Plan

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

GTE-PL-02-V4

Gestión tecnológica
UNIDAD NACIONAL DE PROTECCIÓN
20-01-2022

Tabla de Contenido

1. OBJETIVO 3
2. ALCANCE 3
3. DEFINICIONES 3
4. MARCO LEGAL 5
5. CONDICIONES GENERALES 5
6. CONTENIDO 6
6.1 Estrategias 6
6.2 Proyectos 6
6.3 Acciones 7
7. INDICADOR 18
8. DOCUMENTOS RELACIONADOS. 18
9. CONTROL DE CAMBIOS 18
10. CRÉDITOS 19

1. OBJETIVO

Establecer las actividades definidas en el Modelo de Seguridad y Privacidad de la Información MSPI, alineadas con la NTC/IEC ISO 27001:2013, la Política de Seguridad Digital y Continuidad del servicio, en el Mapa de Procesos de la Unidad Nacional de Protección – UNP.

2. ALCANCE

El modelo de Modelo de Seguridad y Privacidad de la Información – MPSI, está estructurado en la norma NTC/IEC ISO 27001:2013 que define los requisitos del Sistema de gestión de seguridad de la información SGSI. Por ser éste un sistema de gestión, su proceso de implementación incluye las actividades del ciclo de Deming que es PHVA, por lo tanto, la implementación del modelo inicia con las actividades de Planeación y termina con las actividades del actuar, que corresponden al mejoramiento continuo, involucra a todos los niveles de la Unidad Nacional de Protección – UNP, incluyendo servidores Públicos, contratistas, proveedores, operadores y personas o terceros que en razón del cumplimiento de sus funciones y las de la UNP compartan, utilicen, recolecten, procesen, intercambien o consulten información institucional, así como a los Entes de Control, Entidades relacionadas que accedan, interna o externamente a cualquier activo de información de la Entidad, independientemente de su ubicación geográfica.

3. DEFINICIONES.

Activos de información: En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal. Fuente: https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. Fuente: https://www.iso27000.es/glosario.html

Análisis de riesgos: uso sistemático de la información para identificar las fuentes y estimar el riesgo. Fuente: NTC-ISO/IEC 27001

Causa: todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo. Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas – Versión 4 - Riesgos de Gestión, Corrupción y Seguridad Digital Función Pública octubre 2018

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

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. Fuente: (Resolución CRC 2258 de 2009)

Ciclo de Deming: Modelo mejora continua para la implementación de un sistema de mejora continua. Fuente http://www.uniajc.edu.co/documentos/planes/2020/Plan_seguridad_2020.pdf
Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados. Fuente NTC-ISO/IEC 27000).
Control: Medida por la que se modifica el riesgo. Los controles incluyen procesos, políticas, dispositivos, prácticas, entre otras acciones que modifican el riesgo. Es posible que los controles no siempre ejerzan el efecto de modificación previsto o supuesto. Los términos salvaguardan o contramedida son utilizados frecuentemente como sinónimos de control. Fuente: https://www.iso27000.es/glosario.html
Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada. Fuente: https://www.iso27000.es/glosario.html
Impacto: Cambio adverso en el nivel de los objetivos del negocio logrados. NTC-ISO 27005:2008. Tecnologías de la Información. Técnicas de seguridad. Gestión del riesgo en la seguridad de la información. Términos y definiciones. P. 2.
Incidente de seguridad de la información: un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información. fuente NTC-ISO/IEC 27001:2006
Integridad: Propiedad de la información relativa a su exactitud y completitud. Fuente: https://www.iso27000.es/glosario.html
Oficial de Seguridad: Básicamente es un rol cuya función principal es la de alinear la seguridad de la información con los objetivos de negocio. De esta forma se garantiza en todo momento que la información de la empresa está protegida adecuadamente. Fuente: https://www.incibe.es/protege-tu-empresa/blog/ceo-ciso-cio-roles-ciberseguridad#:~:text=El%20CISO%20(Chief%20Information%20Security,con%20los%20objetivos%20de%20negocio.
Riesgo de seguridad de la información: Posibilidad de que una amenaza concreta que pueda aprovechar una vulnerabilidad para causar una pérdida o daño en un activo de información. Seguridad de la información: preservación de la confidencialidad, integridad, y disponibilidad de la información. Fuente (NTC-ISO/IEC 27005).
Riesgo Inherente: Nivel de incertidumbre propio de cada actividad, sin la ejecución de ningún control. Fuente Guía para la administración del riesgo y el diseño de controles en entidades públicas – Versión 4 - Riesgos de Gestión, Corrupción y Seguridad Digital Función Pública octubre 2018
Riesgo Residual: Nivel de riesgo remanente como resultado de la aplicación de medidas de seguridad sobre el activo. **Fuente** Guía para la administración del riesgo y el diseño de controles en entidades públicas – Versión 4 - Riesgos de Gestión, Corrupción y Seguridad Digital Función Pública octubre 2018
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). Fuente EL PORTAL DE ISO 27001 EN ESPAÑOL.
Seguridad de la Información: preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad (*Accountability*), no repudio y fiabilidad: Fuente: **NTC-ISO/IEC 27001**

Sistema de Gestión de Seguridad de la información SGSI: parte del sistema de gestión global, basada en un enfoque hacia los riesgos globales de un negocio, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información. fuente: NTC-ISO/IEC 27001
Vulnerabilidad: debilidad de un activo o control que puede ser explotada por una o más amenazas. Fuente: https://www.iso27000.es/glosario.html

4. MARCO LEGAL

I. Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales.
II. Ley 1712 de 2014 “Ley de transparencia y del derecho de acceso a la información pública nacional”
III. Decreto 1377 de 2013, por el cual se reglamenta parcialmente la Ley 1581 de 2012.
IV. 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”
V. Directiva Presidencial N° 4 de 2012 Eficiencia Administrativa y Lineamientos de la Política Cero Papel en la Administración Pública.
VI. Directiva Presidencial N° 9 de 2018 Directrices de Austeridad.
VII. Modelo de Seguridad y Privacidad de la Información V.3.0.2 – MPSI de la Estrategia de Gobierno en Línea – GEL hoy Gobierno Digital.
VIII. Resolución 3564 de 2015 de Min Tic “Reglamentación de aspectos relacionados con la Ley de Transparencia y Acceso a la Información Pública”
IX. Norma Técnica Colombiana NTC-ISO/IEC 27001 Sistemas de Gestión de la Seguridad de la Información.
X. Norma Técnica Colombiana NTC-ISO/IEC 27002 Tecnología de la Información. Técnica de Seguridad. Código de Práctica para Controles de Seguridad de la Información.
XI. Norma Técnica Colombiana NTC-ISO/IEC 9001 Sistema de Gestión de a Calidad.
XII. Normas Internacionales ISO 9001-ISO 27001-ISO 14001-ISO 45001

5. CONDICIONES GENERALES

El presente documento está enmarcado en las directrices contenidas en Modelo de Seguridad y Privacidad de la Información MSPI, alineadas con la NTC/IEC ISO 27001:2013, la Política de Seguridad Digital y Continuidad del servicio, en el Mapa de Procesos de la Unidad Nacional de Protección – UNP y busca establecer los lineamientos de implementación de las acciones para la seguridad y privacidad de la información.

6. CONTENIDO

6.1 Estrategias

La Unidad Nacional de Protección – UNP, a través de la adopción e implementación del Modelo de Seguridad y Privacidad de la Información, enmarcado en el Sistema de Gestión de Seguridad de la información - SGSI, tiene como objeto proteger, preservar y administrar la confidencialidad, integridad y disponibilidad de la información, mediante una gestión integral de riesgos y la implementación de controles físicos y digitales reduciendo la probabilidad de ocurrencia de incidentes y dando cumplimiento a los requisitos legales y reglamentarios, orientados a la mejora continua y al alto desempeño del Sistema de Gestión de Seguridad de la Información, propendiendo así por el acceso, uso efectivo y apropiación masiva de las TIC. Para lograr el cumplimiento del Plan se definen las siguientes estrategias:

1. Gestionar los riesgos de seguridad y privacidad de la información, de manera integral.
2. Mitigar los impactos y reducir la ocurrencia de posibles incidentes de Seguridad y Privacidad de la Información, de forma efectiva, eficaz y eficiente.
3. Establecer los mecanismos de aseguramiento físico y digital, para fortalecer la confidencialidad, integridad, disponibilidad de la información de la UNP.
4. Definir los lineamientos necesarios para el manejo de la información tanto física como digital en el marco de una gestión documental basada en Seguridad y Privacidad de la Información.
5. Generar conciencia para el cambio organizacional requerido para la apropiación eficaz de la Seguridad y Privacidad de la Información como eje transversal en la UNP.
6. Dar cumplimiento a los requisitos legales y normativos en materia de Seguridad y Privacidad de la información y protección de información personal.

6.2 Proyectos

A continuación, los proyectos propuestos para dar cumplimiento a la aplicación del MSPI, los cuales se deberán analizar de acuerdo con las directrices, capacidades, aprobaciones y apoyo directivo para su ejecución:

1. Apoyo a la gestión documental para el levantamiento de activos de información y fortalecimiento de instrumentos archivísticos.
2. Contrato para el desarrollo de pruebas de penetración (pen test) para análisis de vulnerabilidades.
3. Implementación del sistema de gestión de seguridad de la información.
4. Fortalecimiento, uso y apropiación de herramientas de control y restricción para la seguridad de la información.
5. Microsoft (MFA, Encriptación de comunicaciones, encriptación de archivos, parámetros de auditoría, control de acceso, etc.)

6. Fortalecimiento de la arquitectura de seguridad informática a través de una solución para la de protección de correo, malware, DLP, etc.

6.3 Acciones

Las acciones abajo listadas son la requeridas para dar cumplimiento a los objetivos propuestos del plan de seguridad y privacidad de la información de acuerdo con el estado actual de la Entidad, definiendo metas, productos, responsables y cronograma de ejecución:

Tabla 1: Cronograma Plan de Seguridad y Privacidad de la Información 20222

Cronograma de Actividades					
Ámbito	**Actividad**	**Tareas**	**Responsable**	**Fecha de Cumplimiento**	
Activos de Información	Revisar y actualizar los lineamientos para el levantamiento de activos de información.	Elaboración metodología e instrumento de levantamiento de activos de información	Gestión documental	Trimestre I 2022	
	Levantamiento de Información Activos	Socializar la guía de activos de Información.	Gestión documental	Trimestre I 2022	
		Realizar el levantamiento y actualización de los activos de información partiendo de las TRD aprobadas por AGN.	Gestión Documental, Enlace MIPGSIG.	Trimestre II 2022 – IV Trimestre 2022	
		Actualización del inventario de activos de información cuando se requiera.	Gestión Documental, Enlace MIPGSIG	Trimestre II 2022	IV Trimestre 2022
	Publicación de información de acuerdo con la Ley 1712	Validar los activos de información por proceso.	Gestión Documental, Enlace MIPGSIG	Trimestre II 2022	IV Trimestre 2022

Cronograma de Actividades					
Ámbito	**Actividad**	**Tareas**	**Responsable**	**Fecha de Cumplimiento**	
Activos de Información		Consolidar los activos de información de cada proceso en el instrumento de activos de Información.	Gestión Documental, Enlace MIPGSIG.	Trimestre II 2022	IV Trimestre 2022
		Publicar los instrumentos de activos de información consolidado en el enlace de transparencia.	Gestión Documental, Enlace MIPGSIG	Trimestre III 2022	IV Trimestre 2022
	Valoración de activos de información desde la perspectiva de Seguridad de la Información -CID	Identificar y valorar los activos de información respecto a la Confidencialidad, Integridad y Disponibilidad de la información.	Responsable del proceso, OAPI, CIO, CISO	Trimestre II 2022	IV Trimestre 2022
	Reporte Datos Personales	Reportar al Oficial de Datos personales o Seguridad de la Información la información recolectada en el instrumento de activos de información, correspondiente a bases de datos.	Responsable del proceso	Trimestre I 2022	IV Trimestre 2022
	Actualización de lineamientos de riesgos	Actualizar política y metodología de gestión de riesgos	OAPI, CIO – CISO	I Trimestre 2022	I Trimestre 2022

Cronograma de Actividades					
Ámbito	**Actividad**	**Tareas**	**Responsable**	**Fecha de Cumplimiento**	
Gestión de Riesgos	Sensibilización sobre la metodología	Socialización Guía y Herramienta - Gestión de Riesgos de Seguridad y privacidad de la Información, Seguridad Digital y Continuidad de la Operación	OAPI, CIO – CISO	II Trimestre 2022	II Trimestre 2022
Gestión de Riesgos	Ejecución de metodología de identificación de riesgos de seguridad digital	Diligenciamiento del MIR (Instrumento del Mapa Integral de Riesgos): Identificación, Análisis y Evaluación de Riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación. Aceptación, aprobación Riesgos identificados y planes de tratamiento	OAPI, CIO – CISO, TODOS LOS PROCESOS	II Trimestre 2022	II Trimestre 2022
	Publicación	Publicación Matriz de riesgos	OAPI, CIO – CISO, TODOS LOS PROCESOS	III Trimestre 2022	III Trimestre 2022
	Seguimiento Fase de Tratamiento	Seguimiento Estado planes de tratamiento de riesgos identificados y verificación de evidencias	OAPI, CIO – CISO, TODOS LOS PROCESOS	III Trimestre 2022	IV Trimestre 2022

Cronograma de Actividades					
Ámbito	**Actividad**	**Tareas**	**Responsable**	**Fecha de Cumplimiento**	
Gestión de Riesgos	Evaluación de riesgos residuales	Evaluación de riesgos residuales	OAPI, CIO – CISO, TODOS LOS PROCESOS	III Trimestre 2022	IV Trimestre 2022
	Mejoramiento	Identificación de oportunidades de mejora acorde a los resultados obtenidos durante la evaluación de riesgos residuales	OAPI, CIO – CISO, TODOS LOS PROCESOS	III Trimestre 2022	IV Trimestre 2022
Gestión de Incidentes de Seguridad de la Información	Revisión de procedimiento de gestión de incidentes de seguridad	Ajustes al procedimiento de gestión de incidentes (si aplica) basados en la ISO 27035	Equipo Incidentes	Trimestre I 2022	Trimestre I 2022
	Publicar y Socializar el procedimiento actualizado de incidentes de seguridad de la información	Publicar el procedimiento de gestión de incidentes de Seguridad de la Información en el SIG	Encargado de la Gestión de Incidentes de Seguridad de la Información	Trimestre I 2022	Trimestre I 2022
		Socializar el procedimiento a los especialistas del GGTI, indicando los cambios en el procedimiento	Encargado de la Gestión de Incidentes de Seguridad de la Información	Trimestre I 2022	Trimestre I 2022
		Socializar el procedimiento a los contratistas de la Entidad.	Encargado de la Gestión de Incidentes de Seguridad de la Información	Trimestre I 2022	Trimestre I 2022

Cronograma de Actividades					
Ámbito	**Actividad**	**Tareas**	**Responsable**	**Fecha de Cumplimiento**	
	Gestionar los incidentes de Seguridad de la Información identificados	Gestionar los incidentes de seguridad de la información de acuerdo con lo establecido en el procedimiento definido.	Especialistas GGTI - Gestión de la información	I Trimestre 2022	IV Trimestre 2022
	CSIRT	Socializar los boletines informativos de seguridad, Integrar con CSIRT de Gobierno	Oficial de Seguridad de la Información, Encargado de Seguridad Informática y Equipo de trabajo Interno de Seguridad de la Información de Gobierno Digital	I Trimestre 2022	IV Trimestre 2022
	Eventos/vulnerabilidades	Realizar seguimiento a los informes de eventos y vulnerabilidades asociadas a SGSI	Profesional de la GGTI, encargado de la Gestión de Incidentes de Seguridad de la Información.	I Trimestre 2022	IV Trimestre 2022
	Elaborar el Plan de Cambio y Cultura de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación	Elaborar el documento del Plan de Gestión de Cultura Organizacional en Apropiación del SGSI	Oficial de Seguridad de la Información, profesional del Grupo de uso y apropiación de TIC	I Trimestre 2022	I Trimestre 2022

Cronograma de Actividades					
Ámbito	**Actividad**	**Tareas**	**Responsable**	**Fecha de Cumplimiento**	
Plan de Cambio y Cultura de Seguridad y Privacidad de la Información, Seguridad Digital Plan de Cambio y Cultura de Seguridad y Privacidad de la Información, Seguridad Digital	Elaborar el Plan de Cambio y Cultura de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación	Ejecutar las actividades relacionadas en el Plan de Gestión de Cultura Organizacional en Apropiación del SGSI	Oficial de Seguridad de la Información, profesional del Grupo de uso y apropiación de TIC	I Trimestre 2022	IV Trimestre 2022
	Ejecutar el Plan de Cambio y Cultura de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación	Publicar y Socializar el Plan de Gestión de Cultura Organizacional en Apropiación del SGSI con los gestores de procesos	Oficial de Seguridad de la Información, profesional del Grupo de uso y apropiación de TIC	I Trimestre 2022	IV Trimestre 2022
		Implementar las estrategias del Plan de Gestión de Cultura Organizacional en Apropiación del SGSI	Gestor de procesos	I Trimestre 2022	IV Trimestre 2022
	Analizar el Plan de Cambio y Cultura de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación	Analizar los instrumentos de medición del Plan de Gestión de Cultura Organizacional en Apropiación del SGSI	Oficial de Seguridad de la Información, profesional del Grupo de uso y apropiación de TIC	II Trimestre 2022	II Trimestre 2022
Matriz de verificación de Requisitos Legales de Seguridad de la	Actualizar la Matriz de verificación de Requisitos Legales de Seguridad de la Información	Actualizar Matriz de verificación de Requisitos Legales de Seguridad de la Información	Oficina Asesora Jurídica, Oficial de Seguridad de la información	I Trimestre 2022	IV Trimestre 2022

Cronograma de Actividades					
Ámbito	**Actividad**	**Tareas**	**Responsable**	**Fecha de Cumplimiento**	
Información	Revisión de la Matriz de verificación de Requisitos Legales de Seguridad de la Información	Evidenciar el cumplimiento de los Requisitos Legales de Seguridad de la Información	Oficina Asesora Jurídica, Oficial de Seguridad de la información	I Trimestre 2022	IV Trimestre 2022
Plan de Continuidad del Negocio	Documentación del Análisis de Impacto de la Operación	Elaboración del Análisis de Impacto del Negocio	Equipo de Continuidad del Negocio (OAPI CIO – CISO - GGTI Alta Gerencia) Todos los procesos	I Trimestre 2022	Trimestre 2022
Plan de Continuidad del Negocio		Aprobación y publicación del Análisis de Impacto del Negocio	Alta Gerencia	II Trimestre 2022	II Trimestre 2022
Plan de Continuidad del Negocio	Documentación de Valoración de Riesgos de Interrupción	Elaboración del documento Valoración de Riesgos de interrupción para el plan de continuidad de la operación	(OAPI CIO – CISO - GGTI Alta Dirección)	II Trimestre 2022	II Trimestre 2022
		Aprobación y publicación Valoración de Riesgos de interrupción	Alta Gerencia	II Trimestre 2022	II Trimestre 2022
	Documentación de Estrategias de Continuidad	Elaboración del documento Estrategias de Continuidad de la Operación	(OAPI CIO – CISO - GGTI Alta Dirección)	III Trimestre 2022	III Trimestre 2022
		Publicación Estrategias de Continuidad de la Operación	Alta Dirección	III Trimestre 2022	III Trimestre 2022

Cronograma de Actividades					
Ámbito	**Actividad**	**Tareas**	**Responsable**	**Fecha de Cumplimiento**	
	Documentación del Plan de continuidad de la Operación	Crear Documentación del Plan de continuidad de la Operación	(OAPI CIO – CISO - GGTI Alta Dirección)	III Trimestre 2022	III Trimestre 2022

Fuente: Elaboración propia.

Cronograma de Actividades					
Ámbito	**Actividad**	**Tareas**	**Responsable**	**Fecha de Cumplimiento**	
		Aprobación del Plan de continuidad de la Operación	Alta Dirección	III Trimestre 2022	III Trimestre 2022
Acciones correctivas y Notas de mejoras SGSI	Reporte del estado de las Acciones Correctivas y Oportunidades de Mejora	Generar acciones del estado actual de las AC y OM en SIG	Líder del SGSI	I Trimestre 2022	IV Trimestre 2022
	Generar observaciones o recomendaciones a los acompañamientos realizados a los Procesos	Hacer seguimiento a las observaciones o recomendaciones dejadas a los acompañamientos realizados a los Procesos	Líder del SGSI	I Trimestre 2022	IV Trimestre 2022
Planeación	Revisar y actualizar el Manual Políticas Específicas de Seguridad y Privacidad de la Información	Elaborar el Manual de Políticas Específicas de Seguridad y privacidad de la Información	Oficial de Seguridad de la Información	I Trimestre 2022	IV Trimestre 2022
Gobierno Digital	Adopción de estrategia de Gobierno Digital	Actualizar el documento de autodiagnóstico de la entidad en la implementación de Seguridad y Privacidad de la Información.	CIO, Líder de Gobierno digital, GGTI, Oficial de Seguridad de la Información	I Trimestre 2022	IV Trimestre 2022

Cronograma de Actividades					
Ámbito	**Actividad**	**Tareas**	**Responsable**	**Fecha de Cumplimiento**	
		Revisar y alinear la documentación del SGSI de la Entidad al MSPI, de acuerdo con la Normatividad vigente.	CIO, Líder de Gobierno digital, GGTI, Oficial de Seguridad de la Información	I Trimestre 2022	IV Trimestre 2022
		Revisar el avance de implementación del Plan de Seguridad Digital en la Entidad	CIO, Líder de Gobierno digital, GGTI, Oficial de Seguridad de la Información	I Trimestre 2022	IV Trimestre 2022
		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	CIO, Líder de Gobierno digital, GGTI, Oficial de Seguridad de la Información	I Trimestre 2022	IV Trimestre 2022
	Participación en las mesas de infraestructura crítica	Cumplimiento requerimientos infraestructuras críticas del gobierno	CIO, Oficial de Seguridad de la Información	I Trimestre 2022	IV Trimestre 2022
Auditorías Internas y Externas	Participación en las auditorías internas y externas de la norma ISO 27001:2013	Participar en las auditorías internas y externas de la norma ISO 27001:2013 programadas en el SIG	Todos los procesos	III Trimestre 2022	IV Trimestre 2022

Cronograma de Actividades					
Ámbito	**Actividad**	**Tareas**	**Responsable**	**Fecha de Cumplimiento**	
Revisión de los controles de la norma ISO 27001:2013	Revisión de los controles de la norma ISO 27001:2013,	Aplicar la herramienta diseñada para realizar la validación del cumplimiento de la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación	Oficial de Seguridad de la Información	I Trimestre 2022	IV Trimestre 2022
Indicadores SGSI	Seguimiento a los indicadores de medición del SGSI	Formular, Implementar y actualizar los indicadores del SGSI	Líder del SG, Calidad, Oficial de Seguridad de la Información	I Trimestre 2022	II Trimestre 2022
		Reportar indicadores	Gestores de procesos	I Trimestre 2022	IV Trimestre 2022
	Definir lineamientos para ejecutas las pruebas de vulnerabilidades y pen test	Definir los lineamientos y el alcance para la realización de pruebas de vulnerabilidades	Oficial de Seguridad, GGTI	I Trimestre 2022	II Trimestre 2022
	Contratar Análisis de Vulnerabilidades y Pen test	Definir estudios previos y procesos de contratación para realizar el pen test y análisis de vulnerabilidades teniendo en cuenta el alcance y metodología.	Oficial De Seguridad, GGTI, Profesional de contratos	II Trimestre 2022	III Trimestre 2022

Cronograma de Actividades					
Ámbito	**Actividad**	**Tareas**	**Responsable**	**Fecha de Cumplimiento**	
Vulnerabilidades	Ejecutar las pruebas de vulnerabilidades y pen test	Ejecución de las pruebas de vulnerabilidades y pen test de acuerdo con el alcance y la metodología establecida	Pen tester	II Trimestre 2022	III Trimestre 2022
	Ejecutar plan de remediación	Diseñar el plan de remediación sobre los sistemas y plataforma de acuerdo con los resultados del análisis de vulnerabilidades y pen test	Oficial De Seguridad, GGTI	III Trimestre 2022	IV Trimestre 2022
Protección de datos personales	Identificación	Elaborar y emitir un memorando para la identificación y reporte de bases de datos personales de acuerdo con los estándares emitidos por la SIC	Oficial de Seguridad y Secretaría General Oficial de Protección de datos personales	II Trimestre 2022	IV Trimestre 2022
	Analizar las bases de datos identificadas	Revisar y realimentar la información recolectada por las áreas para el registro de las bases de datos	Oficial De seguridad y gestor de procesos Oficial de Protecci0on de datos personales Líder de Gobierno Digital	II Trimestre 2022	IV Trimestre 2022

Cronograma de Actividades					
Ámbito	**Actividad**	**Tareas**	**Responsable**	**Fecha de Cumplimiento**	
	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	Líder de Gobierno digital, Oficial de seguridad Oficial de Protecci0on de datos personales Líder de Gobierno Digital	II Trimestre 2022	IV Trimestre 2022

Fuente: Elaboración propia.

7. INDICADOR

El indicador del plan es el seguimiento al cumplimiento de las actividades, este seguimiento se hace de manera trimestral.

Indicador = ((Actividades ejecutadas trimestral) / (actividades programadas trimestral))* 100

La **meta** será del 85% de cumplimiento.

8. DOCUMENTOS RELACIONADOS.

- Acta de Reunión (SGE-FT-02)
- Listado de Asistencia (SGE -FT-03)

9. CONTROL DE CAMBIOS

VERSIÓN INICIAL	DESCRIPCIÓN DE LA CREACIÓN O CAMBIO DEL DOCUMENTO	FECHA	VERSIÓN FINAL
00	Creación del Plan Seguridad y Privacidad de la Información	31/01/2019	01
01	Actualización del Plan de Seguridad y Privacidad de la Información para la vigencia 2020	31/01/2020	02
02	Actualización del Plan de Seguridad y Privacidad de la Información para la vigencia 2021	20/01/2021	03
03	Actualización del Plan de Seguridad y Privacidad de la Información para la vigencia 2022	20/01/2022	04

10. CRÉDITOS

FIRMAS DE ELABORACIÓN, REVISIÓN Y APROBACIÓN DEL DOCUMENTO	
Elaboró Nombre: Maria Berenice Parra Parraga Cargo y/o Vinculación/dependencia: Enlace MIPG-SIG. las Tecnologías de Información / Oficina Asesora de Planeación e Información	
Elaboró Nombre: Franz Edwar Rojas Montañez Cargo y/o Vinculación/dependencia: Contratista-CIO-Grupo de Gestión de las Tecnologías de Información / Oficina Asesora de Planeación e Información	
Revisó: Nombre: Samir Manuel Berrio Scaff Cargo: Jefe de la Oficina Asesora de Planeación e Información	
Aprobó: Nombre: Alfonso Campo Martinez Cargo: Director General	
FIRMA DE OFICIALIZACIÓN DEL DOCUMENTO- SISTEMA INTEGRADO DE GESTIÓN MIPG -SIG	
Oficializó: Nombre: Samir Manuel Berrio Scaff Cargo: Jefe de la Oficina Asesora de Planeación e Información	