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

CALARCÁ QUINDÍO

2018

Contenido

1. OBJETIVOS

1.1 Objetivo General

Crear un plan para el tratamiento de riesgos de la seguridad y privacidad de la información que minimice los peligros que día a día nos enfrentamos en la era digital.

1.2 Objetivos Específicos

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Mantener la confianza de sus usuarios y servidores públicos.
- Apoyar la innovación tecnológica.
- Implementar el Plan de Copias de seguridad de la información.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los servidores públicos, practicantes y usuarios de la administración municipal.
- Garantizar la continuidad de los procesos de la administración frente a incidentes de la plataforma tecnológica

2. ALCANCES Y LIMITACIONES

2.1 ALCANCES

- Esta política aplica a toda la entidad, sus funcionarios, contratistas y terceros de la alcaldía municipal de Calarcá, así como a la ciudadanía.
- Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento un 100% de la política.

2.2 LIMITACIONES

Falta de presupuesto municipal para desarrollar todos los parámetros dictados por el MINTIC en lo relacionado con la seguridad y privacidad de la información ya que hay situaciones en las que se requiere de presupuesto para cumplirlas.

3. GESTIÓN DE RIESGOS

3.1 IMPORTANCIA DE LA GESTIÓN DE RIESGOS

La Alcaldía Municipal de Calarcá sigue los lineamientos trazados por el Gobierno Nacional en cumplimiento de la Ley de Transparencia 1712 de 2014 y Mi Colombia Digital 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 actos originados por criminalidad común, por sucesos de origen físico y por negligencia de usuarios y decisiones institucionales son los riesgos más relevantes que se identificaron en la Alcaldía de Calarcá. Una entidad sin un plan de gestión de riesgos está expuesta a perder su información y sus bienes informáticos.

Considerando los riesgos actuales de la Alcaldía de Calarcá anteriormente nombrados se pretende diseñar un plan que mitigue todos estos riesgos y sean subsanados para además entrar a prevenir en vez de corregir.

3.2 DEFINICION GESTIÓN DEL RIESGO

Los riesgos en la seguridad de la información de la Administración Municipal se pueden clasificar en tres grupos: Actos originados por la criminalidad común, Riesgos por sucesos de origen físico y riesgos por sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales

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

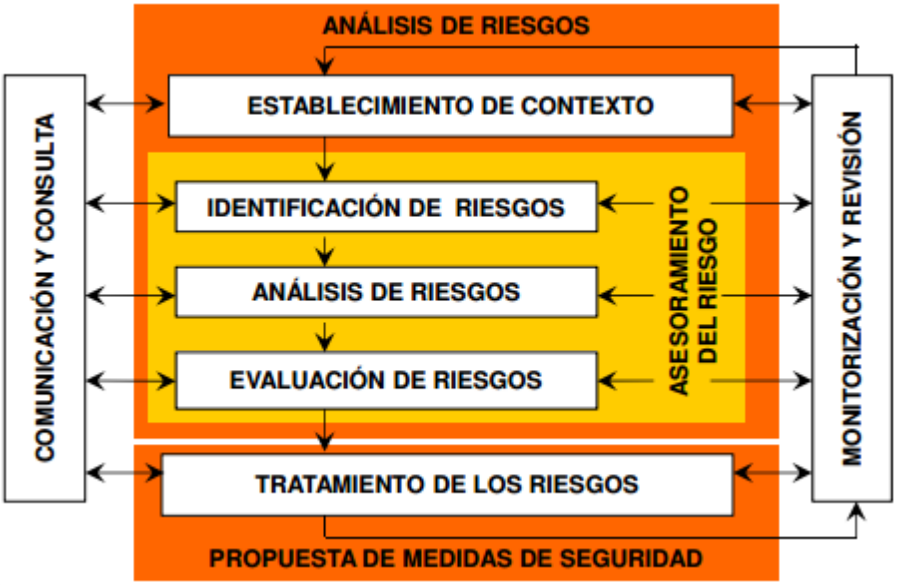


Figura 1 Proceso para la administración del riesgo.

3.4 IDENTIFICACIÓN DEL RIESGO

- Actos originados por la criminalidad común:
- Sabotaje (ataque físico y electrónico)
- Daños por vandalismo
- Fraude / Estafa
- Robo / Hurto (físico)

- Robo / Hurto de información electrónica
- Virus / Ejecución no autorizado de programas
- Violación a derechos de autor
- Riesgos por sucesos de origen físico:
- Incendio
- Inundación
- Sismo
- Polvo
- Falta de ventilación
- Sobrecarga eléctrica
- Falla de corriente (apagones)
- Falla de sistema / Daño disco duro

- Negligencia de usuarios/as y decisiones institucionales:
- Falta de inducción, capacitación y sensibilización sobre riesgos
- Mal manejo de sistemas y herramientas
- Utilización de programas no autorizados / software ilegal
- Falta de pruebas de software nuevo con datos productivos
- Perdida de datos
- Infección de sistemas a través de unidades portables sin escaneo
- Manejo inadecuado de datos críticos (codificar, borrar, etc.)
- Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas)
- Compartir contraseñas o permisos a terceros no autorizados
- Transmisión de contraseñas por teléfono
- Acceso electrónico no autorizado a sistemas externos

4. ORIGEN DEL PLAN DE GESTION

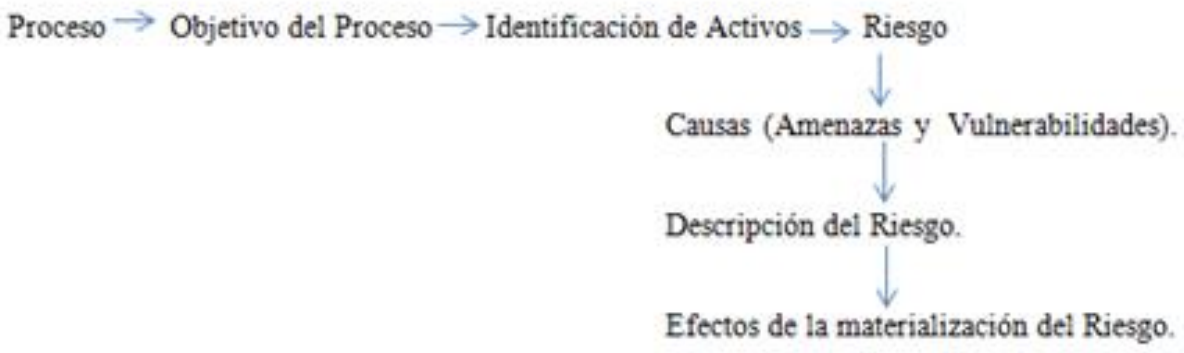
La Oficina Asesora TIC está a cargo del proceso y procedimiento de desarrollo tecnológico e informático estipulado dentro del manual de procesos y procedimientos de la entidad en gestión de calidad. También se tiene una gran ventaja ya que a finales del año 2017 fue creada como tal la Oficina Asesora TIC y teniendo como tal sus responsabilidad, actividades y demás que permiten prestarle la importancia que se merece, anteriormente solo era una función de la Secretaría de Asuntos administrativos.

El gobierno nacional y el ministerio de las TIC han abanderado el proyecto de Mi Colombia Digital que permite conocer el funcionamiento de las alcaldías y entidades públicas en el país. Por ello es necesario que la Alcaldía Municipal de Calarcá 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.

4.2 PROPÓSITO DEL PLAN DE GESTION DE RIESGO DE LA SEGURIDAD DE LA INFORMACIÓN.

- Dar cumplimiento al modelo de seguridad y privacidad de la información proporcionada desde el MINTIC.
- Responder ante incidentes presentados en la entidad relacionados con las TIC.
- Conocer los riesgos y problemas de la entidad respecto al modelo de seguridad y privacidad de la información para dar su oportuno acompañamiento.
- Alcanzar un alto conocimiento en la entidad y la ciudadanía sobre la importancia de todo lo relacionado a las TIC.

4.3 IDENTIFICACIÓN DEL RIESGO



5. ANALISIS DE VULNERABILIDADES

5.1 DESCRIPCIÓN DE VULNERABILIDADES

Aunque la seguridad y privacidad de la información se ve amenazada frecuentemente por errores cometidos por los usuarios o factores externos en la Alcaldía de Calarcá se encontraron otras amenazas e impactos como los siguientes:

- El sistema eléctrico de la Alcaldía de Calarcá no se encuentra en su totalidad con polo a tierra lo que salvaguarda la salud de los equipos de cómputo. Asimismo estamos expuestos a la perdida de información por idas de energía o desconexión de los equipos accidentalmente debido a la falta de UPS.

- Los funcionarios hacen uso de bebidas y comidas en muchos casos que afectan la salud de los equipos de cómputo.

- El papel reutilizable de las dependencias a veces se encuentran información personal que debe ser reservada, identificándose la falta de confidencialidad y privacidad.

.

- La información muchas veces sale de la entidad ya que es transportada por medio de memorias USB y discos externos personales.

- No existe un control para el uso de memorias USB personales por ende no

se conoce el origen ni el destino de la información y conlleva a tener siempre un riesgo de daño o infección por virus.

- Los documentos físicos que se manejan en la entidad en su mayoría no están digitalizados lo que genera un riesgo constante de perdida de la información.

- A pesar de que se realizan copias de seguridad en disco externos pertenecientes a la Oficina Asesora TIC no son suficientes para toda la información de la Alcaldía.

- En caso de ocurrir desastres naturales, incendios u otros pueden ser afectadas las copias de seguridad almacenadas.

- La alcaldía de Calarcá no cuenta con planta de energía, es decir que cada que hay interrupciones de energía existen altas probabilidades de perdida de información en la que se estaba trabajando.

VULNERABILI	DESCRIPCIÓN	CAUSA	EFECTO	CLASIFICACION	CALIFI	EVALUACION	MITIGACION	**VIGENCIA DE CUMPL**
***Afectación de activos de información y activos informáticos.**	Inexistencia del documentos de activos de información.	La inexistencia de las tablas de retención documental debido a su actualizacioòn	El incumplimiento a la ley 1712 que pide este documento.	* Riesgo informatico y administrativo	80	Riesgo Alto	Crear el documento de activos de información en el momento que ya estén actualizadas las tablas de retención documental.	**Vigencia 2018**

***Pérdidade información** ***Pérdida de tiempo productivoen funciones laborales.**	No se cuenta con un software o un servidor potente para toda la salvaguardia de la información Fallas intermitentes en el servicio del prestador de internet	Falta de presupuesto para adquirir servidores o software Daños internos de la empresa que no dependen de nosotros.	Riesgo en la perdida de la informac ión. Lentitud o retraso en las actividad es diarias	*Ries g Tecn ológi co *Riesgoe n Servicio *Riesgod e informaci ón	80 20	Rie sgo alto Rie sgo baj o	Generar estrategias para tener a salvo la información hasta que haya presupuesto Tener paciencia y mandar sugerencias a la empresa	**Vigencia 2018**

							ANALISIS		**VALORACION**	**VIGENCIA DE CUMPL**
VULNERABILIDAD	DESCRIPCION		CAUSA	EFECTO	CLASIFICACION		CALIFICACI	EVALUACION	MITIGACI	
Confidencialidad Integridad de información		En la entidad se utiliza la campaña de cero papel sin embargo a veces se encuentra informa	Exposición de datos personales en papel reutilizable.	incumplimiento de confidencialidad e integridad de la información	*riesgo Información	de	60	Riesgo Alto	Dar a conocer a los funcionarios la importancia de la seguridad y la privacidad de la información en todo sentido..	**Vigencia 2018**

Perdida total Información		No se cuenta con infraestructura totalmente	No se cuentan con los suficientes extintores, alarmas de incendio entre otras.	En caso de un incendio se perdería toda la informaci	*Riesgo información.	de de	50	Riesgo probable	Reestructuración física de la planta de la alcaldía que tenga en cuenta	Vigencia 2018

VULNERABILIDAD	**DESCRIPCION**	**CAUSA**	**EFECTO**	**CLASIFICACION**	**ANALISIS**		**VALORACION**	**VIGENCIA DE CUMPLIM**
					CALIFICACION	EVALUACION	MITIGACION DEL	
*Pérdida de Información	Los funcionarios no tienen a	No hacen copias	Posible pérdida de	*Riesgo de	40	Riesgo Importante	*Capacitar al personal de la alcaldía municipal para el dominio de este tema. *Adquirir un servidor o	Vigencia 2018
	Uso de memorias extraíbles y unidades extraíbles	No hay control de uso	Infección por Virus	*Riesgo Tecnológico				Vigencia 2018

*Pérdida de información y/o deterioro físico	Los documentos no son digitalizados en su totalidad lo que hace que	Solo se digitalizan los documentos que se necesitan digital o para enviar de	Daño de documentos y perdida de la informacion	*Riesgo	40	Riesgo Importante	Dar a conocer la importancia de tener los documentos digitalizados para guardar la información.	Vigencia 2018
Transición IPv4 a IPv6	No existen transición de protocolo de IP	No existen transición de protocolo de IP	No existen transicion de protocolo de IP	*Riesgo tecnológico	20	Riesgo Bajo	Realizar estudio para la posible migración de protocolo.	Vigencia 2018

6. PROPUESTA DE SEGURIDAD

- Fortalecer y completar la infraestructura tecnológica para que cumpla con todos los estándares de calidad y supla las necesidades de la Administración Municipal.

- Adquirir UPS para salvaguardar la información sobre todo a los servidores que son los que manejan más información.

- Complementar la red eléctrica de la Alcaldía con su totalidad de tomas con polo a tierra que vela por la salud de los equipos de cómputo.

- Dar a conocer a los funcionarios de la Alcaldía de Calarcá los planes relacionados con la seguridad y privacidad de la información.

- Cambiar las contraseñas constantemente de los correos institucionales para la seguridad de la información y cuidar la no propagación de las contraseñas.

- Dar a conocer la importancia de la digitalización de los documentos para minimizar los riesgos de perdida de información.

7. PLAN SEGURO PARA EL ACOPIO DE COPIAS DE SEGURIDAD

- Adquirir un servidor con características aptas para almacenar todas las copias de seguridad de cada dependencia.

- Continuar con las copias de seguridad periódicas para salvaguardar la información más importante de la Administración Municipal.

- Trabajar de la mano con los funcionarios a cargo de la seguridad y salud en el trabajo para sopesar los riesgos ocasionados por la naturaleza ya que ellos tienen planes de contingencia establecidos para esos fenómenos.

- Concientizar a los funcionarios de la administración municipal sobre el uso de memorias USB y discos externos personales y su exposición alta a virus.

8. IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD PARA LA INFORMACIÓN

El análisis permite identificar que la Alcaldía de Calarcá va por buen camino en el tema de seguridad y privacidad de la información, se debe fortalecer la difusión y conocimiento con los funcionarios de las diferentes dependencias. Sin embargo se deja claro que la Oficina Asesora TIC siempre se encuentra en disposición para ayudar en la implementación de estos planes.

9. PLAN DE CAPACITACIÓN

La Oficina Asesora TIC cuenta su plan de capacitación en todo los planes relacionados con la seguridad y privacidad de la información, estas capacitaciones son brindadas por el personal de la Oficina Asesora TIC y también se encuentran adoptadas dentro del Plan Anticorrupción para su cumplimiento.

Con las capacitaciones brindadas al personal de la Alcaldía siempre se pretende conocer las falencias y los problemas que se tienen en base a la seguridad y privacidad de la información y ayudar para que no se presenten o aprendan a arreglarlos.

En la Oficina Asesora Tic reposan todas las evidencias fotográficas y de asistencia realizadas de las capacitaciones en este tema.

10. PLAN DE TRANSICIÓN DE IPV4 A IPV6

En la actualidad la Alcaldía de Calarcá no cuenta con el plan de transición de protocolo de IPv4 a IPv6 ya que implicaría una inversión presupuestal y de infraestructura tecnológica.

11. REFERENCIAS

•Ley 1450 de 2011, por el cual se expide el Plan Nacional de Desarrollo 2010-2014, en el artículo N° 55 sobre accesibilidad a servicios de TIC.

• Ley 1341 de 2009 Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones en el artículo 38 sobre Masificación del uso de las TIC y cierre de la brecha digital.

• Decreto 2693 de 2012, por el cual se establecen los lineamientos generales de la estrategia de Gobierno en línea de la República de Colombia, se reglamentan parcialmente las Leyes 1341 de 2009 y 1450 de 2011, y se dictan otras disposiciones.

• Capítulo IV referente a la Gestión de Documentos Electrónicos de Archivo del Decreto 2609 de 2012, por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.

• Ley 1273 de 2009, por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

• Ley 1581 de 2012, reglamentada parcialmente por el Decreto 1377 de 2013, por la cual se dictan disposiciones generales para la protección de datos personales.