

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

**CONTRALORIA MUNICIPAL DE NEIVA**

**2020**

*¡Neiva Bajo Control, Compromiso de Todos!*

**Contraloría  
Municipal  
de Neiva**



*Neiva Bajo Control  
Compromiso de Todos !*

## **FORMATO**

### **INTRODUCCION**

La gestión de los riesgos de seguridad de la información son aquellos procesos que reducen las pérdidas y brindan protección de la información, permitiendo conocer las debilidades que afectan durante todo el ciclo de vida del servicio.

Es muy importante que las organizaciones cuenten con un plan de gestión de riesgos para garantizar la continuidad de los sistemas informáticos y telemáticos. Por este motivo, se ha visto la necesidad de desarrollar un análisis de riesgo de seguridad de la información aplicado en La Contraloría Municipal de Neiva (CMN). Antes de iniciar con este plan de gestión se ha revisado el documento con el diagnóstico del sistema actual de la empresa, donde se conoce la situación actual de la organización y la identificación de los activos con sus respectivas amenazas, para continuar con la medición de riesgos existentes y sugerir las protecciones necesarias que podrían formar parte del plan de gestión de riesgos en la seguridad de la información.

El aporte que arroja este plan permite identificar el nivel de riesgo en que se encuentran los activos mediante el nivel de madurez de la seguridad existente y sobre todo incentivar al personal a seguir las respectivas normas y procedimientos referentes a la seguridad de la información y recursos.

*¡Neiva Bajo Control, Compromiso de Todos!*



## **TABLA DE CONTENIDO**

	Pág.
Introducción	
1. Objetivos	
1.1 Objetivo General.....	6
1.2 Objetivos Específicos.....	6
2. Alcances y Limitaciones	
2.1 Alcance.....	7
2.2 Limitaciones.....	7
3. Gestión de Riesgos	
3.1 Importancia de la Gestión del Riesgo.....	8
3.2 Definición Gestión del Riesgo.....	9
3.3 Visión General para la administración del Riesgo de Seguridad de la Información.....	10
3.4 Identificación del Riesgo.....	10
3.5 Situación no deseada.....	11
4. Origen del plan de gestión de riesgo de SI.....	12
4.1 Propósito del plan de gestión de riesgo de SI.....	13
4.2 Identificación del riesgo.....	13
5. Análisis de vulnerabilidades.....	14
5.1 Descripción de vulnerabilidades.....	14

<p><b>Contraloría Municipal de Neiva</b> <i>Neiva Bajo Control Compromiso de Todos !</i></p>	<p><b>FORMATO</b></p>
--	-----------------------

5.2 Matriz de vulnerabilidades y Mitigación del Riesgo.....17

6. Propuesta de Seguridad.....22

6.1 Plan seguro para el acopio de copias de seguridad.....24

6.2 Plan de continuidad de los sistemas informáticos y telemáticos.....25

6.3 Implementación de políticas.....25

6.4 Plan de capacitación.....25

6.5 Certificación en ISO/IEC 27001 / ISO/IEC 27017.....25

Bibliografía

Conclusiones

**TABLA DE ILUSTRACIONES**

Pág.

Figura 1. Proceso para la Administración del Riesgo.....	10
Figura 2. Matriz de vulnerabilidades y Mitigación de Riesgo.....	19

## **1. OBJETIVOS**

### **1.1 Objetivo General**

Desarrollar un plan de gestión de seguridad y privacidad que permita minimizar los riesgos de pérdida de activos de la información en la Contraloría Municipal de Neiva (CMN).

### **1.2 Objetivos Específicos**

- Plantear modelos de reportes para su posterior uso en cada incidencia presentada en la Contraloría Municipal de Neiva (CMN).
- Gestionar los eventos de seguridad de la información para detectar y tratar con eficiencia, en particular identificar si es necesario o no clasificarlos como incidentes de seguridad de la información.
- Determinar el alcance del plan de gestión de riesgos de la seguridad y privacidad de la información.
- Definir los principales activos a proteger en la Contraloría Municipal de Neiva (CMN).
- Identificar las principales amenazas que afectan a los activos.
- Proponer soluciones para minimizar los riesgos a los que está expuesto cada activo.
- Evaluar y comparar el nivel de riesgo actual con el impacto generado después de implementar el plan de gestión de seguridad de la información

## **2. ALCANCES Y LIMITACIONES**

*¡Neiva Bajo Control, Compromiso de Todos!*

## **2.1 ALCANCES**

- Lograr el compromiso de la Contraloría Municipal de Neiva (CMN) para emprender la implementación del plan de gestión del riesgo en la seguridad de la información.
- Designar funciones de liderazgo para apoyar y asesorar el proceso de diseño e implementación del plan de gestión.
- Capacitar al personal de la entidad en el proceso de plan de gestión del riesgo de la seguridad de la información.

## **2.2 LIMITACIONES**

- Crear el rubro del presupuesto necesario para apoyar la implementación del plan de gestión del riesgo de la seguridad de la información en la Contraloría Municipal de Neiva (CMN).

## **2. GESTIÓN DE RIESGOS**

### **3.1 IMPORTANCIA DE LA GESTIÓN DE RIESGOS**

En el ámbito empresarial se está dando mayor prioridad a salvar, proteger y custodiar el activo de la información, debido a que los sistemas de información y los avances tecnológicos están siendo implementados en todas las empresas del mundo.

La Contraloría Municipal de Neiva (CMN), sigue los lineamientos trazados por el Gobierno Nacional en cumplimiento de la Ley de Transparencia 1712 de 2014 y Gobierno en Línea que viene impulsando actividades dentro de las entidades públicas

*¡Neiva Bajo Control, Compromiso de Todos!*

 <p><b>Contraloría Municipal de Neiva</b> <i>Neiva Bajo Control Compromiso de Todos !</i></p>	<h2>FORMATO</h2>
--	------------------

para que se ajusten a modelos y estándares que permitan brindar seguridad a la información dando cumplimiento al Decreto 1078 de 2015.

Los riesgos por desastres naturales, riesgos inherentes relacionados con procesos no adecuados en el tratamiento de la misma información, desconocimiento de normas y políticas de seguridad y el no cumplimiento de estas, suelen ser los temas más frecuentes y de mayor impacto presentes en las empresas. Una entidad sin un plan de gestión de riesgos está expuesta a perder su información.

Todas las organizaciones deberían implementar planes para gestionar los riesgos que afectan a los sistemas de información, tecnologías de información y activos informáticos, considerando que en la actualidad los riesgos más comunes son generados por ataques dirigidos al software empresarial, afectando la disponibilidad e integridad de la información almacenada o transportada a través de los equipos de comunicación.

Por esta razón hay que estar preparados para prevenir todo tipo de ataques o desastres, ya que cuando el costo de recuperación supera al costo de prevención es preferible tener implementados planes de gestión de riesgos que permitan la continuidad de los sistemas informáticos y telemáticos tras sufrir alguna pérdida o daño en la información de la entidad.

Considerando la situación actual de la Contraloría Municipal de Neiva (CMN), para reducir los niveles de riesgo, es indispensable diseñar un plan para iniciar las prácticas de las normas y políticas de seguridad e implementar procesos que aseguren la continuidad de los servicios.

### **3.2 DEFINICION GESTIÓN DEL RIESGO**

*¡Neiva Bajo Control, Compromiso de Todos!*



La definición estandarizada de riesgo proviene de la Organización Internacional de Normalización (ISO), definiéndolo como “la posibilidad de que una amenaza determinada explote las vulnerabilidades de un activo o grupo de activos y por lo tanto causa daño a la organización”.

### 3.3 VISION GENERAL PARA LA ADMINISTRACIÓN DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN



Figura 1 Proceso para la administración del riesgo.

### 3.4 IDENTIFICACIÓN DEL RIESGO

1. 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

 <p><b>Contraloría Municipal de Neiva</b> <i>Neiva Bajo Control Compromiso de Todos!</i></p>	<p><b>FORMATO</b></p>
---	-----------------------

y el cumplimiento de los objetivos estratégicos, la clara definición de políticas, diseño y conceptualización de la entidad por parte de la alta gerencia.

2. Riesgos de Imagen: Están relacionados con la percepción y la confianza por parte de la ciudadanía hacia la institución.

3. 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 y de la articulación entre dependencias.

4. 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.

5. 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, de acuerdo con su misión.

6. 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.

### **3.5 SITUACION NO DESEADA**

Hurto de información o de equipos informáticos.

Hurto de información durante el cumplimiento de las funciones laborales, por intromisión

Incendio en las instalaciones de la empresa por desastre natural o de manera intencional.

Alteración de claves y de información.

*¡Neiva Bajo Control, Compromiso de Todos!*

Pérdida de información.  
Baja Cobertura de internet.  
Daño de equipos y de información  
Atrasos en la entrega de información  
Atrasos en asistencia técnica  
Fuga de información  
Manipulación indebida de información

#### **4. ORIGEN DEL PLAN DE GESTION**

Debido a que la Contraloría Municipal de Neiva (CMN) no tenía un área de sistemas conformada y se evidenció que no existen procesos asignados a dicha área entre otras vulnerabilidades que se encontraron en el sistema actual, es necesario crear un plan de gestión de riesgos de seguridad de la información que permita proteger el activo más valioso para la entidad; la información.

La situación actual del sistema de seguridad de la información en la entidad se encuentra planteado en el Diagnostico de seguridad y privacidad de la Información con fecha de junio de 2017.

El gobierno nacional y el ministerio de las TIC han abanderado los proyectos de Gobierno en Línea que permite conocer el funcionamiento de las entidades públicas en el país. Es por ello necesario que la Contraloría Municipal de Neiva (CMN) cumpla con los requisitos necesarios para entregar la información de manera oportuna y eficiente a estas entidades, a la población y a la misma CMN.

#### **4.1 PROPÓSITO DEL PLAN DE GESTION DE RIESGO DE LA SEGURIDAD DE LA INFORMACIÓN.**

*¡Neiva Bajo Control, Compromiso de Todos!*

Dar soporte al modelo de seguridad de la información al interior de la entidad.

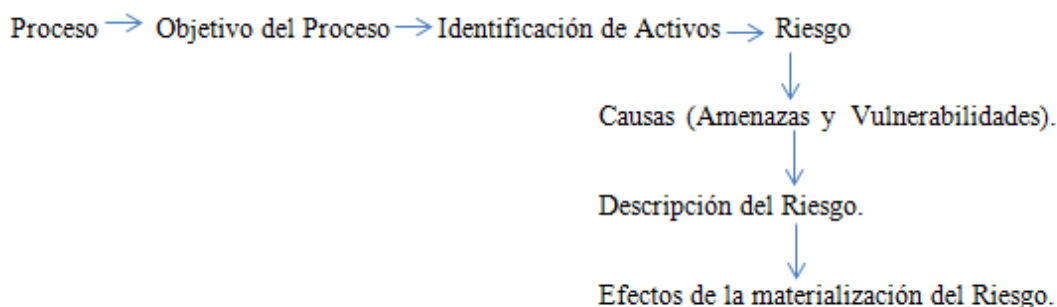
Conformidad legal y evidencias de la debida diligencia.

Preparación de un plan de respuesta a incidentes.

Descripción de los requisitos de seguridad de la información para un producto, un servicio o un mecanismo.

Alcances, límites y organización del proceso de gestión de riesgos en la seguridad de la información.

## 4.2 IDENTIFICACIÓN DEL RIESGO



## 5. ANALISIS DE VULNERABILIDADES

### 5.1 DESCRIPCIÓN DE VULNERABILIDADES

Aunque la protección de la información digital se ve amenazada frecuentemente por errores cometidos por los usuarios, en la Contraloría Municipal de Neiva (CMN) se encontraron otras amenazas e impactos como los siguientes:

*¡Neiva Bajo Control, Compromiso de Todos!*

1. Los puntos de red ubicados en cada oficina no son suficientes y se han dispuesto nuevos según se va presentando la necesidad.
2. Algunos cables de energía no están cerca a los escritorios o no son suficientes para la cantidad de equipos que tiene cada oficina, existe riesgo de pérdida de información en el caso que sean desconectados por accidente y la información procesada por el funcionario no alcanza a ser guardada.
3. Las políticas y normas de seguridad de la información existentes no han sido socializadas con todo el personal, por eso es muy común identificar el incumplimiento a las reglas básicas del cuidado tanto de los equipos informáticos y como de la información física y digital, algunas son:
  - Bebidas y alimentos cerca a los equipos de cómputo, cualquier derrame de líquidos afectan los activos de información y de informática.
  - En algunos papeles reutilizables se encontró información personal que debe ser reservada, identificándose la falta de confidencialidad y privacidad.
  - La información es llevada en memorias o discos duros portátiles personales, por ende la información sale de la entidad.
  - No hay control para el uso de memorias portátiles en los equipos de la Contraloría Municipal de Neiva (CMN), exponiendo a perder la información por virus no detectados o daños irreparables del hardware.
  - No existe un área de sistemas con personal encargado de revisar, documentar, diseñar y controlar los procesos propios de un modelo de seguridad de la información para la Contraloría Municipal de Neiva (CMN).
  - No existe un historial de reportes de los procesos de asistencias y/o mitigación de vulnerabilidades realizados por el personal de sistemas en la entidad.
  - Los documentos físicos que se manejan en la entidad no se han digitalizado por lo tanto están expuestos a pérdidas y daños físicos debido a que los sitios de almacenamiento en las oficinas no son los adecuados.
  - No existe un plan de continuidad de los sistemas informáticos y telemáticos que permitan reanudar las operaciones normales durante o después de interrupciones significativas a las operaciones de la Contraloría Municipal de Neiva (CMN). (en caso de incendio o desastre natural existen altas probabilidades de perder la información de los servidores)



## **FORMATO**

*¡Neiva Bajo Control, Compromiso de Todos!*

## FORMATO

### 5.2 MATRIZ DE VULNERABILIDADES Y MITIGACION DEL RIESGO

VULNERABILIDAD	DESCRIPCIÓN	CAUSA	EFECTO	CLASIFICACIÓN	ANÁLISIS		VALORACIÓN	VIGENCIA DE CUMPLIMIENTO
					CALIFICACIÓN	EVALUACIÓN	MITIGACIÓN DEL RIESGO	
<b>*Fallas eléctricas</b>	Las conexiones no son suficientes, no cumplen con las exigencias el tamaño de la red de equipos de cómputo (cables sueltos, inadecuada estructura y adecuación)	Inadecuada conexión de cableado eléctrico	Posible pérdida de información	*Riesgo tecnológico *Riesgo físico *Riesgo humano	40	Riesgo moderado	Plantear un nuevo diseño de la red eléctrica	Vigencia 2020
<b>*Afectación de activos de información y activos informáticos.</b>	Desconocimiento de las políticas y normas de seguridad de la información.	No socialización No capacitación de las políticas y normas de seguridad.	Acciones no adecuadas en el tratamiento de los activos de información e informáticos	* Riesgo Tecnológico * Riesgo en Servicio * Riesgo de la Información * Riesgo en personal	60	Riesgo Alto	Diseñar, socializar e implementar un Manual de políticas y normas de seguridad de la información en	Vigencia 2020

*¡Neiva Bajo Control, Compromiso de Todos!*

## FORMATO

							la Contraloría Municipal de Neiva (CMN).	
<b>*Pérdida de información de tiempo productivo en funciones laborales.</b>	Las fallas en la señal de internet son constantes.	Señal inalámbrica	Señal débil en las oficinas. Retraso en tiempos de producción para los funcionarios.	*Riesgo Tecnológico *Riesgo en Servicio de información	40	Riesgo Importante	Implantar un modelo de red basado en cableado estructurado.	Vigencia 2020
<b>*Incumplimiento de las actividades de seguridad de la información.</b>	El personal encargado de los sistemas no es suficiente. No se están siguiendo protocolos y normas para garantizar la seguridad de la información en la entidad	No existe personal encargado del proceso de aseguramiento de la información	Ausencia de transferencia de conocimiento y falta de capacitación	*Riesgo de información. *Riesgo de servicio. *Riesgo tecnológico	60	Riesgo Alto	Encargar a personal capacitado para el aseguramiento de la información. Capacitar al personal de la Contraloría Municipal de Neiva (CMN) para el cumplimiento de procesos y actividades de	Vigencia 2020

*¡Neiva Bajo Control, Compromiso de Todos!*



## FORMATO

							seguridad de la información	
<b>Confidencialidad e Integridad de la información</b>	En la entidad se trabaja en la campaña cero papeles, sin embargo se han encontrado dentro del papel reutilizable información personal de algunos pobladores del municipio beneficiarios de programas sociales.	Exposición de datos personales en papel reutilizable.	incumplimiento de confidencialidad e integridad de la información	*riesgo de Información	60	Riesgo Alto	Socializar con los funcionarios de la entidad acerca de las políticas de seguridad y confidencialidad de la información.	Vigencia 2020
<b>*Pérdida de Información</b>	Los funcionarios no realizan copias de seguridad a la información	No hacen copias de seguridad	Posible pérdida de información	*Riesgo de Información * Riesgo en Servicio	40	Riesgo Importante	*Capacitar al personal de la Contraloría Municipal de Neiva (CMN) para el dominio de este	Vigencia 2020

*¡Neiva Bajo Control, Compromiso de Todos!*

## FORMATO

	producto de sus funciones.						tema. *Adquirir un Servidor para almacenar las copias de seguridad. *Adquisición de una nube para almacenamiento de información. *Crear cuentas de usuario con claves.	
	Uso de memorias extraíbles y unidades extraíbles	No hay control de uso	Infección por Virus	*Riesgo Tecnológico				Vigencia 2020
<b>*Pérdida de información y/o deterioro físico</b>	La documentación e información en papel o física está siendo archivada en sitios no adecuados para ello.	No se ha iniciado la ejecución de digitalización de información.	Daño de documentos y deterioro del papel.	*Riesgo de Información	40	Riesgo Importante	Iniciar la ejecución de la digitalización y almacenamiento de la información contenida en papel.	Vigencia 2020

*¡Neiva Bajo Control, Compromiso de Todos!*



## **FORMATO**

*¡Neiva Bajo Control, Compromiso de Todos!*

## **6. PROPUESTA DE SEGURIDAD**

- Revisar, organizar y ubicar las conexiones de electricidad según las necesidades propias de las oficinas.
- Revisar las políticas existentes para identificar debilidades y fortalezas, si es necesario se hacen ajustes, teniendo en cuenta que seguridad informática no es igual a seguridad de la información.
- Socializar las políticas de seguridad y privacidad de la información con el personal de la Contraloría Municipal de Neiva (CMN).
- Crear un rubro del presupuesto para la adquisición de las licencias de los sistemas operativos y aplicaciones ofimáticas para los equipos de la Contraloría Municipal de Neiva (CMN).
- En caso de usar Libre Office se debe capacitar al personal en el manejo del sistema ofimático.
- Migrar a un mejor proveedor de alojamiento web los contenidos del portal y la intranet corporativa, con el fin de garantizar la implementación de mejores políticas de seguridad.
- Adquirir un sistema de copias de seguridad en la nube para toda la organización.
- Crear el área de sistemas o TIC para dirigir la creación y el control de un sistema de seguridad y privacidad de la información en la Contraloría Municipal de Neiva (CMN) junto con otras actividades propias del área.
- Crear los procesos de la oficina de las TIC para la entidad.
- Implementar el sistema de documentación digital en la Contraloría Municipal de Neiva (CMN) para reducir riesgos de pérdida de información física.
- La Contraloría Municipal de Neiva (CMN) comprometida con la campaña cero papel, está próxima en habilitar el software para digitalización de documentos y gestión documental en los próximos meses.

### **6.1 PLAN SEGURO PARA EL ACOPIO DE COPIAS DE SEGURIDAD**

- Adquirir un servidor con características específicas para el almacenamiento de copias de seguridad de la información local manejada en las diferentes dependencias.
- Obtener una nube dedicada para la información de la Contraloría Municipal de Neiva (CMN) con el fin de tener un respaldo en caso de accidentes.
- Contar con un plan alternativo que asegure la continuidad de la actividad de los sistemas informáticos y telemáticos en caso que ocurran incidentes graves.

*¡Neiva Bajo Control, Compromiso de Todos!*

- Nunca se debe olvidar que la realidad es que la entidad puede sufrir un incidente que afecte su continuidad y, dependiendo de la forma en que se gestionen dichos incidentes, las consecuencias pueden ser más o menos graves. Siempre teniendo en cuenta que la información requiere ser protegida y se debe trabajar sobre los tres pilares fundamentales: confidencialidad, integridad y disponibilidad. Una de las principales características que debe poseer la entidad es buscar cómo establecer un Sistema de seguridad enfocado por procesos, resaltando la importancia que tienen las actividades de monitoreo y la correcta configuración para disminuir los riesgos y realizar tratamiento de las diferentes y constantes vulnerabilidades, para lo cual se deberán tener en cuenta los hallazgos y recomendaciones identificadas, cuyo propósito se encamine a mitigar los riesgos encontrados.

## **6.2 PLAN DE CONTINUIDAD DE LOS SISTEMAS INFORMATICOS Y TELEMATICOS**

- Diseñar un formato de chequeo de acuerdo a las necesidades de la organización que permita realizar la auditorías periódicas al con la finalidad de verificar que los objetivos de control, procesos y procedimientos se cumplan.
- Socializar con los directivos, secretaría general y oficina de las TIC la importancia del Plan de Continuidad de los sistemas informáticos y telemáticos, para hacer frente a incidentes graves de seguridad en la Entidad, resumiendo de forma clara y sencilla cada una de las actividades a desarrollar dentro del plan.
- Diseñar estrategias para el proceso de recuperación teniendo en cuenta los tiempos de reacción e implementación de contingencias ante la realización de los eventos identificados.
- Adoptar una de las tres posiciones anteriores, que permita minimizar la ocurrencia o los efectos colaterales sobre la red, esto de acuerdo con los siguientes enfoques:
  - 1) Detectar el riesgo
  - 2) Plantear controles y efectuar las implementaciones respectivas.
  - 3) Mitigar el riesgo.
- Diseñar un Plan de Contingencia teniendo en cuenta que la continuidad de los sistemas informáticos y telemáticos dependerá de los riesgos y amenazas potenciales que serán tratados de acuerdo a lo siguiente:
  - 1) Política de copia de seguridad de datos
  - 2) Procedimientos de almacenamiento fuera de la Contraloría Municipal de Neiva (CMN)
  - 3) Procedimientos de gestión de emergencias, por desastre natural, por incendio o por inundaciones

### **6.3 IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD PARA LA INFORMACIÓN**

El análisis realizado a todo el contexto informático y telemático de la Contraloría Municipal de Neiva (CMN) permitió identificar que se desconocen y poco se cumplen las políticas de seguridad de la información; por lo cual debe quedar integrado con el documento actual. Se recomienda entre otros tener en cuenta:

- Socialización y capacitación de temas de seguridad informática y de la información.
- Ambiente con la seguridad física adecuada.
- Sistemas de respaldo para mantener soporte de la información en caso de eventualidades catastróficas.

### **6.4 PLAN DE CAPACITACIÓN**

Contar con un plan de capacitación para el personal encargado de la seguridad de la información, aspectos a fortalecer como:

- 1) Detectar los requerimientos tecnológicos
- 2) Determinar objetivos de capacitación para personal
- 3) Evaluar los resultados de evaluaciones y monitoreo al sistema de seguridad.
- 4) Elaborar un programa de capacitación en temas de ciberseguridad y políticas de seguridad de la información para todos los funcionarios de la entidad.
- 5) Evaluar los resultados de cada actividad.

### **6.5 ESTABLECIMIENTO DE UN SGSI Y CERTIFICACIÓN EN LA NORMA ISO/IEC 27001 y 27017**

Dada la importancia en establecer y garantizar los procesos, procedimientos y gestiones de la seguridad de la información, la Contraloría Municipal de Neiva (CMN) debe certificarse en la Norma ISO/IEC 27001 eficaz que ayude a establecer un Sistema de Gestión de Seguridad de la Información eficiente, como ventaja competitiva frente a otras organizaciones del mismo sector, ofrecer la oportunidad de optimizar las áreas, dentro de la organización, relacionadas con la información que más le importan a la alta dirección de la empresa.

Es importante reconocer que la norma ISO/IEC 27001 acoge un proceso que está enfocado en establecer, implementar, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información en la organización.

La norma ISO/IEC 27001 se encuentra alineada a otros Sistemas de Gestión, ayudando a la implementación y al correcto funcionamiento a la hora de integrarla con otras normas.

Las principales características de la norma ISO-27001 son:

- Armonía con otros estándares del Sistema de Gestión, como pueden ser ISO 9001, ISO 14001 e ISO 20000.
- Continúo proceso de mejora del propio Sistema de Gestión de Seguridad de la Información.
- Se establecen todos los requisitos para la documentación y los archivos.
- Se valoran los riesgos y los procedimientos de gestión que se utilizan en el modelo de PHVA (planificar, hacer, verificar y actuar) referenciados en el Plan Estratégico TI de la institución.

La norma ISO/IEC 27001 persigue un enfoque muy detallado hacia la Seguridad de la Información. Los activos necesitan proteger la información, ya sea en papel, en formato digital o los activos físicos, los funcionarios y contratistas deben tener los conocimientos necesarios.

Se deben abordar cuestiones como pueden ser el desarrollo de la competencia del personal hasta la protección contra el fraude informático.

La norma ISO27001 facilita la protección de la información, ya que:

- Asegura la confidencialidad, ya que la información se encuentra accesible solo a ciertas personas que están autorizadas.
- Protege la integridad de la precisión y la información en su totalidad, además de los métodos utilizados durante el tratamiento de la información.
- Garantiza la disponibilidad, ya que existen usuarios que tienen acceso a la información.

***¡Neiva Bajo Control, Compromiso de Todos!***

 <p><b>Contraloría Municipal de Neiva</b> <i>Neiva Bajo Control Compromiso de Todos!</i></p>	<p style="text-align: center;"><b>FORMATO</b></p>
---	---

Para poder obtener la certificación, por parte de un organismo certificador, lo primero que debemos tener es implementado un Sistema de Gestión de Seguridad de la Información de una forma efectiva y que cumplan con todos los requisitos que establece la norma ISO/IEC 27001.

*¡Neiva Bajo Control, Compromiso de Todos!*



Contraloría  
Municipal  
de Neiva



Neiva Bajo Control  
Compromiso de Todos !

## FORMATO

## BIBLIOGRAFIA

RAMIREZ M, JE. ANÁLISIS, EVALUACIÓN DE RIESGOS Y ASESORAMIENTO DE LA SEGURIDAD INFORMÁTICA EN EL ÁREA DE REDES Y SISTEMAS DE LA ALCALDÍA DE PAMPLONA - NORTE DE SANTANDER <http://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/3415/1/88030934.pdf>..

MOLINA MIRANDA, MF. [http://www.dit.upm.es/~posgrado/doc/TFM/TFMs2014-2015/TFM\\_Maria\\_Fernanda\\_Molina\\_Miranda\\_2015.pdf](http://www.dit.upm.es/~posgrado/doc/TFM/TFMs2014-2015/TFM_Maria_Fernanda_Molina_Miranda_2015.pdf)

GUIA DE GESTION DE RIESGOS. MINISTERIO. SEGURIDAD Y PRIVACIDAD DE LA INFORMACION. MINISTERIO DE LAS TIC. <http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html>

SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN. Blog especializado. <https://www.pmg-ssi.com/2015/05/por-que-implantar-un-sgsi-basado-en-la-norma-iso-27001/>

PLATAFORMA TECNOLÓGICA PARA LA GESTIÓN DE LA EXCELENCIA. Sistemas de Gestión. <https://www.isotools.org/>

*¡Neiva Bajo Control, Compromiso de Todos!*

## **CONCLUSIONES**

El seguimiento constante a los procesos y la implementación del plan de mitigación de riesgo de seguridad de la información deben ser ejecutados, monitoreados y actualizados frecuentemente.

Es indispensable implementar el plan de gestión de riesgo que permitirá prevenir las posibles amenazas encontradas en la infraestructura tecnológica de la entidad.

Las políticas de seguridad de la información de la Contraloría Municipal de Neiva (CMN) deben ser revisadas y actualizadas conforme al crecimiento, cambios de la estructura organizacional, exigencias del gobierno y los mismos procesos dentro de la entidad.

Lograr establecer un Sistema de Gestión de Seguridad de la Información (SGSI) permitirá a terceros y demás organismos del sector tener más confianza en los procesos misionales de la Contraloría Municipal de Neiva (CMN), así como también lograr la certificación respectiva en la Norma ISO/IEC 27001 y 270017.