


# **PLAN DE GESTION DEL RIESGO EN SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**

**ALCALDIA MUNICIPIO DE LOS PATIOS  
NORTE DE SANTANDER - COLOMBIA  
2017**



Proyecto: Ing. Blanca Gamboa


	<b>GESTION TIC</b>	<b>Código GT-D-02</b>
	<b>PLAN DE GESTION DEL RIESGO DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACION</b>	<b>Versión: 02</b>
	<b>DOCUMENTO</b>	<b>Aprobado: 10/11/17</b>

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

**SECRETARÍA DE LAS TIC**

**ALCALDIA DE LOS PATIOS**

**2017**


	<b>GESTION TIC</b>	<b>Código GT-D-02</b>
	<b>PLAN DE GESTION DEL RIESGO DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACION</b>	<b>Versión: 02</b>
	<b>DOCUMENTO</b>	<b>Aprobado: 10/11/17</b>

## 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 del negocio. Por este motivo, se ha visto la necesidad de desarrollar un análisis de riesgo de seguridad de la información aplicado en La Alcaldía Municipal de Los Patios. 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.

 <b>ALCALDÍA DE LOS PATIOS</b>	<b>GESTION TIC</b>	<b>Código GT-D-02</b>
	<b>PLAN DE GESTION DEL RIESGO DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACION</b>	<b>Versión: 02</b>
	<b>DOCUMENTO</b>	<b>Aprobado: 10/11/17</b>

## TABLA DE CONTENIDO

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

	<b>GESTION TIC</b>	<b>Código GT-D-02</b>
	<b>PLAN DE GESTION DEL RIESGO DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACION</b>	<b>Versión: 02</b>
	<b>DOCUMENTO</b>	<b>Aprobado: 10/11/17</b>

5.2 <a href="#">Matriz de vulnerabilidades y Mitigación del Riesgo</a> .....	17
6. <a href="#">Propuesta de Seguridad</a> .....	22
6.1 <a href="#">Plan seguro para el acopio de copias de seguridad</a> .....	24
6.2 <a href="#">Plan de continuidad del negocio</a> .....	25
6.3 <a href="#">Implementación de políticas</a> .....	26
6.4 <a href="#">Plan de capacitación</a> .....	27
6.5 <a href="#">Plan de transición de IPv4 a IPv6</a> .....	27

[Bibliografía](#)

[Conclusiones](#)



 <b>ALCALDÍA DE LOS PATIOS</b>	<b>GESTION TIC</b>	<b>Código GT-D-02</b>
	<b>PLAN DE GESTION DEL RIESGO DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACION</b>	<b>Versión: 02</b>
	<b>DOCUMENTO</b>	<b>Aprobado: 10/11/17</b>

TABLA DE ILUSTRACIONES

Pág

Figura 1. Proceso para la Administración del Riesgo.....10

Figura 2. Matriz de vulnerabilidades y Mitigación de Riesgo.....19

	<b>GESTION TIC</b>	<b>Código GT-D-02</b>
	<b>PLAN DE GESTION DEL RIESGO DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACION</b>	<b>Versión: 02</b>
	<b>DOCUMENTO</b>	<b>Aprobado: 10/11/17</b>


## 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 alcaldía Municipal de Los Patios.

### 1.2 Objetivos Específicos

- Plantear modelos de reportes para su posterior uso en cada incidencia presentada en la alcaldía municipal.
- 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 alcaldía.
- Identificar las principales amenazas que afectan a los activos.
- Proponer soluciones para minimizar los riesgos a los que está expuesto cada activo.

	<b>GESTION TIC</b>	<b>Código GT-D-02</b>
	<b>PLAN DE GESTION DEL RIESGO DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACION</b>	<b>Versión: 02</b>
	<b>DOCUMENTO</b>	<b>Aprobado: 10/11/17</b>

- 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


### 2.1 ALCANCES

- Lograr el compromiso de la Alcaldía Municipal 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 Alcaldía Municipal de Los Patios.



	<b>GESTION TIC</b>	<b>Código GT-D-02</b>
	<b>PLAN DE GESTION DEL RIESGO DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACION</b>	<b>Versión: 02</b>
	<b>DOCUMENTO</b>	<b>Aprobado: 10/11/17</b>


### 3. 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 alcaldía Municipal de Los Patios, 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 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.

	<b>GESTION TIC</b>	<b>Código GT-D-02</b>
	<b>PLAN DE GESTION DEL RIESGO DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACION</b>	<b>Versión: 02</b>
	<b>DOCUMENTO</b>	<b>Aprobado: 10/11/17</b>

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 del negocio tras sufrir alguna pérdida o daño en la información de la entidad.

Considerando la situación actual de la alcaldía Municipal de Los Patios, 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.

	<b>GESTION TIC</b>	<b>Código GT-D-02</b>
	<b>PLAN DE GESTION DEL RIESGO DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACION</b>	<b>Versión: 02</b>
	<b>DOCUMENTO</b>	<b>Aprobado: 10/11/17</b>


### 3.2 DEFINICION GESTIÓN DEL RIESGO

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.

	<b>GESTION TIC</b>	<b>Código GT-D-02</b>
	<b>PLAN DE GESTION DEL RIESGO DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACION</b>	<b>Versión: 02</b>
	<b>DOCUMENTO</b>	<b>Aprobado: 10/11/17</b>

### 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 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.

	<b>GESTION TIC</b>	<b>Código GT-D-02</b>
	<b>PLAN DE GESTION DEL RIESGO DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACION</b>	<b>Versión: 02</b>
	<b>DOCUMENTO</b>	<b>Aprobado: 10/11/17</b>

### 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.

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 Alcaldía municipal de Los Patios no tenía un área de sistemas conformada y se evidenció que no existen procesos asignados a dicha área entre otras vulnerabilidades que se

	<b>GESTION TIC</b>	<b>Código GT-D-02</b>
	<b>PLAN DE GESTION DEL RIESGO DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACION</b>	<b>Versión: 02</b>
	<b>DOCUMENTO</b>	<b>Aprobado: 10/11/17</b>

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 alcaldías y entidades públicas en el país. Es por ello necesario que la alcaldía municipal de Los Patios cumpla con los requisitos necesarios para entregar la información de manera oportuna y eficiente a estas entidades, a la población y a la misma alcaldía.

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

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

Conformidad legal y evidencias de la debida diligencia.

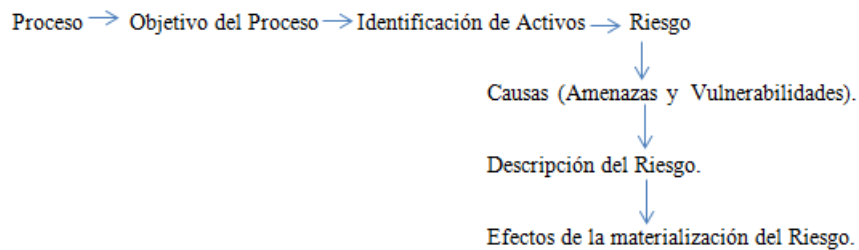
 <b>ALCALDÍA DE LOS PATIOS</b>	<b>GESTION TIC</b>	<b>Código GT-D-02</b>
	<b>PLAN DE GESTION DEL RIESGO DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACION</b>	<b>Versión: 02</b>
	<b>DOCUMENTO</b>	<b>Aprobado: 10/11/17</b>


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



	<b>GESTION TIC</b>	<b>Código GT-D-02</b>
	<b>PLAN DE GESTION DEL RIESGO DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACION</b>	<b>Versión: 02</b>
	<b>DOCUMENTO</b>	<b>Aprobado: 10/11/17</b>


## 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 Alcaldía de los Patios se encontraron otras amenazas e impactos como los siguientes:

1. La red de internet implementada no es la más adecuada teniendo en cuenta que la mayor parte de la alcaldía tiene conexión WiFi y la señal se torna débil o no llega a algunas oficinas. Debido a que la infraestructura física es amplia, compleja y la señal debe atravesar paredes. El internet lento y la pérdida de señal afecta de forma directa los tiempos de producción laboral y desempeño de las funciones.
2. Los puntos de red ubicados en cada oficina no son suficientes y se han dispuesto nuevos según se va presentando la necesidad. No existe una estructura o protocolo fijo y establecido para la infraestructura física de la Alcaldía.




	<b>GESTION TIC</b>	<b>Código GT-D-02</b>
	<b>PLAN DE GESTION DEL RIESGO DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACION</b>	<b>Versión: 02</b>
	<b>DOCUMENTO</b>	<b>Aprobado: 10/11/17</b>


3. Algunos cables de energía están sueltos, 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.
  
4. 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.
  
  - En algunas secretarías de la alcaldía no existen los equipos de cómputo suficientes para el uso de la totalidad de su personal. Existe un riesgo de pérdida de información ya que deben compartir los recursos informáticos.

	<b>GESTION TIC</b>	<b>Código GT-D-02</b>
	<b>PLAN DE GESTION DEL RIESGO DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACION</b>	<b>Versión: 02</b>
	<b>DOCUMENTO</b>	<b>Aprobado: 10/11/17</b>

- El Datacenter de la entidad requiere de algunas características importantes para cumplir con las normas de funcionamiento (alimentación eléctrica estabilizada e ininterrumpida, sistemas contra incendios, control de acceso, extintores, sistemas de cámaras de vigilancia, alarmas contra incendios, control de temperatura y humedad, piso falso entre otros).
- No existen cuentas de usuario y claves para el acceso de los recursos informáticos, en equipos compartidos.
- 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 Alcaldía, exponiendo a perder la información por virus no detectados o daños irreparables del hardware.
- Se identificó un completo desconocimiento del tema de seguridad y privacidad de la información en la alcaldía.

	<b>GESTION TIC</b>	<b>Código GT-D-02</b>
	<b>PLAN DE GESTION DEL RIESGO DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACION</b>	<b>Versión: 02</b>
	<b>DOCUMENTO</b>	<b>Aprobado: 10/11/17</b>


- No existe un Firewall para la red inalámbrica de la alcaldía, solo existe uno dedicado para los servidores de las Secretarías de Hacienda y el Banco.
  
- El sistema ofimático Microsoft Office que se utiliza en la alcaldía no cuenta con licencia de funcionamiento. Actualmente en todos los equipos de la entidad está instalado Office 2010 no tiene licencia de uso en este caso la entidad está incumpliendo la Ley 603 de 2000.
  
- 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 Alcaldía.
  
- 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.

	<b>GESTION TIC</b>	<b>Código GT-D-02</b>
	<b>PLAN DE GESTION DEL RIESGO DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACION</b>	<b>Versión: 02</b>
	<b>DOCUMENTO</b>	<b>Aprobado: 10/11/17</b>

- No existen procesos de copias de seguridad establecidos. Las copias de seguridad se están realizando únicamente en las secretarías y/o equipos donde se manejan software o sistemas de Información con un servidor dedicado a dicho propósito.


Ésta solución no es óptima, ya que existe riesgo de pérdida total de información en caso de ocurrir desastres naturales, incendios u otros que afecten las copias de respaldo almacenadas en el Datacenter ubicado dentro de la misma entidad.

- No existe un plan de continuidad de negocio que permita reanudar las operaciones normales durante o después de interrupciones significativas a las operaciones de la alcaldía. (en caso de incendio o desastre natural existen altas probabilidades de perder la información de los servidores)
- No se cuentan con los tipos de extintores adecuados para cada emergencia.
- La alcaldía cuenta con una planta de energía que en la actualidad no está funcionando, se han presentado cortes de energía suspendiendo los procesos laborales de todas las oficinas.

	<b>GESTION TIC</b>	<b>Código GT-D-02</b>
	<b>PLAN DE GESTION DEL RIESGO DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACION</b>	<b>Versión: 02</b>
	<b>DOCUMENTO</b>	<b>Aprobado: 10/11/17</b>


## 5.2 MATRIZ DE VULNERABILIDADES Y MITIGACION DEL RIESGO

VULNERABILIDAD	DESCRIPCIÓN	CAUSA	EFECTO	CLASIFICACION	ANALISIS		VALORACION	VIGENCIA DE CUMPLIMIENTO
					CALIFICACION	EVALUACION	MITIGACION DEL RIESGO	
*Fallas eléctricas	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 2018
*Afectación de activos de información y activos informáticos.	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 la alcaldía municipal.	Vigencia 2018
*Pérdida de información  *Pérdida de tiempo productivo en funciones laborales.	La red implementada no es la más adecuada para la estructura física de la alcaldía y la cantidad de equipos informáticos. 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  *Riesgo de información	40	Riesgo Importante	Implantar un modelo de red basado en cableado estructurado.	Vigencia 2018

 <b>ALCALDÍA DE LOS PATIOS</b>	<b>GESTION TIC</b>	<b>Código GT-D-02</b>
	<b>PLAN DE GESTION DEL RIESGO DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACION</b>	<b>Versión: 02</b>
	<b>DOCUMENTO</b>	<b>Aprobado: 10/11/17</b>


VULNERABILIDAD	DESCRIPCION	CAUSA	EFECTO	CLASIFICACION	ANALISIS		VALORACION	VIGENCIA DE CUMPLIMIENTO
					CALIFICACION	EVALUACION	MITIGACION DEL RIESGO	
<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 alcaldía municipal para el cumplimiento de procesos y actividades de seguridad de la información	Vigencia 2018
<b>Confidencialidad e Integridad de la información</b>	En la entidad se trabaja en la campaña cero papel, 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 2018
<b>Perdida total de Información</b>	No se cuentan con los tipos de extintores adecuados para cada necesidad.	No se cuentan con los tipos de extintores adecuados para cada necesidad.	*No hay extintores *La planta de energía no funciona	*Riesgo de información. *Riesgo de servicio. *Riesgo tecnológico	60	Riesgo Alto	Adquirir los extintores necesarios. Revisar el funcionamiento y puesta en marcha de la planta de energía	Vigencia 2018

Tabla 1. MATRIZ DE VULNERABILIDADES Y MITIGACION DE RIESGOS

 <b>ALCALDÍA DE LOS PATIOS</b>	<b>GESTION TIC</b>	<b>Código GT-D-02</b>
	<b>PLAN DE GESTION DEL RIESGO DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACION</b>	<b>Versión: 02</b>
	<b>DOCUMENTO</b>	<b>Aprobado: 10/11/17</b>

VULNERABILIDAD	DESCRIPCION	CAUSA	EFECTO	CLASIFICACION	ANALISIS		VALORACION	VIGENCIA DE CUMPLIMIENTO
					CALIFICACION	EVALUACION	MITIGACION DEL RIESGO	
*Pérdida de Información	Los funcionarios no realizan copias de seguridad a la información producto de sus funciones.	No hacen copias de seguridad	Posible pérdida de información	*Riesgo de Información * Riesgo en Servicio	40	Riesgo Importante	*Crear un instructivo de copias de seguridad *Capacitar al personal de la alcaldía municipal para el dominio de este tema. *Adquirir un servidor para almacenar las copias de seguridad. *Adquisición de una nube para almacenamiento de información. *Crear cuentas de usuario con claves.	Vigencia 2018
	Equipos compartidos en algunas secretarías	No existen cuentas de usuario.						Vigencia 2018
*Pérdida de Información	Uso de memorias extraíbles y unidades extraíbles	No hay control de uso	Infección por Virus	*Riesgo Tecnológico				Vigencia 2018
*Perdida de información	El DataCenter no cuenta con todas las especificación exigidas para el correcto funcionamiento y adecuación de un área de tal importancia.	Incendios, ingreso de personal no autorizado, posible robo de servidores,	Perdida de información por catástrofe o riesgo en manos	*Riesgo en Servicio *Riesgo en información	40	Riesgo Moderado	Adecuación del Datacenter de la alcaldía Municipal, cumpliendo con las características exigidas por normas y estándares en Colombia. (Piso falso, cámara de seguridad, extintores adecuados, entre otros)	Vigencia 2018
*Pérdida de información y/o deterioro físico	La documentación e información en papel o	No se ha iniciado la ejecución de	Daño de documentos y	*Riesgo de Información	40	Riesgo Importante	Iniciar la ejecución de la digitalización y	Vigencia 2018




 <b>ALCALDÍA DE LOS PATIOS</b>	<b>GESTION TIC</b>	<b>Código GT-D-02</b>
	<b>PLAN DE GESTION DEL RIESGO DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACION</b>	<b>Versión: 02</b>
	<b>DOCUMENTO</b>	<b>Aprobado: 10/11/17</b>

	física está siendo archivada en sitios no adecuados para ello.	digitalización de información.	deterioro del papel.				almacenamiento de la información contenida en papel.	
<b>No hay respaldo de información en sistemas de información</b>	No existe un proceso establecido de copias de seguridad dentro y fuera de la entidad para la información generada en los sistemas de información.  No Existe un sistema de información para la documentación sensible, como contratos y acuerdos.	No hay procesos de copias de seguridad establecidos	Perdida de información	*Riesgo Tecnológico  *Riesgo de información	60	Riesgo Importante	*Crear procesos de copias de seguridad. *Invertir en un software o sistema de información para el almacenamiento y consulta de la documentación física existente en la alcaldía.	Vigencia 2018
<b>Transición IPv4 a IPv6</b>	No existen transición de protocolo de IP	No existen transición de protocolo de IP	No existen transición de protocolo de IP	*Riesgo tecnológico	20	Riesgo Bajo	*establecer normas para la transición de IPv4 a IPv6 debido a que todos los equipos informáticos de la entidad soportan la nueva versión de IP	Vigencia 2018

## 6. PROPUESTA DE SEGURIDAD

- Se debe cambiar la red inalámbrica actual por cableado estructurado, para minimizar el problema de internet lento y caídas de señal.
- Implementar un firewall para la red que se utiliza en la alcaldía. El que se encuentra en uso está asignado para los servidores del banco y la secretaría de Hacienda.
- Revisar, organizar y ubicar las conexiones de electricidad según las necesidades propias de las oficinas.
- Replantear las políticas de seguridad y privacidad de la información como también las políticas de seguridad informática.
- 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 alcaldía.
- Creación de cuentas de usuario y claves para tratar de mitigar los riesgos de pérdida de información en manos de otro funcionario que use el equipo compartido.
- El personal de sistemas puede crear las cuentas y claves, socializando al personal de la alcaldía la creación de claves en forma correcta.
- Crear un rubro del presupuesto para la adquisición de la licencia del sistema ofimático Office para los equipos de la Alcaldía.
- En caso de usar Libreoffice se debe capacitar al personal en el manejo del sistema ofimático
- 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 Alcaldía 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 alcaldía para reducir riesgos de pérdida de información física.
- La alcaldía comprometida con la campaña cero papel, está próxima en habilitar el software para digitalización de documentos y gestión documental en los próximos meses.

 <b>ALCALDÍA DE LOS PATIOS</b>	<b>GESTION TIC</b>	<b>Código GT-D-02</b>
	<b>PLAN DE GESTION DEL RIESGO DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACION</b>	<b>Versión: 02</b>
	<b>DOCUMENTO</b>	<b>Aprobado: 10/11/17</b>


## 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 secretarías.
- Obtener una nube dedicada para la información de la alcaldía con el fin de tener un respaldo en caso de accidentes en los servidores del Datacenter.
- Contar con un plan alternativo que asegure la continuidad de la actividad del negocio en caso que ocurran incidentes graves.

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 DEL NEGOCIO

- 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.

 <b>ALCALDÍA DE LOS PATIOS</b>	<b>GESTION TIC</b>	<b>Código GT-D-02</b>
	<b>PLAN DE GESTION DEL RIESGO DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACION</b>	<b>Versión: 02</b>
	<b>DOCUMENTO</b>	<b>Aprobado: 10/11/17</b>

- Socializar con los directivos, secretaría general y oficina de las TIC la importancia del Plan de Continuidad de Negocio, 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, 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 en el negocio 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 alcaldía
- 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 permitió identificar que se desconocen y poco se cumplen las políticas de seguridad; por lo cual debe quedar integrado con el documento actual. Se recomienda entre otros tener en cuenta:

- Socialización y capacitación de temas de seguridad.
- Ambiente con la seguridad física adecuada.

 <b>ALCALDÍA DE LOS PATIOS</b>	<b>GESTION TIC</b>	<b>Código GT-D-02</b>
	<b>PLAN DE GESTION DEL RIESGO DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACION</b>	<b>Versión: 02</b>
	<b>DOCUMENTO</b>	<b>Aprobado: 10/11/17</b>

- 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.

#### 6.6 PLAN DE TRANSICIÓN DE IPV4 A IPV6

Se debe establecer un plan para hacer la transición de las direcciones IPv4 existente actualmente por la IPv6 debido a que los equipos informáticos de la alcaldía de Los Patios soportan la nueva versión de IP.


 <b>ALCALDÍA DE LOS PATIOS</b>	<b>GESTION TIC</b>	<b>Código GT-D-02</b>
	<b>PLAN DE GESTION DEL RIESGO DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACION</b>	<b>Versión: 02</b>
	<b>DOCUMENTO</b>	<b>Aprobado: 10/11/17</b>

## 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>

	<b>GESTION TIC</b>	<b>Código GT-D-02</b>
	<b>PLAN DE GESTION DEL RIESGO DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACION</b>	<b>Versión: 02</b>
	<b>DOCUMENTO</b>	<b>Aprobado: 10/11/17</b>

## 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 Alcaldía Municipal de Los Patios deben ser revisadas y actualizadas conforme al crecimiento, cambios de la estructura organizacional, exigencias del gobierno y los mismos procesos dentro de la entidad.