







**Empresa Industrial y Comercial**  
**Lotería de Cundinamarca**  
**Los Lunes, Hágase Rico**

## **Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información – 2022**

Código: 120-DI-D002  
Versión: 1  
Fecha: 21/06/2018  
Página: 2 de 35


### **1. INTRODUCCIÓN**

Al entrar en funcionamiento la protección de la información y la administración de riesgos, que permiten en su objetivo desde un desarrollo método lógico y sistemático que permiten establecer el contexto de la seguridad y privacidad de la información, desde el identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos asociados con una actividad, función o proceso de tal forma que permita a la Lotería como entidad minimizar pérdidas y maximizar oportunidades, frente al desarrollo tecnológico que viene desarrollando.

Si bien, el efecto de la seguridad y privacidad de la información repercute en la trazabilidad del negocio propio de la entidad y su interactuar con el entorno empresarial del sector, permite incluir medidas estrictas de seguridad de la información en la entidad que permite generar un lazo fuerte en la organización para la implementación de penas a quienes no hagan un buen uso de los medios tecnológicos que brindan la información institucional desde el punto de vista de privacidad y seguridad, que permite fortalecer el derecho de los actores externos en el hecho de tener sus datos personales resguardados bajo las medidas de seguridad que le permitan la integridad y la privacidad de la misma, responsabilidad que es de la Lotería como la organización que alberga la información en su sistema al proteger de riesgos la vulnerabilidad con las medidas de seguridad pertinentes al sector y a la actividad empresarial.

Así mismo, los servidores públicos, en cumplimiento de sus funciones, están sometidos a riesgos que pueden hacer fracasar una gestión; por lo tanto, es necesario tomar las medidas, para identificar las causas y consecuencias de la materialización de dichos riesgos. Por esa razón, la presente guía tiene como objetivo orientar y facilitar la implementación y desarrollo de una eficaz, eficiente y efectiva gestión del riesgo, desde la identificación hasta el monitoreo; enfatiza en la importancia de la administración del riesgo, sus fundamentos teóricos y da una orientación para facilitar su identificación, reconocimiento de las causas, efectos, definición de controles y da lineamientos sencillos y claros para su adecuada gestión.

La Lotería como entidad, desarrolla un método de trabajo que se estandariza en la prevención de falencias en Seguridad informática que pueden incurrir en Detrimiento Patrimonial, así como en el soporte y mantenimiento de Sistemas de información que permita desde el funcionario implementar un criterio de seguridad

 <p><b>Empresa Industrial y Comercial</b> <b>Lotería de Cundinamarca</b> <b>Los Lunes, Hágase Rico</b></p>	<p><b>Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información – 2022</b></p>	<p>Código: 120-DI-D002 Versión: 1 Fecha: 21/06/2018 Página: 3 de 35</p>
---	---	---

para la prevención de riesgos y generar los lineamientos de privacidad de la información.

## **2. OBJETIVOS**

### **2.1 Objetivo general**

Establecer los conceptos básicos y metodológicos para una adecuada administración de riesgos a partir de su identificación, manejo y seguimiento.

### **2.2 Objetivos específicos**

- Concientizar a todos los actores internos y externos de los procesos sobre la necesidad e importancia de gestionar de manera adecuada, los riesgos inherentes a la gestión.
- Involucrar y comprometer a todos en la formulación e implementación de controles y acciones encaminadas a prevenir y administrar los riesgos.
- Establecer, mediante una adecuada administración del riesgo, una base confiable para la toma de decisiones y la planificación institucional.

## **3. ALCANCE**

Este Plan de Tratamiento, proporciona la metodología establecida por la Entidad para la administración y gestión de los riesgos a nivel de procesos; orientando sobre las actividades a desarrollar desde la definición del contexto del Plan Estratégico, la identificación de los riesgos, su análisis, valoración y la definición de las opciones de manejo que pueden requerir la formulación de acciones adicionales para garantizar una adecuada gestión del riesgo.

## **4. ÁMBITO DE APLICACIÓN**

Los lineamientos definidos en este Plan de Tratamiento de Riesgos, aplica para todos los procesos de la entidad que se establezcan desde el contexto de la seguridad y privacidad de la información y la gestión de los riesgos.



**Empresa Industrial y Comercial**  
**Lotería de Cundinamarca**  
**Los Lunes, Hágase Rico**

## **Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información – 2022**

Código: 120-DI-D002  
Versión: 1  
Fecha: 21/06/2018  
Página: 4 de 35

### **5. DEFINICIONES**

Para la administración del riesgo, se tendrán en cuenta los siguientes términos y definiciones:

- **Aciertos:** Experiencias exitosas, aspectos que pueden ser replicables, fortalezas, logros, cumplimiento de los objetivos trazados en términos institucionales.
- **Acciones asociadas:** son las acciones que se deben tomar posterior a determinar las opciones de manejo del riesgo (asumir, reducir, evitar compartir o transferir), dependiendo de la evaluación del riesgo residual, orientadas a fortalecer los controles identificados.
- **Acción Correctiva:** Acción tomada para eliminar la causa de una no conformidad detectada u otra situación no deseable.
- **Acción Preventiva:** Acción tomada para eliminar la causa de una no conformidad potencial u otra situación potencial no deseable. (ISO9000:2005)
- **Administración de riesgos:** conjunto de etapas secuenciales que se deben desarrollar para el adecuado tratamiento de los riesgos.
- **Amenaza:** situación externa que no controla la entidad y que puede afectar su operación
- **Análisis del riesgo:** etapa de la administración del riesgo, donde se establece la probabilidad de ocurrencia y el impacto del riesgo antes de determinar los controles (análisis del riesgo inherente).
- **Asumir el riesgo:** opción de manejo donde se acepta la pérdida residual probable, si el riesgo se materializa.
- **Autoridad:** Poder con que se cuenta o que se ha recibido por delegación. (NTCGP1000:2009)
- **Causa:** medios, circunstancias y/o agentes que generan riesgos.
- **8.5 Causa Raíz:** Es el origen de una falla o incumplimiento.



**Empresa Industrial y Comercial**  
**Lotería de Cundinamarca**  
**Los Lunes, Hágase Rico**

## **Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información – 2022**

Código: 120-DI-D002  
Versión: 1  
Fecha: 21/06/2018  
Página: 5 de 35

- 8.6 Control: Medida o acción que modifica el riesgo mediante la afectación ya sea de la probabilidad o del impacto. (GTC137:2011)
- 8.7 Consecuencia: Resultado de un evento que afecta a los objetivos. (GTC137:2011)
- 8.8 Contexto: Combinación de factores internos y externos y de condiciones que pueden afectar al enfoque de una organización, a sus productos, servicios e inversiones y partes interesadas.
- **Calificación del riesgo:** estimación de la probabilidad de ocurrencia del riesgo y el impacto que puede causar su materialización.
- **Compartir o transferir el riesgo:** opción de manejo que determina traspasar o compartir las pérdidas producto de la materialización de un riesgo con otras organizaciones mediante figuras como outsourcing, seguros, sitios alternos.
- **Consecuencia:** efectos que se pueden presentar cuando un riesgo se materializa.
- **Contexto estratégico:** son las condiciones internas y del entorno, que pueden generar eventos que originan oportunidades o afectan negativamente el cumplimiento de la misión y objetivos de una institución.
- **Control:** acción o conjunto de acciones que minimiza la probabilidad de ocurrencia de un riesgo o el impacto producido ante su materialización.
- **Control preventivo:** acción o conjunto de acciones que eliminan o mitigan las causas del riesgo; está orientado a disminuir la probabilidad de ocurrencia del riesgo.
- **Control correctivo:** acción o conjunto de acciones que eliminan o mitigan las consecuencias del riesgo; está orientado a disminuir el nivel de impacto del riesgo.
- **Corrección:** Acción tomada para eliminar una no conformidad detectada.(ISO 9000:2015).



**Empresa Industrial y Comercial**  
**Lotería de Cundinamarca**  
**Los Lunes, Hágase Rico**

## **Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información – 2022**

Código: 120-DI-D002  
Versión: 1  
Fecha: 21/06/2018  
Página: 6 de 35

- **Desaciertos:** Acciones / planes que no arrojaron los resultados esperados, deficiencias en la planeación, fracasos.
- **Debilidad:** situación interna que la entidad puede controlar y que puede afectar su operación.
  - 8.11 Descripción del Riesgo: Declaración estructurada del riesgo que usualmente contiene cuatro elementos: fuentes, eventos, causas y consecuencias. (GTC137:2011).
  - 8.12 Efecto: Desviación de aquello que se espera, sea positivo, negativo o ambos.
  - **Evaluación del riesgo:** resultado del cruce cuantitativo de las calificaciones de probabilidad e impacto, para establecer la zona donde se ubicará el riesgo. Proceso de comparación de los resultados del análisis del riesgo (probabilidad e impacto antes de controles), con los criterios del riesgo (valoración de controles) para determinar si el riesgo, su magnitud o ambos, son aceptables o tolerables. (GTC137:2011).
  - Evento: Ocurrencia o cambio de un conjunto particulares de circunstancias. (GTC137:2011) En algunas ocasiones se hace referencia a un evento como un "incidente" o "accidente".
  - Eventos Potenciales a Evaluar: Son aquellas situaciones ocurridas en un proceso que podrían llegar a ser clasificadas como riesgos materializados, pero se debe hacer un análisis previo para llegar a esa conclusión.
- **Evitar el riesgo:** opción de manejo que determina la formulación de acciones donde se prevenga la materialización del riesgo mediante el fortalecimiento de controles identificado.
  - **Frecuencia:** ocurrencia de un evento expresado como la cantidad de veces que ha ocurrido un evento en un tiempo dado. Número de eventos o efectos por unidad de tiempo definida. (GTC 137:2011).
- **Fuente de un Riesgo:** Elemento que solo o en combinación tiene el potencial intrínseco de originar un riesgo. (GTC137:2011). Puede ser tangible o intangible.



**Empresa Industrial y Comercial**  
**Lotería de Cundinamarca**  
**Los Lunes, Hágase Rico**

## **Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información – 2022**

Código: 120-DI-D002  
Versión: 1  
Fecha: 21/06/2018  
Página: 7 de 35

- **Identificación del riesgo:** etapa de la administración del riesgo donde se establece el riesgo con sus causas (asociadas a factores externos e internos de riesgo), consecuencias y se clasifica de acuerdo con los tipos de riesgo definidos. Proceso para encontrar, reconocer y describir el riesgo. (GTC137: 2011).
- **Impacto:** medida para estimar cuantitativa y cualitativamente el posible efecto de la materialización del riesgo.
- **Lección Aprendida:** Conocimiento adquirido a través de la experiencia organizacional, que analizado y difundido apropiadamente puede convertirse en acciones que lleven a la Entidad a obtener mejores resultados, no repitiendo las acciones erróneas y replicando las que condujeron al éxito.
- **Matriz de Valoración de Riesgos:** Herramienta para la evaluación de los riesgos y su clasificación. También se le dice matriz RAM por sus siglas en inglés. (Matriz RiskAssessmentMatrix). La matriz permite calificar y evaluar los riesgos en términos de impacto y probabilidad.
- **Mapa de riesgos:** documento que, de manera sistemática, muestra el desarrollo de las etapas de la administración del riesgo.
- **Materialización del riesgo:** ocurrencia del riesgo identificado
  - **Nivel de riesgo:** Magnitud de un riesgo o de una combinación de riesgos, expresada en términos de la combinación de las consecuencias y su posibilidad. Sumatoria de la multiplicación de la probabilidad por el impacto de todos los riesgos de un proceso o de la Institución. (GTC137:2011).
  - **Objetivo del Proceso:** Se debe transcribir el objetivo que se ha definido para el proceso al cual se le están identificando los riesgos.
- **Opciones de manejo:** posibilidades disponibles para administrar el riesgo posterior a la valoración de los controles definidos (asumir, reducir, evitar, compartir o transferir el riesgo residual).
  - **Plan de contingencia:** conjunto de acciones inmediatas, recursos, responsables y tiempos establecidos para hacer frente a la materialización





**Empresa Industrial y Comercial**  
**Lotería de Cundinamarca**  
**Los Lunes, Hágase Rico**

## **Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información – 2022**

Código: 120-DI-D002  
Versión: 1  
Fecha: 21/06/2018  
Página: 8 de 35

del riesgo y garantizar la continuidad del servicio. Las acciones o planes de contingencia garantizan que la Institución tiene la capacidad de seguir prestando sus servicios sin interrupciones o con periodos mínimos de interrupción, ante eventos inesperados como terremotos, fallas de sistemas de información, cortes del suministro de servicios públicos, inundaciones, terrorismo, entre otros.

- **Plan de Tratamiento:** Conjunto de acciones que se planean y se ejecutan con el fin de generar controles que eviten la materialización de un riesgo o disminuyan su impacto en caso de que ocurra. (GTC137:2011)
- **Parte Interesada:** Persona u organización que puede afectar, verse afectada, o percibirse como afectada por una decisión o actividad. Ejemplo: clientes, propietarios, personal de la organización, proveedores, socios, entes de control, entre otros.
- **8.26 Posibilidad:** Oportunidad de que algo suceda. (Likelihood). (GTC137:2011).
- **Preguntas Claves para la Identificación del Riesgo:** ¿Qué puede suceder?, ¿Cómo puede suceder? Es importante observar que el proceso de identificación del riesgo es posible realizarlo a partir de varias causas que pueden estar relacionadas.
- **Probabilidad:** medida para estimar cuantitativa y cualitativamente la posibilidad de ocurrencia del riesgo. Posibilidad de que algo ocurra bien sea que se haya definido, medido, o estimado objetiva o subjetivamente, o en términos de los descriptores generales (tales como raro, improbable, probable, casi cierto). La probabilidad puede expresarse cuantitativa o cualitativamente).
- **Procedimiento:** conjunto de especificaciones, relaciones, responsabilidades, controles y ordenamiento de las actividades y tareas requeridas para cumplir con el proceso.
- **Proceso:** conjunto de entradas tangibles o intangibles, suministradas por un proveedor, a estas entradas se les asigna recursos y se aplican controles,



**Empresa Industrial y Comercial**  
**Lotería de Cundinamarca**  
**Los Lunes, Hágase Rico**

## **Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información – 2022**

Código: 120-DI-D002  
Versión: 1  
Fecha: 21/06/2018  
Página: 9 de 35

obteniendo salidas tangibles o intangibles, destinadas a un usuario, generando un impacto en estos. Se clasifican en estratégicos, misionales, de apoyo y de evaluación.

- **Queja:** Es la manifestación de inconformidad por parte de los usuarios, generada por el comportamiento en la atención a los mismos, ya sea de carácter administrativa o por presuntas conductas no deseables de los funcionarios.
- **Reclamo:** Es una oposición por parte del usuario frente a una decisión que se considera injusta relacionada con la prestación de los servicios de una Entidad, que va en contra de los derechos del usuario. El objeto es que se revise el motivo de su inconformidad y se tome una decisión.
- **Riesgo:** eventualidad que tendrá un impacto negativo sobre los objetivos institucionales o del proceso. Efecto de la incertidumbre sobre un resultado esperado. Algo que podría suceder y afectar el logro de los objetivos organizacionales. (GTC 176).
- **Riesgo de corrupción:** posibilidad de que, por acción u omisión, mediante el uso indebido del poder, de los recursos o de la información, se lesionen los intereses de una entidad y en consecuencia del Estado, para la obtención de un beneficio particular.
- **Riesgo inherente:** es aquel al que se enfrenta una entidad o proceso en ausencia de controles y/o acciones para modificar su probabilidad o impacto.
- **Riesgo institucional:** Son los que afectan de manera directa el cumplimiento de los objetivos o la misión institucional. Los riesgos institucionales, son producto del análisis de los riesgos por proceso y son denominados de este tipo cuando cumplen las siguientes características:
  - Los riesgos que han sido clasificados como estratégicos: en el paso de identificación deben haber sido marcados como de clase estratégica, es decir, se relacionan con el cumplimiento de objetivos institucionales, misión y visión.



**Empresa Industrial y Comercial**  
**Lotería de Cundinamarca**  
**Los Lunes, Hágase Rico**

## **Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información – 2022**

Código: 120-DI-D002  
Versión: 1  
Fecha: 21/06/2018  
Página: 10 de 35

- Los riesgos que se encuentran en zona alta o extrema: después de valorar el riesgo (identificación y evaluación de controles), el riesgo residual se ubica en zonas de riesgo alta o extrema, indicando que el grado de exposición a la materialización del riesgo aún se encuentra poco controlado.
- Los riesgos que tengan incidencia en usuario o destinatario final externo: en el caso de la materialización del riesgo la afectación del usuario externo se presenta de manera directa.
- Los riesgos de corrupción: todos los riesgos identificados que hagan referencia a situaciones de corrupción, serán considerados como riesgos de tipo institucional.

- **Riesgo residual:** nivel de riesgo que permanece luego de determinar y aplicar controles para su administración. Remanente después del Tratamiento del Riesgo. (GTC137:2011). Es aquel que permanece aún después de desarrolladas las acciones de tratamiento del riesgo. Capacidad total de riesgo que una organización está dispuesta a aceptar, tolerar, está expuesta a sumir en cualquier momento dado.

- **Riesgo Materializado:** Ocurrencia de un evento que se había identificado como incierto.

- **Tratamiento del Riesgo:** Proceso para modificar el riesgo (GTC137:2011). Conjunto de acciones que permiten a través de la creación, fortalecimiento o implementación de controles, modificar la probabilidad o el impacto de un riesgo.

- **Valoración del riesgo:** establece la identificación y evaluación de los controles para prevenir la ocurrencia del riesgo o reducir los efectos de su materialización. En la etapa de valoración del riesgo se determina el riesgo residual, la opción de manejo a seguir, y si es necesaria.

## **6. ROLES Y RESPONSABILIDADES FRENTE A LA ADMINISTRACIÓN DEL RIESGO**

El éxito de la administración del riesgo depende de la decidida participación de los directivos, funcionarios y contratistas (todos actores); por esto, es preciso identificar los actores que intervienen:



**Empresa Industrial y Comercial**  
**Lotería de Cundinamarca**  
**Los Lunes, Hágase Rico**

## **Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información – 2022**

Código: 120-DI-D002  
Versión: 1  
Fecha: 21/06/2018  
Página: 11 de 35

### • **GERENCIA GENERAL**

- Asegurar que los indicadores que miden la gestión del riesgo estén acordes con los indicadores de gestión de la Empresa.
- Comunicar los beneficios de la gestión del riesgo a todas las partes interesadas.
- Formular conjuntamente con el Comité de Coordinación de Control Interno la política de administración del riesgo.
- Garantizar que la cultura de la organización y la política de riesgos estén alineadas.
- Garantizar que se asignan los recursos necesarios para la gestión del riesgo.
- Revisar periódicamente la política, para garantizar que siga siendo adecuada para la entidad.

La Alta Dirección: aprueba las directrices para la administración del riesgo en la Entidad. La Alta Dirección es la responsable del fortalecimiento de la política de administración del riesgo.

### • **OFICINA DE CONTROL INTERNO**

- Asesorar y capacitar a la alta dirección y a los dueños de procesos, en la metodología para la gestión de riesgos.
- Verificar que los controles existentes sean efectivos para minimizar la probabilidad de impacto de la ocurrencia de los mismos.
- Realizar seguimiento a las acciones establecidas en los planes de manejo de riesgos y emitir informes periódicos a la Gerencia General.
- Emitir recomendaciones para la implementación de controles.
- Control Interno: debe realizar evaluación y seguimiento a la política, los Procedimientos y los controles propios de la administración de riesgos



**Empresa Industrial y Comercial**  
**Lotería de Cundinamarca**  
**Los Lunes, Hágase Rico**

## **Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información – 2022**

Código: 120-DI-D002  
Versión: 1  
Fecha: 21/06/2018  
Página: 12 de 35

- **OFICINA DE PLANEACIÓN**

- Definir la metodología, comunicarla, y asesorar en su implementación.
- Elaborar el plan anticorrupción en coordinación con los dueños de procesos y con base en los mapas de riesgos de corrupción.
- Definir el mapa de riesgos institucional para incluirlo en el mapa de riesgos institucional y lo mismo con los de corrupción.

- **Directores de Procesos:**

- Genera la operatividad de la administración del riesgo inherente a su proceso, identificando, evaluando y valorando el Riesgo.

- **Proceso Administración del Sistema Integrado de Gestión:**

- Genera la metodología para la administración del riesgo de la Entidad, coordina, lidera, capacita y asesora en su aplicación.

- **Responsables Dueños de los procesos:**

- Liderar la identificación de riesgos (incluyendo los de corrupción) con todo su equipo de trabajo.
- Estructurar las medidas para controlarlos, evitarlos y realizar el seguimiento a la efectividad de dichas acciones.
- Registrar y reportar los riesgos materializados a la Oficina de Planeación.
- Mantener actualizado el mapa de riesgos de su proceso.
- Identifican, analizan, evalúan y valoran los riesgos de la entidad (por procesos) al menos una vez al año. Si bien los Líderes SIG apoyan la ejecución de las etapas de gestión del riesgo a nivel de los procesos, esto no quiere decir que el proceso de administración de riesgos este solo bajo su responsabilidad. Al contrario, cada responsable de proceso se encarga de garantizar que en el proceso a su cargo se definan los riesgos que le competen, se establezcan las estrategias y responsabilidades para tratarlos y, sobre todo, que se llegue a cada funcionario que trabaja en dicho proceso. No se debe olvidar que son las personas que trabajan en cada uno de los procesos los que mejor conocen los riesgos existentes en el desarrollo de sus actividades.



**Empresa Industrial y Comercial**  
**Lotería de Cundinamarca**  
**Los Lunes, Hágase Rico**

## **Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información – 2022**

Código: 120-DI-D002  
Versión: 1  
Fecha: 21/06/2018  
Página: 13 de 35

- **TODOS LOS FUNCIONARIOS Y Contratistas:**

- ejecutar los controles y acciones definidas para la administración de los riesgos definidos, aportar en la identificación de posibles riesgos que puedan afectar la gestión de los procesos y/o de la entidad.
- Participar activamente en la identificación de riesgos y la determinación y aplicación de controles.

## **7. POLÍTICA DE ADMINISTRACIÓN DEL RIESGO**

La Empresa Industrial y Comercial Lotería de Cundinamarca se compromete a identificar y administrar de manera integral los riesgos y oportunidades inherentes al cumplimiento de su misión, de sus objetivos estratégicos y de sus procesos, planificando y desarrollando oportunamente acciones orientadas a prevenir o mitigar efectos no deseados, con el fin de garantizar de forma permanente la calidad del servicio y el logro de las metas planificadas. La Lotería expresa además, su compromiso con la identificación y tratamiento de los riesgos de corrupción, lavado de activos y financiación del terrorismo en cualquiera de sus formas, mediante un monitoreo constante a los controles establecidos.

Para ello, la entidad cuenta con una herramienta metodológica que incluye los mecanismos para evaluar y mejorar la eficacia de la gestión del riesgo, personal competente y los recursos físicos y tecnológicos requeridos.

## **8. OBJETIVOS DE LA ADMINISTRACIÓN DE RIESGOS**

### **8.1 GENERAL**

Fortalecer la implementación y desarrollo de la Política de la Administración del Riesgo a través de su adecuado tratamiento, para garantizar el cumplimiento de la misión y objetivos de la Lotería de Cundinamarca, proporcionando las directrices para su correcta gestión.

### **8.2 OBJETIVOS ESPECÍFICOS**



**Empresa Industrial y Comercial**  
**Lotería de Cundinamarca**  
**Los Lunes, Hágase Rico**

## **Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información – 2022**

Código: 120-DI-D002  
Versión: 1  
Fecha: 21/06/2018  
Página: 14 de 35

- 1.- Establecer los lineamientos para Identificar, describir, calificar, evaluar y priorizar el tratamiento de los riesgos que puedan afectar o impedir el logro de los objetivos institucionales.
- 2.- Identificar los parámetros que se deben tener en cuenta para definir acciones de tratamiento que permitan disminuir la probabilidad de ocurrencia de los riesgos y / o disminuir su impacto.
- 3.- Hacer seguimiento a la ejecución de las acciones planificadas y revisar su eficacia.

### **9. ALCANCE**

Aplica a todos los Procesos del Sistema de Gestión Integrado de la Empresa Industrial y Comercial de la Lotería de Cundinamarca.


### **10. ANÁLISIS CONTEXTO ESTRATÉGICO**

El análisis de contexto es una actividad en la que se identifican las cuestiones externas e internas que son pertinentes para el propósito de la entidad y su dirección estratégica.

El contexto externo es el ambiente en el cual la entidad busca alcanzar sus objetivos y para establecerlo se tienen en cuenta el ambiente social y cultural, político, legal, reglamentario, financiero, tecnológico, económico y competitivo, ya sea internacional, nacional, regional o local. También se deben tener en cuenta las relaciones con las partes interesadas externas, sus percepciones y valores.

El contexto interno es el ambiente interno en el cual la organización busca alcanzar sus objetivos y para establecerlo, se tienen en cuenta gobierno y estructura de la organización, funciones y responsabilidades, valores y desempeño, políticas, objetivos y estrategias, capacidades en términos de recursos y conocimientos, sistemas de información, forma y extensión de las relaciones contractuales, entre otros.

El contexto del proceso, está relacionado con el diseño del proceso en cuanto a la claridad en la descripción del alcance y objetivo; interacciones con otros procesos en cuanto a insumos, proveedores, productos, usuarios o clientes; transversalidad, determinando los procesos que proporcionan lineamientos necesarios para el desarrollo de todos los demás; procedimientos asociados,

 <p><b>Empresa Industrial y Comercial</b> <b>Lotería de Cundinamarca</b> <b>Los Lunes, Hágase Rico</b></p>	<p><b>Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información – 2022</b></p>	<p>Código: 120-DI-D002 Versión: 1 Fecha: 21/06/2018 Página: 15 de 35</p>
---	---	--

pertinencia en los procedimientos que desarrollan los proceso; responsables del proceso, el grado de autoridad y responsabilidad de los funcionarios frente al proceso; y comunicación entre los procesos, es la efectividad en los flujos de información determinados en la interacción de los procesos.

## **11. DESARROLLO PRÁCTICO - CONTEXTO ESTRATÉGICO - DOFA**

Análisis de Contexto en la Lotería de Cundinamarca, con el fin de documentar el conocimiento de la Empresa y el análisis de contexto, se deberá diligenciar la Matriz de Análisis DOFA, para lo cual se realizará anualmente una reunión, que será liderada por la Oficina Asesora de Planeación e Informática. A esta reunión deben asistir todos los funcionarios para que aporten su conocimiento acerca del estado y funcionamiento de la empresa. Como primera actividad de esta reunión y para poner en contexto a todos los asistentes, el Jefe de la Oficina de Planeación e Informática deberá presentar a los asistentes de una forma gerencial la siguiente información:

Requisitos de Partes Interesadas.

- Aspectos relevantes para la Lotería del Plan de Desarrollo vigente de la Gobernación de Cundinamarca.
- Requisitos Legales Aplicables (Coljuegos y Superintendencia Nacional de Salud).
- Análisis del sector (competencia y productos).
- Resultados de Desempeño de la Entidad.
- Informe del estado del Sistema de Gestión de Seguridad y Salud en el Trabajo.
- Intenciones de la Gerencia General.
- Resultados de los planes de acción por procesos.
- Resultados de las evaluaciones de clima organizacional.
- Análisis de las autoevaluaciones por procesos.

Nota 1: El Jefe de la Oficina Asesora de Planeación e Informática podrá solicitar a los responsables de la información su presentación en la reunión mencionada.

Nota 2: Debido a la importancia de esta reunión, ya que es la base para la planificación de las actividades de la entidad, se requiere la participación de todos los funcionarios.

## **12. SEGUIMIENTO**





**Empresa Industrial y Comercial**  
**Lotería de Cundinamarca**  
**Los Lunes, Hágase Rico**

## **Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información – 2022**

Código: 120-DI-D002  
Versión: 1  
Fecha: 21/06/2018  
Página: 16 de 35

Cada dueño de proceso debe diligenciar el Formato Seguimiento de de la siguiente forma:

- a) **Actividades a ejecutar en el período:** Del Formato de Planes copie las actividades que se debían ejecutar en el período evaluado.
- b) **% Peso de la Actividad:** Del Formato de Planes relacione el peso de las actividades que se debían ejecutar en el período evaluado.
- c) **Conversión %:** Se debe determinar el porcentaje de las actividades a evaluar en el periodo sobre un valor del 100%. Como ya se conoce el porcentaje de las actividades para todo el plan, hay que determinarlo solo para el periodo a evaluar; para esto se debe utilizar una regla de tres simple.
- d) **Evidencia/Observaciones:** Se debe escribir lo que da evidencia del cumplimiento de la realización de la actividad. Ejemplo: Procedimiento vxxx versión 2, informe de análisis xxx, acta de reunión, etc.
- e) **Fecha Planificada Fin:** Copiar del formato de plan la fecha en la que se debía terminar la actividad. (dd/mm/aa). h. **Fecha Real:** Escribir la fecha (dd/mm/aa) en la que realmente se terminó de ejecutar la actividad.
- f) **Diferencia:** Hacer la diferencia (resta) entre las dos fechas anteriores.
- g) **Costo Planificado:** Copiar del Formato de plan el costo de la actividad inicialmente estimado.
- h) **Costo Real:** Escribir el costo real de la actividad. I. **Diferencia:** Hacer la diferencia (resta) entre los dos valores anteriores. Las columnas de cumple / No cumple serán diligenciadas por la Oficina de Control Interno cuando haga la verificación de la ejecución de los planes.

### **13. IDENTIFICACIÓN DE RIESGOS**

#### **11.1. Clasificación de los riesgos**

Durante la etapa de identificación, se realiza una clasificación del riesgo, según sus características, con el fin de orientar la formulación de un tratamiento adecuado que posibilite la mitigación del riesgo mediante la definición de controles y planes de manejo:

<b>Clases de riesgo</b>	<b>Definición</b>
Estratégico	Son los riesgos relacionados con la misión y el cumplimiento de los objetivos estratégicos, la definición de políticas, diseño y conceptualización de la entidad por parte de la alta gerencia.



**Empresa Industrial y Comercial**  
**Lotería de Cundinamarca**  
**Los Lunes, Hágase Rico**

**Plan de Tratamiento de  
Riesgos de Seguridad y  
Privacidad de la  
Información – 2022**

Código: 120-DI-D002  
Versión: 1  
Fecha: 21/06/2018  
Página: 17 de 35

<b>Clases de riesgo</b>	<b>Definición</b>
	Se asocia con la forma en que se administra la entidad, su manejo asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la clara definición de políticas, diseño y conceptualización de la entidad por parte de la alta dirección.
Operativo	Relacionados con el funcionamiento y operatividad de los sistemas de información de la entidad: definición de procesos, estructura de la entidad, articulación entre dependencias. Comprenden riesgos provenientes del funcionamiento y operatividad de información institucional, de la definición de los procesos, de la estructura de la entidad, de la articulación entre los procesos.
Financieros	Relacionados con el manejo de los recursos de la entidad: ejecución presupuestal, elaboración estados financieros, pagos, manejos de excedentes de tesorería y manejo de los bienes. Se relacionan con el manejo de los recursos de la empresa, que incluyen la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes financieros y el manejo sobre los bienes.
Cumplimiento	Capacidad de cumplir requisitos legales, contractuales, ética pública y compromiso con la comunidad. Se asocian con la capacidad de la entidad para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad.
Tecnología	Capacidad para que la tecnología disponible satisfaga las necesidades actuales y futuras y el cumplimiento de la misión. Están relacionados con la capacidad tecnológica de la entidad para satisfacer sus necesidades actuales y futuras y el cumplimiento de la misión.
Imagen	Tienen que ver con la credibilidad, confianza y percepción de los usuarios de la entidad. Están relacionados con la percepción y la confianza por parte de la ciudadanía hacia la empresa.
Corrupción	Relacionados con acciones, omisiones, uso indebido del poder, de los recursos o de la información para la obtención de un beneficio particular o de un tercero.

## **11.2. Análisis de Riesgos**



**Empresa Industrial y Comercial**  
**Lotería de Cundinamarca**  
**Los Lunes, Hágase Rico**

## **Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información – 2022**

Código: 120-DI-D002  
Versión: 1  
Fecha: 21/06/2018  
Página: 18 de 35

El análisis del riesgo busca establecer la probabilidad de ocurrencia del mismo y sus consecuencias, calificándolos y evaluándolos con el fin de obtener información para establecer el nivel de riesgo.

Se han establecido dos aspectos a tener en cuenta en el análisis de los riesgos identificados, probabilidad e impacto. Por la primera se entiende la posibilidad de ocurrencia del riesgo; esta puede ser medida con criterios de Frecuencia, si se ha materializado, o de Factibilidad teniendo en cuenta la presencia de factores internos y externos que pueden propiciar el riesgo, aunque éste no se haya materializado. Por Impacto se entiende las consecuencias que puede ocasionar a la Entidad la materialización del riesgo. La etapa de análisis de los riesgos se divide en:

### **11.2.1. Calificación del riesgo**

Se logra a través de la estimación de la probabilidad de su ocurrencia y el impacto que puede causar la materialización del riesgo. La primera representa el número de veces que el riesgo se ha presentado en un determinado tiempo o puede presentarse, y la segunda se refiere a la magnitud de sus efectos. Para la determinación de la calificación del riesgo, con base en la probabilidad y el impacto se debe tener en cuenta las siguientes tablas:

<b>Escala para calificar la probabilidad del riesgo</b>		
<b>Nivel</b>	<b>Concepto</b>	<b>Frecuencia</b>
<b>Raro</b>	El evento puede ocurrir solo en circunstancias excepcionales.	No se ha presentado en los últimos 5 años.
<b>Improbable</b>	El evento puede ocurrir en algún momento.	Al menos de 1 vez en los últimos 5 años.
<b>Moderado</b>	El evento podría ocurrir en algún momento.	Al menos de 1 vez en los últimos 2 años.
<b>Probable</b>	El evento probablemente ocurrirá en la mayoría de las circunstancias.	Al menos de 1 vez en el último año.
<b>Casi certeza</b>	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de 1 vez al año.



**Empresa Industrial y Comercial**  
**Lotería de Cundinamarca**  
**Los Lunes, Hágase Rico**

**Plan de Tratamiento de  
Riesgos de Seguridad y  
Privacidad de la  
Información – 2022**

Código: 120-DI-D002  
Versión: 1  
Fecha: 21/06/2018  
Página: 19 de 35

Para la definición del impacto se debe tener en cuenta la clasificación del riesgo (Estratégico, operativo, financieros, cumplimiento, tecnología, imagen) de acuerdo con la clase del riesgo y la magnitud del impacto se debe determinar el nivel en el que se encuentra.

**Escala para calificar el impacto del riesgo**

Tipos de efecto o impacto		a) Estratégico	b) Operativo	c) Financieros	d) Cumplimiento	e) Tecnología	f) Imagen
<b>INSIGNIFICANTE</b>	Si el hecho llegara a presentarse, tendría consecuencias o efectos mínimos o bajos sobre la institución	Afecta el cumplimiento de algunas actividades	Genera ajustes a una actividad concreta	La pérdida financiera no afecta la operación normal de la institución	Genera un requerimiento	Afecta a una persona o una actividad del proceso	Afecta a un grupo de servidores del proceso
<b>MENOR</b>	Si el hecho llegara a presentarse, tendría bajo impacto o efecto sobre la institución	Afecta el cumplimiento de las metas del proceso	Genera ajustes en los procedimientos	La pérdida financiera afecta algunos servicios administrativos de la institución	Genera investigaciones disciplinarias, y/o fiscales y/o penales	Afecta el proceso	Afecta a los servidores del proceso
<b>MODERADO</b>	Si el hecho llegara a presentarse tendría medianas consecuencias o efectos sobre la Institución	Afecta el cumplimiento de las metas de un grupo de procesos	Genera ajustes o cambios en los procesos	La pérdida financiera afecta considerablemente la prestación del servicio	Genera interrupciones en la prestación del bien o servicio	Afecta varios procesos de la institución	Afecta a todos los servidores de la institución
<b>MAYOR</b>	Si el hecho llegara a presentarse tendría altas consecuencias o efectos sobre la institución	Afecta el cumplimiento de las metas de la institución	Genera intermitencia en el servicio	La pérdida financiera afecta considerablemente el presupuesto de la institución	Genera sanciones	Afecta a toda la entidad	Afecta el sector



**Empresa Industrial y Comercial**  
**Lotería de Cundinamarca**  
**Los Lunes, Hágase Rico**

**Plan de Tratamiento de  
Riesgos de Seguridad y  
Privacidad de la  
Información – 2022**

Código: 120-DI-D002  
Versión: 1  
Fecha: 21/06/2018  
Página: 21 de 35

<b>CATASTRÓFICO</b>	Si el hecho llegara a presentarse tendría desastrosas consecuencias o efectos sobre la institución	Afecta el cumplimiento de las metas del sector y del gobierno	Genera paro total de la institución	Afecta al presupuesto de otras entidades o a de la del departamento	Genera cierre definitivo de la institución	Afecta al Departament o	Afecta al Departamento, Gobierno, Todos los usuarios de la institución
---------------------	--	---	-------------------------------------	---	--	-------------------------	--



**Empresa Industrial y Comercial**  
**Lotería de Cundinamarca**  
Los Lunes, Hágase Rico

## Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

Código: 110-DI-D002  
Versión: 1  
Fecha: 21/06/2018  
Página: 22 de 33

### 11.2.2. Evaluación del riesgo

Permite comparar los resultados de la calificación, con los criterios definidos para establecer el grado de exposición al riesgo; de esta forma, se define la zona de ubicación del riesgo inherente (antes de la definición de controles). La evaluación del riesgo se calcula con base en variables cuantitativas y cualitativas.

PROBABILIDAD	IMPACTO				
	Insignificante	Menor	Moderado	Mayor	Catastrófico
Raro	B	B	B	M	M
Improbable	B	M	M	A	A
Moderado	B	M	A	A	E
Probable	M	A	A	E	E
Casi certeza	M	A	E	E	E

Color	Zona de riesgo
E	Zona de riesgo extrema
M	Zona de riesgo moderada
A	Zona de riesgo alta
B	Zona de riesgo baja

Con la evaluación del riesgo, previa a la formulación de controles se obtiene la ubicación del riesgo en la matriz de evaluación; esto se denomina **evaluación del riesgo inherente**.

### 11.2.3. Matriz de Valoración del Riesgo



**Empresa Industrial y Comercial**  
**Lotería de Cundinamarca**  
Los Lunes, Hágase Rico

## Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

Código: 110-DI-D002  
Versión: 1  
Fecha: 21/06/2018  
Página: 23 de 33


ZONA DE RIESGO	QUÉ SE REQUIERE
Extrema	Es obligatorio tomar acciones sobre las actividades que generan riesgo.
Alta	Reducir el riesgo, evitar, compartir o transferir
Moderada	Se deberán definir las opciones de tratamiento teniendo en cuenta: a. Presupuesto disponible después de dar tratamiento a los riesgos de la Zona Extrema. b. Disponibilidad del Recursos Físicos.
Baja	Si no hay excedente de recursos (económicos, humanos, de infraestructura) no es necesario tomar acciones.

### 11.2.4. Desarrollo práctico - Análisis

Formato de Análisis de riesgos, el cual hace parte del proceso Administración del Sistema Integrado de Gestión, donde se debe relacionar la siguiente información:

- **Riesgo:** Relacionar el riesgo redactado en el formato Identificación de riesgos
- **Calificación de probabilidad:** de acuerdo con la información cuantitativa y cualitativa
- **Calificación de impacto:** de acuerdo con la información cuantitativa y cualitativa que
- **Clasificación del riesgo:** Ver componentes de la identificación del riesgo, en el apartado de clasificación de los riesgos.
- **Evaluación:** surge del cruce de los resultados cuantitativos de la calificación para probabilidad e impacto;



 <p><b>Empresa Industrial y Comercial</b> <b>Lotería de Cundinamarca</b> <b>Los Lunes, Hágase Rico</b></p>	<p align="center"><b>Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información</b></p>	<p>Código: 110-DI-D002 Versión: 1 Fecha: 21/06/2018 Página: 24 de 33</p>
---	---	--

## 11.2.5. Valoración y Análisis de Riesgos

### GESTIÓN INFORMÁTICA

Brindar y mantener la Infraestructura Tecnológica de la Lotería, Hardware, Software y Comunicaciones, presentando las propuestas de innovación tecnológica, que apoyen la creación de nuevos productos.

Posibilidad de recibir o solicitar dadas o beneficios a nombre propio o de terceros para debilitar las políticas y tratamientos del sistema de información y el uso del parque tecnológico

#### CAUSAS

Vulnerabilidad del Sistema de Información  
Manipulación, alteración y falta de integralidad en el uso de la información  
Pérdida de Información por falta de copias de seguridad

#### EFFECTOS

Pérdida de Información

#### CONTROLES

Políticas de seguridad de la información y Política de uso de equipos debidamente adoptada y aprobada

Backup de los equipos de los usuarios y relación de permisos y perfiles otorgados.

#### ANÁLISIS DEL RIESGO DETERMINADO:

- a. Falta de control en el uso de perfiles – de usuario y contraseñas
  - Falta de seguridad en el uso de los PC's institucionales para evitar el uso de equipos
  - Ingreso de funcionarios y de personal no autorizado a los PC's de la Empresa
  - Pérdida de imagen / credibilidad / confianza/ clientes, usuarios insatisfechos
- b. Pérdida de Información por falta de copias de seguridad



**Empresa Industrial y Comercial**  
**Lotería de Cundinamarca**  
**Los Lunes, Hágase Rico**

## **Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información**

Código: 110-DI-D002  
Versión: 1  
Fecha: 21/06/2018  
Página: 25 de 33

Sistemas de Información Susceptibles de manipulación y/o adulteración.  
Usar la información de la Empresa para favorecer a propios o a terceros.  
Afectación a los objetivos estratégicos de la Institución  
Pérdida de imagen / credibilidad / confianza/ clientes, usuarios insatisfechos

c. Susceptibilidad a la pérdida de información

Concentración de información de determinadas actividades o procesos en una persona.  
Manipulación susceptible de la información o filtración de la misma  
Pérdida de imagen / credibilidad / confianza/ clientes, usuarios insatisfechos

d. Falta de control o política de Manejo institucional de mail y web


Filtración de información y pérdida de tiempo laboral en el uso de la tecnología fuera de lo requerido por la institucionalidad  
Uso y manejo indebido del sistema de información y de la información institucional  
Afectación a los objetivos estratégicos de la Institución

e. Política de uso y manejos de equipos

Falta de identificación de los usuarios que permita la identificación del mismo; permitiendo el uso de la información institucional o suministrada en los procesos propios  
Uso y manejo indebido del sistema de información y de la información institucional Afectación a los objetivos estratégicos de la Institución

### **11.2.6. ACCIONES PREVENTIVAS**

- a. Establecer los responsables y puntos de control para el manejo del Sistema Integrado de Información
- b. Capacitar a los funcionarios involucrados en el manejo del Sistema Integrado de Información
- c. Publicar en la página web de los Derechos de los ciudadanos y medios para garantizarlos (en relación con la actividad de la Lotería).

 <p><b>Empresa Industrial y Comercial</b> <b>Lotería de Cundinamarca</b> <b>Los Lunes, Hágase Rico</b></p>	<p><b>Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información</b></p>	<p>Código: 110-DI-D002 Versión: 1 Fecha: 21/06/2018 Página: 26 de 33</p>
---	--	--

#### 11.2.7. TRASPARENCIA

- d. Todas las normas generales y reglamentarias, políticas, lineamientos o manuales, las metas y objetivos de las Dependencias, de conformidad con sus programas operativos y los resultados de las auditorías al ejercicio presupuestal e indicadores de desempeño
- e. Publicar la información establecida en la Estrategia de Gobierno en Línea, adoptando el esquema de publicación de conformidad con la Ley 1712 de 2014 y difundirlo a través de la página web de la Empresa
- f. Las clases de información que la Empresa debe publicar de manera proactiva y que en todo caso deberá comprender la información mínima obligatoria
- g. La periodicidad de la divulgación, acorde a los principios administrativos de la función pública.

#### 14. PREVENCIÓN DEL FRAUDE, LA PRIORIDAD DE LOS SECTORES PÚBLICO Y PRIVADO

El uso del análisis de datos para la seguridad y protección de la información trae resultados impactantes, que se ven desde la analítica como una ficha clave en la toma de decisiones.

En los últimos años, la tecnología se ha convertido en la guía a seguir de las entidades, pues resulta ser un factor clave no solo para identificar problemas, sino también para hacer un completo estudio de la situación de cada proceso en la entidad y así poder establecer la estrategia más adecuada.

Es por esto que la analítica se ha convertido en una oportunidad para obtener información relevante de manera que las entidades puedan hacer análisis predictivos, anticipar los problemas y prevenir situaciones de riesgo.

Para nadie es un secreto que un negocio que necesita de herramientas como la analítica para crecer y mantenerse firme en el mercado y que son capaces de medir según las necesidades de la entidad y la proyección de seguridad institucional en el caso de la Lotería, desde el momento en que sale a la venta el producto como parte fundamental del sistema de información.

Tal y como ocurre en la mayoría de empresas donde los gerentes se apoyan del análisis de datos para la toma de decisiones, en la lotería se debe acudir a la



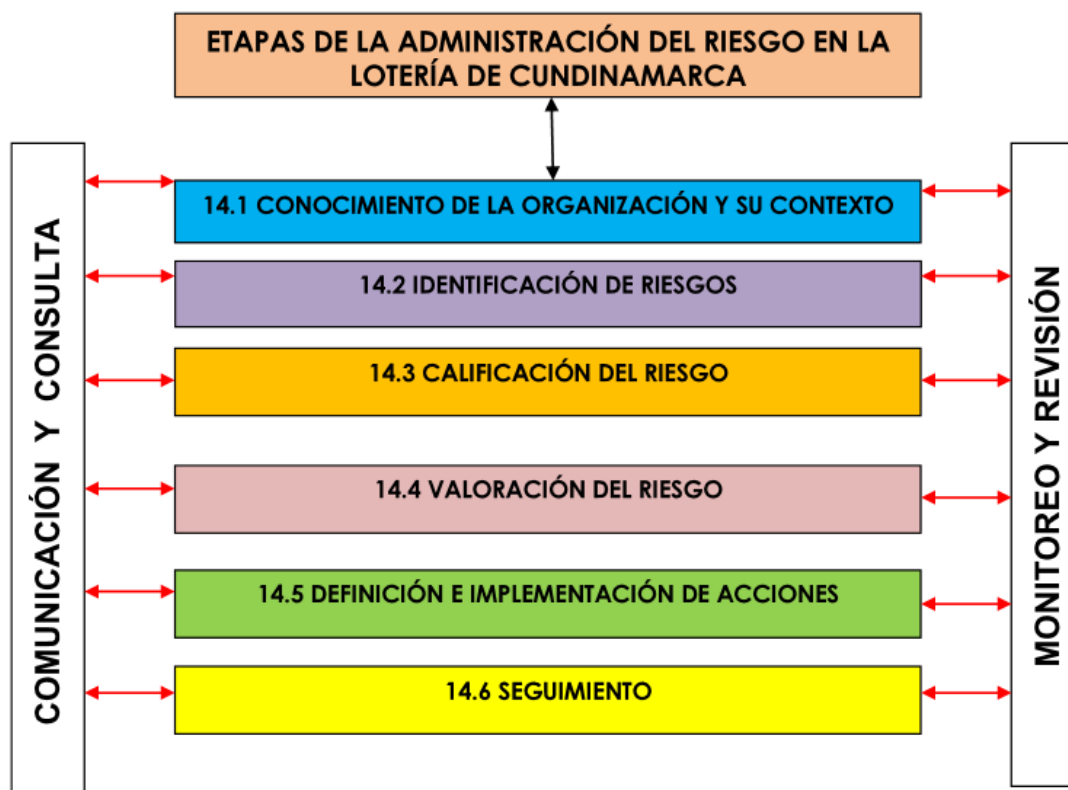
**Empresa Industrial y Comercial**  
**Lotería de Cundinamarca**  
**Los Lunes, Hágase Rico**

## Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

Código: 110-DI-D002  
Versión: 1  
Fecha: 21/06/2018  
Página: 27 de 33

analítica para crear estrategias de contingencias de manejos de riesgos y para seguir dentro del sector industrial del juego y el azar.

### 15. ETAPAS PARA LA ADMINISTRACIÓN DEL RIESGO




Fuente: Elaboración propia

### 16. RIESGOS INHERENTES A LA GESTIÓN DE SEGURIDAD Y PROTECCIÓN DE INFORMACIÓN

#### Riesgos

Definir de manera incorrecta las necesidades a cubrir o para dar solución dentro de las características del sistema de información.

#### Causas

 <p><b>Empresa Industrial y Comercial</b> <b>Lotería de Cundinamarca</b> <b>Los Lunes, Hágase Rico</b></p>	<p><b>Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información</b></p>	<p>Código: 110-DI-D002 Versión: 1 Fecha: 21/06/2018 Página: 28 de 33</p>
---	--	--

Los análisis de la información de los requerimientos fueron definidos de manera según las necesidades a cubrir

### **Efectos**

Afectación a los objetivos estratégicos de la Institución, por la mala Planificación del Sistema de Información

### **Controles Preventivos**

Plan de Acción

PROBABILIDAD	IMPACTO (si se materializara)	CALIFICACION
3	4	12

### **Controles Correctivos**

Se realizan acciones cuando se presenta la necesidad dentro del Sistema

### **Riesgos**

Incumplir con la atención a los requerimientos que permitan un buen funcionamiento del sistema

### **Causas**

No se genera por parte de los usuarios un análisis cierto de la necesidad que permita hacer seguimiento y análisis de los requerimientos.

### **Efectos**

Afectación al recurso humano por la mala atención en los procesos de mantenimiento de equipos y de requerimientos de mejoramiento del Sistema de Información.

### **Controles Preventivos**

Plan de Acción

PROBABILIDAD	IMPACTO (si se materializara)	CALIFICACION
4	4	12

### **Controles Correctivos**

Seguimiento al Plan de acción y generación de controles



**Empresa Industrial y Comercial**  
**Lotería de Cundinamarca**  
**Los Lunes, Hágase Rico**

## **Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información**

Código: 110-DI-D002  
Versión: 1  
Fecha: 21/06/2018  
Página: 29 de 33

### **Riesgos**

Incumplir la planeación y el cumplimiento de los objetivos del Plan estratégico al tener dificultades en la identificación correcta los indicadores

### **Causas**

El análisis de indicadores, el seguimiento al plan de acción, y al cumplimiento de las políticas informáticas.

### **Efectos**

Afectación a los objetivos estratégicos de la Institución, y afectación en el análisis y gestión de tratamiento de la información generada por los indicadores

### **Controles Preventivos**

Matriz de indicadores

<b>PROBABILIDAD</b>	<b>IMPACTO (si se materializara)</b>	<b>CALIFICACION</b>
3	3	9

### **Controles Correctivos**

No hay

### **Riesgos**

Incumplimiento de la política genere consecuencias en el tratamiento de datos, uso de los canales de internet y planeación de los indicadores

### **Causas**

Que los funcionarios no conozcan la Política de Uso y Manejo de los medios Tecnológicos, los objetivos de cumplimiento al mismo, y seguimiento al Plan de Contingencia del uso de la información.

### **Efectos**

Pérdida de imagen / credibilidad / confianza en el sistema de Información, que genere pérdidas económicas por el mal tratamiento de datos que generan la información



**Empresa Industrial y Comercial**  
**Lotería de Cundinamarca**  
**Los Lunes, Hágase Rico**

## **Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información**

Código: 110-DI-D002  
Versión: 1  
Fecha: 21/06/2018  
Página: 30 de 33

Afectación a los Objetivos de la institución. Que no se cuente con los recursos requeridos en el incumplimiento del tratamiento de datos que genere consecuencias en casos fortuitos como la pérdida de la información

### **Controles Preventivos**

Plan de Acción

Plan de tratamiento de datos

Política de Manejo y Uso de los medios tecnológicos

<b>PROBABILIDAD</b>	<b>IMPACTO (si se materializara)</b>	<b>CALIFICACION</b>
3	4	12

### **Controles Correctivos**

Plan de contingencia

### **Riesgos**

Incumplimiento de la información de la vida útil de los equipos de computo

### **Causas**

No existe control de ruta de la vida útil de los equipos de cómputo, ni hoja de vida de los mismos

### **Efectos**

Afectación al bienestar y motivación del Recurso Humano  
Pérdida de equipos por falta de mantenimiento Preventivo y correctivo

### **Controles Preventivos**

Plan de Acción

Programación de Mantenimientos Preventivos de equipos

<b>PROBABILIDAD</b>	<b>IMPACTO (si se materializara)</b>	<b>CALIFICACION</b>
3	5	15

### **Controles Correctivos**



**Empresa Industrial y Comercial**  
**Lotería de Cundinamarca**  
**Los Lunes, Hágase Rico**

## **Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información**

Código: 110-DI-D002  
Versión: 1  
Fecha: 21/06/2018  
Página: 31 de 33

Plan de mantenimiento correctivo.  
Contrato de Mantenimiento

### **17. RIESGOS INHERENTES AL A GESTIÓN DE SEGURIDAD Y PROTECCIÓN DE LOS EQUIPOS DE INFORMACIÓN**

#### **Riesgos**

No acceso oportuno a la información de la Empresa.

#### **Causas**

Daño físico en los equipos de cómputo y servidores.

#### **Efectos**

Interrupción en la Prestación del Servicio  
Programación de Mantenimientos Preventivos de equipos y control de ruta de la vida útil de los equipos de cómputo, ni hoja de vida de los mismos

#### **Controles Preventivos**

Instructivo Mantenimiento Preventivo y Correctivo LC-OPI-GI-I001

#### **Controles Correctivo**

Procedimiento Solución a Requerimientos de Hardware y Software LC-OPI-GI-P004

<b>PROBABILIDAD</b>	<b>IMPACTO (si se materializara)</b>	<b>CALIFICACION</b>
3	5	15

#### **Riesgos**

Pérdida de Información en el Servidor de Producción Linux.

#### **Causas**

Que no se realice el respectivo Backup del Sistema de Información.

#### **Efectos**

Pérdida de imagen / credibilidad / confianza/ clientes, usuarios insatisfechos

#### **Controles Preventivos**

Procedimiento Backup del Sistema de Información





**Empresa Industrial y Comercial**  
**Lotería de Cundinamarca**  
Los Lunes, Hágase Rico

## Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

Código: 110-DI-D002  
Versión: 1  
Fecha: 21/06/2018  
Página: 32 de 33

### Controles Correctivo

Procedimiento Backup del Sistema de Información .

PROBABILIDAD	IMPACTO (si se materializara)	CALIFICACION
3	5	15

### Riesgos

Fallas en la asignación de perfiles de usuarios.

### Causas

Que no estén definidos claramente los perfiles de acceso al Sistema de Información.

### Efectos

Afectación a la Confidencialidad de la Información

### Controles Preventivos

Instructivo de Perfiles LC-OPI-GI-I005

### Controles Correctivo

Instructivo de Perfiles LC-OPI-GI-I005

PROBABILIDAD	IMPACTO (si se materializara)	CALIFICACION
3	5	15

### Riesgos

Demora en la respuesta de los sistemas de apoyo.

### Causas

Alteración de las condiciones ambientales en el Centro de Cómputo.

### Efectos

Interrupción en la Prestación del Servicio

### Controles Preventivos

### Controles Correctivo

PROBABILIDAD	IMPACTO (si se materializara)	CALIFICACION
3	5	15



**Empresa Industrial y Comercial**  
**Lotería de Cundinamarca**  
**Los Lunes, Hágase Rico**

## **Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información**

Código: 110-DI-D002  
Versión: 1  
Fecha: 21/06/2018  
Página: 33 de 33

### **Riesgos**

No envío oportuno de los informes o reportes por parte de los funcionarios a los Entes de Control.

### **Causas**

Caída del servicio del proveedor de Internet que afecta la red interna y externa.

### **Efectos**

Afectación a la Disponibilidad de la Información

### **Controles Preventivos**

Instructivo de Presentación de Informes

### **Controles Correctivo**

Instructivo de Presentación de Informes

<b>PROBABILIDAD</b>	<b>IMPACTO (si se materializara)</b>	<b>CALIFICACION</b>
3	5	15



**Empresa Industrial y Comercial**  
**Lotería de Cundinamarca**  
**Los Lunes, Hágase Rico**

**Plan de Tratamiento de  
Riesgos de Seguridad y  
Privacidad de la  
Información**

Código: 110-DI-D002  
Versión: 1  
Fecha: 21/06/2018  
Página: 34 de 33