GOBERNACIÓN DE BOLÍVAR

PLAN GENERAL PARA EL TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

TABLA DE CONTENIDO

INTRODUCCIÓN 3
2. OBJETIVO 3
3. ALCANCE 4
4. TERMINOS Y DEFINICIONES 4
5. PROCESO DE GESTION DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN 6
5.1 ESTABLECER EL CONTEXTO 7
5.2 EVALUACIÓN DE RIESGOS 7
5.2.1 Identificar riesgo 8
5.2.2 Analizar riesgo 8
5.2.2.1 Probabilidad 8
5.2.2.2 Impacto 9
5.2.3 Evaluar riesgo 10
5.3 TRATAMIENTO DE RIESGOS 10
6 VIGENCIA Y CONTROL DE CAMBIOS 11

INTRODUCCIÓN

La revolución digital está obligando a reconocer el protagonismo de la información en los procesos productivos de todas las empresas y la importancia de tenerla adecuadamente identificada y protegida. Por lo anterior, se amerita dar un tratamiento, manejo y clasificación a la información bajo una correcta administración y custodia.
La GOBERNACIÓN DE BOLÍVAR, atendiendo a su política general de seguridad y privacidad de la información, previamente aprobada, ha decidido vincular un modelo de administración de los riesgos de seguridad de la información el logro de los objetivos de mantener la información de la Entidad confidencial, integra y disponible, a través de su ciclo de vida desde su captura, almacenamiento, explotación, hasta su eliminación.

Los principios de la información se enmarcan en:

- **Confidencialidad:** propiedad que impide la divulgación de información a individuos, entidades o procesos no autorizados, asegurando el acceso a la información únicamente a aquellas personas que cuenten con la debida autorización.

- **Integridad:** propiedad que busca mantener los datos libres de modificaciones no autorizadas. A grosso modo, la integridad es mantener con exactitud la información tal cual fue generada, sin ser manipulada ni alterada por personas o procesos no autorizados.

- **Disponibilidad:** característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.

2. OBJETIVO

Establecer en la GOBERNACIÓN DE BOLIVAR una ruta con enfoque metódico que facilite las pautas necesarias para desarrollar y fortalecer una correcta gestión de los riesgos de seguridad de la información, a través de metodologías que faciliten la determinación del contexto estratégico, la identificación de riesgo y oportunidades, el análisis, la valoración y la generación de políticas.

3. ALCANCE

La gestión de riesgos será aplicada sobre cualquier proceso de la GOBERNACIÓN DE BOLÍVAR, a través de los principios básicos para la administración de los riesgos de seguridad de la información. Dicha gestión, incluye las técnicas, actividades y formularios que permitan y faciliten el desarrollo de las etapas de reconocimiento del contexto, identificación de los riesgos de seguridad de la información, análisis y evaluación, opciones de tratamiento o manejo del riesgo según la zona de riesgo; incluye además pautas y recomendaciones para su seguimiento, monitoreo y evaluación.

4. TERMINOS Y DEFINICIONES

A continuación, se listan algunos términos y definiciones de términos que se utilizarán durante el desarrollo de la gestión de riesgos de seguridad de la información:

- ✓ **Administración del riesgo:** conjunto de elementos de control que al Interrelacionarse brindan a la entidad la capacidad para emprender las acciones necesarias que le permitan el manejo de los eventos que puedan afectar negativamente el logro de los objetivos institucionales y protegerla de los efectos ocasionados por su ocurrencia.
- ✓ **Activo de Información**: en relación con la seguridad de la información, se refiere a cualquier información o elemento de valor para los procesos de la Organización.
- ✓ **Análisis de riesgos**: es un método sistemático de recopilación, evaluación, registro y difusión de información necesaria para formular recomendaciones orientadas a la adopción de una posición o medidas en respuesta a un peligro determinado.
- ✓ **Amenaza:** es la causa potencial de una situación de incidente y no deseada por la organización
- ✓ **Causas**: son todo aquello que se pueda considerar fuente generadora de eventos (riesgos). Las fuentes o agentes generadores son las personas, los métodos, las herramientas, el entorno, lo económico, los insumos o materiales entre otros.
- ✓ **Consecuencia**: resultado de un evento que afecta los objetivos.
- ✓ **Criterios del riesgo**: términos de referencia frente a los cuales la importancia de un riesgo se evaluada.
- ✓ **Control**: medida que modifica el riesgo.

✓ **Evaluación de riesgos**: proceso de comparación de los resultados del análisis del riesgo con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables.

✓ **Evento**: un incidente o situación, que ocurre en un lugar particular durante un intervalo de tiempo específico.

✓ **Estimación del riesgo:** proceso para asignar valores a la probabilidad y las consecuencias de un riesgo.

✓ **Evitación del riesgo:** decisión de no involucrarse en una situación de riesgo o tomar acción para retirarse de dicha situación.

✓ **Factores de riesgo:** situaciones, manifestaciones o características medibles u observables asociadas a un proceso que generan la presencia de riesgo o tienden a aumentar la exposición, pueden ser internos o externos a la entidad.

✓ **Gestión del riesgo**: actividades coordinadas para dirigir y controlar una organización con respecto al riesgo, se compone de la evaluación y el tratamiento de riesgos.

✓ **Identificación del riesgo.:** proceso para encontrar, enumerar y caracterizar los elementos de riesgo.

✓ **Incidente de seguridad de la información**: evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

✓ **Integridad**: propiedad de la información relativa a su exactitud y completitud.

✓ **Impacto: c**ambio adverso en el nivel de los objetivos del negocio logrados.

✓ **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.

✓ **Matriz de riesgos:** instrumento utilizado para ubicar los riesgos en una determinada zona de riesgo según la calificación cualitativa de la probabilidad de ocurrencia y del impacto de un riesgo.

✓ **Monitoreo**: mesa de trabajo anual, la cual tiene como finalidad, revisar, actualizar o redefinir los riesgos de seguridad de la información en cada uno de los procesos, partiendo del resultado de los seguimientos y/o hallazgos de los entes de con trol o las diferentes auditorías de los sistemas integrados de gestión.

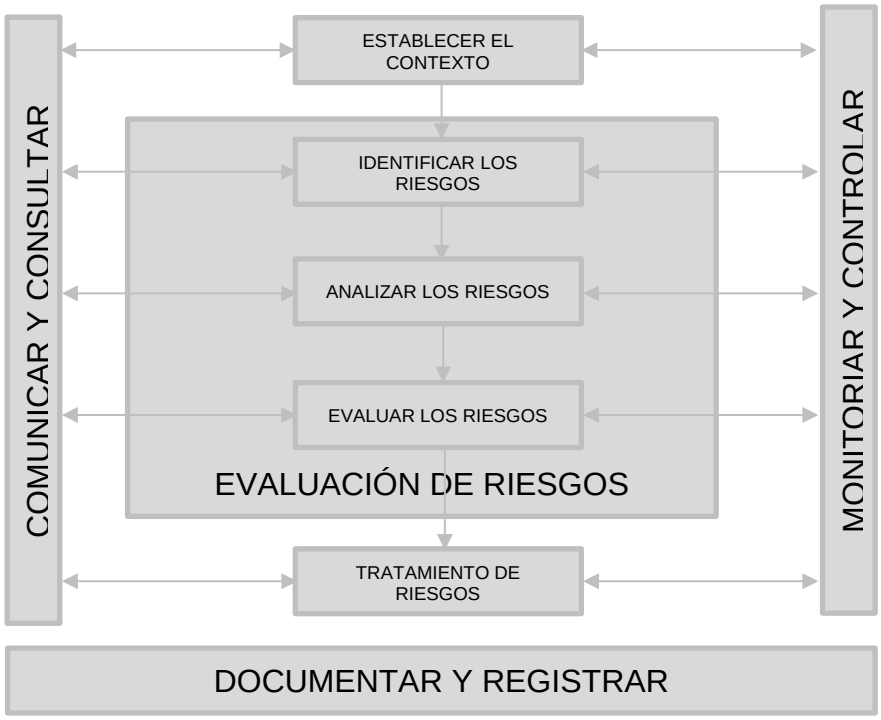
✓ **Propietario del riesgo**: persona o entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo.

✓ **Proceso**: conjunto de actividades interrelacionadas o que interactúan para transformar una entrada en salida.

- ✓ **Riesgo inherente**: es el nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de los controles.
- ✓ **Riesgo Residual**: el riesgo que permanece tras el tratamiento del riesgo o nivel resultante del riesgo después de aplicar los controles.
- ✓ **Riesgo**: efecto de la incertidumbre sobre los objetivos.
- ✓ **Riesgo en la seguridad de la información:** potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la organización.
- ✓ **Reducción del riesgo:** acciones que se toman para disminuir la probabilidad las consecuencias negativas, o ambas, asociadas con un riesgo.
- ✓ **Retención del riesgo:** aceptación de la pérdida o ganancia proveniente de un riesgo particular
- ✓ **Seguimiento**: mesa de trabajo semestral, en el cual se revisa el cumplimiento del plan de acción, indicadores y metas de riesgo y se valida la aplicación n de los controles de seguridad de la información sobre cada uno de los procesos.
- ✓ **Tratamiento del riesgo**: proceso para modificar el riesgo (Icontec Internacional, 2011).
- ✓ **Valoración del riesgo**: proceso global de identificación del riesgo, análisis del riesgo y evaluación de los riesgos.
- ✓ **Vulnerabilidad:** es aquella debilidad de un activo o grupo de activos de información
- ✓ **Seguridad de la información**: preservación de la confidencialidad, integridad y disponibilidad de la información.
- ✓ **SGSI**: Sistema de Gestión de Seguridad de la Información.

5. PROCESO DE GESTION DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Basados en la norma ISO 27005, la GOBERNACIÓN DE BOLÍVAR, ejecutará el siguiente modelo de gestión de riesgos, el cual ayudará a garantizar un tratamiento adecuado de los riesgos de seguridad de la información:



Modelo de gestión de riesgos de seguridad de la información. NTC/ISO 27005

5.1 ESTABLECER EL CONTEXTO

Definir los criterios básicos que serán necesarios para enfocar el ejercicio por parte de la GOBERNACIÓN DE BOLÍVAR y obtener los resultados esperados, basándose en, la identificación de las fuentes que pueden dar origen a los riesgos.

5.2 EVALUACIÓN DE RIESGOS

Identificar los activos de información por proceso en evaluación. Conocer las amenazas que pueden causar daños en la información, los procesos y los soportes. Una vez se valoran los impactos, la probabilidad y las consecuencias de los escenarios de incidentes sobre los activos de información, se obtendrán los niveles de riesgo, para los cuales se deberán comparar frente a los criterios básicos del contexto, para una adecuada y pertinente toma de decisiones basada en riesgos de seguridad de la información y en beneficio de reducir su impacto.

5.2.1 Identificar riesgo

Tiene como objetivo conocer los escenarios que pueden producir en la entidad y los efectos que puedan tener sobre los objetivos de esta.

El procedimiento para la gestión de riesgos contiene el reconocimiento de las causas y la procedencia del riesgo que puedan afectar a los objetivos.

5.2.2 Analizar riesgo

Permite determinar la severidad de este a partir del impacto y la probabilidad de su ocurrencia, así como también determinar el riesgo inherente de cada activo y asignar el responsable.

La probabilidad dirá cuál puede ser la ocurrencia del riesgo y el impacto inherente en la Gobernación de Bolívar sin tener presente los controles al materializarse, por lo que debe verse en el peor de los escenarios posibles.

5.2.2.1 Probabilidad

Valor	Nivel	Descripción	Frecuencia
1	Raro	El evento puede ocurrir solo en circunstancias excepcionales y/o la eficacia de los controles es alta.	No se ha presentado en los últimos 4 años
3	Posible	El evento podría ocurrir en algún momento y/o la eficacia de los controles es baja.	Al menos una vez en los últimos 2 años
5	Casi seguro	Se espera que el evento ocurra en la mayoría de las circunstancias y/o no existen controles o si existen es nula su eficacia.	Más de una vez al año

5.2.2.2 Impacto

Área de impacto	Descripción	Alto (5)	Medio (3)	Bajo (1)
FINANCIERO	Se relacionan con el manejo de los recursos de la entidad, que incluyen la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes.	Superiores a COP$	Mayores e iguales a COP$ e inferiores a COP$	Mayores a COP$ e inferiores a COP$
REPUTACIÓN	Están relacionados con la percepción y la confianza de las partes interesadas hacia la entidad.	Exposición negativa en medios nacionales e internacionales	Campaña de desprestigio en redes sociales	Quejas y reclamos internos
LEGAL	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.	Cierre del establecimiento debido a orden judicial	Multas debido a demandas civiles o estatales	Tutelas y procesos legales ordinarios
PRODUCTIVIDAD	Comprenden riesgos provenientes del funcionamiento y operatividad de los sistemas de información institucional, de la	No hay acceso a las plataformas de la entidad por más de XX horas.	No hay acceso a las plataformas de la entidad entre XX y XX horas.	No hay acceso a las plataformas de la entidad por menos de XX horas.

	definición de los procesos, de la estructura de la entidad y la articulación entre dependencias.			

**Valores en rojo deberán se definidos por el comité.*

5.2.3 Evaluar riesgo

PROBABILIDAD	IMPACTO		
	Bajo (1)	**Medio (3)**	**Alto (5)**
Raro (1)	1	3	5
Posible (3)	3	9	15
Casi Seguro (5)	5	15	25

Igual a 1: zona de riesgo baja: asumir el riesgo.
Mayor a 1 menor a 9: zona de riesgo moderada: asumir el riesgo, reducir el riesgo.
Mayor o igual a 9: zona de riesgo alta: Reducir el riesgo, evitar, compartir o transferir.

5.3 TRATAMIENTO DE RIESGOS

Seleccionar una opción de tratamiento basados en la evaluación de riesgos:

✓ **Evitar el riesgo:** su propósito es no proceder con la actividad o la acción que da origen al riesgo.
✓ **Transferir o compartir el riesgo:** entregando la gestión del riesgo a un tercero.
✓ **Reducir o Mitigar el riesgo**: seleccionando e implementando los controles o medidas adecuadas que logren que se reduzca la probabilidad o el impacto
✓ **Retener o aceptar el riesgo**: no se tomará la decisión de implementar medidas de control adicionales. Será monitoreado para confirmar que no se incrementa.

6 VIGENCIA Y CONTROL DE CAMBIOS

FECHA	AUTOR	VERSIÓN	CAMBIOS
28 de diciembre 2018	Dirección TIC	1.0	Versión inicial
26 de diciembre 2019	Dirección TIC	2.0	- Se detallo la evaluación del riesgo asociados la seguridad y privacidad de la información