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
2021

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 al Modelo de

Seguridad y Privacidad de la Información –MSPI de Corpoboyacá y con la Política Nacional de Gobierno Digital.

El presente Plan de Tratamiento del Riesgo de Seguridad y Privacidad de la Información, tiene el propósito generar lineamientos institucionales que orienten en la correcta identificación, análisis, valoración y administración del riesgo; que permitan el aseguramiento y protección de la información de acuerdo a lo exigido en la Política Nacional de Gobierno Digital.

2. OBJETIVO GENERAL

Establecer el plan de Tratamiento del riesgo de seguridad y privacidad de la información de CORPOBOYACÁ, generando lineamientos que orienten en la correcta identificación, análisis, valoración y administración del riesgo; que permitan el aseguramiento y protección de la información.

2.1. OBJETIVOS ESPECIFICOS

3.1. Establecer riesgos en seguridad digital

- ✓ Identificación y clasificación de activos de información.
- ✓ Identificación de riesgos.

3.2. Realizar valoración de riesgos:

- ✓ Definición de criterios de probabilidad, impacto y zonas de riesgo aceptable.
- ✓ Valoración de riesgos.

3. ALCANCE

El alcance del presente plan de tratamiento del riesgo es de identificar los riesgos en seguridad digital y evaluar los activos de información que resulten críticos para la Entidad, para su posterior tratamiento.

4. 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.

5. TERMINOS Y DEFINICIONES

Activo de Información. Recurso tangible e intangible del o 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). Situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización

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.

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 de riesgos de seguridad digital: Es el conjunto de actividades coordinadas dentro de una organización o entre organizaciones, para abordar el riesgo de seguridad digital, mientras se maximizan oportunidades. Es una parte integral de la toma de decisiones y de un marco de trabajo integral para gestionar el riesgo de las actividades económicas y sociales. Se basa en un conjunto flexible y sistemático de procesos cíclicos lo más transparente y lo más explícito posible. Este conjunto de procesos ayuda a asegurar que las medidas de gestión de riesgos de seguridad digital (medidas de seguridad) sean apropiadas para el riesgo y los objetivos económicos y sociales en juego.

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.

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

Política de Administración de riesgos: Es Declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del riesgo, (NTC ISO31000 Numeral 2.4). La gestión o administración del riesgo establece lineamientos precisos acerca del tratamiento, manejo y seguimiento a los riesgos.

Riesgo: es el efecto de incertidumbres sobre objetivos y puede resultar de eventos en donde las amenazas cibernéticas se combinan con vulnerabilidades generando consecuencias económicas.

Riesgo de seguridad digital: es la expresión usada para describir una categoría de riesgo relacionada con el desarrollo de cualquier actividad en el entorno digital. Este riesgo puede resultar de la combinación de amenazas y vulnerabilidades en el ambiente digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. El riesgo de seguridad digital es de naturaleza dinámica. Incluye aspectos relacionados con el ambiente físico y digital, las personas involucradas en las actividades y los procesos organizacionales que las soportan

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 la gerencia de 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 medidas para modificar el riesgo.

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

6. ACTIVIDADES A DESARROLLAR DEL PLAN DE 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	Enero 2021
CONOCIMIENTO ACERCA DE LA ENTIDAD	Revisar y documentar Misión Revisar y documentar Visión	Primer semestre de 2021
IDENTIFICACIÓN DE ACTIVOS DE INFORMACION	Realizar identificación o actualización de activos de	Primer semestre de 2021
IDENTIFICACIÓN DE INFRAESTRUCTURA CRITICA	Identificar infraestructura crítica cibernética.	Primer semestre de 2021
IDENTIFICACIÓN DE RIESGOS DIGITALES	Realizar identificación de riesgos de información de la infraestructura	Segundo semestre de 2021
VALORACION DE RIESGOS DOGITALES	Realizar análisis y valoración de riesgos de información de la	Segundo semestre de 2021

7. 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 de Plan del riesgo de
2	20/01/2021	Alfredo Orjuela Peña	Establecimiento de Plan del riesgo de seguridad y privacidad