Centro Nacional de Memoria Histórica

# PLAN DE TRATAMIENTO DE RIESGOS

## CentroNacional de Memoria Histórica

**Enero de 2021**

Centro Nacional de Memoria Histórica

# Contenido

## 1. INTRODUCCION

Las empresas hoy día, nos encontramos inmersas en la denominada revolución digital, en donde se reconoce 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.
La Seguridad de la Información en las empresas tiene como objetivo la protección de los activos de información en cualquiera de sus estados ante una serie de 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.

## 2. ASPECTOS GENERALES

### 2.1. OBJETIVO

Brindar al Centro Nacional de Memoria Historica una herramienta que proporcione las pautas necesarias para el adecuado tratamiento de los riesgos a los que están expuestos los activos de información, 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. ALCANCE

Este inventario fue desarrollado para los procesos del alcance del SGSI y son los siguientes:

- ✓ Difusión de Memoria Histórica
- ✓ Acuerdos de la Verdad
- ✓ Investigaciones
- ✓ Registro y Acopio
- ✓ Procesamiento
- ✓ Talento Humano

- ✓ Gestión de las TIC

## 2.3. DEFINICIONES

**Activo:** Cualquier elemento que tiene valor para la organización y que para la gestión de riesgos de seguridad de la información se consideran los siguientes tales como: la información, el software, elementos físicos, los servicios, las personas e intangibles.

**Amenaza:** Causa potencial de un incidente no deseado, el cual puede resultar en daño al sistema o a la Organización.
[Fuente: ISO 27000]

**Confidencialidad:** Propiedad de la información que hace que no esté disponible o que sea revelada a individuos no autorizados, entidades o procesos.

**Disponibilidad:** Propiedad de ser accesible y utilizable ante la demanda de una entidad autorizada.
[Fuente: ISO 27000]

**Importancia del activo**: Valor que refleja el nivel de protección requerido por un activo de información frente a las tres propiedades de la seguridad de la información: integridad, confidencialidad y disponibilidad.

**Integridad:** Propiedad de precisión y completitud.
[Fuente: ISO 27000]

**Monitoreo:** Verificación, supervisión, observación crítica o determinación continua del estado con el fin de identificar cambios con respecto al nivel de desempeño exigido o esperado.

**Parte involucrada:** Persona u organización que puede afectar, verse afectada o percibirse así misma como afectada por una decisión o una actividad. Una persona que toma decisiones puede ser una parte involucrada.
[Fuente: ISO 31000]

**Propietario del activo:** Persona o cargo que administra, autoriza el uso, regula o gestiona el activo de información. El propietario del activo aprueba el nivel de protección requerido frente a confidencialidad, integridad y disponibilidad.

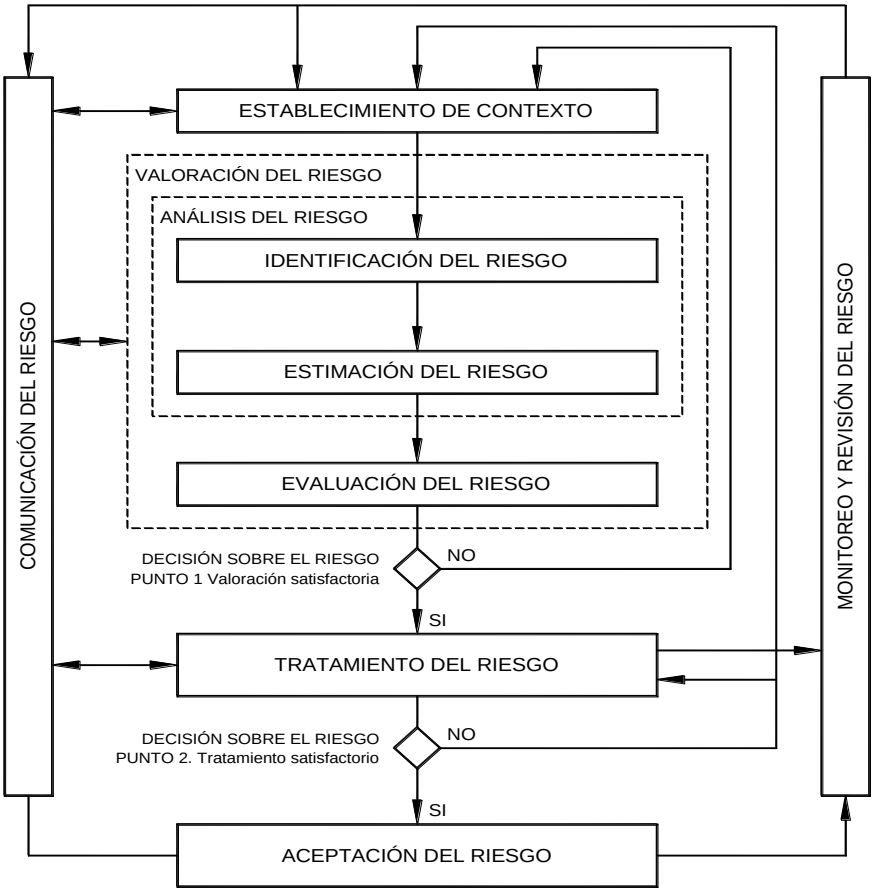
**Riesgo:** Efecto de la incertidumbre sobre los objetivos. Un efecto es una desviación de aquello que se espera, sea positivo, negativo o ambos. Los objetivos pueden tener aspectos

diferentes (económicos, de imagen, medio ambiente) y se pueden aplicar a niveles diferentes (estratégico, operacional, toda la organización)
[Fuente: ISO 31000]

**Vulnerabilidad:** Debilidad identificada sobre un activo que puede ser aprovechada por una amenaza para causar una afectación sobre la confidencialidad, integridad y/o disponibilidad de la información.

## 3. VISION GENERAL DEL PROCESO DE GESTION DE RIESGO EN LA SEGURIDAD DE LA INFORMACION

A continuación, se presenta el modelo de gestión de riesgos de seguridad de la información diseñado basado tanto en la norma ISO/IEC 31000 como en la ISO 27005 para la adecuada administración de riesgos en la seguridad de la información; los elementos que lo componen son:



La gestión de riesgos de seguridad de la información deberá ser iterativa para las actividades de valoración de riesgos y/o tratamiento de estos.

## 3.1. ESTABLECIMIENTO DEL CONTEXTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

El contexto de gestión de riesgos de seguridad de la información define los criterios básicos que serán necesarios para enfocar el ejercicio por parte del CNMH y obtener los resultados esperados, basándose en, la identificación de las fuentes que pueden dar origen a los riesgos y oportunidades en los procesos ded CNMH, en el análisis de las debilidades y amenazas asociadas, en la valoración de los riesgos en términos de sus consecuencias para la Entidad y en la probabilidad de su ocurrencia, al igual que en la construcción de acciones de mitigación en beneficio de lograr y mantener niveles de riesgos aceptables para la Entidad.

Como criterios para la gestión de riesgos de seguridad de la información se establecen:

### 3.1.1. Criterios de evaluación del riesgo de seguridad de la información:

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

- El valor estratégico del proceso de información en el CNMH.
- 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 del CNMH.
- Las expectativas y percepciones de las partes interesadas y las consecuencias negativas para el buen nombre y reputación del Centro.

### 3.1.2. Criterios de Impacto

Los criterios de impacto se especificarán en términos del grado, daño o de los costos para la el CNMH, 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

### 3.2. VALORACIÓN DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Los riesgos se deberán identificar, describir cuantitativamente o cualitativamente y priorizarse frente a los criterios de evaluación del riesgo y los objetivos relevantes para el CNMH, esta fase consta de las siguientes etapas:
La valoración del Riesgo de seguridad de la información consta de las siguientes actividades:

- Análisis del riesgo
    - Identificación de los riesgos
    - Estimación del riesgo
- Evaluación del riesgo

#### 3.2.1. Identificación del riesgo

Para la evaluación de riesgos de seguridad de la información en primer lugar se deberán identificar los activos de información por proceso en evaluación.
Los **activos de información** se clasifican en dos tipos:

a) **Primarios**:

**a. Procesos o subprocesos y actividades del Negocio:** procesos cuya pérdida o degradación hacen imposible llevar

Centro Nacional de Memoria Histórica

a cabo la misión de la organización; procesos que contienen procesos secretos o que implican tecnología propietaria; procesos que, si se modifican, pueden afectar de manera muy significativa el cumplimiento de la misión de la organización; procesos que son necesarios para el cumplimiento de los requisitos contractuales, legales o reglamentarios.

b. **Información**: información vital para la ejecución de la misión o el negocio de la organización; información personal que se puede definir específicamente en el sentido de las leyes relacionadas con la privacidad; información estratégica que se requiere para alcanzar los objetivos determinados por las orientaciones estratégicas; información del alto costo cuya recolección, almacenamiento, procesamiento y transmisión exigen un largo periodo de tiempo y/o implican un alto costo de adquisición, etc.

c. **Actividades y procesos de negocio**: que tienen que ver con propiedad intelectual, los que si se degradan hacen imposible la ejecución de las tareas de la empresa, los necesarios para el cumplimiento legal o contractual, etc.

b) **De Soporte**

a. **Hardware**: Consta de todos los elementos físicos que dan soporte a los procesos (PC, portátiles, servidores, impresoras, discos, documentos en papel, etc.).
b. **Software**: Consiste en todos los programas que contribuyen al funcionamiento de un conjunto de procesamiento de datos (sistemas operativos, paquetes de software o estándar, aplicaciones, mantenimiento o administración, etc.)
c. **Redes**: Consiste en todos los dispositivos de telecomunicaciones utilizados para interconectar varios computadores remotos físicamente o los elementos de un sistema de información (conmutadores, cableado, puntos de acceso, etc.)
d. **Personal**: Consiste en todos los grupos de personas involucradas en el sistema de información (usuarios, desarrolladores, responsables, etc.)

e. **Sitio**: Comprende todos los lugares en los cuales se pueden aplicar los medios de seguridad de la organización (Edificios, salas, y sus servicios, etc.)
f. **Estructura organizativa**: responsables, áreas, contratistas, etc.

Después de tener una relación con todos los activos se han de conocer las **amenazas** que pueden causar daños en la información, los procesos y los soportes. La identificación de las amenazas y la valoración de los daños que pueden producir se puede obtener preguntando a los propietarios de los activos, usuarios, expertos, etc.

- Posterior a la identificación del listado de activos, sus amenazas y las medidas que ya se han tomado, a continuación, se revisarán las **vulnerabilidades** que podrían aprovechar las amenazas y causar daños a los activos de información del CNMH. Existen Entrevistas con líderes de procesos y usuarios
- Inspección física
- Uso de las herramientas para el escaneo automatizado

Para cada una de las **amenazas** analizaremos las **vulnerabilidades** (debilidades) que podrían ser explotadas.

Finalmente se identificarán las **consecuencias**, es decir, cómo estas amenazas y vulnerabilidades podrían afectar la confidencialidad, integridad y disponibilidad de los activos de información.

### 3.2.2. Estimación del riesgo

La estimación del riesgo busca establecer la probabilidad de ocurrencia de los riesgos y el impacto de sus consecuencias, calificándolos y evaluándolos con el fin de obtener información para establecer el nivel de riesgo, su priorización y estrategia de tratamiento de estos. El objetivo de esta etapa es el de establecer una valoración y priorización de los riesgos.

Para adelantar la estimación del riesgo se deben considerar los siguientes aspectos:

- **Probabilidad**: La posibilidad de ocurrencia del riesgo, representa el número de veces que el riesgo se ha presentado en un determinado tiempo o pudiese presentarse.
- **Impacto**: Hace referencia a las consecuencias que puede ocasionar al CNMH la materialización del riesgo; se refiere a la magnitud de sus efectos.

Se sugiere realizar este análisis con todas o las personas que más conozcan del proceso, y 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.

| PROBABILIDAD | | | |
|---|---|---|---|
| **Concepto** | **Valor** | **Descripción** | **Frecuencia** |
| Raro | 1 | El evento puede ocurrir sólo en circunstancias excepcionales. | No se ha presentado en los últimos 5 años |
| Improbable | 2 | Es muy poco factible que el evento se presente. | Al menos de 1 vez en Los últimos 5 años. |
| Posible | 3 | El evento podría ocurrir en algún momento. | Al menos de 1 vez en Los últimos 2 años. |
| Probable | 4 | El evento probablemente ocurrirá en la mayoría de las circunstancias, | Al menos de 1 vez en El último año. |
| Casi Certeza | 5 | Se espera que ocurra en la mayoría de las circunstancias | Más de 1 vez al año. |

| IMPACTO | | |
|---|---|---|
| **Concepto** | **Valor** | **Descripción** |
| Insignificante | 1 | La materialización del riesgo **puede ser controlado** por los participantes del proceso, y **no afecta los objetivos del proceso**. |
| Menor | 6 | La materialización del riesgo ocasiona **pequeñas demoras** en el cumplimiento de las actividades del proceso, y **no afecta significativamente el cumplimiento de los objetivos** del CNMH. Tiene un impacto bajo en los procesos de otras áreas de la Entidad. |
| Moderado | 7 | La materialización del riesgo **demora el cumplimiento de los objetivos del proceso,** y tiene un **impacto moderado en los procesos de otras áreas** de la Entidad. Puede además causar un deterioro en el desarrollo del proceso dificultando o retrasando el cumplimiento de sus objetivos, impidiendo que éste se desarrolle en forma normal. |
| Mayor | 11 | La materialización del riesgo **retrasa el cumplimiento de los objetivos del CNMH** y tiene un **impacto significativo en la imagen pública** de la Entidad y/o de la Nación. Puede además generar impactos en: la industria; sectores económicos, el cumplimiento de acuerdos y obligaciones legales |

| | | |
|---|---|---|
| | | nacionales e internacionales; multas y las finanzas públicas; entre otras |
| Catastrófico | 13 | La materialización del riesgo **imposibilita el cumplimiento de los objetivos de la Entidad**, tiene un **impacto catastrófico en la imagen pública de la Entidad y/o de la Nación**. 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. |

### 3.2.3. 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.

Centro Nacional de Memoria Histórica

| PROBABILIDAD | | IMPACTO | | | | |
|---|---|---|---|---|---|---|
| | | INSIGNIFICANTE (1) | MENOR (6) | MODERADO (7) | MAYOR (11) | CATASTROFICO (13) |
| E (RARO) | 1 | 1 Zona 1 de riesgo Baja (B) Asumir el riesgo | 6 Zona 4 de riesgo Baja (B) Asumir el riesgo | 7 Zona 8 de riesgo Moderada (M) Asumir el riesgo Reducir el riesgo. | 11 Zona 15 de riesgo Alta (A) Reducir el riesgo. Evitar el riesgo Compartir o transferir el riesgo | 13 Zona 17 de riesgo Alta (A) Reducir el riesgo. Evitar el riesgo Compartir o transferir el riesgo |
| D (IMPROBABLE) | 2 | 2 Zona 2 de riesgo Baja (B) Asumir el riesgo | 12 Zona 5 de riesgo Baja (B) Asumir el riesgo | 14 Zona 9 de riesgo Moderada (M) Asumir el riesgo Reducir el riesgo. | 22 Zona 16 de riesgo Alta (A) Reducir el riesgo. Evitar el riesgo Compartir o transferir el riesgo | 26 Zona 22 de riesgo Extrema (E) Evitar el riesgo Reducir el riesgo. Compartir o transferir el riesgo |
| C (POSIBLE) | 3 | 3 Zona 3 de riesgo Baja (B) Asumir el riesgo | 18 Zona 7 de riesgo Moderada (M) Asumir el riesgo Reducir el riesgo. | 21 Zona 13 de riesgo Alta (A) Reducir el riesgo. Evitar el riesgo Compartir o transferir el riesgo | 33 Zona 19 de riesgo Extrema (E) Evitar el riesgo Reducir el riesgo. Compartir o transferir el riesgo | 39 Zona 23 de riesgo Extrema (E) Evitar el riesgo Reducir el riesgo. Compartir o transferir el riesgo |
| B (PROBABLE) | 4 | 4 Zona 6 de riesgo Moderada (M) Asumir el riesgo Reducir el riesgo. | 24 Zona 11 de riesgo Alta (A) Reducir el riesgo. Evitar el riesgo Compartir o transferir el riesgo | 28 Zona 14 de riesgo Alta (A) Reducir el riesgo. Evitar el riesgo Compartir o transferir el riesgo | 44 Zona 20 de riesgo Extrema (E) Evitar el riesgo Reducir el riesgo. Compartir o transferir el riesgo | 52 Zona 24 de riesgo Extrema (E) Evitar el riesgo Reducir el riesgo. Compartir o transferir el riesgo |
| A (CASI SEGURO) | 5 | 5 Zona 10 de riesgo Alta (A) Reducir el riesgo. Evitar el riesgo Compartir o transferir el riesgo | 30 Zona 12 de riesgo Alta (A) Reducir el riesgo. Evitar el riesgo Compartir o transferir el riesgo | 35 Zona 18 de riesgo Extrema (E) Evitar el riesgo Reducir el riesgo. Compartir o transferir el riesgo | 55 Zona 21 de riesgo Extrema (E) Evitar el riesgo Reducir el riesgo. Compartir o transferir el riesgo | 65 Zona 25 de riesgo Extrema (E) Evitar el riesgo Reducir el riesgo. Compartir o transferir el riesgo |

| ZONA | NIVEL DE RIESGO |
|---|---|
| ZONA RIESGO BAJO | Z-1 |
| | Z-2 |
| | Z-3 |
| | Z- 4 |
| | Z- 5 |
| ZONA RIESGO MODERADO | Z-6 |
| | Z-7 |
| | Z-8 |
| | Z-9 |
| ZONA DE RIESGO ALTA | Z-10 |
| | Z-11 |
| | Z-12 |
| | Z-13 |
| | Z-14 |
| | Z-15 |
| | Z-16 |
| | Z-17 |
| ZONA DE RIESGO EXTREMA | Z-18 |
| | Z-19 |
| | Z-20 |
| | Z-21 |
| | Z-22 |
| | Z-23 |
| | Z-24 |
| | Z-25 |

Las zonas de riesgo se diferencian por colores y por número de la zona de la siguiente manera:

| Zona de Riesgo |
|---|
| B: Zona de riesgo Baja (Color Verde): 5 zonas, siendo Z- 5 la zona de mayor riesgo. |
| M: Zona de riesgo Moderada (color Amarillo): 4 zonas, siendo Z- 9 la zona de mayor riesgo. |
| A: Zona de riesgo Alta (Color Rojo): 8 zonas, siendo Z- 17 la zona de mayor riesgo. |
| ***E: Zona de riesgo Extrema (Color Vino tinto): 8 zonas, siendo la Z-25 la de más alto riesgo.*** |

### 3.2.4. Evaluación de los riesgos

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 a la Alta Entidad.

## 3.3. 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.
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.

| COSTO - BENEFICIO | OPCION DE TRATAMIENTO |
|---|---|
| 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 (ejemplo, dejando de realizar una actividad, tomar otra alternativa, etc.) |

| COSTO - BENEFICIO | OPCION DE TRATAMIENTO |
|---|---|
| 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 (ejemplo, contratando un seguro o subcontratando el servicio). |
| El costo y el tiempo del tratamiento es adecuado 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 |
| La implementación de medidas de control adicionales no generará valor agregado para reducir niveles de ocurrencia o de impacto. | **Retener o aceptar** el riesgo, no se tomará la decisión de implementar medidas de control adicionales. Monitorizarlo para confirmar que no se incrementa |

El resultado de esta fase se concreta en un plan de tratamiento de riesgos, 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.

### 3.4. MONITOREO Y SEGUIMIENTO DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

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: (1) nuevos activos o modificaciones en el valor de los activos, (2) nuevas amenazas • (3) cambios o aparición de nuevas vulnerabilidades • (4) aumento de las consecuencias o impactos, (5) 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 al sistema de gestión de riesgos de la seguridad de la información que permitan contextualizar una toma de decisiones de manera oportuna.

## 4. METODOLOGÍA

Para llevar a cabo la implementación del Modelo de Seguridad y Privacidad de la Información, 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.

## 5. ACTIVIDADES

| CRONOGRAMA | S1 | S2 | S3 | S4 | S1 | S2 | S3 | S4 | S1 | S2 | S3 | S4 | S1 | S2 | S3 | S4 | S1 | S2 | S3 | S4 | S1 | S2 | S3 | S4 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | FEBRERO | | | | MARZO | | | | ABRIL | | | | MAYO | | | | JUNIO | | | | JULIO | | | |
| Diseño del Plan de tratamieto de riesgos. | | | | | | | | | | | | | | | | | | | | | | | | |
| Valoracion de Activos. | | | | | | | | | | | | | | | | | | | | | | | | |
| Realizar la Identificación de los Riesgos. | | | | | | | | | | | | | | | | | | | | | | | | |
| Diseño del Plan de tratamieto de riesgos. | | | | | | | | | | | | | | | | | | | | | | | | |
| Desarrollo, ejecucion de Actividades definidas en el plan de tratamiento de riesgos. | | | | | | | | | | | | | | | | | | | | | | | | |
| Informe de Riesgos a la Gerencia. | | | | | | | | | | | | | | | | | | | | | | | | |