CORPORACIÓN AUTÓNOMA REGIONAL DE BOYACÁ
CORPOBOYACÁ

PLAN DE TRATAMIENTO DEL RIESGO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

Corpoboyacá

Región estratégica para la sostenibilidad

SOPORTE TECNOLÓGICO
SUBDIRECCIÓN DE PLANEACIÓN Y SISTEMAS DE INFORMACIÓN
CORPOBOYACÁ
Enero, 2024

TABLA DE CONTENIDO

1. INTRODUCCIÓN

La Corporación Autónoma Regional de Boyacá, Corpoboyacá, creada por la Ley 99 del 22 de diciembre de 1993, lidera el desarrollo sostenible a través del ejercicio de autoridad ambiental, la administración y protección de los recursos naturales renovables y el ambiente, y la formación de cultura ambiental, de manera planificada y participativa.

Con el crecimiento y uso masivo de los ciudadanos en las Tecnologías de la Información y las Comunicaciones (TIC) en Colombia, se ha reflejado un aumento significativo en la participación digital y uso de las redes de comunicación por parte de los ciudadanos; desafortunadamente, el incremento en la participación digital de los ciudadanos, trae consigo nuevas y más sofisticadas formas para atentar contra la seguridad de la Información; situación que obedece a fortalecer las capacidades institucionales en la adecuada Gestión del Riesgo de Seguridad Digital.

La Seguridad de la Información, como principio de la Política de Gobierno Digital, busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado y de los servicios que prestan al ciudadano, es precisamente por esto que la política nacional de seguridad digital, incluye la gestión de riesgo como uno de los elementos más importantes para abordar la seguridad digital.

El Departamento Administrativo de la Función Pública -DAFP, consolida lineamientos para la administración de riesgos en la “Guía para la administración del riesgo y el diseño de controles en entidades públicas” con el fin de facilitar la identificación y tratamiento de riesgos

Corpoboyacá entendiendo la importancia de una adecuada gestión de la información y los riesgos sobre la misma, requiere contar con un Plan de Tratamiento del Riesgo, de acuerdo a la guía mencionando anteriormente, como metodología de gestión de riesgo de seguridad de la información, al Modelo de Seguridad y Privacidad de la Información –MSPI de Corpoboyacá.

El presente plan tiene el propósito de presentar los objetivos, alcance, marco legal, actividades a desarrollar del Plan de Tratamiento del Riesgo en Seguridad y Privacidad de la Información (PTRI), la gestión de activos, la gestión de riesgos, para la continuidad en la prestación de los servicios ofrecidos por la Entidad.

2. OBJETIVO GENERAL

Establecer el Plan de Tratamiento del Riesgo de Seguridad y Privacidad de la Información de la Corporación Autónoma Regional de Boyacá, Corpoboyacá, con las actividades de identificación de activos de información, establecimiento de riesgos en seguridad digital, análisis y valoración de los riesgos asociados; que permitan el aseguramiento y protección de los activos de información, de manera que le permita minimiza los riesgos asociados a los activos de información.

3. OBJETIVOS ESPECIFICOS

- ✓ Realizar la Identificación y actualización de activos de información
- ✓ Establecer los riesgos en seguridad digital.
- ✓ Realizar análisis y valoración de los riesgos asociados de los activos de información considerados como críticos en la Entidad.
- ✓ Administrar los riesgos de seguridad de la información para mantenerlos en niveles aceptables.

4. ALCANCE

El alcance del presente Plan de Tratamiento del Riesgo -PTRI es el de identificar y actualizar los activos de información que resulten críticos para la Entidad, para su posterior análisis, valoración y tratamiento de los riesgos asociados a la seguridad digital.

5. MARCO LEGAL APLICABLE

- **Constitución Política de Colombia de 1991,** Articulo 15, consagra que todas las personas tienen el derecho a su intimidad personal y familiar y a su buen nombre. De igual modo, tienen el derecho a conocer, actualizar y a rectificar las informaciones que hayan recogido sobre ellas en los bancos de datos y en los archivos de las entidades públicas y privadas.
- **Ley 23 de 1982,** Ley de propiedad intelectual y derechos de autor.
- **Ley 527 de 1999,** Ley por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación.
- **Ley 594 de 2000**, Ley General de Archivos, la presente ley tiene por objeto establecer las reglas y principios generales que regulan la función archivística del Estado.
- **Ley 1266 de 2008**, Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
- **Ley 1437 de 2011**, Código de procedimiento Administrativo y de lo contencioso
- administrativo
- **Ley Estatutaria 1581 de 2012,** Por la cual se dictan disposiciones generales para la protección de datos personales. Reglamentada parcialmente en el decreto 1377 de 2013 y en el capítulo 25 del decreto 1074 de 2015,
- **Decreto 2578 de 2012,** Por medio del cual se reglamenta el Sistema Nacional de Archivos. Incluye “El deber de entregar inventario de los documentos de archivo a cargo del servidor público, se circunscribe tanto a los documentos físicos en archivos tradicionales, como a los documentos electrónicos que se encuentren en equipos de cómputo, sistemas de información, medios portátiles” entre otras disposiciones.
- **Decreto 2609 de 2012,** Por medio del cual se reglamenta el Título V de la Ley General de Archivo del año 2000. Incluye aspectos que se deben considerar para la adecuada gestión de los documentos electrónicos.
- **Norma técnica colombiana NTC/ISO 27001:2013,** Sistema de seguridad de la Información
- **Norma ISO 27001,** Sistemas de Gestión de la Seguridad de la Información.
- **Ley 1712 DE 2014,** Ley de Transparencia y del derecho de acceso a la información pública nacional.
- **Decreto 1078 de 2015,** Decreto único reglamentario del sector de Tecnologías de la Información, por la cual se establece la estrategia de gobierno en línea y dentro de la cual se establece el componente de seguridad y privacidad de la información.
- **CONPES 3854 de 2016,** Política Nacional de Seguridad Digital.
- **Decreto 612 de 2018,** Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.

- **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. Tiene como principio la seguridad de la información, que busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado, y de los servicios que prestan al ciudadano.
- **Decreto 2106 de 2019,** Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública.
- **Resolución 00500 de 2021,** Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital.
- **Decreto 767 de 2022,** 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.

6. TERMINOS Y DEFINICIONES

Activo de Información. Recurso tangible e intangible de los sistemas de información o relacionado con éste, necesario para que la organización funcione correctamente y alcance los objetivos propuestos por su dirección. Entendiendo por cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la entidad. En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, Hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.

Análisis del riesgo. Uso sistemático de la información para identificar las fuentes y calcular el riesgo.

Amenaza. Son los eventos que pueden desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos de información, puede ser de dos tipos: Amenazas internas y Amenazas externas. Una amenaza informática es toda circunstancia, evento o persona que tiene el potencial de causar daño a un sistema en forma de robo, destrucción, divulgación, modificación de datos o negación de servicio (DoS).

Ciberseguridad: Protección de activos de información, mediante el tratamiento de las amenazas que ponen en riesgo la información que se procesa, almacena y transporta mediante los sistemas de información que se encuentran interconectados.

Ciberespacio: Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

Control. Medios para manejar el riesgo; incluyendo políticas, procedimientos, lineamientos, prácticas o estructuras organizacionales, las cuales pueden ser administrativas, técnicas, de gestión o de naturaleza legal. Medida que permite reducir o mitigar un riesgo.

Diagnóstico. Es el análisis que se realiza para determinar cualquier situación y cuáles son las tendencias. Esta determinación se realiza sobre la base de datos y hechos recogidos y ordenados sistemáticamente, que permiten juzgar mejor qué es lo que está pasando.

Evaluación del riesgo. Proceso de comparar el riesgo estimado con un criterio de riesgo dado para determinar la importancia del riesgo.

Evaluación de la Amenaza. Es el proceso mediante el cual se determina la probabilidad de ocurrencia y la severidad de un evento en un tiempo específico y en un área determinada. Representa la ocurrencia estimada y la ubicación geográfica de eventos probables.

Evento de seguridad de la información. Cualquier evento de seguridad de la información es una ocurrencia identificada del estado de un sistema, servicio o red indicando una posible

falla en la política de seguridad de la información o falla en las salvaguardas, o una situación previamente desconocida.

Gestión del riesgo. Actividades coordinadas para dirigir y controlar una organización con relación al riesgo.
Información. Conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.

Impacto. Es la consecuencia negativa sobre un activo de la materialización de una amenaza.

Incidente de seguridad de la información. Evento que atenta contra la confidencialidad, integridad o disponibilidad de la información y los recursos tecnológicos. Evento o una serie de eventos inesperados de seguridad de la información que tienen una probabilidad significativa de comprometer las operaciones comerciales y amenazar la seguridad de la información.

Lineamiento. Una descripción que aclara qué se debiera hacer y cómo, para lograr los objetivos.

MinTic: Sigla de Ministerio de Tecnología y de Comunicaciones del Gobierno de Colombia

MSPI. Sigla de Modelo de Seguridad y privacidad de la Información MSPI, dispuesto a aplicar por las entidades del estado en el marco de la Política de Gobierno Digital por MinTic.

Normas ISO 27000. El estándar ISO 27000 apunta a exigir niveles concretos y adecuados de seguridad informática, niveles necesarios para las empresas que compiten a través del comercio electrónico y que por lo tanto tienen que exponer sus infraestructuras de información.

Política. Intención y dirección general expresada formalmente por la Dirección.

Principios de seguridad de la Información:

- **Confidencialidad.** Es la propiedad de la información, por la que se gestiona que es accesible únicamente a personal autorizado a conocer la información.
- **Integridad.** Garantizar que la información no será alterada, eliminada o destruida por entidades no autorizadas.
- **Disponibilidad.** Asegurar que los usuarios autorizados tendrán acceso a la información cuando la requieran.

Probabilidad: Se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.

Riesgo. Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales. Nota: Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos.

Riesgo de seguridad de la información: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

Riesgo inherente: Nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto, nos permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad.

Riesgo residual: El resultado de aplicar la efectividad de los controles al riesgo inherente.
Seguridad de la información: La seguridad de la información es el conjunto de medidas técnicas, operativas, organizativas, y legales que permiten a las organizaciones resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma.

SGSI: Sistema de Gestión de la Seguridad de la Información, es utilizada para referirse a la gestión de los procesos y mecanismos de control que son utilizados para custodiar y proteger de amenazas la información sensible de las organizaciones. Los SGSI permiten a las organizaciones determinar con objetividad que información requiere ser protegida, por qué debe ser protegida, de qué debe ser protegida y como protegerla mediante la planificación e implantación de políticas, procedimientos y controles que mantengan siempre el riesgo por debajo del nivel asumible por la propia organización.

Tratamiento del riesgo: Proceso de selección e implementación de acciones o medidas para mitigar o reducir el nivel del riesgo. El tratamiento de riesgos consiste en buscar los niveles de riesgos aceptables para la organización.

Vulnerabilidad: Debilidad de un activo que puede ser aprovechada por una amenaza. Una vulnerabilidad es un estado viciado en un sistema informático (o conjunto de sistemas) que afecta las propiedades de confidencialidad, integridad y disponibilidad de los sistemas. Representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

7. POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE CORPOBOYACÁ

"La Corporación Autónoma Regional de Boyacá, Corpoboyacá, velará por preservar la integridad, disponibilidad y confidencialidad de los activos de información de tal forma que contribuyan al logro de los objetivos institucionales, mediante la adopción de buenas prácticas, estableciendo lineamientos, controles y concientizando a las partes interesadas en la gestión de riesgos asociados a los mismos."

La eficiencia de la política de seguridad de la información se construye a través del liderazgo y compromiso y la participación activa de todos los líderes, funcionarios, contratistas y terceros, con quienes mancomunadamente se deberá alcanzar el nivel de cumplimiento de los lineamientos, políticas y requisitos de seguridad de la información, así como el desarrollo de estrategias de seguridad, mejora continua y de gestión frente a incidentes o eventos de seguridad de la información.

7.1. Alcance de la política de seguridad de la información

Las políticas de seguridad digital y de la información establecidas, deben ser conocidas y aplicadas por todos los funcionarios, contratistas, pasantes, administradores de plataformas, proveedores de servicios informáticos y demás partes interesadas que hagan uso de la plataforma tecnológica e informática de la Corporación Autónoma Regional de Boyacá-Corpoboyacá.

8. PLAN DE TRATAMIENTO DEL RIESGO EN SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

En el Plan de Tratamiento del Riesgo en Seguridad y Privacidad - PTRI de la Información, se establecen las siguientes actividades para la gestión adecuada de la gestión del riesgo en seguridad de la información y la continuidad en la prestación de los servicios ofrecidos por la Entidad.

8.1. Plan de actividades para el tratamiento del riesgo en seguridad y privacidad de la información

CRITERIO	ACTIVIDAD	Periodo
PLAN DE TRATAMIENTO DEL RIESGO	Elaboración y publicación del plan del Tratamiento de Riesgo de Seguridad y Privacidad de la Información.	Primer semestre de 2024
IDENTIFICACIÓN DE ACTIVOS DE	Realizar identificación o actualización de los activos de información.	Primer semestre de 2024
IDENTIFICACIÓN DE INFRAESTRUCTURA CRITICA	Realizar identificación de activos que resulte como críticas en la respectiva Matriz de riesgos.	Primer semestre de 2024
IDENTIFICACIÓN DE RIESGOS	Realizar la identificación de riesgos sobre los activos de información considerados como críticos e identificados en la etapa anterior.	Primer semestre de 2024
ANALAISIS Y VALORACION DE RIESGOS DIGITALES	Realizar el análisis del riesgo, identificación de controles de riesgos de los activos de información, previamente identificados.	Primer semestre de 2024
TRATAMIENTO DE RIESGOS DIGITALES	Realizar el tratamiento de riesgos de los activos de información, previamente identificados y considerados como críticos.	Segundo semestre de 2024
MONITOREO Y REVISION	Realizar el monitoreo y la revisión de la matriz de riesgos.	Segundo semestre de 2024

8.2. Políticas de Administración del Riesgo Corpoboyacá

- Las medidas para tratar los riesgos identificados se encaminarán a prevenir su materialización, para lo cual se deben generar los diferentes mecanismos que garanticen el monitoreo de los controles definidos.

- Se deben identificar y monitorear los factores internos y externos que puedan afectar el entorno institucional a fin de establecer y adoptar estrategias, mecanismos y actividades para la gestión integral del riesgo e implementar medidas que permitan reducir los factores identificados mediante la optimización de los procedimientos y la implementación de controles apropiados, definiendo niveles de responsabilidad en un tiempo determinado.

- En caso de materialización de un riesgo identificado, se deben activar los mecanismos definidos dentro del sistema de gestión con el fin de generar una respuesta oportuna frente a su ocurrencia para lo cual es pertinente adelantar el análisis de causa y las acciones de respuesta que permitan su adecuado tratamiento y seguimiento hacia la prevención de posibles eventos similares.

- La Corporación Autónoma Regional de Boyacá – CORPOBOYACÁ, consciente que en el desarrollo de sus actividades se pueden presentar riesgos de corrupción, se compromete a monitorear los factores externos e internos que puedan afectar el entorno institucional a fin de establecer y adoptar estrategias, mecanismos y actividades necesarias para la gestión integral de los mismos acogiendo una autorregulación prudencial, determinando su nivel de exposición frente a los impactos, con el propósito de priorizar su tratamiento y estructurar criterios orientadores para definir controles en la toma de decisiones en pro del mejoramiento continuo, la atención al usuario, la transparencia y el buen gobierno

- Los bienes muebles propiedad de la corporación deberán estar debidamente registrados, identificados y asignados para su utilización y adecuada administración por parte del proceso de recursos físicos y financieros y de lo cual periódicamente se deberán cotejar los inventarios asignados al personal responsable como medio de control sobre su uso y custodia.

- Los bienes muebles propiedad de la entidad deben estar amparados por las respectivas pólizas de protección que permitan su recuperación frente a posible pérdida, hurto o siniestro.

8.3. Metodología de Administración del Riesgo

La metodología de administración de riesgo de la Corporación se presenta a continuación, y está basada en lo establecido en la "*Guía para la administración del riesgo y el diseño de controles en entidades públicas*" del Departamento Administrativo de la Función Pública – DAFP, enmarcada dentro del contexto de la seguridad digital.

Antes de iniciar con la metodología, se debe conocer dos (2) aspectos fundamentes:

- Conocimiento de la entidad: (Misión, visión, objetivos estratégicos, entre otros aspectos)
- Modelo de operación por procesos (Caracterización de los procesos)

Paso 1: Lineamientos de la Política de administración de riesgos.

Paso 2: Identificación de riesgo: Identificación y clasificación de los riesgos asociados a la seguridad de la información.

Paso 3: Valoración del riesgo: Análisis, evaluación, monitoreo y revisión de los riesgos.

Paso 4: Lineamientos: Generación de lineamientos de los riesgos asociados a la seguridad de la información.

9. CONTROL DE CAMBIOS

CONTROL DE CAMBIOS			
Versión	**Fecha**	**Elaboró**	**Descripción del cambio**
0	30/07/2018	Lilian Mercedes García Gallo	Documento inicial
1	20/01/2020	Alfredo Orjuela Peña	Establecimiento del Plan del riesgo de seguridad y privacidad
2	20/01/2021	Alfredo Orjuela Peña	Establecimiento del Plan del riesgo de seguridad y privacidad
3	20/01/2022	Alfredo Orjuela Peña	Establecimiento de Plan del riesgo de seguridad y privacidad
4	16/01/2023	Alfredo Orjuela Peña	Establecimiento de Plan del riesgo de seguridad y privacidad
5	29/01/2024	Alfredo Orjuela Peña	Actualización general en normativa, términos y definiciones, política de seguridad, plan del riesgo, inclusión de políticas de administración del riesgo de Corpoboyacá y metodología del riesgo.