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

NEIVA, ENERO DE 2024

TABLA DE CONTENIDO

GLOSARIO

- **Riesgo**: Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales.
- **Riesgo de Seguridad de la Información**: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).
- **Amenaza:** es un ente o escenario interno o externo que puede hacer uso de una vulnerabilidad para generar un perjuicio o impacto negativo en la institución (materializar el riesgo).
- **Vulnerabilidad**: es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos.
- **Probabilidad**: se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando.
- **Impacto**: consecuencias que puede ocasionar a la organización la materialización del riesgo.
- **Control o Medida**: Medida que permite reducir o mitigar un riesgo.

1 INTRODUCCIÓN

El plan de tratamiento de riesgos de Seguridad y Privacidad de la información, de la Alcaldía de Neiva, se basa en una orientación estratégica que requiere el desarrollo de una cultura de carácter preventivo, de manera que, al comprender el concepto de riesgo, así como el contexto, se planean acciones que reduzcan la afectación a la entidad en caso de materialización, adicionalmente busca desarrollar estrategias para la identificación, análisis, tratamiento, evaluación y monitoreo de dichos riesgos con mayor objetividad, dando a conocer aquellas situaciones que pueden comprometer el cumplimiento de los objetivos trazados por la entidad.

Lo anterior dando cumplimiento a la normativa establecida por el estado colombiano, CONPES 3995 de 2020, Modelo de Seguridad y Privacidad de MINTIC y lo establecido en el decreto 1008 de 14 de junio 2018, a la Resolución 500 de 2021, por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital adoptando las buenas prácticas y los lineamientos de los estándares ISO 27001, ISO 31000:2018 y la guía para la administración del riesgo y el diseño de controles en entidades públicas – Riesgos de gestión, corrupción y seguridad digital, establecidos en el Modelo Integrado de Planeación y Gestión.

2 OBJETIVO

Establecer las actividades que permitan mantener la seguridad y privacidad de la información, sistemas de información y plataforma tecnológica que circula en los procesos de la Alcaldía Municipal de Neiva por medio del tratamiento de los riesgos, lo cual conlleva dar frente a las amenazas y vulnerabilidades asociadas a los activos de información, fortaleciendo el enfoque preventivo referente a la seguridad y privacidad de la Información, y garantizando su confidencialidad, integridad y disponibilidad, alineados al Modelo de Seguridad y Privacidad de la Información – MSPI de la política de Gobierno Digital del MinTIC, la norma NTC/IEC ISO 27001, la Política pública de Seguridad Digital, y los criterios de Continuidad de la operación de los servicios.

3 INFORMACIÓN DE LA ORGANIZACIÓN

3.1 ORGANIZACIÓN

ALCALDÍA MUNICIPAL DE NEIVA

3.2 ACTIVIDAD ECONÓMICA

ACTIVIDADES EJECUTIVAS DE LA ADMINISTRACIÓN PÚBLICA

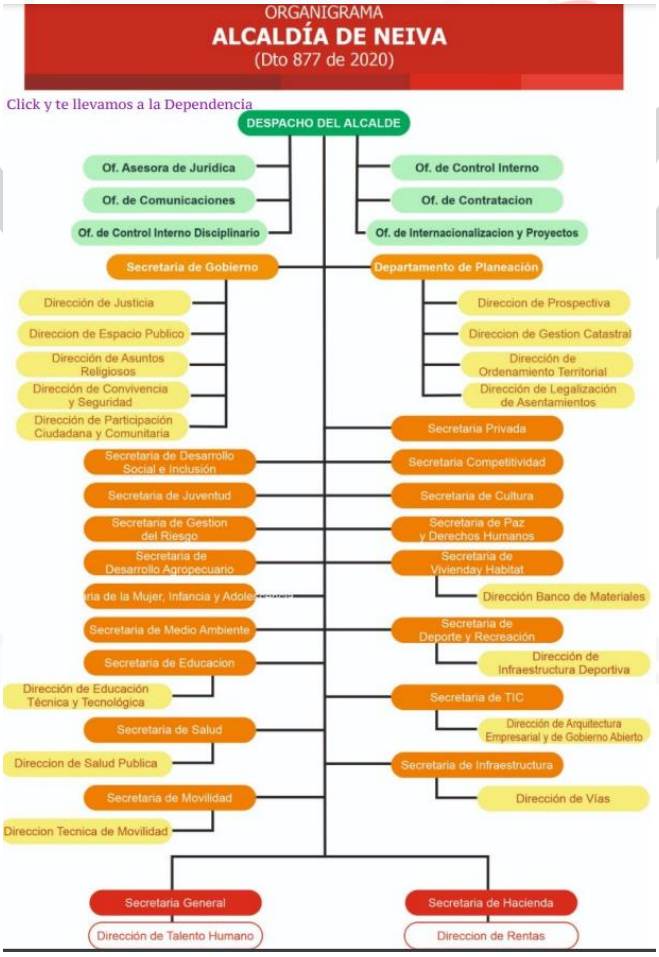
3.3 RESEÑA ALCALDÍA DE NEIVA

La misión de la Administración Municipal de Neiva es servir a la comunidad, promover la prosperidad general, prestar los servicios públicos que determine la constitución y la ley, construir obras públicas que demande el progresos local, ordenar el desarrollo de su territorio, promover la participación comunitaria, la convivencia ciudadana, el mejoramiento social y cultural de sus habitantes y garantizar la efectividad de los principios, derechos y deberes constitucionales que le corresponden como fundamento en los principios orientadores de la función pública.

Neiva y su área de influencia será una región ambiental y económicamente sostenible; culta, socialmente educativa y solidaria, con sólidos valores, donde el avance científico y tecnológico nos inserte competitivamente en el mundo globalizado, para la convivencia y el bienestar de sus habitantes.

3.4 ORGANIGRAMA

Figura 1. Organigrama Alcaldía de Neiva vigente



Fuente: https://www.alcaldianeiva.gov.co/NuestraAlcaldia/Paginas/Organigrama.aspx

4 NORMATIVIDAD

- Constitución Política de Colombia. Artículos 15, 20, 23 y 74.
- Ley 2088 de 2012. Por la cual se regula el trabajo en casa y se dictan otras disposiciones
- Ley 2052 de 2020. Por medio de la cual se expide el código general disciplinario
- Ley 1915 de 2018. Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.
- Ley 1755 de 2015. Por medio de la cual se regula el Derecho Fundamental de Petición y se sustituye un título del Código de Procedimiento Administrativo y de lo Contencioso Administrativo.
- 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.
- Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.
- Ley 1437 de 2011. Por la cual se expide el código de procedimiento administrativo y de lo contencioso administrativo.
- 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.
- Ley 1221 del 2008. Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones.
- Ley 1266 de 2008. Por la cual se dictan las disposiciones generales del Hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
- Ley 962 de 2005. Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos.
- Ley 594 de 2000. Por medio de la cual se regula el Derecho Fundamental de Petición y se sustituye un título del Código de Procedimiento Administrativo y de lo Contencioso Administrativo.
- Ley 527 de 1999. Por la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen las entidades de certificación y se dictan otras disposiciones.
- Ley 44 de 1993. Por la cual se modifica y adiciona la Ley 23 de 2082 y se modifica la Ley 29 de 2044 y Decisión Andina 351 de 2015 (Derechos de autor).
- Ley 23 de 1982. Sobre derechos de autor
- Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones. Decreto 767 de 2022. Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

- Decreto 88 de 2022. Por el cual se adiciona el Título 20 a la Parte 2 del Libro 2 del Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2015, para reglamentar los artículos 3, 5 Y 6 de la Ley 2052 de 2020, estableciendo los conceptos, lineamientos, plazos y condiciones para la digitalización y automatización de trámites y su realización en línea
- Decreto 1287 de 2020. Por el cual se reglamenta el Decreto Legislativo 491 del 28 de marzo de 2020, en lo relacionado con la seguridad de los documentos firmados durante el trabajo en casa, en el marco de la Emergencia Sanitaria.
- Decreto 2106 de 2019. Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública.
- Decreto 1008 del 2018. Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
- Decreto 612 de 2018. Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.
- Decreto 1499 de 2017. Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.
- Decreto 728 de 2017. Por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el modelo de Gobierno Digital en las entidades del orden nacional del Estado colombiano, a través de la implementación de zonas de acceso público a Internet inalámbrico
- Decreto 1074 de 2015. Por medio del cual se expide el Decreto Reglamentario del Sector Comercio, Industria y Turismo. Reglamenta parcialmente la Ley 1581 de 2012 e imparten instrucciones sobre el Registro Nacional de Bases de Datos. Artículos 25 y 26.
- Decreto 1078 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- Decreto 886 de 2014. Por el cual se reglamenta el Registro Nacional de Bases de Datos.
- Decreto 2364 de 2012. Por medio del cual se reglamenta el artículo 7° de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones.
- 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.
- Decreto 884 de 2012 Por medio del cual se reglamenta la Ley 1221 de 2008 y se dictan otras disposiciones.
- Resolución 1838 de 2022. Por la cual se reglamentan las modalidades de teletrabajo, se establecen las condiciones de trabajo en casa y se definen los lineamientos de desconexión laboral en el MINTIC, y se deroga la resolución 1151 del 16 de mayo de 2019.
- Resolución 746 de 2022. Por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales a los establecidos en la Resolución No. 500 de 2021

- Resolución 500 de 2021. Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la Política de Gobierno Digital
- Resolución 1519 de 2020. Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos.

5 MARCO REFERENCIAL

La Alcaldía adopta la presente metodología de administración del riesgo tomando como referencia los lineamientos nacionales y otras normas internacionales que apliquen, con el fin de lograr el entendimiento y aplicación en cada proceso. Para el diseño de la metodología se tuvieron en cuenta los parámetros de la Guía para la administración del riesgo y el diseño de controles en entidades públicas diciembre de 2020 (Riesgos de Gestión, Corrupción y seguridad de la información) y la NTC ISO 31000 Gestión del Riesgo, así como los lineamientos de la Secretaría de Transparencia del Departamento Administrativo de la Presidencia de la República, materializado en la presente política y la estructura del mapa de riesgos, incluidos los de Corrupción.

Para los Riesgos de Gestión, Riesgos de Corrupción y Riesgos de Seguridad de la Información, por proceso se identifican, clasifican y analizan los riesgos en relación a su impacto y probabilidad para determinar el grado de vulnerabilidad. Adicionalmente, se valoran los riesgos confrontando los resultados con los controles eficaces que existan actualmente en la entidad, con el fin de evaluar si estos son suficientes para mitigarlos o definir si se requieren controles adicionales y tipo de tratamiento a aplicar de acuerdo con la metodología definida.

En los Riesgos de seguridad de Seguridad de la información se da por afectación de gravedad en la integridad, disponibilidad y confidencialidad de la información debido al interés particular de empleados y terceros.

En caso de los Riesgos de Corrupción, las acciones que debe tener en cuenta la alta dirección para su administración son:

- Evitar el riesgo: “Tomar las medidas encaminadas a prevenir su materialización. Es siempre la primera alternativa a considerar, se logra cuando al interior de los procesos se generan cambios sustanciales por mejoramiento, rediseño o eliminación, resultado de unos adecuados controles y acciones emprendidas”.

- Reducir el Riesgo: implica tomar medidas encaminadas a disminuir la probabilidad (medidas de prevención). “La reducción del riesgo es probablemente el método más sencillo y económico para superar las debilidades antes de aplicar medidas más costosas y difíciles”.

En este orden de ideas, la política de Riesgos será complementada con la construcción del procedimiento de riesgos de la entidad, el cual complementará la metodología a desarrollar para identificar, mitigar,

evaluar y tratar los Riesgos de gestión, Riesgos de Corrupción y Riesgos de la seguridad de la información, así mismo se construirá el procedimiento de gestión del riesgo el cual será transversal a las funciones establecidas para la secretaria de general de la Alcaldía de Neiva. Siendo estas las herramientas que determinaran el actuar a la entidad ante la configuración de cualquier riesgo principalmente los identificados como riesgos de corrupción, para que a partir de ahí se realice un monitoreo a los controles establecidos para los mismos. Esto con el fin de garantizar la toma de decisiones oportunas desde el nivel más alto de la organización mediante la coordinación de actividades tendientes a reducirlos y evitarlos, y que a la vez se establezcan los responsables acordes con los procesos y procedimientos susceptibles de riesgos de corrupción en la entidad.

5.1 FORMULA DE ACEPTACIÓN DEL RIESGO

Se establecer el siguiente criterio como factor de evaluación en el componente de aceptación del riesgo según la tipología de los riesgos, quedando establecida así:

Riesgos de Seguridad de la Información

- Zona de riesgo BAJA: Se ASUMIRÁ el riesgo y se administra por medio de las actividades propias del proyecto o proceso asociado y se realiza en el reporte mensual de su desempeño.
- Zona de riesgo MODERADO: Se establecen acciones de control preventivas que permitan REDUCIR la probabilidad de ocurrencia del riesgo, se hace seguimiento CUATRIMESTRAL.
- Zona de riesgo ALTA Y EXTREMA: Se debe incluir el riesgo tanto en el Mapa de riesgo del Proceso como en el Mapa de Riesgo Institucional y se establecen acciones de Control Preventivas que permitan MITIGAR la posible materialización del riesgo. Se monitorea MENSUALMENTE.

5.2 DETERMINACIÓN DE PROBABILIDAD

Se determina como la posibilidad de ocurrencia del riesgo y sus consecuencias o impactos que se presentan en la entidad.

La probabilidad de ocurrencia estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. De este modo, la probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año. Bajo este esquema, la subjetividad que usualmente afecta este tipo de análisis se elimina, ya que se puede determinar con claridad la frecuencia con la que se lleva a cabo una actividad, en vez de considerar los posibles eventos que pudiesen haberse dado en el pasado, ya que, bajo esta óptica, si nunca se han presentado eventos, todos los riesgos tendrán la tendencia a quedar ubica dos en niveles bajos, situación que no es real frente a la gestión de las entidades públicas colombianas. Como referente, a continuación, se muestra una tabla de actividades típicas relacionadas con la gestión de una entidad pública, bajo las cuales se definen las escalas de probabilidad:

Tabla No.1 Criterios para determinar la probabilidad

Actividad	Frecuencia de la Actividad	Probabilidad frente al Riesgo
Planeación estratégica	1 vez al año	Muy baja
Actividades de talento humano,jurídica, administrativa	Mensual	Media
Contabilidad, cartera	Semanal	Alta
Tecnología (incluye disponibilidad de aplicativos),tesorería	Diaria	Muy alta

Fuente: Guía para la administración del riesgo DAFP

Teniendo en cuenta lo explicado en el punto anterior sobre el nivel de probabilidad, la exposición al riesgo estará asociada al proceso o actividad que se esté analizando, es decir, al número de veces que se pasa por el punto de riesgo en el periodo de 1 año, en la tabla siguiente se establecen los criterios para definir el nivel de probabilidad.

Tabla No.2 Definir el nivel de probabilidad

	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	20%
Baja	La actividad que conlleva el riesgo se ejecutade 3 a 24 veces por año	40%
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	100%

Fuente: Guía para la administración del riesgo DAFP

5.3 DETERMINACIÓN DEL IMPACTO

Para la construcción de la tabla de criterios se definen los impactos económicos y reputacionales como las variables principales. Cabe señalar que en la versión 2018 de la Guía de administración del riesgo se contemplaban afectaciones a la ejecución presupuestal, pagos por sanciones económicas, indemnizaciones a terceros, sanciones por incumplimientos de tipo legal; así como afectación a la imagen

institucional por vulneraciones a la información o por fallas en la prestación del servicio, todos estos temas se agrupan en impacto económico y reputacional en la versión 2020.

Cuando se presenten ambos impactos para un riesgo, tanto económico como reputacional, con diferentes niveles se debe tomar el nivel más alto.

Tabla No.3 Criterios para definir el nivel de impacto

	Afectación Económica	Reputacional
Leve 20%	Afectación menor a 10 SMLMV	El riesgo afecta la imagen de algúnárea de la organización.
Menor-40%	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores.
Moderado 60%	Entre 50 y 100 SMLMV	El riesgo afecta la entidad imagen de la con algunos usuarios logro de relevancia frente al de los objetivos.
Mayor 80%	Entre 100 y 500 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental omunicipal.
Catastrófico 100%	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país.

Fuente: Guía para la administración del riesgo DAFP

Dependiendo del tamaño y complejidad de los procesos en la entidad, la tabla podrá ser ajustada o adaptada a las necesidades.

Frente al análisis de probabilidad e impacto no se utiliza criterio experto, esto quiere decir que el líder del proceso, como conocedor de su quehacer, define cuántas veces desarrolla la actividad, esto para el nivel de probabilidad, y es a través de la tabla establecida que se ubica en el nivel correspondiente, dicha situación se repite para el impacto, ya que no se trata de un análisis subjetivo.

Se debe señalar que el criterio experto, es decir el conocimiento y experticia del líder del proceso, se utiliza para definir aspectos como: número de veces que se ejecuta la actividad, cadena de valor del proceso, factores generadores y para la definición de los controles.

6 EVALUACIÓN DEL RIESGO

La evaluación del riesgo es partir del análisis de la probabilidad de ocurrencia y sus consecuencias o impactos, se busca determinar la zona de riesgo inicial.

Tabla No.4 Matriz de calor (niveles de severidad del riesgo)

IMPACTO								
PROBABILIDAD	**MUY ALTA 100%**							**EXTREMO**
	ALTA 80%							**ALTO**
	MEDIA 60%							**MODERADO**
	BAJA 40%							**BAJO**
	MUY BAJA 20%							
		LEVE 20%	**MENOR 40%**	**MODERADO 60%**	**MAYOR 80%**	**CATASTROFICO 100%**		

Fuente: Política Administración del Riesgos Alcaldía de Neiva

LINEAMIENTOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

En primer lugar, se debe tener en cuenta que la política de seguridad digital se vincula al modelo de seguridad y privacidad de la información, el cual se encuentra alineado con el marco de referencia de arquitectura y soporta transversalmente los otros habilitadores de la política de gobierno digital: seguridad de la información, arquitectura, servicios ciudadanos digitales.

IDENTIFICACIÓN DE LOS ACTIVOS DE SEGURIDAD DE LA INFORMACIÓN

Como primer paso para la identificación de riesgos de seguridad de la información es necesario identificar los activos de información del proceso.

Tabla No.5 Identificación de activos de información

¿Qué son los activos?	¿Por qué identificar los activos?
Un activo es cualquier elemento que tenga valor para la organización, sin embargo, en el contexto de seguridad digital, son activos elementos tales como: -Aplicaciones de la organización.	Permite determinar qué es lo más importante que cada entidad y sus procesos poseen (sean bases de datos, archivos, servidores web o aplicaciones clave para que la entidad pueda prestar sus servicios).
-Servicios web -Redes -Información física o digital -Tecnologías de información TI -Tecnologías de operación TO que utiliza la organización para funcionar en el entorno digital	La entidad puede saber qué es lo que debe proteger para garantizar tanto su funcionamiento interno como su funcionamiento de cara al ciudadano, aumentando así su confianza en el uso del entorno digital.

Fuente: Política Administración del Riesgos Alcaldía de Neiva

6.1 VALORACIÓN DE CONTROLES PARA TRATAMIENTO DE RIESGOS

Con base en la información referente al nivel de riesgo identificado y el tratamiento que se debe efectuar, se verifican los controles y/o procedimientos existentes en la Administración Municipal, estandarizados en el Anexo A de la norma NTC-ISO/IEC 27001:2013, el cual funciona como lista de chequeo para la implementación de controles y/o medidas de seguridad. Posteriormente se definen controles y/o procedimientos a implementar para seguir el tratamiento de riesgos indicado.

6.2 DECLARACIÓN DE APLICABILIDAD SOA

La presente declaración se establece sobre los controles que son relevantes para el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de la Administración Municipal de Neiva y aplicables al mismo. Adicionalmente en ella se encuentran justificada la exclusión de algunos de los controles y se muestra el motivo de selección de los controles aplicables, entre los motivos de selección se pueden encontrar: resultados y conclusiones de la evaluación de riesgos y en los procesos de tratamiento del riesgo, requisitos legales o reglamentos, obligaciones contractuales y necesidades empresariales de la organización en materia de seguridad de la información:

LR: requerimientos legales, CO: obligaciones contractuales, BR/BP: requerimientos del negocio/mejores prácticas adoptadas, RRA: resultado de la valoración de riesgos;

Tabla No.6 Declaración de aplicabilidad vigente

ISO 27001:2013 Controles de Seguridad			Controles actuales	Comentarios (justificación de exclusión)	Controles seleccionados y razones de selección				Comentarios (visión general de la implementación)
					LR	CO	BR/BP	RRA	
Cláusula	Sección	Objetivo de control / control							
5 Políticas de Seguridad	5,1	Dirección de la alta gerencia para la seguridad de la información							
	5.1.1	Políticas de seguridad de la información	Política general de SI publicada en el SIGC		X		X	X	Establecer y documentar políticas de SI, y posterior inclusión en el SIG
	5.1.2	Revisión de las políticas de seguridad de la información	Revisión anual de la Política general de SI		X		X	X	Revisión anual periódica de políticas de SI, y posterior inclusión en el SIG
6 Organización de la Seguridad de la Información	6,1	Organización interna							
	6.1.1	Roles y responsabilidad de seguridad de la información	Política general de SI publicada en el SIGC				X	X	Se deben añadir las responsabilidades incluidas en las políticas, en los contratos de los funcionarios
	6.1.2	Segregación de deberes	Asignación de responsabilidad sobre activos de información				X	X	Se debe establecer procesos de verificación periódica de no duplicidad de funciones entre funcionarios de planta administrativa, contratistas y proveedores
	6.1.3	Contacto con autoridades	Red de emergencias mediante empresa de seguridad		X		X		Establecer y documentar procedimientos
	6.1.4	Contacto con grupos de interés especial	No existe asignación de responsabilidad para contactar grupos de interés				X		Establecer y documentar procedimientos
	6.1.5	Seguridad de la información en la gestión de proyectos	No se han definido aplicación de políticas y/o procedimiento de SI en los proyectos		X	X	X	X	Se deben incluir cláusulas referentes a seguridad y confidencialidad de la información interna en los proyectos
	6,2	Dispositivos móviles y teletrabajo							
	6.2.1	Política de dispositivos móviles	No existe política para dispositivos móviles, pero existen directrices elevadas por talento humano		X	X	X	X	Establecer, documentar e implementar
	6.2.2	Teletrabajo	Se fomenta y aplican lineamientos de la política de teletrabajo pero no existe trazabilidad		X				Establecer, documentar e implementar procedimientos para acoger dicha estrategia al interior de la entidad
Hasta en los Recu	7,1	Previo al empleo							
	7.1.1	Verificación de antecedentes	Solicitud de antecedentes disciplinarios, fiscales, judiciales y profesionales		X	X	X		Se deben incluir las responsabilidades incluidas en las políticas en los contratos de

ISO 27001:2013 Controles de Seguridad			Controles actuales	Comentarios (justificación de exclusión)	Controles seleccionados y razones de selección				Comentarios (visión general de la implementación)
					LR	CO	BR/BP	RRA	
									los funcionarios
	7.1.2	Términos y condiciones del empleo	Explícitamente no se definen obligaciones sobre la información a manejar		X	X	X		Se debe establecer procesos de verificación periódica de no duplicidad de funciones entre funcionarios de planta administrativa, contratistas y proveedores
	7,2	Durante el empleo							
	7.2.1	Responsabilidades de la Alta Gerencia	No existen procedimientos que garanticen responsabilidades de funcionarios sobre SI		X	X	X	X	Seguimiento mediante Control Interno
	7.2.2	Conciencia, educación y entrenamiento de seguridad de la información	No existe conciencia de SI		X	X	X	X	Establecer, documentar e implementar Plan de capacitación y circulares internas
	7.2.3	Proceso disciplinario	No existen procesos disciplinarios para violaciones de SI		X	X			Proveer lineamientos jurídicos y establecer procesos de control interno disciplinario
	7,3	Terminación y cambio de empleo							
	7.3.1	Termino de responsabilidades o cambio de empleo	No se establecen acuerdos de confidencialidad con funcionarios		X	X			Se deben añadir las responsabilidades incluidas en las políticas, en los contratos de los funcionarios
8 Gestión de Activos	8,1	Responsabilidad de los activos							
	8.1.1	Inventario de activos	Inventario desactualizado, pendiente de revisión, asignación de responsabilidad y aprobación por la alta dirección		X	X	X	X	Parametrización y modificación de aplicativo de inventario, para que incluya perfiles destinados a la gestión de activos TI por parte de la Oficina TIC
	8.1.2	Propiedad de activos	Se aplica formato de traslado de activos, pero se debe revisar clasificación y asignación final		X	X	X	X	Establecer y documentar procedimiento de seguimientos a la responsabilidad sobre los activos.
	8.1.3	Uso aceptable de los activos	Es necesario sensibilización para el uso eficiente de los activos			X	X		Establecer, documentar e implementar política de uso de activos TI (hardware y software)
	8.1.4	Devolución de activos	Formato de traslado de activos y manual de almacén, pero es necesario socializar y divulgar		X	X	X		Verificar su cumplimiento
	8,2	Clasificación de la información							
	8.2.1	Clasificación de la información	Procedimientos de clasificación de información por parte de Archivo Municipal		X	X	X	X	Establecer y documentar procedimientos para la clasificación de la información
	8.2.2	Etiquetado de la información	Procedimiento de etiquetado para activos de información, que no se aplica a cabalidad		X	X	X		Establecer y documentar procedimientos para la clasificación de la información
	8.2.3	Manejo de activos	Procedimientos establecidos en Manual de Almacén				X		Establecer y documentar política de uso de activos TI (hardware y software)
	8,3	Manejo de medios							
	8.3.1	Gestión de medios removibles	Procedimiento de gestión de medios, pendiente de divulgar		X	X	X		Establecer, documentar e implementar política de uso de activos TI (hardware y

ISO 27001:2013 Controles de Seguridad			Controles actuales	Comentarios (justificación de exclusión)	Controles seleccionados y razones de selección				Comentarios (visión general de la implementación)
					LR	CO	BR/BP	RRA	
									software)
	8.3.2	Eliminación de medios	Procedimiento inexistente		X	X	X		Establecer, documentar e implementar política de uso de activos TI (hardware y software)
	8.3.3	Transporte de medios físicos	Directrices formales por parte de la Alta Dirección		X	X	X	X	Establecer, documentar e implementar política de uso de activos TI (hardware y software)
9 Control de Acceso	9,1	Requerimientos de negocio para el control de acceso							
	9.1.1	Política de control de acceso	Procedimientos de control de acceso que no se cumplen en su totalidad		X	X	X	X	Establecer, documentar e implementar política de control de acceso
	9.1.2	Acceso a redes y servicios de red	No existe política de acceso a redes y servicios de red			X	X	X	Establecer, documentar e implementar política de control de acceso
	9,2	Gestión de accesos de usuario							
	9.2.1	Registro y baja del usuario	Manual de almacén, no se cumple el procedimiento en su totalidad		X	X	X	X	Establecer, documentar e implementar política de control de acceso
	9.2.2	Provisión de acceso a usuarios	Formato de solicitud de cuentas de usuario, pero no se realiza trazabilidad al acceso						Incluir en la política de control de acceso
	9.2.3	Gestión de derechos de acceso privilegiados	Formato de solicitud de cuentas de usuario, pero no se realiza trazabilidad al acceso						Incluir en la política de control de acceso
	9.2.4	Gestión de información de autenticación secreta de usuarios	No existe política de gestión de información de autenticación secreta de usuarios		X	X	X		Establecer, documentar e implementar política de control de acceso
	9.2.5	Revisión de derechos de acceso de usuarios	No se realizan revisiones periódicas de derechos de acceso a usuarios			X	X		Establecer, documentar e implementar política de control de acceso
	9.2.6	Eliminación o ajuste de derechos de acceso	Formato de solicitud de cuentas de usuario			X	X		Establecer, documentar e implementar política de control de acceso
	9,3	Responsabilidades del usuario							
	9.3.1	Uso de información de autenticación secreta	No existe política de gestión de información de autenticación secreta de usuarios		X	X	X		Establecer, documentar e implementar política de control de acceso
	9,4	Control de acceso de sistemas y aplicaciones							
	9.4.1	Restricción de acceso a la información	Formato de solicitud de cuentas de usuario, no existe políticas de control de acceso		X	X	X		Establecer, documentar e implementar política de control de acceso
	9.4.2	Procedimientos de inicio de sesión seguro	No existe procedimiento de ingreso seguro a sistemas y aplicaciones		X	X	X	X	Establecer, documentar e implementar política de control de acceso
	9.4.3	Sistema de gestión de contraseñas	No existe política de gestión de contraseñas, pero si se gestionan las contraseñas del correo institucional				X	X	Establecer, documentar e Implementar política de control de contraseñas
	9.4.4	Uso de programas y utilidades	Formato de solicitud de cuentas de usuario para		X	X	X	X	Establecer, documentar e implementar

ISO 27001:2013 Controles de Seguridad			Controles actuales	Comentarios (justificación de exclusión)	Controles seleccionados y razones de selección				Comentarios (visión general de la implementación)
					LR	CO	BR/BP	RRA	
		privilegiadas	aplicativos de la Administración, para otros programas y utilidades no existe procedimiento de control de software						política de control de acceso
	9.4.5	Control de acceso al código fuente del programa	No existe procedimiento de gestión de código fuente de aplicativos						Establecer, documentar e implementar políticas de seguimiento al control de códigos
10 Criptografía	10,1	Controles criptográficos							
	10.1.1	Política en el uso de controles criptográficos	SE EXCLUYE	No se aplican controles criptográficos	X	X	X	X	
	10.1.2	Gestión de llaves	No existe procedimiento de gestión llaves cifradas de acceso		X	X	X	X	Establecer, documentar e implementar políticas de gestión de llaves cifradas
11 Seguridad Física y del Entorno	11,1	Áreas seguras							
	11.1.1	Perímetro de seguridad físico	Restricciones mediante Vigilancia, cámaras y avisos de "Solo personal autorizado", sin definición general en la entidad		X	X	X	X	Definir y aplicar de perímetro de seguridad físico
	11.1.2	Controles físicos de entrada	No existen controles robustos de ingreso a las instalaciones		X	X	X	X	Establecer, documentar y definir formatos de control de llaves y de control de acceso a oficinas de gestión de información, e incluirlos en políticas de control de acceso
	11.1.3	Seguridad de oficinas, habitaciones y facilidades	Restricciones mediante Vigilancia, cámaras y avisos de "Solo personal autorizado", sin definición general en la entidad			X	X		Establecer, documentar y definir formatos de control de llaves y de control de acceso a oficinas de gestión de información, e incluirlos en políticas de control de acceso
	11.1.4	Protección contra amenazas externas y del ambiente	Se encuentran definidos riesgos en el SGSST, mas no está implementada en áreas críticas de tecnología		X	X	X	X	Realizar verificación y aplicación de medidas de mitigación de riesgos del SGSST
	11.1.5	Trabajo en áreas seguras	No existe procedimiento de trabajo en áreas seguras			X	X		Establecer, documentar y definir procesos de trabajo en áreas seguras
	11.1.6	Áreas de entrega y carga	Existen directrices asignadas a personal de vigilancia y bitácora de ingreso en entrada principal de cada sede, pero estas no están consolidadas en toda la entidad				X		Establecer, documentar y definir formatos de control de acceso a oficinas, e incluirlos en políticas de control de acceso
	11,2	Equipo							
	11.2.1	Instalación y protección de equipo	No existen directrices claras, por tanto no hay cumplimiento de las mismas por parte de funcionarios			X	X	X	Establecer, documentar e implementar lista de chequeo de mobiliario para uso de activos TI e incluirla en políticas de uso de hardware
	11.2.2	Servicios de soporte	No se cumple a cabalidad con los servicios de soporte requeridos en la entidad (electricidad,			X	X		Establecer, documentar e implementar plan de verificación y mantenimiento preventivo

ISO 27001:2013 Controles de Seguridad			Controles actuales	Comentarios (justificación de exclusión)	Controles seleccionados y razones de selección				Comentarios (visión general de la implementación)
					LR	CO	BR/BP	RRA	
			telecomunicaciones, aire acondicionado, etc.)						periódico de sistemas de respaldo eléctrico (UPS y Planta Eléctrica)
	11.2.3	Seguridad en el cableado	No existen medidas de protección y seguridad del cableado electico y de telecomunicaciones, de acuerdo a estándares internacionales			X	X	X	Establecer, documentar e implementar plan de verificación y mantenimiento preventivo periódico de cableado estructurado
	11.2.4	Mantenimiento de equipos	No existe plan de mantenimiento de equipos			X	X	X	Establecer, documentar e implementar plan de verificación y mantenimiento preventivo periódico de equipos
	11.2.5	Retiro de activos	No existen directrices ni políticas definidas para retiro temporal de activos, aunque se aplica servicio de vigilancia y bitácora de ingreso en entrada principal de cada sede			X	X		Establecer, documentar e implementar formatos de retiro de activos e incluirlos en las políticas y procedimientos de uso y administración de hardware
	11.2.6	Seguridad del equipo y activos fuera de las instalaciones	No existen medidas de seguridad para activos que se encuentran fuera de las instalaciones			X	X		Establecer, documentar e implementar formatos de retiro de activos e incluirlos en las políticas y procedimientos de uso y administración de hardware
	11.2.7	Eliminación segura o reusó del equipo	No existen directrices para disposición segura o reúso de equipos		X	X	X		Establecer, documentar e implementar procedimientos para la eliminación segura o reúso de activos TI
	11.2.8	Equipo de usuario desatendido	No existen directrices definidas ni procedimientos establecidos al respecto			X	X	X	Establecer, documentar e implementar procedimientos para bloqueo de sesión de usuario en equipos
	11.2.9	Política de escritorio limpio y pantalla limpia	No existen directrices ni políticas de escritorio y pantalla limpia			X	X	X	Adoptar procedimientos para escritorio y pantalla limpios
12 Seguridad en las Operaciones	12,1	Procedimientos Operacionales y Responsabilidades							
	12.1.1	Documentación de procedimientos operacionales	Manual de funciones. No existen procedimientos de operación detallados.		X	X	X		Incluir funciones y obligaciones contractuales de SI y a su vez incluir en Manual de funciones y Portal de Contratación
	12.1.2	Gestión de cambios	No existe procedimiento de control de cambios formalizado			X	X		Establecer formato de gestión de cambios en los procesos
	12.1.3	Gestión de la capacidad	No existen procedimientos de gestión de capacidad.			X	X		Establecer, documentar e implementar plan periódico de diagnóstico de equipos
	12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	No existe procedimientos para la separación de ambientes						Realizar identificación de ambientes y señalizar debidamente
	12,2	Protección de Software Malicioso							
	12.2.1	Controles contra software malicioso	No existen políticas de prohibición de uso de software no autorizado, sin embargo, se realizan sensibilizaciones al respecto.			X	X		Plan de adquisición y mantenimiento de aplicativo de protección contra software malicioso

ISO 27001:2013 Controles de Seguridad			Controles actuales	Comentarios (justificación de exclusión)	Controles seleccionados y razones de selección				Comentarios (visión general de la implementación)
					LR	CO	BR/BP	RRA	
	12,3	Respaldo							
	12.3.1	Respaldo de información	Se realizan Backups de algunos sistemas de información, sin un procedimiento establecido para almacenamiento y pruebas de restauración		X	X	X	X	Estandarizar y promover mediante políticas
	12,4	Bitácoras y monitoreo							
	12.4.1	Bitácoras de eventos	No existe un registro de eventos u actividades de SI		X	X	X	X	Establecer, documentar e implementar política de monitoreo de usuarios y eventos de seguridad
	12.4.2	Protección de información en bitácoras	No existe procedimiento de control de la información de bitácoras		X		X	X	Establecer, documentar e implementar política de monitoreo de usuarios y eventos de seguridad
	12.4.3	Bitácoras de administrador y operador	No existe registros de actividades de administrador ni de operadores		X		X	X	Establecer, documentar e implementar política de monitoreo de usuarios y eventos de seguridad
	12.4.4	Sincronización de relojes	No se cuenta con fuente de referencia de tiempo única				X		Establecer, documentar e implementar política de monitoreo de usuarios y eventos de seguridad
	12,5	Control de software operacional							
	12.5.1	Instalación de software en sistemas operacionales	No se realizan controles de actualizaciones de software			X	X		Establecer, documentar e implementar política de uso de activos TI (hardware y software) y de control de acceso
	12,6	Gestión de vulnerabilidades técnicas							
	12.6.1	Gestión de vulnerabilidades técnicas	Solo existe el Mapa de Riesgos por Proceso en el SIG para gestión de riesgos, pero no abarca vulnerabilidades técnicas de los mismos			X	X	X	Establecer y documentar análisis y evaluación de riesgos TI
	12.6.2	Restricciones en la instalación de software	Se efectúan restricciones para la instalación de software pero no existe proceso documentado		X	X	X	X	Establecer, documentar e implementar política de uso de activos TI (hardware y software) y de control de acceso
	12,7	Consideraciones de auditoria de sistemas de información							
	12.7.1	Controles de auditoría de sistemas de información	Procedimientos de Auditoría Interna y Planes de Mejora Continua			X	X		Establecer, documentar e implementar plan de auditoría de sistemas de información para Control Interno
13 Seguridad en las Comunicaciones	13,1	Gestión de seguridad en red							
	13.1.1	Controles de red	En algunos casos se aplica el Formato de solicitud de cuentas de usuario, para aplicativos a los que se requiere acceso, perfil requerido, etc. Existen directrices de seguridad en redes, pero no son cumplidas por los funcionarios						Efectuar análisis periódicos de tráfico de red, realizar reporte de anomalías detectadas y aplicar medidas preventivas y correctivas cuando sea el caso.

ISO 27001:2013 Controles de Seguridad			Controles actuales	Comentarios (justificación de exclusión)	Controles seleccionados y razones de selección				Comentarios (visión general de la implementación)
					LR	CO	BR/BP	RRA	
	13.1.2	Seguridad en los servicios en red	No se tienen identificados en todos los servicios de red directrices de seguridad en información			X	X	X	Establecer, documentar e implementar plan de verificación y mantenimiento preventivo periódico de cableado estructurado
	13.1.3	Segregación en redes	Existen procedimientos básicos no documentados de segregación de redes en la entidad				X	X	Establecer, documentar e implementar plan de verificación y mantenimiento preventivo periódico de cableado estructurado
	13,2	Transferencia de información							
	13.2.1	Políticas y procedimientos para la transferencia de información	No existe seguimiento de flujo de comunicaciones en la red			X	X	X	Establecer, documentar e implementar políticas de transferencia de información al interior de la Administración Municipal
	13.2.2	Acuerdos en la transferencia de información	No existen directrices u acuerdos de transferencia de información		X	X	X	X	Establecer, documentar e implementar políticas de transferencia de información al interior de la Administración Municipal
	13.2.3	Mensajería electrónica	No existen directrices u definiciones de protección formal para mensajería electrónica			X	X	X	Establecer, documentar e implementar políticas de uso del correo electrónico institucional
	13.2.4	Acuerdos de confidencialidad o no-revelación	No existen acuerdos ni políticas de confidencialidad de información transmitida		X	X	X	X	Establecer, documentar e implementar políticas de uso del correo electrónico institucional, y acuerdos de confidencialidad en los procesos contractuales y de gestión de proyectos
14 Adquisición, Desarrollo y Mantenimiento de Sistemas	14,1	Requerimientos de seguridad en sistemas de información							
	14.1.1	Análisis y especificación de requerimientos de seguridad	No existen directrices ni políticas de requerimientos de SI en Fichas Técnicas y Estudios Previos Contractuales		X	X	X	X	Incluir en estudios de conveniencia previos y procesos contractuales
	14.1.2	Aseguramiento de servicios de aplicación en redes públicas	No existen directrices de seguridad formales de servicios en aplicaciones de redes públicas.		X	X	X		Incluir encriptación de comunicaciones en características técnicas de aplicaciones que trabajen sobre redes públicas
	14.1.3	Protección de transacciones en servicios de aplicación	No existen directrices de protección de transacciones en los servicios disponibles en la entidad		X	X	X	X	Establecer e implementar medidas de protección de transacciones
	14,2	Seguridad en el proceso de desarrollo y soporte							
	14.2.1	Política de desarrollo seguro	No existen políticas de desarrollo seguro de software						Establecer, documentar e implementar políticas de desarrollo seguro de software
	14.2.2	Procedimientos de control de cambios del sistema	No existen directrices en el control de cambio de sistemas			X	X		Validación por funcionarios de TIC mediante formato estándar
	14.2.3	Revisión técnica de aplicaciones	No existen directrices de revisión técnica de			X	X		Validación por funcionarios de TIC mediante

ISO 27001:2013 Controles de Seguridad			Controles actuales	Comentarios (justificación de exclusión)	Controles seleccionados y razones de selección				Comentarios (visión general de la implementación)
					LR	CO	BR/BP	RRA	
		después de cambios a la plataforma operativa	aplicaciones						formato estándar
	14.2.4	Restricción de cambios en paquetes de software	No existen directrices de restricción de cambios en paquetes de software			X	X		Establecer, documentar e implementar políticas de desarrollo seguro de software
	14.2.5	Principios de seguridad en la ingeniería de sistemas	No existe procedimiento de construcción de sistemas seguros						Establecer, documentar e implementar políticas de desarrollo seguro de software
	14.2.6	Entorno de desarrollo seguro	No existen políticas para ambientes de desarrollo seguro						Establecer, documentar e implementar políticas de desarrollo seguro de software
	14.2.7	Desarrollo tercerizado	No existen directrices para desarrollos contratados externamente			X	X		Validación por funcionarios de TIC mediante formato estándar
	14.2.8	Pruebas de seguridad del sistema	No existen procedimientos de pruebas de seguridad						Validación por funcionarios de TIC mediante formato estándar
	14.2.9	Pruebas de aceptación del sistema	No existen procedimientos de pruebas para aceptación de sistemas			X	X		Validación por funcionarios de TIC mediante formato estándar
	14,3	Datos de prueba							
	14.3.1	Protección de datos de prueba	Se realizan Backups de sistemas de información, pero no existen procedimientos para protección de datos de prueba			X	X		Establecer, documentar e implementar procedimiento para el almacenamiento seguro de datos de prueba
15 Relaciones con Proveedores	15,1	Seguridad de la información en relaciones con el proveedor							
	15.1.1	Política de seguridad de la información en las relaciones con el proveedor	No existen políticas de SI para relaciones con proveedores			X	X		Establecer e implementar
	15.1.2	Atención de tópicos de seguridad en los acuerdos con el proveedor	No existen políticas de SI para relaciones con proveedores			X	X		Establecer e implementar
	15.1.3	Cadena de suministros de tecnologías de la información y comunicaciones	No existen políticas de SI para relaciones con proveedores			X	X		Establecer e implementar
	15,2	Gestión de entrega de servicios de proveedor							
	15.2.1	Monitoreo y revisión de servicios del proveedor	No existen políticas de SI para relaciones con proveedores		X	X	X		Validación por funcionarios de TIC mediante formato estándar
	15.2.2	Gestión de cambios a los servicios del proveedor	No existen políticas de SI para relaciones con proveedores		X	X	X		Establecer e implementar Política de seguridad de la información en las relaciones con el proveedor
Incidentes de Seguridad de la	16,1	Gestión de incidentes de seguridad de la información y mejoras							
	16.1.1	Responsabilidades y procedimientos	No existe asignación de responsabilidades y procedimientos de respuesta rápida a incidentes de seguridad			X	X	X	Establecer, documentar e implementar plan de contingencia

ISO 27001:2013 Controles de Seguridad			Controles actuales	Comentarios (justificación de exclusión)	Controles seleccionados y razones de selección				Comentarios (visión general de la implementación)
					LR	CO	BR/BP	RRA	
	16.1.2	Reporte de eventos de seguridad de la información	No existen directrices ni procedimientos para aplicar en eventos de SI			X	X	X	Establecer, documentar e implementar plan de contingencia
	16.1.3	Reporte de debilidades de seguridad de la información	No existe procedimiento de reporte de eventos de SI, pero se realizan reportes informales de los servidores por dependencia			X	X	X	Establecer, documentar e implementar plan de contingencia
	16.1.4	Valoración y decisión de eventos de seguridad de la información	No existe reporte de eventos de SI			X	X	X	Establecer, documentar e implementar plan de contingencia
	16.1.5	Respuesta a incidentes de seguridad de la información	No existen procedimientos de respuesta a incidentes de SI			X	X	X	Establecer, documentar e implementar plan de contingencia
	16.1.6	Aprendizaje de incidentes de seguridad de la información	No existen procedimientos de respuesta a incidentes de SI, ni registro de incidentes			X	X	X	Establecer, documentar e implementar plan de contingencia
	16.1.7	Colección de evidencia	Existen procedimientos de custodia de archivos como Tablas de retención documental, más no se aplican procedimientos para la identificación, recolección, adquisición y preservación de información			X	X	X	Establecer, documentar e implementar plan de contingencia
17 Aspectos de Seguridad de la Información para la Gestión de la Continuidad del Negocio	17,1	Continuidad de la seguridad de la información							
	17.1.1	Planeación de la continuidad de la seguridad de la información	No se tiene formalidad del BCP y no se tiene cumplimiento por parte de los funcionarios		X		X		Establecer, documentar e implementar plan de continuidad del negocio
	17.1.2	Implementación de la continuidad de la seguridad de la información	Existen procedimientos para el mantenimiento de la información física de la entidad, pero no se tiene formalidad del BCP		X		X		Establecer, documentar e implementar plan de continuidad del negocio
	17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	No se han realizado pruebas de funcionalidad en SI		X		X		Establecer, documentar e implementar plan de continuidad del negocio
	17,2	Redundancias							
	17.2.1	Disponibilidad de facilidades de procesamiento de información	No cuenta con elementos redundantes		X		X	X	
18 Cumplimiento	18,1	Cumplimiento con Requerimientos Legales y Contractuales							
	18.1.1	Identificación de legislación aplicable y requerimientos contractuales	Existen responsables para el cumplimiento de las leyes y tiene responsables en la identificación		X	X	X		Incluir dentro de los procedimientos y la declaración de aplicación de políticas de seguridad de la información, la normatividad, reglamentación y legislación respectiva
	18.1.2	Derechos de propiedad intelectual (IPR)	No se cuentan con procedimientos documentados y aprobados para tal fin, pero se entregan derechos contractuales de		X	X	X		Establecer, documentar e implementar plan de verificación y seguimiento a licenciamiento de aplicaciones y software

ISO 27001:2013 Controles de Seguridad			Controles actuales	Comentarios (justificación de exclusión)	Controles seleccionados y razones de selección				Comentarios (visión general de la implementación)
					LR	CO	BR/BP	RRA	
			documentos realizados por contratistas						
	18.1.3	Protección de registros	Existen tablas de retención documental que especifican los registros y el periodo por el cual se deberían retener, además del almacenamiento, manejo y destrucción		X	X	X		Establecer, documentar e implementar plan de verificación y seguimiento a licenciamiento de aplicaciones y software
	18.1.4	Privacidad y protección de información personal identificable (PIR)	Existen algunas políticas de protección de información por aplicativo		X	X	X		Establecer, documentar e implementar plan de capacitación, promoción, divulgación y aplicación de Ley 1273 de 2009
	18.1.5	Regulación de controles criptográficos	SE EXCLUYE	No se aplican controles criptográficos en la entidad	X	X	X		
	18,2	Revisiones de seguridad de la información							
	18.2.1	Revisión independiente de seguridad de la información	Se cuentan con auditorias en SI		X	X	X		Establecer, documentar e implementar planes de auditoría interna las políticas de SI
	18.2.2	Cumplimiento con políticas y estándares de seguridad	No se realizan procedimientos de SI		X	X	X		Establecer, documentar e implementar planes de auditoría interna las políticas de SI
	18.2.3	Revisión del cumplimiento técnico	Se realiza revisión en algunos sistemas de información		X	X	X		Establecer, documentar e implementar planes de auditoría interna las políticas de SI

7 METODOLOGÍA

El Plan de Tratamiento de Riesgos contempla la definición de las actividades a desarrollar en aras de mitigar los riesgos sobre los activos identificados en la entidad, estas actividades se estructuraron de la siguiente manera, siguiendo las recomendaciones de la Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información (MinTIC:2016).

Tabla No.7 Cronograma Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

Gestión	Actividades	Tareas	Responsable de la Tarea	Evidencia	Fechas Programación Tareas	
					Fecha Inicio	Fecha Final
Gestión de Riesgos	Actualización de lineamientos de riesgos	Apoyar cuando se requiera la actualización de la política, metodología y lineamientos de la gestión de riesgos	Equipo TIC - MIPG	Correos electrónicos, Documentación actualizada en Sistema de Gestión Página web	15-feb-24	30-mar-24
	Identificación de Riesgos de Seguridad y Privacidad de la Información	Contexto, Identificación, Análisis y Evaluación de Riesgos - Seguridad y Privacidad de la Información y Seguridad Digital	Equipo TIC - MIPG	Correos electrónicos Mapas de riesgos	1-ago-24	30-oct-24
		Realimentación, revisión y verificación de los riesgos identificados (Ajustes)	Equipo TIC - MIPG	Correos electrónicos Mapas de riesgos	1-ago-24	30-oct-24
	Aceptación de Riesgos Identificados	Aceptación, aprobación riesgos identificados y planes de tratamiento	Equipo TIC - MIPG	Memorandos de aceptación mapas de riesgos	1-nov-24	30-nov-24
	Publicación	Publicación mapas de riesgos de los procesos Sistema de Gestión	Equipo TIC	Mapas de riesgos publicados Sistema de Gestión	15-dic-24	30-dic-24

Gestión	Actividades	Tareas	Responsable de la Tarea	Evidencia	Fechas Programación Tareas	
					Fecha Inicio	Fecha Final
	Seguimiento Fase de Tratamiento	Seguimiento implementación de controles y planes de tratamiento de riesgos los identificados (verificación de evidencias)	Equipo TIC	Seguimiento mapas de riesgo	1-nov-24	30-dic-24

Fuente: Elaboración Propia

Control de Cambios

Versión	Fecha	Descripción
1.0	17/06/2018	Versión Inicial Ing. Brayan Alexander Beleño García - Contratista Secretaría TIC y Competitividad. Revisión: Ing. Oscar Hernando Motta Valencia – Asesor TIC del Despacho.
1.1	24/01/2020	Actualización. Ing. German Yobany Beltrán Rondón, Líder de TIC – Asesor de Despacho. Ing. Juan Carlos Rodríguez – Contratista Secretaría de TIC y Competitividad.
1.2	30/12/2020	Actualización. Ing. German Yobany Beltrán Rondón, Secretario de TIC. Ing. Jorge Esneider Henao González – Contratista Secretaría de TIC.
1.3	28/01/2022	Actualización. Ing. German Yobany Beltrán Rondón, Secretario de TIC. Ing. Luis Ernesto Arias Méndez – Contratista Secretaría de TIC.
1.4	25/01/2023	Actualización. Ing. German Yobany Beltrán Rondón, Secretario de TIC.
1.5	26/01/2024	Actualización. Secretaría de TIC