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

<

Empresa Industrial y Comercial del Estado Administradora del Monopolio
Rentístico de los Juegos de Suerte y Azar

COLJUEGOS EICE
Bogotá D.C., enero 2021

Tabla de contenido

1. Introducción 3
2. Objetivo General 3
2.1. Objetivos Específicos 3
3. Marco normativo 3
4. Alcance 4
5. Marco Referencial 4
6. Desarrollo metodológico 4
7. Metodología - Plan de tratamiento 5
8. Recursos 7
9. Medición del modelo de seguridad y privacidad de la información 7

1. Introducción

El plan de tratamiento de riesgos Sistema de Gestión de la Seguridad de la Información (**SGSI**), está orientado a una cultura de carácter preventivo que permita establecer las acciones para la reducción de la afectación en el caso de materialización, de igual manera en el presente documento se desarrollará estrategias para el tratamiento, evaluación y monitoreo de los riesgos, con el propósito de no comprometer los objetivos demarcados por **la Empresa Industrial y Comercial del Estado Administradora del Monopolio Rentístico de los Juegos de Suerte y Azar – Coljuegos.**

2. Objetivo General

Definir y aplicar los lineamientos para el tratamiento de los riesgos de Seguridad de la Información, de tal manera que permita alcanzar los objetivos propuestos, la misión y visión institucional, alcanzando la integridad, confidencialidad, disponibilidad y autenticidad de la información.

2.1. Objetivos Específicos

- Dar cumplimiento con los requisitos legales y reglamentos aplicables.

- Gestionar el tratamiento de los riesgos de Seguridad de la Información.

3. Marco normativo

Documento CONPES 3854 de 2017 “Política Nacional de Seguridad Digital”

Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones

Decreto 1008 de 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”

ISO 27001:2013 para los Sistemas Gestión de la Seguridad de la Información permite a las organizaciones la evaluación del riesgo y la aplicación de los controles necesarios para mitigarlos o eliminarlos.

ISO 27001:2018, Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información - Descripción general y vocabulario

Guía para la administración del riesgo y el diseño de controles en entidad públicas, Versión 5, diciembre de 2020, Departamento Administrativo de la Función Pública.

Demás normas o políticas aplicables o que modifiquen, adicionen o sustituyan las normas

antes enunciadas.

4. Alcance

El presente documento establece la gestión de los riesgos de seguridad de la información con el fin de integrar los procesos, las buenas prácticas para la toma de decisiones y prevenir incidentes que afecten el logro de los objetivos.

Para la elaboración del plan de tratamientos se tendrá en cuenta la Guía para la administración del riesgo y el diseño de controles en entidad públicas.

5. Marco Referencial

Política de administración de riesgos, cuyo propósito es establecer lineamientos acerca del tratamiento, manejo y seguimiento a los riesgos, los niveles de responsabilidad y las acciones frente a una posible materialización, con el fin de cumplir con los objetivos estratégicos.

COLJUEGOS define su política de administración de riesgos tomando como referente los parámetros del Modelo Integrado de Planeación y Gestión - MIPG, en el cual se articulan los riesgos de gestión, corrupción y seguridad de la información. Así mismo se acoge la metodología elaborada por el Departamento Administrativo de la Función Pública, Secretaria de Transparencia de la Presidencia de la República y el Ministerio de Tecnología de la Información y Comunicaciones, quienes para el efecto elaboraron la Guía para la administración del Riesgo y el Diseño de Controles.

6. Desarrollo metodológico

Fase 1: Análisis de la información En esta etapa se evaluarán los resultados de las entrevistas con cada uno de los procesos, del cual se desarrollarán las siguientes actividades:

- Aplicación de la Política de tratamiento de riesgos.
- Revisión de riesgos.
- Valoración de riesgos.

Fase 2: Revisión y análisis de las acciones de tratamiento. En esta fase se realizarán las actividades que permitan la estructuración de las acciones de tratamiento.

- Determinar el nombre de la acción de tratamiento.
- Definición de las acciones de tratamiento relacionadas con cada riesgo.
- Definir los responsables de cada acción de tratamiento.
- Definir las fechas en las que se desarrollarán las acciones de tratamiento.
- Análisis de la aplicabilidad de las acciones de tratamiento.

Fase 3: Consolidación de la matriz de riesgos: En esta fase se realizará la consolidación de la matriz de riesgos identificados por cada uno de los procesos, estará liderada por la Oficina Asesora de Planeación.

Fase 4: Ciclo de vida del tratamiento de riesgos: Realizar seguimiento a cada una de las acciones de tratamiento establecidas, basado en las fechas de cumplimiento, entregable y responsable.

7. Metodología - Plan de tratamiento

El plan de tratamiento de riesgos contempla la definición de las actividades a desarrollar en aras de mitigar los riesgos, estructurada por tareas, responsable, fecha y entregables, atendiendo las recomendaciones de la Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información

Actividad	Tarea	Responsable	Fecha	Entregable
Actualizar Política de administración de riesgos con respecto a la Seguridad a la Información	Validar si la política administración de riesgos se debe modificar teniendo en cuenta las nuevas reglas del DAFP	Oficina Asesora de Planeación	30-06-2021	Política administración de riesgos
Actualizar Política de administración de riesgos con respecto a la Seguridad a la Información	Socializar la política de administración de riesgos (*si se generan modificaciones)*	Oficina Asesora de Planeación	30-06-2021	Campaña de socialización efectuada
Actualizar documentación de administración de riesgos con respecto a la Seguridad a la Información	Actualizar la documentación relacionada con la administración de riesgos en el SINGE *(si se genera modificaciones en la política de administración de riesgos)*	Oficina Asesora de Planeación	30-06-2021	Documentación de riesgos actualizada
Actualizar los activos de información.	Actualizar los activos de información.	Líder del proceso / Oficina de Tecnología	30-06-2021	Instrumento activos de información.

Validar los activos de información	Validar los activos de información reportados por cada líder de Proceso.	Líder del proceso / Oficina de Tecnología y Oficina Asesora de Planeación	31-12-2021	Instrumento activos de información.
Consolidar la matriz de activos de información	Consolidar la matriz de activos de información reportados por cada líder de Proceso	Oficina de Tecnología	31-12-2021	Instrumento activos de información
Publicar los activos de información	Publicar los activos de información en transparencia.	Oficina Asesora de Planeación	31-12-2021	Cuadro de pantalla reporte de publicación.
Revisión de los Riesgos de Seguridad de la Información	Analizar si dentro de la revisión de los riesgos para la entidad están contemplados los riesgos de fraude electrónico para los juegos en línea y tiempo real.	Oficina Asesora de Planeación.	31-12-2021	Matriz de riesgos
Revisión de los Riesgos de Seguridad de la Información	Analizar si los riesgos relacionados con pérdidas de recursos y/o vulnerabilidad de la información, deberían estar ubicados en zona de riesgo extrema	Oficina Asesora de Planeación.	31-12-2021	Matriz de riesgos
Aprobación Matriz de Riesgos	Aprobación de la matriz de riesgos y los planes de tratamiento	Comité Institucional de Control Interno.	31-12-2021	Acta de aprobación.
Publicación	Publicación de la Matriz de riesgos	Oficina Asesora de Planeación.	31-12-2021	Cuadro de pantalla de registro de publicación

Los controles seleccionados serán confrontados con los estándares ISO 27001:2013 y su anexo A; a fin de determinar las falencias de la **Empresa Industrial y Comercial del Estado Administradora del Monopolio Rentístico de los Juegos de Suerte y Azar**.

8. Recursos

Las actividades señaladas anteriormente se realizarán con los profesionales con los que cuentan las áreas responsables, no se utilizarán recursos adicionales

9. Medición del modelo de seguridad y privacidad de la información

La medición se realiza a través de indicadores de gestión que está orientada principalmente en la medición de eficacia de los componentes de implementación y gestión definidos en el modelo de operación del marco de seguridad y privacidad de la información, indicador que se alimenta de indicadores internos en el marco de la implementación del Eje de Seguridad de la Información y que servirán como insumo para el componente de mejora continua permitiendo adoptar decisiones de mejora sobre Seguridad de la informa.