni se capturan excepciones.

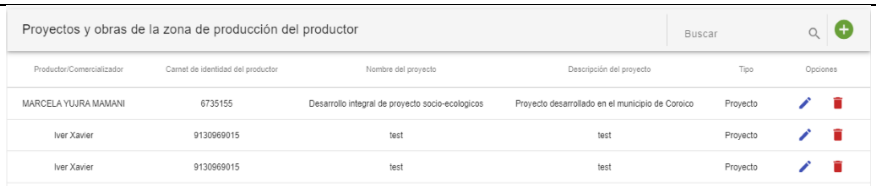
6.3. Revisión de funcionalidad del sistema

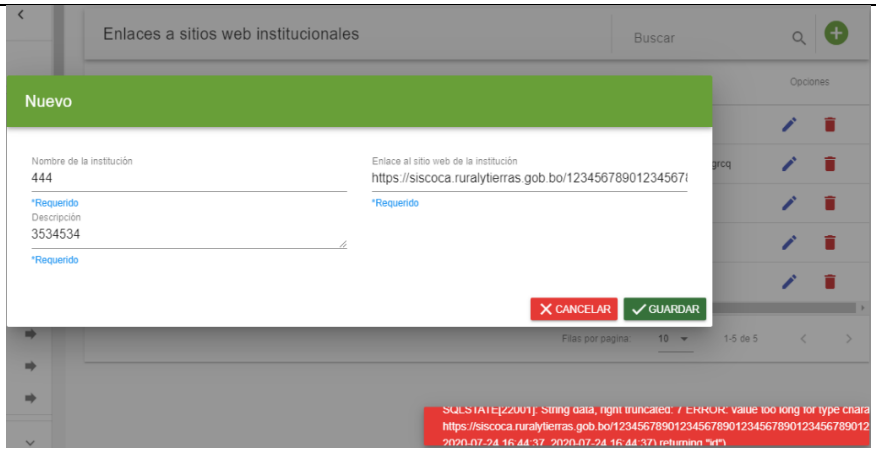
6.3.1. Pruebas funcionales

Personalización de mensajes de error	
Gravedad	Alto
URL	https://siscoca.ruralytierras.gob.bo/usuarios (caso 1) https://siscoca.ruralytierras.gob.bo/rutas (caso 2)
Módulo	Todos los módulos que contienen la opción de creación y/o edición.
Riesgo	-Expuesto a vulneración a base de datos ya que la consulta SQL se despliega en pantalla. -Información desplegada no entendible para el usuario final.
Causa	Al realizar la creación/edición de un registro con errores de validación de datos, unicidad de campos, ingreso de espacios en blanco en cada input del formulario, etc. dentro del formulario, los mensajes de error muestran una consulta SQL con toda la información ingresada y el atributo afectado. En adición, para el caso de espacios en blanco se presentan los siguientes casos: 1. El mensaje de error SQL se despliega luego de presionar el botón guardar. 2. Dentro del módulo de Parametrización, el error se despliega al ingresar espacios en blanco en el campo “Código” y pasar al siguiente campo.
Posible Solución	-Controlar y personalizar las excepciones generadas al manipular el aplicativo. -Restringir el ingreso de espacios en blanco al inicio y final de cada input del aplicativo o mostrar el correspondiente texto de error al pasar al siguiente campo el formulario (caso 2).
Evidencia	 Caso 1. Alerta de error al guardar el formulario

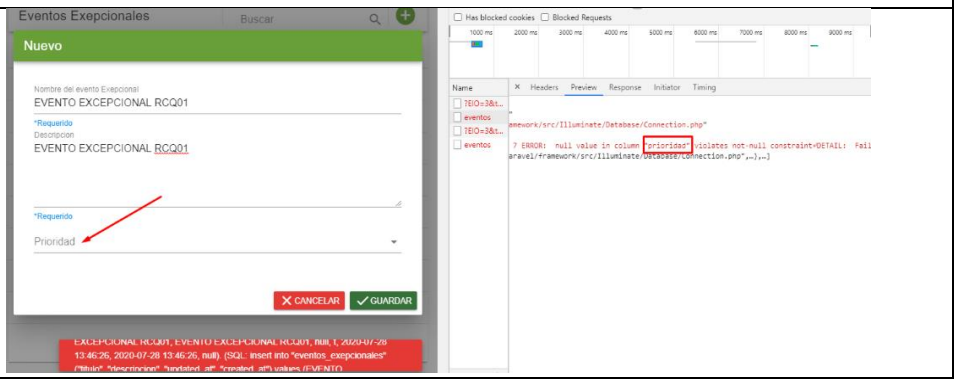


Caso 2. Alerta de error al ingresar espacios en blanco en Código

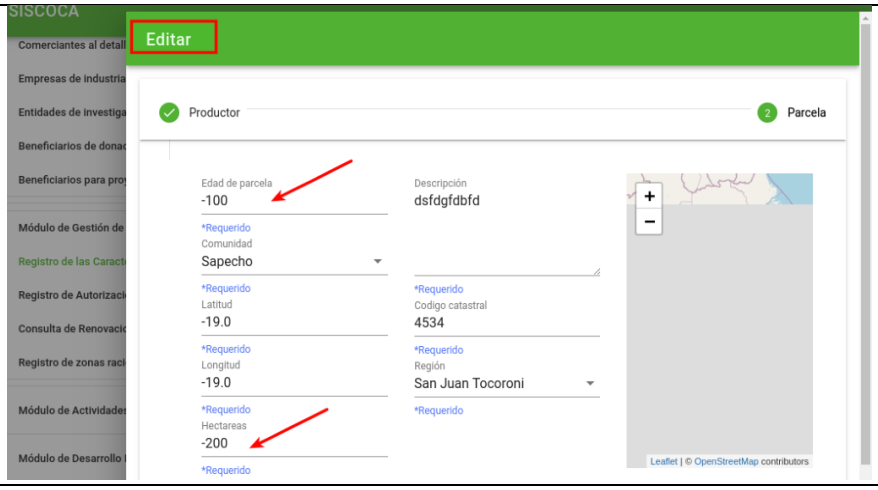
Duplicidad de registros en base de datos	
Gravedad	Alto
URL	https://siscoca.ruralytierras.gob.bo/proyecto_obras
Módulo	Todos los módulos del sistema -Módulo de Portal Informativo (Ejemplo)
Riesgo	Permite crear registros duplicados dentro de la base de datos.
Causa	Falta de control de campos sensibles como ser códigos, nombres, etc.
Posible Solución	Aplicar control de datos sensibles desde formularios de creación y edición, esto para optimizar el almacenamiento y rendimiento de la base de datos.
Evidencia	

Validación de longitudes máximas	
Gravedad	Alto
URL	https://siscoca.ruralytierras.gob.bo/enlaces_institucionales https://siscoca.ruralytierras.gob.bo/resoluciones_administrativas https://siscoca.ruralytierras.gob.bo/usuarios
Módulo	Todos los módulos que contienen formularios de creación y/o edición.
Riesgo	No permite finalizar el flujo de registro/edición con éxito.
Causa	Al realizar la creación/edición de un registro, dentro del formulario desplegado, la validación de caracteres máximos permitidos no se muestra para todos los campos, por lo que al ingresar valores grandes se genera una excepción SQL.
Posible Solución	Realizar la validación de longitudes máximas permitidas desde backend y frontend de acuerdo a las longitudes definidas desde base de datos. Por otro lado, mostrar el texto de error para el input correspondiente.
Evidencia	

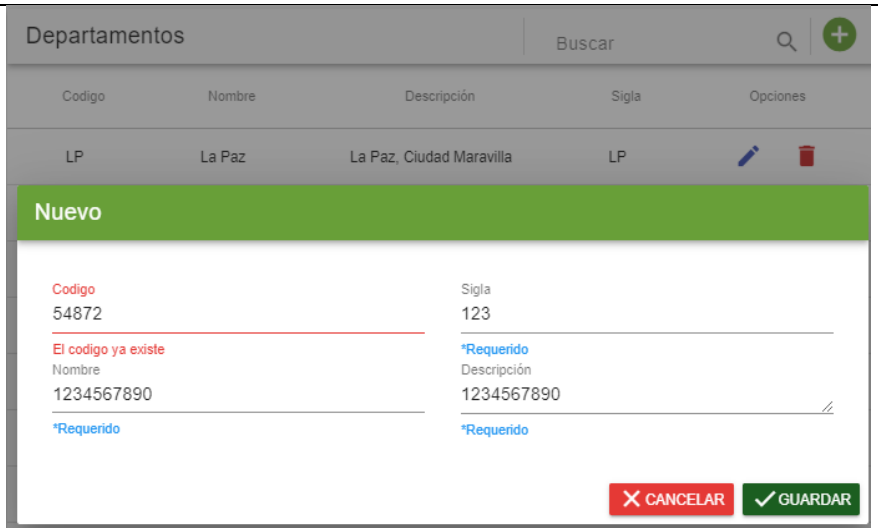
Validación de tipos de datos – Obligatoriedad de datos	
Gravedad	Alto
URL	https://siscoca.ruralytierras.gob.bo/callcenters https://siscoca.ruralytierras.gob.bo/convocatorias_oii https://siscoca.ruralytierras.gob.bo/priorizacion_oii https://siscoca.ruralytierras.gob.bo/supervision_oii https://siscoca.ruralytierras.gob.bo/cierre_obra_oii https://siscoca.ruralytierras.gob.bo/evaluacion_impacto_oii https://siscoca.ruralytierras.gob.bo/infracciones https://siscoca.ruralytierras.gob.bo/firmas https://siscoca.ruralytierras.gob.bo/notificaciones https://siscoca.ruralytierras.gob.bo/registro_eventos
Módulo	-Módulo de Portal Informativo -Módulo de OII

	-Módulo de Parametrización -Alertas y Notificaciones -Módulo de Auditoria
Riesgo	No permite finalizar un flujo con éxito.
Causa	Campos obligatorios se muestran como opciones dentro del formulario. Ejemplo: 1. Centro de llamadas: Campos “Nombres y Apellidos” y “Teléfono’. 2. Convocatorias para OII: Campos “Términos de referencia” y “Indicaciones calificables”. 3. Priorización para OII: “Conclusiones”. 4. Registro de Supervisión OII, Cierre de OII y Evaluación de impacto de OII: Campo “Fotografía PDF”. 5. Infracciones: Campo “Descripción”. 6. Firmas: Imagen de fotografía. 7. Parametrización de Eventos Excepcionales: Campo “Prioridad”. 8. Registro de Eventos del Sistema: Campo “Usuario”.
Posible Solución	Aplicar validaciones de obligatoriedad a los campos necesarios.
Evidencia	

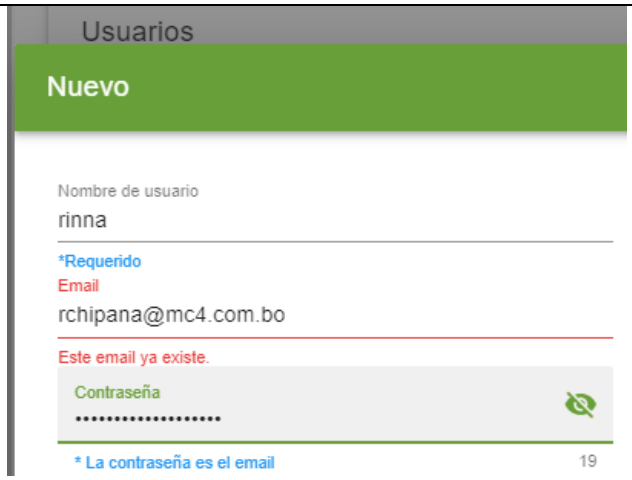
Validación de tipos de datos – Valores Numéricos	
Gravedad	Alto
URL	https://siscoca.ruralytierras.gob.bo/montos https://siscoca.ruralytierras.gob.bo/caracteristicas_produccion https://siscoca.ruralytierras.gob.bo/empresas
Módulo	-Módulo de Parametrización -Módulo de Gestión de Actividades de Producción -Módulo de Registro
Riesgo	Almacenamiento de datos basura en base de datos.
Causa	El aplicativo no cuenta con validación de datos de tipo numérico desde backend ni frontend. Ejemplo:

	1. Los campos numéricos como "Valor" de Montos y "Hectáreas, Edad de Parcela" de Registro de las Características de la Producción de Coca permiten el registro de valores iguales y menores a 0. 2. Empresa de industrialización: Los campos NIT, Número de Fundempresa, Carnet de identidad, Teléfono/Celular permiten el ingreso de textos.
Posible Solución	-Aplicar control de datos numéricos para los campos necesarios. -Restringir ingreso de valores menores o iguales a 0 para casos que lo requieran.
Evidencia	

Validación de tipos de datos – Formato de correo electrónico	
Gravedad	Alto
URL	https://siscoca.ruralytierras.gob.bo/productores https://siscoca.ruralytierras.gob.bo/productores-al-detalle https://siscoca.ruralytierras.gob.bo/comercializadores https://siscoca.ruralytierras.gob.bo/empresas https://siscoca.ruralytierras.gob.bo/entidad-de-investigacion https://siscoca.ruralytierras.gob.bo/beneficiarios-de-donaciones https://siscoca.ruralytierras.gob.bo/beneficiarios-de-desarrollo
Módulo	Módulo de Registro
Riesgo	Correo inválido registrado como válido dentro del aplicativo.
Causa	No existe validación en campo Email de formularios.
Posible Solución	Aplicar la validación de email.
Evidencia	

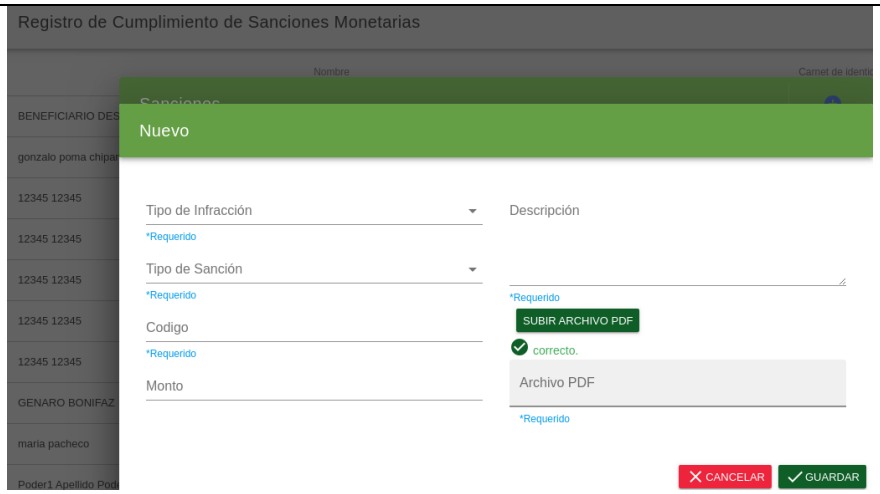
Validación errónea de unicidad sobre datos que no existentes en base de datos	
Gravedad	Alto
URL	https://siscoca.ruralytierras.gob.bo/zona_autorizada https://siscoca.ruralytierras.gob.bo/departamentos https://siscoca.ruralytierras.gob.bo/provincias https://siscoca.ruralytierras.gob.bo/municipios
Módulo	Módulo de Parametrización
Riesgo	No permite realizar la actualización de datos con éxito
Causa	Aplica unicidad de código sobre valores que no existen en base de datos
Posible Solución	Validar campo código sobre registros activos existentes en base de datos
Evidencia	

Validación de unicidad de datos sobre registros ya eliminados	
Gravedad	Alto
URL	https://siscoca.ruralytierras.gob.bo/usuarios https://siscoca.ruralytierras.gob.bo/roles https://siscoca.ruralytierras.gob.bo/permisos
Módulo	Módulo de Usuarios, Roles y Permisos
Riesgo	No permite finalizar el flujo de creación/edición con éxito.
Causa	La unicidad de campos sensibles se realiza sobre todos los registros existentes en base de datos. Se presentan dos casos: 1. La validación se aplica luego de presionar el botón guardar (caso Nombre de rol y permiso) 2. La validación se aplica al pasar al siguiente campo del formulario (caso Email de usuario)
Posible Solución	Aplicar unicidad de datos sobre registros activos o habilitados en base de datos, no considerar aquellos que fueron eliminados.

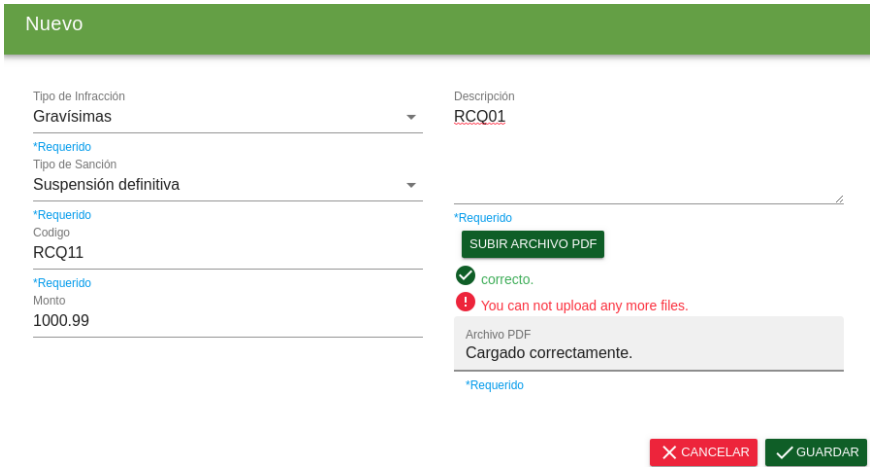
Evidencia	

Archivo adjunto no reseteado en formulario nuevo	
Gravedad	Alto
URL	https://siscoca.ruralytierras.gob.bo/autorizacion_renov_parcela https://siscoca.ruralytierras.gob.bo/evaluacion_viabilidad_oii https://siscoca.ruralytierras.gob.bo/sanciones_monetarias https://siscoca.ruralytierras.gob.bo/registro_eventos
Módulo	-Módulo de Gestión de Actividades de Producción -Módulo de Obras de Impacto Inmediato -Módulo de Resoluciones Administrativas -Módulo de Auditoria
Riesgo	Información errónea para el usuario final
Causa	El componente para la carga de archivos no se reinicia luego de cancelar el formulario de creación. Al abrir el formulario nuevamente se visualiza el archivo cargado anteriormente. Luego de cancelar un formulario de creación con un archivo cargado y abrirlo nuevamente, el nuevo formulario contiene el PDF cargado anteriormente.
Posible Solución	Limpiar el archivo PDF adjunto de los formularios de creación luego de presionar guardar o cancelar.

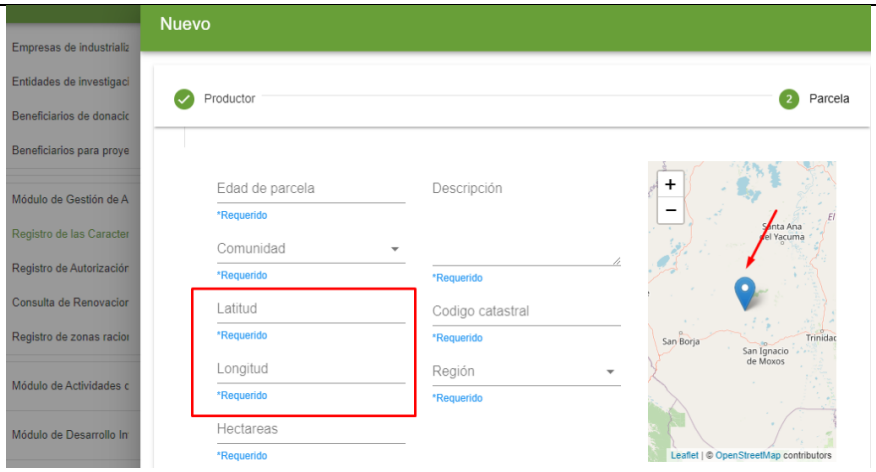
Evidencia



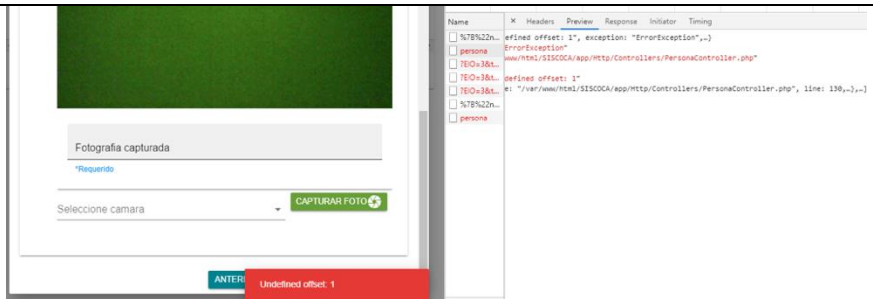
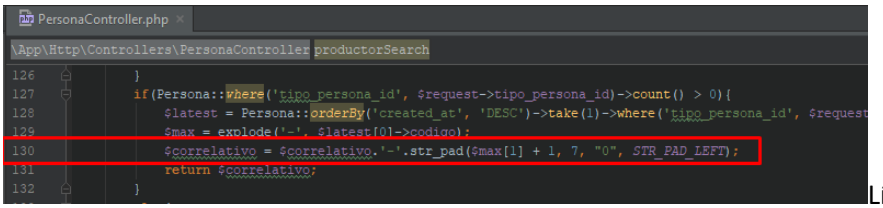
Formulario de creación con adjunto cargado anteriormente

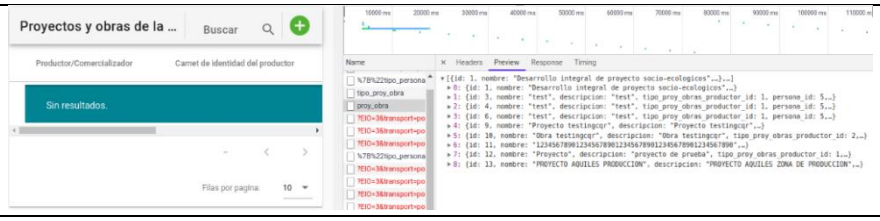


Error en pantalla al insertar nuevo adjunto

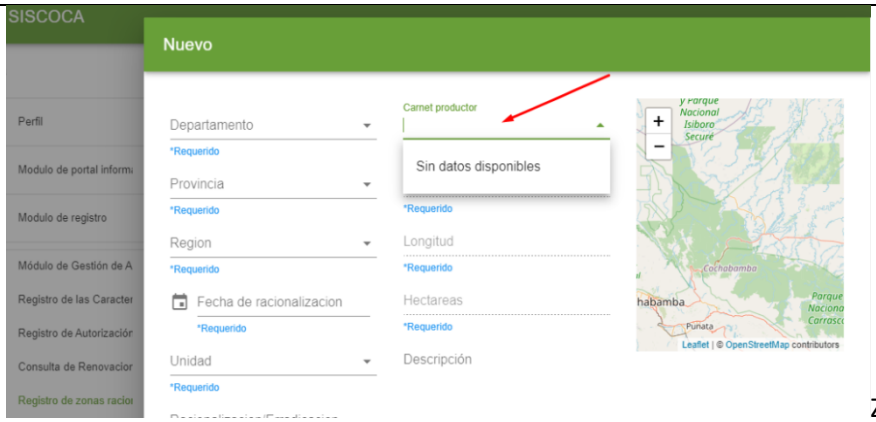
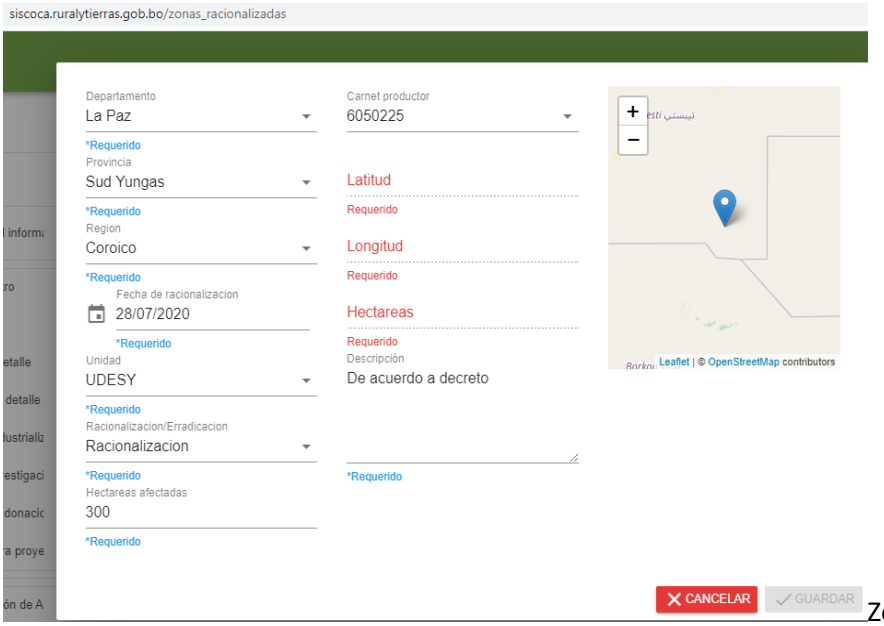
Mapa geo-referencial no tiene funcionalidad	
Gravedad	Alto
URL	https://siscoca.ruralytierras.gob.bo/caracteristicas_produccion
Módulo	Módulo de gestión de actividades de producción
Riesgo	El componente mapa no es funcional si se desea registrar coordenadas, lo que obliga al usuario a ingresarlas manualmente.
Causa	Posible funcionalidad deshabilitada
Posible Solución	Habilitar opción de ubicar coordenadas desde el mapa.
Evidencia	

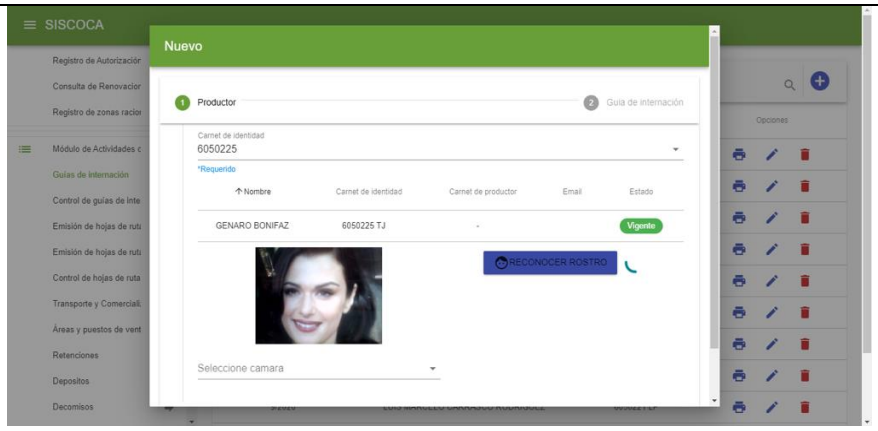
Código correlativo de productor al detalle	
Gravedad	Alto
URL	https://siscoca.ruralytierras.gob.bo/productores-al-detalle https://siscoca.ruralytierras.gob.bo/comercializadores (formulario de creación y opción sustituir)
Módulo	Módulo de Registro
Riesgo	No permite finalizar el flujo de creación con éxito
Causa	Desde interfaz se desconoce el motivo, pero luego de revisar el código fuente, en la línea 130 de PersonaController.php se evidencia que el problema se debe al valor correlativo. Luego de llenar el formulario y presionar el botón Guardar, se despliega el mensaje de error “Undefined offset: 1”
Posible Solución	-Controlar que se mantenga vigente la opción seleccionada

Evidencia	 Error Desplegado en pantalla  Línea de Código Fuente causal del error

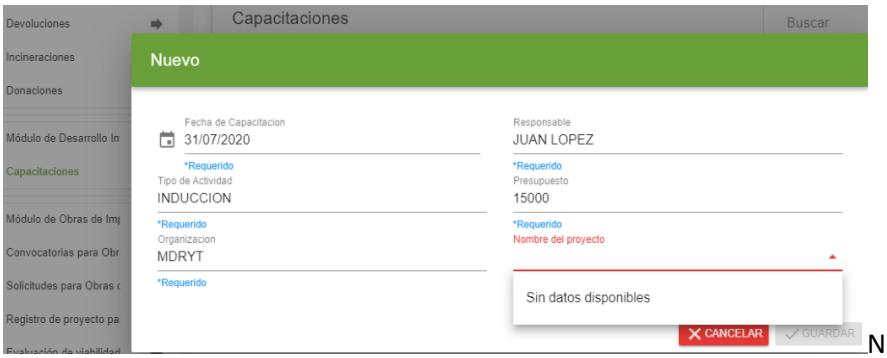
Datos de Proyectos y Obras no desplegados en pantalla	
Gravedad	Alto
URL	https://siscoca.ruralytierras.gob.bo/proyecto_obras
Módulo	Módulo de portal informativo
Riesgo	No permite operar por la pantalla con normalidad
Causa	La interfaz no recupera los registros.
Posible Solución	-Revisar componente y conexión a los servicios web expuestos.
Evidencia	

Flujos no concluidos exitosamente	
Gravedad	Alto
URL	https://siscoca.ruralytierras.gob.bo/zonas_racionalizadas https://siscoca.ruralytierras.gob.bo/guias_internacion https://siscoca.ruralytierras.gob.bo/capacitaciones https://siscoca.ruralytierras.gob.bo/evaluacion_viabilidad_oii https://siscoca.ruralytierras.gob.bo/supervision_oii
Módulo	-Módulo de Gestión de Actividades de Producción -Módulo de Actividades de Comercialización e industrialización -Módulo de Desarrollo Integral -Módulo de Obras de Impacto Inmediato

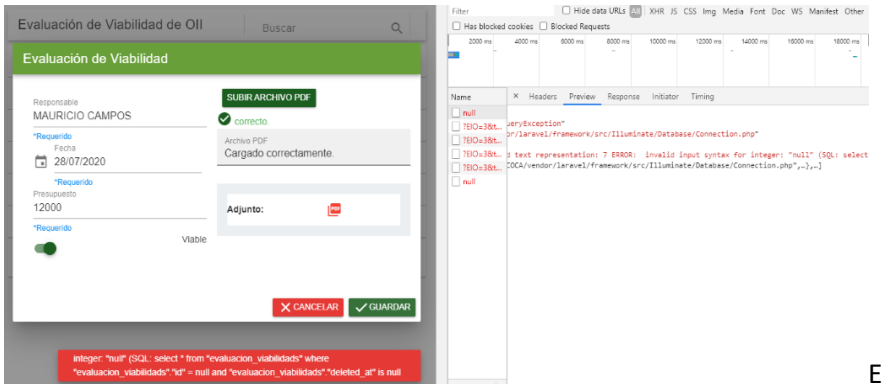
Riesgo	No permite crear un registro con éxito
Causa	Se tienen los siguientes casos: 1. Zonas Racionalizadas: No recupera listado de carnets de productores. Al ingresar manualmente un valor y cancelar el formulario, los campos latitud, longitud, hectáreas, no pueden ser recuperados del nuevo formulario abierto. 2. Módulo de Actividades de Comercialización e industrialización: En la mayoría de los casos no realiza el reconocimiento de rostro con éxito, además demora varios minutos en realizar el proceso. 3. Capacitaciones: No se despliegan proyectos disponibles. 4. Módulo de OII: Despliegue de error null al guardar un nuevo registro.
Posible Solución	Revisar método guardar y tipo de datos ingresados.
Evidencia	 Zonas Racionalizadas. Caso no recupera listado de carnets  Zonas Racionalizadas. No recupera datos para carnet existente



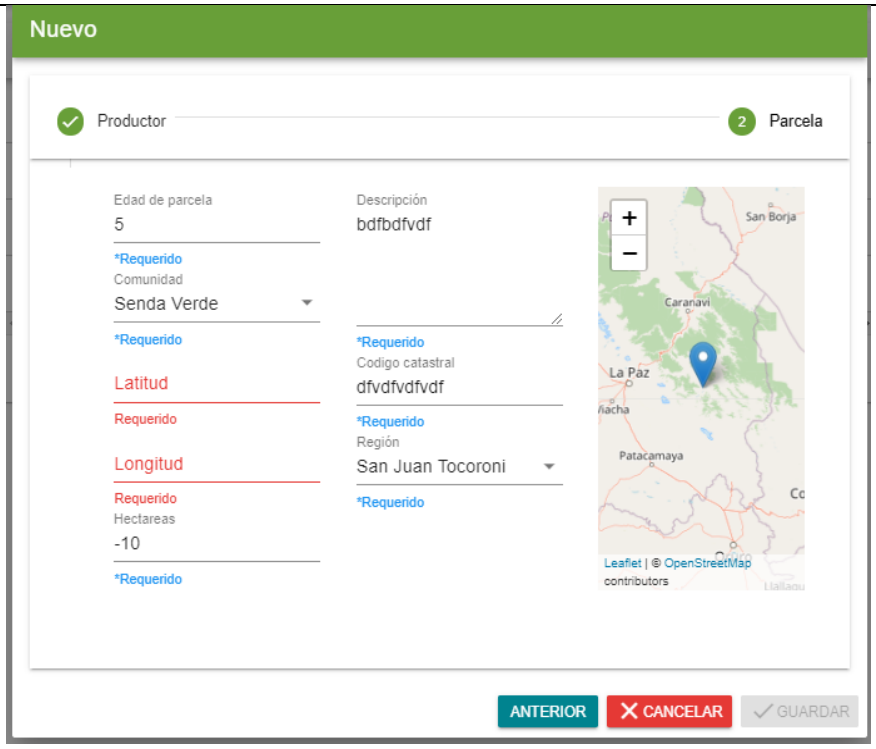
Demora en reconocimiento de rostro con resultado fallido



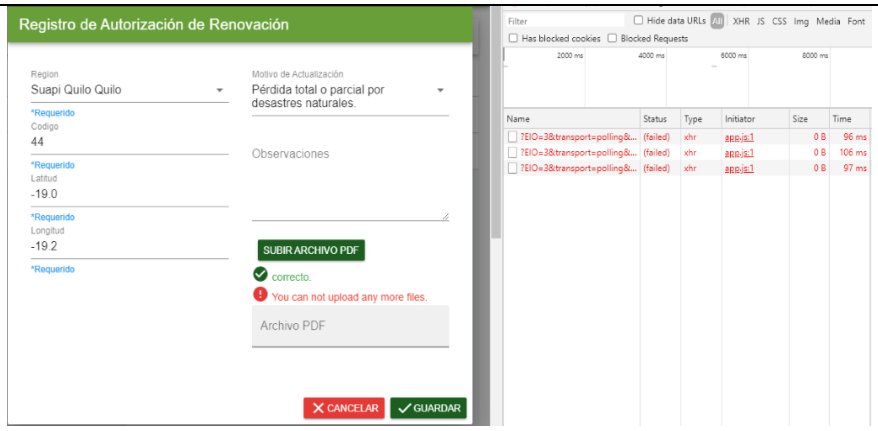
No Recupera listado de proyectos



Error al guardar evaluación de viabilidad de proyecto

Creación de registro - Error	
Gravedad	Alto
URL	https://siscoca.ruralytierras.gob.bo/caracteristicas_produccion
Módulo	Módulo de Gestión de Actividades de Producción: Registro de las características de la producción de coca
Riesgo	No permite crear un registro
Causa	-No es posible seleccionar una ubicación geo-referencial en el mapa
Posible Solución	-Verificar componente mapa
Evidencia	

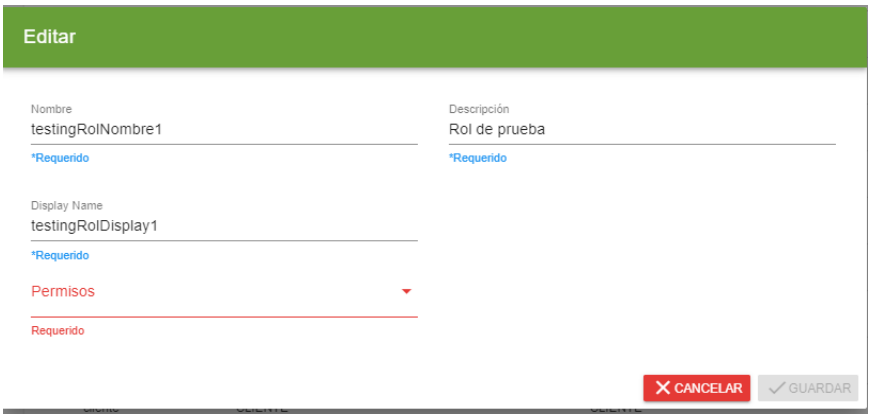
Creación de registro de renovaciones – Botón sin funcionalidad	
Gravedad	Alto
URL	https://siscoca.ruralytierras.gob.bo/autorizacion_renov_parcela
Módulo	Módulo de Gestión de Actividades de Producción
Riesgo	- Registro de Renovación: No permite crear nuevos registros - Verificación de Renovación: Solo contiene opción Cancelar.
Causa	- Registro de Renovación: El botón Guardar no tiene funcionalidad - Verificación de Renovación: No contiene funcionalidad de guardar registro.
Posible Solución	-Revisar método guardar de creación

Evidencia	 Registro de Renovación  Verificación de Renovación

Edición de registro – Error a realizar la acción	
Gravedad	Alto
URL	https://siscoca.ruralytierras.gob.bo/centrales https://siscoca.ruralytierras.gob.bo/notificaciones
Módulo	-Módulo de Parametrización -Alertas y Notificaciones
Riesgo	No permite la actualización de datos con éxito
Causa	El botón guardar del formulario de edición no sigue la correcta funcionalidad. Pese a que se despliega un mensaje de éxito, no se visualiza el cambio en pantalla.
Posible Solución	Revisar método de edición
Evidencia	

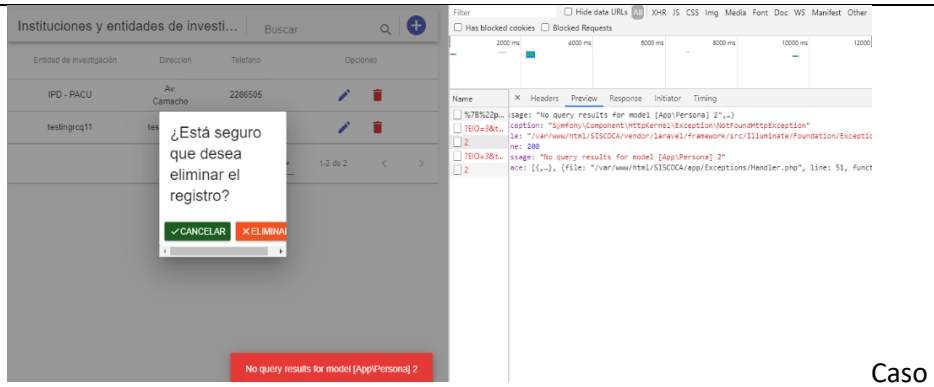
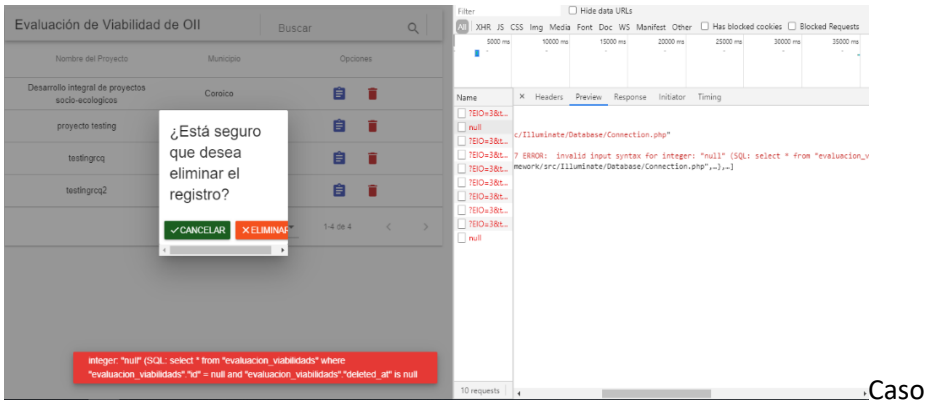
Edición de registro – No recupera datos	
Gravedad	Alto
URL	https://siscoca.ruralytierras.gob.bo/profile/ https://siscoca.ruralytierras.gob.bo/convocatorias_oii https://siscoca.ruralytierras.gob.bo/poderes https://siscoca.ruralytierras.gob.bo/decomisos https://siscoca.ruralytierras.gob.bo/roles
Módulo	-Perfil -Módulo de Obras de Impacto Inmediato -Módulo de Actividades de Comercialización e industrialización -Módulo de Usuarios, Roles y Permisos
Riesgo	Pérdida de datos registrados desde el formulario de creación.
Causa	Luego de realizar la creación de un registro e ingresa a su opción respectiva de edición, no se recuperan todos los datos ingresados. Ejemplos: 1. Perfil: no recupera apellidos. 2. Convocatoria OII: Las fechas seleccionadas son reemplazadas con la fecha actual. 3. Transporte y comercialización con Poder: Solo la segunda parte del formulario se muestra disponible de edición. 4. Roles: no recupera combo de permisos.
Posible Solución	-Verificar método correspondiente. -Verificar que los datos del nuevo usuario existan en base de datos.
Evidencia	 Usuario nuevo

Perfil de usuario creado

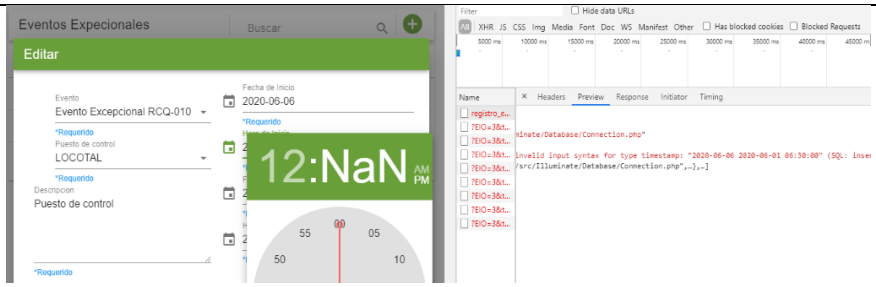


Caso roles: No recupera listado de permisos

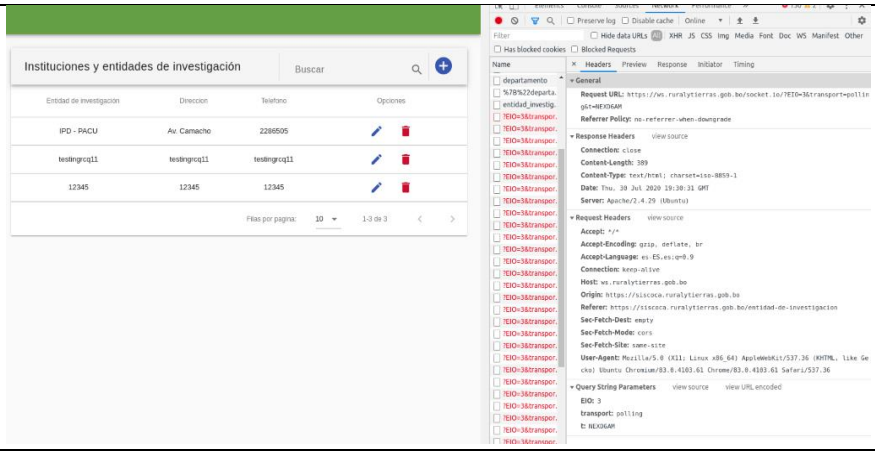
Eliminación de registro - Error	
Gravedad	Alto
URL	https://siscoca.ruralytierras.gob.bo/entidad-de-investigacion https://siscoca.ruralytierras.gob.bo/beneficiarios-de-donaciones https://siscoca.ruralytierras.gob.bo/notificaciones https://siscoca.ruralytierras.gob.bo/notificaciones/nueva https://siscoca.ruralytierras.gob.bo/notificaciones/monitoreo https://siscoca.ruralytierras.gob.bo/evaluacion_viabilidad_oii https://siscoca.ruralytierras.gob.bo/priorizacion_oii https://siscoca.ruralytierras.gob.bo/supervision_oii https://siscoca.ruralytierras.gob.bo/evaluacion_impacto_oii
Módulo	-Módulo de Registro -Alertas y Notificaciones -Módulo de Obras de Impacto Inmediato

Riesgo	No permite eliminar un registro con éxito
Causa	-Problemas con el método para eliminar
Posible Solución	-Verificar método de eliminación
Evidencia	 Caso Modulo de registro y alertas  Caso Módulo de OII

Formato de componente Calendar y Hora	
Gravedad	Alto
URL	https://siscoca.ruralytierras.gob.bo/notificaciones/nueva (calendar/hora) https://siscoca.ruralytierras.gob.bo/notificaciones/monitoreo (calendar/hora) https://siscoca.ruralytierras.gob.bo/reportes_des_integral https://siscoca.ruralytierras.gob.bo/guias_internacion https://siscoca.ruralytierras.gob.bo/hojas_de_ruta https://siscoca.ruralytierras.gob.bo/registro_eventos (seteo fecha actual) https://siscoca.ruralytierras.gob.bo/evaluacion_viabilidad_oii (invalid date)
Módulo	-Alertas y Notificaciones -Módulo de Reportes -Módulo de Actividades de Comercialización e industrialización

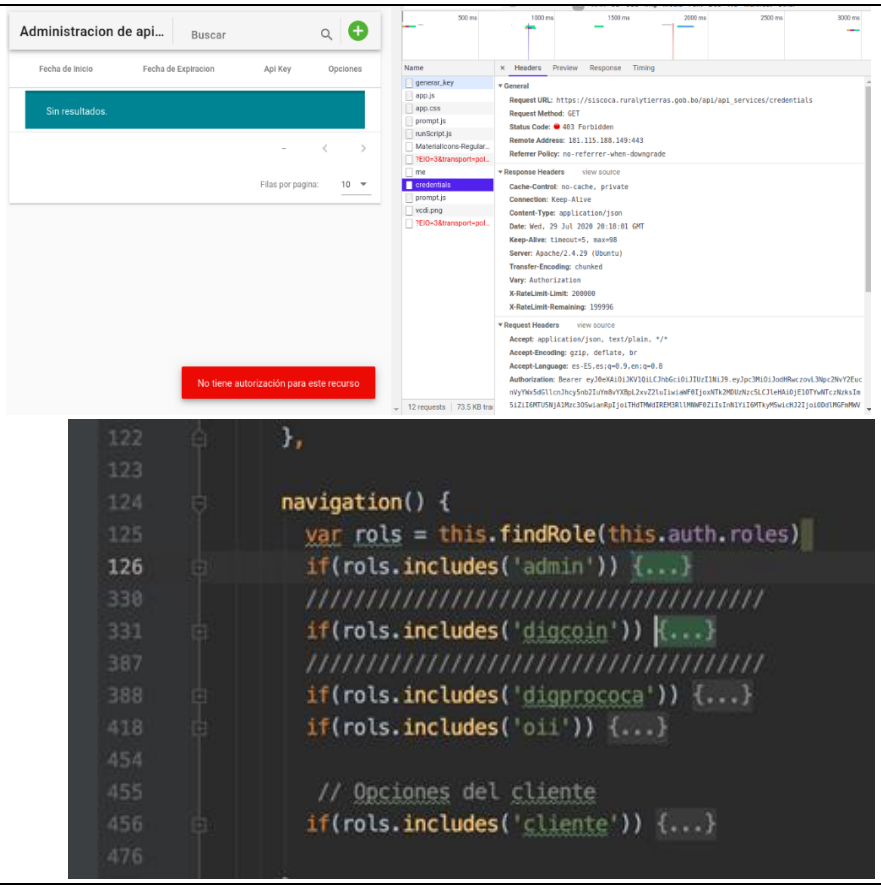
	-Módulo de Auditoria -Módulo de Obras de Impacto Inmediato
Riesgo	-El formato de fechas en pantalla se muestran en formato yyyy-mm-dd -El formato de fecha en Excel se muestra como dd/Jul/yyyy (mes literal yyyy - año)
Causa	- No se aplica patrón de fecha dd/mm/yyyy en componente fecha de formulario, el formato actual es yyyy-mm-dd - No se aplica patrón de fecha dd/mm/yyyy (dia/mes/año) en reportes Excel y PDF de reportes, el formato actual es dd-Mes Literal-yyyy (año) -En el módulo de auditoria, el formulario de edición setea la fecha actual, no a la seleccionada. -En el módulo de OII el componente fecha de la opción Evaluación de OII muestra “Invalid date”. -En el módulo de alertas y notificaciones: La edición no recupera la hora seleccionada y muestra el texto NaN, por lo que no permite seleccionar una nueva hora. Por otro lado, en los campos de hora se muestra la fecha y hora edición se pierden las fechas de inicio y fin y los datos se muestran solo en hora y formato fecha invertido, y no deja seleccionar nuevo minuto NaN, ver imagen 0724_eventosExcepcionalesEditar
Posible Solución	-Aplicar estandarización de formato de fecha dd/mm/yyyy (año).
Evidencia	 Edición de campo Hora

Eliminación de registro - Diálogo de eliminación no desaparece	
Gravedad	Medio
URL	https://siscoca.ruralytierras.gob.bo/comercializadores
Módulo	Módulo de Registro
Riesgo	-Resulta un bucle innecesario para el usuario final
Causa	El diálogo no desaparece luego confirmar la eliminación de un registro
Posible Solución	Luego de confirmar la acción, cerrar el diálogo de eliminación
Evidencia	

Intentos de conexión a sockets sin éxito	
Gravedad	Medio
URL	Todos
Módulo	Todos
Riesgo	No se controlan eventos en tiempo real de manera correcta.
Causa	La aplicación intenta conectarse constantemente a los sockets.
Posible Solución	Verificar función de conexión de socket.
Evidencia	

6.3.2. Pruebas de diseño

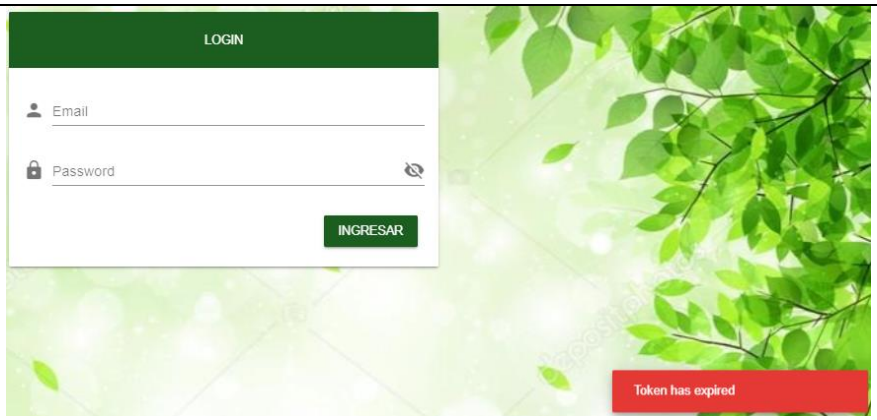
Pruebas de usabilidad – Accesos denegados	
Gravedad	Alto
URL	https://siscoca.ruralytierras.gob.bo/hojas_de_ruta (Rol digcoin) https://siscoca.ruralytierras.gob.bo/supervision_oii (Rol OII) https://siscoca.ruralytierras.gob.bo/generar_key (Rol cliente)
Módulo	Todos los módulos para rol DIGCOIN, OII, CLIENTE
Riesgo	No permite acceder correctamente a la pantalla debido a que no se cuentan con los permisos necesarios
Causa	No se cuentan con los accesos correctamente configurados para los roles Digcoin, OII y Cliente.
Posible Solución	-Revisar si la URL actual es la correcta. -Revisar permisos de rol correspondiente.

Evidencia	

Pruebas de compatibilidad – Navegadores	
Gravedad	Alto
URL	Todas
Módulo	Todos
Riesgo	No es posible manipular correctamente el sistema desde el navegador Internet Explorer especificado dentro del manual de usuario.
Causa	Los componentes que conforman el sistema no son compatibles con el navegador Internet Explorer por lo que el sistema no cargaba de manera correcta en el navegador.
Posible Solución	-Si el sistema debe ser manipulado en IE como un requerimiento, revisar la compatibilidad de estilos con el navegador. -Caso contrario, actualizar el manual de usuario, indicando que debe utilizarse el navegador Microsoft Edge en lugar de Internet Explorer. **Nota.** El sistema pudo manipularse de manera correcta en los navegadores: Google Chrome, Mozilla Firefox, Opera y Safari.
Evidencia	

Pruebas de navegabilidad – Menú principal	
Gravedad	Medio
URL	
Módulo	Todos los módulos
Riesgo	No permite navegar con normalidad por las opciones de menú.
Causa	El diseño responsive se aplica correctamente al contraer el menú de opciones.
Posible Solución	Revisar o modificar el diseño responsive de la aplicación.
Evidencia	

Pruebas de contenido – Mostrar contenido, componentes y alertas de éxito en idioma español	
Gravedad	Medio
URL	Nombre campo en inglés: https://siscoca.ruralytierras.gob.bo/roles Componente calendar en inglés: https://siscoca.ruralytierras.gob.bo/beneficiarios-de-desarrollo https://siscoca.ruralytierras.gob.bo/incineraciones https://siscoca.ruralytierras.gob.bo/reportes_comercializacion https://siscoca.ruralytierras.gob.bo/reportes_industrializacion https://siscoca.ruralytierras.gob.bo/reportes_des_integral
Módulo	-Módulo de usuarios, roles y permisos -Módulo de registro -Módulo de Actividades de Comercialización e Industrialización -Módulo de Desarrollo Integral -Todos los módulos respecto a inputs
Riesgo	Contenido de la aplicación no entendible para usuarios finales.
Causa	Nombre de campos, componente de fechas, errores de inputs y mensajes de error no personalizadas.
Posible Solución	-Verificar contenido del aplicativo y mensajes de error a idioma español. -Ejemplo 1: Mensaje de expiración de sesión: “La sesión ha expirado”. -Ejemplo 2: Traducir a idioma español el campo “Display Name” localizado en el formulario de Rol -Ejemplo 3: Componente Fecha muestra meses en inglés. -Ejemplo 4: Errores de inputs (ejemplo: Login)

Evidencia	

Pruebas de contenido – Corrección de Ortografía	
Gravedad	Medio
URL	https://siscoca.ruralytierras.gob.bo/comercializadores https://siscoca.ruralytierras.gob.bo/poderes https://siscoca.ruralytierras.gob.bo/notificaciones https://siscoca.ruralytierras.gob.bo/notificaciones/nueva
Módulo	-Módulo de Registro -Módulo de Actividades de Comercialización e Industrialización -Alertas y Notificaciones
Riesgo	Contenido de aplicación con faltas de ortografía y acentuación
Causa	Falta de revisión
Posible Solución	-Revisar y corregir que cada palabra del menú de opciones (Ejemplo: Alertas y Notificaciones) y alertas de la aplicación inicien con letra mayúscula -Revisar y corregir ortografía de menú de opciones: acentuar módulo. -Acentuar textos necesarios de menú de opciones y contenido de la aplicación. -Corregir ortografía del motivo de sustitución “Suspensión definitiva” por “Suspensión definitiva”. -Corregir ortografía de campo “Motivo de la conseción de poder” por “Motivo de la concesión de poder” -Corregir por “Excepcional” el menú y títulos de pantalla
Evidencia	

Pruebas de contenido – Botones de acción innecesarios	
Gravedad	Medio
URL	https://siscoca.ruralytierras.gob.bo/empresas https://siscoca.ruralytierras.gob.bo/entidad-de-investigacion https://siscoca.ruralytierras.gob.bo/beneficiarios-de-donaciones https://siscoca.ruralytierras.gob.bo/beneficiarios-de-desarrollo

Módulo	Módulo de Registro
Riesgo	Propone que el flujo continúa con una siguiente pestaña dentro del formulario, siendo que el usuario se localiza en la última pestaña.
Causa	El botón Siguiente continúa mostrándose en la última pestaña de un formulario que consta de más de un paso
Posible Solución	Quitar los botones innecesarios del formulario.
Evidencia	

Pruebas de contenido – Estilos de contenidos vs Estilo general de la aplicación	
Gravedad	Bajo
URL	https://siscoca.ruralytierras.gob.bo/productores https://siscoca.ruralytierras.gob.bo/caracteristicas_produccion https://siscoca.ruralytierras.gob.bo/guias_internacion https://siscoca.ruralytierras.gob.bo/convocatorias_oii https://siscoca.ruralytierras.gob.bo/recepcion_solicitud_oii https://siscoca.ruralytierras.gob.bo/proyectos https://siscoca.ruralytierras.gob.bo/zona_autorizada https://siscoca.ruralytierras.gob.bo/regionales https://siscoca.ruralytierras.gob.bo/localidades https://siscoca.ruralytierras.gob.bo/comunidades https://siscoca.ruralytierras.gob.bo/marcas_vehiculos https://siscoca.ruralytierras.gob.bo/vehiculos
Módulo	-Módulo de Registro (todos los submódulos) -Módulo de Gestión de Actividades de Producción -Módulo de Actividades de Comercialización e Industrialización (todos excepto Control de hojas de ruta) -Módulo de Obras e Impacto Inmediato -Módulo de Parametrización
Riesgo	No sigue el lineamiento de estilo definido para el aplicativo
Causa	Estilos diferentes en iconos “Nuevo” son de color azul
Posible Solución	Cambiar estilos de color azul por color verde
Evidencia	

6.4. Análisis de código fuente

A partir del código fuente proporcionado por Mario Adolfo Valverde Suarez y Gonzalo Poma, dependientes del Ministerio de Desarrollo Rural y Tierras, se realizó el escaneo para evaluar la calidad y seguridad del código fuente con la herramienta SonarQube.

SonarQube, es una herramienta que permite evaluar la calidad del código fuente, realiza un análisis estático sobre el código con el objetivo de identificar los puntos a mejorar y obtener métricas que ayuden

a mejorar el código. El término de análisis estático se refiere al proceso de evaluar un software sin ejecutarlo.

6.4.1 Análisis de código fuente del lado del servidor (Backend)

De acuerdo a los resultados obtenidos se pudo evidenciar lo siguiente:

- El código fuente cumple los umbrales aceptables por las métricas de la herramienta por lo cual lleva el texto PASSED.
- No existen errores ni vulnerabilidades.
- Posibles problemas con la mantenibilidad de código por futuros desarrolladores, siendo 247 el total de casos sospechosos, cuya deuda se cubriría en siete días.
- La cantidad total de bloques de código repetido es de 17, representando un porcentaje de 1.8%.

El resumen se ilustra en la siguiente imagen:

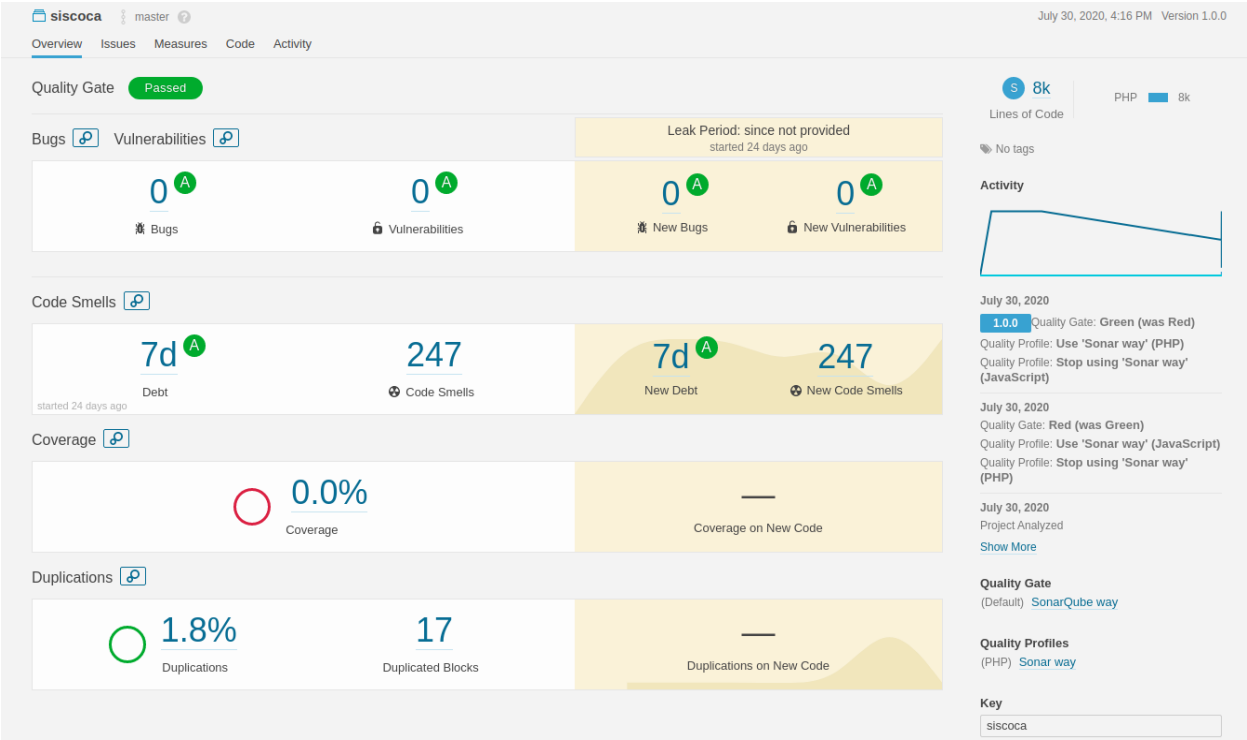


Figura 1: Resultado del análisis de código fuente backend

6.4.2 Análisis de código fuente de la aplicación web (Frontend)

De acuerdo a los resultados obtenidos se pudo evidenciar lo siguiente:

- El código fuente cumple los umbrales aceptables por las métricas de la herramienta por lo cual lleva el texto PASSED.
- No existen vulnerabilidades, pero sí se detectaron 14 errores de programación.
- Posibles problemas con la mantenibilidad de código por futuros desarrolladores, un total de 30 posibles casos cuya duración para su resolución abarcaría cuatro horas.

- La cantidad total de bloques de código repetido es de 878, representando un porcentaje de 19.8%.

El resumen se ilustra en la siguiente imagen:

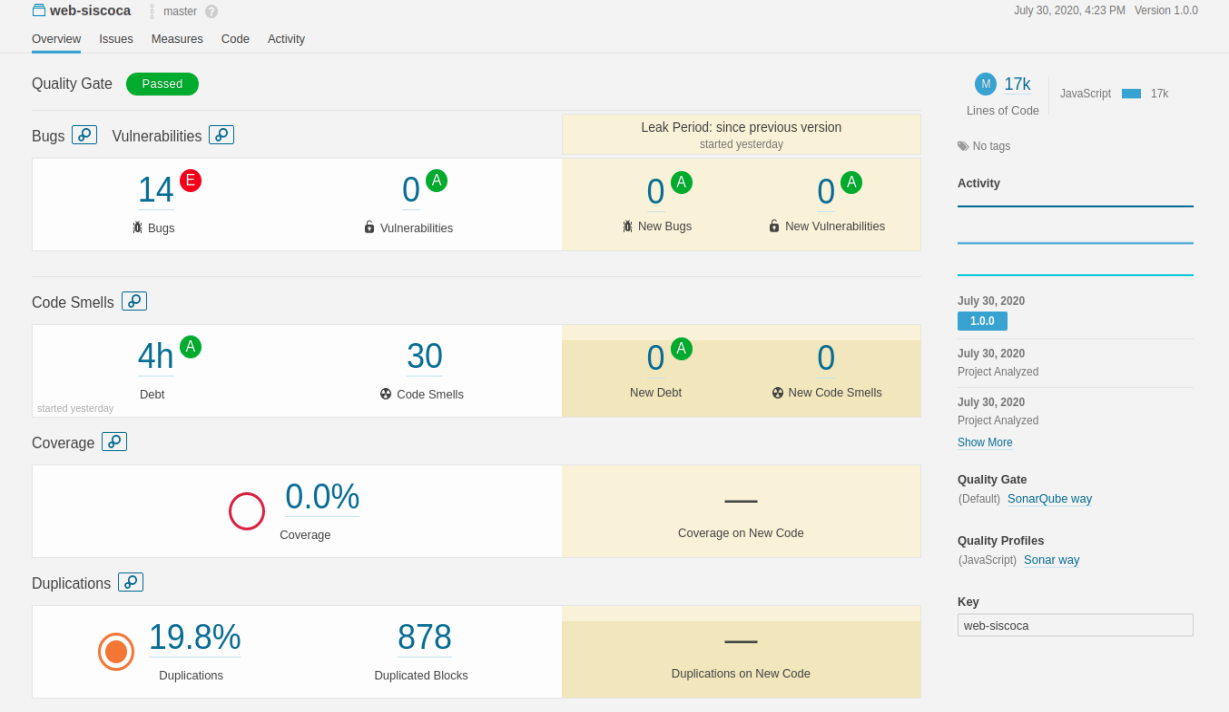


Figura 2: Resultado del análisis de código fuente de la aplicación web (frontend)

6.5. Análisis de vulnerabilidades del sistema

A partir del acceso público a la aplicación web SISCOCA proporcionada por Gonzalo Poma, dependiente del Ministerio de Desarrollo Rural y Tierras se realizó el análisis de seguridad utilizando la herramienta Owasp ZAP la cual permite simular ataques a sitios web y encontrar vulnerabilidades que pueden ser utilizadas por atacantes externos.

El resumen de alertas detectadas por la herramienta se ilustra a continuación:

Summary of Alerts

Risk Level	Number of Alerts
High	1
Medium	6
Low	28
Informational	5

Figura 3: Reporte de alertas de Owasp ZAP

Del resultado obtenido es necesario mencionar dos puntos importantes:

- La alerta calificada con riesgo Alto se refiere a la “Inyección SQL”, este tipo de ataque permite insertar sentencias SQL maliciosas en la aplicación web, obteniendo así accesos a datos sensibles de la base de datos.
- "Desbordamiento de Buffer” este fallo de seguridad figura dentro del listado de alertas de riesgo medio e indica que el sistema no considera o verifica sus límites de almacenamiento por lo que la memoria del sistema recibe una cantidad de datos mayor a la que realmente puede procesar.

Nota. El reporte completo del análisis se encuentra en el Anexo 4 - ReporteOwasp.

6.6. Análisis de arquitectura

6.6.1. Criterios de arquitectura de software

Para el análisis de arquitectura se han toman en cuenta los siguientes criterios:

- Rendimiento: se refiere a la respuesta del sistema, es el tiempo requerido para responder a un estímulo (evento) o número de eventos por unidad de tiempo, por ejemplo: una posible medida podría ser la cantidad de transacciones por segundo.
- Confiabilidad: es la habilidad del sistema de continuar operando sobre el tiempo, usualmente es una medida en tiempo promedio entre fallas.
- Disponibilidad: es la porción de tiempo en el que el sistema esta levantado y corriendo, se mide como el tiempo transcurrido entre fallas, así decir cuan rápido el sistema esta apto para reanudar y quedar operativo ante una falla.
- Seguridad: es la medida de la habilidad del sistema de resistirse al uso no autorizado y negar los servicios, mientras los provee a usuarios legítimos.
- Portabilidad: es la habilidad del sistema de correr sobre diferentes ambientes, estos ambientes pueden ser de hardware, de software o una combinación de ambos. Portabilidad es un caso particular de modificabilidad.
- Funcionalidad: es la habilidad del sistema de hacer el trabajo para el cual fue construido.

6.6.2. Evaluación de arquitectura de Siscoca

CRITERIO DE ARQUITECTURA	DESCRIPCION	CUMPLIMIENTO
Rendimiento	En la sección de análisis de rendimiento del sistema se evidenció y documentó que el sistema Siscoca, tiene tiempos de respuesta elevados (mayor a 10 segundos) en funcionalidades críticas y tiende a ser mayor en función de la cantidad de datos que almacena.	No cumple

Confiabilidad	En la sección de pruebas funcionales y análisis de manejo de transacciones en procesos críticos, se ha evidenciado que el sistema no realiza validaciones a nivel de los formularios web ni en la capa de servicios. También se ha evidenciado que no realiza ningún manejo de transacción y por consiguiente no existe ninguna garantía que los datos administrados por el sistema sean los correctos.	No cumple
Disponibilidad	En la sección de análisis de rendimiento del sistema se ha evidenciado que cuando el sistema se estresa, se tiene que realizar modificaciones manuales a los datos o reiniciar el servidor, también se ha evidenciado que las caídas pueden ocurrir con mayor frecuencia si existe gran volumen de datos.	No Cumple
Seguridad	Al no aplicar paginación en los servicios web (API REST), se exponen todos los datos de la tabla por servicios web. Los datos retornados por servicios web (API REST) se devuelven con todas sus relaciones, por consiguiente, se está exponiendo información sensible de manera completa a usuarios que no tienen permiso. La herramienta OWASP ZAP ha detectado que el sistema es vulnerable a ataques de "Inyección SQL", aspecto que se encuentra documentado en el Anexo 4 – ReporteOwasp.	No Cumple
Portabilidad	En la sección pruebas de diseño se ha evidenciado que la aplicación web tiene comportamiento inadecuado en Internet Explorer, por consiguiente, no cumple con el criterio de portabilidad.	No cumple
Funcionalidad	En la sección de pruebas funcionales se ha evidenciado que todos los módulos del sistema presentan problemas de validaciones básicos, reconocimiento facial, opciones que no funcionan, etc.	No cumple

7. Conclusiones y Recomendaciones

7.1. Conclusiones

Luego de realizar las evaluaciones correspondientes utilizando los métodos y herramientas descritos en las secciones previas, se concluye lo siguiente:

- Que el sistema no está optimizado para un ambiente de alto tráfico y su acceso será limitado por el ancho de banda de las conexiones a internet, puesto que, en las pruebas de estrés y funcionalidad, se ha evidenciado y documentado que el sistema presenta problemas de rendimiento; esto debido que los API REST recuperan todo el contenido de las tablas para

visualizar en la interfaz web y además recuperan las entidades con la mayoría de sus relaciones. Es así que en el "Módulo de registro" la funcionalidad "Productores" demora aproximada dos minutos en cargar los datos y solo tiene 19 registros, pero descarga aproximadamente 21.1 MB de datos. Esto fue corroborado con el escaneo de seguridad y rendimiento que se realizó al sistema con la herramienta Owasp ZAP, puesto que ha detectado 165 recursos de la aplicación web que presenta problemas de "Buffer Overflow" (Sobrecarga de Memoria) que causa un error 500 a nivel del servidor y podría causar la caída del servidor.

- Que el sistema no administra de manera correcta los procesos concurrentes, puesto que en las evaluaciones del estrés se ha evidenciado y documentado que en un contexto de alto tráfico y concurrente se genera errores **irrecuperables** por la generación de códigos de productores duplicados, aspecto que se encuentra documentado en la sección Pruebas de estrés y que sólo se logró solucionar modificando manualmente un registro a nivel de base de datos.
- Que el sistema no administra de manera correcta los procesos transaccionales, puesto que se logró generar inconsistencias en la base de datos al momento de registrar los poderes en el "Módulo de Actividades de Comercialización e Industrialización", mismo se encuentra documentado en la sección Análisis de manejo de transacciones en procesos críticos
- Que el sistema no aplica validaciones de entrada en los formularios web ni en la capa de servicios, puesto en las pruebas de funcionalidades se ha logrado enviar peticiones con contenidos erróneos o caracteres especiales (# $%' ') o espacios en blanco y los mismos han generado error en el servidor, lo mencionado se encuentra documentado en la sección Pruebas funcionales.
- Que la configuración de servidor no es apta para un ambiente productivo, puesto que en el reporte de seguridad de la herramienta Owasp ZAP, se ha evidenciado que no se consideran el uso de cabeceras de seguridad en la configuración del servidor.
- Que el sistema se ha implementado sobre una arquitectura monolítica, esto dificulta el despliegue en ambientes de alta disponibilidad.
- Que las API REST implementadas no contemplan las buenas prácticas de desarrollo, puesto que la mayoría de los servicios que filtran información reciben como parámetro de ruta objetos json.

7.2. Recomendaciones

7.2.1. Recomendaciones a nivel de la aplicación Frontend

Se debe considerar implementar las siguientes recomendaciones:

- Implementar validaciones de datos en todos los formularios de la aplicación web, en lo posible se debe utilizar expresiones regulares para validar los datos de entrada.
- Se debe enmascarar los errores que se generan a nivel de servidor con mensajes personalizados, a fin de no divulgar información sensible del servidor.
- Se debe estandarizar el uso de los formatos de fecha.
- Se debe adecuar la aplicación web para que soporte la creación de roles y permisos de forma dinámica.

- Considerar mejorar o quitar el reconocimiento facial de los flujos de control de hojas de ruta, puesto que en un 90% de las pruebas realizadas ha fallado o ha tomado un tiempo prolongado en completar la prueba.

7.2.2. Recomendaciones a nivel de la aplicación Backend

Se debe considerar implementar las siguientes recomendaciones:

- Se debe considerar de manera imperativa aplicar un trabajo de reingeniería a la arquitectura del sistema, en el que se contemple procesos concurrentes, transaccionales optimizados para ambientes de alta disponibilidad.
- Se debe considerar implementar una arquitectura para desplegar en un ambiente de alta disponibilidad (Contenedores o ambientes cluster).
- Se debe considerar que los archivos (imágenes, documentos) deben ser administrados por un servidor de archivos independiente de los servidores en los que se implementa la lógica de negocio o la aplicación web. Esto con el propósito de lograra una arquitectura de alta disponibilidad.
- Se debe considerar realizar trabajos de reestructuración a nivel de la capa de servicios para implementar técnicas de paginación, manejo de transacciones, validaciones en los procesos de inserción, actualización y extracción de datos.
- Se debe considerar el uso **secuencias de base de datos** para los algoritmos de generación de códigos únicos.
- En la implementación de los API REST se debe considerar retornar entidades con la menor cantidad de relaciones posibles, con el propósito de no retornar datos innecesarios.
- Considerar subsanar las observaciones de seguridad de la herramienta Owasp ZAP, que se encuentra en Anexos, las mismas hacen referencia a configuración del servidor para incluir cabeceras.