MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

ELIECER ARTEAGA VARGAS

Alcalde

MARTA CECILIA RIVERA HIGUITA
Subsecretaria Gestión Tics y Documental

APARTADO ANTIOQUIA
Enero del 2019

CONTENIDO

1. OBJETIVO

El documento MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN PARA LA ALCALDIA DE APARTADO tiene como objetivo PRINCIPAL el de garantizar un adecuado manejo de la información pública en poder de las entidades destinatarias, la cual es uno de los activos más valiosos para la toma de decisiones.

El modelo propende por un doble enfoque a saber: a nivel de seguridad marcando un derrotero para que la Alcaldía de Apartado construya unas políticas de seguridad sobre la información a fin de salvaguardar la misma a nivel físico y lógico, de manera que se pueda en todo momento garantizar su integridad, disponibilidad y autenticidad. En esa línea el aseguramiento de los procesos relacionados con los sistemas de información debe complementarse con un enfoque de privacidad para garantizar tanto la protección de los derechos a la intimidad y el buen nombre o la salvaguarda de secretos profesionales, industriales o de información privilegiada de particulares en poder de la administración como el acceso a la información pública cuando esta no se encuentre sometida a reserva.

Otros de sus objetivos son:

- Describir el entorno general de la seguridad y privacidad de la información en la Alcaldia de Apartado así como el marco normativo aplicable.
- Describir y explicar de forma detallada el modelo de seguridad y privacidad de la información que se aplica en la Alcaldía de Apartado
- Explicar cada una de las etapas del modelo y la forma en que se abordarán por parte de la entidad.

2. ALCANCE Y PÚBLICO OBJETIVO

El MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE LA ALCALDIA DE APARTADO tiene como alcance todas las dependencias de la Alcaldia de Apartado, colaboradores, contratistas y visitantes en los casos que aplique. Apunta a proteger y preservar las características de integridad, confidencialidad y disponibilidad de los activos de información que se identifiquen como parte de esta política.

Está hecho para lectura y aplicación por parte de todos los colaboradores de todas las dependencias de la ALCALDIA DE APARTADO, especialmente aquellos que tienen bajo su responsabilidad activos de información de todo tipo.

También debe extenderse a visitantes que tengan acceso en mayor o menor grado a la infraestructura de almacenamiento, transporte o procesamiento de datos e información de LA ALCALDIA DE APARTADO.

3. NORMATIVIDAD APLICABLE

El MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN se basa, principalmente, en las siguientes leyes, normas o decretos:

Ley, norma o decreto	Ámbito de aplicación
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
Ley 1341 de 2009	Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones TIC.
Ley 1581 de 2012	Protección de datos personales
Decreto 1377 de 2013	Reglamentación parcial de la Ley 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
Decreto único reglamentario 1078 de 2015	Define el componente de seguridad y privacidad de la información, como parte integral de la estrategia GEL

4. DEFINICIONES

ACCESO A LA INFORMACIÓN PÚBLICA: Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4)

ACTIVO: Cualquier cosa que tiene valor para la organización (ISO27001:2005)

ACTIVO DE INFORMACIÓN: Revisión de la efectividad de los controles establecidos y su apoyo al cumplimiento de los objetivos de seguridad.

ACUERDO DE CONFIDENCIALIDAD O CONTRATO DE CONFIDENCIALIDAD: Es un acuerdo legal entre al menos dos entidades para compartir material confidencial o conocimiento para ciertos propósitos, pero restringiendo su uso público.

ADMINISTRACIÓN DE RIESGOS: Conjunto de elementos de control que al interrelacionarse permiten a la Entidad Pública evaluar aquellos eventos negativos, tanto internos como externos, que puedan afectar o impedir el logro de sus objetivos institucionales o los eventos positivos, que permitan identificar oportunidades para un mejor cumplimiento de su función. Se constituye en el componente de control que al interactuar sus diferentes elementos le permite a la entidad pública autocontrolar aquellos eventos que pueden afectar el cumplimiento de sus objetivos. (Función Pública. Guía para la Administración del Riesgo. Bogotá, 2011)

AMENAZAS: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

ANÁLISIS DE RIESGO: Elemento de control que permite establecer la probabilidad de ocurrencia de los eventos positivos y/o negativos y el impacto de sus consecuencias, calificándolos y evaluándolos a fin de determinar la capacidad de la entidad pública para su aceptación y manejo. Se debe llevar a cabo un uso sistemático de la información disponible para determinar cuán frecuentemente pueden ocurrir eventos especificados y la magnitud de sus consecuencias (Función Pública. Guía para la Administración del Riesgo. Bogotá, 2011)

ARCHIVO: "Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3)".

AUDITORÍA | AUDITORIA INTERNA: Proceso sistemático, independiente y documentado para obtener evidencias que, al evaluarse de manera objetiva, permiten determinar la extensión en que se cumplen los criterios de auditoria, concebida para agregar valor y mejorar las operaciones de la Entidad.

AUTORIZACIÓN: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3)

AVISO DE PRIVACIDAD: Comunicación verbal o escrita generada por el Responsable, dirigida al Titular para el Tratamiento de sus datos personales, mediante la cual se le informa acerca de la existencia de las políticas de Tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las finalidades del Tratamiento que se pretende dar a los datos personales. (Ley 1581 de 2012)

BASES DE DATOS PERSONALES: Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3)

CIBERESPACIO: Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

CIBERSEGURIDAD: Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).

CLASIFICACIÓN DE LA INFORMACIÓN: "Es el ejercicio por medio del cual se determina que la información pertenece a uno de los niveles de clasificación estipulados en la Entidad. Tiene como objetivo asegurar que la información recibe el nivel de protección adecuado"

CONFIDENCIALIDAD: Propiedad que determina que la información sólo esté disponible y sea revelada a individuos, entidades o procesos autorizados (ISO/IEC 27000:2013)

CONTINGENCIA | DESASTRE: Interrupción de la capacidad de procesamiento y/o acceso a la misma desde cualquier medio, que puede generar dificultades en la operación normal de un negocio.

CONTRAMEDIDA (SALVAGUARDA): Medida o medidas de control que se establecen para evitar una situación de riesgo

CONTROL: Cualquier medida que tome la dirección y otras partes para gestionar los riesgos y aumentar la probabilidad de alcanzar los objetivos y metas establecidos. La dirección, planifica, organiza y dirige la

realización de las acciones suficientes para proporcionar una seguridad razonable de que se alcanzaran los objetivos y metas, de forma eficiente y económica.
CONTROL DE ACCESO: Mecanismos que en función de la identificación ya autenticada permite acceder a datos o recursos.

CUSTODIO: Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo encargado de administrar y hacer efectivos los controles de seguridad que el propietario de la información haya definido, tales como copias de seguridad, asignación privilegios de acceso, modificación y borrado (ISO/IEC 27002:2013).

DATO PÚBLICO: "Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3)"

DATOS ABIERTOS: "Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6)"

DATOS PERSONALES: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

DATOS PERSONALES MIXTOS: Es la información que contiene datos personales públicos junto con datos privados o sensibles.

DATOS PERSONALES PRIVADOS: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h).

DATOS SENSIBLES: "Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3)"

DERECHO A LA INTIMIDAD: Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).

DISPONIBILIDAD: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada, cuando ésta así lo requiera (ISO/IEC 27000:2013)

DOCUMENTO EN CONSTRUCCIÓN: No será considerada información pública aquella información preliminar y no definitiva, propia del proceso deliberatorio de un sujeto obligado en su calidad de tal.

ENCARGADO DEL TRATAMIENTO DE DATOS: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento. (Ley 1581 de 2012, art 3)
ETIQUETADO: El etiquetado de la información también se conoce como rotulado y tiene como propósito advertir de manera explícita a la persona que debe hacer la custodia de la información o quien la consulta, acerca del nivel de confidencialidad que tiene y por tanto las restricciones para su utilización y divulgación.

EVALUACIÓN DEL RIESGO: Su objetivo es comparar los resultados del análisis de riesgos con los controles establecidos, para determinar la zona de riesgo final (Función Pública. Guía para la Administración del Riesgo. Bogotá, 2011)

IMPACTO: Consecuencia que se produce al interior de cualquier organización, al materializarse una amenaza.

INFORMACIÓN: Conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen. (ley 1712 del 2014)

INFORMACIÓN PÚBLICA: Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal. (ley 1712 del 2014)

INFORMACIÓN PÚBLICA CLASIFICADA: "Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)"

INFORMACIÓN PÚBLICA RESERVADA: "Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)"

INTEGRIDAD: Propiedad de salvaguardar la exactitud y estado completo de los activos (ISO/IEC 27000:2013) ISO 27001. Estándar para sistemas de gestión de la seguridad de la información adoptado por ISO transcribiendo la segunda parte de BS 7799. Es certificable. Primera publicación en 2005.

LISTA DE CHEQUEO DE SEGURIDAD: Lista de apoyo para el auditor con los puntos a auditar, que ayuda a mantener claros los objetivos de la auditoría, sirve de evidencia del plan de auditoría, asegura su continuidad y profundidad y reduce los prejuicios del auditor y su carga de trabajo. Este tipo de listas también se pueden utilizar durante la implantación del SGSI para facilitar su desarrollo.

MECANISMOS DE PROTECCIÓN DE DATOS PERSONALES; Lo constituyen las distintas alternativas con que cuentan las entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anonimización o cifrado.

PARTES INTERESADAS (STAKEHOLDER): Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

PLAN DE CONTINUIDAD DEL NEGOCIO: Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).

PLAN DE TRATAMIENTO DE RIESGOS: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

POLÍTICA: Directriz emitida por la dirección que constituye la base de los procedimientos

POLÍTICA DE SEGURIDAD: Documento que establece el compromiso de la Dirección y el enfoque de la organización en la gestión de la seguridad de la información.

PRIVACIDAD: "En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente".

PROCEDIMIENTO DOCUMENTADO: Documento en donde se establece la forma para llevar a cabo una actividad o un proceso, en la cual se debe definir como mínimo quien hace que, donde, cuando, porque y como.

PROPIETARIO DE LA INFORMACIÓN: Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo que tiene la responsabilidad de garantizar que la información y los activos asociados con los servicios de procesamiento de información se clasifican adecuadamente, y de definir y revisar periódicamente las restricciones y clasificaciones del acceso, teniendo en cuenta las políticas aplicables sobre el control del acceso

REGISTRO: Documento que presenta resultados obtenidos o proporciona evidencia de actividades desempeñadas.

REGISTRO NACIONAL DE BASES DE DATOS: Directorio público de las bases de datos sujetas a Tratamiento que operan en el país. (Ley 1581 de 2012, art 25)

RESPONSABILIDAD DEMOSTRADA: Conducta desplegada por los Responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.

RESPONSABLE DEL TRATAMIENTO DE DATOS: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art 3).

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).

SEGURIDAD DE LA INFORMACIÓN: Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN SGSI: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una

política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).
TABLA DE RETENCIÓN DOCUMENTAL: Listado de series con sus correspondientes tipos documentales, a las cuales se asigna el tiempo de permanencia en cada etapa del ciclo vital de los documentos

TITULARES DE LA INFORMACIÓN: Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3)

TRANSFERENCIA: La transferencia de datos tiene lugar cuando el Responsable y/o Encargado del Tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es Responsable del Tratamiento y se encuentra dentro o fuera del país (Ley 1581 de 2012)

TRANSMISIÓN: Tratamiento de datos personales que implica la comunicación de los mismos dentro o fuera del territorio de la República de Colombia cuando tenga por objeto la realización de un Tratamiento por el Encargado por cuenta del Responsable (Ley 1581 de 2012)

TRATAMIENTO DE DATOS PERSONALES: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).

TRAZABILIDAD: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).

TRIADA DE SEGURIDAD: Denominación que se da a las tres características fundamentales de la seguridad de la información: CONFIDENCIALIDAD, DISPONIBILIDAD e INTEGRIDAD.

USUARIO: Cualquier persona, entidad, cargo, proceso, sistema automatizado o grupo de trabajo, que genere, obtenga, transforme, conserve o utilice información en papel o en medio digital, físicamente o a través de las Redes de datos y los sistemas de información de la Unidad, para propósitos propios de su labor y que tendrán el derecho manifiesto de uso dentro del inventario de información (ISO/IEC 27002:2013)

VALOR JURIDICO: Nivel de protección legal que requiere la información para el logro de objetivos misionales.

VALOR ORGANIZACIONAL: Nivel de importancia de la información en el logro de los objetivos misionales.

VALORACIÓN DE LOS RIESGOS: La valoración del riesgo es el producto de confrontar los resultados de la evaluación del riesgo con los controles identificados, esto se hace con el objetivo de establecer prioridades para su manejo y para la fijación de políticas (Función Pública. Guía para la Administración del Riesgo. Bogotá, 2011)

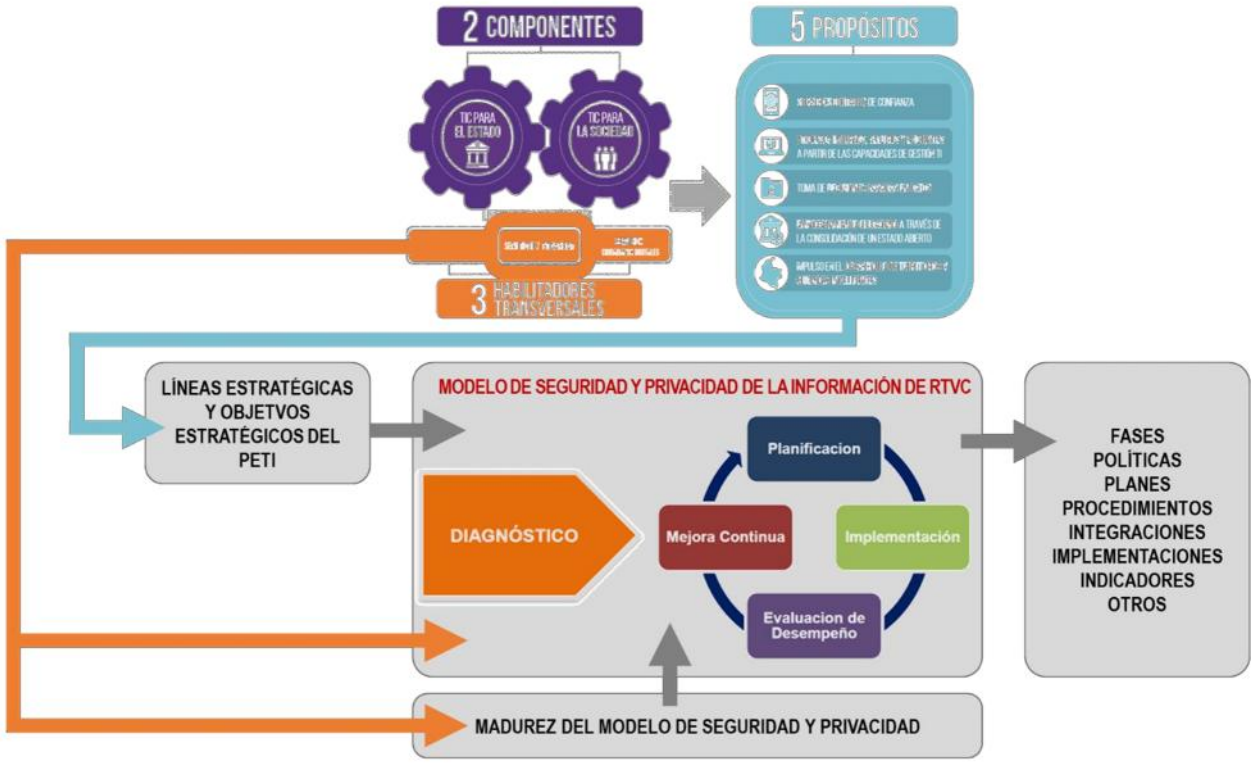
VULNERABILIDAD: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

TRATAMIENTO DEL RIESGO: El resultado obtenido a través de la valoración del riesgo es denominado también Valoración del riesgo de proceso ya que se “involucra la selección de una o más opciones para modificar los riesgos y la implementación de tales acciones” así el desplazamiento dentro de la Matriz de Evaluación y Calificación determinará finalmente la selección de las opciones de tratamiento del riesgo, así:, Evitar el riesgo, Reducir el riesgo, Compartir o transferir el riesgo, Asumir un riesgo.

DECLARACIÓN DE APLICABILIDAD: Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).

5. MARCO NORMATIVO Y CORPORATIVO DEL MODELO

La siguiente figura muestra cómo se articula el MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE LA ALCALDIA DE APARTADO, con su MODELO DE MADUREZ, con las normas de GOBIERNO DIGITAL y con los OBJETI VOS ESTRATÉGICOS DEL PETI:



Articulación del modelo de seguridad y privacidad de la información de LA ALCALDIA DE APARTADO

5.1. NORMA GEL DE SEGURIDAD

La nueva estrategia de GOBIERNO DIGITAL le provee al MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE LA ALCALDIA DE APARTADO lo siguiente:

- Lineamientos gubernamentales al Plan Estratégico de TI (PETI) el cual, a su vez, provee las líneas estratégicas y los objetivos estratégicos para el cumplimiento de la seguridad y privacidad de la información.
- Lineamientos gubernamentales sobre los propósitos 5 propósitos del GOBIERNO DIGITAL. Estos propósitos también influyen en la generación de las líneas estratégicas de LA ALCALDIA DE APARTADO.
- Lineamientos gubernamentales al MODELO DE SEGURIDAD Y PRIVACIDAD desde el habilitador transversal SEGURIDAD Y PRIVACIDAD. Estos lineamientos permiten establecer cuán adelantado está el modelo respecto de lo esperado por la estrategia de GOBIERNO DIGITAL

5.2. OBJETIVOS ESTRATÉGICOS DEL PETI

El MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE LA ALCALDIA DE APARTADO se enmarca en la línea estratégica "CONVERGENCIA TECNOLÓGICA CON CALIDAD Y SEGURIDAD" del PETI y cuyo propósito es el de "buscar que los contenidos convergentes que se entregan por parte de la dirección de TC a los usuarios finales no presenten problemas de disponibilidad, de calidad, de acceso, de tiempo de respuesta u otros"

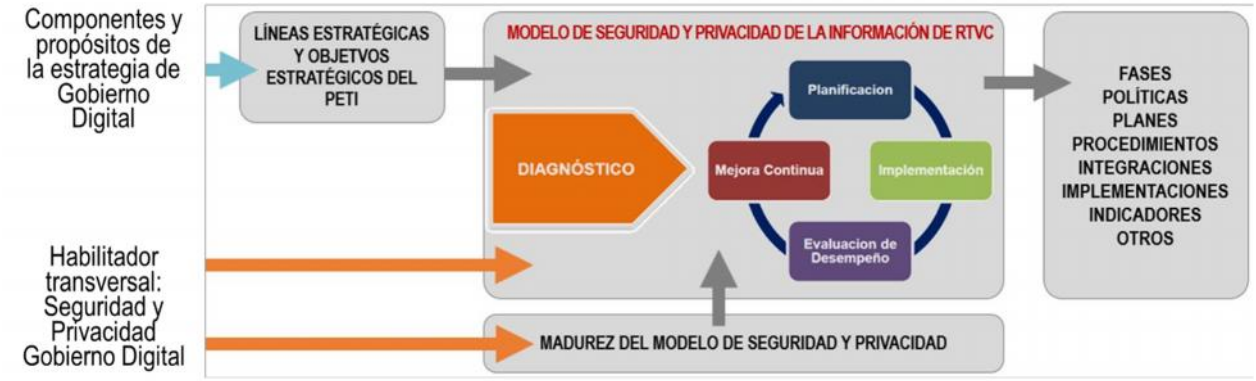
5.3. MADUREZ DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN EN LA ALCALDIA DE APARTADO

La madurez del MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN EN LA ALCALDIA DE APARTADO se evalúa con base en el modelo propuesto por la estrategia de Gobierno Digital del MINTIC. En este sentido, se toman las variables y mediciones sugeridas, así como los ejercicios previos de diagnóstico de años anteriores.

6. MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN PARA LA ALCALDIA DE APARTADO

La siguiente figura muestra el modelo de seguridad y privacidad de la información de LA ALCALDIA DE APARTADO y cada uno de sus componentes, entradas y salidas.

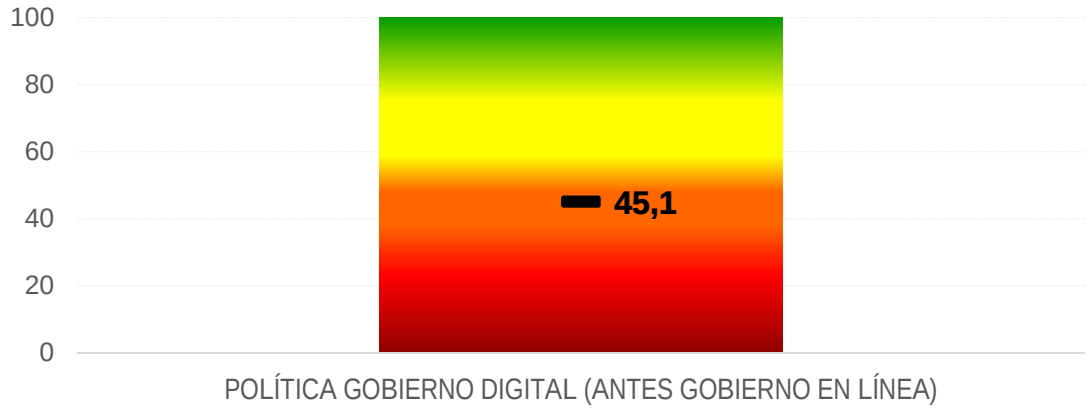
El modelo se basa en uno de los 3 habilitadores transversales de la estrategia de Gobierno Digital del MINTIC:



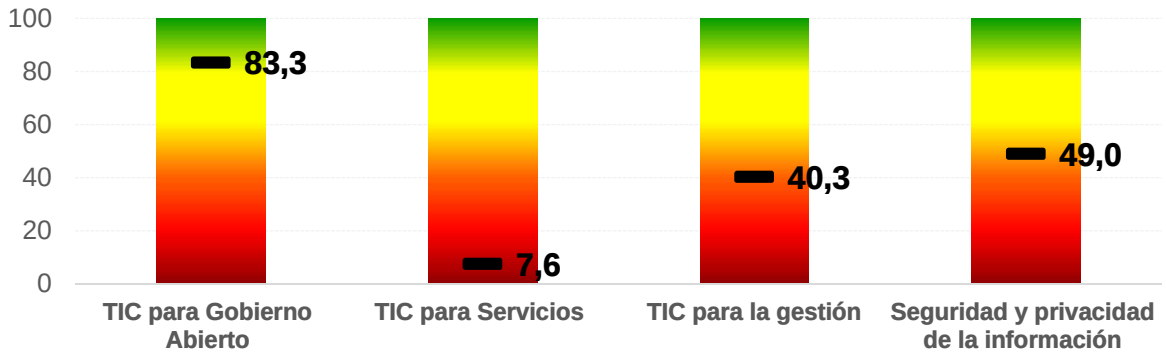
Modelo de seguridad y privacidad de la información de la Alcaldía de Apartado

6.1 DIAGNÓSTICO

LA ALCALDIA DE APARTADO para el 2018 realizó el audiagnóstico de la POLITICA DE GOBIERNO DIGITAL establecida en MIPG, dando como resultado las siguientes gráficas para cada componente:

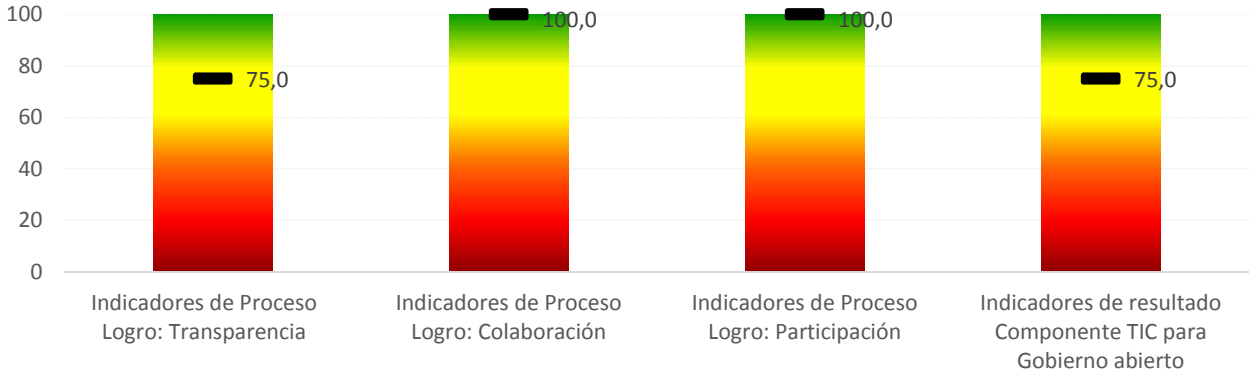


CLASIFICACION POR COMPONENTES

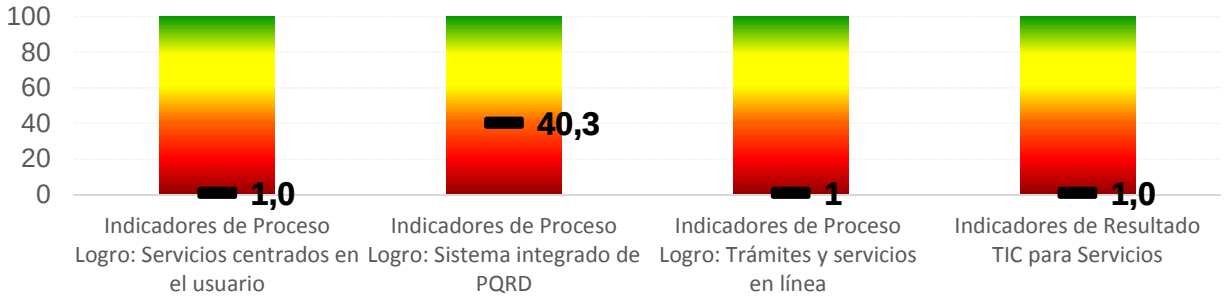


CALIFICACION POR CATEGORIAS

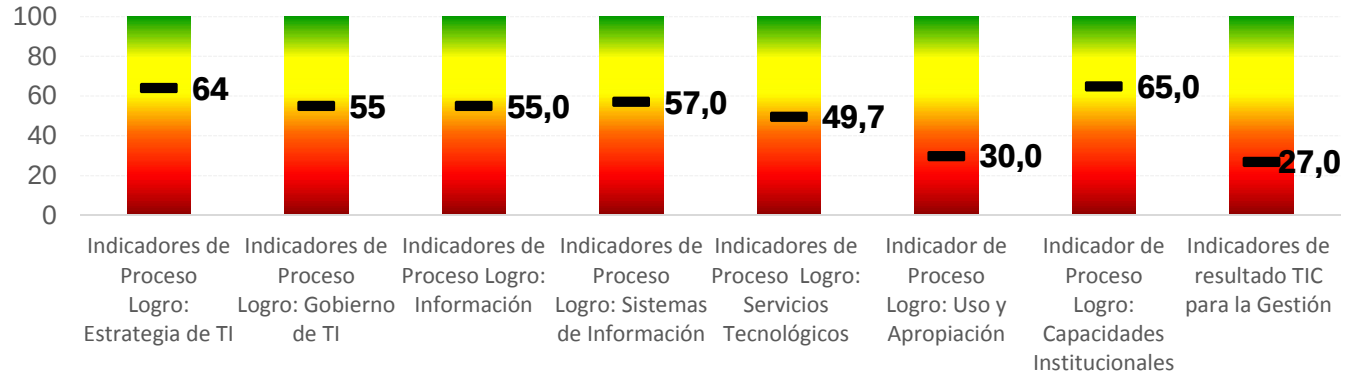
TIC PARA GOBIERNO ABIERTO



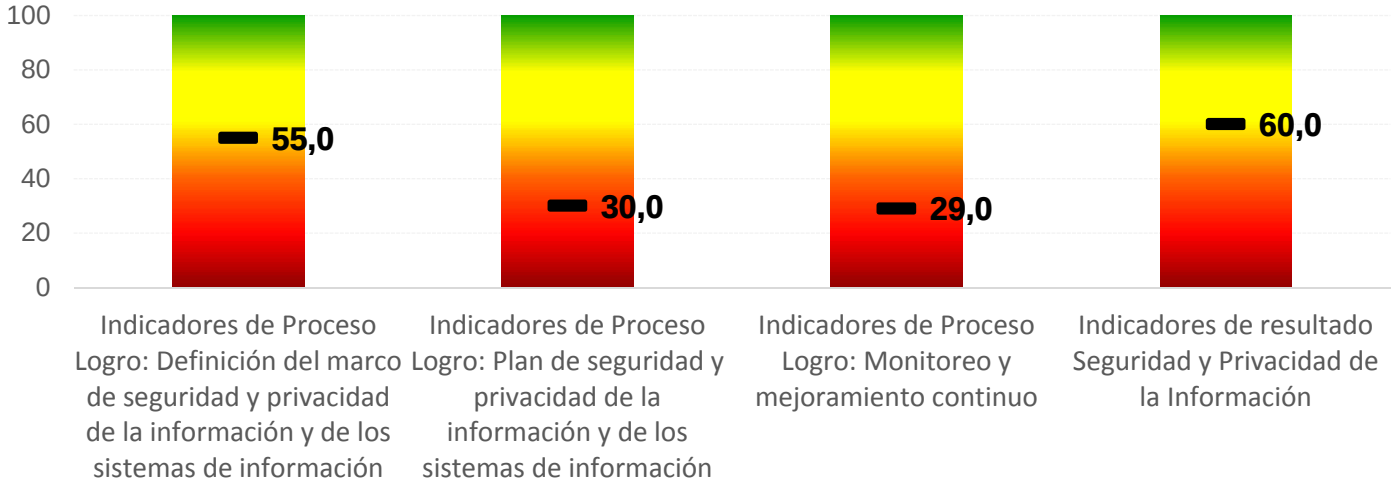
TIC PARA SERVICIOS



TIC PARA LA GESTIÓN



SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN



Para la implementación del Modelo de Privacidad y seguridad de la información se ha construido El Plan de Seguridad y Privacidad de la Información donde se desarrollan todas las actividades y que se encuentra como documento anexo para poder cumplir en el mediano plazo con las directrices del Mintic.

6.2 PLANEACIÓN

6.2.1 PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

- Política de seguridad y privacidad de la información. Se encuentra en construcción la Política de seguridad y privacidad de la Información

- Procedimientos de Seguridad de la Información

A continuación, se relacionan el estado de implementación de cada uno de los controles que propone el Modelo MSPI a través de la Guía No. 3 (Versión 1.0.0 del 25/04/2016)

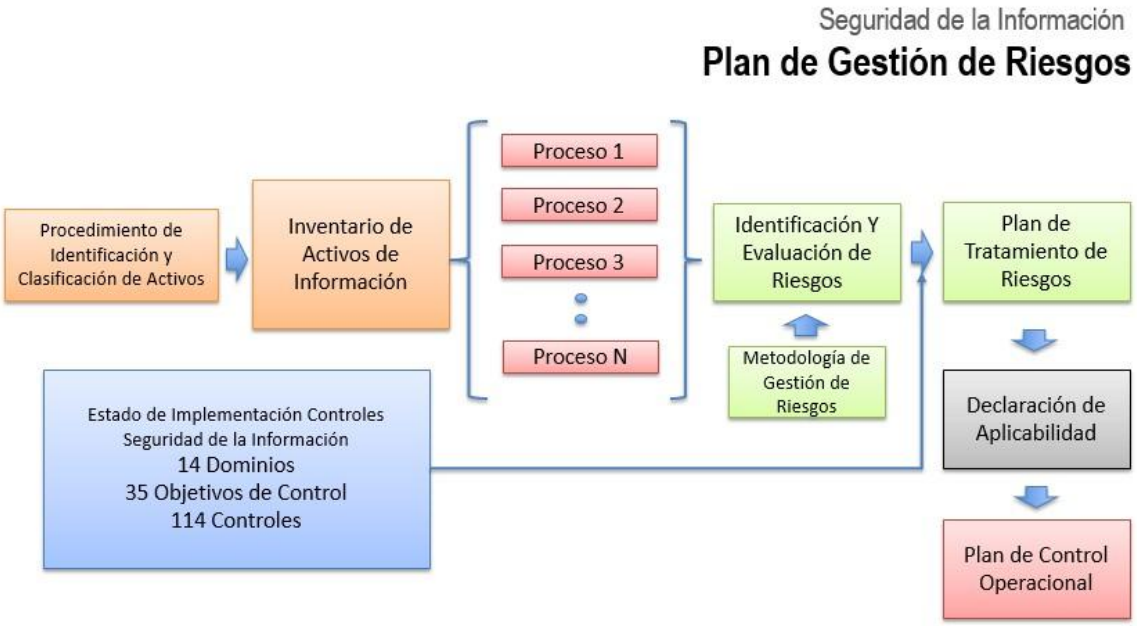
Los procedimientos referenciados en Construcción hacen parte de la Gestión del año 2019-2020

DOMINIO	No.	PROCEDIMIENTO	ESTADO
Seguridad Del Recurso Humano	1	Procedimiento De Capacitación Y Sensibilización Del Personal	Aprobado: P-SGE-TH-15
	2	Procedimiento De Ingreso Y Desvinculación Del Personal	Aprobado: P-SGE-TH-13 y : P-SGE-TH-14
Gestión De Activos	3	Procedimiento De Identificación Y Clasificación De Activos	En construcción
Control De Acceso	4	Procedimiento Para Ingreso Seguro A Los Sistemas De Información	En construcción
	5	Procedimiento De Gestión De Usuarios Y Contraseñas	Esta definido como politica
Criptografía	6	Procedimiento De Controles Criptográficos	No se ha realizado
	7	Procedimiento De Gestión De Llaves Criptográficas	No se ha realizado
Seguridad Física Y Del Entorno	8	Procedimiento De Control De Acceso Físico	No se ha realizado
	9	Procedimiento De Protección De Activos	No se ha realizado
	10	Procedimiento De Retiro De Activos	No se ha realizado
	11	Procedimiento De Mantenimiento De Equipos:	Aprobado P-SGE-GI-06

Seguridad De Las Operaciones	12	Procedimiento De Gestión De Cambios:	En construcion
	13	Procedimiento De Gestión De Capacidad	No se ha realizado
	14	Procedimiento De Separación De Ambientes	No se ha realizado
	15	Procedimiento De Protección Contra Códigos Maliciosos	No se ha realizado
Seguridad De Las Comunicaciones	16	Procedimiento De Aseguramiento De Servicios En La Red	No se ha realizado
	17	Procedimiento De Transferencia De Información	No se ha realizado
Relaciones Con Los Proveedores	18	Procedimiento Para El Tratamiento De La Seguridad En Los Acuerdos Con Los Proveedores	No se ha realizado
Adquisición, Desarrollo Y Mantenimiento De Sistemas De Información	19	Procedimiento Adquisición, Desarrollo Y Mantenimiento De Software	No se ha realizado
	20	Procedimiento De Control Software	No se ha realizado
Gestión De Incidentes De Seguridad De La Información	21	Procedimiento De Gestión De Incidentes De Seguridad De La Información	onstrucción
Aspectos De Seguridad De La Información De La Gestión De Continuidad De Negocio	22	Procedimiento De Gestión De La Continuidad De Negocio	No se ha realizado

6.2.2 IDENTIFICACIÓN, VALORACIÓN Y TRATAMIENTO DE RIESGOS

La siguiente figura muestra el esquema de identificación, valoración y tratamiento de riesgos relacionados con el MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN:



Tratamiento de riesgos de seguridad y privacidad en LA ALCALDIA DE APARTADO

De acuerdo con el inventario de activos de información, los líderes de procesos deben revisar anualmente los cambios en el direccionamiento estratégico o en el entorno y como estos pueden generar nuevos riesgos de Seguridad y Privacidad de la Información o modificar los que ya se tienen identificados en cada uno de sus procesos, para la actualización de riesgos de su proceso. Así como realizar una revisión del adecuado diseño y ejecución de los controles establecidos para la mitigación de los riesgos, tomando como referencia la tabla de Controles propuesta por el MSPI.

6.3 IMPLEMENTACIÓN

Aquí se indica cómo se implementa el modelo y lo que se espera obtener en los siguientes años. Recordar que la implementación tiene cuatro temas principales:

6.3.1 PLANIFICACIÓN Y CONTROL OPERACIONAL

La Alcaldía de Apartado debe planificar, implementar y controlar los procesos necesarios para cumplir con los requisitos de seguridad y privacidad de la información que permitan implementar las acciones determinadas en el plan de tratamiento de riesgos 2019. Acciones que serán ejecutadas en la vigencia 2019 y 2020, según se definan por los líderes de los procesos, el comité de seguridad y demás responsables.

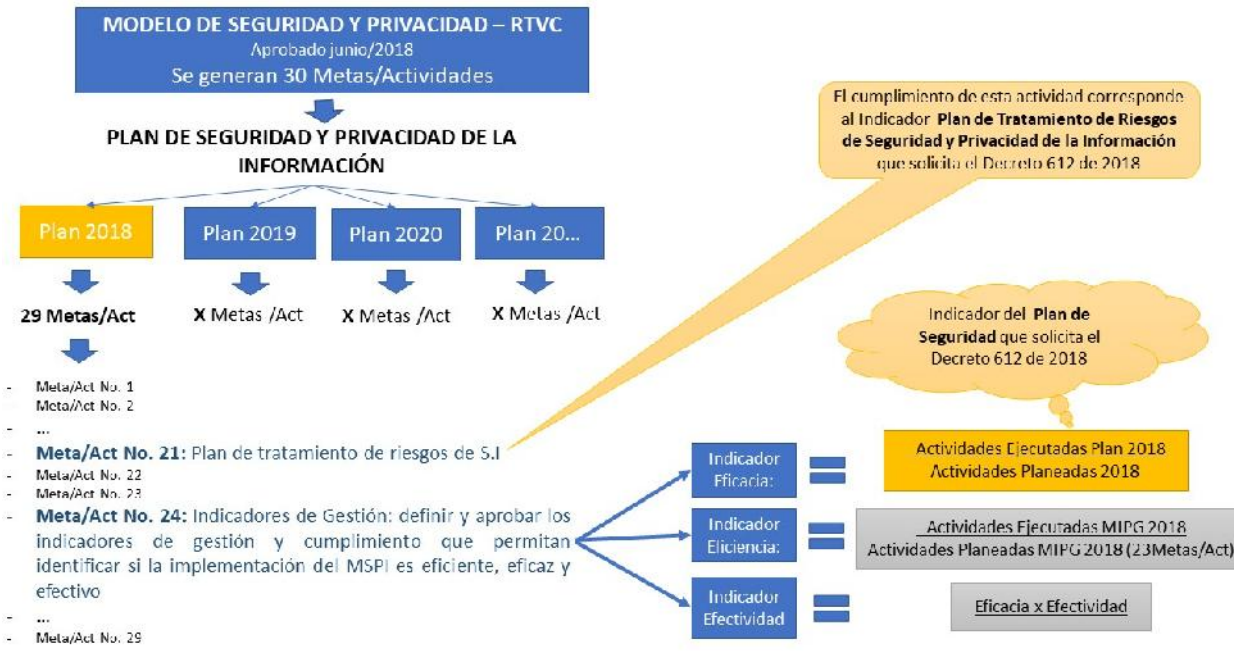
Se debe tener información documentada en la medida necesaria para tener la confianza en que los procesos se han llevado a cabo según lo planificado, adicionalmente, deberá llevarse un control de cambios que le permitan tomar acciones para mitigar efectos adversos cuando sea necesario.

6.3.2 IMPLEMENTACIÓN DEL CONTROL DE RIESGOS

El plan de tratamiento de riesgos de seguridad de la información debe identificar los controles a aplicar para llevar cada uno de los riesgos a un nivel aceptable para la entidad, en donde la base para ejecutar esta actividad es la Guía No 8 - de controles de seguridad y privacidad del MSPI. En donde la aplicación de los controles sobre los riesgos detectados debe estar aprobada por el responsable de cada proceso. El estado de implementación de los controles se revisará periódicamente y estará alineado a los planes de acción propuestos la revisión y actualización de la matriz de riesgos de seguridad y privacidad de la información

6.3.3 INDICADORES DE GESTIÓN

La siguiente figura muestra la estructura de los indicadores de gestión definidos para la medición y seguimiento del modelo:



6.3.4 PLAN DE TRANSICIÓN IPV4 A IPV6

No se ha iniciado con la elaboración del Plan transición

7.4 EVALUACIÓN DE DESEMPEÑO

No se ha realizado la evaluación y monitoreo periódico del modelo. En el cronograma adjunto a este documento se encuentra la fecha estimada para ejecutar esta actividad.

7.4.1 PLAN DE REVISIÓN Y SEGUIMIENTO A LA IMPLEMENTACIÓN DEL MODELO

ACTIVIDAD	PERIODICIDAD MINIMA DE EJECUCIÓN
Revisión de la efectividad de los controles establecidos y su apoyo al cumplimiento de los objetivos de seguridad.	Dos veces al año
Revisión de la evaluación de los niveles de riesgo y riesgo residual después de la aplicación de controles y medidas administrativas.	Una vez al año
Seguimiento a la programación y ejecución de las actividades de autorías internas y externas del MSPI.	Una vez al año

ACTIVIDAD	PERIODICIDAD MINIMA DE EJECUCIÓN
Seguimiento al alcance y a la implementación del MSPI.	Dos veces al año
Seguimiento a los registros de acciones y eventos / incidentes que podrían tener impacto en la eficacia o desempeño de la seguridad de la información al interior de la entidad.	Trimestralmente
Medición de los indicadores de gestión del MSPI	Cuatrimestralmente
Revisiones de acciones o planes de mejora (solo aplica en la segunda revisión del MSPI)	Una vez al año

7.4.2 PLAN DE EJECUCIÓN DE AUDITORÍAS

Auditorías Internas: El plan de ejecución de auditorías nace producto del Programa Anual de auditorías de Control Interno y/o el programa de auditorías internas de calidad. A cargo del Comité de Coordinación de Control Interno.

Los planes del 2017 se encuentran disponibles en la página web oficial de la entidad:

http://www.apartado-antioquia.gov.co/Transparencia/Paginas/Control-y-Rendicion-de-Cuentas.aspx

7.5 PLAN DE MEJORA CONTINUA

Las acciones de mejora (acciones preventivas, correctivas y/o de mejora) correspondientes a las auditorías al proceso de Gestión Tic , son tratadas de acuerdo con el Proceso de Mejora Continua y son documentadas en los planes de mejoramiento de la Alcaldía de Apartado.

8. REFERENCIAS Y DOCUMENTOS ASOCIADOS

El MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN PARA LA ALCALDIA DE APARTADO se articula con las siguientes referencias y documentos asociados:

- MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN. Departamento Administrativo de Planeación Nacional
- ESTRATEGIA DE GOBIERNO DIGITAL. Ministerio de las TIC
- PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. Decreto 612 de 2018 - DAFP
- PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. Decreto 612 de 2018 - DAFP

Marta C. Rivera

MARTA CECILIA RIVERA HIGUITA
Subsecretario de Tics y Gestión Documental.

Elaboró: Marta C Rivera