Departamento del Cesar

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

Valledupar, Colombia
Noviembre de 2019

## TABLA DE CONTENIDO

## LISTA DE TABLAS

## GLOSARIO

**AMENAZA**: (Inglés: Threat). Según [ISO/IEC 13335-1:2004]: causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.

**CRITERIO DE RIESGOS:** Términos de referencia por los que se evalúa la importancia del riesgo

**CONTEXTO ESTRATÉGICO:** Son las condiciones internas y del entorno, que pueden generar eventos que originan oportunidades o afectan negativamente el cumplimiento de la misión y objetivos de una institución.

**CAUSAS (FACTORES INTERNOS O EXTERNOS):** Son los medios, las circunstancias y agentes generadores de riesgo. Los agentes generadores que se entienden como todos los sujetos u objetos que tienen la capacidad de originar un riesgo.

**DESCRIPCIÓN**: Se refiere a las características generales o las formas en que se observa o manifiesta el riesgo identificado.

**EFECTOS:** Constituyen las consecuencias de la ocurrencia del riesgo sobre los objetivos de la entidad; generalmente se dan sobre las personas o los bienes materiales o inmateriales con incidencias importantes tales como daños físicos y fallecimiento, sanciones, pérdidas económicas, de información, de bienes, de imagen, de credibilidad y de confianza, interrupción del servicio y daño ambiental.

**GESTIÓN DE RIESGOS:** Actividades coordinadas para dirigir y controlar una empresa en relación con el riesgo

**RIESGO**: (Inglés: Risk). Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Según [ISO Guía 73:2002]: combinación de la probabilidad de un evento y sus consecuencias.

**RIESGO RESIDUAL:** Riesgo que permanece después del tratamiento de riesgos

**RIESGO ESTRATÉGICO:** Se asocia con la forma en que se administra la entidad. El manejo del riesgo estratégico se enfoca a asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la clara definición de políticas, diseño y conceptualización de la entidad por parte de la alta gerencia.

**RIESGOS DE IMAGEN:** Están relacionados con la percepción y la confianza por parte de la ciudadanía hacia la institución.

**RIESGOS OPERATIVOS**: Comprenden riesgos provenientes del funcionamiento y operatividad de los sistemas de información institucional, de la definición de los procesos, de la estructura de la entidad, de la articulación entre dependencias.
**RIESGOS FINANCIEROS:** 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.

**RIESGOS DE CUMPLIMIENTO:** 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.

**RIESGOS DE TECNOLOGÍA:** Están relacionados con la capacidad tecnológica de la Entidad para satisfacer sus necesidades actuales y futuras y el cumplimiento de la misión.

**VULNERABILIDAD:** (inglés: Vulnerability). Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo. Según [ISO/IEC 13335-1:2004]: debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.

## INTRODUCCIÓN

Hoy día, las empresas inmersas en la denominada revolución digital, reconocen el protagonismo de la información en sus procesos productivos, por tanto la importancia de tener su información adecuadamente identificada y protegida, como también la proporcionada por sus partes interesadas, enmarcada bajo las relaciones de cumplimiento, comerciales y contractuales como los son acuerdos de confidencialidad y demás compromisos, que obligan a dar un tratamiento, manejo y clasificación a la información bajo una correcta administración y custodia.

Para ello la Seguridad de la Información en las empresas tiene como objetivo la protección de los activos de información en cualquiera de sus estados ante las amenazas o brechas que atenten contra sus principios fundamentales de confidencialidad, integridad y su disponibilidad, a través de la implementación de medidas de control de seguridad de la información, que permitan gestionar y reducir los riesgos e impactos a que está expuesta y se logre alcanzar el máximo retorno de las inversiones en las oportunidades de negocio.

El Departamento del Cesar con la implementación del presente plan, busca identificar los riesgos de información causados por situaciones Internas y/o externas que puedan generar eventos que afecten negativamente el cumplimiento de la misión y objetivo de la institución, así como establecer los controles pertinentes que permitan mitigar, eliminar o trasladar el riesgo con el fin de garantizar la Integridad, Disponibilidad y la confidencialidad de la información.

Para ello se consideraron los activos de información con nivel de clasificación ALTA dependiendo de la calificación de los criterios de Confidencialidad, Integridad y Disponibilidad que hace mención la Guía de Gestión de Riesgos del Ministerio de las Tecnologías de la Información y las Comunicaciones MINTIC.

## 1. OBJETIVO GENERAL

Establecer las acciones necesarias para mitigar los riesgos de seguridad de la información, a través de la determinación del contexto estratégico de la entidad, la identificación de riesgo, el análisis, la valoración, el seguimiento y monitoreo permanente enfocado a su cumplimiento y mejoramiento continuo.

### 1.1. OBJETIVOS ESPECÍFICOS

- Brindar lineamientos y unificar criterios para la administración de los riesgos de seguridad de la información.
- Proteger el valor de los activos de información de la entidad, implementando controles y acciones de mitigación frente al riesgo.
- Generar una cultura enfocada a la identificación de los riesgos de seguridad de la información y su mitigación, para evitar que se produzca un determinado impacto en la información.
- Cumplir con los principios de seguridad de la información: disponibilidad, integridad y confidencialidad de la información.

## 2. ALCANCE

El proceso parte de los principios básicos y metodológicos para la administración de los riesgos de seguridad de la información desde la identificación de los riesgos, su análisis, valoración y formulación de acciones, seguimiento, monitoreo y evaluación, para garantizar una adecuada gestión de riesgos de seguridad de la información dentro de la entidad.

## 3. CONTEXTO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

El contexto de gestión de riesgos de seguridad de la información de la entidad se basa en la identificación de las fuentes que pueden dar origen a los riesgos, la valoración de los riesgos en términos de las consecuencias para la institución, la probabilidad de su ocurrencia, así como la construcción de acciones de mitigación en beneficio de lograr y mantener niveles de riesgos aceptables.

### 3.1. INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

De acuerdo con lo descrito en la norma GTC-ISO/IEC 27035, un incidente de seguridad de la información está definido como “Evento o serie de eventos no deseados o inesperados, que tienen probabilidad significativa de comprometer.

Las actividades que vulneran la seguridad representan Riesgos de Seguridad y Privacidad de la Información.

Los factores de riesgos identificados en la entidad son los siguientes:

**Tabla No.1.** Factores Internos y Externos que pueden generar diferentes tipos de Riesgo

| FACTORES EXTERNOS | TTPOS RIESGOS | | FACTORES INTERNOS | TTPOS RIESGOS |
|---|---|---|---|---|
| **Económicos:**<br>1. Embargo a la Gobernación | Riesgo financiero | | **Infraestructura:**<br>1.Disponibilidad de los Activos<br>2. Capacidad de los Activos | Riesgo Operativo. |
| **Medioambientales:**<br>1. Catástrofe Natural<br>2. Falta o Falla de Energía | Riesgo Operativo.<br>Riesgo Financiero<br>Riesgo Cumplimiento.<br>Riesgo Estratégico | | **Personal:**<br>1. capacidad del personal.<br>2. Salud.<br>3. Seguridad | Riesgo Operativo.<br>Riesgo Estratégico |
| **Políticos:**<br>1. Cambio de Gobierno<br>2. Voluntad Política | Riesgo Estratégico | | **Procesos:**<br>1. Capacidad, Diseño y Ejecución<br>2. Proveedores.<br>3. Entradas y Salidas<br>4. Conocimiento | Riesgo Operativo. |
| **Sociales:**<br>1. Terrorismo<br>2. situaciones que afecten el orden Público.<br>3. Responsabilidad Social | Riesgo Operativo. | | **Tecnología:**<br>1.Integridad de datos, disponibilidad de datos y sistemas<br>2. Desarrollo, producción y mantenimiento | Riesgo de Tecnología |
| **Tecnológicos:**<br>1. interrupciones. | Riesgo Cumplimiento.<br>Riesgo de Tecnología | | | |

**Fuente:** Elaboración Propia

## 3.2. MAPA DE PROCESOS DEL DEPARTAMENTO DEL CESAR

**Tabla No. 2.** Mapa de Procesos Departamento del Cesar

| MISIONALES | ESTRATEGICOS | DE APOYO | GESTION DE EVALUACION INDPENDIENTE |
|---|---|---|---|
| Gestión del Desarrollo | Planeación de Desarrollo | Administración de los Recursos Físicos | Gestión de la Evaluación Independiente. |
| Gestión Educativa | | Gestión del Talento Humano | |

| | | | |
|---|---|---|---|
| Gestión en Salud y Promoción Social | | Contratación e Interventoría | |
| Apoyo a la Gestión Territorial | | Gestión Jurídica | |
| Atención Ciudadana | Mejoramiento Institucional | Gestión Financiera | |
| Gestión de Tramites | | Gestión Documental | |
| Inspección Vigilancia y Control | | Gestión de las TIC | |
| Seguimiento y Evaluación a la Gestión Municipal | | | |

**Fuente:** Departamento del Cesar

### 3.3. CARACTERIZACIÓN DE LOS PROCESOS

| | | |
|---|---|---|
| **PROCESO:** | Planeación del Desarrollo | |
| **OBJETIVO:** | Organizar las necesidades y requerimientos de los diferentes grupos de interés de la comunidad, en el corto, mediano y largo plazo mediante la formulación, seguimiento y evaluación de los planes estratégicos, basados en la normatividad vigente. | |
| **RESPONSABLES:** | **DIRIGE:** | Gobernador |
| | **EJECUTA:** | Oficina Asesora de Planeación Departamental |
| | **CONTROLA:** | Jefe de Oficina Asesora de Planeación |

| | | |
|---|---|---|
| **PROCESO:** | Mejoramiento Institucional | |
| **OBJETIVO:** | Garantizar el cumplimiento de objetivos y el fortalecimiento institucional a través de una planeación y retroalimentación permanente que permita potencializar las oportunidades de mejora y aumentar la efectividad de los procesos de la entidad | |
| **RESPONSABLES:** | **DIRIGE:** | Gobernador |
| | **EJECUTA:** | Oficina Asesora de Planeación Departamental, Equipo MECI-CALIDAD, Coordinación de Gestión Humana |
| | **CONTROLA:** | Representante de la Dirección y Equipo de MECI-CALIDAD. |

| | | |
|---|---|---|
| **PROCESO:** | Comunicación Estratégica | |
| **OBJETIVO:** | Fortalecer la identidad institucional de la Gobernación del Cesar y la disposición organizacional para la apertura, la interlocución, la visibilidad en sus relaciones y los flujos de información con los clientes internos y externos, que contribuyan con la efectividad y transparencia de su gestión. | |
| **RESPONSABLES:** | **DIRIGE:** | Gobernador |
| | **EJECUTA:** | Asesor de Prensa, Oficina de Asuntos Internos |

| | | |
|---|---|---|
| | **CONTROLA:** | Despacho, Comité MECI-CALIDAD |

| | | |
|---|---|---|
| **PROCESO:** | Gestión del Desarrollo | |
| **OBJETIVO:** | Generar condiciones y estrategias que permitan el desarrollo económico, social, de infraestructura y servicios públicos, y la participación ciudadana en el ejercicio de los derechos políticos, con el fin de lograr el bienestar de la comunidad cesarense. | |
| **RESPONSABLES:** | **DIRIGE:** | Gobernador |
| | **EJECUTA:** | Secretarios de Agricultura, Minas, Infraestructura, Gobierno, Educación y Cultura, Salud, Recreación y Deportes; Oficinas Asesoras de Política Social, Paz. |
| | **CONTROLA:** | Oficina Asesora de Planeación, Representante de la Dirección y equipo MECI-CALIDAD. |

| | | |
|---|---|---|
| **PROCESO:** | Inspección, Vigilancia y Control | |
| **OBJETIVO:** | Ejercer inspección, vigilancia y control de las actividades y/o servicios realizados directamente por las entidades estatales o particulares en el Departamento del Cesar, para garantizar el cumplimiento de las normas establecidas, sean de competencia del Departamento o por delegación de funciones. | |
| **RESPONSABLES:** | **DIRIGE:** | Oficina Asesora de Planeación |
| | **EJECUTA:** | Secretaria de Salud, Educación y Cultura, Minas e Infraestructura. |
| | **CONTROLA:** | Oficina de Control Interno. |

| | | |
|---|---|---|
| **PROCESO:** | Apoyo a la Gestión Territorial | |
| **OBJETIVO:** | Prestar asistencia técnica y/o asesoría a los Municipios del Departamento del Cesar, con el fin de fomentar el desarrollo integral de los mismos. | |
| **RESPONSABLES:** | **DIRIGE:** | Gobernador |
| | **EJECUTA:** | Secretarias Misionales y de Apoyo |
| | **CONTROLA:** | Oficina Asesora de Planeación, Representante de la Dirección y Equipo MECI-CALIDAD |

| | | |
|---|---|---|
| **PROCESO:** | Gestión de Trámites | |
| **OBJETIVO:** | Atender oportunamente las solicitudes de los diferentes trámites que por ley que le corresponda adelantar a la entidad. | |
| **RESPONSABLES:** | **DIRIGE:** | Asuntos Internos |
| | **EJECUTA:** | Secretarías que gestionan trámites |
| | **CONTROLA:** | Asuntos Internos |

| | |
|---|---|
| **PROCESO:** | Administración de los recursos físicos |

| | | |
|---|---|---|
| **OBJETIVO:** | Dotar con herramientas necesarias a las diferentes sectoriales de la Gobernación del Cesar, mantener la infraestructura y los archivos y liderar la transformación tecnológica e informática, gestionando y desarrollando estrategias que garanticen la permanente disponibilidad de la plataforma existente de la entidad, para lograr su óptima operación. | |
| **RESPONSABLES:** | **DIRIGE:** | Secretaría General |
| | **EJECUTA:** | Coordinación de Recursos Físicos y Tecnológicos |
| | **CONTROLA:** | Representante de la Dirección y equipo MECI-CALIDAD. |

| | | |
|---|---|---|
| **PROCESO:** | Gestión del talento humano | |
| **OBJETIVO:** | Contribuir al desarrollo de las potencialidades, destrezas y habilidades del talento humano de la Gobernación del Cesar, y evaluar su conducta de tal manera que se favorezca el desarrollo integral de los funcionarios, con el fin de optimizar la prestación del servicio público y lograr que se desempeñen como dinamizadores de la gestión administrativa departamental | |
| **RESPONSABLES:** | **DIRIGE:** | Gobernador |
| | **EJECUTA:** | Coordinador de la Gestión Humana |
| | **CONTROLA:** | Secretaria General |

| | | |
|---|---|---|
| **PROCESO:** | Contratación e Interventoría | |
| **OBJETIVO:** | Asegurar que la adquisición y ejecución de bienes y servicios demandados por la Administración Departamental, cumplan con los requisitos legales vigentes y con los establecidos por la Entidad para dar lograr darle cumplimiento a sus metas. | |
| **RESPONSABLES:** | **DIRIGE:** | Gobernador |
| | **EJECUTA:** | Todas las sectoriales |
| | **CONTROLA:** | Oficina de Asuntos Jurídicos, Secretaria de Hacienda. |

| | | |
|---|---|---|
| **PROCESO:** | Gestión Jurídica | |
| **OBJETIVO:** | Asesorar y representar efectivamente a la gobernación del Cesar en los asuntos jurídicos de interés de la entidad para garantizar que los mismos se encuentren dentro de los parámetros legales y constitucionales vigentes. | |
| **RESPONSABLES:** | **DIRIGE:** | Asesor Jurídico |
| | **EJECUTA:** | Funcionarios de la oficina Asesora Jurídica y Abogados Externos |
| | **CONTROLA:** | Asesor Juíridico. |

| | | |
|---|---|---|
| **PROCESO:** | Gestión Financiera | |
| **OBJETIVO:** | Administrar con efectividad los recursos económicos del Departamento del Cesar con el propósito de distribuirlos con equidad, legalidad y progresividad en los planes, programas y proyectos establecidos por la administración. | |
| **RESPONSABLES:** | **DIRIGE:** | Gobernador |
| | **EJECUTA:** | Coordinadores de Secretaría de hacienda y Tesorería |
| | **CONTROLA:** | Secretario de Hacienda |

| | | |
|---|---|---|
| **PROCESO:** | Gestión de Evaluación Independiente | |
| **OBJETIVO:** | Verificar y evaluar el esquema de la organización y el conjunto de planes, programas, normas, procedimientos con el fin de procurar que todas las actividades, operaciones y actuaciones, así como la administración de la información y los recursos, se realicen de acuerdo con las normas constitucionales y legales vigentes dentro de las políticas trazadas por la dirección y en atención a las metas u objetivos previos. | |
| **RESPONSABLES:** | **DIRIGE:** | Asesor de Control Interno |
| | **EJECUTA:** | Funcionarios Oficina Asesora de Control Interno |
| | **CONTROLA:** | Asesor de Control Interno |

| | | |
|---|---|---|
| **PROCESO:** | Atención Ciudadana | |
| **OBJETIVO:** | Garantizar calidad en la atención, oportunidad y capacidad de respuesta a la ciudadanía, mediante la implementación de políticas de servicio y protocolos de atención, a través de los canales telefónico, virtual y presencial, con calidad, oportunidad y en cumplimiento de la normatividad vigente. | |
| **RESPONSABLES:** | **DIRIGE:** | Asesor de Asuntos Internos |
| | **EJECUTA:** | Todas las dependencias |
| | **CONTROLA:** | Jefe Oficina Asesora de Control Interno |

| | | |
|---|---|---|
| **PROCESO:** | Seguimiento y Evaluación de la Gestión Municipal | |
| **OBJETIVO:** | Verificar que los entes municipales cumplan con la información para la evaluación de la planificación financiera y desempeño integral. | |
| **RESPONSABLES:** | **DIRIGE:** | Jefe Oficina Asesora de Planeación Departamental |
| | **EJECUTA:** | Profesional de Planeación Departamental |
| | **CONTROLA:** | Jefe Oficina Asesora de Planeación Departamental |

| | | |
|---|---|---|
| **PROCESO:** | Gestión de la TIC | |
| **OBJETIVO:** | Asegurar la disponibilidad, actualización y optimización de las tecnologías de la información y las comunicaciones, de forma oportuna y eficaz. | |
| **RESPONSABLES:** | **DIRIGE:** | Asesor de la TIC |

| | | |
|---|---|---|
| | **EJECUTA:** | Profesional Especializado de Sistemas |
| | **CONTROLA:** | Secretario(a) de Planeación |

| | | |
|---|---|---|
| **PROCESO:** | Gestión Documental | |
| **OBJETIVO:** | Gestionar el manejo de la información recibida y producida por la entidad, mediante la planeación, gestión, organización y conservación de acuerdo con los lineamientos archivísticos de ley e independiente del soporte o medio de registro en el que se encuentre o produzca toda la información. | |
| **RESPONSABLES:** | **DIRIGE:** | Secretario General |
| | **EJECUTA:** | Todas las dependencias |
| | **CONTROLA:** | Grupo de Gestión Documental y Oficina Asesora de Control Interno. |

| | | |
|---|---|---|
| **PROCESO:** | Gestión de Salud y Promoción Social | |
| **OBJETIVO:** | Acciones que sobre una población específica, con individuos identificables y caracterizables deben realizar las entidades públicas o privadas para disminuir la probabilidad de ocurrencia de un evento no deseado, evitable y negativo para la salud del individuo. De igual manera se debe atender determinantes particulares que conllevan a la inequidad social y sanitaria por ciclo de vida, etnia, género, víctimas y personas con discapacidad. | |
| **RESPONSABLES:** | **DIRIGE:** | Ministerio de Salud y Protección Social |
| | **EJECUTA:** | Entidades territoriales, EPS, IPS, otros sectores y la comunidad |
| | **CONTROLA:** | Secretario de Salud Departamental, Secretarios de Salud Municipales, Ministerio de Salud, Supersalud, veedurías, asociaciones de usuarios, comités de discapacidad, mesa de víctimas, procuraduría, contraloría. |

| | | |
|---|---|---|
| **PROCESO:** | Gestión Educativa | |
| **OBJETIVO:** | Definir y desarrollar la organización y la prestación de la educación formal, educación para el trabajo y desarrollo humano en los establecimientos educativos oficiales de los 24 municipios no certificados del Departamento del Cesar. | |
| **RESPONSABLES:** | **DIRIGE:** | Secretario de Educación |
| | **EJECUTA:** | Todas las dependencias de la Secretaría de Educación |
| | **CONTROLA:** | Jefe de la Oficina Asesora de Control Interno. |

| | |
|---|---|
| **PROCESO:** | Gestión de Trámites |
| **OBJETIVO:** | Garantizar la prestación de servicios oportunos, transparentes y confiables, con el fin de contribuir al acercamiento entre el ciudadano y |

| | | |
|---|---|---|
| | el estado a través de los diferentes canales de atención acorde a la normatividad legal aplicable aumentado la satisfacción de los ciudadanos, lo anterior para dar cumplimiento a las políticas y estrategias de eficiencia administrativa y racionalización de trámites. | |
| **RESPONSABLES:** | **DIRIGE:** | Jefe Oficina Asesora de Planeación Departamental |
| | **EJECUTA:** | Secretaria de Salud, Secretaria de Educación, Secretaría de Hacienda, Secretaría de Recreación y Deportes, Secretaría de Gobierno. |
| | **CONTROLA:** | Oficina Asesora de Asuntos Internos. |

### 3.4. ROLES Y RESPONSABLES

- **LÍDER DE PROCESO**

Funcionarios que ejercen el rol de Secretarios de despacho, Asesores de Despacho, Grupos de Gestión, Jefes de Oficina y líderes de programa encargados de realizar la identificación de riesgos de seguridad de la información, sobre los procesos que tiene a su cargo, con el acompañamiento del Profesional Especializado del Grupo de Recursos Físicos y Tecnológicos.

- **PROFESIONAL ESPECIALIZADO DEL GRUPO DE RECURSOS FÍSICOS Y TECNOLÓGICOS**

Funcionario encargado de acompañar al líder de proceso en la identificación de riesgos de seguridad de la información, sobre los procesos que tiene a cargo.

- **ASESOR DE PLANEACIÓN DEPARTAMENTAL**

Funcionario responsable de elaborar, actualizar, publicar y manejar los instrumentos de gestión de riesgos y orientar a las dependencias intervienen en este proceso.

- **SERVIDORES PÚBLICOS**

Funcionarios o contratistas comprometidos con el manejo responsable de los activos de la información de la entidad.

## 4. RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El análisis de riesgos de seguridad y privacidad de la información es un proceso que comprende la identificación de activos informáticos, sus vulnerabilidades y amenazas a los que se encuentran expuestos, así como su probabilidad de ocurrencia y el impacto de las mismas, a fin de determinar los controles adecuados para aceptar, disminuir, transferir o evitar la ocurrencia del riesgo.

Teniendo en cuenta que la explotación de un riesgo causaría daños o pérdidas financieras o administrativas a la entidad, se tiene la necesidad de poder estimar la magnitud del impacto del riesgo a que se encuentra expuesta mediante la aplicación de controles. Dichos controles, para que sean efectivos, deben ser implementados en conjunto formando una arquitectura de seguridad con la finalidad de preservar las propiedades de confidencialidad, integridad y disponibilidad de los recursos objetos de riesgo.

## 4.1. EVALUACIÓN DEL RIESGO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La entidad adoptará los criterios establecidos en la Guía No. 7: Gestión de Riesgos del Ministerio de las Tecnología de Información y las comunicaciones MINTIC, la cual se basa en la metodología del Departamento Administrativo de la Función Pública (DAFP), buscando la integración con el Mapa de Riesgos adoptado por el Departamento del Cesar, y de éste modo aprovechar la labor adelantada en la identificación de Riesgos, para ser complementados con los Riesgos de Seguridad.

La evaluación de los riesgos de seguridad de la información se enfocará en:

- El valor estratégico del proceso de información.
- La criticidad de los activos de información involucrados.
- Los requisitos legales y reglamentarios, así como las obligaciones contractuales.
- La importancia de la disponibilidad, integridad y confidencialidad para las operaciones de la Entidad
- Las expectativas y percepciones de las partes interesadas y las consecuencias negativas para el buen nombre y reputación de la Entidad.

Se sugiere realizar este análisis con los funcionarios con más comprensión del proceso, que por sus conocimientos o experiencia puedan determinar el impacto y la probabilidad del riesgo de acuerdo con los rangos señalados en las tablas que se muestran más adelante.

Como criterios para la estimación del riesgo desde el enfoque de impacto y consecuencias se podrán tener en cuenta: pérdidas financieras, costes de reparación o sustitución, interrupción del servicio, disminución del rendimiento, infracciones legales, pérdida de ventaja competitiva, daños personales, entre otros. Además de medir las posibles consecuencias se deberán analizar o estimar la probabilidad de ocurrencia de situaciones que generen impactos sobre los activos de información o la operación del negocio.

## 4.2. CRITERIOS DE PROBABILIDAD

**Tabla No. 3.** Criterios de Probabilidad

| NIVEL | DESCRIPTOR | DESCRIPCIÓN | FRECUENCIA |
|---|---|---|---|
| 1 | Raro | El evento puede ocurrir sólo en circunstancias excepcionales. | No se ha presentado en los últimos 5 años |

| | | | |
|---|---|---|---|
| 2 | Improbable | El evento puede ocurrir en algún momento. | Al menos de una vez en los últimos 5 años |
| 3 | Posible | El evento probablemente ocurrirá en la mayoría de las circunstancias. | Al menos de una vez en los últimos 2 años |
| 4 | Probable | Se espera que el evento ocurra en la mayoría de circunstancias | Al menos de una vez en el último año |
| 5 | Casi Seguro | Se espera que el evento ocurra en la mayoría de circunstancias. | Más de una vez al año |

**Fuente:** Guía para la Administración del Riesgo – DAFP

### 4.3. CRITERIOS DE IMPACTO

Los criterios de impacto se especificarán en términos del grado, daño o de los costos para la Entidad, causados por un evento de seguridad de la información, considerando aspectos tales como:

- Nivel de clasificación de los activos de información impactados
- Brechas en la seguridad de la información (pérdida de la confidencialidad, integridad y disponibilidad).
- Operaciones deterioradas (afectación a partes internas o terceras partes)
- Pérdida del negocio y del valor financiero
- Alteración de planes o fechas límites
- Daños en la reputación
- Incumplimiento de los requisitos legales, reglamentarios o contractuales

Los niveles de clasificación de impacto establecidos por la Entidad se definen a continuación:

**Tabla No. 4.** Criterios de Impacto

| NIVEL | DESCRIPTOR | DESCRIPCIÓN |
|---|---|---|
| 1 | Insignificante | La materialización del riesgo puede ser controlado por el(los) responsables del proceso, y no afecta el objetivo del proceso. |
| 2 | Menor | La materialización del riesgo ocasiona pequeñas demoras en el cumplimiento de las actividades del proceso, por tanto no afecta significativamente el cumplimiento de los objetivos de la Entidad. Tiene un impacto bajo en los procesos de otras áreas de la Entidad. |
| 3 | Moderado | La materialización del riesgo retrasa el cumplimiento del objetivo del proceso, y tiene un impacto moderado en los procesos de otras áreas de la Entidad. |
| 4 | Mayor | La materialización del riesgo retrasa el cumplimiento de los objetivos del Departamento del Cesar y tiene un impacto significativo en la imagen pública de la Entidad. |

| | | |
|---|---|---|
| | | Puede además generar impactos negativos en uno o varios sectores, el cumplimiento de acuerdos y obligaciones legales nacionales e internacionales, multas y/o sanciones embargos entre otros. |
| 5 | Catastrófico | La materialización del riesgo imposibilita el cumplimiento de los objetivos del Departamento del Cesar, tiene un impacto catastrófico en la imagen pública de la Entidad. Puede además generar impactos en: sectores económicos, los mercados; la industria, el cumplimiento de acuerdos y obligaciones legales nacionales e internacionales; multas y las finanzas públicas; entre otras. |

**Fuente:** Adaptación de la Guía para la Administración del Riesgo – DAFP

## 4.4. DETERMINACIÓN DEL RIESGO INHERENTE Y RESIDUAL

El análisis del riesgo determinado por su probabilidad e impacto permite tener una primera evaluación del riesgo inherente (escenario sin controles) y ver el grado de exposición al riesgo que tiene la entidad. La exposición al riesgo es la ponderación de la probabilidad e impacto, y se puede ver gráficamente en la matriz de riesgo, instrumento que muestra las zonas de riesgos y que facilita el análisis gráfico. Permite analizar de manera global los riesgos que deben priorizarse según la zona en que quedan ubicados los mismos (zona de riesgo bajo, moderado, alto o extremo) facilitando la organización de prioridades para la decisión del tratamiento e implementación de planes de acción.

**Tabla No. 5.** Matriz de Calificación, Evaluación y Respuesta a los Riesgos

| **PROBABILIDAD** | | **IMPACTO** | | | | |
|---|---|---|---|---|---|---|
| | | **Insignificante** | **Menor** | **Moderado** | **Mayor** | **Catastrófico** |
| | | **1** | **2** | **3** | **4** | **5** |
| Raro | **1** | B | B | M | A | A |
| Improbable | **2** | B | B | M | A | E |
| Posible | **3** | B | M | A | E | E |
| Probable | **4** | M | A | A | E | E |
| Casi Seguro | **5** | A | A | E | E | E |

| | | |
|---|---|---|
| B | Zona de Riesgo Baja | Asumir el Riesgo |
| M | Zona de Riesgo Moderada | Asumir el riesgo, Reducir el riesgo |
| A | Zona de Riesgo Alta | Reducir el Riesgo, Evitar, Compartir o Transferir |
| E | Zona de Riesgo Extrema | Reducir el Riesgo, Evitar, Compartir o Transferir |

**Fuente:** Guía para la Administración del Riesgo – DAFP

### 4.4.1. TRATAMIENTO DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Como resultado de la etapa de evaluación del riesgo tendremos una lista ordenada de riesgos o una matriz con la identificación de los niveles de riesgo de acuerdo con la zona de ubicación, por

tanto, se deberá elegir la(s) estrategia(s) de tratamiento del riesgo en virtud de su valoración y de los criterios establecidos en el contexto de gestión de riesgos mencionados anteriormente.

De acuerdo con el nivel evaluación de los riesgos, se deberá seleccionar la opción de tratamiento adecuada por cada uno de los riesgos identificados; el costo/beneficio del tratamiento deberá ser un factor de decisión relevante para la decisión.

**Tabla No. 6.** Tratamiento de Riesgos

| COSTO-BENEFICIO | OPCIÓN DE TRATAMIENTO | EJEMPLOS |
|---|---|---|
| El nivel de riesgo está muy alejado del nivel de tolerancia, su costo y tiempo del tratamiento es muy superior a los beneficios. | **Evitar el riesgo**, su propósito es no proceder con la actividad o la acción que da origen al riesgo. | • Tomar otra alternativa.<br>• Eliminar una actividad, un procedimiento o un proceso que puede ser la causa del incidente. |
| El costo del tratamiento por parte de terceros (internos o externos) es más beneficioso que el tratamiento directo. | **Transferir o compartir el riesgo**, entregando la gestión del riesgo a un tercero. | • Adquirir una póliza de seguros.<br>• Contratar o Subcontratar el servicio. |
| El costo y el tiempo del tratamiento son adecuados a los beneficios. | **Reducir o Mitigar el riesgo**, seleccionando e implementando los controles o medidas adecuadas que logren que se reduzca la probabilidad o el impacto | • Instalación de Firewall<br>• Sistemas para el control de incendios.<br>• Contratar servicios en la Nube para salvaguardar la información. |
| La implementación de medidas de control adicionales no generará valor agregado para reducir niveles de ocurrencia o de impacto. | **Asumir el riesgo**, no se tomará la decisión de implementar medidas de control adicionales. Monitorizarlo para confirmar que no se incrementa. | • Elaboración de controles de tipo preventivo y/o correctivo. |

**Fuente:** Elaboración propia

El resultado de estas fase se concreta en el mapa de riesgos de seguridad y privacidad de la información, es decir, la selección y justificación de una o varias opciones para cada riesgo identificado, que permitan establecer la relación de riesgos residuales, es decir, aquellos que aún siguen existiendo a pesar de las medidas tomadas.

## 5. MONITOREO Y SEGUIMIENTO DE LOS RIESGOS

Periódicamente se revisará el valor de los activos, impactos, amenazas, vulnerabilidades y probabilidades en busca de posibles cambios, que exijan la valoración iterativa de los riesgos de seguridad de la información.

Los riesgos son dinámicos como la misma Entidad por tanto podrán cambiar de forma o manera radical sin previo aviso. Por ello es necesaria una supervisión continua que detecte: nuevos activos o modificaciones en el valor de los activos, nuevas amenazas, cambios o aparición de nuevas vulnerabilidades, aumento de las consecuencias o impactos, incidentes de seguridad de la información.

Con el propósito de conocer los estados de cumplimiento de los objetivos de la gestión de los riesgos de seguridad de la información, se deberán definir esquemas de seguimiento y medición que permitan contextualizar una toma de decisiones de manera oportuna.

## 6. COMUNICACIÓN Y CONSULTA

La comunicación y consulta con las partes interesadas tanto internas como externas se debe realizar durante todas las etapas de la metodología para la administración de los riesgos de seguridad y privacidad de la información.

Se debe tener en cuenta que la producción y modificación de información es constante, por lo que se sugiere que la actualización del Registro de Activos de Información y sus respectivos riesgos, se realice cada vez que se presente alguna modificación de la categoría o serie de información.

El Grupo de Recursos Físicos y Tecnológicos, estará acompañando a los procesos en la identificación de los riesgos de seguridad y privacidad de la información, con el acompañamiento de la Oficina Asesora de Planeación Departamental.

## 7. MAPA DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (ANEXO)

El Consejo Asesor del Gobierno nacional en materia de control interno consideró necesario unificar la metodología existente para la administración del riesgo de gestión y corrupción, con el fin de hacer más sencilla la utilización de esta herramienta gerencial para las entidades públicas y así evitar duplicidades o reprocesos.

Actualmente la entidad cuenta con un único mapa de riesgos institucional que pretende identificar las actividades o procesos sujetos a riesgo, cuantificar la probabilidad de estos eventos y medir el daño potencial asociado a su ocurrencia. Por tanto, los riesgos de seguridad y privacidad de la información serán identificados, evaluados y monitorizados atendiendo los criterios de dicho instrumento. (Ver Anexo No. 1)

**Control de Cambios**

| FECHA | VERSION | CAMBIOS |
|---|---|---|
| 18/01/2019 | VER- 1.0 | |
| | | |
| | | |

| Elaboró | Revisó | Aprobó |
|---|---|---|
| **CARLOS OROZCO**<br>IBARRA<br>Contratista | **ALGONSO GARCÍA PAYARES**<br>Profesional Especializado<br>Grupo Recursos Físicos y Tecnológicos | **COMIÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO** |