MINISTERIO DE MINAS Y ENERGÍA
OFICINA DE CONTROL INTERNO

AUDITORÍA AL SISTEMA DE INFORMACIÓN DE COMBUSTIBLES LÍQUIDOS DEL MINISTERIO DE MINAS Y ENERGÍA - SICOM

A 30 DE SEPTIEMBRE DE 2018

BOGOTÁ D.C. OCTUBRE DE 2018

OCI-INFORME-082-2018
TRD 15.73 Auditoría Sistema de Información SICOM

TABLA DE CONTENIDO

Calle 43 No 57-31 CAN Bogotá, Colombia
Conmutador (57 1) 2200 300
Código postal 111321
www.minminas.gov.co

AUDITORÍA AL SISTEMA DE INFORMACIÓN DE COMBUSTIBLES LÍQUIDOS DEL MINISTERIO DE MINAS Y ENERGÍA - SICOM

1. OBJETIVO

Verificar la funcionalidad de los módulos del Sistema de Información de Combustibles Líquidos - SICOM, requisitos y niveles de seguridad establecidos, la integralidad entre sus módulos y con otros sistemas de información, así como la operatividad por parte de la Dirección de Hidrocarburos.

2. ALCANCE

La Auditoría cubrirá los siguientes aspectos:

a. Seguimiento y análisis funcional a los módulos del Sistema de Información de Combustibles Líquidos – SICOM.
b. Análisis al plan de mejoras y gestión de cambios, realizado al SICOM.
c. Verificación y Análisis de los requisitos de seguridad implementados y en mejora, al Sistema de Información de Combustibles Líquidos.
d. Análisis de material documental de apoyo, para el uso y manejo del SICOM.
e. Análisis y verificación de planes de recuperación ante desastres aplicables al Sistema de Información de Combustibles Líquidos – SICOM.

3. CLIENTES

Los clientes de la Auditoría son la Ministra de Minas y Energía, el Viceministro de Energía, el Director de la dirección de Hidrocarburos, así como el Coordinador del Grupo de Tecnologías de Información y Comunicación y la ciudadanía en general.

4. EQUIPO DE TRABAJO

El equipo de trabajo está conformado por Ingrid Cecilia Espinosa Sánchez, Jefe de la Oficina de Control Interno, quien supervisará la Auditoría realizada por Andru Cabrales Álvarez y Rezzan Leonardo Chamorro Gómez, Contratistas de la misma Oficina y Gladys Yolanda Ramos Quintero, Profesional Especializado con Asignación de Funciones de Jefe de Oficina de Control Interno, quien revisó el informe preliminar para validación y aprobó el informe final.

Calle 43 No 57-31 CAN Bogotá, Colombia
Conmutador (57 1) 2200 300
Código postal 111321
www.minminas.gov.co

5. CRITERIOS DE AUDITORÍA

Las normas que se utilizarán como parámetros para realizar la evaluación serán las siguientes:

- Norma técnica colombiana NTC 5854 de 2011.
- Norma técnica colombiana NTC-ISO/IEC 27001 de 2013
- Resolución 1652 de 2008
- Guía No. 8 Controles de Seguridad y Privacidad de la Información – MINTIC.
- Ley 87 de 1993.
- Ley 1712 de 2014

6. METODOLOGÍA

La Auditoría se realizó mediante mesas de trabajo, aplicación y verificación de cuestionarios de control interno, solicitud de información, revisión documental, así como análisis a la funcionalidad del Sistema de Información de Combustibles Líquidos – SICOM.

6.1 MEDICIÓN DEL RIESGO

Se procedió a determinar si la variable analizada cuenta con riesgo identificado en el Mapa de Riesgos. Cuando no se encontró documentado el riesgo, la Oficina de Control Interno procedió a identificarlo con base en el criterio normativo aplicable, para posteriormente analizarlo, valorarlo y determinar su **materialización.**

El criterio aplicado para establecer la materialización del riesgo de las variables analizadas, correspondió a los siguientes parámetros de valoración y medición del nivel del riesgo:

Nivel del Riesgo	
Bajo	
Mediano	
Alto	

Bajo: Se refiere a que el tópico analizado muestra un grado de desarrollo importante y aporta de manera sustancial al logro de los objetivos. De manera no significativa, presenta algunas dificultades, pero los resultados finales se obtienen sin mayor contratiempo. *No presenta Materialización de Riesgo* respecto del cumplimiento normativo y del procedimiento establecido. [Se identifica con el color **Verde**]

Mediano: Es cuando el tópico analizado muestra un grado de desarrollo. Su aporte al logro de los objetivos no es sustancial y presenta dificultades operativas que

Calle 43 No 57-31 CAN Bogotá, Colombia
Conmutador (57 1) 2200 300
Código postal 111321
www.minminas.gov.co

retrasan la ejecución de las metas previstas. *Presenta algún grado de Materialización de Riesgo* respecto del cumplimiento normativo y del procedimiento establecido. [Se identifica con el color **Amarillo**]

Alto: Significa que el tópico muestra un desarrollo, pero su funcionamiento causa problemas para la normal ejecución de la gestión. Si bien no impide el logro de los resultados, los retrasa de manera importante y sólo se obtienen de manera parcial. *Presenta Materialización de Riesgo* respecto del cumplimiento normativo y del procedimiento establecido. [Se identifica con el color **Rojo**]

6.2 MEDICIÓN DEL CONTROL

Se procedió a determinar si la variable analizada cuenta con control identificado en el Mapa de Riesgos o en el procedimiento documentado. Cuando no se encontró documentado el control, la Oficina de Control Interno procedió a describirlo con base en el riesgo identificado, para posteriormente analizarlo y determinar su **eficiencia.**

El criterio aplicado para determinar la *Eficiencia* o *Ineficiencia* del control descrito de la variable evaluada, correspondió a los siguientes parámetros de medición del control.

Control Eficiente: Cuando el control contribuye con la prevención de la materialización del riesgo inherente, indica que el control se aplica o es apropiado.

Control Ineficiente: Cuando el control no contribuye con la prevención de la materialización del riesgo inherente, indica que el control no se aplica, es ineficaz o inapropiado.

6.3 MEDICIÓN DE LA GESTIÓN

Con base en el análisis e impacto del resultado alcanzado por el ejecutor de la variable analizada, la materialización del riesgo inherente y la eficiencia del control, la Oficina de Control Interno procedió a establecer la **efectividad** de la gestión.

El criterio aplicado para determinar la Efectividad o No Efectividad de la gestión del ejecutor de la variable evaluada, correspondió a los siguientes parámetros.

Gestión Efectiva: Cuando la acción realizada condujo al logro de los resultados programados, a la observancia normativa o al cumplimiento del procedimiento establecido, a través del uso óptimo de los recursos utilizados[1], la no materialización del riesgo inherente o la eficiencia del control.

[1] Desde el punto de vista de la Economía, definida como la ausencia de desperdicio en la obtención de un resultado determinado. Glosario DAFP, del 6 de marzo de 2012

Calle 43 No 57-31 CAN Bogotá, Colombia
Conmutador (57 1) 2200 300
Código postal 111321
www.minminas.gov.co

Gestión No Efectiva: Cuando la acción realizada no condujo al logro de los resultados programados, a la observancia normativa o al cumplimiento del procedimiento establecido, viéndose afectada por la no utilización óptima de los recursos, la materialización del riesgo inherente o la ineficiencia del control.

6.4 VALIDACIÓN

La información contenida en el presente documento, surtió el proceso de validación con la Dirección de Hidrocarburos y el Grupo de Tecnologías de Información y Comunicación.

7. SISTEMA DE INFORMACIÓN

7.1 ANTECEDENTES DEL SISTEMA

El Sistema de Información de Combustibles Líquidos del Ministerio de Minas y Energía SICOM, es la única fuente de información oficial a la cual deben dirigirse todas las autoridades administrativas de cualquier orden, que requieran información de los Agentes de la Cadena de Distribución de combustibles en el país.

Este Sistema de Información integra a todos los agentes de la cadena a nivel nacional mediante el cual se organiza, controla y sistematiza la comercialización, distribución, transporte y almacenamiento de combustibles líquidos derivados del petróleo, alcohol carburante y biodiesel, adquirido a la firma Unión Soluciones y Energía desde el año 2009.

El Sistema de Información de Combustibles - SICOM, fue certificado por el Departamento Nacional de Estadística (DANE) en el proceso de *"Registro de Distribución de Combustibles Líquidos Derivados del Petróleo"* – por la calidad de la información, la cual permite al ciudadano realizar análisis y estadísticas de información, dado al cumplimiento de la ley 1712 de 2014 Transparencia y del Derecho de Acceso a la Información Pública Nacional y a la alta dirección del Ministerio de Minas y Energía, con el fin de tomar decisiones, basados en la información reportada por cada uno de los diferentes agentes que hacen parte de la cadena.

Este Sistema de Información integra todos los agentes de la cadena a nivel nacional mediante el cual se organiza, controla y sistematiza la comercialización, distribución, transporte y almacenamiento de combustibles líquidos derivados del petróleo, alcohol carburante y biodiesel desde el año 2009.

Calle 43 No 57-31 CAN Bogotá, Colombia
Conmutador (57 1) 2200 300
Código postal 111321
www.minminas.gov.co

La supervisión del Sistema de Información de Combustibles, es liderada por la Dirección de Hidrocarburos, quien realiza el seguimiento temático y el Grupo de Tecnologías de Información y Comunicación del Ministerio de Minas y Energía es el encargado de realizar el seguimiento técnico ambos mediante contrato GGC 230 de 2016 – Operabilidad del Sistema de Combustibles Líquidos SICOM, realizado la compañía Colombiana de Servicios de Valor Agregado y Telemáticos – COLVATEL S.A, el cual presta los servicios de operación y administración del Sistema.

La operación y administración del SICOM se encuentra tercerizada bajo la modalidad de servicio de hosting, servidor dedicado de aplicaciones en la ciudad de Bogotá, el cual comprende los siguientes elementos: Procesamiento, Licenciamiento integral, Conectividad y Comunicaciones, Centro de Procesamiento de Datos Principal, Centro de Procesamiento de datos Alterno, gestión documental y Call Center.

Toda la infraestructura necesaria para la operación del SICOM, es exclusiva para el servicio del Ministerio de Minas y Energía. El servicio ofrecido tiene disponibilidad 7*24*365.[2]

7.2 INFORMACIÓN CONTENIDA EN EL SISTEMA

El SICOM contiene información de todos los movimientos de combustibles líquidos derivados del petróleo, a nivel nacional, de todos los agentes de la cadena de distribución de combustibles - Importador, Refinador, Productor de alcohol y biodiesel, Distribuidor Mayorista, Grandes Consumidores y Distribuidores Minorista (Estaciones de Servicio de Aviación, Marítima, Fluvial, Automotriz y comercializador industrial).

A través de órdenes de pedido se registran los movimientos de combustible de todos los agentes de la cadena, importador, refinador, productor de alcohol y biodiesel, distribuidor mayorista, grandes consumidores y distribuidores minorista (EDS Aviación, marítima fluvial, automotriz y comercializador industrial), sin embargo no se registran importaciones o exportación de combustibles líquidos, así como ventas al consumidor final. No obstante, los agentes de la cadena realizan a través de la declaración de información mensual, reportan las importaciones y exportaciones que realizan.

7.3 ESTRUCTURA DEL SISTEMA DE INFORMACIÓN

El Sistema de Información de Combustibles Líquidos del Ministerio de Minas y Energías cuenta con los siguientes módulos principales:

[2] Servicio de disponibilidad y soporte al cliente del SICOM suministrado por Colvatel S.A

Calle 43 No 57-31 CAN Bogotá, Colombia
Conmutador (57 1) 2200 300
Código postal 111321
www.minminas.gov.co

- Módulo de Datos Generales, que permite el registro de datos del Agente como: Datos básicos del Agente, Acuerdos de compra, Documentos, Productos y Plantas de abastecimiento.

- Módulo de Declaración de Información, que permite el registro de la declaración de la información mensual como: Inventario, Recibo, Despacho, Uso, Carga a Planta y Declaración de Producción.

- Módulo Órdenes de Pedido, que permite el registro de los volúmenes de las transacciones de combustible entre el Cliente y el Proveedor: Orden Simple, Orden Múltiple, Orden Programada, Orden Anticipada, Transferencia y Traslados.

- Los Módulos de Configuración y de Seguridad, hacen parte de la Administración del Sistema.

El SICOM, tiene cuatro (4) Subsistemas en la solución que proveen su funcionalidad y se describen a continuación:

✓ Subsistema web de contenido (Portal SICOM)

Está compuesto por las páginas web del sitio http://www.sicom.gov.co, en él se puede acceder a las siguientes secciones:

- Inicio
- Objetivos y funciones
- Normas vigentes
- Preguntas frecuentes
- Trámites y servicios
- Contacto
- Área de niños y niñas
- Anuncios de rendición de cuentas

✓ Subsistema de información web (SICOM Transaccional)

Está compuesto por la aplicación SICOM transaccional por medio del cual se accede a través de la URL: https://www.sicom.gov.co/sicom.

✓ Subsistema de servicios web (Web Services SICOM)

Corresponde a servicios web con funcionalidad de la aplicación SICOM, que se exponen para que los grandes Agentes de la Cadena, integren sus sistemas de información propios al SICOM.

✓ Subsistema de inteligencia de Negocio (BI).

Calle 43 No 57-31 CAN Bogotá, Colombia
Conmutador (57 1) 2200 300
Código postal 111321
www.minminas.gov.co

Corresponde a distintos reportes y herramientas para el análisis masivo y especializado de la información del SICOM.

8. RESULTADOS DE LA AUDITORIA

8.1 FUNCIONALIDAD DE LOS MODULOS DEL SICOM

Riesgo Identificado por la Oficina de Control Interno: Que los módulos del sistema de Información de Combustibles Líquidos – SICOM, no cuenten con la funcionalidad adecuada para el cual fueron desarrollados.

Control Identificado por la Oficina de Control Interno: Verificar el funcionamiento efectivo de cada uno los Módulos del SICOM.

La OCI, en mesa de trabajo realizada el 14 de septiembre de 2018[3], revisó la funcionalidad de los Módulos a cargo de la Dirección de Hidrocarburos y el Grupo TIC, para identificar y revisar puntos de control relevantes en la gestión y mitigación del riesgo en la administración funcional del sistema de información SICOM. Los resultados del proceso se relacionan a continuación:

Para la validación de los resultados y determinar el nivel de riesgo de cumplimiento se tuvo en cuenta la metodología descrita en el numeral 6, del presente informe.

Verificación: La OCI verificó que el Sistema de Información “SICOM”, dispone de los siguientes módulos: Datos Generales, Declaración de Información, Ordenes de Pedido, Configuración y Seguridad; los cuales son funcionales y permiten verificar en tiempo real los movimientos de los procesos realizados a nivel nacional, obteniendo buenos tiempos de respuesta.

En mesa de trabajo realizada el día 14 de septiembre de 2018, se verificó el detalle de la información mediante consulta al módulo Datos Generales, permitiendo analizar el tiempo de respuesta y la calidad de la información suministrada, arrojando resultados detallados en cuanto a Datos generales del Agente con código SICOM: 635560, así como los acuerdos de compra realizados por el Agente, los Documentos Contractuales, Productos que maneja, el detalle de los transportes de combustibles realizados, su información de contacto, precios y ubicación, así como la respectiva Declaración de información en sus respectivos periodos de validación de la misma, evidenciando información clara y precisa respecto a la consulta realizada.

[3] Mesa de trabajo realizada con la dirección de Hidrocarburos y el Grupo TIC.

Calle 43 No 57-31 CAN Bogotá, Colombia
Conmutador (57 1) 2200 300
Código postal 111321
www.minminas.gov.co

Así mismo se realizó análisis al nivel de respuesta del aplicativo en ambientes de red local permitiendo verificar el desempeño del Sistema de información mediante las solicitudes hechas a consultas realizadas.

A continuación se relaciona la tabla de los cinco (5) módulos y el nivel de riesgo respecto a su funcionalidad.

FUNCIONALIDAD SICOM				
ITEM	MÓDULO	FUNCIONALIDAD		NIVEL DE RIESGO EVALUADO
		SI	NO	
1	Módulo Datos Generales	X		Bajo
2	Módulo Declaración de Información	X		Bajo
3	Módulo Ordenes de pedido	X		Bajo
4	Módulo de Configuración	X		Bajo
5	Módulo de Seguridad	X		Bajo

Fuente: Resultado de análisis funcional al SICOM por OCI

Observación: Los módulos del SICOM administrados por la Dirección de Hidrocarburos, se encuentran funcionando de conformidad con su diseño y desarrollo, realizando consultas en tiempo real por los distintos usuarios del Sistema.

De acuerdo con los resultados obtenidos de la verificación se determina que el riesgo *"Que los módulos del sistema de Información de Combustibles Líquidos no cuenten con la funcionalidad adecuada para el cual fueron desarrollados*, no se materializó, ubicándose en un nivel de riesgo bajo, permitiendo determinar que el control aplicado fue 100% eficiente y que la gestión fue 100% efectiva**.**

8.2 PLAN DE MEJORAS Y GESTIÓN DE CAMBIOS

Riesgo Identificado por la Oficina de Control Interno: Que el Sistema de Información de Combustibles Líquidos – SICOM, no cuente con un plan de mejoras y gestión de cambios.

Control Identificado por la Oficina de Control Interno: Verificar que se cuente con el procedimiento de plan de mejoras y gestión de cambios por parte del Ministerio de Minas y Energías y su debida ejecución.

Calle 43 No 57-31 CAN Bogotá, Colombia
Conmutador (57 1) 2200 300
Código postal 111321
www.minminas.gov.co

La Oficina de Control Interno, mediante solicitud escrita a las áreas de Dirección de Hidrocarburos y Grupo de Tecnologías de Información y Comunicación, solicitó la documentación requerida para analizar el cumplimiento por parte del Ministerio de Minas en cuanto a la puesta en marcha de un plan de mejoras y la gestión de cambios aplicada al Sistema de Información de Combustibles Líquidos SICOM.

Verificación: La Dirección de Hidrocarburos mediante radicado 2018067448 realizó el envío de la documentación requerida, entre ellos el documento de trazabilidad de control de cambios realizados al Sistema y mediante mesas de trabajo realizadas con las áreas auditadas, la OCI verifico el cumplimiento por parte del Ministerio de Minas y Energías en la ejecución de planes de mejora y gestión de cambios al Sistema de Información de Combustibles Líquidos.

Observación: El Sistema de Información de Combustibles Líquidos cuenta con la documentación requerida y la ejecución de Planes de mejora y gestión de cambios para la correcta funcionalidad del SICOM.

De acuerdo con los resultados obtenidos de la verificación se determina que el riesgo *"Que el Sistema de Información de Combustibles Líquidos – SICOM, no cuente con un plan de mejoras y gestión de cambios"*, no se materializó, ubicándose en un nivel de riesgo bajo, permitiendo determinar que el control aplicado fue 100% eficiente y que la gestión fue 100% efectiva.

8.3 REQUISITOS TÉCNICOS DE SEGURIDAD DEL SICOM

Criterio Normativo: Norma técnica colombiana NTC-ISO/IEC 27001 de 2013, Técnicas de Seguridad, Sistemas de gestión de la seguridad de la información, Requisitos para establecer, implementar, mantener y mejorar continuamente un Sistema de gestión de la Seguridad de la Información dentro del contexto de la organización.

Riesgo Identificado por la Oficina de Control Interno: Que no se cumplan los requisitos que gestionen la seguridad de la información del Sistema de Información de Combustibles Líquidos – SICOM.

Control Identificado por la Oficina de Control Interno: Verificar el cumplimiento de los requisitos para la gestión de la seguridad de la información contenida en el Sistema de Información de Combustibles Líquidos – SICOM.

La Oficina de Control Interno, mediante visitas técnicas realizadas los días 18 y 26 de septiembre a las Instalaciones de la compañía Colombiana de Servicios de Valor

Calle 43 No 57-31 CAN Bogotá, Colombia
Conmutador (57 1) 2200 300
Código postal 111321
www.minminas.gov.co

Agregado y Telemáticos – COLVATEL S.A, la cual presta los servicios de operación y administración del Sistema de Información de Combustibles Líquidos – SICOM, y a su vez, a las instalaciones donde se encuentra el Datacenter de TIVIT COLOMBIA S.A.S, firma encargada de suministrar el servicio de Hosting y servidor dedicado para la conectividad, comunicación y procesamiento de datos del Sistema de Información SICOM con el objetivo de verificar los niveles de seguridad y requisitos de cumplimiento para la gestión de la seguridad de la información.

Verificación: Durante la realización de la visita técnica, se verificó el cumplimiento de la normatividad vigente para los diferentes requisitos de validación en temas de seguridad informática, aplicando una lista de chequeo, evaluando los siguientes aspectos:

- Políticas de seguridad
- Organización de la seguridad
- Administración de activos
- Seguridad de los recursos humanos
- Seguridad física y del ambiente
- Gestión de las comunicaciones y operaciones
- Control de accesos
- Desarrollo y mantenimiento de los sistemas
- Administración de incidentes
- Gestión de continuidad del negocio

El resultado de la verificación técnica se encuentra consignado en el Anexo “Check List Análisis Técnico – SICOM”, el cual hace parte integral del presente informe.

Realizada la aplicación de la lista de chequeo se logra evidenciar lo siguiente acorde a los aspectos evaluados:

- **Políticas de Seguridad**: Se cuenta con la documentación requerida en cuanto a Políticas de Seguridad, los respectivos responsables y los procedimientos documentados para la ejecución de la misma.

- **Organización de la Seguridad**: Por parte de la administración del operador se encuentran definidos los roles y responsabilidades implicados en el tema de seguridad, así mismo se cuenta con las condiciones de seguridad establecidas con terceros.

  Se realizan procedimientos periódicos de análisis de vulnerabilidades al sistema, así mismo la procedencia de los ataques y la respectiva documentación requerida que permite realizar tomas de decisiones de lo

Calle 43 No 57-31 CAN Bogotá, Colombia
Conmutador (57 1) 2200 300
Código postal 111321
www.minminas.gov.co

expuesto junto con las debidas recomendaciones como resultado del proceso realizado.

- **Administración de Activos**: La administración de Activos informáticos se encuentra tercerizado con convenio interadministrativo con la compañía Colombiana de Servicios de Valor Agregado y Telemáticos – COLVATEL S.A y a su vez con TIVIT COLOMBIA S.A.S firma encargada del servicio de Hosting, Procesamiento de Datos y Comunicaciones del Sistema de Información.

- **Seguridad de los RRHH**: El Recurso humano encargado de la operación y administración del SICOM, es sujeto a pruebas de selección, permitiendo evidenciar el nivel de cumplimiento para los perfiles requeridos, así mismo cuentan con las responsabilidades Jurídicas y Contractuales requeridas, permitiendo salvaguardar la confidencialidad de los procesos realizados.

- **Seguridad Física y del Ambiente:** Colvatel S.A, cuenta el personal de seguridad responsable de velar por el correcto funcionamiento de la parte operativa en cuanto los niveles de seguridad establecidos para el correcto desempeño de sus funciones.

  El servicio de administración, soporte tecnológico y seguridad de medios informáticos se encuentra mediante Convenio Interadministrativo entre Colvatel S.A y TIVIT COLOMBIA S.A.S.

  - Las instalaciones del Datacenter cuentan con los requerimientos de Sismo Resistencia requeridos.
  - Cuenta con perímetro de seguridad de cerca eléctrica.
  - Las instalaciones cuenta con los requisitos exigidos por la Norma para la protección de equipos electrónicos procesadores de datos por computadora NFPA.
  - El suministro eléctrico es liderado por un Generador de 2 MW de potencia, así mismo 2 motores alternos con suministro de 72 horas e intermitencia de 20 segundos entre el cambio de un servicio a otro.
  - Se realiza Monitoreo permanente mediante CCTV en las distintas áreas, en especial aquellas de más alto flujo de personal.
  - Cuentan con 4 Bancos de Ups divididos en dos sectores, permitiendo redundancia interna dentro de las mismas máquinas y baterías.

- **Gestión de Comunicaciones y Operaciones:** La administración y operación del sistema se encuentra tercerizada a través de Colvatel S.A, mediante el contrato GGC 230 de 2016 y Otrosí No. 1, de ampliación de fecha de finalización de contrato a 31 de diciembre de 2018.

Calle 43 No 57-31 CAN Bogotá, Colombia
Conmutador (57 1) 2200 300
Código postal 111321
www.minminas.gov.co

Los niveles de respuesta entre la administración del Sistema, por parte de Colvatel S.A y lo requerido por parte del Ministerio de Minas y Energía y la Dirección de Hidrocarburos, cumple con lo exigido dado a los informes mensuales de ejecución que se envían al MME por parte del operador.

La Supervisión técnica del Sistema de Información está a cargo del Grupo de Tecnologías de Información y Comunicación del Ministerio de Minas y Energías.

La Supervisión temática del SICOM, está a cargo de la Dirección de Hidrocarburos del MME.

La implementación de Certificados SSL a nivel de aplicación se implementa con la finalidad de asegurar las transacciones realizadas en el Sistema de Información desde los distintos ámbitos de usabilidad.

- **Control de Accesos**: El Sistema de Seguridad Unificado (SSU) del SICOM, está formado por varios componentes de aplicación que garantizan la totalidad de los requisitos de seguridad.

  Los Datos de acceso de los usuarios del SICOM son encriptados antes de ser persistidos en la base de datos de la aplicación, garantizando así mismo la privacidad de la misma. Utilizan el estándar de encriptación digital (DES: Digital Encryption Standard).

- **Desarrollo y Mantenimiento de los Sistemas**: Colvatel S.A, cuenta con diferentes ambientes de Desarrollo para los procesos de Mejora y Modernización del Sistema de Información de Combustibles, así mismo con los requerimientos de seguridad en sus respectivos desarrollos, cumpliendo con los requisitos exigidos por parte del Ministerio de Minas y la Supervisión del Grupo Tic.

- **Administración de Incidentes**: La respuesta a incidentes es efectiva dado al servicio 7*24*365 suministrado por Colvatel S.A, con muy buenos tiempos de respuesta a eventualidades requeridas desde los diferentes ámbitos de usabilidad del Sistema.

- **Gestión de la Continuidad del Negocio:** El Ministerio de Minas y Energías, cuenta con procedimientos establecidos para la planificación y ejecución del Plan de Continuidad del negocio, realizando actividades con el Centro Alterno de Datos Pre, Durante y Post a eventualidades, arrojando resultados satisfactorios, quedando registrados en la documentación requerida.

Observación: El SICOM cumple con los requisitos para establecer, implementar, mantener y mejorar la gestión de la seguridad de la información, con base en la

Calle 43 No 57-31 CAN Bogotá, Colombia
Conmutador (57 1) 2200 300
Código postal 111321
www.minminas.gov.co

verificación de la lista de chequeo técnico aplicada, atendiendo los lineamientos de la Norma técnica colombiana NTC-ISO/IEC 27001 de 2013.

8.3.1 NIVEL DE CUMPLIMIENTO TÉCNICO.

Aplicado el análisis técnico y la lista de chequeo, la oficina de control interno procede a ponderar los resultados obtenidos mediante la evaluación realizada al nivel de seguridad implementado en la ejecución de los procedimientos que permitan brindar las garantías necesarias a salvaguardar la información procesada y almacenada por SICOM, así como los procedimientos de comunicación y demás aspectos evaluados.
El nivel de cumplimiento técnico, se genera a partir de los resultados obtenidos en la lista de chequeo aplicada a los procedimientos de seguridad y demás aspectos evaluados, como se describe en la siguiente gráfica.

Gráfica 1: Nivel de Cumplimiento análisis técnico – SICOM.

El resultado del nivel de cumplimiento técnico se encuentra consignado en el Anexo “Check List Análisis Técnico – SICOM”, el cual hace parte integral del presente informe.

Observación: Como resultado del análisis del nivel de cumplimiento se estableció el 98.9% de aplicación en los requisitos para establecer, implementar, mantener y mejorar los niveles de seguridad establecidos para la continua funcionalidad del SICOM y un 1.1% no aplicables al Sistema.

Calle 43 No 57-31 CAN Bogotá, Colombia
Conmutador (57 1) 2200 300
Código postal 111321
www.minminas.gov.co

De acuerdo con los resultados obtenidos en la verificación, se determina que el riesgo *"Que no se cumplan los requisitos que gestionen la seguridad de la información del Sistema de Información de Combustibles Líquidos – SICOM"*, no se materializó ubicándose en un nivel de riesgo bajo, permitiendo determinar que el control aplicado fue 100% eficiente y que la gestión fue 100% efectiva.

8.4 DOCUMENTOS DE APOYO Y MANEJO DEL SICOM

Riesgo Identificado por la Oficina de Control Interno: Que el Sistema de Información de Combustibles Líquidos – SICOM, no cuente con la documentación requerida para su respectivo uso y manejo.

Control Identificado por la Oficina de Control Interno: Verificar el cumplimiento y publicación por parte del SICOM de la documentación requerida para el correcto uso y manejo del mismo.

La Oficina de Control Interno, mediante solicitud escrita a las áreas de Dirección de Hidrocarburos y Grupo de Tecnologías de Información y Comunicación, solicitó la documentación requerida para analizar el cumplimiento por parte del SICOM, en cuanto a la documentación requerida para el correcto uso y manejo del Sistema de Información de Combustibles Líquidos SICOM.

Verificación: La Dirección de Hidrocarburos mediante radicado 2018067448 realizó el envío de la documentación requerida, entre ellos los Manuales de Usuario técnico y operativo y de sus respectivos módulos, así mismo la OCI verifico el cumplimiento en cuanto a la publicación a través del sitio web de la documentación de ayuda para el manejo y uso del Sistema de Información de Combustibles Líquidos.

Observación: El Sistema de Información de Combustibles Líquidos cuenta con la documentación requerida, manuales de usuario y de operatividad para el correcto uso y manejo de la herramienta.

De acuerdo con los resultados obtenidos de la verificación se determina que el riesgo *"Que el Sistema de Información de Combustibles Líquidos – SICOM, no cuente con la documentación requerida para su respectivo uso y manejo"*, no se materializó, ubicándose en un nivel de riesgo bajo, permitiendo determinar que el control aplicado fue 100% eficiente y que la gestión fue 100% efectiva.

Calle 43 No 57-31 CAN Bogotá, Colombia
Conmutador (57 1) 2200 300
Código postal 111321
www.minminas.gov.co

8.5 PLAN DE RECUPERACIÓN ANTE DESASTRES - DRP

Riesgo Identificado por la Oficina de Control Interno: Que el Sistema de Información de Combustibles Líquidos – SICOM, no cuente con un plan de recuperación ante desastres.

Control Identificado por la Oficina de Control Interno: Verificar el cumplimiento e implementación del plan de recuperación ante desastres que permita salvaguardar la operación y la información del SICOM.

La Oficina de Control Interno, solicitó a las áreas de Dirección de Hidrocarburos y Grupo de Tecnologías de Información y Comunicación, la documentación requerida para analizar el cumplimiento por parte del SICOM, en cuanto a la implementación del Plan de Recuperación de Desastres - DRP y su debida ejecución.

Verificación: La Dirección de Hidrocarburos mediante radicado 2018067448 realizó el envío del respectivo Plan de Recuperación de Desastres – DRP, así mismo la OCI verifico el cumplimiento en cuanto a los niveles de seguridad establecidos por el operador del SICOM, y la firma encargada del servicio de Hosting y comunicación, permitiendo mantener una actividad constante de monitoreo en cuanto a la funcionalidad del Sistema y los procedimientos de respuesta en eventualidad que permitan alternar la operación con el Centro alterno de datos.

Observación: El Sistema de Información de Combustibles Líquidos cuenta con la documentación del Plan de Recuperación ante Desastres - DRP, la respectiva implementación, permitiendo mantener la continua operación y salvaguardando la información del Sistema.

De acuerdo con los resultados obtenidos de la verificación se determina que el riesgo *"Que el Sistema de Información de Combustibles Líquidos – SICOM, no cuente con un plan de recuperación ante desastres"*, no se materializó, ubicándose en un nivel de riesgo bajo, permitiendo determinar que el control aplicado fue 100% eficiente y que la gestión fue 100% efectiva.

9. VALORACIÓN DEL RIESGO Y EFECTIVIDAD DE LA GESTIÓN

Con base en la evaluación realizada, la Oficina de Control Interno determinó la *Eficiencia* del control establecido para el cumplimiento de las variables analizadas,

Calle 43 No 57-31 CAN Bogotá, Colombia
Conmutador (57 1) 2200 300
Código postal 111321
www.minminas.gov.co

la valoración del *riesgo* inherente y la *Efectividad* de la gestión realizada, cuyo resultado se muestra en la siguiente tabla.

SISTEMA DE INFORMACIÓN DE COMBUSTIBLES LIQUIDOS DEL MME - SICOM	RIESGO IDENTIFICADO		
VARIABLE ANALIZADA	No Acoger Oportunidad de Mejoramiento OCI		
	Control Eficiente	Valoración del Riesgo	Gestión Efectiva
8.1 Funcionalidad de los Módulos del SICOM	Si	Bajo	Si
8.2 Plan de mejoras y gestión de cambios	Si	Bajo	Si
8.3 Requisitos técnicos y de seguridad del SICOM	Si	Bajo	Si
8.4 Documentos de apoyo y manejo del SICOM	Si	Bajo	Si
8.5 Plan de recuperación ante desastres - DRP	Si	Bajo	Si

Fuente: Valoración del riesgo en variables analizadas OCI

10. FIRMAS

GLADYS YOLANDA RAMOS QUINTERO.
Profesional especializada con asignación de funciones de Jefe de Oficina de Control Interno

ANDRO CABRALES ALVAREZ
Contratista Oficina de Control Interno

REZZAN LEONARDO CHAMORRO G.
Contratista Oficina de Control Interno

Calle 43 No 57-31 CAN Bogotá, Colombia
Conmutador (57 1) 2200 300
Código postal 111321
www.minminas.gov.co

11. ANEXO - CHECK LIST ANÁLISIS TÉCNICO – SICOM

Calle 43 No 57-31 CAN Bogotá, Colombia
Conmutador (57 1) 2200 300
Código postal 111321
www.minminas.gov.co

FORMULARIO ANÁLISIS TÉCNICO - SICOM

ITEM	ASPECTO EVALUADO				NIVEL DE CUMPLIMIENTO			OBSERVACIÓN
1	**POLÍTICAS DE SEGURIDAD**				SI	NO	N/A	
1,1	•Existen documento(s) de políticas de seguridad del SI	☑ VERDADERO	1		100,0%	0,0%	0,0%	Se cuenta con la documentación requerida en cuanto a Politicas de Seguridad, los respectivos responsables y los procedimientos documentados para la ejecución de la misma.
1,2	•Existe documentos de procedimientos relativos a la seguridad de SI	☑ VERDADERO	1					
1,3	•Existe un responsable de las políticas, normas y procedimientos	☑ VERDADERO	1					
1,4	•Existen mecanismos para la comunicación a los usuarios de las normas	☑ VERDADERO	1					
1,5	•Existen controles regulares para verificar la efectividad de las políticas	☑ VERDADERO	1					
			5					
2	**ORGANIZACIÓN DE LA SEGURIDAD**				SI	NO	N/A	
2,1	•Existen roles y responsabilidades definidos para las personas implicadas en la seguridad	☑ VERDADERO	1		100,0%	0,0%	0,0%	Por parte de la administración del operador se encuentran definidos los roles y responsabilidades implicados en el tema de seguridad, asi mismo se cuenta con las condiciones de seguridad establecidas con terceros. Se realizan procedimientos periodicos de análisis de vulnerabilidades al sistema, asi mismo la procedencia de los ataques y la respectiva documentación requerida que permite realizar tomas de decisiones de lo expuesto junto con las debidas recomendaciones como resultado del proceso realizado.
2,2	•Existe un responsable encargado de evaluar la adquisición y cambios de SI	☑ VERDADERO	1					
2,3	•La Dirección y las áreas de la Organización participa en temas de seguridad	☑ VERDADERO	1					
2,4	•Existen condiciones contractuales de seguridad con terceros y outsourcing	☑ VERDADERO	1					
2,5	•Existen programas de formación en seguridad para los empleados, clientes y terceros	☑ VERDADERO	1					
2,6	•Existe un acuerdo de confidencialidad de la información que se accesa.	☑ VERDADERO	1					
2,7	•Se revisa la organización de la seguridad periódicamente por una empresa externa	☑ VERDADERO	1					
			7					
3	**ADMINISTRACIÓN DE ACTIVOS**				SI	NO	N/A	
3,1	•Existen un inventario de activos actualizado	☑ VERDADERO	1		100,0%	0,0%	0,0%	La administración de Activos informaticos se encuentra tercerizado con convenio interadministrativo con la compañía Colombiana de Servicios de Valor Agregado y Telemáticos – COLVATEL S.A y a su vez con TIVIT COLOMBIA S.A.S, encargado del servicio de Hosting, Procesamiento de datos y Comunicaciones del Sistema de Información.
3,2	•El Inventario contiene activos de datos, software, equipos y servicios	☑ VERDADERO	1					
3,3	•Se lleva registro de cambio de activos si es requerido	☑ VERDADERO	1					
3,4	•Existe un responsable de los activos	☑ VERDADERO	1					
			4					
4	**SEGURIDAD DE LOS RRHH**				SI	NO	N/A	
4,1	•Se tienen definidas responsabilidades y roles de seguridad	☑ VERDADERO	1		88,9%	0,0%	11,1%	El Recurso humano encargado de la operaciòn y administración del SICOM, es sujeto a pruebas de selección, permitiendo evidneciar el nivel de cumplimiento para los perfiles requeridos, asi mismo cuentan con las responsabilidades Juridicas y Contractuales requeridas, permitiendo salvaguardar la confidencialidad de los procesos realizados. Colvatel S.A, cuenta el personal de seguridad responsable de velar por el correcto funcionamiento de la parte operativa en cuanto los niveles de seguridad establecidos para el correcto desempeño de sus funciones.
4,2	•Se tiene en cuenta la seguridad en la selección y baja del personal	☑ VERDADERO	1					
4,3	•Se plasman las condiciones de confidencialidad y responsabilidades en los contratos	☑ VERDADERO	1					
4,4	•Se imparte la formación adecuada de seguridad y tratamiento de activos	☐ NO APLICA	0					
4,5	•Existe un canal y procedimientos claros a seguir en caso de incidente de seguridad	☑ VERDADERO	1					
4,6	•Se recogen los datos de los incidentes de forma detallada	☑ VERDADERO	1					
4,7	•Informan los usuarios de las vulnerabilidades observadas o sospechadas	☑ VERDADERO	1					
4,8	•Se informa a los usuarios de que no deben, bajo ninguna circunstancia, probar las vulnerabilidades	☑ VERDADERO	1					
4,9	• Existe un proceso disciplinario de la seguridad de la información	☑ VERDADERO	1					
			8					
5	**SEGURIDAD FÍSICA Y DEL AMBIENTE**				SI	NO	N/A	
5,1	•Existe perímetro de seguridad física(una pared, puerta con llave).	☑ VERDADERO	1		100,0%	0,0%	0,0%	El servicio de administración, soporte tecnológico y seguridad de medios informáticos se encuentra mediante Convenio Interadministrativo entre Colvatel S.A y TIVIT. - Las instalaciones del Datacenter cuentan con los requerimientos de Sismo Resistencia requeridos. - Cuenta con perímetro de seguridad de cerca eléctrica. - Las instalaciones cuenta con los requisitos exigidos por la Norma para la protección de equipos electrónicos procesadores de datos por computadora NFPA. - El suministro eléctrico es liderado por un Generador de 2 MW de potencia, así mismo 2 motores alternos con suministro de 72 horas e intermitencia de 20 segundos entre el cambio de un servicio a otro. - Se realiza Monitoreo permanente mediante CCTV en las distintas areas, en especial aquellas de mas alto flujo de personal. - Cuentan con 4 Bancos de Ups divididos en dos sectores, permitiendo
5,2	•Existen controles de entrada para protegerse frente al acceso de personal no autorizado	☑ VERDADERO	1					
5,3	•Un área segura ha de estar cerrada, aislada y protegida de eventos naturales	☑ VERDADERO	1					
5,4	•En las áreas seguras existen controles adicionales al personal propio y ajeno	☑ VERDADERO	1					
5,5	•Las áreas de carga y expedición están aisladas de las áreas de SI	☑ VERDADERO	1					
5,6	•La ubicación de los equipos está de tal manera para minimizar accesos innecesarios.	☑ VERDADERO	1					
5,7	•Existen protecciones frente a fallos en la alimentación eléctrica	☑ VERDADERO	1					
5,8	•Existe seguridad en el cableado frente a daños e intercepciones	☑ VERDADERO	1					
5,9	•Se asegura la disponibilidad e integridad de todos los equipos	☑ VERDADERO	1					
5,10	•Existe algún tipo de seguridad para los equipos retirados o ubicados exteriormente	☑ VERDADERO	1					

5,11	•Se incluye la seguridad en equipos moviles	☑VERDADERO	1					redundancia interna dentro de las mismas maquinas y baterias.
			11					
6	**GESTIÓN DE COMUNICACIONES Y OPERACIONES**				**SI**	**NO**	**N/A**	
6,2	•Estan establecidas responsabilidades para controlar los cambios en equipos	☑VERDADERO	1					
6,3	•Estan establecidas responsabilidades para asegurar una respuesta rápida, ordenada y efectiva frente a incidentes de seguridad	☑VERDADERO	1					La administración y operación del sistema se encuentra tercerizada a través de Colvatel S.A, mediante el contrato GGC 230 de 2016 y Otrosi No. 1, de amplación de fecha de finalización de contrato a 31 de diciembre de 2018.
6,5	•Existen contratistas externos para la gestión de los Sistemas de Información	☑VERDADERO	1					
6,6	•Existe un Plan de Capacidad para asegurar la adecuada capacidad de proceso y de almacenamiento	☑VERDADERO	1					Los niveles de respuesta entre la administración del Sistema, por parte de Colvatel S.A y lo requerido por parte del Ministerio de Minas y Energía y la Dirección de Hidrocarburos, cumple con lo exigido dado a los informes mensuales de ejecución que se envían al MME por parte del operador.
6,7	•Existen criterios de aceptación de nuevos SI, incluyendo actualizaciones y nuevas versiones	☑VERDADERO	1					
6,8	•Controles contra software maligno	☑VERDADERO	1					
6,9	•Las copias de backup de la información se realizan periodicamente	☑VERDADERO	1					
6,10	•Existen logs para las actividades realizadas por los operadores y administradores	☑VERDADERO	1		100,0%	0,0%	0,0%	La Supervisión tecnica del Sistema de Información está a cargo del Grupo de Tecnologías de Información y Comunicación del Ministerio de Minas y Energías.
6,11	•Existen logs de los fallos detectados	☑VERDADERO	1					
6,12	•Existen rastro de auditoría	☑VERDADERO	1					
6,13	•Hay controles establecidos para realizar la gestión de los medios informáticos.(cintas, discos, removibles, informes impresos)	☑VERDADERO	1					La Supervisión temática del SICOM, está a cargo de la Direción de Hidrocarburos del MME.
6,14	•Existen acuerdos para intercambio de información y software	☑VERDADERO	1					
6,15	•Existe interoperatibilidad con otros Sistemas de Información	☑VERDADERO	1					
6,16	•Implementan el uso de Certificados SSL para la transmision de datos entre el Servidor y el Usuario	☑VERDADERO	1					La implementación de Certificados SSL a nivel de aplicación se emplementa con la finalidad de asegurar las transaciones realizadas en el Sistema de Información desde los distintos ambitos de usabilidad.
6,17	•Existen medidas de seguridad en las transacciones en linea	☑VERDADERO	1					
6,18	•Se monitorean las actividades relacionadas a la seguridad	☑VERDADERO	1					
			16					
7	**CONTROL DE ACCESOS**				**SI**	**NO**	**N/A**	
7,1	•Existe una política de control de accesos	☑VERDADERO	1					El Sistema de Seguridad Unificado (SSU) del SICOM, está formado por varios componentes de aplicación que garantizan la totalidad de los requisitos de seguridad
7,2	•Existe un procedimiento formal de registro y baja de accesos	☑VERDADERO	1					
7,3	•Se controla y restringe la asignación y uso de privilegios en entornos multi-usuario	☑VERDADERO	1					
7,4	•Existe una gestión de los password de usuarios	☑VERDADERO	1		100,0%	0,0%	0,0%	Los Datos de acceso de los usuarios del SICOM son encriptados antes de ser persistidos en la base de datos de la aplicación, garantizando así mismo la privacidad de la misma. Utilizan el estándar de encriptación digital (DES: Digital Encryption Standard).
7,7	•Existe una autenticación de usuarios en conexiones externas	☑VERDADERO	1					
7,8	•Existe un control de la conexión de redes	☑VERDADERO	1					
			6					
8	**DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS**				**SI**	**NO**	**N/A**	
8,1	•Existen controles criptográficos.	☑VERDADERO	1					Colvatel S.A, cuenta con diferentes ambientes de Desarrollo para los procesos de Mejora y Modernización del Sistema de Información de Combustibles, asi mismo con los requerimientos de seguridad en sus respectivos desarrollos, cumpliendo con los requisitos exigidos por parte del Ministerio de Minas y la Supervisión del Grupo Tic.
8,2	•Existe una separación de los entornos de desarrollo y producción	☑VERDADERO	1					
8,4	•Existen controles de seguridad para los resultados de los sistemas	☑VERDADERO	1		100,0%	0,0%	0,0%	
8,5	•Existe la gestión de cambios documentada	☑VERDADERO	1					
8,6	•Se controlan las vulnerabilidades de los equipos	☑VERDADERO	1					
			5					
9	**ADMINISTRACIÓN DE INCIDENTES**				**SI**	**NO**	**N/A**	
9,1	•Se comunican los eventos de seguridad	☑VERDADERO	1					
9,2	•Se comunican los debilidades de seguridad	☑VERDADERO	1					La respuesta a incidentes es efectiva dado al servicio 7*24*365 suministrado por Colvatel S.A, con muy buenos tiempos de respuesta a eventualidades requeridas desde los diferentes ambitos de usabilidad del Sistema.
9,3	•Existe definidas las responsabilidades antes un incidente.	☑VERDADERO	1		100,0%	0,0%	0,0%	
9,4	•Existe un procedimiento formal de respuesta	☑VERDADERO	1					
9,5	•Existe la gestión de incidentes	☑VERDADERO	1					
			5					
10	**GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO**				**SI**	**NO**	**N/A**	
10,1	•Existen procesos para la gestión de la continuidad.	☑VERDADERO	1					El Ministerio de Minas y Energías, cuenta con procedimientos establecidos para la planificación y ejecución del Plan de Continuidad del negocio, realizando actividades con el Centro Alterno de Datos Pre, Durante y Post a eventualidades, arrojando resultados satisfactorios, quedando registrados en la documentación requerida.
10,2	•Existe un plan de continuidad del negocio y análisis de impacto	☑VERDADERO	1					
10,3	•Existe un diseño, redacción e implantación de planes de continuidad	☑VERDADERO	1		100,0%	0,0%	0,0%	
10,4	•Existe un marco de planificación para la continuidad del negocio	☑VERDADERO	1					
10,5	•Existen prueba, mantenimiento y reevaluación de los planes de continuidad del negocio.	☑VERDADERO	1					
			5					

RESULTADOS AUTODIAGNÓSTICO
GENERAL

Nivel de Cumplimiento		
SI	NO	N/A
98,9%	0,0%	1,1%