CORPORACION AUTONOMA REGIONAL DE BOYACA
CORPOBOYACA

Corpoboyacá

Región estratégica para la sostenibilidad

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

**Versión 0**

## 1. INTRODUCCIÓN

El presente documento tiene como fin generar una cultura de prevención contra los riesgos a los que día a día se pudieran ver sometidos los activos de información de la Corporación Autónoma Regional de Boyacá - CORPOBOYACA. Basados en un enfoque de planeación de gestión del riesgo se pretende realizar una estrategia que permita diagnosticar, evaluar, implementar y desarrollar la gestión de incidentes que afectan al activo de información e implantar unas contramedidas en el sistema de gestión informático para disminuir la probabilidad de su materialización.

## 2. OBJETIVOS

### 2.1 OBJETIVO GENERAL

Establecer una guía metodológica para el adecuado tratamiento de los riesgos a los que están expuestos los activos de información de la Corporación Autónoma Regional de Boyacá - CORPOBOYACA., que permitan una adecuada toma de decisiones para disminuir la probabilidad que se materialice una amenaza o bien reducir la vulnerabilidad del sistema o el posible impacto en la Entidad, así como permitir la recuperación del sistema o la trasferencia del problema a un tercero.

### 2.2 OBJETIVOS ESPECIFICOS

- Consolidar una administración de riesgos acorde con las necesidades de la Corporación Autónoma Regional de Boyacá - CORPOBOYACA.
- Proteger los activos de información de la Corporación de acuerdo a su clasificación y criterios de Confidencialidad, Integridad y Disponibilidad
- Crear compromiso en los usuarios del proceso en la Formulación y desarrollo del presente plan en aras de la prevención y administración del riesgo de seguridad de la información.
- Crear conciencia a nivel institucional de la importancia y la necesidad de una correcta gestión del riesgo de seguridad de la información.

## 3. ALCANCE

La guía metodológica contempla la implementación y la administración de la gestión del tratamiento riesgo de seguridad de la información en la Corporación Autónoma Regional de Boyacá - CORPOBOYACA., la cual será la pauta para desarrollar las actividades a través de la metodología PHVA (Planear – Hacer – Verificar - actuar) y las directrices de MINTIC.

## 4. DEFINICIONES

- **Acceso a la Información Pública**
  Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).

- **Activo**

En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).

- **Activo de Información**
  En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controlar en su calidad de tal.

- **Archivo**
  Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3).

- **Amenazas**
  Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

- **Análisis de Riesgo**
  Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

- **Auditoría**
  Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000).

- **Autorización**
  Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3).

- **Bases de Datos Personales**
  Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3).

- **Ciberseguridad**
  Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).

- **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**
  Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

- **Datos Abiertos**

Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6).

- **Datos Personales**
  Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

- **Datos Personales Públicos**
  Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3).

- **Datos Personales Privados**
  Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h).

- **Datos Personales Mixtos**
  Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.

- **Datos Personales Sensibles**
  Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3).

- **Declaración de aplicabilidad**
  Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).

- **Derecho a la Intimidad**
  Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).

- **Encargado del Tratamiento de Datos**
  Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento. (Ley 1581 de 2012, art 3)

- **Gestión de incidentes de seguridad de la información**
  Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

- **Información Pública Clasificada**
  Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).

- **Información Pública Reservada**
  Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)

- **Plan de continuidad del negocio**
  Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).

- **Plan de tratamiento de riesgos**
  Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

- **Privacidad**
  En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

- **Responsabilidad Demostrada**
  Conducta desplegada por los Responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.
- **Responsable del Tratamiento de Datos**
  Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art 3).

- **Riesgo**
  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. (ISO/IEC 27000).

- **Seguridad de la información**
  Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

- **Sistema de Gestión de Seguridad de la Información SGSI**
  Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de

seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

- **Titulares de la información**
  Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3).

- **Trazabilidad**
  Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).

## 5. LAS RESPONSABILIDADES, LOS ROLES, LOS RECURSOS Y LA METODOLOGIA DE CARA A LA GESTION DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN.

### 5.1 LOS RESPONSABLES Y LOS ROLES

- ✓ **Los Responsables** de los procesos: Identifican, analizan, evalúan y valoran los riesgos por lo menos una vez al año.

  Los funcionarios en el desarrollo de sus actividades conocen e identifican cuales son los riesgos existentes por ende deben proponer estrategias para tratarlos y minimizar su impacto en la Corporación.

- ✓ **La Dirección.** Aprueba las directrices para la administración del riesgo de la seguridad de la información de la Corporación.

- ✓ **El proceso de Calidad.** En cuanto a la administración del riesgo en la Corporación, orienta, coordina, y ajusta los requisitos normativos en El Sistema Integrado de gestión de la calidad. Almera, SGI de la Corporación.

- ✓ **Los Líderes del proceso de Planeación y Sistemas de Información**. Apoyan la gestión en cuanto a Liderazgo.

- ✓ **El Líder de Soporte Tecnológico.** Apoya la gestión en el desarrollo de las actividades.

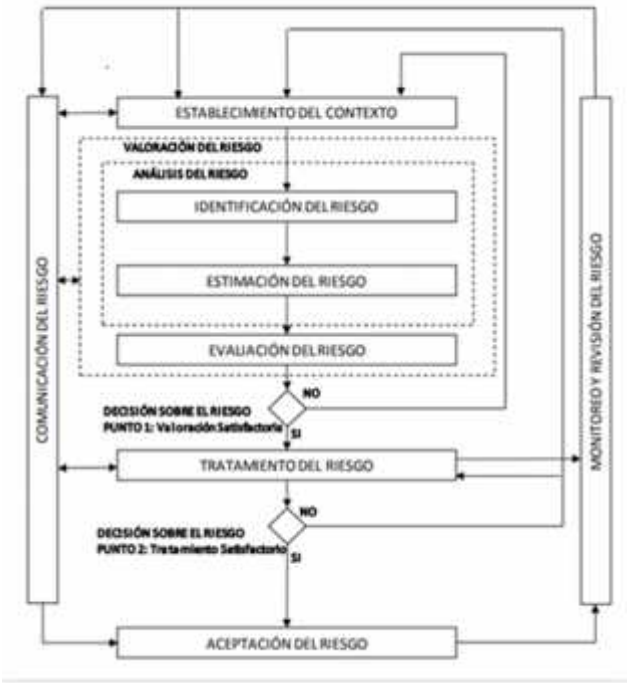
- ✓ **Los Líderes SIG.** Apoyan la ejecución de las etapas de gestión del riesgo a nivel de los procesos.

- ✓ **Los Funcionarios internos y Contratistas**. Son llamados a ejecutar los controles y acciones definidas para la administración de los riesgos con el fin de aportar en la identificación de posibles riesgos que puedan afectar la gestión de los procesos de la Corporación.

- ✓ **El área de Control Interno.** Se encarga de realizar evaluación y seguimiento a los sistemas y su posible impacto en la Corporación.

## 6. ETAPAS PARA LA ADMINISTRACIÓN DEL RIESGO

El proceso de gestión del riesgo en la seguridad de la información puede ser iterativo para las actividades de valoración del riesgo y/o el tratamiento del mismo. Este enfoque puede incrementar la profundidad y el detalle de la valoración en cada iteración como se muestra en la figura tomada de la NTC ISO IEC 27005.




Gráfica1.Etapas para la administración del riesgo

Las etapas a considerar durante la administración del riesgo para la Corporación Autónoma Regional de Boyacá son las siguientes:

- **Contexto estratégico:** Se determinarán los factores externos e internos del riesgo.
- **Identificación**: Se identificaran las causas, riesgo, consecuencias y clasificación del riesgo.
- **Análisis:** Se calificará y evaluará el riesgo inherente**.**
- **Valoración:** se identificará y evaluaran los controles; se deberá incluir la determinación del riesgo residual**.**
- **Manejo:** Se determinará, si es necesario, acciones para el fortalecimiento de los controles.
- **Seguimiento:** Se evaluará los riesgos de manera integral**.**

## 7. METODOLOGÍA DE IMPLEMENTACIÓN

Para llevar a cabo la implementación del Modelo de Seguridad y Privacidad de la Información en el CORPOBOYACA, se toma como base la metodología PHVA (Planear, Hacer, Verificar y Actuar) y los lineamientos emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, a través de los decretos emitidos.

De acuerdo con esto, se definen las siguientes fases de implementación del MSPI:

1. Diagnosticar
2. Planear
3. Hacer
4. Verificar
5. Actuar

Ilustración 1 – Marco de Seguridad y Privacidad de la Información

Fuente: Modelo de Seguridad y Privacidad de la Información emitida por MinTIC

## 8. ACTIVIDADES

1. Realizar Diagnóstico
2. Elaborar el Alcance del Plan del Tratamiento de Riesgo de Seguridad y Privacidad de la Información
3. Realizar la Identificación de los Riesgos con los líderes del Proceso.
   3.1. Entrevistar con los líderes del Proceso
4. Valorar del riesgo y del riesgo residual
5. Realizar Mapas de calor donde se ubican los riesgos
6. Plantear al plan de tratamiento de riego aprobado por los lideres

## *9.* CRONOGRAMA

CRONOGRAMA DE ACTIVIDADES PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

| ACTIVIDAD | AGOSTO 2018 | | | | SEPTIEMBRE 2018 | | | OCTUBRE 2018 | | | NOVIEMBRE 2018 | | | DICIEMBRE 2018 | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Realizar diagnóstico | | | | | | | | | | | | | | | | | |
| Elaborar el Alcance del Plan del Tratamiento de Riesgo de Seguridad y Privacidad de la Información | | | | | | | | | | | | | | | | | |
| Realizar la Identificación de los Riesgos con los lideres del Proceso | | | | | | | | | | | | | | | | | |
| Entrevista con los líderes del Proceso | | | | | | | | | | | | | | | | | |
| Valorar del riesgo y del riesgo residual | | | | | | | | | | | | | | | | | |
| Realizar Mapas de calor donde se ubican los riesgos | | | | | | | | | | | | | | | | | |
| Plantear al plan de tratamiento de riego aprobado por los lideres | | | | | | | | | | | | | | | | | |

## *10.* SEGUIMIENTO y EVALUACIÓN

Cada seis (6) meses Control Interno realizará seguimiento a todo el componente de administración de riesgos y verificará aspectos como:

Cumplimiento de las políticas y directrices para la administración del riesgo: metodología de Administración del Riesgo (diseño y funcionamiento).
Administración de los riesgos por proceso e institucionales: calificación y evaluación, efectividad de los controles y cumplimiento de las acciones.

Los resultados de la evaluación y las observaciones de la persona que haga las veces de Control Interno deben ser presentados a la Alta Dirección, para que se tomen las decisiones pertinentes que garanticen la sostenibilidad de la Administración del Riesgo en la organización.

## *11.* ENTREGABLES

- Informe de avance o resumen ejecutivo
- Acta de Reunión.
- Plan de tratamiento de riego aprobado por los lideres
- Política de Seguridad
- Productos de cada etapa

## *12.* MARCO NORMATIVO.

Guía de Gestión de riesgos. Guía No.7 (Seguridad y Privacidad de la Información) de MINTIC. “Todas las referencias a las políticas, definiciones o contenido relacionado, publicadas en la norma técnica colombiana NTC ISO/IEC 27001 vigente e ISO 27005 vigente, así como a los anexos con derechos reservados por parte de ISO/ICONTEC.”

## *13.* CONTROL DE CAMBIOS

| FECHA | VERSIÓN | CAMBIOS |
|---|---|---|
| Julio 30 2018 | 0 | Documento inicial |
| | | |
| | | |