La Paz, 12 de diciembre de 2022

Señor
xxxxxxxxxxxxxxxxxxx
Director General de Comercialización e Industrialización de la Hoja de Coca (DIGCOIN)
Presente. -

Ref. NOTA TECNICA - ESTADO DE SITUACION SISCOCA – SAR

De nuestra mayor consideración.

En el marco del 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, Contrato n° DCI/LA/2017/392-699, y la misión de corto plazo DI-023/3 – Actualización del diseño y desarrollo de los módulos de Control, Producción y Comercialización de la hoja de coca (Fase 3), se ha realizado un diagnóstico basado en riesgos de seguridad de la información e informática sobre la situación del SISCOCA en el VCDI, esto con base a las características actuales de la infraestructura informática implementada, los sistemas informáticos de soporte, el flujo de información procesado por los sistemas de DIGCOIN, al respecto informarle que el sistema SISCOCA-SAR esta expuesto a 6 riesgos importantes a los que su autoridad debería gestionar su tratamiento en coordinación con el VCDI, el detalle a continuación:

ID	Descripción del riesgo	Impulsores del riesgo
R1	Perdida e indisponibilidad de servicio	➢ La red local y de comunicaciones no establece un esquema de seguridad adecuado en cuanto al cableado y emplazamiento de su centro de comunicaciones. ➢ los usuarios y recursos críticos como el servidor de base de datos y de aplicación se encuentran en la misma red local, no se define un segmento propio para los servicios y servidores. ➢ 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 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. ➢ Funcionarios de la regional de Cochabamba acceden a SISCOCA a través de teamviwer, y expone a la red ante posibles riesgos de ciberseguridad.
R2	Acceso indebido y perdida de información	➢ 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.

ID	Descripción del riesgo	Impulsores del riesgo
R3	Software de base de datos y lenguaje de desarrollo obsoletos	➢ 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.
R4	Falsificación de Hojas de ruta / Falsificación de Credenciales de comercialización / inadecuado monitoreo de las operaciones de los usuarios	Se identificaron los siguientes aspectos relacionados con sistema SISCOCA-SAR: ➢ La carnetización de productores 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 para la impresión. ➢ La impresión de carnets no cuenta con controles como contadores de impresión o reimpresión y captura de usuarios. ➢ 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 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 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	Interrupción de operaciones	➢ 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.

ID	Descripción del riesgo	Impulsores del riesgo
R6	Proceso de cambios en el sistema SISCOCA indisponible.	➢ 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 o complementaciones 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.

Los riesgos identificados fueron detallados en el Apéndice 1 del informe final, cuyo contenido también detalla los medios de mitigación de cada riesgo; asimismo, como recordará en fecha 22 de noviembre se dio a conocer los resultados de la consultoría cuyo contenido expresaba lo indicado; por otro lado, se presentó al Viceministro el apéndice 6 que complementa la definición de una ruta crítica para la implementación de un plan de fortalecimiento y modernización como acción prioritaria para solventar y mitigar los riesgos identificados.

Mencionar también que la consultoría implicaba una priorización de desarrollos informáticos cuyo detalle es presentado en el apéndice 5 del informe final. El informe final al cual el presente hace referencia es entregado a la asistencia técnica de DITISA, el cual enviará dicho informe y los respectivos apéndices para su conocimiento al VCDI.

La descripción indicativa de los equipamientos necesarios para la mitigación de los riesgos relacionados con la infraestructura informática y comunicaciones se encuentra identificados en el Apéndice 6 componente 1 del Informe final

Sin otro particular, nos despedimos, atentamente.

Oscar Martinez
Consultor Corto Plazo DITISA
Cel. 71505112
Correo: osmartinez@gmail.com