AGENCIA LOGÍSTICA
FUERZAS MILITARES
La unión de nuestras Fuerzas

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN VIGENCIA 2022

ELABORÓ	FECHA			ELABORÓ	FECHA			REVISÓ	FECHA		
	20	04	2022		20	04	2022		25	04	2022
NOMBRE: Ing. Daris Yaneth Padilla Díaz				NOMBRE: Ing. Deiby Leandro Alvarado Rodríguez				NOMBRE: Ing. Roberto Velásquez Arango			
CARGO: Profesional Oficina TIC's				CARGO: Profesional Seguridad de la Información				CARGO: Coordinador Grupo Informática (E)			
FIRMA				FIRMA				FIRMA			
REVISÓ	FECHA			REVISÓ	FECHA			APROBÓ	FECHA		
	25	04	2022		25	04	2022		26	04	2022
NOMBRE: Ing. Cesar Adolfo González Peña				NOMBRE: CR. (RA) Sonia Dolly Gutiérrez Carrillo				NOMBRE: CR. Carlos Augusto Morales Hernandez			
CARGO: Coordinador Grupo de Redes e Infraestructura Tecnológica				CARGO: Jefe Oficina TIC's				CARGO: Director General Agencia Logística de las Fuerzas Militares (E)			
FIRMA				FIRMA				FIRMA			
PROCESO y/o DEPENDENCIA:				OFICINA TIC'S							

TABLA DE CONTENIDO

1. GENERALIDADES

El Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC a través de la Dirección de Gobierno Digital, dando cumplimiento a sus funciones publica "El Modelo de Seguridad y Privacidad de la Información (MSPI)", el cual se encuentra alineado con el Marco de Referencia de Arquitectura TI, el Modelo Integrado de Planeación y Gestión (MIPG) y la Guía para la Administración del Riesgo y el Diseño Controles en Entidades Públicas (Documento emitido por el Departamento Administrativo de la Función Pública, última actualización Diciembre 2020), este modelo pertenece al habilitador transversal de Seguridad y Privacidad de la Política de Gobierno Digital.

El Modelo de Seguridad y Privacidad para estar acorde con las buenas prácticas de seguridad es actualizado periódicamente; reuniendo los cambios técnicos de la norma ISO 27001 del 2013, legislación de la Ley de Protección de Datos Personales, Transparencia y Acceso a la Información Pública, entre otras, las cuales se deben tener en cuenta para la gestión de la información.

La seguridad de la información, según ISO/IEC 27001:2013, consiste en preservar la confidencialidad, integridad y disponibilidad de la información, mediante la aplicación de un proceso de Gestión de Riesgo, (ISO/ IEC 27001 VERSION 2013), para lo cual, la Agencia Logística de las Fuerzas Militares (ALFM), mediante el avance paulatino de la implementación del MSPI, busca cumplir con los lineamientos que el Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC) presenta para todas las entidades públicas.

A nivel metodológico es importante tener presente que el MSPI cuenta con guías anexas que ayudan a las entidades a cumplir lo solicitado por cada una de las fases del modelo, buscando a su vez comprender cuáles son los resultados a obtener y como desarrollarlos.

Adicionalmente, se cuenta con el "Instrumento de Evaluación MSPI", herramienta que fue creada por MinTIC con el fin de identificar el nivel de madurez en la implementación del Modelo de Seguridad y Privacidad de la Información, permitiendo establecer el estado de la gestión y adopción de controles técnicos y administrativos al interior de las Entidades Públicas, según lo definido en la Estrategia de Gobierno en Línea en su cuarto componente "Seguridad y Privacidad de la Información".

La implementación del Modelo de Seguridad y Privacidad de la Información - MSPI en la Entidad estará determinada por las necesidades objetivas, los requisitos de seguridad, procesos, el tamaño y la estructura de la misma, todo con el objetivo de preservar la confidencialidad, integridad, disponibilidad de los activos de información, garantizando su buen uso y la privacidad de los datos, trabajo que se viene adelantado y madurando año tras año.

Mediante la adopción del Modelo de Seguridad y Privacidad por parte de las Entidades del Estado se busca contribuir al incremento de la transparencia en la Gestión Pública, promoviendo el uso de las mejores prácticas de Seguridad de la Información.

De acuerdo al trabajo de revisión y autodiagnóstico realizado con relación al MSPI por parte de las Oficinas de Planeación y TIC de la ALFM en los últimos años, se tiene detectado que la implementación del MSPI desbordan la capacidad de gestión institucional, debido a que pertenecen a un ámbito específico y la entidad no cuenta con las herramientas técnicas y el recurso humano especializado para adelantar dichas acciones con los resultados esperados, más aun considerando el cambio del recurso humano de la Agencia ante el proceso de Carrera Administrativa en curso desde 2018 y que a la fecha de actualización de este documento sigue sin concluir. Por esta razón se va evaluar la contratación de consultorías previamente definidas en su alcance, calidad y resultados esperados.

Por lo todo anterior y en consecuencia, se plantea para 2022, mejorar el nivel de calificación de la Autoevaluación en al menos cinco (5) puntos con el desarrollo de las actividades planteadas en el presente documento.

2. REFERENCIA NORMATIVA

Marco Normativo	Año	Descripción
Ley 527 (agosto 18)	1999	Por medio de 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 1266 (diciembre 31)	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 1273 (enero 5)	2009	Congreso de la República. Por medio del cual se modifica el código penal, se crea un nuevo bien jurídico tutelado-Denominado "De la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
Ley 1581 (octubre 17)	2012	Disposiciones Generales para tratamiento de datos personales.
Ley 1712 (marzo 6)	2014	Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública.
NTC-ISO/IEC 27001	2013	Tecnologías de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos.

Decreto 1078 (mayo 26)	2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
Decreto 1413 (agosto 25)	2017	Por el cual se adiciona el título 17 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 reglamentarse parcialmente el capítulo IV del título 111 de la Ley 1437 de 2011 y el artículo 45 de la Ley 1753 de 2015, estableciendo lineamientos generales en el uso y operación de los servicios ciudadanos digitales".
Decreto 612 (abril 4)	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 1008 (junio 14)	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 088 (enero 24)	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 articulas 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.
Directiva Permanente Ministerio de Defensa No. 018 (junio 19)	2014	Políticas de seguridad de la información para el Sector Defensa.
Directiva Permanente Ministerio de Defensa No. 03 (enero 23)	2019	Lineamientos para la definición de la Política de Tratamiento de Datos Personales en el Ministerio de Defensa Nacional.
Directiva Presidencial No. 03 (marzo 15)	2021	Lineamientos para el uso de servicios en la nube, inteligencia artificial, seguridad digital y gestión de datos.
Directiva Presidencial No. 02	2022	Reiteración de la política pública en materia de seguridad digital.

(febrero 24)		
Resolución 001519 (agosto 24)	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.
Resolución 500 (marzo 10)	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 0463 (febrero 09)	2022	Por la cual se define el uso de las Tecnologías en la Nube para el Sector Defensa y se dictan otras disposiciones.
Resolución 000460 (febrero 15)	2022	Por la cual se expide el Plan Nacional de Infraestructura de Datos y su hoja de ruta en el desarrollo de la Política de Gobierno Digital, y se dictan los lineamientos generales para su implementación.
Resolución 000746 (marzo 11)	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
Circular 018 (septiembre 22)	2021	Implementación de la 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." Del Ministerio de las Tecnologías de la Información y las Comunicaciones (MINTIC) y la aplicación de la Matriz ITA.
CONPES 3854 (abril 11)	2016	Política Nacional de Seguridad Digital.
CONPES 3920 (abril 17)	2018	Política nacional de explotación de datos (BIG DATA).
CONPES 3995 (julio 1)	2020	Nacional de confianza y seguridad Digital.
Manual de Gobierno Digital (diciembre versión. 6)	2018	En este documento se desarrolla el proceso de implementación de la Política de Gobierno Digital a través de los siguientes cuatro (4) momentos: 1. Conocer la política; 2. Planear la política; 3. Ejecutar la política; y 4. Medir la política; cada uno de ellos incorpora las acciones que permitirán desarrollar la Política en las entidades públicas de nivel nacional y territorial.
Manual Integrado de Gestión	2019	Manual integrado de gestión, código: GI-MA-02, versión No. 20

(septiembre 27)		
GUIA ADCP (diciembre versión. 5)	2020	Guía para la Administración del Riesgo y el Diseño Controles en entidades Públicas, (Documento emitido por el Departamento Administrativo de la Función Pública, última actualización diciembre.

3. DEFINICIONES

Para los efectos del presente plan se tendrán en cuenta las siguientes definiciones:

- **Activos tecnológicos o informáticos:** Se consideran activos tecnológicos o informáticos todos los elementos de hardware, software, información y de comunicaciones entregados por la entidad al funcionario con el fin de facilitarle el desempeño de sus funciones. De esta manera, son activos tecnológicos, además de los programas (software aplicativo y de ofimática), los computadores o equipos de cómputo junto con sus periféricos (tarjeta de red, mouse, teclado, monitor, parlantes, unidades externas de almacenamiento, micrófono, entre otros), impresoras, escáneres, etc. También los equipos y elementos de comunicaciones (telefonía, switches, routers, cableado, etc.) y la información almacenada en los diversos equipos y bases de datos.

- **Análisis de riesgo:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

- **Auditoría:** Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (ISO/IEC 27000).

- **Gobierno Digital:** Es una política del Estado Colombiano encaminada a promover el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un Estado y ciudadanos competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital.

- **Modelo de Seguridad y Privacidad de la Información (MSPI):** Es un conjunto de mejores prácticas que permiten a la ALFM mejorar sus estándares en seguridad de la información. Conducen a la preservación de la confidencialidad, integridad, disponibilidad de la información, permitiendo garantizar la privacidad de los datos, mediante la aplicación de un proceso de gestión del riesgo, brindando confianza a las partes interesadas acerca de la adecuada gestión de riesgos.

- **Modelo Integrado de Planeación y Gestión (MIPG):** Es el marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión de las entidades públicas

con el fin de generar resultados que atiendan a los planes de desarrollo y que resuelvan las necesidades y problemas de los ciudadanos con integridad y calidad en los servicios.

- **Partes interesadas (Stakeholders):** Personas u organizaciones que puede afectar o ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

- **Plan de Tratamiento de Riesgos (PTR):** 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).

- **Riesgo:** 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).

- **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).

- **Tecnologías de la información y las comunicaciones (TIC):** Son el conjunto de recursos, herramientas, equipos, programas informáticos, aplicaciones, redes y medios, que permiten la compilación, procesamiento, almacenamiento, transmisión de información como voz, datos, texto, video e imágenes.

- **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).

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

4. OBJETIVOS

El Plan de Seguridad de la Información es un documento que tiene por objetivo trazar y planificar la manera como la ALFM continuará con la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), y por ende con el cumplimiento de la Norma ISO 27000.

5. ALCANCE

Se definirán las actividades a cumplir durante la presente vigencia (2022) para avanzar en la implementación del MSPI. Para esta labor se involucrarán algunos procesos de la ALFM, los cuales deberán entregar la información que se requiera al grupo encargado de avanzar en la implementación.

6. DESCRIPCIÓN GENERAL DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (MSPI)

El MSPI debe contemplar, como mínimo, los siguientes aspectos:

6.1. Establecimiento y Gestión del MSPI

- Establecimiento del MSPI.
- Implementación y operación del MSPI.
- Seguimiento y revisión del MSPI.
- Mantenimiento y mejora del MSPI.

6.2. Requisitos de documentación

- Generalidades.
- Control de Documentos.
- Control de Registros.

6.3. Responsabilidad de la Dirección

- Compromiso de la Dirección.
- Gestión de Recursos.
- Provisión de Recursos.
- Formación, toma de conciencia y competencia.

6.4. Auditorías internas del MSPI - revisión del MSPI por la Dirección

- Generalidades.
- Información para la revisión.
- Resultados de la revisión.

6.5. Mejora del MSPI

- Mejora continua.

- Acción correctiva.
- Acción preventiva.

7. ACTIVIDADES

7.1. Plan de sensibilización en temas relacionados a riesgos cibernéticos Oficina Principal y Regionales ALFM.

Continuar con el plan de sensibilización, capacitación y apropiación del MSPI para la ALFM (funcionarios operativos y administrativos) de la sede Principal y Regionales de la ALFM.

Metas	Resultado	Instrumento	Seguimientos y Monitoreos
Plan de sensibilización en temas relacionados a riesgos cibernéticos Oficina Principal y Regionales ALFM.	Plan de actividades de sensibilización y concientización en temas relacionadas a seguridad digital y de la información dirigido a todos los funcionarios de la Entidad. Jornadas de Capacitación de nuevas tendencias en riesgos cibernéticos, ingeniería social, y prevención orientada con el centro cibernético de la Policía Nacional.	Apoyo Guía No 14 - Plan de Capacitación, Sensibilización Y Comunicación De Seguridad De La Información Solicitud de capacitación a través correo electrónico a 'dijin.cecip-jef@policia.gov.co' (20/01/2021) Solicitud al CENTRO CIBERNETICO DE LA POLICIA NACIONAL) actividades y estrategias para sensibilización. Convocatorias vigentes lideradas por MINTIC, Gobierno Digital, OEA, entidades de Seguridad Nacional.	Plazo: Primer y Segundo semestre. Evidencia: Informe semestral de los avances del plan de sensibilización efectuado.
	Seguimiento al estado de avance del MSPI	Instrumento MSPI actualizado Auditoría al MSPI	Plazo: Primer y Segundo semestre. Evidencia: Actualización Instrumento de Autodiagnóstico de MINTIC.

7.2. Inventario de activos de información

Inventario de Activos: Matriz de Activos de Información, continuar con su completitud y maduración con el levantamiento y aprobación de los procesos y las dependencias de la ALFM.

Metas	Resultado	Instrumento	Seguimientos y Monitoreos
Inventario de activos de información	Actualización del inventario de activos de información, organizada por Procesos de acuerdo a la Matriz (sede Principal y Regionales). Inclusión de columna "descripción de la ubicación" en la matriz de activos. Matriz de Activos firmada y aprobada por la Alta Dirección.	Guía No 5 - Gestión De Activos Matriz de Activos de Información actualizada con asignación de custodio y valoración de confidencialidad, disponibilidad e integridad, de acuerdo a lo establecido en la Guía.	Plazo: Cuatrimestral. Evidencia: Matriz de activos de información actualizada, actividad controlada mediante el Plan de Anticorrupción y Atención al Ciudadano vigencia 2022. Plazo: Primer Semestre. Evidencia: Capacitación y actualización de matriz de activos de las Regionales.

7.3. Actualización Plan de Continuidad del Negocio

Continuar con la actualización del Plan de Continuidad del Negocio.

Metas	Resultado	Instrumento	Seguimientos y Monitoreos
Actualización Plan de Continuidad del Negocio	Actualización Plan de Continuidad del Negocio Plan de Continuidad firmado y aprobado por la Alta Dirección.	Guía 10 - Continuidad de Negocio	Plazo: Segundo semestre. Evidencia: Plan aprobado y firmado.

7.4. Revisión de las Políticas ante el MIPG.

Metas	Resultado	Instrumento	Seguimientos y Monitoreos
Actualización de la Política de Seguridad y Privacidad de la Información.	Documento Actualizado con la Política de seguridad de la información, debidamente aprobados por la Alta Dirección y socializadas al interior de la Entidad.	Guía No 2 – Política General MSPI (Numeral 6): Política general de Seguridad y Privacidad de la Información.	Plazo: Segundo semestre. Evidencia: Documentos Actualizados
	Manual con las Políticas de seguridad y privacidad de la Información, debidamente aprobados por la Alta Dirección y socializadas al interior de la Entidad.	Guía No 2 – Política General MSPI (Numeral 9): Políticas específicas recomendadas para la implementación de controles de seguridad de la información.	
Revisión de los Procedimientos de Seguridad de la Información.	Procedimientos, debidamente documentados, socializados y aprobados	Guía No 3 – (Numeral 6): Procedimientos de Seguridad y Privacidad de la Información	
Revisión y actualización de la Matriz de aplicabilidad Anexo A ISO27001.	Matriz de aplicabilidad actualizada	Guía 8 - Controles de Seguridad de la Información.	
Elaboración de Plan de actividades con la Oficina de Planeación para el ajuste, actualización y completitud de los documentos de los procesos de la Entidad acorde al resultado del diligenciamiento de la herramienta, identificación del nivel de madurez del MSPI en la Entidad.	Plan de continuidad al instrumento para la madurez del MSPI.		Plazo: Primer semestre. Evidencia: Actualización de manuales, guías, procesos, procedimientos y planes
Elaboración de un procedimiento para la gestión de incidentes.	Procedimiento de incidentes documentado y firmado.	Guía No 2 – Política General MSPI (Numeral 9): Políticas específicas recomendadas para la implementación de controles de seguridad de la información.	Plazo: Segundo semestre Evidencia: Formato aprobado
Documentar el control que se tiene para modificar los Sistemas de Información o definir el documento del ciclo de vida de los Sistemas de información.	Guía ciclo de vida de sistemas de información		Plazo: Segundo semestre Evidencia: Formato aprobado

8. SEGUIMIENTO

Articulación con el Plan de Acción Institucional 2022

En atención al 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", en su ARTÍCULO 1. Adicionar al Capítulo 3 del Título 22 de la Parte 2 del Libro 2 del Decreto 1083 de 2015, Único Reglamentario del Sector de Función Pública, los siguientes artículos: "2.2.22.3.14. Integración de los planes institucionales y estratégicos al Plan de Acción. Las entidades del Estado, de acuerdo con el ámbito de aplicación del Modelo Integrado de Planeación y Gestión, al Plan de Acción de que trata el artículo 74 de la Ley 1474 de 2011, deberán integrar los planes institucionales y estratégicos...". De acuerdo a mesas de trabajo adelantadas se realizará la articulación del: Plan de seguridad y privacidad de la información.

Soporte de las actividades publicadas en la plataforma SUITE VISION.

9. ANÁLISIS Y MEDICIÓN

Seguimiento mediante el instrumento de Autodiagnóstico de MINTIC.

10. CONTROL DE CAMBIOS

VERSIÓN	DESCRIPCIÓN DE CAMBIOS
00	Documento inicial según NMO.
01	Se actualiza el Plan para el año 2019
02	Se actualiza el Plan para el año 2020
03	Se actualiza el Plan para el año 2021
04	Se actualiza el Plan para el año 2022
05	Se actualiza Normativa de acuerdo a Decretos, Resoluciones y Directivas presidenciales para la vigencia 2022 Ajuste de fechas para la ejecución de actividades

11. ANEXO

TAREAS	EVIDENCIA / ENTREGABLE	Fecha Inicio (día-mes-año)	Fecha Fin (día-mes-año)	Dependencia Responsable	Proceso Asociado	Responsable de documentar y registrar la Tarea en la SVE	Responsable de Aprobar la Tarea en la SVE
Plan sensibilización, capacitación y apropiación del MSPI.	Documento del Plan con su cronograma	01-03-2022 01-07-2022	08-07-2022 13-01-2022	Oficina TIC's	Gestión TIC	Oficial de seguridad	Jefe Oficina TIC's
Seguimiento mediante el instrumento de Autodiagnóstico de MINTIC	Instrumento de Autodiagnóstico de MINTIC	01-07-2022 01-11-2022	30-07-2022 30-11-2022	Oficina TIC's	Gestión TIC	Oficial de seguridad	Jefe Oficina TIC's
Capacitación y actualización de matriz de activos de las Regionales.	Actas y/o listados de asistencias	01-03-2022	31-05-2022	Oficina TIC's	Gestión TIC	Oficial de seguridad	Jefe Oficina TIC's
Actualización Plan de Continuidad del Negocio.	Documento del Plan ajustado y firmado	01-03-2022	30-11-2022	Oficina TIC's	Gestión TIC	Oficial de seguridad	Jefe Oficina TIC's
Actualización de la Política de Seguridad y Privacidad de la Información.	Documento de la Directiva Actualizada y firmada	01-04-2022	29-07-2022	Oficina TIC's	Gestión TIC	Oficial de seguridad	Jefe Oficina TIC's
Revisión de los Procedimientos de Seguridad de la Información.	Documento de procedimiento codificado y aprobado	01-05-2022	31-10-2022	Oficina TIC's	Gestión TIC	Oficial de seguridad	Jefe Oficina TIC's
Revisión y actualización de la Matriz de aplicabilidad Anexo A ISO27001.	Matriz De aplicabilidad actualizada	01-08-2022	30-09-2022	Oficina TIC's	Gestión TIC	Oficial de seguridad	Jefe Oficina TIC's
Elaboración de Plan de actividades con la Oficina de Planeación para el ajuste, actualización y completitud de los documentos de los procesos de la Entidad acorde al resultado del diligenciamiento de la herramienta,	Plan de continuidad al instrumento para la madurez del MSPI.	01-03-2022	06-05-2022	Oficina TIC's	Gestión TIC	Oficial de seguridad	Jefe Oficina TIC's

TAREAS	EVIDENCIA / ENTREGABLE	Fecha Inicio (día-mes-año)	Fecha Fin (día-mes-año)	Dependencia Responsable	Proceso Asociado	Responsable de documentar y registrar la Tarea en la SVE	Responsable de Aprobar la Tarea en la SVE
identificación del nivel de madurez del MSPI en la Entidad.							
Elaboración de un procedimiento para la gestión de incidentes	Procediendo aprobado y firmado	01-08-2022	30-09-2022	Oficina TIC's	Gestión TIC	Oficial de seguridad	Jefe Oficina TIC's
Documentar el control que se tiene para modificar los Sistemas de Información o definir el documento del ciclo de vida de los Sistemas de información	Guía Sistemas de Información	01-08-2022	30-09-2022	Oficina TIC's	Gestión TIC	Oficial de seguridad	Jefe Oficina TIC's