

	ALCALDÍA MUNICIPAL DE ACACÍAS			 <div>Management System ISO 9001:2008 ISO 14001:2004 OHSAS 18001:2007 www.tuv.com ID: 9105085574</div> 
	PROCESO GESTIÓN TIC			
	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN			
	Fecha: 27/07/2018	Código: GTIC – PL – 01	Versión: 1	

1004

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

MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN










	ALCALDÍA MUNICIPAL DE ACACÍAS			 <div>Management System ISO 9001:2008 ISO 14001:2004 OHSAS 18001:2007 www.tuv.com ID: 9105085574</div> 
	PROCESO GESTIÓN TIC			
	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN			
	Fecha: 27/07/2018	Código: GTIC – PL – 01	Versión: 1	

TABLA DE CONTENIDO

1. OBJETIVO	3
2. ALCANCE Y RESPONSABILIDADES	3
3. NORMATIVIDAD	3
4. TERMINOS Y DEFINICIONES	4
6. VALORACION DE ACTIVOS	6
6.1 IDENTIFICACION DE AMENAZAS	7
6.2 VALORACION DE LAS AMENAZAS	9
6.3 IDENTIFICACIÓN DE VULNERABILIDADES	10
6.4 VALORACION DEL RIESGO	10
6.5 REVISION DE CONTROLES IMPLEMENTADOS	11
6.6 VALORACION DEL RIESGO RESIDUAL	11
6.7 ACEPTACION DEL RIESGO	11
6.8 REVISION DE LOS RIESGOS Y REEVALUACION	12
6.9 OPCIONES DE TRATAMIENTO	12
6.10 PLAN DE TRATAMIENTO DE RIESGOS	13



	ALCALDÍA MUNICIPAL DE ACACÍAS			  
	PROCESO GESTIÓN TIC			
	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN			
	Fecha: 27/07/2018	Código: GTIC – PL – 01	Versión: 1	

1. OBJETIVO

Establecer lineamientos en el análisis y valoración del riesgo de los activos de información, en cuanto a la seguridad de la información a través de una secuencia de actividades humanas que incluyen evaluación de riesgo, estrategias de desarrollo para manejarlo y mitigación del riesgo utilizando recursos gerenciales. Los lineamientos incluyen transferir el riesgo a otra parte, evadir el riesgo, reducir los efectos negativos del riesgo y aceptar algunas o todas las consecuencias de un riesgo particular.

2. ALCANCE Y RESPONSABILIDADES

Aplica a los activos de información de la Alcaldía Municipal de Acacias Meta todos los funcionarios y terceros que laboren o tengan relación con la entidad, que sean dueños de activos de información de la entidad, son responsables por el análisis y valoración de los riesgos asociados a estos.

3. NORMATIVIDAD





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: "Por la cual se dictan disposiciones generales para la protección de datos personales".

Ley 1712 de 2014: "Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones",

ISO 27001:2013: Sistemas De Gestión De Seguridad De La Información



	ALCALDÍA MUNICIPAL DE ACACÍAS			  
	PROCESO GESTIÓN TIC			
	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN			
	Fecha: 27/07/2018	Código: GTIC – PL – 01	Versión: 1	

4. TERMINOS Y DEFINICIONES

Aceptación del Riesgo: Decisión de aceptar un riesgo.

Activo de Información: todo lo que representa valor para la Entidad

Información: Son todos aquellos elementos básicos de la información (en cualquier formato) que se generan, recogen, gestionan, transmiten y destruyen en la Alcaldía Municipal de Acacias Ejemplo: archivo de Excel

Activos físicos: hace referencia a los activos fijos tales como equipos de cómputo, de comunicaciones, de soporte (impresoras, escáner y teléfono IP) y demás bienes muebles.

Aplicaciones: Es todo el software que se utiliza para la gestión de la información. Ejemplo: SYSMAN

Personal: Es todo el personal de la Alcaldía Municipal de Acacias, subcontratado, los clientes, usuarios y en general, todos aquellos que tengan acceso de una manera u otra a los activos de información de la Entidad.

Servicios: Son tanto los servicios internos, como los externos, aquellos que la organización suministra a personal interno, clientes y usuarios. Ejemplo: Certificado de Paz y Salvo del impuesto Predial




Administración del Riesgo: Actividades encaminadas a la intervención de los riesgos de la entidad, a través de la identificación, valoración, evaluación, manejo y monitoreo de los mismos de forma que se apoye el cumplimiento de los objetivos de la entidad.

Análisis de Riesgos: Determinación del impacto en función de la consecuencia o efecto y de la probabilidad de ocurrencia del riesgo.

Activos de Información: Es el elemento de información que cada entidad territorial recibe o produce en el ejercicio de sus funciones. Incluye la información que se encuentre presente en forma impresa, escrita en papel, transmitida por cualquier medio electrónico o almacenado en equipos de cómputo, incluyendo datos contenidos en registros, archivos, bases de datos, videos e imágenes.

Amenaza: Es un evento accidental o intencionado que puede causar un daño a un activo de información. Puede ser:



	ALCALDÍA MUNICIPAL DE ACACÍAS			 <div>Management System ISO 9001:2008 ISO 14001:2004 OHSAS 18001:2007 www.tuv.com ID: 9105085574</div> 
	PROCESO GESTIÓN TIC			
	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN			
	Fecha: 27/07/2018	Código: GTIC – PL – 01	Versión: 1	

Natural: Terremoto.

Agente externo: Virus o malware.

Agentes internos: Funcionario molesto

Consecuencias: Hechos o acontecimientos que se derivan o resultan de la ocurrencia o la materialización de un riesgo.

Corrupción: Uso del poder para desviar la gestión de lo público hacia el beneficio privado.

Causas: Medios, circunstancias, situaciones o agentes generadores del evento.

Control: Los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido.

Evento: Hecho que se genera durante la gestión de un proceso afectando el logro del objetivo del mismo, tiene relación directa con las actividades críticas de los planes operativos, las actividades de ruta crítica de los Proyectos de Inversión y las actividades críticas de control de los procesos.

Frecuencia: Periodicidad con que ha ocurrido un evento.

Gestor del Riesgo: Funcionario líder de la dependencia, quien apoya al responsable del riesgo.

Identificación del Riesgo: Descripción de la situación no deseada.

Impacto: consecuencias de la materialización de una amenaza.

Mapa de riesgos: Herramienta metodológica que permite hacer un inventario de los riesgos por proceso, haciendo la descripción de cada uno de ellos, las posibles consecuencias y su forma de tratamiento.





Políticas de manejo del Riesgo: Son los criterios que orientan la toma de decisiones para tratar, y en lo posible minimizar, los riesgos en la entidad, en función de su evaluación.

Probabilidad: Medida para estimar la posibilidad de que ocurra un evento.

Responsable del riesgo: Es el encargado de identificar, valorar y definir el plan de contingencia, el manejo y monitoreo para cada uno de los riesgos del proceso bajo su responsabilidad.

Riesgo: Es la probabilidad de que una amenaza se materialice sobre la vulnerabilidad de un activo.



	ALCALDÍA MUNICIPAL DE ACACÍAS			  
	PROCESO GESTIÓN TIC			
	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN			
	Fecha: 27/07/2018	Código: GTIC – PL – 01	Versión: 1	

Riesgo Residual: Nivel de riesgo que permanece luego de tomar medidas de tratamiento de riesgo.

Riesgo Inherente: Es el riesgo puro, al cual no se han aplicado controles, para controlarlo y buscar evitar su materialización.

Riesgo de corrupción: Posibilidad de que, por acción u omisión, se use el poder para poder desviar la gestión de lo público hacia un beneficio privado.

Riesgo de seguridad de la información: Posibilidad de que una amenaza concreta que pueda aprovechar una vulnerabilidad para causar una pérdida o daño en un activo de información; *estos daños consisten en la afectación de la confidencialidad, integridad o disponibilidad de la información.* Cuando la amenaza se convierta en una oportunidad se debe tener en cuenta en el beneficio que se genera.

También se puede generar riesgo positivo en la seguridad de la información por el aprovechamiento de oportunidades y fortalezas que se presenten.

Tratamiento: Opciones que determinan el tipo de acciones a implementar para administrar el riesgo.

Valoración: Grado de exposición al riesgo con la clasificación de probabilidad e impacto aplicando los controles existentes.

Vulnerabilidad: Debilidad de un activo que puede ser aprovechada por una amenaza para producir pérdidas o daños a la entidad.




6. VALORACION DE ACTIVOS

Se realiza la valoración de activos teniendo en cuenta su impacto, es decir cómo afecta la disponibilidad, integridad y confidencialidad si se produce una falla o pérdida del activo. Consultar matriz de riesgo.

Cada activo se valora de acuerdo a la siguiente escala cualitativa:

NIVEL	DESCRIPTOR	DESCRIPCIÓN
1	INSIGNIFICANTE	Si el hecho llegara a presentarse, tendría consecuencias o efectos mínimos sobre la entidad.



	ALCALDÍA MUNICIPAL DE ACACÍAS			 
	PROCESO GESTIÓN TIC			
	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN			
	Fecha: 27/07/2018	Código: GTIC – PL – 01	Versión: 1	

2	MENOR	Si el hecho llegara a presentarse, tendría bajo impacto o efecto sobre la entidad.
3	MODERADO	Si el hecho llegara a presentarse, tendría medianas consecuencias o efectos sobre la entidad.
4	MAYOR	Si el hecho llegara a presentarse, tendría altas consecuencias o efectos sobre la entidad
5	CATASTRÓFICO	Si el hecho llegara a presentarse, tendría desastrosas consecuencias o efectos sobre la entidad.

Un activo tiene una valoración alta en disponibilidad si una amenaza ocasiona desastrosas consecuencias para la Entidad, al causar una pérdida o inactividad del activo y una valoración baja si su pérdida por un periodo prolongado trae consecuencias mínimas sobre la Entidad.

Un activo tiene una valoración alta en Integridad si una amenaza ocasiona desastrosas consecuencias para la Entidad, al causar una alteración o cambios en el activo y una valoración baja si los cambios o alteraciones traen consecuencias mínimas sobre la Entidad.

Un activo tiene una valoración alta en Confidencialidad si su divulgación ocasiona desastrosas consecuencias para la Entidad, y una valoración baja si su divulgación trae consecuencias mínimas sobre la Entidad.

6.1 IDENTIFICACION DE AMENAZAS





La identificación de las amenazas que pueden afectar los activos de información de la Alcaldía Administración Municipal, de acuerdo a su integridad, confidencialidad y disponibilidad.

FUEGO: Posibilidad que el fuego ocasiona daños en los recursos del sistema.

INUNDACION: Posibilidad que el agua ocasiona daños en los recursos del sistema.

TORMENTAS ELECTRICAS: Posibilidad que los rayos y descargas eléctricas ocasiona daños en los activos.



	ALCALDÍA MUNICIPAL DE ACACÍAS			  
	PROCESO GESTIÓN TIC			
	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN			
	Fecha: 27/07/2018	Código: GTIC – PL – 01	Versión: 1	

ALTERACION DE ORDEN PÚBLICO: Desordenes que atenten contra personas y activos de información, que ocasionan daños y pérdidas.

CONTAMINACION MECANICA: Vibraciones, polvo, suciedad que causan daños en los activos.

CONTAMINACION ELECTROMAGNETICA: Interferencias de radio, ondas electromagnéticas, luz ultravioleta.

DAÑO FISICO POR DETERIORO NATURAL: Desgaste de un activo por el uso y paso del tiempo.

FALLO EN EL SERVICIO DE COMUNICACIONES: Cese de la capacidad de transmisión de la red, ya sea por daños físicos o lógicos.

DEGRADACION DE MEDIOS DE ALMACENAMIENTO: Desgaste de los medios de almacenamiento por el paso del tiempo.

ERRORES DE LOS USUARIOS: Equivocaciones de las personas cuando usan los servicios, datos, etc.

ERRORES DE CONFIGURACION: Introducción de datos de configuración erróneos u omisión de parámetros de configuración.

SOFTWARE DAÑINO: Virus, programas espías (spyware), gusanos, troyanos, bombas lógicas, spam, entre otros.





FUGA DE INFORMACION: Revelación por indiscreción de manera verbal, medios electrónicos, soportes en papel, entre otros.

ALTERACION DE INFORMACION: Alteración o cambios en la información.

DESTRUCCION DE INFORMACION: Eliminación de la información.

ERRORES EN EL SOFTWARE: Defectos en el código que originan una operación defectuosa, sin intención por parte del usuario, pero que trae consecuencias en la eficiencia del sistema.



	ALCALDÍA MUNICIPAL DE ACACÍAS			  
	PROCESO GESTIÓN TIC			
	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN			
	Fecha: 27/07/2018	Código: GTIC – PL – 01	Versión: 1	

INGENIERIA SOCIAL: Uso de la buena fe de las personas para realizar actividades que interesan a un tercero.

INSTALACION DE SOFTWARE NO AUTORIZADO: Instalación de software no licenciado.

CAIDA SERVIDOR EXTERNO: Fallos en servidor externo a la Entidad.

ACCESOS NO AUTORIZADO: Se tiene acceso a los activos sin estar autorizado para ello.

DENEGACION DEL SERVICIO: Indisponibilidad del uso del servicio ya sea por ataques intencionados o por agotamiento de recursos.

ROBO: Sustracción de un activo de información, que provoca la carencia de este medio para prestar algún servicio.

INTERCEPTACION DE INFORMACION: Tener acceso a la información, sin que esta sea alterada.

REPUDIO: Negación posterior de actuaciones.

CORTE DE SUMINISTRO ELECTRICO: Cese o interrupción del servicio de fluido eléctrico.

EMANACIONES ELECTROMAGNETICAS: Poner en el campo electromagnético datos para beneficios de terceros.




ERRORES DE SEGUIMIENTO – LOGS: Falta de seguimiento, inadecuado registro de actividades: falta de registros, registros incompletos o incorrectos.

SANCIONES POR ENTES DE CONTROL: Sanciones por incumplimiento en la normatividad.

6.2 VALORACION DE LAS AMENAZAS

Se realiza la valoración de las amenazas teniendo en cuenta su posibilidad de ocurrencia, de acuerdo con la siguiente escala cualitativa:



	ALCALDÍA MUNICIPAL DE ACACÍAS			 <div>Management System ISO 9001:2008 ISO 14001:2004 OHSAS 18001:2007 www.tuv.com ID 9105085574</div> 
	PROCESO GESTIÓN TIC			
	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN			
	Fecha: 27/07/2018	Código: GTIC – PL – 01	Versión: 1	

NIVEL	DESCRIPTOR	DESCRIPCIÓN	FRECUENCIA
1	RARO	El evento puede ocurrir solo en circunstancias excepcionales	No se ha presentado en el último año
2	IMPROBABLE	El evento puede ocurrir en algún momento	Al menos una vez en el último año
3	POSIBLE	El evento podría ocurrir en algún momento	Al menos una vez Mensualmente
4	PROBABLE	El evento probablemente ocurrirá en la mayoría de las circunstancias	Al menos una vez semanalmente
5	CASI SEGURO	Se espera que el evento ocurra en la mayoría de las circunstancias	Al menos una vez en el Día

6.3 IDENTIFICACIÓN DE VULNERABILIDADES

La identificación de las vulnerabilidades o debilidades los activos de información de la Alcaldía Municipal de Acacias Meta, las realiza el dueño del activo.





A cada activo de información se le identifica las vulnerabilidades que puedan ser explotadas por una amenaza.

6.4 VALORACION DEL RIESGO

Para valorar el riesgo se utilizará la siguiente tabla, que permite realizar un análisis con una escala cualitativa, relacionando el impacto y la frecuencia o probabilidad de que ocurra una amenaza, sin tener en cuenta los controles existentes.

PROBABILIDAD	IMPACTO				
	INSIGNIFICANTE (1)	MENOR (2)	MODERADO (3)	MAYOR (4)	CATASTRÓFICO (5)
RARO (1)	B	B	M	A	A
IMPROBABLE (2)	B	B	M	A	E
POSIBLE (3)	B	M	A	E	E
PROBABLE (4)	M	A	A	E	E



	ALCALDÍA MUNICIPAL DE ACACIAS			  
	PROCESO GESTIÓN TIC			
	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN			
	Fecha: 27/07/2018	Código: GTIC – PL – 01	Versión: 1	

CASI SEGURO (5)	A	A	E	E	E
B: Zona de Riesgo Baja: Asumir Riesgo					
M: Zona de Riesgo Moderada: Asumir el Riesgo, Reducir el Riesgo					
A: Zona de Riesgo Alta: Reducir el Riesgo, Evitar, Compartir o Transferir					
E: Zona de Riesgo Extrema: Reducir el Riesgo, Evitar, Compartir o Transferir					

6.5 REVISION DE CONTROLES IMPLEMENTADOS

Se deben identificar los controles existentes que tienen los activos de información para evitar la pérdida de integridad, confidencialidad y disponibilidad y medir su eficiencia.

Los controles permiten ver el grado de exposición frente a la materialización de un riesgo, un control mal implementado genera una vulnerabilidad.

Para medir su efectividad en la mitigación de los riesgos, se utiliza la siguiente escala.

NIVEL	DESCRIPTOR	DESCRIPCIÓN
1	DEBIL	No existen controles o no son efectivos
2	MODERADO	Existen controles, pero no son lo suficientemente efectivos. Pueden o no estar documentados
3	FUERTE	Existen controles efectivos y documentados




6.6 VALORACION DEL RIESGO RESIDUAL

Para valorar el riesgo residual se utilizarán las escalas señaladas anteriormente en el cálculo de la probabilidad y el impacto, pero se tienen en cuenta los controles implementados que se identificaron en el paso anterior.

6.7 ACEPTACION DEL RIESGO

La aceptación del nivel de riesgo es de acuerdo a lo que la Entidad ha definido como zona de riesgo baja y moderada, los riesgos residuales que sean clasificados en esas zonas serán aceptados temporalmente y los demás que sean valorados en las zonas altas y extremas recibirán tratamiento de acuerdo a las opciones correspondientes.



	ALCALDÍA MUNICIPAL DE ACACÍAS			 
	PROCESO GESTIÓN TIC			
	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN			
	Fecha: 27/07/2018	Código: GTIC – PL – 01	Versión: 1	

6.8 REVISION DE LOS RIESGOS Y REEVALUACION

Los resultados del análisis y evaluación de riesgos deben ser revisados por el comité GET, con el fin de que los riesgos sean identificados y aceptados para establecer las opciones de su tratamiento.

Igualmente destinar los recursos, tiempo y responsabilidades en la mitigación de los riesgos.

Los resultados deben revisarse con regularidad a fin visualizar cualquier modificación en cuanto a la estructura organizacional, las actividades que se realizan, la tecnología utilizada, la rotación de funcionarios y la aparición de nuevas amenazas y vulnerabilidades.

Una vez se haya detectado el riesgo, debe recalcularse e identificar las alteraciones en las opciones de tratamiento de riesgo, así como en los controles.

6.9 OPCIONES DE TRATAMIENTO

Una vez se calcularon los riesgos residuales, se inicia el proceso de toma de decisiones en cuanto a cómo se trataran los riesgos identificados de acuerdo a la disponibilidad de recursos, cultura organizacional e impacto en la Entidad.





Para este caso se deben seleccionar opciones de tratamiento de riesgo que permitan reducir riesgos, evitar riesgos, asumir riesgos o transferir riesgos.

ASUMIR EL RIESGO: En este caso la Entidad acepta las consecuencias de no realizar ninguna acción o aplicación de controles sobre el activo, debido a que no se pueden diseñar controles, o que la implantación de estos puede tener altos costos, o que resulta más alto el costo de implantación que la materialización de las amenazas.

Para aceptar las consecuencias de ese riesgo, se debe reservar los recursos económicos o crear fondos de contingencia para cuando los riesgos se hagan realidad.

TRANSFERENCIA DEL RIESGO: La Entidad puede transferir un riesgo cuando no sea viable económicamente, ni técnicamente la aplicación de medidas para reducir el riesgo, en ese caso puede apoyarse en aseguradoras y/o outsourcing.



	ALCALDÍA MUNICIPAL DE ACACÍAS			  
	PROCESO GESTIÓN TIC			
	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN			
	Fecha: 27/07/2018	Código: GTIC – PL – 01	Versión: 1	

Puede externalizar la administración de un activo, repartiendo responsabilidades técnicas y legales, tal como se acuerde en la prestación del servicio.

EVITAR EL RIESGO: Evitar el riesgo es una manera de realizar cambios en actividades o activos susceptibles a riesgos, para impedir su ocurrencia. Para lo cual se pueden seleccionar actividades o activos alternativos reproduzcan los mismos resultados, pero con riesgos menores.

6.10 PLAN DE TRATAMIENTO DE RIESGOS

Los planes de tratamiento de riesgos al interior de los procesos deben ser establecidos por los líderes de éstos, dueños de los activos de información y deben ser aprobados por el comité GEL-T. Se utilizara el formato de plan de tratamiento de riesgos.

El Comité GEL-T es responsable de decidir el orden en cual se implementaran las actividades de tratamiento, de acuerdo a los beneficios y presupuesto asignado.

