PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Empresa Inmobiliaria y de Servicios Logísticos de Cundinamarca
Sede Administrativa Calle 26 51-53. Torre Beneficencia Piso 3.
Bogotá, D.C. Tel. 749 1535 - 749 1541

/ElCundinamarca @InmobCund
contactenos@eic.gov.co www.eic.gov.co

Tabla de Contenido

1. Introducción

La Empresa Inmobiliaria y de Servicios Logísticos de Cundinamarca en cumplimiento a lo establecido por el estado colombiano, CONPES 3854 de 2016, Modelo de Seguridad y Privacidad de MINTIC y lo establecido en el decreto 1008 de 14 de junio 2018 "Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones", presenta el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información para la vigencia 2020, donde se establece un conjunto de actividades para crear condiciones de uso confiable en el entorno físico y digital de la información, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información de la Entidad a través de su ciclo de vida desde su captura, almacenamiento, explotación, hasta su eliminación

2. Objetivo

Definir y aplicar los lineamientos para tratar de manera integral los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación a los que la EIC pueda estar expuesta, y de esta manera alcanzar los objetivos, la misión y la visión institucional, protegiendo y preservando la integridad, confidencialidad, disponibilidad y autenticidad de la información

3. Alcance

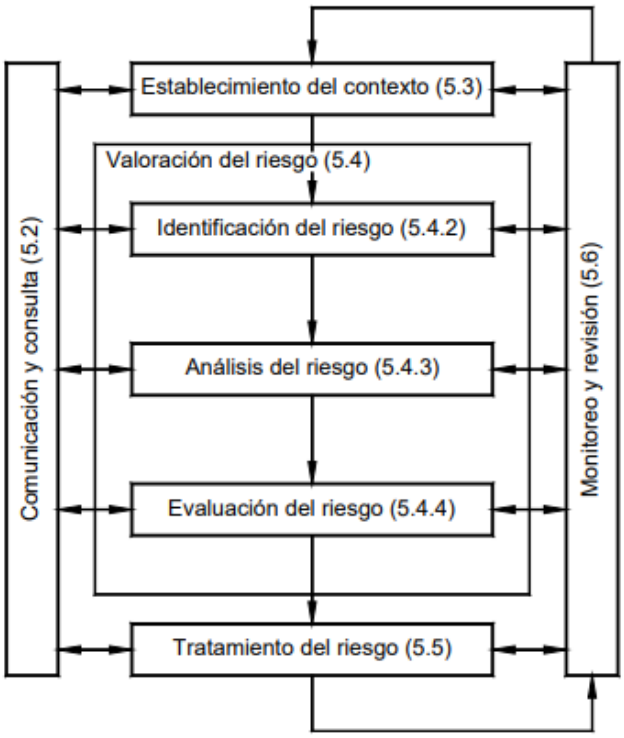
La gestión y el tratamiento de los riesgos de seguridad de la información se aplicará, a través de la aplicación de principios básicos y metodológicos para la administración de la información, así como técnicas, actividades y buenas prácticas que contribuyan a la toma de decisiones para la prevención de incidentes al interior de la Entidad

4. Metodología y etapas para la gestión de riesgos

La Empresa Inmobiliaria y de Servicios Logísticos de Cundinamarca, realiza la identificación y tratamiento de riesgos a través de una metodología alineada con la ISO 31000:2009. A través de la cual se establecen las siguientes actividades:

Empresa Inmobiliaria y de Servicios Logísticos de Cundinamarca
Sede Administrativa Calle 26 51-53. Torre Beneficencia Piso 3.
Bogotá, D.C. Tel. 749 1535 - 749 1541
/EICundinamarca @InmobCund
contactenos@eic.gov.co www.eic.gov.co

NORMA TÉCNICA COLOMBIANA NTC-ISO 31000



Fuente: ISO 31000:2009

4.1. Contexto

Para realizar la gestión de los riesgos se establece n contexto, en el cual se identifican los procesos realizados al interior de la Entidad, la interrelación que dichos procesos tienen con otros procesos, los procedimientos que se desarrollan en cada proceso y el grado de autoridad y responsabilidad de los funcionarios frente a cada proceso.

4.2. Identificación de Riesgos

Al establecer el contexto de la organización, se realiza la identificación de los principales riesgos a los que se encuentran expuestos los procesos de la Entidad. Se identificarán los riesgos teniendo en cuenta la responsabilidad que tienen los encargados de cada proceso y la manera en que estos pueden afectar los objetivos y/o estrategias definidas en la Entidad. Dicho proceso se realizará a través de:

- Reuniones con las áreas de la Entidad
- Encuestas a Funcionarios y Contratistas

Una vez sean identificados los riesgos de cada una de las áreas, serán clasificados en:

Tipo de Riesgo	Descripción
Estratégico	Relacionado con los objetivos estratégicos alineados con la misión de la EIC
De imagen	Relacionado con la percepción y confianza de la ciudadanía hacia la EIC
Financiero	Relacionado con el uso eficaz y eficiente de los recursos financieros
Operacional	Derivado de deficiencias o fallas en procesos, usuarios, sistemas o eventos internos y externos
Tecnológicos	Relacionado con la capacidad tecnológica de la Entidad para satisfacer las necesidades actuales y futuras en cumplimiento de la misión de la Entidad
Cumplimiento	Relacionado con el cumplimiento de leyes y regulaciones a las que se encuentra sujeta la Entidad

4.3. Estimación de Riesgos

La estimación del riesgo es el procedimiento mediante el cual se establece la probabilidad de ocurrencia de los riesgos y el impacto que estos pueden tener sobre los procesos de la Entidad, esto se realiza teniendo en cuenta lo siguiente:

Probabilidad		Descripción
1	Raro	Puede ocurrir en circunstancias excepcionales entre 0 y 1 vez en un semestre
2	Improbable	Puede ocurrir pocas veces, entre 2 y 5 veces en un semestre
3	Posible	Puede ocurrir algunas veces, entre 6 y 10 veces en un semestre
4	Probable	Puede ocurrir casi siempre, entre 11 y 15 veces en un semestre
5	Casi Seguro	Puede ocurrir en la mayoría de las circunstancias, más de 15 veces en un semestre

Impacto		Descripción
1	Insignificante	Impacta de forma leve la imagen y operación de la Entidad, no tiene impacto financiero
2	Menor	Impacta la imagen y operación de un proceso. Puede representar sobrecostos
3	Moderado	Afecta negativamente la imagen institucional por retrasos en la prestación del servicio. Puede sobrellevar reprocesos, sobrecostos y aumento de carga operativa
4	Mayor	Impacta la imagen y operación por el incumplimiento en la prestación de servicios. Puede presentar reprocesos, sobrecostos y posibilidad de recibir investigación disciplinaria
5	Catastrófico	Impacta de manera importante la imagen de la entidad por el incumplimiento de sus objetivos estratégicos. Puede sobrellevar reprocesos, sobrecostos, aumento de carga operativa importante y sanciones o intervenciones por entes de control

4.4. Evaluación de controles para mitigación de los riesgos

La evaluación se realiza cuando se ha establecido un riesgo inherente para los procesos y su impacto y probabilidad de ocurrencia, con el propósito de establecer el control que se puede tener sobre el mismo, la documentación de este, las evidencias y un plan de acción detectivo, preventivo y correctivo Adicional a esto, se identifican las amaneces que pueden llegar a materializar los riesgos mencionados

4.5. Tratamiento del Riesgo

Teniendo en cuenta los resultados obtenidos en el análisis del riesgo, se establecen los niveles del riesgo y las acciones de mejora que propenden a la conservación de la confidencialidad, integridad y disponibilidad de la información.

Tipo de Riesgo	Acción requerida
Riego Catastrófico	Requiere acciones inmediatas para evitar la pérdida de la confidencialidad, integridad y disponibilidad de la información
Riesgo alto	Requiere acciones rápidas por parte de la Alta Dirección para disminuir el Riesgo
Riesgo Moderado	Requiere controles definidos para el riesgo y revisar la eficacia de estos.
Riesgo Bajo	Se mitiga con actividades propias y mediante acciones detectivas y preventivas
Riesgo insignificante	No representa un impacto para la Entidad

Las acciones de tratamiento se pueden dividir en:

- Eliminar el riesgo prescindiendo del proceso, la actividad o las circunstancias que lo generan.
- Asumir el riesgo, aun aumentándolo, con el fin de incrementar una posible oportunidad.
- Tomar acciones para disminuir la probabilidad del riesgo.
- Implementar acciones que disminuyan el impacto negativo del riesgo.
- Compartir el riesgo (cláusulas en contratos o comprar pólizas de seguros).
- Retener el riesgo con base en información confiable.

4.6. Seguimiento y revisión del proceso de Gestión del Riesgo

El seguimiento y la revisión son parte vital del proceso de Gestión de Riesgos, ya que se realiza el seguimiento, monitoreo y evaluación de cada uno de los aspectos de este con el propósito de identificar y ejecutar acciones de mejora en los procedimientos. Dentro de este proceso se tienen en cuenta las siguientes actividades:

- Análisis de los cambios, las tendencias, los éxitos y los fracasos dentro del proceso de gestión de riesgos de seguridad de la información.

- Detección de cambios en el contexto interno o externo, incluyendo los cambios que se puedan presentar en los criterios de riesgos de seguridad de la información.
- Revisión la implementación de los planes de tratamiento de riesgo de seguridad de la información y las prioridades de implementación de estos.
- Identificación de nuevos riesgos de seguridad de la información