PLAN DE TRATAMIENTO DEL RIESGO EN

SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

ALCALDIA MUNICIPAL DE SOPÓ

CUNDINAMARCA - COLOMBIA

2020

PLAN DE TRATAMIENTO DEL RIESGO EN SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Miguel Alejandro Rico Suarez
Alcalde Municipal

Segundo Hipólito Sanabria Alarcón
Secretaria de Desarrollo Institucional

Diego Fabián León Beltrán
Profesional Universitario Área de Sistemas de Información

Juan Carlos Rodríguez Camargo
Contratista

Sopó, Junio de 2020

INTRODUCCION

El riesgo en una de sus definiciones es la posibilidad de sufrir daños o pérdidas.

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 tratamiento 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 Sopó. Antes de iniciar con este plan de tratamiento 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 tratamiento 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.

Tabla de contenido

1. OBJETIVOS

1.1 OBJETIVO GENERAL

Desarrollar un plan de tratamiento de seguridad y privacidad que permita minimizar los riesgos de pérdida de activos de la información en la alcaldía Municipal de Sopó.

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 tratamiento 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.
- Evaluar y comparar el nivel de riesgo actual con el impacto generado después de implementar el plan de tratamiento 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 tratamiento 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 tratamiento.
- Capacitar al personal de la entidad en el proceso de plan de tratamiento del riesgo de la seguridad de la información.

2.2 LIMITACIONES

- Crear el rubro del presupuesto necesario para apoyar la implementación del plan de tratamiento del riesgo de la seguridad de la información en la Alcaldía Municipal de Sopó, o realizar la ampliación de los rubros direccionados a la Secretaría de Desarrollo Institucional, que es la tiene bajo su cobertura al Área de Sistemas de Información.

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 Sopó, 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 tratamiento de riesgos está expuesta a perder su información.

Todas las organizaciones deben 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 Sopó, 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

La definición estandarizada de riesgo proviene de la Organización Internacional de Normalización (ISO) en su Norma ISO 31000 de la siguiente manera:

a. **Riesgo:** Efecto de la incertidumbre sobre los objetos.
    - Un efecto es una desviación de aquello que se espera, sea positivo, negativo o ambos.
    - Los objetivos pueden tener aspectos diferentes y se pueden aplicar en niveles diferentes.
    - El riesgo está caracterizado por la referencia a los eventos potenciales y a las consecuencias o a una combinación de estos.
    - El riesgo se expresa en términos de una combinación de las consecuencias de un evento y en la probabilidad de que suceda.
    - Incertidumbre es el estado, incluso parcial, de deficiencia de información relacionada con la comprensión o el conocimiento de un evento, su consecuencia o probabilidad.

b. **Gestión del Riesgo:** Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

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

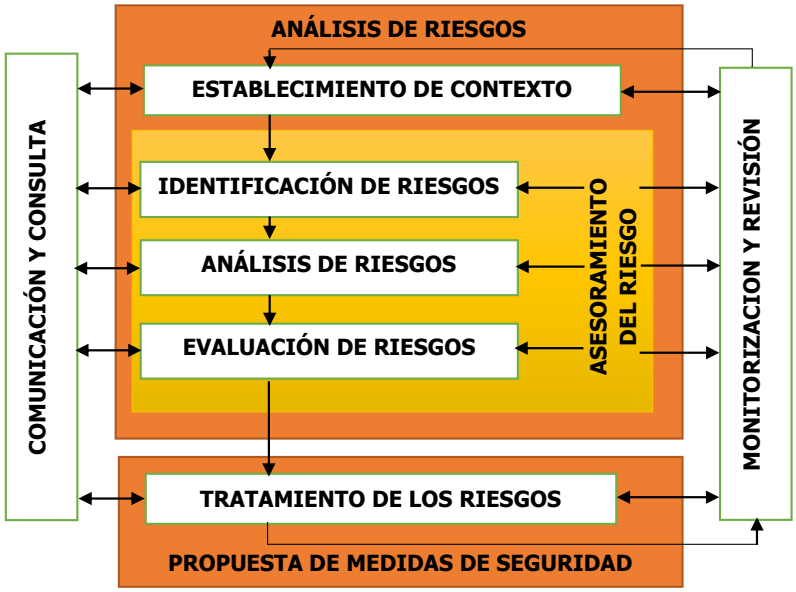

Figura 1. Proceso para la Administración del Riesgo

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 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.
- 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

La Alcaldía municipal de Sopó tiene un área de sistemas conformada, y esta a su vez evidenció que existen vulnerabilidades que se encontraron en el sistema actual, se hace necesario crear un plan de tratamiento de riesgos de seguridad de la información que permita proteger el activo más valioso para la entidad; la información.

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 Sopó 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.
- 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

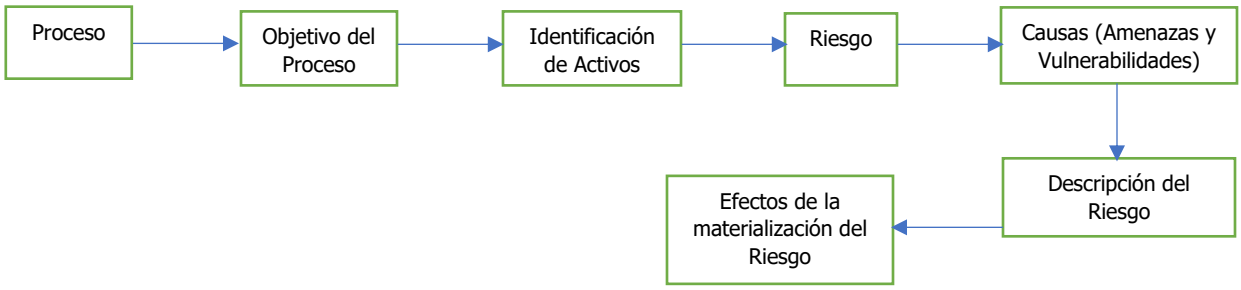

Figura 2. Matriz de vulnerabilidades y Mitigación de Riesgo

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

1. 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.

2. 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.

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, aunque este ítem se ha socializado a través del correo electrónico no está definido a través de las políticas o no se ha socializado a todo el personal de la Alcaldía.

- En algunos papeles reutilizables se encontró información personal que debe ser reservada, identificándose la falta de confidencialidad y privacidad.

- Las dependencias cuentan con la cantidad total de equipos para sus funcionarios, pero varios de ellos se encuentran aún en Windows XP SP3, y como sabemos, Microsoft

retiró toda actualización y soporte para este sistema operativo desde 2014, lo cual representa una vulnerabilidad e inestabilidad del SO en cuanto seguridad e información. Ahora, muchos de esos equipos no permiten la instalación del SO Windows 10, ya que sus placas de procesamiento son muy antiguas y no cuentan con la memoria de procesamiento suficiente.

- El Datacenter de la entidad requiere de algunas características importantes para cumplir con las normas de funcionamiento (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.

- No existe un Firewall para la red interna de la alcaldía

- El sistema ofimático Microsoft Office que se utiliza en la alcaldía cuenta algunas licencias de funcionamiento. Actualmente en todos los equipos de la entidad está instalado Office, desde 2003 hasta 2016, pero algunas de estas licencias no se encuentran activadas, y así como mencionábamos en un ítem anterior, Office desde la versión 2013 ya no es compatible con Windows XP SP3, lo cual también nos genera problemas de actualización de formatos, archivos y modos de compatibilidad de la información de los usuarios de la Alcaldía Municipal.

- Los documentos físicos que se manejan en la entidad se encuentran en proceso de digitalización, pero el proceso ha sido complejo debido a la cantidad de información por digitalizar, así como la que aún no se ha radicado ni entregado al Archivo Municipal.

- La alcaldía cuenta con una planta de energía que en la actualidad no se encuentra funcionando adecuadamente, ya que ha tenido fallas a la hora de realizar el suministro a la infraestructura de la Alcaldía Municipal, ocasionando pérdidas de trabajo en algunas ocasiones, de manera considerable.

5.2 MATRIZ DE VULNERABILIDADES Y MITIGACION DEL RIESGO					ANALISIS		VALORACION	VIGENCIA
VULNERABILIDAD	DESCRIPCIÓN	CAUSA	EFECTO	CLASIFICACION	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	60	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
Incumplimiento de las actividades de seguridad de la información.	El personal encargado de los sistemas no son 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

Confidencialidad e Integridad de la información	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 2018
*Pérdida de Información *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

*Pérdida de Información *Pérdida de Información *Perdida de información	Equipos compartidos en algunas secretarías Uso de memorias extraíbles y unidades extraíbles El DataCenter no cuenta con todas las especificaciones exigidas para el correcto funcionamiento y adecuación de un área de tal importancia.	No existen cuentas de usuario. No hay control de uso. Incendios, ingreso de personal no autorizado, posible robo de servidores,	Posible pérdida de información Infección por Virus. Perdida de información por catástrofe o riesgo en manos	*Riesgo de Información * Riesgo en Servicio *Riesgo Tecnológico. *Riesgo en Servicio *Riesgo en información	40	Riesgo Importante Riesgo Moderado	*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. *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 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	Vigencia 2018
Transición IPv4 a IPv6	No existe transición de protocolo de IP	No existe 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

- Implementar un firewall para la red que se utiliza en la alcaldía.
- 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.
- Ampliar el rubro del presupuesto para la adquisición de equipos de cómputo y así renovar los que se encuentran actualmente en la Alcaldía.
- Realizar un proceso de mejora continua del sistema de documentación digital en la alcaldía para reducir riesgos de pérdida de información física.
- La alcaldía se debe comprometer con la campaña cero papeles, buscando la manera de firmar la documentación con su respectivo certificado de seguridad.

6.1 PLAN SEGURO PARA EL ACOPIO DE COPIAS DE SEGURIDAD

- 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

- Socializar con los directivos, secretaría general y área de Sistemas de información 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.

• 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 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 Sopó soportan la nueva versión de IP.

Las recomendaciones que se deben tener en cuenta para esta transición son:

1) Realizar una topografía de red para comprobar que el cableado y conexiones estructuradas funcionen en su totalidad sin intermitencias.
2) Verificar que los equipos acepten el protocolo IPV6, esto a través de un inventario con sus respectivas características físicas y tecnológicas.
3) Realizar la gestión de la implementación del protocolo en los diferentes puntos, tanto internos como externos de la Alcaldía Municipal.

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

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

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 tratamiento 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 Sopó deben ser revisadas y actualizadas conforme al crecimiento, cambios de la estructura organizacional, exigencias del gobierno y los mismos procesos dentro de la entidad.