PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

TABLA DE CONTENIDO

INTRODUCCIÓN

Hoy en día, la información está definida como uno de los activos más valiosos y primordiales para cualquier tipo de organización, la cual, sólo tiene sentido cuando está disponible y es utilizada de forma adecuada, integra, oportuna, responsable y segura, lo que implica, que es necesario que las organizaciones tengan una adecuada gestión de sus recursos y activos de información con el objetivo de asegurar y controlar el debido acceso, tratamiento y uso de la información.

El aseguramiento y la protección de la seguridad de la información de las organizaciones y de los datos de carácter personal de los usuarios, representan un reto al momento de pretender garantizar su confidencialidad, integridad, disponibilidad y privacidad, razón por la cual, la seguridad de la información se ha convertido en uno de los aspectos de mayor preocupación a nivel mundial. Cualquier tipo de organización independiente de su tamaño y naturaleza, debe ser consciente que la diversidad de amenazas existentes que actualmente atentan contra la seguridad y privacidad de la información, representan un riesgo que al materializarse no solo les puede acarrear costos económicos, sanciónales legales, afectación de su imagen y reputación, sino que pueden afectar la continuidad y supervivencia del negocio.

Lo anterior, sumando a un entorno tecnológico en donde cada día se hace más complejo de administrar y asegurar, genera que cada vez más la seguridad de la información forme parte de los objetivos y planes estratégicos de las organizaciones. Por lo tanto, es indispensable que los responsables dentro de las organizaciones encargados de velar por la protección y seguridad de sus recursos, infraestructura e información, contantemente estén adoptando, implementando y mejorando medidas de seguridad orientadas a prevenir y/o detectar los riesgos que pueden llegar a comprometer la disponibilidad, integridad y confidencialidad de los activos de información a través de los cuales se gestiona la información del negocio, independientemente si está es de carácter organizacional o personal, o de tipo pública o privada. En la medida que las organizaciones tengan una visión general de los riesgos que pueden afectar la seguridad y privacidad de la información, podrán establecer controles y medidas efectivas, viables y transversales con el propósito de salvaguardar la disponibilidad, integridad y confidencialidad tanto de la información del negocio como los datos de carácter personal de sus empleados, usuarios y partes interesadas. Es indispensable que las organizaciones realicen una adecuada identificación, clasificación, valoración, gestión y tratamiento de los riegos que pueden afectar su seguridad, con el propósito de implementar medidas y controles efectivos que les permitan estar preparados ante situaciones adversas que puedan comprometer tanto la seguridad física y lógica de sus instalaciones, personas, recursos y sistemas, como la seguridad de su información.

1. OBJETIVOS

1.1. OBJETIVO GENERAL

Establecer un Plan de Seguridad y Privacidad de la Información que integre la gestión de seguridad de la información con la estrategia organizacional que permita apoyar los objetivos misionales de la Alcaldía de Acacías, a través de la gestión adecuada de los riesgos y así fortalecer la seguridad en los componentes de integridad, disponibilidad y confidencialidad.

1.2. OBJETIVOS ESPECÍFICOS

- Definir las etapas para establecer la estrategia de seguridad de la información de la entidad.

- Establecer lineamientos para la implementación y/o adopción de mejores prácticas de seguridad de la información en la entidad.

- Optimizar la gestión de la seguridad de la información al interior de la entidad.

2. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE LA ALCALDÍA DE ACACÍAS (Resolución 1084 de 2018)

La Política de Seguridad y Privacidad de la Información es la declaración general que representa la posición de la administración de la Alcaldía de Acacias Meta con respecto a la protección de los activos de información (los funcionarios, contratistas, terceros, la información, los procesos, las tecnologías de información incluido el hardware y el software), que soportan los procesos de la Entidad y apoyan la implementación del Modelo de Seguridad y Privacidad de la Información, por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

3. OBJETIVOS ESPECÍFICOS DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE LA ALCALDÍA DE ACACÍAS (Resolución 1084 de 2018)

1. Proteger los activos de información.
2. Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de la Entidad
3. Cumplir con los principios de la función administrativa.
4. Mantener la confianza de los funcionarios, contratistas y terceros.
5. Apoyar la innovación tecnológica.
6. Garantizar la continuidad del negocio frente a incidentes.

4. ALCANCE DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE LA ALCALDÍA DE ACACÍAS

Las políticas de seguridad de la información aplican en todos los aspectos administrativos y de control que deben ser cumplidos por las partes interesadas de la Alcaldía Municipal de Acacías Meta, para alcanzar un nivel de protección de la información satisfactorio.

5. MANUAL DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE LA ALCALDÍA DE ACACÍAS

5.1. OBJETIVO DEL MANUAL DE LA POLÍTICA

Brindar las directrices y lineamientos necesarios que deben cumplir las partes interesadas de la Alcaldía de Acacías, con el fin de garantizar la disponibilidad, integridad y confidencialidad de la información en la Entidad.

5.2. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

5.2.1. Políticas de dispositivos móviles, teletrabajo y trabajo en casa

- La Entidad establece las condiciones para el uso seguro de los dispositivos móviles (portátiles, teléfonos, inteligentes, tabletas, entre otros) institucionales que hagan uso de servicios de la Entidad como son: Establecer contraseñas de acceso robustas, cifrar la información almacenada, mantener el dispositivo móvil con el sistema operativo siempre actualizado y con un antivirus activo.

- Es responsabilidad del servidor público al que se le asignó el dispositivo móvil evitar la instalación de programas desde fuentes desconocidas, evitar el uso de redes inalámbricas públicas, y mantener desactivadas las redes inalámbricas como WIFI, Bluetooth, o infrarrojos en los dispositivos móviles institucionales asignados.

- Los servidores públicos deben evitar conectar los dispositivos móviles institucionales a puertos USB de computadores públicos, hoteles o cafés internet, terminales, y demás sitios de acceso público.

- Todos los dispositivos móviles propiedad de la Entidad pueden ser monitoreados y sometidos a la aplicación de controles en cuanto a tipo, versión de aplicaciones instaladas, contenido restringido y de ser necesario se podrá restringir conexiones hacia ciertos servicios de información que sean considerados maliciosos.

- Toda información gestionada por la Entidad, y que sea accedida remotamente debe ser utilizada solamente para el cumplimiento de las funciones del cargo o de las obligaciones contractuales con esta.

- La Entidad brinda los lineamientos de seguridad digital para la protección de la

información a la que se tiene acceso, se procesa o almacena en lugares en los que se realiza Teletrabajo o Trabajo En Casa y se hace uso de los recursos tecnológicos autorizados por la Entidad para el desarrollo de las actividades de Teletrabajo.

- La Entidad establece los requerimientos para autorizar conexiones remotas a la infraestructura tecnológica necesaria para la ejecución de las funciones de los servidores públicos y contratistas de la entidad, garantizando las herramientas y controles para proteger la confidencialidad, integridad y disponibilidad de las conexiones remotas.

5.2.2. Políticas de seguridad de los recursos humanos

- El área que realice la contratación de personal en la Entidad realiza las verificaciones de los antecedentes (Procuraduría, Contraloría, Policía) de los candidatos al cargo, la formación académica, experiencia y demás información que se requiera, de acuerdo con las leyes, reglamentos de la Entidad y ética pertinente.

- Todo servidor público y contratista debe recibir inducción y procesos periódicos de sensibilización en seguridad y privacidad de la información en la Entidad.

- La Entidad establece directrices para asegurar que los servidores públicos y contratistas tengan conocimiento sobre los derechos, deberes y responsabilidades en relación a la seguridad de la información.

- Los acuerdos contractuales entre la Entidad y los servidores públicos o contratistas especifican el cumplimiento a los lineamientos de seguridad de la información establecidos en la Entidad.

- El proceso de Talento Humano y/o contratación realiza el proceso de desvinculación, licencias, vacaciones o cambio de labores de los servidores públicos y contratistas llevando a cabo los procedimientos y ejecutando los controles establecidos para tal fin. Así mismo, los directores, jefes, supervisores de contrato o líderes deben informar la desvinculación o cambio de labores de acuerdo con los procedimientos, está información debe ser entregada oportunamente al proceso de TI.

- La Entidad debe incorporar los roles y responsabilidades en seguridad de la información dentro de las funciones y obligaciones contractuales de los Colaboradores y Terceros.

- El incumplimiento o la violación de las políticas de seguridad de la información de la Entidad, por parte de los Colaboradores o Terceros, se les aplicará lo establecido en el proceso de investigaciones disciplinarias

5.2.3. Políticas gestión de activos

- La Entidad establece los métodos de identificación, clasificación y valoración de activos de información, así como la definición de la asignación de responsabilidades, manteniendo mecanismos acordes para el control de riesgos de la información.

- Cada activo de información de la Entidad debe tener un responsable que debe velar por su seguridad. Los propietarios de la información deben garantizar que todos los activos de información reciban un apropiado nivel de protección basados en su valor de confidencialidad, integridad, disponibilidad, riesgos identificados y/o requerimientos legales de retención.

- Los servidores públicos y contratistas deben hacer la devolución de los activos de información asignados a su cargo una vez finalice la relación contractual con la Entidad.

- Todos los activos de información deben contar con un responsable, que asegure la protección de la información y los datos que son almacenados en cada uno de ellos.

5.2.4. Políticas control de acceso

- La Entidad define los lineamientos para asegurar un acceso controlado, físico o lógico, a la información y plataforma tecnológica, considerándolas importantes para el sistema de gestión de seguridad de la información.

- La Entidad establece procedimientos la creación de datos de acceso, suministro de accesos a la información, revisión periódica de los accesos otorgados, y desactivación o eliminación de las cuentas de usuario una vez finalizada la relación contractual.

- Si una Entidad, empresa o personal externo requiere acceso a información sensible o crítica, se deben suscribir acuerdos de confidencialidad o de no divulgación para la salvaguarda de la información, así como el cumplimiento de la normatividad vigente para la Entidad.

- Las claves son de uso personal e intransferible y es responsabilidad del usuario el uso de las credenciales asignadas.

- Todos los usuarios en su primer inicio de sesión deben cambiar las contraseñas suministradas de acceso a la red, sistemas de información, aplicaciones, entre otros.

5.2.5. Políticas seguridad física y del entorno

- Las oficinas administrativas, áreas de procesamiento de información, equipos tecnológicos y de soporte, información de medios físicos entre otros, son base para el cumplimiento de los objetivos de la Entidad, por tanto, se establecen y mantienen

controles para resguardar la seguridad de las instalaciones y ambientes de trabajo, el acceso a las áreas.

- Los equipos de cómputo que pasen a un estado de retiro o se requieran para la reutilización deberán cumplir los siguientes lineamientos:

- Al momento de retirar un equipo en la organización (almacén), el proceso de TI realiza una copia de respaldo de la información almacenada en este activo.

- El proceso de TI realiza el proceso de borrado seguro de la información almacenada en los equipos que van a ser cedidos o reutilizados en la organización.

- Para todos los usuarios de las aplicaciones y sistemas de información de la Entidad, es obligatorio que las sesiones sean cerradas al finalizar las actividades y no se deben dejar abiertas o desatendidas**.**

5.2.6. Políticas de controles criptográficos

- El acceso remoto a la red y los sistemas de información de la Entidad desde una red externa, será a través de conexiones seguras.

- Se debe contar con buenas prácticas para la gestión de llaves.

5.2.7. Políticas seguridad en las operaciones

- La Entidad garantiza que las operaciones Tecnológicas se gesten de forma correctas y se brinde seguridad a las instalaciones de procesamiento de información.

- Según la clasificación de la información establecida por la Entidad, se establecen las medidas de respaldo de la información a través de mecanismos como cintas, discos de almacenamiento o en la nube.

5.2.8. Políticas seguridad de las comunicaciones

- El Proceso de TI realiza el bloqueo a las páginas de contenido para adultos, mensajería instantánea y demás páginas que no sean de uso institucional, mediante el uso de servidor proxy, firewall o control que mejor se ajuste a la necesidad.

- El proceso de TI implementa y mantiene la separación de las redes virtuales para garantizar la confidencialidad de la información en la red de telecomunicaciones de la Entidad.

5.2.9. Políticas adquisición, desarrollo y mantenimiento de sistemas

- La Entidad garantiza que los sistemas de información estén asociados a lineamientos, procesos, buenas prácticas y demás requisitos que sirvan para regular los desarrollos de software internos en un ambiente controlado, así mismo se identifican y gestionan los posibles riesgos referentes a seguridad de la información durante todo el ciclo de vida del software.

- La Entidad busca que la Seguridad de la Información sea parte integral dentro ciclo de vida de desarrollo de los sistemas de información y en la adquisición de aquellos que presen servicios a la Entidad, para ello establece el procedimiento de desarrollo seguro de software, la revisión técnica y de seguridad de las aplicaciones para detectar vulnerabilidades antes de salir a producción y la aplicación del procedimiento gestión de cambios.

- La Entidad establece controles técnicos para proteger la confidencialidad, integridad y disponibilidad de los sistemas de información que son públicos mediante herramientas de seguridad perimetral de proveedores o de forma local.

5.2.10. Políticas relaciones con los proveedores

- Para proveedores críticos de tecnología, así como de procesos misionales, la Entidad exige que cuente con planes de continuidad de negocio y recuperación de desastres definidos e implementados, de modo que proveedor contratado puedan responder ante eventuales escenarios que afecten el suministro de servicios o productos a la Entidad.

- Cualquier cambio que se realice con algún proveedor crítico de TI o de los procesos misionales, debe aplicarse mediante el procedimiento de gestión de cambios establecido en la Entidad.

5.2.11. Políticas gestión de incidentes

La Entidad debe asegurarse que todos los servidores públicos y contratistas conocen y aplican un procedimiento rápido y eficaz para actuar ante cualquier incidente en materia de seguridad de la información. Por lo tanto, se debe establecer los mecanismos para registrar los incidentes con sus pruebas y evidencias con objeto de estudiar su origen y evitar que ocurran en un futuro.

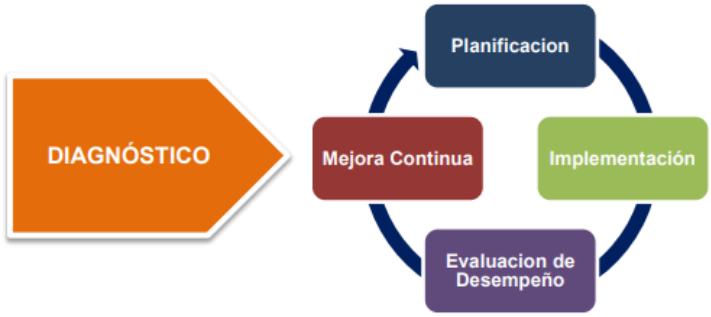
La Entidad establece y ejecuta procedimientos para identificar, analizar, valorar y dar un tratamiento adecuado a los incidentes, y que se hace una adecuada evaluación del impacto en el negocio de los incidentes de seguridad de la información.

5.2.12. Políticas cumplimiento

La Entidad gestiona la seguridad de la información de tal forma que se dé cumplimiento adecuado a la legislación vigente. Para esto, analiza los requisitos legales aplicables a la información, incluyendo los derechos de propiedad intelectual, protección de datos personales, los tiempos de retención de registros y los delitos informáticos.

6. CICLO DE OPERACIÓN

El Modelo de Seguridad y Privacidad de la Información de la Política de Gobierno Digital contempla el siguiente ciclo de operación que contempla cinco (5) fases, las cuales permiten que las entidades puedan gestionar adecuadamente la seguridad y privacidad de sus activos de información



Ciclo de operación Modelo de Seguridad y Privacidad de la Información
Fuente:https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

- ✓ **Fase Diagnostico:** Permite identificar el estado actual de la entidad con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información.

- ✓ **Fase Planificación (Planear**): En esta fase se establecen los objetivos a alcanzar y las actividades del proceso susceptibles de mejora, así como los indicadores de medición para controlar y cuantificar los objetivos.

- ✓ **Fase Implementación (Hacer):** En esta fase se ejecuta el plan establecido que consiste en implementar las acciones para lograr mejoras planteadas.

- ✓ **Fase Evaluación de desempeño (Verificar):** Una vez implantada la mejora, se establece un periodo de prueba para verificar el correcto funcionamiento de las acciones implementadas.

- ✓ **Fase Mejora Continua (Actuar):** Se analizan los resultados de las acciones implementadas y si estas no se cumplen los objetivos definidos se analizan las causas de las desviaciones y se generan los respectivos planes de acciones.

7. COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

Las funciones del comité de Seguridad de la Información son asumidas por el Comité Institucional de Gestión y Desempeño de la Alcaldía de Acacías-Meta, mediante Decreto No. 189 de 2018.

8. PLAN DE IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El Plan de implementación para la dimensión de Seguridad y Privacidad de la Información es tomado con base en el Instrumento_Evaluacion_MSPI definido por el Ministerio de las TIC para definir el nivel de madurez de la alcaldía de Acacías en esta temática.

Comprende el siguiente cronograma y se le debe realizar el respectivo seguimiento.

GESTIÓN	ACTIVIDADES	TAREAS	RESPONSABLE DE LA TAREA	FECHAS PROGRAMACIÓN TAREAS	
				FECHA INICIO	FECHA FINAL
Activos de Información	Definir lineamientos para el levantamiento de activos de información	Actualización del procedimiento y matriz de los activos de información de la entidad	Profesional Universitario/ Profesional Seguridad digital	01-feb-23	31-mar-23
	Levantamiento Activos de Información	Socializar la matriz para el levantamiento de activos de Información	Profesional Universitario/ Profesional Gobierno Digital	04-abril-23	28-abril-23
		Validar activos de información en GTIC - F - 21 Matriz instrumentos de gestión de información construido en la vigencia anterior, realizar correcciones, Cambios físicos de la ubicación entre otros de los activos de información	Profesional Universitario Oficina TIC/ Profesional Gobierno Digital	18-abr-23	29-Sep- 29

GESTIÓN	ACTIVIDADES	TAREAS	RESPONSABLE DE LA TAREA	FECHAS PROGRAMACIÓN TAREAS	
				FECHA INICIO	FECHA FINAL
Activos de Información		Identificar e ingresar nuevos activos de información en cada dependencia a la matriz	Profesional Universitario Oficina TIC/ Profesional Gobierno Digital	29-sep-23	30-oct- 23
	Publicación de Activos de Información	Consolidar el instrumento de activos de Información	Profesional Universitario Oficina TIC/ Profesional Gobierno Digital	01-nov- 23	17-nov-23
		Gestionar la elaboración firma y publicación del acto administrativo mediante el cual se adopta la actualización de los instrumentos de gestión de información	Profesional Universitario Oficina TIC/ Profesional Gobierno Digital	20-Nov-23	11-Dic- 23
		Publicación del Registro Activos de Información en el sitio web de la Entidad.	Profesional Oficina TIC	12-dic- 23	28-dic- 23
Gestión de Riesgos	Actualización de lineamientos de riesgos	Identificación, Análisis y Evaluación de Riesgos - Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación	Profesional Universitario Oficina TIC/ Profesional Seguridad Digital	1-feb-23	29-dic-23
		Realimentación, revisión y verificación de los riesgos identificados (Ajustes)	Profesional Gobierno Digital/ Profesional Oficina TIC Profesional gestión documental - Profesional SIG	1-feb-23	29-dic-23

GESTIÓN	ACTIVIDADES	TAREAS	RESPONSABLE DE LA TAREA	FECHAS PROGRAMACIÓN TAREAS	
				FECHA INICIO	FECHA FINAL
Gestión de Riesgos	Actualización de lineamientos de riesgos	Evaluación de riesgos residuales	Profesional Gobierno Digital/ Profesional Oficina TIC - Profesional gestión documental - Profesional SIG	1-feb-23	29-dic-23
		Actualizar el Mapa de Riesgos de Seguridad de la información	Profesional Gobierno Digital/ Profesional Oficina TIC - Profesional gestión documental - Profesional SIG	1-feb-23	29-dic-23
	Sensibilización	Socialización el Mapa de Riesgos de Seguridad de la información	Profesional Gobierno Digital/ Profesional Oficina TIC -	1-feb-23	29-dic-23
Gestión de Incidentes de Seguridad de la Información	Revisión procedimiento incidentes de seguridad de la información GTIC-PD-16	Revisión del procedimiento de incidentes de seguridad de la información Socializar el procedimiento de incidentes de seguridad de la información a los funcionarios de la entidad	Profesional Seguridad Digital Profesional Oficina TIC	01-mar-23	14-mar-23
	Gestionar los incidentes de Seguridad de la Información identificados	Gestionar los incidentes de seguridad de la información de acuerdo a lo establecido en el procedimiento definido.	Profesional Seguridad Digital/ Profesional Oficina TIC	1-feb-23	29-dic-23

GESTIÓN	ACTIVIDADES	TAREAS	RESPONSABLE DE LA TAREA	FECHAS PROGRAMACIÓN TAREAS	
				FECHA INICIO	FECHA FINAL
Gestión de Incidentes de Seguridad de la Información	CSIRT	Socializar los boletines informativos de seguridad, Integrar con CSIRT de Gobierno	Profesional Seguridad Digital	1-feb-23	29-dic-23
	Eventos/vulnerabilidades	Realizar seguimiento a los informes de eventos y vulnerabilidades asociados a SGSI	Profesional Gobierno Digital/ Profesional Oficina TIC	1-feb-23	29-dic-23
Plan de Continuidad del Negocio	Documentación del Plan de continuidad de la Operación	Seguimiento del Plan de continuidad Tecnológica	Profesional Gobierno Digital/ Profesional Seguridad Digital/ Profesional Oficina TIC	1-feb-23	29-dic-23
		Actualización del Plan de continuidad Tecnológica	Profesional Gobierno Digital/ Profesional Seguridad Digital/ Profesional Oficina TIC	01-feb-23	28-feb-23
Gobierno Digital		Actualizar el documento de autodiagnóstico de la entidad en la implementación de Seguridad y Privacidad de la Información.	Profesional Gobierno Digital/ Profesional Seguridad Digital/ Profesional Oficina TIC	3-Mar-23	27-Oct-23
		Revisar el avance de implementación del Plan de Seguridad Digital en la Entidad	Profesional Gobierno Digital/ Profesional Oficina TIC/ Profesional Seguridad Digital	03-Mar-23	29-dic-23

GESTIÓN	ACTIVIDADES	TAREAS	RESPONSABLE DE LA TAREA	FECHAS PROGRAMACIÓN TAREAS	
				FECHA INICIO	FECHA FINAL
Gobierno Digital		Reuniones de Socialización de los avances de la implementación del plan de Seguridad Digital y la Estrategia del Modelo de Seguridad y Privacidad de la información	Profesional Gobierno Digital/ Profesional Seguridad Digital/ Profesional Oficina TIC	03-may-23	29-dic-23
		Validar Cumplimiento requerimientos infraestructuras críticas del gobierno	Profesional Gobierno Digital/ Profesional Oficina TIC/ Profesional Seguridad Digital	04-Abr-23	29-dic-23
Indicadores SI	CCOC	Formular, Implementar y actualizar los indicadores del SI	Profesional Gobierno Digital/ Profesional Oficina TIC - Profesional SIG /Profesional Seguridad Digital/	01-Feb-23	29-dic-23
	Provisión de información a los indicadores de medición del SI	Reportar indicadores	Profesional Gobierno Digital/ Profesional Oficina TIC/ Profesional Seguridad Digital	01-Feb-23	29-dic-23

GESTIÓN	ACTIVIDADES	TAREAS	RESPONSABLE DE LA TAREA	FECHAS PROGRAMACIÓN TAREAS	
				FECHA INICIO	FECHA FINAL
Vulnerabilidades	Definir lineamientos para ejecutas las pruebas de vulnerabilidades y pen test	Definir los lineamientos y el alcance para la realización de pruebas de vulnerabilidades	Profesional Oficina TIC /Profesional Seguridad Digital/	01-Feb-23	15-mar-23
	Ejecutar las pruebas de vulnerabilidades y pen test	Ejecución de las pruebas de vulnerabilidades y pen test de acuerdo al alcance y la metodología establecida	Profesional Gobierno Digital/ Profesional Seguridad Digital/ Profesional Oficina TIC	15-mar-23	29-dic-23
Protección de datos personales	Recolectar bases de datos	Elaborar y emitir un memorando para la recolección de bases de datos personales	Profesional Gobierno Digital/ Profesional Oficina TIC/	04-abr-23	31-may- 23
	Revisión de bases de datos	Revisar y retroalimentar la información recolectada por las áreas para el registro de las bases de datos	Profesional Gobierno Digital/ Profesional Oficina TIC	04-abr-23	29-dic-23
	Registro y actualización de las bases de datos	Registrar o actualizar las bases de datos teniendo en cuenta la información suministrada por las áreas y el levantamiento de activos de información	Profesional Gobierno Digital/ Profesional Oficina TIC	03-feb-23	29-dic-23

GESTIÓN	ACTIVIDADES	TAREAS	RESPONSABLE DE LA TAREA	FECHAS PROGRAMACIÓN TAREAS	
				FECHA INICIO	FECHA FINAL
Planeación	Revisión Manual Políticas de Seguridad de la Información	Actualizar Manual Políticas de Seguridad de la Información	Profesional Gobierno Digital/ Profesional Oficina TIC /Profesional Seguridad Digital/	04-abr-23	29-dic-23
		Adquisición, desarrollo y mantenimiento de sistemas Seguridad Física y ambiental de los equipos Responsabilidades y procedimientos de operación Intercambio de Información con partes externas	Profesional Gobierno Digital/ Profesional Oficina TIC /Profesional Seguridad Digital/	01-feb-23	29-dic-23
		Informe cumplimiento de los controles por dominios asignados (Políticas, Manual, etc.)	Apoyo profesional seguridad de la información	21-feb-23	29-dic-23

9. CONTROL DE CAMBIOS

Fecha de Aprobación	Versión	Descripción y Razón del Cambio
7/01/2019	1	Creación del documento
15/01/2020	2	Actualización del Plan de Seguridad y Privacidad de la Información
28/01/2021	3	Actualización del Plan de Seguridad y Privacidad de la Información
20/01/2022	4	Actualización, conformación proyectos 2022
22/07/2022	5	Actualización estructura documental.

Fecha de Aprobación	Versión	Descripción y Razón del Cambio
17/01/2023	6	Actualización del plan de implementación del modelo de seguridad y privacidad de la información
25/01/2023	7	Actualización del plan para la vigencia 2023

ELABORÓ	REVISÓ	APROBÓ
Nombre: RODOLFO DÍAZ CLAVIJO Cargo: Profesional Universitario	Nombre: ESTHER RODRÍGUEZ GARAVITO Cargo: Profesional Especializado SIG	Nombre: EDILBERTO ROMERO TRUJILLO Cargo: Jefe Oficina de Tecnologías de la información y las Telecomunicaciones Comité Institucional de Gestión y Desempeño