Fomento a la construcción de capacidades en relación a las políticas públicas apoyadas por Contratos de Reforma Sectorial (CRS) en Bolivia 2014/25

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

DI-023/3 – Actualización del diseño y desarrollo de los módulos de Control, Producción y Comercialización de la hoja de coca (Fase 3)

APENDICE 1

P1. Diagnóstico actualizado de situación del SISCOCA: infraestructura y sistemas (medios; alimentación; reportes;) con recomendaciones (Sostenibilidad de mediano y largo plazo y ampliación de funciones).

Contrato n° DCI/LA/2017/392-699

Proyecto Financiado por la Unión Europea

Implementada por el consorcio:
AGRER — AECOM — TRANSTEC
Bruselas, abril 2022

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

DI-023/3 – Actualización del diseño y desarrollo de los módulos de Control, Producción y Comercialización de la hoja de coca (Fase 3)

APENDICE 1

P1. Diagnóstico actualizado de situación del SISCOCA: infraestructura y sistemas (medios; alimentación; reportes;) con recomendaciones (Sostenibilidad de mediano y largo plazo y ampliación de funciones).

Autor: Oscar Martinez / Carlos Machicado

La Paz, noviembre 2022

Consorcio AGRER – DT GLOBAL – COWATER

INDÍCE

LISTA DE LAS TABLAS

LISTA DE GRÁFICOS

ACRÓNIMOS

AP	Apoyo presupuestario
APS	Apoyo presupuestario sectorial
AT	Asistencia técnica
DIC	Desarrollo integral con coca
DIGCOIN	Dirección General de la Hoja de Coca e Industrialización.
DIGPROCOCA	Dirección General de Desarrollo Integral de las Regiones Productoras de Coca.
DITISA	Desarrollo integral con coca, tráfico ilícito de drogas y seguridad alimentaria para una eficiente gestión del apoyo presupuestario sectorial en Bolivia
DUE	Delegación de la Unión Europea.
JAT	Jefatura de Asistencia Técnica
MDRyT	Ministerio de Desarrollo Rural y Tierras
MED	Marco de evaluación de desempeño (uno por APS)

PAPS	Programa de Apoyo Presupuestario Sectorial.
PEI	Plan estratégico institucional
PFI	Programa de fortalecimiento institucional
POA	Plan operativo anual
RO	Reglamento operativo
SISCOCA	Sistema Único de la Coca
TIC	Tecnologías de la Información y las comunicaciones
TI	Tecnologías de la Información
UDESTRO	Unidad de Desarrollo Económico y Social del Trópico de Cochabamba.
UDESY	Unidad de Desarrollo Económico y Social de Yungas de La Paz.
UE	Unión Europea.
VCDI	Viceministerio de Coca y Desarrollo Integral (MDRyT)

TERMINOS

Backup	(Copia de seguridad) Un recurso que es, o puede usarse, como un sustituto cuando falla un recurso principal o cuando un archivo se ha dañado. La palabra también se usa como verbo, respaldar, es decir, hacer una copia anticipando fallas o daños futuros. Así, un volcado forma una copia de seguridad que se utilizará en los casos en que el archivo de un usuario se haya vuelto inservible; la realización del volcado se puede considerar como una copia de seguridad de la versión en el disco.
Código fuente	La forma de un programa que se ingresa a un compilador o transpiler para conversión en código objeto equivalente.
IDE (Interactive development environment)	Entorno de desarrollo interactivo Un conjunto de programas para el desarrollo de programas o aplicaciones con un usuario común que interactúa, a menudo usa una interfaz gráfica de usuario e incluye herramientas de software para escribir y editar código, compilar, ejecutar y depurar con una manera fácil y consistente de moverse entre las diversas funciones.
Log	Registro generado por procedimiento que implica registrar todos los datos e interacciones que pasan por un punto particular de un sistema. El punto elegido suele ser parte de un bucle de comunicación o una ruta de datos hacia o desde un dispositivo como un teclado y una pantalla en la que los datos son transitorios. Si ocurre una falla del sistema o un resultado inesperado, es posible reconstruir la situación que existía. Por lo general, estos registros no se archivan y se pueden sobrescribir una vez que se haya completado el trabajo asociado.
Módulo	Es una construcción de programación o especificación que define un componente de software. A menudo, un módulo es una unidad de software que proporciona a los usuarios algunos tipos de datos y operaciones sobre esos tipos de datos, y puede en algunos casos compilarse por separado.
Seguridad informática	Es el conjunto de normas, procedimientos y herramientas, las cuales se enfocan en la protección de la infraestructura computacional y todo lo relacionado con ésta y, especialmente, la información contenida o circulante.

Seguridad de la información	la seguridad de la información es la preservación de la confidencialidad, integridad y disponibilidad de la información; además, también pueden estar involucradas otras propiedades como la autenticidad, responsabilidad, no repudio y confiabilidad
Plan de contingencia	Es un instrumento que comprende métodos y el conjunto de acciones para el buen gobierno de las Tecnologías de la Información y Comunicación en el dominio del soporte y el desempeño, contiene las medidas técnicas, humanas y organizativas necesarias para garantizar la continuidad del servicio y las operaciones de una entidad, en circunstancias de riesgo, crisis y otras situaciones anómalas.
Responsable de Seguridad de la Información (RSI)	Servidor público responsable de gestionar, planificar, desarrollar e implementar el Plan Institucional de Seguridad de la Información. y
RTO: (Tiempo Objetivo de Recuperación):	Es el periodo de tiempo real dentro del cual la entidad debe recuperarse después de una interrupción. También hace referencia al tiempo transcurrido entre la interrupción y recuperación e indica el tiempo disponible para recuperar lo interrumpido.
RPO: (Punto Objetivo de Recuperación)	Es la tolerancia o sensibilidad que tienen los procesos críticos de la entidad para su operación, respecto a la pérdida de información sensible.
Red	Son las instalaciones que en su conjunto establecen conexiones o comunicaciones entre dos o más puntos para conducir símbolos, señales, textos, imágenes, voz, sonidos, datos, información de cualquier naturaleza u otro tipo de señales electrónicas, mediante líneas físicas, ondas electromagnéticas, medios ópticos u otro tipo de conexión. Los equipos y programas son parte de la red. Las redes podrán ser: red pública, red privada u otras.
Tecnologías de Información y Comunicación – TIC	. Comprende al conjunto de recursos, herramientas, equipos, programas informáticos, aplicaciones, redes y medios, que permiten la compilación, procesamiento, almacenamiento, transmisión y recepción de información, voz, datos, texto, video e imágenes. Se consideran como sus componentes el hardware, el software y los servicios.
Telecomunicaciones	Comprende la transmisión, emisión y recepción, de señales, símbolos, textos, imágenes, video, voz, sonidos, datos o información de cualquier naturaleza o aplicaciones que facilitan los mismos, por cable o línea física, radioelectricidad, ondas hertzianas, medios ópticos u otros sistemas radioeléctricos de cualquier índole o especie, a través de una red pública o privada.
Política de Seguridad de la Información (PSI)	Acciones o directrices que establecen la postura institucional en relación a la seguridad de la información, incluidas dentro del Plan Institucional de Seguridad de la Información
Confidencialidad	Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados
Disponibilidad.	Propiedad de acceso y uso de información a entidades autorizadas cuando estas lo requieran.
Integridad.	Propiedad que salvaguarda la exactitud y completitud de la información

1. INTRODUCCIÓN

A través de la misión corta DI - 023/3 "Actualización del diseño y desarrollo de los módulos de Control, Producción y Comercialización de la hoja de coca (Fase 3)" con base a un análisis de riesgos del principal activo de la información que es el SISCOCA (SISCOCA-SAR y SIICATCOCA - MODULO DE PRODUCCIÓN), se realiza la identificación de los principales aspectos de riesgo que deben ser valorados por el VCDI, DIGPROCOCA y DIGCOIN respecto de la infraestructura que soporta los sistemas indicados, las funcionalidades implementadas, la seguridad incorporada para evitar perdida de información, es por eso que el presente documento presenta resultados en relación al diagnóstico y la priorización de mejoras al SISOCOCA.

2. OBJETIVO

De acuerdo al alcance definido en los términos de referencia de la misión se establece los siguientes objetivos.

2.1 Objetivo general

La misión establece el siguiente objetivo:

"Fortalecer las competencias y capacidades del Viceministerio de Coca y Desarrollo Integral en el monitoreo y control de las superficies de cultivos de coca, y en el registro y trazabilidad de la cadena de comercialización de hoja de coca en los mercados autorizados."

2.2 Objetivos específicos

- Efectuar un diagnóstico de la situación del SISCOCA, en cuanto a la infraestructura y el sistema informático implementado, tomando en cuenta los medios de registro, su procesamiento, y la generación de reportes; asimismo, la definición de recomendaciones relacionados con la sostenibilidad de mediano y largo plazo y la ampliación de funciones del sistema.

3. ALCANCE

Se define que el alcance del documento es:

- Efectuar un diagnóstico de situación actual del SISCOCA
- Evaluar la infraestructura que soporta el SISCOCA en DIGPROCOCA y DIGCOIN
- Evaluar el sistema SISCOCA en cuento a la operativa de medios disponibles, registro (alimentación) de la base de datos, la emisión de reportes
- Efectuar recomendaciones relacionadas con la sostenibilidad de mediano y largo plazo; además de identificar una posible ampliación de funciones y funcionalidades.

3.1. Limitaciones al alcance

Se define como principales limitaciones lo siguiente:

- La definición del producto esta circunscrito en el alcance del producto P1 según el plan de trabajo definido.
- Los factores externos que surjan y que implique posibles cambios en el alcance del logro del producto no serán realizados en el marco de la misión, pero si serán informados a la JAT de DITISA.
- No es de responsabilidad la compra de equipamiento o contratación de consultores.
- No es de responsabilidad de la consultoría el diseño de políticas, procedimientos técnicos que impliquen los sistemas de información en producción.

3.2 Identificación de la entidad

Nombre de entidad: Autoridad: Dirección Oficina Central: Teléfonos:	VICEMINISTERIO DE COCA Y DESARROLLO INTEGRAL – VCDI Arlem Lovera Esprella Viceministro de Coca y Desarrollo Integral Av. Sanchez Lima Edif. Orion Nro. 2072 PB, entre Calles Ecuador y Aspiazu, Zona Sopocachi contacto@vcdi.gob.bo (591-2) 2422310 - 2421308 - 2426560 Fax-Administración: (591-2) 2129750
Nombre de entidad: Autoridad: Dirección Oficina Central: Teléfonos:	Dirección General de Desarrollo Integral de las Regiones Productoras de Coca - DIGPROCOCA Mario Condori Palli Director General DIGPROCOCA Av. Sanchez Lima Edif. Orion Nro. 2072 PB, entre Calles Ecuador y Aspiazu, Zona Sopocachi (591-2) 2422310 - 2421308 - 2426560 Fax-Administración: (591-2) 2129750
Nombre de entidad: Autoridad: Dirección Oficina Central: Teléfonos:	Dirección General de la Hoja de Coca e Industrialización - DIGCOIN Dario Manrique Choque Director General DIGCOIN Villa Fatima Calle Covendo
Jefe de asistencia Técnica Asistente técnico AT-VCDI	Marko Letho / Alessandro Boccoli Oscar Martinez Carlos Machicado

4. METODOLOGIA DE TRABAJO

El esquema metodológico define también una fase de "Evaluación", que corresponde al análisis de la estructura organizativa, del VCDI, DIGPROCOCA y DIGCOIN, La evaluación de la infraestructura tecnológica de soporte al SISCOCA, la evaluación y análisis efectuado al sistema SISCOCA, como producto principal de esta fase corresponde al "Diagnostico actualizado de la situación del SISCOCA (Producto 1)".

Tabla 1: Metodología de trabajo Arquitecto de sistemas

	Evaluación Inicial	Evaluación	Desarrollo y mantenimiento	Implementación
Actividades	• Reunión inicial de coordinación de la misión • Trabajo de entendimiento adecuado de las expectativas de DIGPROCOCA Y DIGCOIN • Evaluación inicial sobre el entendimiento de los sistemas de información SISCOCA MODULO DE PRODUCCIÓN Y SISCOCA MODULO DE COMERCIALIZACIÓN DE DIGPROCOCA Y DIGCOIN respectivamente. • Revisión de documentos y normativa asociada.	• Análisis la estructura organizacional del VCDI, DIGPROCOCA y DIGCOIN • Evaluación de la infraestructura de tecnologías de la información de DIGPROCOCA y DIGCOIN • Recorrido y análisis del sistema SISCOCA producción y comercialización • Evaluación y diseño organizacional del área de TI de VCDI, DIGPROCOCA y DIGCOIN.	• Realización de las notas técnicas sobre las especificaciones técnicas de equipos para los módulos de producción y comercialización • Realización de informes de avance mensuales • Coordinación del desarrollo de las adecuaciones del sistema SISCOCA • Trabajo de campo para la definición de las adecuaciones de SISCOCA Producción y comercialización	• Coordinación de las pruebas e instalación de los ajustes al sistema SISCOCA y obtención de conformidad • Elaboración del informe final de la misión.
Productos	• P0: Plan de Trabajo, metodología y cronograma de la misión de corta duración y de sus fases de implementación	• P1. Diagnóstico actualizado de situación del SISCOCA • P3: Documento de conformación organizacional de la Unidad de Sistema en el VCDI (DIGPROCOCA), con perfiles de personal y descripción de dotaciones operacionales; • P4: Documento de conformación de la Unidad de Sistemas del VCDI (Perfiles de personal y criterios de evaluación);	• P2: Notas técnicas de asesoría sobre especificaciones técnicas de equipos para los módulos de Producción y Comercialización del SISCOCA, y nota de conformidad a la recepción;	• P5. Informe final de Misión

La evaluación y diagnóstico de la situación del SISCOCA ha implicado las siguientes actividades específicas:

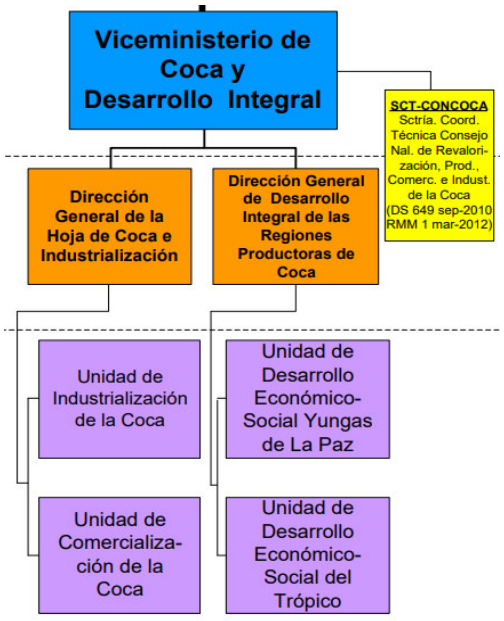
- Revisión documentaria general normativa, manuales, organizacional.
- Reunión de trabajo con los responsables de sistemas de VCDI, DIGPROCOCA y DIGCOIN, para efectuar un recorrido por los sistemas de información de producción y comercialización.
- Determinación del inventario de priorizaciones de desarrollo.
- Revisión de la infraestructura tecnológica de VCDI y DIGCOIN (Revisión de hardware y software).
- Revisión del esquema de red y de comunicaciones que soporta al SISCOCA.
- Análisis de riesgos SISCOCA.
- Reuniones de discusión con responsable de VCDI, DIGPROCOCA y DIGCOIN.

5. DIAGNOSTICO

5.1. Diagnóstico de la organización

Para lograr una comprensión sobre la situación del VCDI, DIGRPOCOCA y DIGCOIN, es preciso inicialmente que tengamos un conocimiento global de la organización de dichas entidades y su relacionamiento con el SISCOCA; al respecto, se tuvo acceso al organigrama oficial aprobado por resolución del MDRyT No 322 de 8 de septiembre de 2021, en el cual se encuentra publicado en la página WEB del Ministerio y del Viceministerio, dicho organigrama presente dos direcciones:

Gráfico 1: Organigrama General VCDI



Dirección General de Comercialización e Industrialización de la Hoja de Coca (DIGCOIN), tiene como competencias principales el supervisar, dirigir y ejecutar acciones técnicas y operativas de control, fiscalización de flujos de comercio de la hoja de coca en rutas nacionales en coordinación con las diferentes entidades públicas nacionales involucradas, así también ejecutar acciones para promover políticas, planes, programas y proyectos de industrialización y revalorización basado en el aprovechamiento cultural, medicinal e industrial de la hoja de coca en el Estado Plurinacional de Bolivia (Tierras, 2021).

Esta Dirección cuenta con el sistema denominado SISCOCA - SAR - Comercialización, aplicación de escritorio desarrollada en lenguaje de programación Visual Basic 6 (La última versión fue la 6, liberada en 1998, para la que Microsoft extendió el soporte hasta marzo de 2008), su motor de base de datos SQL Server 2008(Microsoft deja de dar soporte extendido a su software SQL Server 2008 y SQL Server 2008 R2 a partir de 2019), cuyo equipo servidor esta con un Sistema Operativo Windows 32 bits (Windows 7, NT, Versiones Actuales soporte 32 bits).

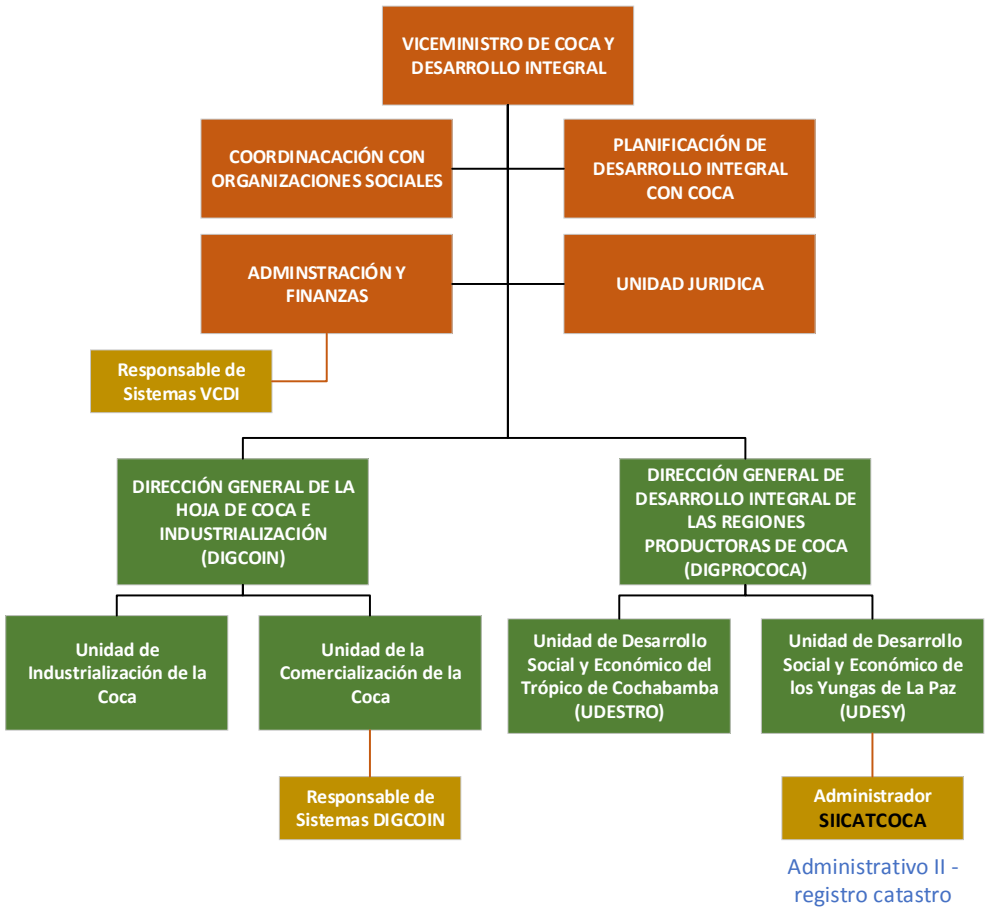
Dirección General de Desarrollo Integral de las Regiones Productoras de Coca (DIGPROCOCA), tiene como principales competencias la promoción y seguimiento a las acciones generadas para el Desarrollo Integral, técnicas y operativas para el control de cultivos de coca a través de la concertación, control social comunitario en las regiones autorizadas de productoras de Coca situadas en los Yungas de La Paz y el Trópico de Cochabamba (Tierras, 2021).

DIGPROCOCA, cuenta con dos unidades: Unidad de Desarrollo Social y Económico del Trópico de Cochabamba (UDESTRO) y Unidad de Desarrollo Social y Económico de los Yungas de La Paz (UDESY). Se identifica que los sistemas utilizados por estas unidades con el Sistema de Administración de Catos de Coca del Trópico de Cochabamba (SACCTC) y el sistema Integrado Catastral de Productores de Coca

(MODULO DE PRODUCCIÓN) desarrollado con lenguaje de programación PHP y framework CodeIgniter, base de datos PostgreSQL 9.3.

Por otro lado, del relevamiento efectuado a las unidades organizacionales del VCDI se pudo identificar el siguiente organigrama general que identifica las principales funciones de tecnologías de la información y las comunicaciones, el gráfico 2 expone dichas funciones en los cajones de color naranja.

Gráfico 2: Organigrama VCDI



Fuente: VCDI / DIGPROCOCA/DIGCOIN – Organigrama MDRyT
Elaboración: Propia

Se puede identificar que el VCDI cuenta con un área de sistemas dependiente de la Unidad Administrativa y Financiera a cargo de un "Responsable de sistemas" que tiene como funciones principales la de gestionar y administrar los recursos informáticos de la entidad; asimismo, la de otorgar soporte informático a los áreas funcionales, la gestión de la seguridad informática, y el aseguramiento de la continuidad de los servicios informáticos del VCDI; asimismo, tiene a su cargo la administración de los equipos de comunicaciones, y servidores principales del VCDI, donde se aloja el sistema SISCOCA – MODULO DE PRODUCCIÓN, no efectúa desarrollo ni mantenimiento de los sistemas

existentes en el VCDI, a la fecha del presente diagnóstico no se identifican proyectos de desarrollos en ejecución.

De la misma manera se solicitó el Manual de Organización y Funciones, y un organigrama por cargo a nivel de detalle para el VCDI con el objeto de identificar adecuadamente la función de tecnologías de la información, al respecto el Viceministerio no presenta un organigrama formal que muestre los cargos y las funciones debidamente descritos.

Asimismo, se pudo identificar que DIGPROCOCA es responsable de la administración del sistema SISCOCA – MODULO DE PRODUCCIÓN quien a través del técnico con cargo “Administrativo II - registro catastro”, es el administrador del sistema cuya función es el registro, control de la producción, gestión de usuarios, y la administración en general de dicho sistema.

Asimismo, DIGCOIN cuenta con un sistema denominado SISCOCA – SAR, que esta administrado por un “Responsable de sistemas”, que tiene como función la administración, gestión y otorgar soporte a los usuarios de DIGCOIN. Tiene a su cargo una infraestructura tecnológica de comunicaciones y red, servidores y equipos en general, se pudo identificar que tiene como funciones complementarias funciones administrativas relacionadas al control de hojas de ruta, emisión de carnets de comercialización, novedades en general. No se tiene evidencia que las funciones de tecnologías de la información y comunicaciones estén formalizadas en un manual de funciones y cargos.

5.2. Diagnóstico de la infraestructura implementada

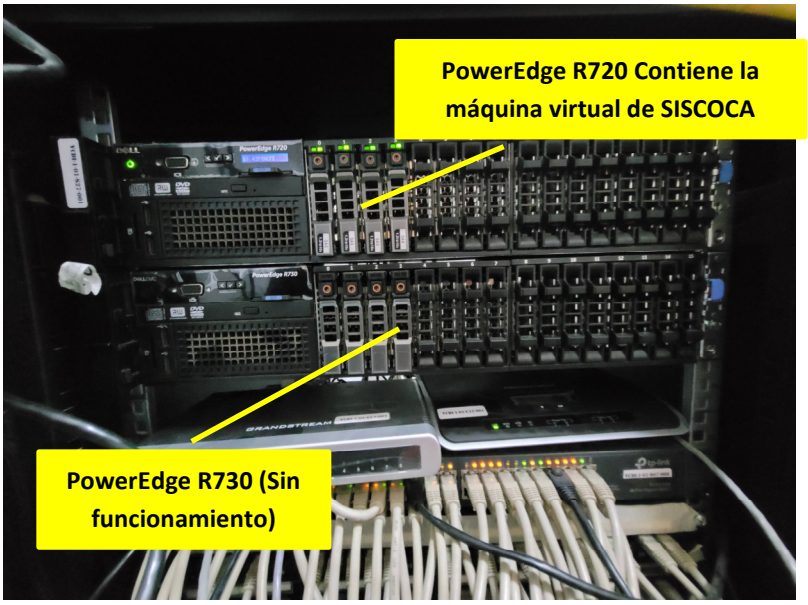
La infraestructura implementada por el Viceministerio de Coca y Desarrollo Integral - VCDI, cuenta con el siguiente esquema de comunicaciones.

- Cuenta con una conexión de internet conectada la red del VCDI a través de un Router MIKROTIK´, cuya principal función es la de efectuar NAT de la IP publica, con el propósito de generar un enmascaramiento interno para convertir la IP pública en varias direcciones IP.
- Cuenta con una red segmentada, cuyos puertos son distribuidos a una red local a través de un Switch TPLINK, el cual conecta la telefonía IP, un DVR de administración de cámaras y los usuarios en general; asimismo, se define un segmento para un servidor en RACK (DELL PowerEdge R720) que actualmente está configurada con PROXMOX de virtualización, de acuerdo al gráfico 3 se puede identificar que cuenta con 7 servidores virtualizados con sistemas operativos Linux y Windows, de los cuales dos corresponden al sistema SISCOCA - MODULO DE PRODUCCIÓN.
- Cuenta con una red de comunicaciones de complejidad “Baja” o no compleja.
- Los equipos de comunicaciones y de cómputo como los servidores, no cuentan con un programa de mantenimiento preventivo para reducir riesgos de continuidad, los mantenimientos son realizados a demanda o bien cuando un equipo tiene un desperfecto.
- Todos los equipos de cómputo y comunicaciones, incluido el mobiliario asignado están cubiertos con polvo.

- No se ha define una seguridad física ambiental, el rack de comunicaciones y cómputo está en un espacio compartido con el área de trabajo del responsable de sistemas, esta área cuenta con un solo acceso a través de una puerta de madera con chapa.
- El área de comunicaciones y servidores no cuenta con una organización adecuada y existe presencia de material de trabajo; además, de cajones con cables.
- No cuenta con un perímetro de seguridad diferenciado del área común de trabajo, no se identifica la instalación de sensores de calor, humedad; así como, un sistema de aire para mantener los equipos a temperatura recomendada.
- Los equipos servidor no cuentan con un antivirus o anti malware que permita establecer un adecuado aseguramiento ante posibles pérdidas de información o servicio.
- No se define un perímetro de seguridad externo gestionado a través de un firewall, que defina las políticas de seguridad de la red y las comunicaciones.

Los activos de información con mayor criticidad en el VCDI son la estructura de comunicaciones y el servidor PowerEdge R720 con sistema operativo PROXMOX debido a que este se encuentra funcionamiento y en operaciones con servidores virtuales; asimismo, se identificó que existen 2 servidores que no están en funcionamiento.

Gráfico 3: Servidores VCDI

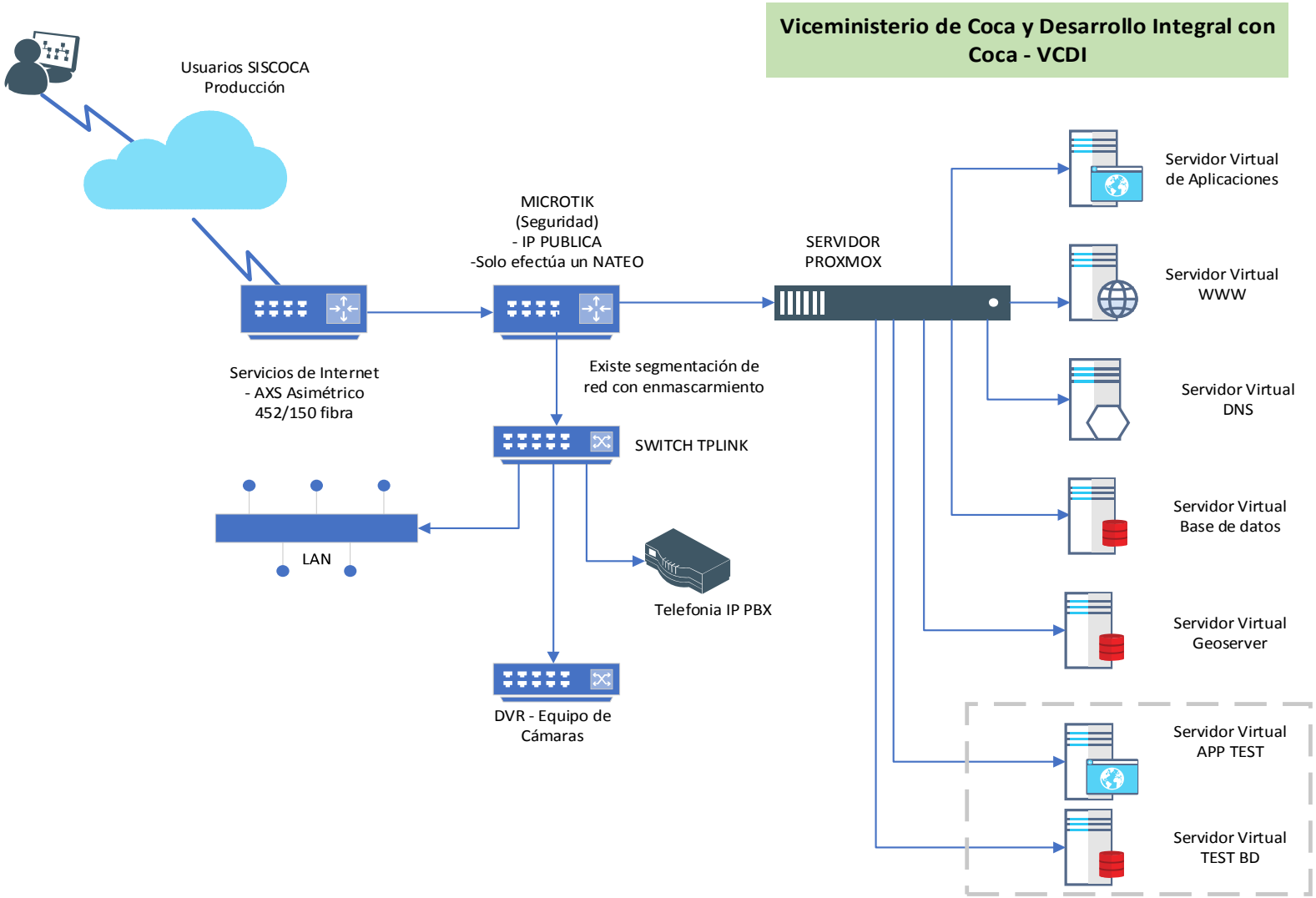


El Anexo 2: Evidencia fotográfica Área de Sistemas y CPD TI – VCDI, corresponde a los aspectos identificados en la visita y el diagnóstico realizado.

Por otro lado, el esquema de comunicaciones identificado según el gráfico 4, no define adecuadamente un esquema de seguridad, debido a que el perímetro de seguridad interno y externo no está resguardado por un firewall o una solución similar, si definen un router que permite el

enmascaramiento de IPs, los equipos de cómputo crítico son accesibles a los funcionarios de la entidad cuando acceden al área de trabajo de TI, los principales servicios comparten la misma red de datos que los usuarios en general.

Gráfico 4: Esquema de red y comunicaciones VCDI



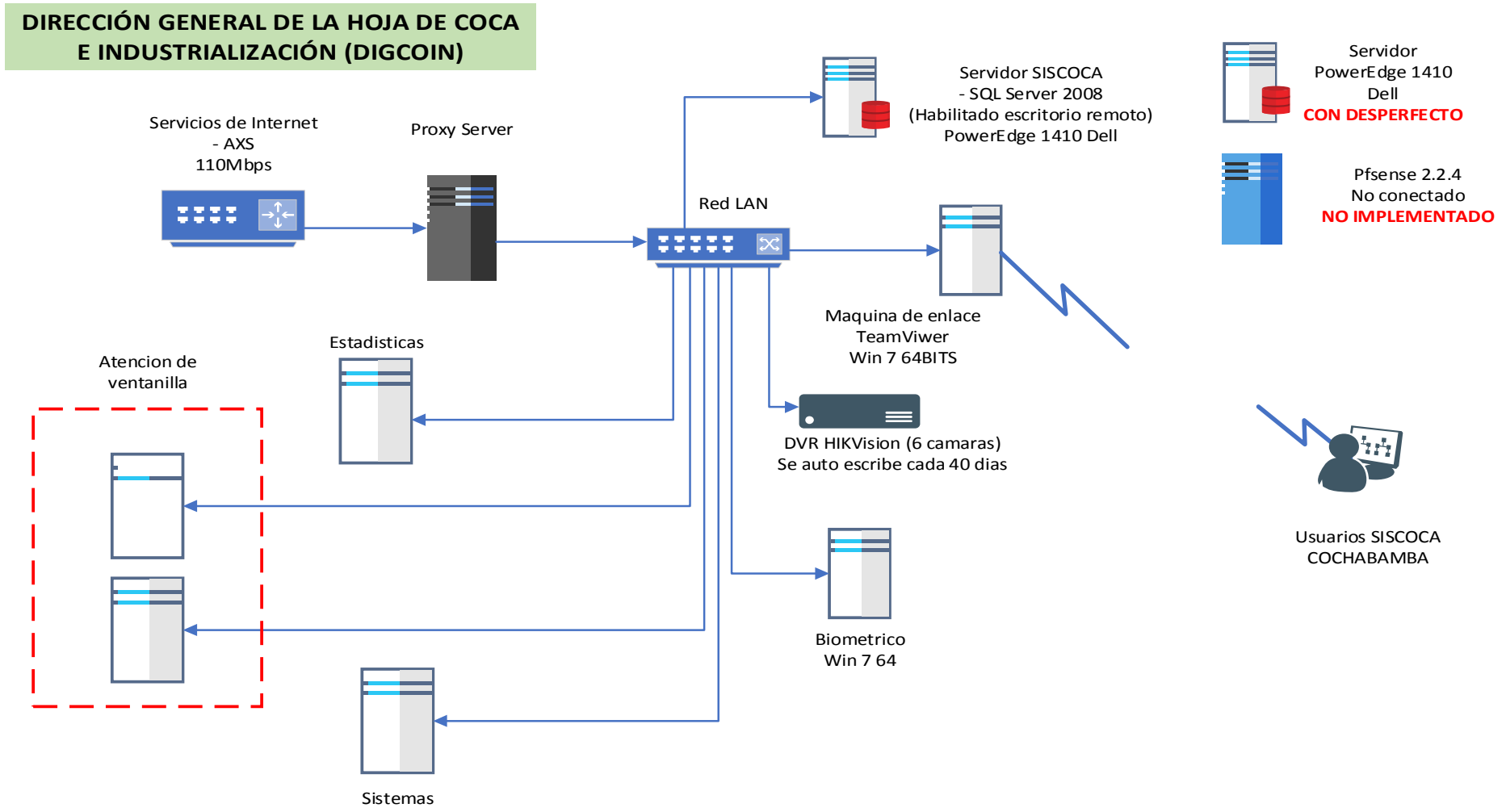
La infraestructura implementada por la Dirección General de la Hoja de Coca e Industrialización (DIGCOIN), cuenta con las siguientes características.

- Cuenta con una conexión de internet vinculada a la red de DIGCOIN, esta conexión esta intermediada por un servidor Proxy, el cual permite rutear el tráfico de red, y controlar las peticiones de internet; sin embargo, no permite ningún control o monitoreo del tráfico.
- Cuenta con una red local mediante la implementación de un Switch central, el cual conecta las estaciones de trabajo (Estadísticas, Atención en ventanilla, Sistemas, el equipo biométrico), el servidor de base de datos y aplicación del SISCOCA-SAR; se implementa también, un equipo de enlace para usuarios de Cochabamba a través teamviwer, para gestionar el sistema y emitir las hojas de Ruta.
- Cuenta con una red de comunicaciones de complejidad “Baja” o no compleja.
- Los equipos de comunicaciones y los servidores, no cuentan con un programa de mantenimiento preventivo para reducir riesgos de continuidad (no se efectuaron procesos de mantenimiento).
- El rack de comunicaciones y computo está en un espacio diferenciado del área de trabajo del responsable de sistemas, esta área cuenta con un solo acceso a través de una puerta de madera con chapa, dicha área no cuenta con una organización adecuada y existe presencia de material de trabajo; además, de cajones con cables, equipos en desuso, documentos de bolsas (Ver Anexo 3: Evidencia fotográfica Área de Sistemas DIGCOIN).
- Los equipos servidor no cuentan con un antivirus o anti malware que permita establecer un adecuado aseguramiento ante posibles pérdidas de información o servicio.
- No se define un perímetro de seguridad externo gestionado a través de un firewall, que defina las políticas de seguridad de la red y las comunicaciones.
- Se identifica que existe un servidor similar al que se encuentra en producción el cual esta con algún desperfecto físico.
- Se tiene un equipo implementado con un firewall pfsense, pero el mismo no esta en funcionamiento.

Por otro lado, el esquema de comunicaciones identificado según el gráfico 5, no define adecuadamente un esquema de seguridad, debido a que el perímetro de seguridad interno y externo no está resguardado por un firewall o una solución similar, si definen un proxy que permite el control del tráfico de internet, pero no se identifica procesos de monitoreo al mismo, los principales servicios y recursos comparten la misma red de datos que los usuarios en general.

La Dirección General de Desarrollo Integral de las Regiones Productoras de Coca (DIGPROCOCA), no establece un área de sistemas, el soporte informático es otorgado por el área de sistemas del VCDI, quien se ocupa de dar soporte y hospedar el sistema SISCOCA-MODULO DE PRODUCCIÓN.

Gráfico 5: Esquema de red y comunicaciones DIGCOIN

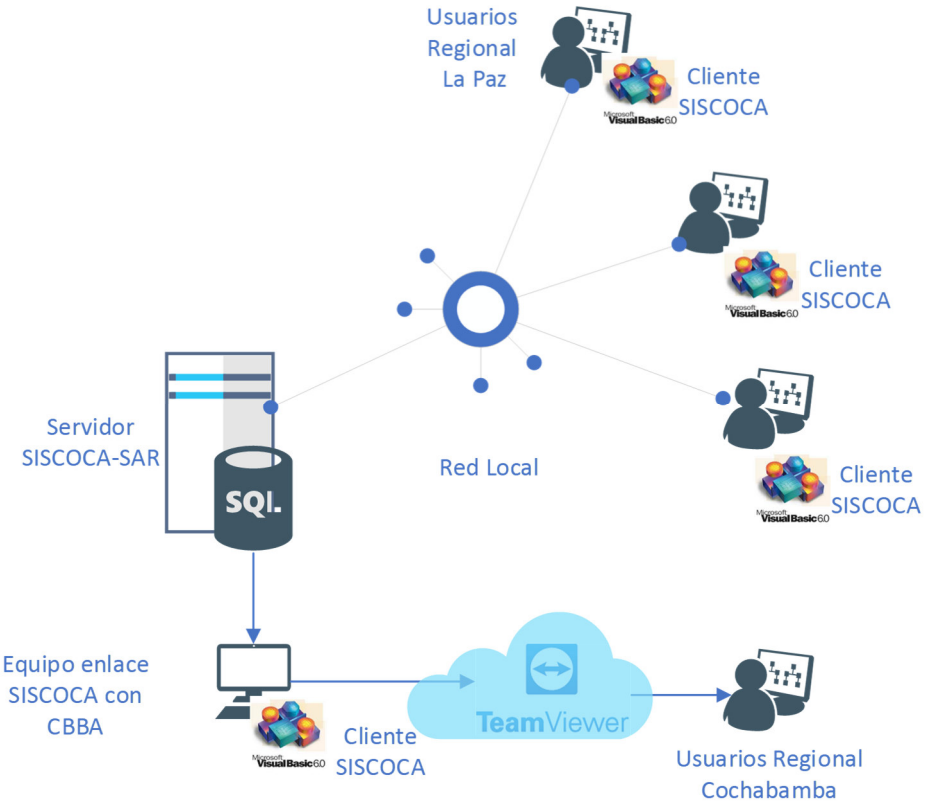


5.3. Diagnóstico del SISCOCA

5.3.1. Sistema SISCOCA -SAR

La Dirección General de la Hoja de Coca e Industrialización (DIGCOIN) cuenta con un sistema denominado SISCOCA - SAR, su arquitectura corresponde a una aplicación de escritorio, desarrollado en lenguaje de programación Visual Basic 6.0 con una base de datos SQL Server 2008, ver gráfico 6.

Gráfico 6: Arquitectura del sistema SISCOCA-SAR DIGCOIN



De acuerdo a la arquitectura presentada por el sistema, se pudo identificar lo siguiente:

- Se define un servidor central que contiene la base de datos del sistema SISCOCA-SAR implementado en SQLServer 2008.
- El acceso a la base de datos es a través de aplicaciones cliente que debe ser instalado en cada equipo de trabajo.
- Los usuarios de la regional de Cochabamba acceden a la aplicación a través de TeamViwer.
- Tanto los usuarios como el servidor principal comparten la misma red de datos.
- Se identifica que el servidor tiene instalado un sistema operativo Windows Server® 2008 Standard SP2 de 32 Bits, que implementa el motor de la base de datos y la aplicación.

Aspectos identificados sobre el sistema SISCOCA-SAR respeto a la seguridad y sus funcionalidades más importantes:

- El sistema SISCOCA-SAR establece funcionalidad para la gestión de usuarios, esta funcionalidad está a cargo del responsable de sistema de DIGCOIN, quien tiene la labor de adicionar, modificar o inactivar usuarios, de la revisión de usuarios se pudo identificar que solo los usuarios en función se encuentran activos.
- El sistema SISCOCA-SAR no define logs de auditoría que establezca una la trazabilidad de las operaciones realizadas por los usuarios.
- Los usuarios definidos en el sistema no están relacionados a un perfil de accesos, actualmente parte de los usuarios cuentan con todos los accesos a las funcionalidades del sistema SISCOCA-SAR.
- La carnetización de comercializadores cuenta con un módulo de registro en el SISCOCA-SAR; sin embargo, el proceso de emisión de carnets es efectuado a través de un proceso manual complementario; donde, el responsable del sistema una vez registrado en el sistema efectúa una copia de los registros de comercializador en planillas Excel y esta es vinculada con el dispositivo de impresión, por lo que la emisión del carnet no es realizada por el sistema.
- Los carnets de comercialización cuentan con códigos de barra y QR pero los mismos no almacenan datos relevantes, por lo que es posible que los mismos sean objeto de falsificación.
- La impresión de carnets no cuenta con controles como contadores de impresión o reimpresión y captura de usuarios.
- La emisión de hojas de ruta no cuenta con logs de auditoría, y controles de impresión o reimpresión.
- La trazabilidad de las hojas de ruta respecto del recorrido que debería seguir en cada viaje no está implementada en el sistema.
- Las hojas de ruta no están digitalizadas en el sistema para un adecuado resguardo y control histórico de cumplimiento de ruta.
- Las hojas de ruta cuentan con un código de barra que identifica el número secuencial que es almacenado en el sistema, dicho código no puede ser contrastado en puntos de control con la base de datos, no establece controles adecuados de seguridad para verificar su autenticidad contra la base de datos, esto significa que una hoja de ruta podría ser objeto de clonación, ya que los controles en los puestos no son contrastados digitalmente.
- El sistema no cuenta con módulos de parametrización de los puestos de control, donde se define la posición geográfica (punto o polígono geográfico), responsables de control, dispositivos autorizados para verificar las hojas de ruta y carnets de comercialización, en cuanto al cumplimiento de la ruta y su autenticidad.
- No se cuenta con controles automatizados que permita la verificación digital de las hojas de ruta y los carnets en los puestos de control, el control se basa principalmente en el paso físico de cada hoja de ruta por punto de control y el sello respectivo.
- El control de hojas de ruta sobre el cumplimiento de la ruta es efectuado manualmente por personal encargado de la emisión de las hojas de ruta, cualquier incumplimiento es verificado

manualmente sin el apoyo del sistema SISCOCA-SAR, respecto a la trazabilidad de cada hoja de ruta.

- Existen parámetros que son gestionados directamente en las bases de datos, los cuales no cuentan con módulos de mantenimiento (ABM, como por ejemplo los precios).

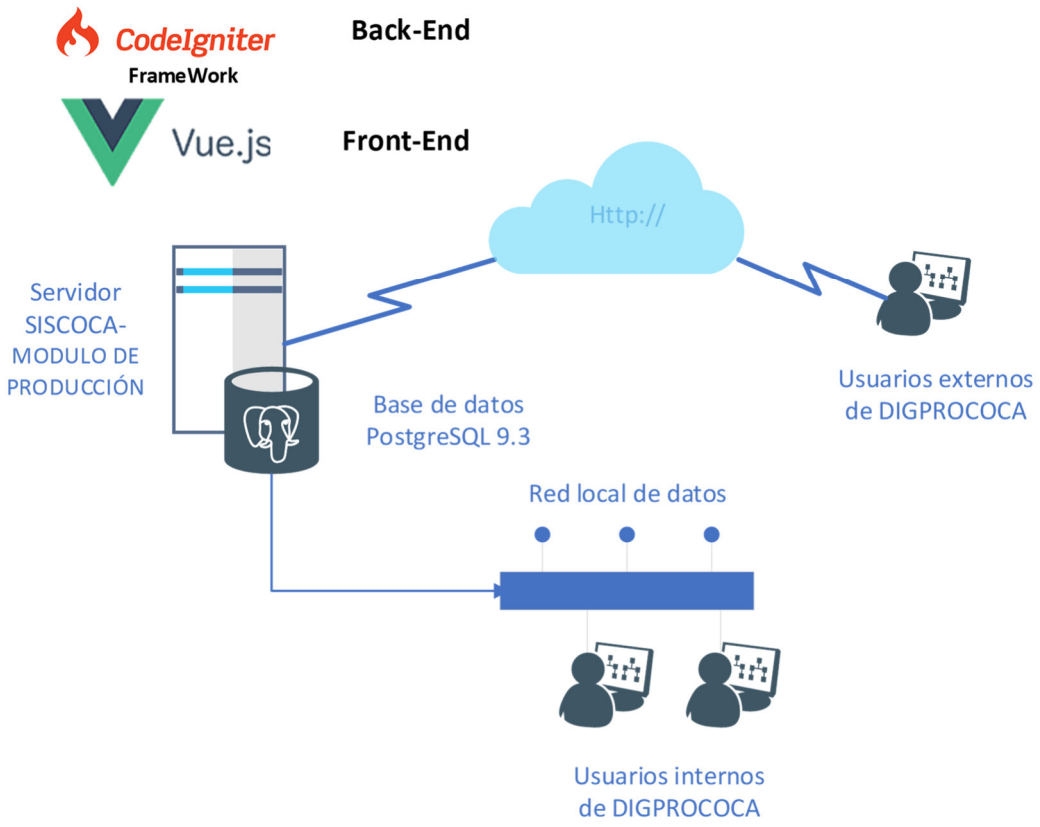
Otros aspectos de la gestión de la información y su aseguramiento:

- No se define políticas formales de respaldo para el sistema SISCOCA-SAR, los respaldos efectuados no son programados y no tienen un procedimiento que defina la periodicidad y el tipo de respaldo en función a un RTO y RPO basado en un análisis de riesgo.
- No se definen políticas de resguardo de código fuente, por lo que, el código fuente de SISCOCA-SAR no corresponde a la versión en producción, debido a que en el proceso de restauración del código fuente y compilación del mismos para replicar la versión de producción, no fue posible debido a que el mismo no está completo y faltan partes de código, por lo que, no es posible efectuar modificaciones al sistema.
- No se puedo evidenciar una documentación técnica del sistema SISCOCA-SAR que permita orientar sobre la estructura de bases de datos, objetos, y arquitectura; para efectuar un entendimiento adecuado y propiciar un mantenimiento o actualización.
- La base de datos del SISCOCA-SAR se encuentra instalado en el único servidor, por lo que un desperfecto, una contingencia física o robo del mismo, podría interrumpir las operaciones de DIGCOIN, y no se tiene establecido un plan de contingencia y continuidad para responder a posibles incidentes.
- La plataforma de programación Visual Basic 6 y MS SQLServer 2008 no cuentan con soporte, y el grado de obsolescencia de estas herramientas ponen en riesgo la información gestionada debido a aspectos de seguridad que no fueron resueltos por Microsoft y actualmente ya no son compatibles con sistemas operativos actuales.

5.3.2. Sistema SISCOCA - MODULO DE PRODUCCIÓN

La Dirección General de Desarrollo Integral de las Regiones Productoras de Coca (DIGPROCOCA) cuenta con un sistema denominado SISCOCA - MODULO DE PRODUCCIÓN, su arquitectura corresponde a una aplicación de WEB, desarrollado en lenguaje de programación PHP implementando el framework de programación CodeIgniter como Back-End y la Librería VUE.js como herramienta Front-End con una base de datos SQL PostgreSQL 9.3, ver gráfico 7.

Gráfico 7: Arquitectura del sistema SISCOCA-MODULO DE PRODUCCIÓN - DIGPROCOCA



De acuerdo a la arquitectura presentada por el sistema, se pudo identificar lo siguiente:

- Se define un servidor virtual WEB en el cual se publica la aplicación SISCOCA- MODULO DE PRODUCCIÓN y la base de datos Postgres 9.3.
- El acceso a la base de datos es a través de aplicaciones WEB accesible internamente a través de un explorador, accesible desde el exterior a través del internet.
- Se identifica que el servidor tiene instalado un sistema operativo Ubuntu, que implementa el motor de la base de datos y la aplicación.

Aspectos identificados sobre el sistema SISCOCA- MODULO DE PRODUCCIÓN respeto a la seguridad y sus funcionalidades más importantes:

- El sistema SISCOCA- MODULO DE PRODUCCIÓN establece una funcionalidad para la autenticación de usuarios el cual permite verificar los accesos al sistema
- El sistema SISCOCA- MODULO DE PRODUCCIÓN establece funcionalidad para la gestión de usuarios, esta funcionalidad está a cargo del responsable técnico de DIGPROCOCA - UDESY, quien tiene la labor de adicionar, modificar o inactivar usuarios, de la revisión de usuarios se pudo identificar que solo los usuarios en función se encuentran activos.
- El sistema SISCOCA- MODULO DE PRODUCCIÓN no define logs de auditoría que establezca una la trazabilidad de las operaciones realizadas por los usuarios.
- La carnetización de productores cuenta con un módulo de registro en el SISCOCA- MODULO DE PRODUCCIÓN; sin embargo, el proceso de emisión de carnets es efectuado a través de un proceso manual complementario; donde, el responsable técnico una vez registrado en el sistema efectúa una copia de los registros de comercializador en planillas Excel y esta es vinculada con el dispositivo de impresión, por lo que la emisión del carnet no es realizada por el sistema.
- Los carnets de comercialización cuentan con códigos QR que contiene la información del productor.
- La impresión de carnets no establece controles de la cantidad de impresiones o reimpresiones realizadas.
- No toda la información de productores se encuentra registrada en el sistema de MODULO DE PRODUCCIÓN, solo los productores con catastro están en la base de datos, el resto de productores de zonas originarias ancestrales se encuentran en planillas Excel
- No se implementa una interoperabilidad entre las las bases de datos de productores de los Yungas con productores del Trópico de Cochabamba, por lo que las labores de validación de superficies, existencia, duplicidad de catos por un productor en ambas regiones son realizadas manualmente.
- No se tiene en producción un sistema GIS que permita inventariar los cultivos de hoja de coca, superficies para cada productor, los cuales estén relacionados con los registros de productores.

Otros aspectos de la gestión de la información y su aseguramiento:

- No se define políticas formales de respaldo para el sistema SISCOCA- MODULO DE PRODUCCIÓN, los respaldos efectuados no son programados y no tienen un procedimiento que defina la periodicidad y el tipo de respaldo en función a un RTO y RPO basado en un análisis de riesgo.
- El código fuente de SISCOCA- MODULO DE PRODUCCIÓN para el front-end esta ofuscado para la versión en producción, por lo que la restauración de los códigos fuente no es posible; ello evidencia que, no se definen políticas de resguardo de código fuente.
- No se puedo evidenciar una documentación técnica del sistema SISCOCA- MODULO DE PRODUCCIÓN que permita orientar sobre la estructura de bases de datos, objetos, y arquitectura; para efectuar un entendimiento adecuado y propiciar un mantenimiento o actualización.
- La base de datos del SISCOCA- MODULO DE PRODUCCIÓN se encuentra instalado en un servidor; asimismo, se cuenta con réplica del mismo en servidores virtuales; sin embargo, no se tiene establecido un plan de contingencia y continuidad para responder a posibles incidentes de perdida de operaciones.

5.4. Diagnóstico de la Seguridad informática y seguridad de la información, relacionados con el SISCOCA

Del análisis de situación realizado sobre el sistema SISCOCA – MODULO DE PRODUCCIÓN de DIGPROCOCA y SISCOCA-SAR de DIGCOIN relacionados a aspectos de seguridad informática y seguridad de la información pudimos identificar los siguientes hallazgos.

- No se pudo identificar que el Viceministerio haya definido políticas y procedimientos formales relacionados con la seguridad informática y seguridad de la información vinculado al Lineamientos para la elaboración e Implementación de Planes Institucionales de Seguridad de la Información de las entidades del Sector Público (PISI) emitidos por AGETIC (CTIC, 2017)
- No se tiene identificado un esquema de respaldos formalmente implementado que responda a niveles adecuados de RTO y RPO, por lo que los respaldos efectuados no son programados o gestionados de forma organizada.
- La gestión de usuarios no establece protocolos de seguridad.
- No se define un ambiente de seguridad física y perimetral de los principales recursos de TIC.
- Los equipos de comunicaciones y computo (Servidores) no cuentan con programas de mantenimiento preventivo para asegurar un adecuado funcionamiento de los mismos.
- No se han trabajado aspectos de contingencia tecnológica (DRP) o continuidad de las operaciones institucionales del VCDI.
- No se gestionan los incidentes de seguridad relacionados a la perdida de información o servicios referidos al SISCOCA.
- Los códigos fuente de los sistemas no fueron controlados por lo que no se tiene códigos fuente para efectuar el mantenimiento del SISCOCA.
- No se establecen políticas de control de cambios relacionados con bases de datos de SISCOCA.
- No se tiene el control de accesos privilegiados (personal de sistemas, o administradores de sistemas).
- El esquema de seguridad de comunicaciones no establece políticas de ciberseguridad por lo que proyectos de sistemas relacionados con el internet son de alto riesgo en relación a la perdida de la información por Ciberrobo.
- No se establecen una política de licenciamiento (Ofimática y SO).
- No se tiene implementado software especializado para evitar Malware y virus, por lo que la perdida de información es de alto riesgo.

Los aspectos identificados son los de mayor riesgo relacionados con la seguridad de la información del activo de información SISCOCA.

5.5. Análisis de riesgos del SISCOCA

Del diagnóstico contextual realizado sobre el estado de situación del sistema SISCOCA para DIGCPROCOCA y DIGCOIN, se han logrado un entendimiento sobre los principales aspectos relacionados con la organización de la administración de TI, la infraestructura que soporta el funcionamiento y las operaciones del sistema, las políticas de seguridad de la información e informática.

Con este contexto se efectúa un análisis de riesgo, el cual permitirá identificar los principales aspectos que deben ser abordados e implementados para mitigar los riesgos sobre el sistema SISCOCA -SAR y SISCOCA-MODULO DE PRODUCCIÓN, es así que el análisis efectuado, se realiza en función a una metodología descrita en el anexo 4 del presente documento.

5.5.1. Identificación de amenazas y vulnerabilidades

Para efectuar un análisis y evaluación de los riesgos es preciso determinar que amenazas[1] podrían afectar las operaciones de los sistemas SISCOCA-SAR y SISCOCA-MODULO DE PRODUCCIÓN; de la misma manera, se debe determinar las vulnerabilidades[2] que podrían ser explotadas para dañar o afectar los sistemas en evaluación. La tabla 2 es el inventario de amenazas que podrían afectar las operaciones de los sistemas, dichas amenazas fueron identificadas en función al contexto IDENTIFICADO, respecto de los principales hallazgos del diagnóstico de situación, .

Tabla 2: Inventarios de amenazas

Amenaza	Descripción
Ataque malicioso	Un hackeo u otro ataque lógico a los sistemas por parte de actores maliciosos
Credenciales comprometidas	Las credenciales se ponen a disposición de partes no autorizadas, lo que les permite la capacidad de hacerse pasar por un usuario específico.
Amenaza interna	Un actor malicioso que los usuarios facilitan obstinadamente el acceso a los sistemas y datos con fines maliciosos a través de subterfugios.
Error de administrador	Errores cometidos por los administradores del sistema que dan lugar a configuraciones erróneas o impactos en la calidad de los datos.
Desastre natural	Un evento de fuerza mayor como terremoto, inundaciones, etc.
Extracción	La copia o eliminación deliberada de datos con el fin de divulgarlos a otras partes.
Error de desarrollador	Errores cometidos por los desarrolladores que resultan en errores o vulnerabilidades en los sistemas.
Software no compatible	El riesgo de que el software se vuelva obsoleto, lo que significa que las vulnerabilidades de seguridad no se pueden parchear y los errores de software no se pueden resolver.
Acceso físico	El riesgo de que un usuario no autorizado tenga acceso físico a un sistema, lo que permite que sea atacado.
Malware	Código o software malicioso que destruye datos o sistemas, roba información, cifra datos haciéndolos indisponibles o que de otra manera causa malaperación de los sistemas que afecta su disponibilidad.
Personal indisponible	Personal indispuesto, ya sea por ausencia, enfermedad o cese de su situación laboral.
Equipo defectuoso	Activos de información informáticos que no cuentan con soporte o mantenimiento preventivo.
Monitoreo inadecuado	El monitoreo a las operaciones con deficiencia o insuficiente, no se definen registros de monitoreo sobre las operaciones de los usuarios y sistemas.
Aspectos sociales y políticos	Que el país afronte convulsiones, actos de terrorismo, pandemia, paros y bloqueos
Legislación	Cambios legislativos in normativos de estado podrían cambias el modelo de gestión o controles establecidos.

[1] Amenaza: causa potencial de un incidente no deseado, que puede resultar en daño a un sistema u organización (3.50)
[2] Vulnerabilidad: debilidad de un activo o control (3.14 ISO 27001) que puede ser explotada por una o más amenazas

La table 3, corresponde al inventario de posibles vulnerabilidades que podrían ser explotados para materializar las amenazas.

Tabla 3: Inventario de Vulnerabilidades

Vulnerabilidades	Descripción
Plataforma insegura	Plataformas que contienen vulnerabilidades que pueden ser explotadas para obtener acceso o amenazar la disponibilidad
Usuario	Los usuarios son fuentes potenciales de error, malversación y negligencia
Actor malicioso	Los actores malintencionados han utilizado subterfugios para llevar a cabo la malversación.
Diseño del sistema	El diseño de mala calidad introduce un riesgo para la disponibilidad de los sistemas y, potencialmente, para la calidad de los datos a través de errores.
Incumplimiento	El error o las acciones deliberadas de los usuarios para no seguir correctamente un proceso especificado
Gestión inadecuada de recursos	un fallo del proceso o la falta de disponibilidad de recursos para realizar las funciones de seguridad necesarias
Equipos	Equipos son sistemas operativos incompatibles y sin soporte, equipos obsoletos, equipos sin paches de seguridad, equipos defectuosos.
Continuidad y contingencia	Gestión inadecuada de las contingencias o bien inexistencia de procesos de continuidad y contingencia

NOTA: para fines del análisis y evaluación de los riesgos se han aplicado solo las amenazas (Tabla 2) y vulnerabilidades (Tabla 3) marcados como aplicados.

5.5.2. Identificación y evaluación de los riesgos

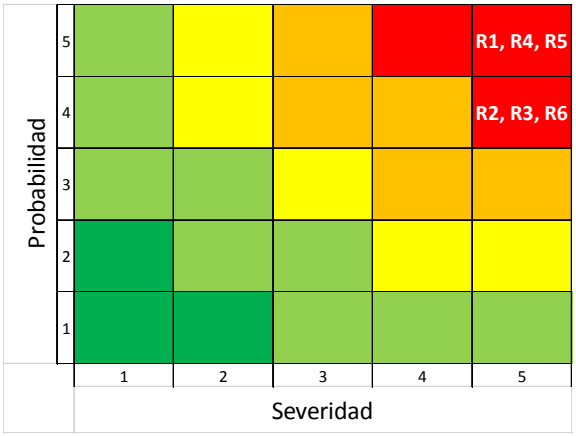
Para efectuar la identificación y evaluación de los riesgos, lo primero que se hizo fue la identificación de los activos a ser evaluados, en este caso son dos sistemas de información SISCOCA-SAR y SISCOCA-MODULO DE PRODUCCIÓN, la evaluación de los riesgos es detallados en el Anexo 5: Análisis de riesgo SISCOCA-SAR, y Anexo 6: Análisis de riesgo SISCOCA-MODULO DE PRODUCCIÓN., al respecto se pudieron identificar los siguientes riesgos para SISCOCA-SAR (el análisis solo tomo en cuenta los riesgos más significativos):

Tabla 4: Riesgos SISCOCA-SAR

ID RIESGO	DESCRIPTION OF THE RISK (DESCRIPCIÓN DEL RIESGO)
R1	Perdida e indisponibilidad de servicio
R2	Acceso indebido y perdida de información
R3	Software de base de datos y lenguaje de desarrollo obsoletos
R4	Falsificación de Hojas de ruta / Falsificación de Credenciales de comercialización / inadecuado monitoreo de las operaciones de los usuarios
R5	Interrupción de operaciones
R6	Proceso de cambios en el sistema SISCOCA indisponible.

De los riesgos identificados (Tabla 4), el mapeo (Gráfico 8) expone que todos los riesgos identificados son críticos, cuya probabilidad de ocurrencia es alta, y el impacto o la severidad proyectada es alta, por lo que su tratamiento es prioritario.

Gráfico 8: Mapeo de riesgos del SISCOCA-SAR



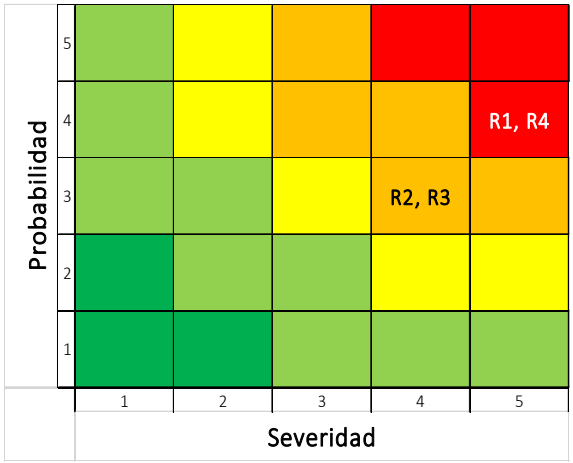
De la misma manera los riesgos asociados al sistema SISCOCA-MODULO DE PRODUCCIÓN son expuestos en la tabla 5, este detalle fue identificado en función a la priorización de los riesgos más significativos.

Tabla 5: Riesgos SISCOCA-MODULO DE PRODUCCIÓN

ID RIESGO	DESCRIPTION OF THE RISK (DESCRIPCIÓN DEL RIESGO)
R1	Perdida e indisponibilidad de servicio
R2	Posible acceso indebido, credenciales de productores falsificados o reimpresos sin control
R3	Interrupción de operaciones
R4	Proceso de cambios en el sistema SISCOCA -MODULO DE PRODUCCIÓN indisponible.

El gráfico 9 referido al mapeo de los riesgos identificados, define que 2 de los riesgos R1 y R4 son de alta prioridad en su tratamiento, debido a que su probabilidad y severidad son altamente críticos, los detalles del análisis efectuado se encuentran identificados en el anexo 6.

Gráfico 9: Mapeo de los riesgos del SISCOCA-MODULO DE PRODUCCIÓN



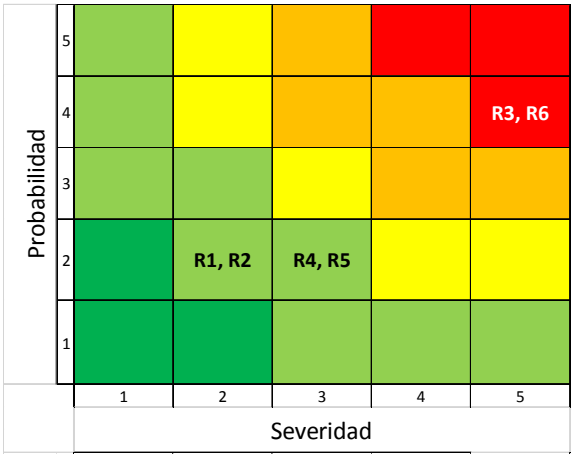
5.5.3. Tratamiento de los riesgos asociados al SISCOCA

El proceso de tratamiento de riesgos[3] implica principalmente en mitigar los riesgos en función a la aplicación de controles (en nuestro ejercicio se aplicó como referencia la NB ISO/IEC 27001 y NB ISO/IEC 27002); a los cuales se han asociado acciones que van desde la definición de tareas preventivas, creación de políticas y procedimientos necesarios.

Como resultado del tratamiento de los riesgos (Anexo 7) se tiene los riesgos residuales[4] que corresponde al remanente de los riesgos luego de su mitigación o su aceptación.

El gráfico 10, expone que los riesgos R1, R2, R4 y R5 luego del tratamiento realizado, podrían disminuir su probabilidad y severidad, debido a que es posible su mitigación; por otro lado, los riesgos R3 y R6 no puede ser objeto de mitigación debido a que R3 corresponde al riesgo relacionado con la plataforma implementada actualmente que contiene un grado de obsolescencia alto y la actualización del mismo implica la creación de un nuevo sistema y R6 está relacionado con la implementación del código fuente para efectos de mantenimiento del sistema SISCOCA -SAR; por ello, es que ambos riesgo seguirán coexistiendo, por lo que tanto DIGPROCOCA y DIGCOIN deben de mantener la plataforma en operaciones hasta resolver estos aspectos.

Gráfico 10: Mapeo de riesgos residuales del SISCOCA-SAR



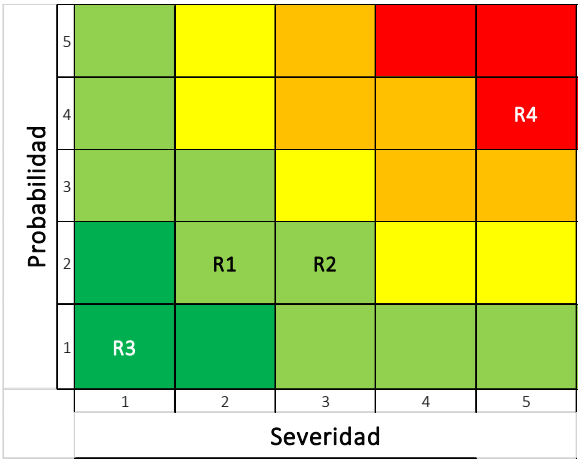
Por otor lado, el grafico 11 expone los riesgos del sistema SISCOCA-MODULO DE PRODUCCIÓN, luego de su tratamiento, podemos identificar que los riesgos R1, R2 y R3 pueden ser mitigados con las acciones y controles de definidos; sin embargo, el riesgo R4 que está relacionado con los códigos fuente no puede ser mitigado por el momento, debido a que implica que no es posible su modificación debido a que el

[3] Tratamiento de riesgos: proceso para modificar el riesgo. El tratamiento del riesgo puede implicar:
— evitar el riesgo decidiendo no iniciar o continuar con la actividad que genera el riesgo;
— asumir o aumentar el riesgo para aprovechar una oportunidad;
— eliminar la fuente de riesgo;
— cambiar la probabilidad;
— cambiar las consecuencias;
— compartir el riesgo con otra parte o partes (incluidos los contratos y la financiación del riesgo);
— retener el riesgo mediante una elección informada.

[4] Riesgo residual: riesgo (3.61) remanente después del tratamiento del riesgo (3.72)

front-ent se encuentra ofuscado por lo que su mantenimiento no es posible, ni se cuenta con documentación técnica para un adecuado entendimiento.

Gráfico 11: Mapeo de riesgos residuales del SISCOCA-MODULO DE PRODUCCIÓN



5.6. Priorizaciones y desarrollos

De los riesgos identificados para SISCOCA-SAR y el análisis efectuado se pudo identificar que el riesgo R8 asociado al sistema, implica efectuar ajustes al sistema como se puede identificar en la tabla 6, mediante el cual se ha priorizado la realización de desarrollos complementarios:

Tabla 6: Riesgo relacionado a las funcionalidades de SISCOCA-SAR

ID RIESGO	Descripción del riesgo	Risks drivers/causes (Impulsores/causas del riesgo)
R4	Falsificación de Hojas de ruta / Falsificación de Credenciales de comercialización / inadecuado monitoreo de las operaciones de los usuarios	R4.1. Los carnets de comercialización cuentan con códigos de barra y QR pero los mismos no almacenan datos relevantes, por lo que es posible que los mismos sean objeto de falsificación. R4.2. La impresión de carnets no cuenta con controles como contadores de impresión o reimpresión y captura de usuarios, el mismo es efectuado a través de procesamiento manual. R4.3. La emisión de hojas de ruta no cuenta con logs de auditoría, controles de impresión o reimpresión, fechas y usuarios. R4.4. Las hojas de ruta no están digitalizadas en el sistema para un adecuado resguardo y control histórico de cumplimiento de ruta. R4.5. Las hojas de ruta cuentan con un código de barra que identifica el número secuencial que es almacenado en el sistema, dicho código no puede ser contrastado en puntos de control con la base de datos, no establece controles adecuados de seguridad para verificar su autenticidad contra la base de datos, esto significa que una hoja de ruta podría ser objeto de clonación, ya que los controles en los puestos no son efectuados o contrastados digitalmente. R4.6. No se cuenta con controles automatizados que permita la verificación digital de las hojas de ruta y los carnets en los puestos de control, el control se basa principalmente en el paso físico de cada hoja de ruta por punto de control y el sello respectivo.

ID RIESGO	Descripción del riesgo	Risks drivers/causes (Impulsores/causas del riesgo)
		R4.7. El control de hojas de ruta sobre el cumplimiento de la ruta es efectuado manualmente por personal encargado de la emisión de las hojas de ruta, cualquier incumplimiento es verificado manualmente sin el apoyo del sistema SISCOCA-SAR, respecto a la trazabilidad de cada hoja de ruta. R4.8. Cambios en bases de datos para parámetros de precios, no cuentan con funcionalidades de mantenimiento.

Los impulsores del riesgo R8 han generado la priorización de desarrollos complementarios que mitigan los riesgos asociados con las funcionalidades implementadas en SISCOCA-SAR, la table 7 asocia las priorizaciones y los impulsores del riesgo.

Tabla 7: Inventario de desarrollos priorizados para SISCOCA-SAR

Desarrollo y mantenimiento del SISCOCA - Módulo de Comercialización - DIGCOIN		PRODUCTOS	NOTAS	Impulsores asociados según el riesgo R8
5	Desarrollo y mejora del submódulo de hoja de ruta, en cuanto a la seguridad relacionada con los controles de trazabilidad con los puestos de control	- Complementación de un módulo de seguridad y control de la trazabilidad de las hojas de ruta.	- El módulo deberá realizar la lectura del código del comercializador en los puntos de control y recuperar los datos de la hoja de ruta en tránsito y validar contra la base de datos. - Se crearán tablas complementarias para los datos geográficos de cada punto de control, para ser utilizados por la aplicación móvil.	R4.3
6	Digitalización de la hoja de ruta cuando este concluya su recorrido y sea cargado al sistema	- Funcionalidad para digitalizar la hoja de ruta de comercialización, cuando los productores soliciten su siguiente cupo (Escaneado en PDF)	- El sistema debe permitir registrar la hoja de ruta digitalizada (PDF)	R4.4
7	Implementar el funcionamiento de los controles de trazabilidad en los Puestos de Control	- Desarrollo de una aplicación móvil para registrar las hojas de ruta en línea desde los puestos de control.	- La aplicación deberá registrar centralmente las lecturas realizadas en los puestos de control. - las lecturas realizadas en puestos de control por la aplicación debe ser validado contra el polígono parametrizado en el servidor, no debe permitir registro si esta fuera de cualquier polígono de puesto de control.	R4.5, R4.6 y R4.7
8	Apoyar a la Unidad de Sistemas en la identificación e implementación y aplicación de medidas	- Reporte de hojas de ruta que no cumplieron con su tura. - Desarrollo del Back-end	- Contiene funcionalidades y tablas complementarias en la base de datos	R4.5, R4.6 y R4.7

Desarrollo y mantenimiento del SISCOCA - Módulo de Comercialización - DIGCOIN		PRODUCTOS	NOTAS	Impulsores asociados según el riesgo R8
	de seguridad a las hojas de ruta			
9	Desarrollar mejoras en el funcionamiento del sub-módulo de carnetización y automatización de impresión de los carnets de productores	- Desarrollo de un módulo complementario de carnetización.	- El módulo de carnetización deberá permitir la impresión del carnet de comercializador.	R4.1 y R4.2
10	Validación de los ajustes y modificaciones evidenciadas en el desarrollo de la misión	- Modulo complementario para la actualización de precios.	- Se contará con una interface que permita actualizar los precios.	R4.8

De los riesgos identificados para SISCOCA-MODULO DE PRODUCCIÓN y el análisis efectuado se pudo identificar que el riesgo R2 asociado al sistema, implica efectuar ajustes al sistema como se puede identificar en la tabla 7, mediante el cual se ha priorizado la realización de desarrollos complementarios:

Tabla 8: Riesgo relacionado a las funcionalidades de SISCOCA-MODULO DE PRODUCCIÓN

ID RIESGO	Descripción del riesgo	Risks drivers/causes (Impulsores/causas del riesgo)
R2	Posible acceso indebido, credenciales de productores falsificados o reimpresos sin control	*R2.1. El sistema SISCOCA- MODULO DE PRODUCCIÓN no define logs de auditoría que establezca una la trazabilidad de las operaciones realizadas por los usuarios.* R2.2. La carnetización de productores cuenta con un módulo de registro en el SISCOCA-MODULO DE PRODUCCIÓN; sin embargo, el proceso de emisión de carnets es efectuado a través de un proceso manual complementario; donde, el responsable técnico una vez registrado en el sistema efectúa una copia de los registros de comercializador en planillas Excel y esta es vinculada con el dispositivo de impresión, por lo que la emisión del carnet no es realizada por el sistema. *R2.3. Los carnets de comercialización cuentan con códigos QR que contiene la información del productor; sin embargo, no pueden ser validados contra la base de datos del sistema.* R2.4. La impresión de carnets no establece controles de la cantidad de impresiones o reimpresiones realizadas. R2.5. No toda la información de productores se encuentra registrada en el sistema de MODULO DE PRODUCCIÓN, solo los productores con catastro están en la base de datos, el resto de productores de zonas originarias ancestrales se encuentran en planillas Excel *R2.6. No se implementa una interoperabilidad entre las las bases de datos de productores de los Yungas con productores del Trópico de Cochabamba, por lo que las labores de validación de superficies, existencia, publicidad de catos por un productor en ambas regiones son realizadas manualmente.*

ID RIESGO	Descripción del riesgo	Risks drivers/causes (Impulsores/causas del riesgo)
		R2.7. *No se tiene en producción un sistema GIS que permita inventariar los cultivos de hoja de coca, superficies para cada productor, los cuales estén relacionados con los registros de productores.* R2.8. Errores de programación en el despliegue de registros de trámites administrativos.

Los impulsores del riesgo R2 han generado la priorización de desarrollos complementarios que mitigan los riesgos asociados con las funcionalidades implementadas en SISCOCA-MODULO DE PRODUCCIÓN, la tabla 9 asocia las priorizaciones y los impulsores del riesgo.

Tabla 9: Inventario de desarrollos priorizados para SISCOCA-MODULO DE PRODUCCIÓN

Desarrollo y mantenimiento del SISCOCA - Módulo de Producción - DIGPROCOCA		**PRODUCTOS**	**NOTAS**	**Impulsores asociados según el riesgo R2**
1	Mejora y automatización de la emisión del carnet de Productor	- Modulo de registro e impresión de carnet de productor	Debe permitir imprimir directamente desde la aplicación a la impresora de carnetización.	R2.2, R2.4
2	Proceso de migración de datos históricos a la base de datos principal (Registro de productores históricos)	- Migración de registros históricos productores Originario ancestral con registro catastro - **convenio 2008** (según planilla excel) - Módulo de registro productores Originario ancestral con registro catastro	No implica carnetización / Solo debe realizar registro y consulta.	R.2.5
3	Modificaciones al módulo de Producción Generación de Reportes en materia de seguimiento de trámites administrativos, seguimiento y control al registro de productores, por categoría y tipos de municipio	- Registro de productores por zona de producción (originaria ancestral, originario ancestral con registro catastro -2008, registro castro)	- La interface debe visualizar el ultimo registro de productor e incluir un botón de despliegue de los (propietarios del predio) registros históricos. - El reporte definido para esta sección debe desplegar al último propietario del predio.	R2.5
4	Validar ajustes realizados al registro y trámites de productores	- Generación de reportes incluir código de productor - Trámites administrativos (validar duplicidad, validar que cuando se derive debe desaparecer de la mesa de entrada actual)	- Los trámites administrativos, no deben duplicarse en la bandeja de entrada o creación. - No puede haber dos tramites de solicitud de un mismo registro.	R2.8

6. CONCLUSIONES

Del diagnóstico realizado sobre el estado de situación del sistema SISCOCA, contempla las siguientes conclusiones:

Sistema SISCOCA-MODULO DE PRODUCCIÓN – DIGPROCOCA - UDESY:

- DIGPROCOCA, no cuenta con un área de sistemas, este es apoyado por el área de sistemas del VCDI por lo que el ambiente de TI implementado soporta los principales activos de información como el sistema SISCOCA-MODULO DE PRODUCCIÓN; la administración del área de sistemas está a cargo de un responsable de sistemas quien se ocupa de otorgar soporte a los requerimientos de TI.
- La infraestructura define un esquema de comunicaciones y redes de complejidad baja, se implementa una configuración de red segmentada y enmascarada, no se define un perímetro de seguridad como un firewall que permita un aseguramiento ante posibles intentos de intrusión externo o interno, intentos de hackeo y robo de información, cuenta con 3 equipos servidor de los cuales solo uno está en funcionamiento y en operaciones, dicho servidor esta virtualizado y contiene 7 servidores virtuales (aplicaciones, web, DNS, base de datos, Geoserver, servidor de pruebas app, y servidor de pruebas de base de datos), los servidores no cuentan con protección de malware o virus adecuados, por lo que se identifica como un entorno inseguro.
- La organización y emplazamiento de los equipos de cómputo y comunicaciones están instalados en un rack el cual no cuenta con una organización adecuada, el área asignada a los equipos críticos de comunicaciones y servidores no está diferenciado con el área de trabajo de TI; asimismo, dicha área sirve de almacenamiento para paquetes, cables y material en desuso, los equipos en general están cubiertos de polvo, no se identifica una seguridad física adecuada.
- El sistema SISCOCA-MODULO DE PRODUCCIÓN, es una aplicación WEB implementada en un servidor virtual del VCDI, dicha aplicación es operada por personal de DIGPROCOCA para el registro de productores, y trámites administrativos, de acuerdo al análisis de riesgos realizado sobre el sistema SISCOCA-MODULO DE PRODUCCIÓN se pudo identificar que existen aspectos que deben ser resueltos de forma prioritaria, se identificaron riesgos de: Perdida e indisponibilidad de servicio por posibles riesgos de seguridad física en CPD y ausencia de perímetros de seguridad adecuados, posible acceso indebido debido a una gestión de credenciales sin políticas y procedimientos formales, posibles riesgos de credenciales de productores falsificados o reimpresos sin control, Interrupción de operaciones, y proceso de cambios o mantenimiento en el sistema SISCOCA-MODULO DE PRODUCCIÓN indisponible debido a que una parte del código fuente esta ofuscado. Asimismo, como medidas de mitigación de los riesgos y en concordancia con los términos de referencia y los tiempos establecidos para realizar labores de desarrollo se efectuó la priorización de desarrollos definido en la table 6 y tabla 7 del documento.
- Aún se identifica labores que deben ser realizadas como, por ejemplo: Logs de auditoría que establezca una la trazabilidad de las operaciones realizadas por los usuarios, Datos de los carnets de comercialización con aspectos de seguridad relacionados con controles digitales en tiempo real, No se tiene interoperabilidad entre las bases de datos de productores de los Yungas (UDESY) con productores del Trópico de Cochabamba (UDESTRO) para efectos de emisión de reportes de control, un sistema operativo GIS que permita inventariar los cultivos de hoja de coca, superficies para cada productor, los cuales estén relacionados con los registros de productores.

Sistema SISCOCA-SAR - DIGCOIN:

- DIGCOIN, cuenta con un responsable del sistema que administra el sistema SISCOCA-SAR; asimismo, aspectos operativos de infraestructura, es apoyado por personal del VCDI.
- La infraestructura que soporta los sistemas informáticos de DIGCOIN, cuenta con un esquema de comunicaciones y redes de complejidad baja, se implementa una configuración de red simple y controlada por un Proxy Server, cuenta con un servidor donde se implementa el sistema SISCOCA-SAR, dicho servidor es el único recurso en operaciones, por lo que existen riesgos de perdida de información o indisponibilidad del sistema, que podrían generar la suspensión de las operaciones con efecto en la suspensión de servicios al público.
- La organización y emplazamiento de los equipos de cómputo y comunicaciones están instalados en un rack el cual no cuenta con una organización adecuada, el área asignada a los equipos críticos de comunicaciones y servidores se encuentra diferenciada de las demás áreas; sin embargo, dicha área sirve de almacén de paquetes, cables y material en desuso, documentación en bolsas; los equipos en general están cubiertos de polvo, no se identifica una seguridad física ambiental adecuada.; ello significa, que podría surgir incidentes respecto a la continuidad de los servicios y las comunicaciones.
- El esquema de seguridad implementado contempla un equipo PROXY server, no se define un perímetro de seguridad como un firewall para un aseguramiento ante posibles intentos de intrusión externo o interno, intentos de hackeo y robo de información.
- El sistema SISCOCA-SAR, es una aplicación cliente-servidor, administrada por un responsable de sistemas, de acuerdo al análisis de riesgos realizado sobre el sistema SISCOCA-SAR se pudo identificar que existen aspectos que deben ser resueltos de forma prioritaria, se identificaron riesgos de: Perdida e indisponibilidad de servicio por posibles riesgos de seguridad física en CPD que soporta al servidor en producción, posible acceso indebido debido a una gestión de credenciales sin políticas y procedimientos formales, riesgos en la emisión de credenciales de comercializadores que podrían verse afectados por falsificación, o reimpresos sin control; Interrupción de operaciones, y proceso de cambios o mantenimiento en el sistema SISCOCA-SAR indisponible debido a que el código fuente no corresponde a la última versión en producción; asimismo, se identifica un riesgo relacionado al grado de obsolescencia de la plataforma del SISCOCA-SAR debido a que no cuenta con soporte y es incompatible con el proveedor. Asimismo, como medidas de mitigación de los riesgos y en concordancia con los términos de referencia y los tiempos establecidos para realizar labores de desarrollo se realiza la validación y priorización un inventario de acciones definido en la table 4 y tabla 5 del documento.
- Aún se identifica labores que deben ser realizados como, por ejemplo: Logs de auditoría que establezca una la trazabilidad de las operaciones realizadas por los usuarios, Datos de los carnets de comercialización con aspectos de seguridad relacionados con controles digitales en tiempo real, no se tiene interoperabilidad entre las bases de datos de productores de los Yungas (UDESY) con productores del Trópico de Cochabamba (UDESTRO) para efectos de emisión de reportes de control cruzado, un sistema operativo GIS que permita inventariar los cultivos de hoja de coca, superficies para cada productor, los cuales estén relacionados con los registros de productores.

7. RECOMENDACIONES

Del diagnóstico realizado sobre el estado de situación del sistema SISCOCA, se identifican las siguientes acciones que el VCDI, DIGPROCOCA y DIGCOIN deben implementar en el corto plazo:

- Con una visión a futuro y de renovación tecnológica del Viceministerio de Coca y Desarrollo Integral, debe establecer un programa de modernización digital que tome en cuenta los siguientes aspectos o componentes:

  - **Infraestructura**: a través de un proyecto técnico, efectuar la renovación, ordenamiento y aseguramiento del equipamiento principalmente de comunicaciones (Firewall, switchs, reorganización del cableado, aseguramiento de los servicios por Wifi, otros); asimismo, se debe definir un esquema de seguridad integral entre el VCDI, DIGPROCOCA, DIGCOIN para lograr una integración a través de una red única y privada, que configure una estructura informática que responda adecuadamente ante cualquier incidente de seguridad y ciberseguridad, y que defina un ambiente de TI Seguro para los servicios y sistemas de información.
  - **Sistemas SISCOCA-SAR:** de los riesgos identificados al SISCOCA-SAR, es preciso renovar el sistema e integrar los desarrollos realizados en el marco de la actual misión, debido a que el mismo se apoya en una plataforma obsoleta y sin el soporte requerido, el código fuente no cuenta con la integridad suficiente, ni se cuenta con documentación técnica.
  - **Sistemas SISCOCA-MODULO DE PRODUCCIÓN:** de los riesgos identificados al SISCOCA-CIICATCOCA, es preciso renovar el sistema, debido a que el mismo no define un esquema de seguridad adecuado, el código fuente no cuenta con la integridad suficiente ya que parte esta ofuscado, ni se cuenta con documentación técnica.
  - **Seguridad de la información**: en el marco de los lineamientos para la implementación de Planes Institucionales de Seguridad de la Información de las entidades del Sector Público (PISI) emitidos por AGETIC (CTIC, 2017), es preciso tomar en cuenta este aspecto, debido a que los riesgos identificados deben ser mitigados para otorgarle un adecuado aseguramiento al activo de información más importante de DIGCOIN y UDESY como la información procesada por el sistema SISCOCA-SAR y SISCOCA-CIICATCOCA, esta labor debe ser realizada con el fin de reducir los riesgos e incidentes que podrían afectar la seguridad de la información y propiciar un escenario de resiliencia ante la materialización de los riesgos y propiciar respuestas oportunas para proteger los activos de información del VCDI. Por ello, se debe llevar adelante el PISI para implementar los controles de resguardo del SISCOCA-SAR y SISCOCA-MODULO DE PRODUCCIÓN.
  - **Organización de la función de sistemas**: Con base a el análisis preliminar de la organización de sistemas en el VCDI, DIGPROCOCA y DIGCOIN, es preciso formalizar un organigrama, manual de cargos y funciones, un manual de funciones para una adecuada definición del alcance que debe la función de sistemas en VCDI, DIGPROCOCA y DIGCOIN.

- Para llevar adelante el punto anterior y con el fin de otorgar sostenibilidad de los esfuerzos, inicialmente se deberá definir una ruta crítica tomando en cuenta los riesgos inherentes al sector y que defina las principales prioridades para lograr un avance tecnológico por fases. Posteriormente se deberá diseñar un plan integral de implementación en función a las prioridades definidas por la ruta crítica, para ello es preciso asegurar los recursos financieros y técnicos.

8. BIBLIOGRÁFIA

CTIC. (2017). *Lineamientos para la elaboración e Implementación de Planes Institucionales de Seguridad de la Información de las entidades del Sector Público.* La Paz: CTIC - AGETIC.

Normalización, I. -O. (2018). *Online Browsing Platform (OBP) - ISO/IEC 27000:2018(es)*. Obtenido de https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:fr

Tierras, M. d. (2021). *Manual de Organización y Funciones 2021.* La Paz.

ANEXOS

Anexo 1: Personas de Trabajo y Contactadas

NOMBRE	CARGO	TELÉFONO	CORREO ELECTRÓNICO O TELÉFONO
VICEMINISTERIO DE COCA Y DESARROLLO INTEGRAL - VCDI			
Carlos Perez	Encargado de Sistemas VCDI	70129636	Carlos.perez@ruralytierras.gob.bo
DIRECCIÓN GENERAL DE DESARROLLO INTEGRAL DE LAS REGIONES PRODUCTORAS DE COCA - DIGPROCOCA			
Gonzalo Poma	Técnico UDESY	68121105	Gonzalo.poma@ruralytierras.gob.bo
DIRECCIÓN GENERAL DE LA HOJA DE COCA E INDUSTRIALIZACIÓN - DIGCOIN			
Roque Guarachi	Encargado de sistemas	69802332	roqueh31@gmail.com
CONSULTOR DITISA			
Oscar Martinez	Consultor	71505112	osmartinez@gmail.com
Carlos Machicado	Consultor	69984850	carlos.alberto.machicado@gmail.com

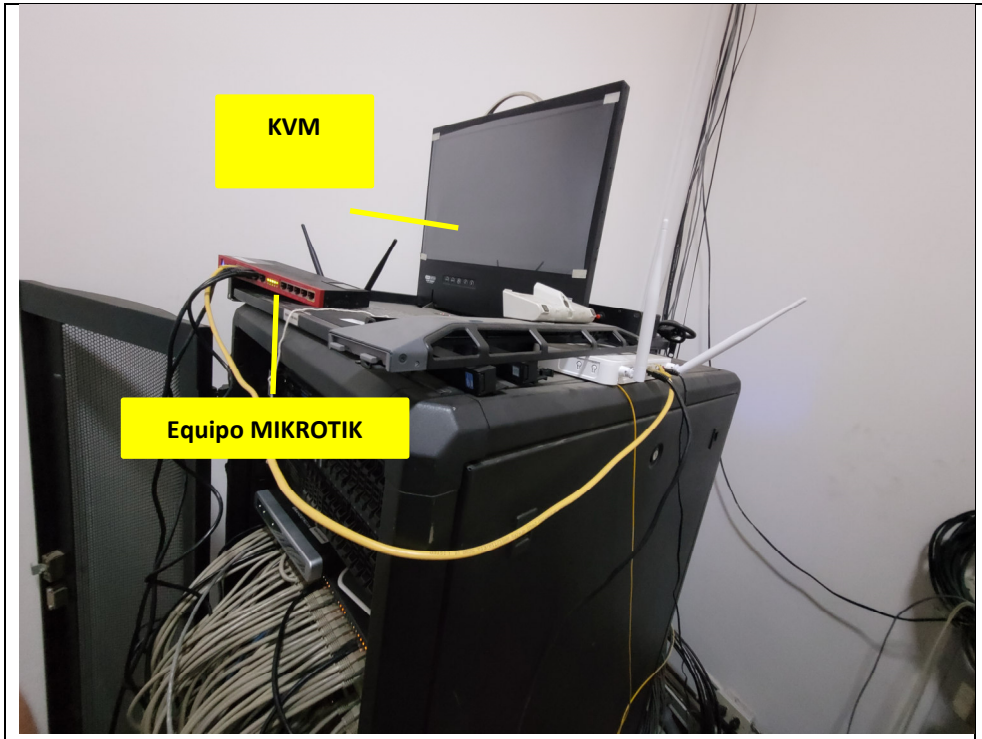
Anexo 2: Evidencia fotográfica Área de Sistemas y CPD TI - VCDI

Oficina área de sistemas del VCDI vista al ingreso de la puerta principal.

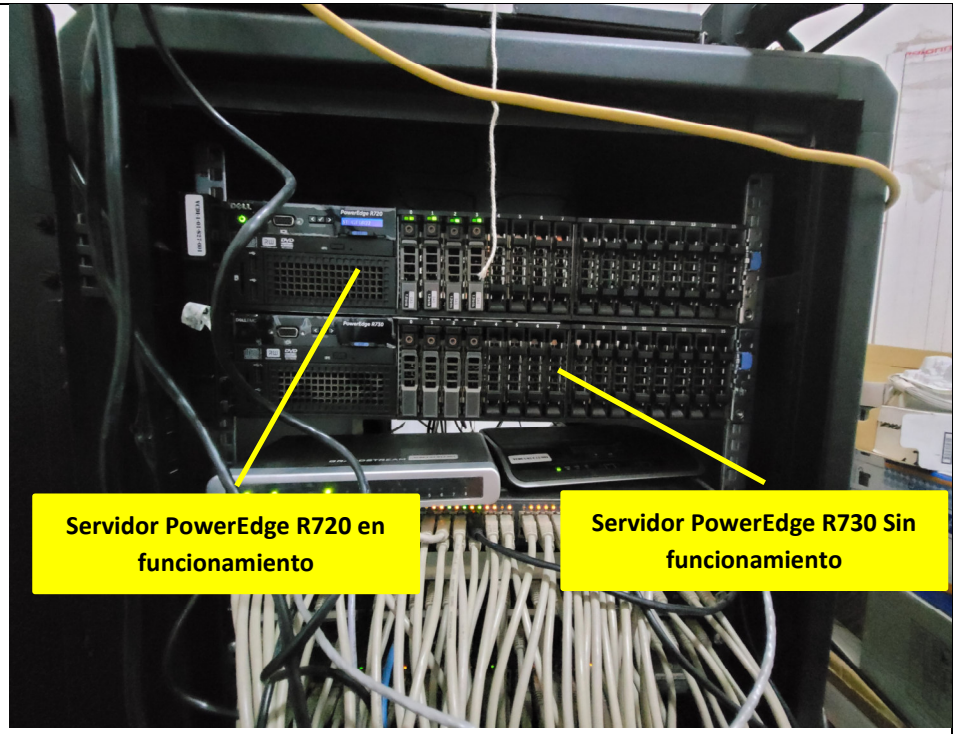
Oficina área de sistemas del VCDI vista lateral a la puerta de acceso principal puerta con chapa.

Zona del rack de procesamiento de datos principal del área de TI del VCDI, material de trabajo, cables y cajoneria, y presencia de un ventanal.

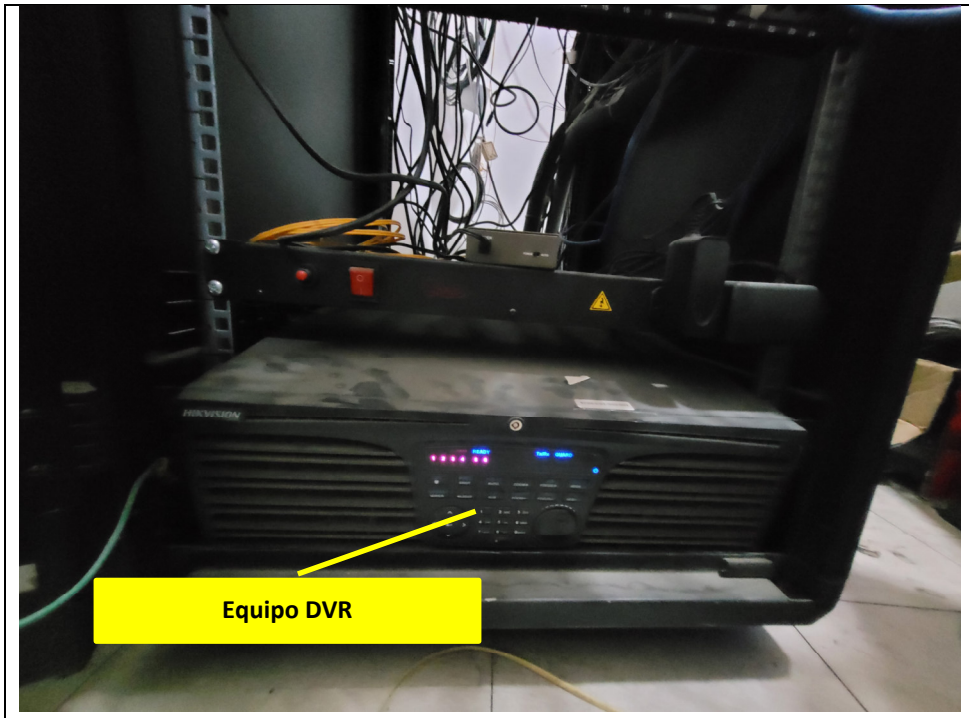
Pasillo de acceso a la zona del rack vista lateral al acceso principal del área de sistemas.



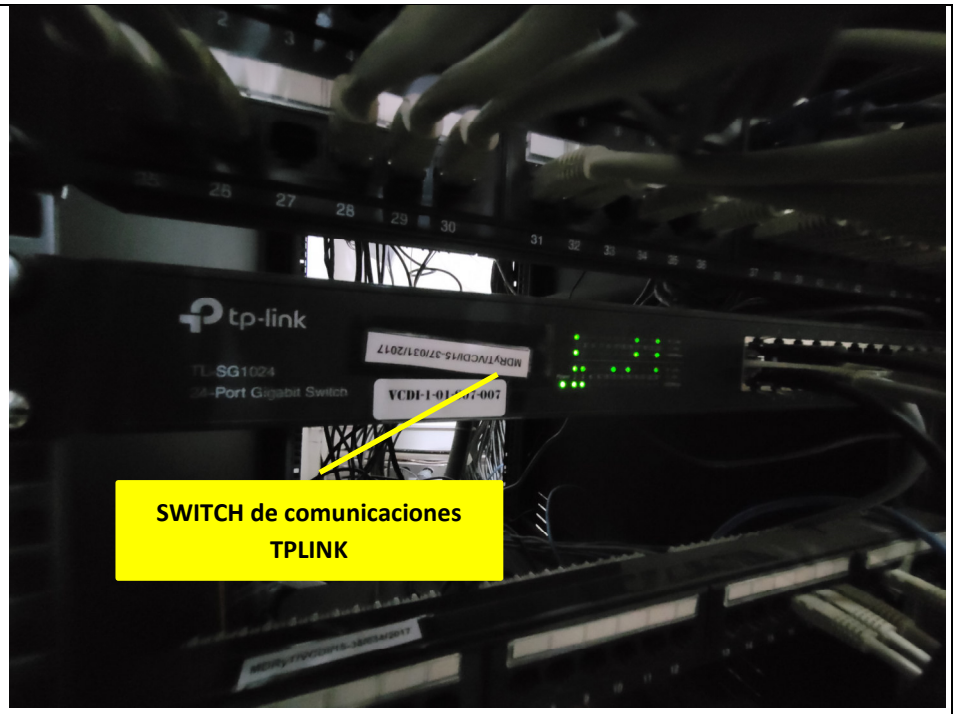
Vista del Rack de comunicaciones, se visualiza el equipo Router MIKROTIK (color rojo), un KVM de administración de servidores, y el router del proveedor de internet AXS (color blanco).



Vista de los servidores principales, en la parte superior el servidor PowerEdge R720 en funcionamiento, y en la parte inferiór un servidor Dell PowerEdge R730 sin funcionamiento.

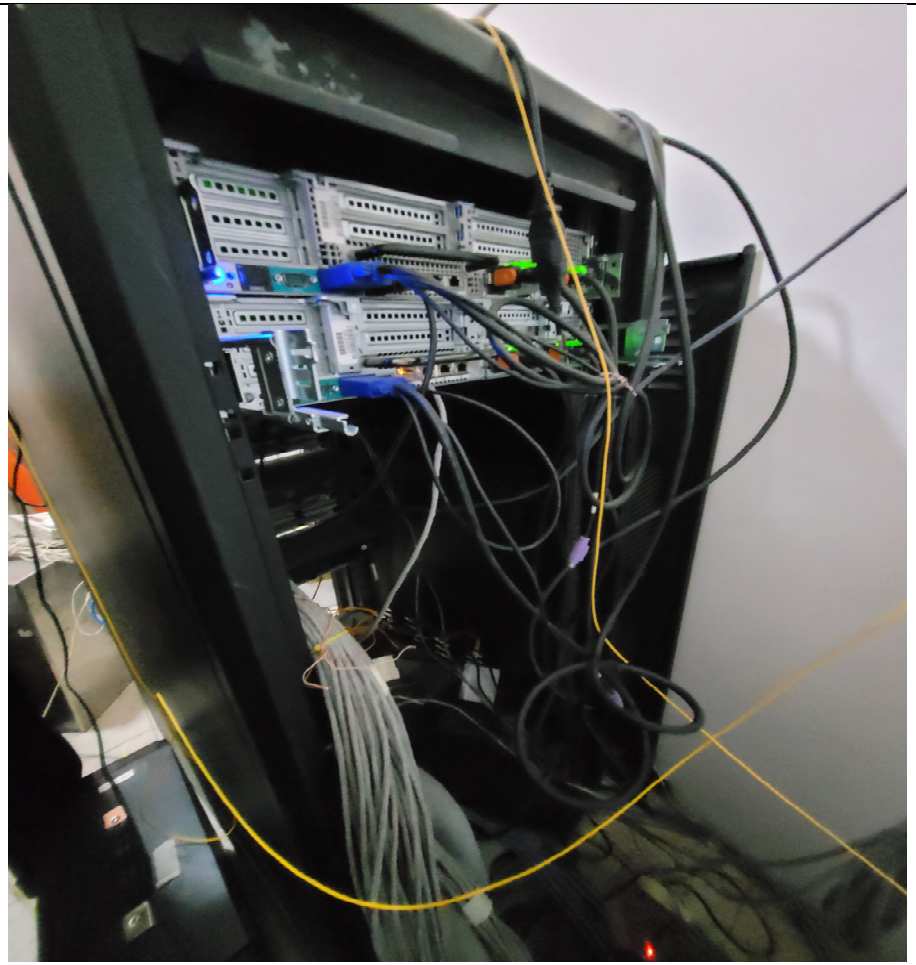


Equipo DVR concentrador de las camaras de seguridad implemntados en el VCDI



Vista del equipo Switch TPLINK para la distribución de red interna.

Bista tracera superior del RACK,



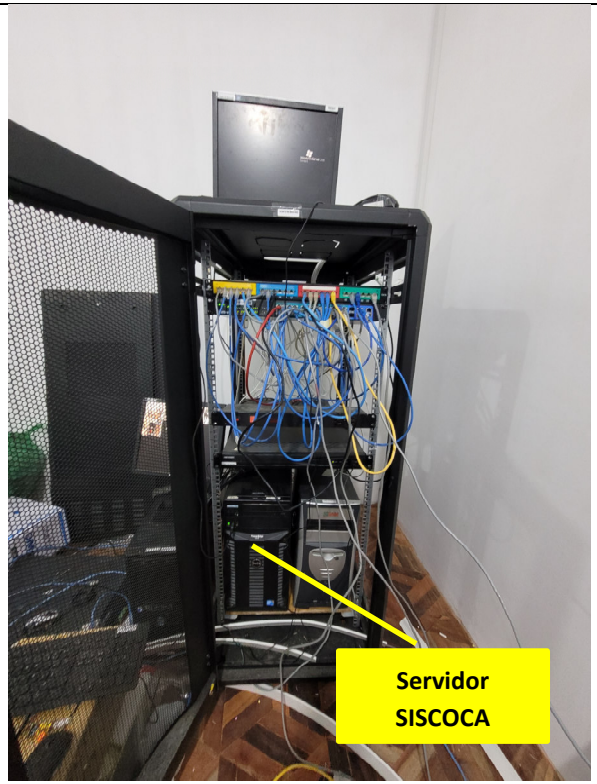
Vista tracera del Rack de comunicaciones y cableado implementado.

	
Vista del equipo MIKROTIK donde se conectan la conexión de internet, la red LAN, el Servidor principal del VCDI (DELL PowerEdge R720)	Vista lateral del área del rack de comunicaciones y servidores – existencia de material de cableado y cajones de carton..

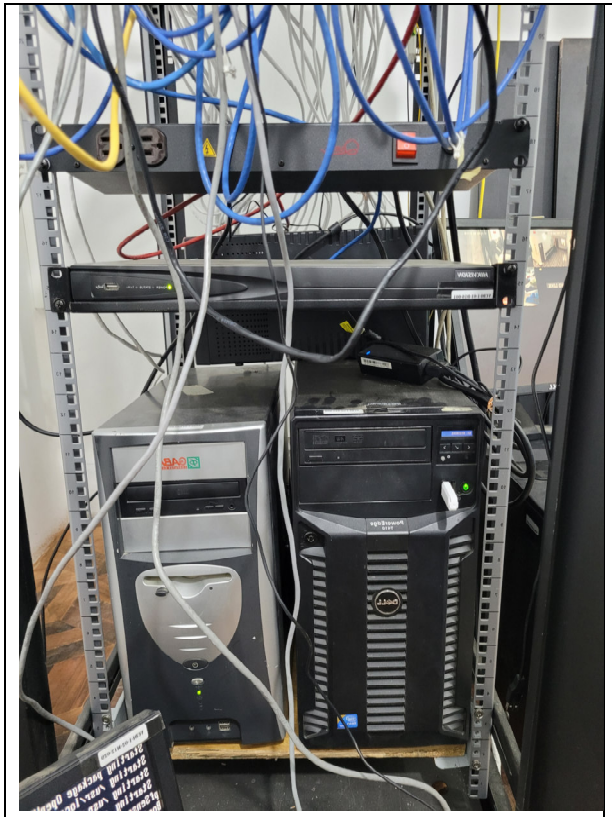
Anexo 3: Evidencia fotográfica Área de Sistemas DIGCOIN

Acceso principal al área de sistemas y el área de equipos de computo CPD

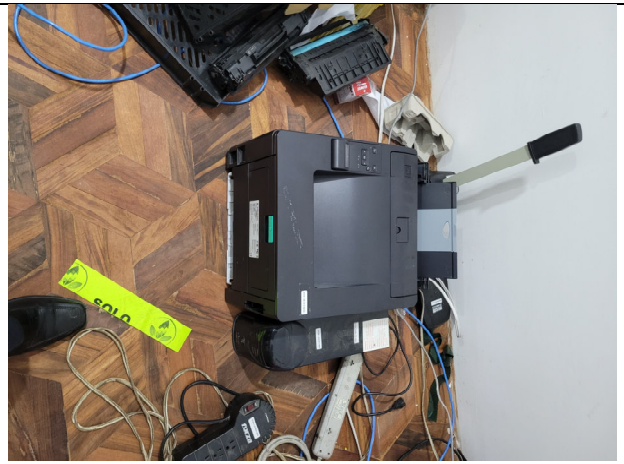
Área del centro de procesamiento de datos de DIGCOIN, presencia de documentación en bolsas.



Rack principal de comunicaciones y computo, presencia de un equipo router de acceso a internet, switch, servidor y equipo de computo (linux Pfsense sin funcionamiento), al lado equipo de computo PROXY (en funcionamiento).

		
Vista del rack ptincipal de comunicaciones DIGCOIN	Vista lateral del Rack de equipos de comunicaciones y computo de DIGCOIN	Servidor DELL en DESPERFECTO

Swicht CISCO sin funcionamiento



Equipos de impresión sin funcionamiento

Material inflamable, cajones material en desuso, cables, y documento en área.

Equipo DVR sin funcionamiento

+

Nodo de comunicaciones principal

METODOLOGÍA DE EVALUACIÓN Y TRATAMIENTO DE RIESGOS

Evaluación de riesgos

La evaluación de riesgos se implementa a través de la Tabla de Evaluación de Riesgos. El proceso de evaluación de riesgos está coordinado con el grupo de referencia de la misión, la identificación de amenazas, vulnerabilidades y riesgos es realizada de forma conjunta con los propietarios de los activos que para efectos es también el propietario de los riesgos.

Activos, vulnerabilidades y amenazas

El primer paso en la evaluación de riesgos es la identificación de todos los activos en el ámbito del SISCOCA, es decir, de todos los activos que pueden interrumpir las operaciones. Los activos pueden incluir documentos en papel o en formato electrónico, aplicaciones y bases de datos, personas, equipos de TI, infraestructura, herramientas, maquinaria, instalaciones de producción y servicios externos / procesos subcontratados. Al identificar activos, también es necesario identificar a sus propietarios: la persona o unidad organizativa responsable de cada activo. Para fines de nuestra evaluación se tiene solo el SISCOCA-SAR y SISCOCA- MODULO DE PRODUCCIÓN como activos principales.

El siguiente paso es identificar todas las amenazas y vulnerabilidades asociadas con cada activo. Las amenazas y vulnerabilidades se identifican utilizando los catálogos incluidos en la Tabla de Evaluación de Riesgos. Cada activo puede estar asociado con varias amenazas, y cada amenaza puede estar asociada con varias vulnerabilidades.

Los activos y sus propietarios se definen en la Tabla de Activos del Registro de Riesgos.

Determinación de los propietarios del riesgo

Para cada riesgo, se debe identificar un propietario del riesgo: la persona o unidad organizativa responsable de cada riesgo. Para el caso de DIGPROCOCA y DIGCOIN el propietario del activo es también responsable de los riesgos, en este caso en específico las Direcciones principales.

Los propietarios de riesgos se definen en la Tabla de Evaluación de Riesgos en el Registro de Riesgos.

Consecuencias y probabilidad

Una vez que se han identificado los propietarios de riesgos, es necesario evaluar las consecuencias de cada combinación de amenazas y vulnerabilidades para un activo individual si dicho riesgo se materializa:

Consecuencia insignificante	1	Impacto no importante en el negocio, el flujo de caja de la organización, las operaciones, las obligaciones legales o contractuales, o su reputación.
Consecuencias menores	2	Pequeño impacto en el negocio, el flujo de caja de la organización, las operaciones, las obligaciones legales o contractuales, o su reputación.
Consecuencia moderada	3	Gran impacto en el negocio, el flujo de caja de la organización, las operaciones, las obligaciones legales o contractuales, o su reputación.
Consecuencias importantes	4	Gran impacto en el negocio, el flujo de caja de la organización, las operaciones, las obligaciones legales o contractuales, o su reputación.
Consecuencia crítica	5	Impacto catastrófico en el negocio, el flujo de caja de la organización, las operaciones, las obligaciones legales o contractuales, o su reputación.

Después de la evaluación de las consecuencias, es necesario evaluar la probabilidad de ocurrencia de tal riesgo, es decir, la probabilidad de que una amenaza explote la vulnerabilidad del activo respectivo:

Probabilidad rara	1	La probabilidad de que una amenaza explote la vulnerabilidad del activo respectivo solo ocurriría en circunstancias excepcionales.
Probabilidad improbable	2	No se espera que ocurra la probabilidad de que una amenaza explote la vulnerabilidad del activo respectivo.
Posible probabilidad	3	La probabilidad de que una amenaza explote la vulnerabilidad del activo respectivo podría ocurrir en algún momento.
Probabilidad probable	4	La probabilidad de que una amenaza explote la vulnerabilidad del activo respectivo probablemente ocurrirá en la mayoría de las circunstancias.
Probabilidad casi segura	5	Se espera que la probabilidad de que una amenaza explote la vulnerabilidad del activo respectivo ocurra en la mayoría de las circunstancias.

Al introducir los valores de consecuencia y probabilidad en la tabla de evaluación de riesgos, el nivel de riesgo se calcula automáticamente sumando los dos valores. Los controles de seguridad existentes deben introducirse en los dos últimos capítulos del cuadro de evaluación de riesgos.

Calificación de riesgo

Sobre la base de la evaluación de la probabilidad y la consecuencia, se obtiene una calificación de riesgo a través de la siguiente matriz:

Probabilidad					
5	Bajo	Medio	Alto	Crítico	Crítico
4	Bajo	Medio	Alto	Alto	Crítico
3	Bajo	Bajo	Medio	Alto	Alto
2	Muy bajo	Bajo	Bajo	Medio	Medio
1	Muy bajo	Muy bajo	Bajo	Bajo	Bajo
	1	2	3	4	5
	Consecuencia				

La clasificación de cada riesgo se registrará como insumo para la etapa de evaluación de riesgos del proceso.

Evaluación de riesgos

El propósito de la evaluación de riesgos es decidir qué riesgos pueden ser aceptados y cuáles deben ser tratados. Esto tendrá en cuenta los criterios de aceptación de riesgos.

Criterios de aceptación de riesgos

Los valores muy bajos – bajos son riesgos aceptables, mientras que los valores medios – críticos son riesgos inaceptables. Los riesgos inaceptables deben ser tratados (formalmente aceptados, mitigados, transferidos o evitados).

Tratamiento de riesgos

El tratamiento de riesgos se implementa a través de la Tabla de Tratamiento de Riesgos, copiando todos los riesgos identificados como inaceptables de la Tabla de Evaluación de Riesgos.

1. Se deben seleccionar una o más soluciones de tratamiento para riesgos valorados como medio-críticos:
2. Selección de control o controles que mejor mitiguen los riesgos puede también apoyarse en el catálogo de controles anexo A de la NB/ISO 27001 2013.
3. Transferir los riesgos a un tercero, por ejemplo, comprando una póliza de seguro o firmando un contrato con proveedores o socios
4. Evitar el riesgo al interrumpir una actividad comercial que causa dicho riesgo
5. Aceptar el riesgo: esta opción solo se permite si la selección de otras opciones de tratamiento de riesgo costaría más que el impacto potencial en caso de que dicho riesgo se materialice.

La selección de opciones se implementa a través de la Tabla de Tratamiento de Riesgos. Por lo general, se selecciona la opción 1: selección de uno o más controles de seguridad. Cuando se seleccionan varios controles de seguridad para un riesgo, se insertan filas adicionales en la tabla inmediatamente debajo de la fila que especifica el riesgo.

En el caso de la opción 1 (selección de controles de seguridad), es necesario evaluar el nuevo valor (riesgos residuales) de consecuencia y probabilidad en la Tabla de Tratamiento de Riesgos, con el fin de evaluar la efectividad de los controles planificados

Anexo 5: Análisis de riesgo SISCOCA-SAR

ID ACTIVO	Asset (Activo)	Activo detallado
1	*Sistema SISCOCA- SAR*	*Sistema denominado SISCOCA - SAR implementado en la unidad de comercialización, aplicación de escritorio permite el registro de comercializadores al detalle, registro y emisión e hojas de ruta, registro de trámites relacionados.*

ID RIESGO	Threat (Amenaza)	Vulnerability (Vulnerabilidad)	Risk Área (Área de Riesgo)	Description of the risk (Descripción del riesgo)	Risk Owner (Propietario del riesgo)	Risks drivers/causes (Impulsores/causas del riesgo)	Inherent risk			Controls implemented (Controles Implementados)	
							Probabilidad	Severidad del riesgo	Calificación del riesgo	Current actions (Acciones actuales)	Mapping to ISO Annex A chapters (referencia del control según anexo A)
R1	*Ataque malicioso /Equipo defectuoso*	*Plataforma insegura/ Gestión inadecuada de recursos / Equipos*	*Comunicaciones y redes*	Perdida e indisponibilidad de servicio	*Dirección General de Desarrollo Integral de las Regiones Productoras de Coca (DIGPROCOCA),*	- La red local y de comunicaciones no establece un esquema de seguridad adecuado - los usuarios y recursos críticos como el servidor de base de datos y de aplicación comparten los segmentos de red - Funcionarios de la regional de Cochabamba acceden a SISCOCA a través de teamviwer, y expone a la red ante posibles riesgos de ciberseguridad. - Los equipos de comunicaciones y los servidores, no cuentan con un programa de mantenimiento preventivo para reducir riesgos de continuidad (no se efectuaron procesos de mantenimiento). - Los equipos servidor no cuentan con un antivirus o anti malware que permita un adecuado aseguramiento ante posibles pérdidas de información o servicio. - No se define un perímetro de	5	5	**5**	Se ha implementado un servidor Proxy, que permite el rutear del tráfico de red, y controlar las peticiones de internet.	A.12.2.1 Controles contra el malware A.11.2.1 Emplazamiento y protección de equipo A.11.2.3 Seguridad de cableado A.11.2.4 Mantenimiento de equipos A.13.1.1 Controles de red

ID RIESGO	Threat (Amenaza)	Vulnerability (Vulnerabilidad)	Risk Área (Área de Riesgo)	Description of the risk (Descripción del riesgo)	Risk Owner (Propietario del riesgo)	Risks drivers/causes (Impulsores/causas del riesgo)	Inherent risk			Controls implemented (Controles Implementados)	
							Probabilidad	Severidad del riesgo	Calificación del riesgo	Current actions (Acciones actuales)	Mapping to ISO Annex A chapters (referencia del control según anexo A)
						seguridad externo gestionado a través de un firewall, que defina las políticas de seguridad de la red y las comunicaciones. - Área de comunicaciones y computo con material en desuso, documentos en bolsas, cajas de cables.					
R2	*Credenciales comprometidas / Monitoreo inadecuado/Extracción*	*Usuario / Actor malicioso*	*Datos*	Acceso indebido y perdida de información	*Dirección General de Desarrollo Integral de las Regiones Productoras de Coca (DIGPROCOCA),*	Los usuarios definidos en el sistema no están relacionados a un perfil de accesos, actualmente parte de los usuarios cuentan con todos los accesos a las funcionalidades del sistema SISCOCA-SAR (Sistemas, Estadísticas,). Asimismo, la gestión de accesos y usuarios no están formalmente definidos en DIGCOIN.	4	5	**5**	No se ha identificado ninguna acción correctiva; sin embargo, la base de datos identifica que los usuarios habilitados corresponden a funcionario en función.	A.9.2 Administración de accesos a los usuarios A.9.3 Responsabilidad de usuarios A.9.4 Control de acceso de sistemas y aplicaciones
R3	*Software no compatible*	*Plataforma insegura*	*Datos*	Software de base de datos y lenguaje de desarrollo obsoletos	*Dirección General de Desarrollo Integral de las Regiones Productoras de Coca (DIGPROCOCA),*	La plataforma de programación Visual Basic 6 y MS SQLServer 2008 no cuentan con soporte, y el grado de obsolescencia de estas herramientas ponen en riesgo la información gestionada debido a aspectos de seguridad que no fueron resueltos por Microsoft y actualmente ya no son compatibles con sistemas operativos actuales.	4	5	**5**	Se han realizado diagnósticos, y propuestas para desarrollar un nuevo sistema SISCOCA; sin embargo, el mismo, no fue desarrollados; asimismo, se está complementando el sistema con desarrollos satélite con plataformas actuales.	A.12.6.1 Administración de vulnerabilidades técnicas
R4	*Amenaza interna*	*Diseño del sistema/ Actor malicioso*	*Documento*	Falsificación de Hojas de ruta / Falsificación de Credenciales de comercialización / inadecuado monitoreo de	*Dirección General de Desarrollo Integral de las Regiones Productoras de Coca (DIGPROCOCA),*	- Los carnets de comercialización cuentan con códigos de barra y QR pero los mismos no almacenan datos relevantes, por lo que es posible que los mismos sean objeto de falsificación. - La impresión de carnets no cuenta con controles como contadores de impresión o reimpresión y captura de	5	5	**5**	Se efectuará un control sobre el correlativo preimpreso de las hojas de ruta / Los sellos de emisión son cambiados periódicamente / existe control en los	A.14.1.1 Análisis y especificación de los requisitos de la información A.14.1.3 Protección de transacciones de servicios de aplicación A.14.2.6 Entorno de desarrollo seguro

ID RIESGO	Threat (Amenaza)	Vulnerability (Vulnerabilidad)	Risk Área (Área de Riesgo)	Description of the risk (Descripción del riesgo)	Risk Owner (Propietario del riesgo)	Risks drivers/causes (Impulsores/causas del riesgo)	Inherent risk			Controls implemented (Controles Implementados)	
							Probabilidad	Severidad del riesgo	Calificación del riesgo	Current actions (Acciones actuales)	Mapping to ISO Annex A chapters (referencia del control según anexo A)
				las operaciones de los usuarios		usuarios. - La emisión de hojas de ruta no cuenta con logs de auditoría, controles de impresión o reimpresión, fechas y usuarios. - Las hojas de ruta no están digitalizadas en el sistema para un adecuado resguardo y control histórico de cumplimiento de ruta. - Las hojas de ruta cuentan con un código de barra que identifica el número secuencial que es almacenado en el sistema, dicho código no puede ser contrastado en puntos de control con la base de datos, no establece controles adecuados de seguridad para verificar su autenticidad contra la base de datos, esto significa que una hoja de ruta podría ser objeto de clonación, ya que los controles en los puestos no son efectuados o contrastados digitalmente. - No se cuenta con controles automatizados que permita la verificación digital de las hojas de ruta y los carnets en los puestos de control, el control se basa principalmente en el paso físico de cada hoja de ruta por punto de control y el sello respectivo. - El control de hojas de ruta sobre el cumplimiento de la ruta es efectuado manualmente por personal encargado de la emisión de las hojas de ruta, cualquier incumplimiento es verificado manualmente sin el apoyo del sistema				puestos de control / se realizan incautaciones y detención de personas	A.14.2.7 Desarrollo externalizado A.14.2.8 Pruebas de seguridad de sistemas Vinculación con la tabla de priorización de desarrollos.

ID RIESGO	Threat (Amenaza)	Vulnerability (Vulnerabilidad)	Risk Área (Área de Riesgo)	Description of the risk (Descripción del riesgo)	Risk Owner (Propietario del riesgo)	Risks drivers/causes (Impulsores/causas del riesgo)	Inherent risk			Controls implemented (Controles Implementados)	
							Probabilidad	Severidad del riesgo	Calificación del riesgo	Current actions (Acciones actuales)	Mapping to ISO Annex A chapters (referencia del control según anexo A)
						SISCOCA-SAR, respecto a la trazabilidad de cada hoja de ruta. - Cambios en bases de datos para parámetros de precios, no cuentan con funcionalidades de mantenimiento.					
R5	*Personal indisponible / Error de administrador / Desastre natural / Aspectos sociales y políticos*	*Continuidad y contingencia*	*Servicios*	Interrupción de operaciones	*Dirección General de Desarrollo Integral de las Regiones Productoras de Coca (DIGPROCOCA),*	No se define políticas formales de respaldo para el sistema SISCOCA-SAR, los respaldos efectuados no son programados y no tienen un procedimiento que defina la periodicidad y el tipo de respaldo en función a un RTO y RPO basado en un análisis de riesgo. La base de datos del SISCOCA-SAR se encuentra instalado en el único servidor, por lo que un desperfecto, una contingencia física o robo del mismo, podría interrumpir las operaciones de DIGCOIN, y no se tiene establecido un plan de contingencia y continuidad para responder a posibles incidentes. No se establece un plan de continuidad de las operaciones en caso de contingencia por aspectos externos.	5	5	**5**	Se realizan bakcups de la base de datos en periodos no planificados.	A.12.3.1 Respaldo de información A.17.1. Continuidad de la seguridad de la información
R6	*Legislación / error de desarrollo*	*Diseño del sistema/ incumplimiento / plataforma insegura*	*Software*	Proceso de cambios en el sistema SISCOCA indisponible.	*Dirección General de Desarrollo Integral de las Regiones Productoras de Coca (DIGPROCOCA),*	- No se definen políticas de resguardo de código fuente, por lo que, el código fuente de SISCOCA-SAR no corresponde a la versión en producción, debido a que en el proceso de restauración del código fuente y compilación del mismos para replicar la versión de producción, no fue posible debido a que el mismo no	4	5	**5**	No se ha identificado ninguna acción relacionada con la documentación.	A.9.4.5 Control de acceso al código fuente del programa A.14.1.1 Análisis y especificación de los requisitos de la información A.14.2.1 Política de desarrollo seguro A.14.2.2 Procedimientos de

ID RIESGO	Threat (Amenaza)	Vulnerability (Vulnerabilidad)	Risk Área (Área de Riesgo)	Description of the risk (Descripción del riesgo)	Risk Owner (Propietario del riesgo)	Risks drivers/causes (Impulsores/causas del riesgo)	Inherent risk			Controls implemented (Controles Implementados)	
							Probabilidad	Severidad del riesgo	Calificación del riesgo	Current actions (Acciones actuales)	Mapping to ISO Annex A chapters (referencia del control según anexo A)
						está completo y faltan partes de código, por lo que, no es posible efectuar modificaciones al sistema. - No se cuenta con documentación técnica del sistema SISCOCA-SAR que permita orientar sobre la estructura de bases de datos, objetos, y arquitectura; para efectuar un entendimiento adecuado y propiciar un mantenimiento o actualización.					control de cambios del sistema

Anexo 6: Análisis de riesgo SISCOCA-MODULO DE PRODUCCIÓN

ID ACTIVO	Asset (Activo)	Activo detallado
2	*Sistema SISCOCA- MODULO DE PRODUCCIÓN*	*Sistema Integrado Catastral de Productores de Coca, permite el registro de la superficie de catos, registro de productores, y trámites relacionados*

ID RIESGO	Threat (Amenaza)	Vulnerability (Vulnerabilidad)	Risk Área (Área de Riesgo)	Description of the risk (Descripción del riesgo)	Risk Owner (Propietario del riesgo)	Risks drivers/causes (Impulsores/causas del riesgo)	Inherent risk			Controls implemented (Controles Implementados)	
							Probabilidad	Severidad del riesgo	Calificación del riesgo	Current actions (Acciones actuales)	Mapping to ISO Annex A chapters (referencia del control según anexo A)
R1	*Ataque malicioso /Equipo defectuoso*	*Plataforma insegura/ Gestión inadecuada de recursos / Equipos*	*Comunicaciones y redes*	Perdida e indisponibilidad de servicio	*Dirección General de Desarrollo Integral de las Regiones Productoras de Coca (DIGPROCOCA),*	- Los equipos de cómputo y comunicaciones, incluido el mobiliario asignado están cubiertos con polvo. - No se define una seguridad física ambiental, el rack de comunicaciones y computo está en un espacio compartido con el área de trabajo del responsable de sistemas, esta área cuenta con un solo acceso a través de una puerta de madera con chapa. - El área de comunicaciones y servidores no cuenta con una organización adecuada y existe presencia de material de trabajo; además, de cajones con cables. - No cuenta con un perímetro de seguridad diferenciado del área común de trabajo - No se define una adecuada seguridad físico ambiental (sensores de calor, humedad, sistema de aire). - Los equipos servidor no cuentan con un antivirus o anti malware que permita establecer un adecuado aseguramiento ante posibles pérdidas	4	5	**5**	Se ha implementado un servidor Proxy, que permite el rutear del tráfico de red, y controlar las peticiones de internet.	A.12.2.1 Controles contra el malware A.11.2.1 Emplazamiento y protección de equipo A.11.2.3 Seguridad de cableado A.11.2.4 Mantenimiento de equipos A.13.1.1 Controles de red

ID RIESGO	Threat (Amenaza)	Vulnerability (Vulnerabilidad)	Risk Área (Área de Riesgo)	Description of the risk (Descripción del riesgo)	Risk Owner (Propietario del riesgo)	Risks drivers/causes (Impulsores/causas del riesgo)	Inherent risk			Controls implemented (Controles Implementados)	
							Probabilidad	Severidad del riesgo	Calificación del riesgo	Current actions (Acciones actuales)	Mapping to ISO Annex A chapters (referencia del control según anexo A)
						de información o servicio. - No se define un perímetro de seguridad externo gestionado a través de un firewall, que defina las políticas de seguridad de la red y las comunicaciones.					
R2	*Amenaza interna*	*Diseño del sistema / Actor malicioso*	*Documento*	Posible acceso indebido, credenciales de productores falsificados o reimpresos sin control	*Dirección General de Desarrollo Integral de las Regiones Productoras de Coca (DIGPROCOCA),*	- El sistema SISCOCA- MODULO DE PRODUCCIÓN no define logs de auditoría que establezca una la trazabilidad de las operaciones realizadas por los usuarios. - La carnetización de productores cuenta con un módulo de registro en el SISCOCA- MODULO DE PRODUCCIÓN; sin embargo, el proceso de emisión de carnets es efectuado a través de un proceso manual complementario; donde, el responsable técnico una vez registrado en el sistema efectúa una copia de los registros de comercializador en planillas Excel y esta es vinculada con el dispositivo de impresión, por lo que la emisión del carnet no es realizada por el sistema. - Los carnets de comercialización cuentan con códigos QR que contiene la información del productor; sin embargo, no pueden ser validados contra la base de datos del sistema. - La impresión de carnets no establece controles de la cantidad de impresiones o reimpresiones realizadas.	3	4	**4**	Actualmente se están desarrollando programas satélites para la impresión de las credenciales. Los demás aspectos no serán resueltos aún debido a que los códigos fuente no pudieron replicar el ambiente de desarrollo.	A.14.1.1 Análisis y especificación de los requisitos de la información A.14.1.3 Protección de transacciones de servicios de aplicación A.14.2.6 Entorno de desarrollo seguro A.14.2.7 Desarrollo externalizado A.14.2.8 Pruebas de seguridad de sistemas Vinculación con la tabla de priorización de desarrollos.

ID RIESGO	Threat (Amenaza)	Vulnerability (Vulnerabilidad)	Risk Área (Área de Riesgo)	Description of the risk (Descripción del riesgo)	Risk Owner (Propietario del riesgo)	Risks drivers/causes (Impulsores/causas del riesgo)	Inherent risk			Controls implemented (Controles Implementados)	
							Probabilidad	Severidad del riesgo	Calificación del riesgo	Current actions (Acciones actuales)	Mapping to ISO Annex A chapters (referencia del control según anexo A)
						- No toda la información de productores se encuentra registrada en el sistema de MODULO DE PRODUCCIÓN, solo los productores con catastro están en la base de datos, el resto de productores de zonas originarias ancestrales se encuentran en planillas Excel - No se implementa una interoperabilidad entre las las bases de datos de productores de los Yungas con productores del Trópico de Cochabamba, por lo que las labores de validación de superficies, existencia, publicidad de catos por un productor en ambas regiones son realizadas manualmente. - No se tiene en producción un sistema GIS que permita inventariar los cultivos de hoja de coca, superficies para cada productor, los cuales estén relacionados con los registros de productores. - Errores de programación en el despliegue de registros de trámites administrativos.					
R3	*Personal indisponible / Error de administrador /Aspectos sociales y políticos*	*Continuidad y contingencia*	*Servicios*	Interrupción de operaciones	*Dirección General de Desarrollo Integral de las Regiones Productoras de Coca (DIGPROCOCA),*	No se define políticas formales de respaldo para el sistema SISCOCA-MODULO DE PRODUCCIÓN, los respaldos efectuados no son programados y no tienen un procedimiento que defina la periodicidad y el tipo de respaldo en función a un RTO y RPO basado en un	3	4	**4**	Se realizan bakcups de la base de datos en periodos no planificados.	A.12.3.1 Respaldo de información A.17.1 Continuidad de la seguridad de la información

ID RIESGO	Threat (Amenaza)	Vulnerability (Vulnerabilidad)	Risk Área (Área de Riesgo)	Description of the risk (Descripción del riesgo)	Risk Owner (Propietario del riesgo)	Risks drivers/causes (Impulsores/causas del riesgo)	Inherent risk			Controls implemented (Controles Implementados)	
							Probabilidad	Severidad del riesgo	Calificación del riesgo	Current actions (Acciones actuales)	Mapping to ISO Annex A chapters (referencia del control según anexo A)
						análisis de riesgo. No se establece un plan de continuidad de las operaciones en caso de contingencia por aspectos externos.					
R4	*Legislación / error de desarrollo*	*Diseño del sistema/ incumplimiento / plataforma insegura*	*Software*	Proceso de cambios en el sistema SISCOCA -MODULO DE PRODUCCIÓN indisponible.	*Dirección General de Desarrollo Integral de las Regiones Productoras de Coca (DIGPROCOCA),*	- No se definen políticas de resguardo de código fuente. - El código fuente de SISCOCA-MODULO DE PRODUCCIÓN esta ofuscado, por lo que procesos de mantenimiento no pueden ser realizados. - No se cuenta con documentación técnica del sistema SISCOCA-MODULO DE PRODUCCIÓN que permita orientar sobre la estructura de bases de datos, objetos, y arquitectura; para efectuar un entendimiento adecuado y propiciar un mantenimiento o actualización.	4	5	**5**	No se ha identificado ninguna acción relacionada con la documentación o el código fuente.	A.9.4.5 Control de acceso al código fuente del programa A.14.1.1 Análisis y especificación de los requisitos de la información A.14.2.1 Política de desarrollo seguro A.14.2.2 Procedimientos de control de cambios del sistema

Anexo 7: Tratamiento de los riesgos sistemas SISCOCA-SAR y SISCOCA-MODULO DE PRODUCCIÓN

ID	Riesgo	Propietario del riesgo	Tratamiento	Acciones de mitigación	Annex A reference/control objective	Prioridad	Probabilidad residual	Impacto residual	Riesgo residual
	SISTEMA SISCOCA-SAR DIGCOIN								
R1	Perdida e indisponibilidad de servicio	*Dirección General de la Hoja de Coca e Industrialización (DIGCOIN)*	Mitigar el Riesgo	- Plan de mantenimiento preventivo programado a equipos informativos críticos (Servidores y comunicaciones) - Implementación de Antivirus y Antimalware para servidores Windows y Linux. - Implementación de un perímetro de seguridad para el área de servidores y equipos de comunicaciones - Implementación de la seguridad física del área de CPD del VCDI - Trabajo de limpieza del área y organización de cableado. - Implementación de un firewall - Consultoría para la implementación de un esquema de seguridad adecuado.	A.12.2.1 Controles contra el malware A.11.2.1 Emplazamiento y protección de equipo A.11.2.3 Seguridad de cableado A.11.2.4 Mantenimiento de equipos A.13.1.1 Controles de red	ALTO	2	2	**2**
R2	Acceso indebido y perdida de información	*Dirección General de la Hoja de Coca e Industrialización (DIGCOIN)*	Mitigar el Riesgo	- Política de control de accesos. - Procedimiento de administración de accesos (crear, borrar y modificar usuarios y accesos) - Revisión de los accesos y usuarios de las bases de datos. - Política monitoreo de las operaciones de usuarios.	A.9.2 Administración de accesos a los usuarios A.9.3 Responsabilidad de usuarios A.9.4 Control de acceso de sistemas y aplicaciones	ALTO	2	2	**2**
R3	Software de base de datos y lenguaje de desarrollo obsoletos	*Dirección General de la Hoja de Coca e Industrialización (DIGCOIN)*	Aceptar - el riesgo es aceptable	- Nota técnica para Informar a la Dirección sobre los riesgos asociados a la plataforma.	A.12.6.1 Administración de vulnerabilidades técnicas	ALTO	4	5	**5**

ID	Riesgo	Propietario del riesgo	Tratamiento	Acciones de mitigación	Annex A reference/control objective	Prioridad	Probabilidad residual	Impacto residual	Riesgo residual
R4	Falsificación de Hojas de ruta / Falsificación de Credenciales de comercialización / inadecuado monitoreo de las operaciones de los usuarios	*Dirección General de la Hoja de Coca e Industrialización (DIGCOIN)*	Mitigar el Riesgo	- Inventario de desarrollos priorizados para mitigar el riesgo. - Políticas y procedimiento para el desarrollo seguro	A.14.1.1 Análisis y especificación de los requisitos de la información A.14.1.3 Protección de transacciones de servicios de aplicación A.14.2.6 Entorno de desarrollo seguro A.14.2.7 Desarrollo externalizado A.14.2.8 Pruebas de seguridad de sistemas Vinculación con la tabla de priorización de desarrollos.	ALTO	2	3	**2**
R5	Interrupción de operaciones	*Dirección General de la Hoja de Coca e Industrialización (DIGCOIN)*	Mitigar el Riesgo	- Política de respaldo de la información - Procedimiento de respaldo de la información - Plan de contingencias tecnológica - Replica de base de datos SISCOCA-SAR en VCDI.	A.12.3.1 Respaldo de información A.17.1 Continuidad de la seguridad de la información	ALTO	2	3	**2**
R6	Proceso de cambios en el sistema SISCOCA indisponible.	*Dirección General de la Hoja de Coca e Industrialización (DIGCOIN)*	Aceptar - el riesgo es aceptable	- Nota técnica para Informar a la Dirección sobre los riesgos asociados con la gestión del código fuente y los cambios al sistema.	A.9.4.5 Control de acceso al código fuente del programa A.14.1.1 Análisis y especificación de los requisitos de la información A.14.2.1 Política de desarrollo seguro A.14.2.2 Procedimientos de control de cambios del sistema	MEDIUM	4	5	**5**

ID	Riesgo	Propietario del riesgo	Tratamiento	Acciones de mitigación	Annex A reference/control objective	Prioridad	Probabilidad residual	Impacto residual	Riesgo residual
	SISTEMA SISCOCA-MODULO DE PRODUCCIÓN DIGPROCOCA								
R1	Perdida e indisponibilidad de servicio	*Dirección General de Desarrollo Integral de las Regiones Productoras de Coca (DIGPROCOCA),*	Mitigar el Riesgo	- Plan de mantenimiento preventivo programado a equipos informativos críticos (Servidores y comunicaciones) - Implementación de Antivirus y Antimalware para servidores Windows y Linux. - Trabajo de limpieza del área y organización de cableado. - Implementación de un firewall - Consultoría para la implementación de un esquema de seguridad adecuado.	A.12.2.1 Controles contra el malware A.11.2.1 Emplazamiento y protección de equipo A.11.2.3 Seguridad de cableado A.11.2.4 Mantenimiento de equipos A.13.1.1 Controles de red	ALTO	2	2	**2**
R2	Posible acceso indebido, credenciales de productores falsificados o reimpresos sin control	*Dirección General de Desarrollo Integral de las Regiones Productoras de Coca (DIGPROCOCA),*	Mitigar el Riesgo	- Política de control de accesos. - Procedimiento de administración de accesos (crear, borrar y modificar usuarios y accesos) - Revisión de los accesos y usuarios de las bases de datos. - Política monitoreo de las operaciones de usuarios. - Nota técnica para Informar a la Dirección sobre los riesgos asociados a la plataforma.	A.14.1.1 Análisis y especificación de los requisitos de la información A.14.1.3 Protección de transacciones de servicios de aplicación A.14.2.6 Entorno de desarrollo seguro A.14.2.7 Desarrollo externalizado A.14.2.8 Pruebas de seguridad de sistemas Vinculación con la tabla de priorización de desarrollos.	ALTO	2	3	**2**
R3	Interrupción de operaciones	*Dirección General de Desarrollo Integral de las Regiones Productoras de Coca (DIGPROCOCA),*	Mitigar el Riesgo	- Política de respaldo de la información - Procedimiento de respaldo de la información - Plan de contingencias tecnológica - Replica de base de datos SISCOCA-MODULO DE PRODUCCIÓN en sitio externo.	A.12.3.1 Respaldo de información A.17.1 Continuidad de la seguridad de la información	ALTO	1	1	**1**

ID	Riesgo	Propietario del riesgo	Tratamiento	Acciones de mitigación	Annex A reference/control objective	Prioridad	Probabilidad residual	Impacto residual	Riesgo residual
R4	Proceso de cambios en el sistema SISCOCA - MODULO DE PRODUCCIÓN indisponible.	*Dirección General de Desarrollo Integral de las Regiones Productoras de Coca (DIGPROCOCA),*	Aceptar - el riesgo es aceptable	- Nota técnica para Informar a la Dirección sobre los riesgos asociados con la gestión del código fuente, y los cambios al sistema.	A.9.4.5 Control de acceso al código fuente del programa A.14.1.1 Análisis y especificación de los requisitos de la información A.14.2.1 Política de desarrollo seguro A.14.2.2 Procedimientos de control de cambios del sistema	ALTO	4	5	5