LQ COLOMBIA
REVISORES FISCALES & AUDITORES EXTERNOS

Bogotá D.C., 07 junio de 2023
L&Q-12796-23

Señores:
CPIP- CONSEJO PROFESIONAL DE INGENIERÍA DE PETRÓLEOS
Atn. Sr. Manuel Guillermo Hoyos Trujillo
Representante Legal
Ciudad.

ASUNTO: INFORME DE RECOMENDACIONES PARA FORTALECER LA SEGURIDAD Y CONTROLES GENERALES EN LOS SISTEMAS DE INFORMACIÓN

Respetados señores:

Para su conocimiento y fines pertinentes, estamos enviando el informe de recomendaciones para fortalecer las seguridades y controles en los sistemas de información.

Es prudente mencionar que nuestra labor se desarrolló de acuerdo con las normas de auditoría generalmente aceptadas en Colombia, utilizando los procedimientos y pruebas que aconseja la profesión y con base en pruebas selectivas, lo que hace que el cumplimiento de la auditoría no sea el cien por ciento de los aspectos relacionados con las seguridades y controles, sino una selección técnica de ellos.

La auditoría fue realizada el 25 de abril por medio de la plataforma Meet, atendida por el Ingeniero Misael Regino Arroyo y demás colaboradores la socialización de los hallazgos mencionados el día 18 de mayo de 2023 en presencia del ingeniero Alberto Valencia y demás colaboradores

Elaborado por:
LYNA MARGARYTA COY VILLANUEVA

7/06/2023 16:08
Design By:
LQ Revisores Fiscales,
Auditores Externos S.A.S.

COLOMBIA

ACTIVIDADES DESARROLLADAS:

La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización. Así pues, estos tres términos constituyen la base sobre la que se cimienta todo el edificio de la seguridad de la información:

- **Confidencialidad**: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.

- **Integridad**: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

- **Disponibilidad**: acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

Como resultado de estas actividades fueron identificados los siguientes hallazgos y observaciones:

I. POLÍTICAS DE SEGURIDAD

Sustento Conceptual

La política de seguridad es un instrumento que desarrolla todos los objetivos de seguridad de la empresa, tiene que mostrar el compromiso de la alta dirección para cumplir con los requisitos de todas las partes interesadas y mejorar de forma continua el Sistema de Gestión de Seguridad de la Información.

La política se debe comunicar dentro de la organización y a todas las partes interesadas, la mejor práctica es definir quién es el responsable de la comunicación, administración y actualización, la política debe ser revisada de forma continua por parte del encargado y ser del conocimiento de la alta dirección de la organización. Esto garantiza el compromiso por parte de la empresa, que es el factor clave para conseguir el éxito.

La creación de indicadores de gestión está orientada principalmente en la medición de efectividad, eficiencia y eficacia de los componentes de implementación y gestión definidos en el modelo de operación del marco de seguridad y privacidad de la información, servirán como insumo para el componente de mejora continua permitiendo adoptar decisiones de mejora. Los objetivos de estos procesos de medición en seguridad de la información son:

- Evaluar la efectividad de la implementación de los controles de seguridad
- Evaluar la eficiencia del Modelo de Seguridad y Privacidad de la Información al interior de la entidad.
- Proveer estados de seguridad que sirvan de guía en las revisiones del Modelo de Seguridad y Privacidad de la Información, facilitando mejoras en seguridad de la información y nuevas entradas a auditar.
- Comunicar valores de seguridad al interior de la entidad.
- Servir como insumos al plan de análisis y tratamiento de riesgos.

Hallazgos

A la fecha de la auditoría se observó que:

1. No existe una política especifica de seguridad asociada a sistemas informáticos
2. No existen mecanismos para la comunicación a los usuarios de las normas sobre S Aquí falto concluir la frase

Riesgos

Afrontar crecimiento de problemas de seguridad internos, tales como intrusiones, robo de información falta de gestión y evolución del modelo de seguridad y privacidad de la información al interior de una entidad de acuerdo con sus políticas.

Oportunidades de Mejora

La Revisoría Fiscal sugiere a la administración de **CPIP:**

1. Implementar una política relaciona a lineamientos de seguridad de la información acorde a la infraestructura y recursos del club del comercio. ¿Què tiene que ver el Club del Comercio con el CPIP?
2. Crear estrategia para comunicar y compartir con sus funcionarios la política de seguridad.
3. Crear mecanismos para verificar el cumplimiento de esta política.

II. GESTIÓN DE CONTINUIDAD

A. Respuesta a incidentes

Sustento Conceptual

El objetivo principal de un modelo de respuesta a Incidentes de seguridad de la información es tener un enfoque estructurado y bien planificado que permita:

- Administrar adecuadamente los eventos tecnológicos.
- Gestionar los incidentes de seguridad de la información
- Integrar los procedimientos de atención para estos dos tipos de sucesos

Es conveniente establecer el reporte formal del evento y procedimientos de contingencia; Todos los empleados, contratistas y usuarios de terceras partes deben tener conciencia sobre los procedimientos para el reporte de los diferentes tipos de evento y las debilidades que puedan tener impacto en la seguridad de los activos de la organización.

Hallazgos

A la fecha de auditoría se observó que el **CPIP,** no cuenta con un procedimiento formal de respuesta ante incidentes de seguridad de la información e informática.

Riesgos

El **CPIP** no está preparada para afrontar la contención, erradicación y recuperación de eventualidades en la seguridad de la información, ya que no está definiendo las responsabilidades y procedimientos para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.

Oportunidades de mejora

La Revisoría Fiscal sugiere a la administración de **CPIP,** establecer un documento formal para la gestión de incidentes de seguridad.

B. Matriz de Riesgos vs Controles
Sustento Conceptual

Definir el plan de tratamiento de riesgos que hacen parte del Sistema de Gestión de Seguridad de la Información, para así aplicar los controles con los cuales se buscan mitigar los riesgos, de esta forma se busca que, mediante el tratamiento de los riesgos y la mejora continua de la Seguridad y Privacidad de la Información, las partes interesadas tengan mayor confianza en el tratamiento de la información que se almacena y maneja en la Entidad.

Una matriz de riesgo identifica las actividades de una empresa, clasifica el tipo de riesgo según su intensidad y los diferentes factores que pueden producirlo. Del mismo modo, la matriz posibilita medir la efectividad de una gestión de riesgo adecuada.

A partir de la información documentada en la matriz, se diagnostica la situación de riesgo de una entidad. Por tanto, este método debe abarcar los diferentes frentes de negocio de una empresa con el fin de comparar los proyectos, las áreas, los productos y los procesos**.**

Hallazgos

A la fecha de auditoría se observó que en **CPIP**, aunque existe una matriz de riesgos frente a los controles, en ella no se contemplan todos los riesgos y tampoco todos los controles frente a incidentes de seguridad de la información, algunas acciones no están actualizadas a los procesos e infraestructura actuales

Riesgos

La ausencia de métodos de identificación, el análisis, la evaluación de riesgos y controles que permitan reaccionar ante una posible materialización del riesgo, puede traer consecuencias graves, como pérdida fuga o robo de información, alteración de documentos, negación de servicios etc.

Oportunidades de mejora

La Revisoría Fiscal sugiere a la administración de **CPIP,** definir todos los riegos y sus respectivos controles dentro de la matriz para poder identificar los riesgos a los que están expuestos los sistemas de información de acuerdo a sus recursos e infraestructura y las tareas para mitigarlos.

III. MANTENIMIENTO DE EQUIPOS

A. Mantenimiento de software y hardware.

Sustento Conceptual

Gran parte de los problemas que se presentan en los sistemas de cómputo se pueden evitar o prevenir si se realiza un mantenimiento periódico de cada uno de sus componentes. El mantenimiento preventivo se refiere a todas las acciones que garantían y optimizan el funcionamiento del equipo electrónico

Hallazgos

A la fecha de auditoría se observó que no se tiene establecido un cronograma de mantenimiento preventivo del hardware y software de sus equipos de cómputo ni se tiene registro de la actividad realizada.

Riesgos

Los equipos pueden presentar fallas tanto de software o hardware; el rendimiento y desempeño de estos equipos se ve directamente afectado.

Oportunidades de mejora

La Revisoría Fiscal sugiere a la administración de **CPIP**, realizar un mantenimiento preventivo periódico y llevar un registro de las operaciones de mantenimiento, en el que se reflejen los resultados de las tareas realizadas, se enumeren las operaciones de mantenimiento para cada elemento, debiendo figurar información sobre: tipo de mantenimiento y ubicación, responsable del mantenimiento, fecha de ejecución, operaciones realizadas, lista de materiales sustituidos, cuando sea el caso, y todas las observaciones que se consideren oportunas.

.

IV. BACKUP (COPIAS DE RESPALDO DE LA INFORMACIÓN)

Sustento Conceptual

El respaldo de información es la copia de los datos importantes de un dispositivo primario en uno ó varios dispositivos secundarios, ello para que en caso de que el primer dispositivo sufra una avería electromecánica ó un error en su estructura lógica, sea posible contar con la mayor parte de la información necesaria para continuar con las actividades rutinarias y evitar pérdida generalizada de datos.

Además, cuando se presenta un incidente o una interrupción que requiera la activación de un plan de recuperación o continuidad, generalmente, una de las actividades primordiales está relacionada con el uso de respaldos de información. En ese sentido, Los backup de información resultan de vital importancia en el contexto de la continuidad del negocio, que busca restaurar las actividades críticas en un tiempo prudente y regresar a la normalidad de las operaciones de manera progresiva.

Hallazgos

A la fecha de auditoría se observó que en **CPIP,** la política no define claramente los procedimientos, condiciones, y cronograma de ejecución de las copias de respaldo de la información.

Riesgos

CPIP, está expuesta a perder de forma parcial o total su información al no tener copias regulares de seguridad de su información.

Oportunidades de mejora

La Revisoría Fiscal sugiere a la administración de **CPIP,** definir un cronograma claro para la ejecución de las copias de respaldo de información

OBSERVACIONES

1. Se recomienda firmar un acuerdo de confidencialidad con el contratista que manejan para soporte ocasional
2. Se debe revisar la seguridad en las copias generadas en los discos duros.

¿ESTAS SON OBSERVACIONES O SON RECOMENDACIONES?

POR FAVOR PROFUNDIZAR EN LO QUE SE ESTA SUGIRIENDO QUE SE HAGA O IMPLEMENTE

REFERENCIAS

Cisco y/o sus filiales. (2014). Cinco pasos para la protección del Data Center: Las soluciones de seguridad tradicionales pueden no ser suficientes, 1–6.

ESET. (2018). Contenido. *ESET Security Report 2018*, 1–16.

Alzate, A. T. U. N. de C. S. M. (1998). Planeación estratégica de sistemas de información, (2).

IFS. (2017). Investigaciones de causa de incendio _ Instituto para la Prevención de Pérdidas e Investigación de Daños de Aseguradoras Públicas eV.