AUDITORIA DE SEGUIMIENTO A MATRICES DE RIESGOS

Empresa: PEOPLE CONTACT S.A.S. EN REESTRUCUTRACION
Unidad auditable: Todos los procesos
Auditor delegado: Ricardo Stoltze
Fecha de corte: agosto 31 de 2024

ISR-PCS-240924

Manizales, 3 de septiembre de 2024

Señores
PEOPLE CONTACT S.A.S. EN REESTRUCUTRACION
Doctor: Juan José Silva Serna
Gerente
Manizales, Caldas

Asunto: Auditoría de seguimiento a matrices de riesgos

De manera muy cordial presentamos nuestro informe resultante de la revisión efectuada al proceso de tratamiento de riesgos de la entidad.

Es importante indicar que el objetivo general del trabajo efectuado, consistió en revisar el estado actual de la matriz de riesgos de la entidad teniendo en cuenta los procedimientos y las normas aplicables a la entidad.

De acuerdo con lo anterior, se adelantó un trabajo de auditoría siguiendo las actividades de diagnóstico y evaluación con el fin de determinar el nivel de madurez del mismo y generar las acciones de mejora correspondientes.

Se precisa que nuestra labor fue ejecutada bajo la técnica de muestreo y áreas críticas, por tal motivo, podría o no detectarse errores materiales o ausencia de controles, dado que la revisión no abordó la totalidad de las operaciones ejecutadas en **PEOPLE CONTACT**, en consecuencia es la administración y los funcionarios en quien ella delegue, los responsables de velar porque las operaciones ejecutadas se efectúen con las técnicas de calidad profesionalmente admisibles, y que las actividades de control desarrolladas de manera rutinaria al interior de la entidad, sean efectivas, eficaces y concluyentes, de tal manera que se salvaguarden los intereses comunes y corporativos, en procura de minimizar errores y de mitigar riesgos, de manera tal, que se proteja el patrimonio del ente económico.

Para fines de comprensión nuestros informes están sometidos a la respectiva socialización y conocimiento previo por parte de los administradores y líderes de cada proceso, quienes, en ejercicio de su derecho de controversia o contradicción, pueden establecer disposiciones sobre nuestras valoraciones u observaciones técnicas de las cuales se deja evidencia en los informes emitidos. Lo antes expuesto, no significa, que aceptemos o estemos de acuerdo con las mismas, y mucho menos que la inclusión de éstas, en dichos documentos, se conviertan en una medida de retractación o de corrección por parte nuestra.

Así las cosas, cumpliendo con nuestras políticas internas el presente escrito se envía como un **informe en etapa definitivo** por cuanto fue socializado con los líderes delegados por la entidad.

Agradecemos la colaboración y oportunidad brindada por el equipo de trabajo de **PEOPLE CONTACT** en el desarrollo de la auditoría.

Atentamente,

RICARDO F. STOLTZE CARMONA
Asesor delegado Control Interno
Socio – Gerente general
En Representación de Auditores y Consultores - Audicons S.A.S.

1. OBJETIVOS

El objetivo general de la revisión de un mapa de riesgos y su tratamiento es identificar, evaluar, priorizar y gestionar de manera efectiva los riesgos que podrían afectar el cumplimiento de los objetivos de la entidad. Este proceso tiene como finalidad asegurar que los riesgos sean manejados de manera proactiva y oportuna, minimizando su impacto negativo y maximizando las oportunidades, contribuyendo así a la sostenibilidad y éxito de la organización. Esto implica actualizar la información, mejorar las estrategias de mitigación y garantizar la adecuación de las respuestas planificadas a los riesgos identificados.

2. ALCANCE

- ✓ Evaluación de Riesgos Existentes: Reexaminar los riesgos previamente identificados para determinar si su probabilidad de ocurrencia y su impacto han cambiado, y ajustar su clasificación en consecuencia.
- ✓ Eficacia de las Medidas de Mitigación: Analizar la efectividad de las estrategias y controles implementados para mitigar los riesgos, y determinar si necesitan ser modificados o reforzados.
- ✓ Actualización de Planes de Tratamiento: Revisar y actualizar los planes de tratamiento de riesgos para asegurar que las acciones sean pertinentes y estén alineadas con los objetivos actuales de la organización.
- ✓ Monitoreo Continuo: Establecer o mejorar los mecanismos de monitoreo continuo para detectar cambios en el entorno que puedan afectar la naturaleza o el impacto de los riesgos.
- ✓ Cumplimiento Normativo y Regulatorio: Asegurar que la gestión de riesgos cumpla con las normativas, leyes y estándares relevantes, y que esté alineada con las mejores prácticas.
- ✓ Comunicación y Reportes: Revisar los canales de comunicación y los informes relacionados con los riesgos para garantizar que la información crítica llegue a las partes interesadas de manera oportuna y clara.
- ✓ Capacitación y Conciencia: Evaluar la necesidad de capacitación adicional para el personal sobre la gestión de riesgos, asegurando que todos los miembros relevantes de la organización comprendan su papel en la mitigación y tratamiento de riesgos.

3. ASPECTOS LEGALES

En consideración con lo señalado en el alcance de este informe, se tuvieron en cuenta las buenas prácticas establecidas en las normas de auditoría consagradas en el Marco Internacional para la Práctica Profesional de Auditoría - MIPP, que rigen el ejercicio de la labor, como es entre otras: la planeación, realización de la evaluación, determinación de los resultados, efectuar una evaluación equilibrada de todas las circunstancias relevantes y brindar una opinión con integridad, independencia, prudencia y objetividad.

- ✓ Guía para la administración del riesgo.
- ✓ NTC-ISO 31000:2018 Gestión del riesgo. Directrices.
- ✓ ISO 31000 señala una familia de normas sobre gestión del riesgo, normas codificadas por la International Organization for Standardization.
- ✓ ISO 31000:2009 es proporcionar principios y directrices para la gestión de riesgos y el proceso implementado en el nivel estratégico y operativo.

4. INFORME EJECUTIVO

4.1. OPORTUNIDADES DE MEJORA

Prioridad	Descripción
Alta	Requiere intervenciones o ajustes en el corto plazo (menos de 1 mes).
Media	Requiere intervenciones o ajustes en el mediano plazo (entre 6 meses y un año).
Baja	Requiere intervenciones o ajustes menores.

Del análisis resultante, se lograron detectar las siguientes situaciones:

4.1.1. OBSERVACIÓN: MATRIZ DE RIESGOS POR PROCESOS

Prioridad	Descripción
Media	Requiere intervenciones o ajustes en el mediano plazo (entre 6 meses y un año).

Una vez evaluada la matriz de riesgos por procesos, donde se evaluó el tratamiento de los riesgos aleatoriamente por la presente auditoría, se identificaron las siguientes situaciones:

- ✓ Se observa que la matriz de riesgos, no es actualizada desde el ultimo seguimiento por parte de control interno, el cual data de abril de 2024.
- ✓ No todos los riesgos identificados son claros, debido a que los mismos no cuentan en su totalidad o son confusos en los elementos que configuran la estructura de un riesgo, como son:
  - Activo comprometido: los recursos tangibles o intangibles con los que cuenta la empresa y que tienen valor, los cuales pueden verse comprometidos.
  - Vulnerabilidad: Exposición a un riesgo, debilidad, fallo o hueco de seguridad detectado en alguna organización, proceso, procedimiento, programa o sistema
  - Causa: Motivo, razón o circunstancia por la cual se genera algo.
  - Agente generador (Amenazas): Cualquier situación, evento o ente con potencial de daño, que pueda presentarse. Todas aquellas personas, cosas, eventos, acciones o circunstancias que tienen la capacidad de generar un riesgo.
  - Consecuencia o efecto: Es el producto de un evento expresado cualitativa o cuantitativamente, sea este una pérdida, perjuicio, desventaja o ganancia.
- ✓ No se evidencia un seguimiento y resulados de los controles establecidos, donde a través de un informe o control de cambios, se puede visualizar si los controles son efectivos o no.
- ✓ Algunos controles establecidos para los riesgos evaluados, no se configuran como la medida que modifica o mitiga el riesgo.
- ✓ Se observa tratamiento de riesgos incompletos, por locual no es posible identificar el riesgo residual.
- ✓ No se utiliza una metodología del tratamiento de riesgos del sector publico o aplicando buenas prácticas como el marco de referencia NTC-ISO 31000.
- ✓ No hay un glosario y diccionario de datos que ilustre las formulas utilizadas.
- ✓ No se observa una representación gráfica de los riesgos, donde se permite vincular la probabilidad de ocurrencia y su impacto en forma clara y objetiva.
- ✓ Existente riesgos no controlados.
- ✓ La matriz de riesgos no se encuentra normalizada, asimismo, no hay evidencia del conocimiento y participación de todos los procesos.

Recomendación:

Cabe resaltar que la presente auditoría, eligió varios riesgos de esta matriz, no obstante, es importante que el área responsable de la gestión del riesgo, revise la totalidad de las matrices por procesos, para ajustar y actualizar.

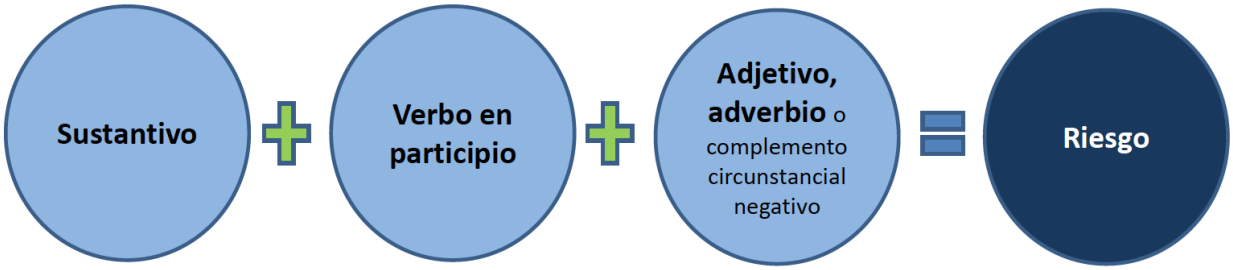
- ✓ Utilizar una metodología como la Guía para la administración del riesgo o la NTC-ISO 31000.
- ✓ Utilizar la metodología MAGERIT V3: Siguiendo la terminología de la normativa ISO 31000, MAGERIT responde al Proceso de Gestión de Riesgos dentro de un marco de trabajo para que las partes interesadas tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información.

Según las buenas prácticas y el marco de referencia NTC-ISO 31000, se debe tener en cuenta los siguientes aspectos para una adecuada gestión del riesgo:

- ✓ Es importante entonces que, al momento de configurar el riesgo de acuerdo a los elementos anteriormente expuestos, se identifique lo siguiente: Cuando una amenaza explota y/o aprovecha una vulnerabilidad, generando consecuencias negativas sobre cualquier tipo de activo.
- ✓ Identificación del riesgo. Proceso para encontrar, reconocer y describir el riesgo. La identificación de las fuentes de riesgo, los eventos, sus causas y sus consecuencias potenciales.
- ✓ La identificación del riesgo puede involucrar datos históricos, análisis teóricos, opiniones informadas y expertas, y las necesidades de las partes involucradas.
- ✓ Redacte de forma clara, específica y directa sin dar lugar a ambigüedades.
- ✓ Procure evitar calificativos como “malo” o “poco”; prefiera otros más precisos como “deficiente”, “insuficiente” o “ineficiente”
- ✓ No redacte comenzando como “falta de…” u otras frases similares que llevan implícito el sesgo hacia una supuesta solución particular.

Estructura o redacción de un riesgo.

CONTROL INTERNO



- ✓ Evaluar de forma individual cada riesgo en la severidad de su grado de probabilidad e impacto de ocurrencia. Es importante involucrar los dos calificativos.
- ✓ La etapa de tratamiento del riesgo, es un proceso para modificar el riesgo, por esta razón el tratamiento del riesgo puede implicar:
  - ✓ evitar el riesgo decidiendo no iniciar o continuar la actividad que lo originó;
  - ✓ tomar o incrementar el riesgo con el fin de perseguir una oportunidad;
  - ✓ retirar la fuente del riesgo;
  - ✓ cambiar la probabilidad;
  - ✓ cambiar las consecuencias;

- ✓ compartir el riesgo con una o varias de las partes (incluyendo los contratos y la financiación del riesgo); y
- ✓ retener el riesgo a través de la decisión informada.

✓ Para una adecuada gestión del riesgo, se debe tener en cuenta las ppropiedades de los riesgos:
- ✓ Es algo que se ubica en el futuro, no en el presente.
- ✓ Es algo que posiblemente ocurra, aunque no hay certeza de que ocurra.
- ✓ Es algo que potencialmente es perjudicial, no es necesariamente beneficioso o neutro.
- ✓ Es algo que con el tiempo puede crecer, decrecer, desaparecer o concretarse.

✓ Es recomendable incluir una representación gráfica de los riesgos, donde se permite vincular la probabilidad de ocurrencia y su impacto en forma clara y objetiva.

✓ Elaborar el diccionario de datos de la matriz de riesgos.

Comentario del auditado – Leandro López Gómez - Director de Planeación y Mejora Continua:

Se pueden radicar los informes en definitivo, entendiendo que los planes de acción se diseñarán de acuerdo con las observaciones presentadas por ustedes y la pertinencia de acuerdo con nuestra naturaleza.

4.1.2. OBSERVACIÓN: MATRIZ DE RIESGOS DE CORRUPCIÓN

Prioridad	**Descripción**
Media	Requiere intervenciones o ajustes en el mediano plazo (entre 6 meses y un año).

Una vez evaluada la matriz de riesgos de corrupción, donde se evaluó el tratamiento de los riesgos aleatoriamente por la presente auditoría, se identificaron las siguientes situaciones:

- ✓ Se observa que la matriz de riesgos, no es actualizada desde el ultimo seguimiento por parte de control interno, el cual data de abril de 2024.
- ✓ No todos los riesgos identificados son claros, debido a que los mismos no cuentan en su totalidad o son confusos en los elementos que configuran la estructura de un riesgo, como son:
  - Activo comprometido: los recursos tangibles o intangibles con los que cuenta la empresa y que tienen valor, los cuales pueden verse comprometidos.
  - Vulnerabilidad: Exposición a un riesgo, debilidad, fallo o hueco de seguridad detectado en alguna organización, proceso, procedimiento, programa o sistema
  - Causa: Motivo, razón o circunstancia por la cual se genera algo.
  - Agente generador (Amenazas): Cualquier situación, evento o ente con potencial de daño, que pueda presentarse. Todas aquellas personas, cosas, eventos, acciones o circunstancias que tienen la capacidad de generar un riesgo.
  - Consecuencia o efecto: Es el producto de un evento expresado cualitativa o cuantitativamente, sea este una pérdida, perjuicio, desventaja o ganancia.
- ✓ No se evidencia un seguimiento y resultados de los controles establecidos, donde a través de un informe o control de cambios, se puede visualizar si los controles son efectivos o no.
- ✓ Algunos controles establecidos para los riesgos evaluados, no se configuran como la medida que modifica o mitiga el riesgo.
- ✓ Se observa tratamiento de riesgos incompletos, por locual no es posible identificar el riesgo residual.
- ✓ No se utiliza una metodología del tratamiento de riesgos del sector publico o aplicando buenas prácticas como el marco de referencia NTC-ISO 31000.
- ✓ No hay un glosario y diccionario de datos que ilustre las formulas utilizadas.
- ✓ No se observa una representación gráfica de los riesgos, donde se permite vincular la probabilidad de ocurrencia y su impacto en forma clara y objetiva.

- ✓ Existente riesgos no controlados, por lo cual esta auditoria concluye que se asume el riesgo sin importante su tipo. Se llama la atención en este punto, toda vez que la organización está en un nivel de riesgos de corrupción altos.
- ✓ El riesgo Nro. 1 se encuentra desactualizado, toda vez que las circulares que se mencionan allí, se encuentran derogadas por el Capítulo X de la Circular Básica Jurídica.
- ✓ La matriz de riesgos no se encuentra normalizada, asimismo, no hay evidencia del conocimiento y participación de todos los procesos.

Recomendación:

Cabe resaltar que la presente auditoría, eligió varios riesgos de esta matriz, no obstante, es importante que el área responsable de la gestión del riesgo, revise la totalidad de las matrices por procesos, para ajustar y actualizar.

- ✓ Utilizar una metodología como la Guía para la administración del riesgo o la NTC-ISO 31000.
- ✓ Utilizar la metodología MAGERIT V3: Siguiendo la terminología de la normativa ISO 31000, MAGERIT responde al Proceso de Gestión de Riesgos dentro de un marco de trabajo para que las partes interesadas tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información.

Según las buenas prácticas y el marco de referencia NTC-ISO 31000, se debe tener en cuenta los siguientes aspectos para una adecuada gestión del riesgo:

- ✓ Es importante entonces que, al momento de configurar el riesgo de acuerdo a los elementos anteriormente expuestos, se identifique lo siguiente: Cuando una amenaza explota y/o aprovecha una vulnerabilidad, generando consecuencias negativas sobre cualquier tipo de activo.
- ✓ Identificación del riesgo. Proceso para encontrar, reconocer y describir el riesgo. La identificación de las fuentes de riesgo, los eventos, sus causas y sus consecuencias potenciales.
- ✓ La identificación del riesgo puede involucrar datos históricos, análisis teóricos, opiniones informadas y expertas, y las necesidades de las partes involucradas.
- ✓ Redacte de forma clara, específica y directa sin dar lugar a ambigüedades.
- ✓ Procure evitar calificativos como “malo” o “poco”; prefiera otros más precisos como “deficiente”, “insuficiente” o “ineficiente”
- ✓ No redacte comenzando como “falta de…” u otras frases similares que llevan implícito el sesgo hacia una supuesta solución particular.
- ✓ Evaluar de forma individual cada riesgo en la severidad de su grado de probabilidad e impacto de ocurrencia. Es importante involucrar los dos calificativos.
- ✓ La etapa de tratamiento del riesgo, es un proceso para modificar el riesgo, por esta razón el tratamiento del riesgo puede implicar:
  - ✓ evitar el riesgo decidiendo no iniciar o continuar la actividad que lo originó;
  - ✓ tomar o incrementar el riesgo con el fin de perseguir una oportunidad;
  - ✓ retirar la fuente del riesgo;
  - ✓ cambiar la probabilidad;
  - ✓ cambiar las consecuencias;
  - ✓ compartir el riesgo con una o varias de las partes (incluyendo los contratos y la financiación del riesgo); y
  - ✓ retener el riesgo a través de la decisión informada.
- ✓ Para una adecuada gestión del riesgo, se debe tener en cuenta las propiedades de los riesgos:
  - ✓ Es algo que se ubica en el futuro, no en el presente.
  - ✓ Es algo que posiblemente ocurra, aunque no hay certeza de que ocurra.
  - ✓ Es algo que potencialmente es perjudicial, no es necesariamente beneficioso o neutro.

- ✓ Es algo que con el tiempo puede crecer, decrecer, desaparecer o concretarse.

✓ Es recomendable incluir una representación gráfica de los riesgos, donde se permite vincular la probabilidad de ocurrencia y su impacto en forma clara y objetiva.
✓ Elaborar el diccionario de datos de la matriz de riesgos.

Comentario del auditado – Leandro López Gómez - Director de Planeación y Mejora Continua:

Se pueden radicar los informes en definitivo, entendiendo que los planes de acción se diseñarán de acuerdo con las observaciones presentadas por ustedes y la pertinencia de acuerdo con nuestra naturaleza.

5. CONCLUSIONES

✓ Se realizaron recomendaciones orientadas a actualizar la identificación del riesgo y los controles y tratamientos, así como la tipificación de los mismos, por lo que la entidad debe hacer la revisión para que la matriz sea actualizada siguiendo estos lineamientos.
✓ Se recomienda aprobar una metodología teniendo en cuenta la guía de la administración del riesgo de la gestión pública o la NTC-ISO 31000 y por ende aplicar dicho procedimiento de manera transversal a todos los procesos de la entidad.
✓ Se sugiere la revisión de controles de que cada uno de los procesos de la entidad, toda vez que no se observa un seguimiento.

Se recomienda en general para todas las matrices de riesgos que se realicen las siguientes actividades:

✓ Evaluación de Riesgos Existentes: Reexaminar los riesgos previamente identificados para determinar si su probabilidad de ocurrencia y su impacto han cambiado, y ajustar su clasificación en consecuencia.
✓ Eficacia de las Medidas de Mitigación: Analizar la efectividad de las estrategias y controles implementados para mitigar los riesgos, y determinar si necesitan ser modificados o reforzados.
✓ Actualización de Planes de Tratamiento: Revisar y actualizar los planes de tratamiento de riesgos para asegurar que las acciones sean pertinentes y estén alineadas con los objetivos actuales de la organización.
✓ Monitoreo Continuo: Establecer o mejorar los mecanismos de monitoreo continuo para detectar cambios en el entorno que puedan afectar la naturaleza o el impacto de los riesgos.
✓ Cumplimiento Normativo y Regulatorio: Asegurar que la gestión de riesgos cumpla con las normativas, leyes y estándares relevantes, y que esté alineada con las mejores prácticas.
✓ Comunicación y Reportes: Revisar los canales de comunicación y los informes relacionados con los riesgos para garantizar que la información crítica llegue a las partes interesadas de manera oportuna y clara.
✓ Capacitación y Conciencia: Evaluar la necesidad de capacitación adicional para el personal sobre la gestión de riesgos, asegurando que todos los miembros relevantes de la organización comprendan su papel en la mitigación y tratamiento de riesgos.

Es importante mencionar que la auditoria se llevó a cabo teniendo en cuenta la normatividad vigente existente en PEOPLE CONTACT y el buen criterio del auditor de Control Interno independiente. Así mismo, de conformidad con el Decreto 2420 de 2015, Anexo No. 4, que incorpora las Normas Internacionales de Auditoría (NIA) y las ISAE (Estándares Internacionales de Servicios de Aseguramiento). Dichas normas exigen que se cumpla con los requerimientos de ética, así como que planifique y ejecute la auditoría.