COLOMBIA POTENCIA DE LA VIDA

Fondo Adaptación

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2023-2026

Impulsando el desarrollo sostenible del país, a través de la adaptación al cambio climático

Versión 2.0, Mayo 2023

Equipo Directivo Fondo Adaptación:

Piedad Muñoz Rojas
Gerente (E)

Helga María Rivas Ardila
Subgerente de Gestión del Riesgo

Paola María Miranda Morales
Subgerente de Proyectos

Piedad Muñoz Rojas
Subgerente de Estructuración

Jorge Andrés Charry Gómez
Subgerente de Regiones

Fanny Jeannette Mora Monroy
Secretaria General

Jacqueline Andrade Zapata
Jefe Oficina Asesora de Planeación y Cumplimiento (E)

Investigación y textos:

EQUIPO DE TRABAJO
Tecnologías de la Información

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2023-2026.
Versión 2.0 Mayo 2023, Bogotá D.C.

CONTROL DE CAMBIOS Y NOMENCLATURA

VERSIÓN	FECHA	DESCRIPCIÓN
1.0	2023/01/31	Documento Inicial
1.1	2023/02/01	Documento ajustado alcance y marco legal
2.0	2023/05/31	Documento ajustado alcance, objetivos y actividades

Tabla de contenido

INTRODUCCIÓN

El Modelo de Seguridad y Privacidad de la Información (MSPI) se compone de las fases de diagnóstico, planeación, implementación, verificación y actuar, y a través de la implementación del Sistema de Gestión de Seguridad de la Información (en adelante SGSI) se cumple con lo requerido y exigido en los lineamientos y directrices emitidas por MinTIC.

Dentro del Sistema de Gestión de Seguridad de la Información, se contemplan grandes conjuntos de actividades dentro de cada una de las fases como son:

- Diagnóstico y Planificación: Se realiza una validación inicial del estado del MSPI, con el fin de identificar la brecha y las acciones que se deben ejecutar para su mitigación, donde se desarrollan los planes de implementación que involucran actividades como: Actualización o elaboración de la documentación, sensibilización y capacitación, identificación y clasificación de los activos de información, identificación, valoración y gestión y tratamiento del riesgo de seguridad digital, entre otras a desarrollar en estas fases.
- Implementación: Se realiza la implementación de los planes definidos en lase anterior como son tratamiento de riesgos, sensibilización, capacitación e implementación de controles.
- Verificación: Revisiones del sistema, auditorías internas y externas.
- Actuar: Monitoreo, revisión y mejora para las actividades propias de SGSI.

Este plan esta enfocado a las actividades que realizara el FONDO para la implementación de dicho Modelo.

OBJETIVOS

Los siguientes son los objetivos del plan:

1. Definir la hoja de ruta de implementación y mantenimiento del modelo de seguridad y privacidad de la información en la Entidad y el Sistema de Gestión de Seguridad de la Información.
2. Articular la metodología de gestión de riesgos de seguridad digital en todos los procesos de la Entidad.
3. Definir una estrategia de cultura digital en seguridad de la información, con el fin de promover el uso de mejores prácticas en la Entidad a nivel interno y con todas las partes interesadas.
4. Velar por el cumplimiento normativo emitido por el Gobierno a través del Ministerio de las TIC, con respecto a la Seguridad y Privacidad de la Información en todas las entidades del Estado del orden Nacional y Territorial.

ALCANCE

El Plan de Seguridad y Privacidad de la Información de la entidad toma como referencia el Modelo Nacional de Gestión de Riesgos de Seguridad Digital (MGRSI) y el Modelo de Seguridad y Privacidad de la Información (MSPI), ambos del Ministerio de las TIC como órgano regulador en la materia. Existe una interacción entre estos dos modelos que se puede ver en la Figura 1.

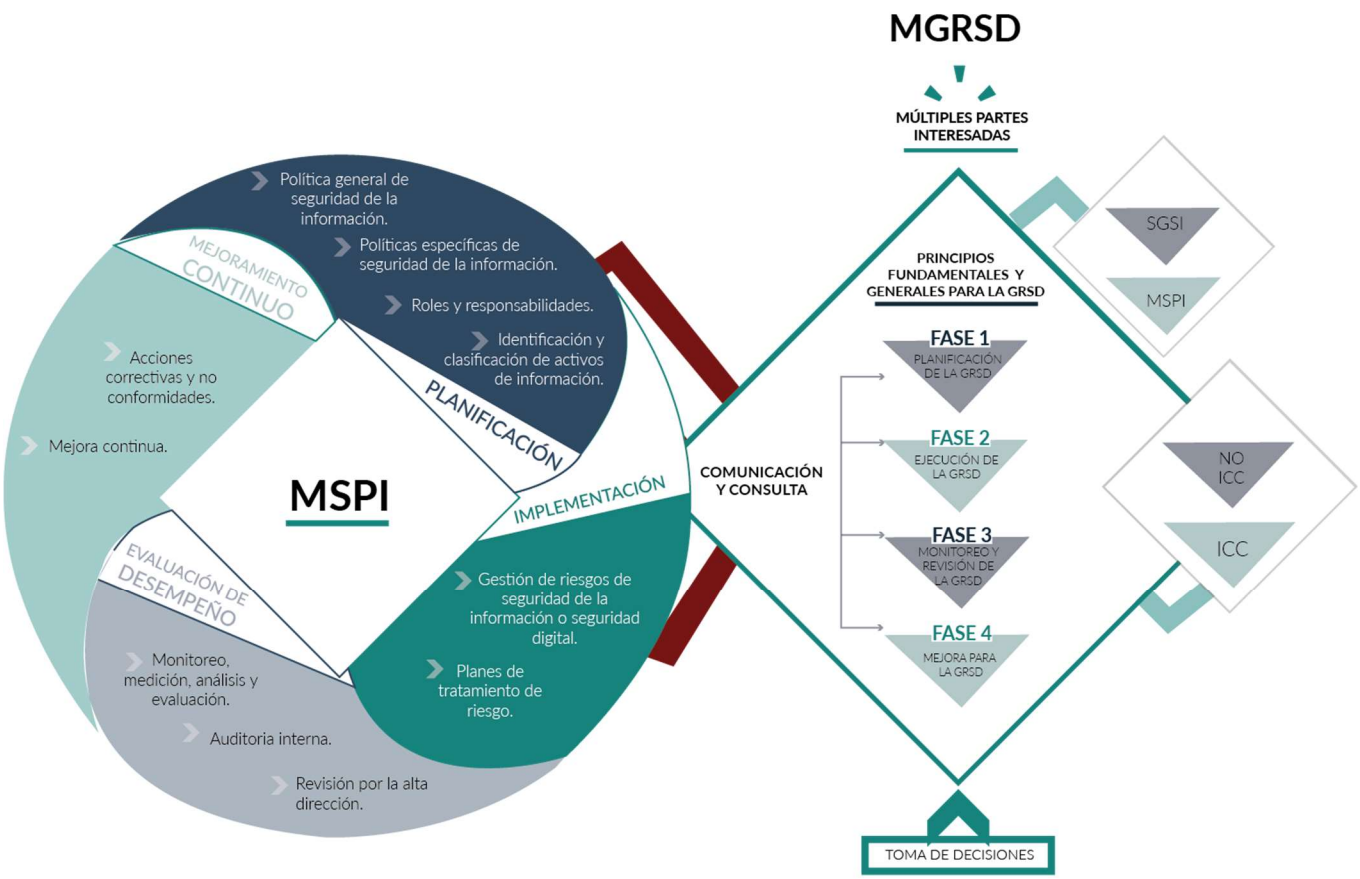

Figura 1 Interacción entre el MSPI y el MGRSD.
Fuente: MinTIC.

El alcance en el Plan de Seguridad y Privacidad de la Información abarca la planificación, el diagnóstico, planeación, implementación, verificación y actuar del MSPI y SGSI, así como la planificación, la ejecución, el monitoreo, revisión y mejora de todas las fases del MGRSI.

El alcance del plan aplica para todo el personal de planta, contratista y terceros cuando es el caso.

Es importante mencionar que la Entidad tiene una Política de Seguridad de la Información desde el año 2014 y que ha venido siendo actualizada cada año. Esta política puede ser consultada en el siguiente vínculo:

https://drive.google.com/file/d/1mjSBJmXB7m7AEjwCLvXPOFAqTdl2qNMz/view?usp=sharing

DEFINICIONES

- MSPI: Modelo de seguridad y privacidad de la información.
- MGRSI: Modelo Nacional de Gestión de Riesgos de Seguridad Digital.
- MGRSD: Modelo nacional de gestión de riesgos de seguridad digital.
- SGSI: Sistema de Gestión de Seguridad de la Información.

- Confidencialidad: propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizados.
- Disponibilidad: propiedad de la información de ser accesible, utilizable y recuperable a demanda por una entidad.
- Estándar: Regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares son orientaciones obligatorias que buscan hacer cumplir las políticas. En este documento se habla de las Norma Técnica Colombiana ISO27001:2013 e ISO31000:2019.
- Gestión de riesgos: Proceso de identificación, control y minimización o eliminación, a un coste aceptable, de los riesgos que afecten a la información de la organización. Incluye la valoración de riesgos y el tratamiento de riesgos.
- Incidente de seguridad de la información: Resultado de intentos intencionales o accidentales de romper las medidas de seguridad de la información impactando en la confidencialidad, integridad o disponibilidad de la información.
- Integridad: propiedad de la información de ser completa, exacta e inalterada exactitud y completitud.
- Información: Es un conjunto organizado de datos, que constituyen un mensaje sobre un determinado ente o fenómeno. Indicación o evento llevado al conocimiento de una persona o de un grupo. Es posible crearla, mantenerla, conservarla y transmitirla.

1 LINEAMIENTOS PARA IMPLEMENTACIÓN DEL PLAN

La alta dirección a través del Equipo de trabajo de tecnologías de la información y teniendo en cuenta la política de seguridad digital de la entidad dará las directrices para la implementación del Modelo de Seguridad y Privacidad de la Información, Modelo de Gestión de Riesgos de Seguridad y Privacidad de la Información y el Sistema de Gestión de Seguridad de la Información.

El Equipo de trabajo de tecnologías de la información debe articular, con la dirección de entidad, los esfuerzos, recursos, metodologías y estrategias para asegurar la implementación de los Modelos y Sistemas.

La Alta Dirección designará un representante ante el Sistema de Gestión de Seguridad de la Información y al responsable de la seguridad de la información de la entidad; mientras no exista una designación explicita diferente el líder del Equipo de Trabajo de Tecnologías de la Información tendrá a su cargo ambos responsabilidades, quien a su vez se apoyará en expertos técnicos para la implementación, puesta en marcha, mantenimiento, supervisión y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI).

2 MARCO NORMATIVO

2.1 Marco legal

A continuación, se enumera la normativa legal (Leyes, Decretos y similares) que se cumple con este plan:

- Ley 23 de 1982 de Propiedad Intelectual - Derechos de Autor
- Ley 1032 de 2006, por el cual se dictan disposiciones generales del Habeas Data y se regula el manejo de la información contenida en base de datos personales.

- Ley 1266 de 2007, por la cual se dictan disposiciones generales del Habeas Data y se regula el manejo de la información contenida en base de datos personales.
- Ley 1273 de 2009, "Delitos Informáticos" protección de la información y los datos.
- Ley 1437 de 2011, "Código de procedimiento administrativo y de lo contencioso administrativo".
- Ley 1581 de 2012, "Protección de Datos personales".
- Decreto 2609 de 2012, por la cual se reglamenta la ley 594 de 200 y ley 1437 de 2011.
- Decreto 1377 de 2013, por la cual se reglamenta la ley 1581 de 2012.
- Ley 1712 de 2014, “De transparencia y del derecho de acceso a la información pública nacional”.
- Decreto 1078 de 2015, por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- Ley 962 de 2005. “Simplificación y Racionalización de Trámite. Atributos de seguridad en la Información electrónica de entidades públicas;”
- Ley 1150 de 2007. “Seguridad de la información electrónica en contratación en línea”.
- Ley 1341 de 2009. “Tecnologías de la Información y aplicación de seguridad”.
- Decreto 2952 de 2010. “Por el cual se reglamentan los artículos 12 y 13 de la Ley 1266 de 2008”.
- Decreto 886 de 2014. “Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012”.
- Decreto 1008 de 2018 “por la cual se establecen los lineamientos generales para la Política de Gobierno Digital…”
- Decreto 1083 de 2015. “Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012”.
- CONPES 3701 de 2011 Lineamientos de Política para Ciberseguridad y Ciberdefensa.
- CONPES 3854 de 2016 Política Nacional de Seguridad Digital.
- Resolución Número 00500 DE MARZO 10 DE 2021
- Resolución 746 de 2022 Modelo de Seguridad y Privacidad de la Información.
- Directiva Presidencial 02 “Para garantizar la implementación segura de la Política de Gobierno Digital liderada por el Ministerio de Tecnologías de la Información y las comunicaciones (MinTIC)”

2.2 Requisitos técnicos

A continuación, se relacionan las normas técnicas tenidas en cuenta:

- Modelo de Seguridad y Privacidad de la Información – MINTIC.
- Modelo Nacional de Gestión de Riesgos de Seguridad Digital – MINTIC.
- Norma Técnica Colombiana NTC/ISO 27001:2013 y 2022 Sistemas de gestión de la seguridad de la información.
- Norma Técnica Colombiana NTC/ISO 17799 Código de práctica para la gestión de la seguridad.

3 MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN – MSPI

El Modelo de Seguridad y Privacidad de la Información (MSPI) desarrollado por MINTIC, contempla un ciclo de operación que consta de cinco (5) fases, las cuales permiten que las entidades puedan gestionar adecuadamente la seguridad y privacidad de sus activos de información. En la figura 2 se presenta el ciclo de operación.

El MSPI propone unas metas, resultados e instrumentos que deben ser ejecutados de acuerdo con unos lineamientos y guías que propone el Ministerio de las TIC, basado en las mejores prácticas en la materia.

Este modelo conduce a la preservación de la confidencialidad, integridad y disponibilidad de la información, permitiendo asegurar la privacidad de la información y los datos, mediante la aplicación de un adecuado proceso de gestión del riesgo y operación del Sistema de Gestión de Seguridad de la Información brindado confianza a las partes interesadas.

Figura 2 Ciclo de operación del Modelo de Seguridad y Privacidad de la Información
Fuente: MINTIC

4 MODELO NACIONAL DE GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL – MGRSD

Este modelo fue desarrollado por MINTIC, para dar cumplimiento a la política nacional de seguridad establecida en el documento CONPES 3854 del 11 de abril de 2015. El modelo está orientado a incrementar la conciencia ciudadana y las capacidades del Gobierno y de las empresas en general para identificar, analizar, evaluar y tratar los riesgos de seguridad digital.

En este modelo también se presentan guías para la gestión del riesgo de seguridad digital según el tipo de sector. (Gobierno nacional, territoriales y sector público; sector privado y mixto; sector fuerza pública y ciudadanía en general).

El MGRSD está estructurado como lo indica la Figura 3:

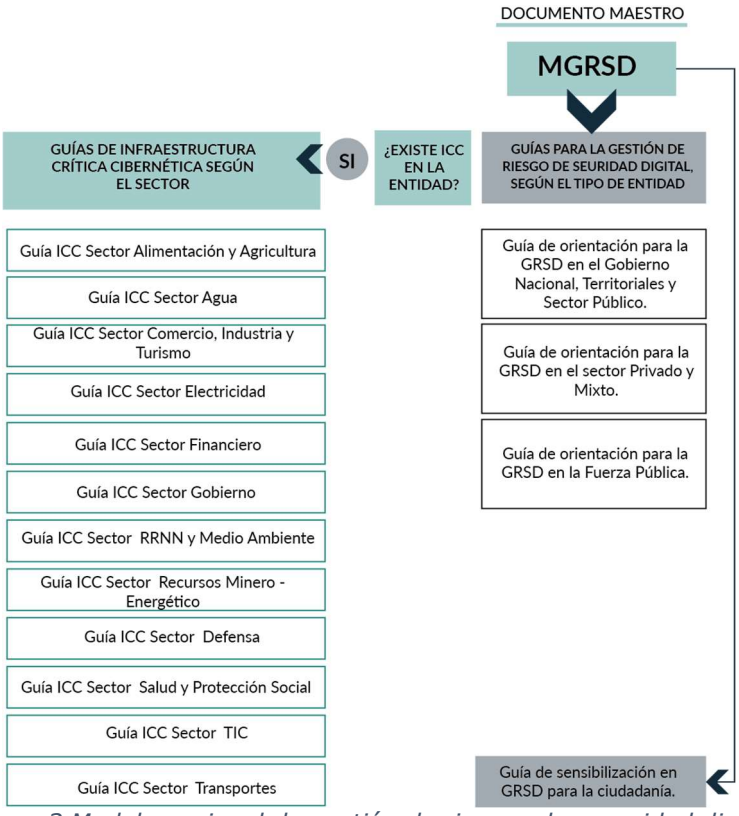

Figura 3 Modelo nacional de gestión de riesgos de seguridad digital
Fuente: MINTIC

El marco conceptual del modelo propone las fases que se presentan en la figura 4.

- **Planificación de la GRSD**: Consiste en la definición de contextos, variables para posterior análisis y evaluación de riesgos y en general todos los aspectos que se desarrollarán en los demás componentes.
- **Ejecución de la GRSD**: Consiste en el desarrollo de las actividades para el análisis y evaluación de los riesgos de seguridad digital, se identifican aspectos inherentes y residuales de los mismos, así como la definición del tratamiento de los riesgos en el marco de la seguridad de la información y particularmente en las ICC.
- **Monitoreo y Revisión de la GRSD**: Consiste en la permanente evaluación que permita asegurar que dicha gestión se está llevando a cabo bajo los aspectos y lineamientos definidos por cualquier entidad para sus riesgos de seguridad digital. Se desprenden aspectos de reporte y aseguramiento del seguimiento de todos los planes de tratamiento que se derivan de su aplicación.
- **Mejora de la GRSD:** Componente que tiene una orientación para establecer los mecanismos que permitan alcanzar un mayor grado de madurez de la GRSD en cualquier entidad. El mejoramiento continuo se estará dando de forma progresiva en la medida que se cumplan con los objetivos de la GRSD; así como la definición y aplicación modelos de evaluación de riesgos de seguridad digital con una orientación menos subjetiva y basada en modelos matemáticos que brinden mayor exactitud en la medición de las variables de impacto de los riesgos de seguridad digital sobre los activos de información y las ICC identificadas.

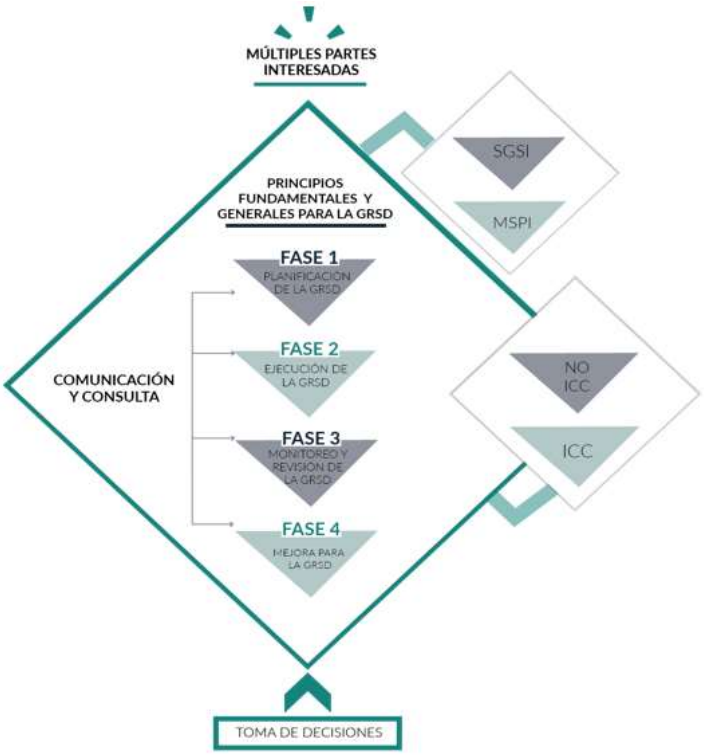

Figura 4 Fase modelo nacional de gestión de riesgos de seguridad digital
Fuente: MINTIC

5 POLÍTICA Y LINEAMIENTOS DE GESTIÓN DEL RIESGO EN EL FONDO ADAPTACIÓN

La política y lineamientos de gestión del riesgo en el Fondo Adaptación integran un proceso de gestión del riesgo de manera transversal en toda la gestión de la entidad, en sus activos de información, políticas de operación y en general en la cultura organizacional. Incluye además los planteamientos legales y reglamentarios referidos a la gestión del riesgo de seguridad digital, de acuerdo con el Anexo 4 de la Guía para la administración del riesgo y el diseño de controles en entidades públicas. En el siguiente vínculo se puede consultar la política:

https://drive.google.com/file/d/15RjZBzZPUgHOwGUlr2DqCIfa7ZlbX746/view?usp=sharing

6 ACTIVIDADES DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y DEL PLAN DE TRATAMIENTO DE RIESGOS

De acuerdo con los modelos anteriormente descritos y la política y lineamientos de gestión del riesgo del Fondo Adaptación, se proponen el cronograma de actividades anexo para la implementación del Modelo de Seguridad y Privacidad de la Información y el Sistema de Gestión de Seguridad de la Información.

El cronograma de actividades se presenta como un anexo a este documento.

7 PRESUPUESTO

La presente contratación se suscribirá con cargo a los gastos operativos por concepto de “Contratos de Estudio y Apoyos Transversales” del Proyecto de Inversión 2019011000191 “Reconstrucción de zonas e infraestructuras afectadas por la ocurrencia del fenómeno de la Niña 2010-2011. Nacional”, cuyo objetivo es “Reconstruir zonas e infraestructuras afectadas por la ocurrencia del fenómeno de La Niña 2010-2011, el cual fue declarado de importancia estratégica por el documento CONPES 3776 de 2013”.

De acuerdo con lo establecido en el parágrafo segundo del artículo 5º del Decreto Ley 4819 de 2010, con cargo a los recursos señalados en el citado decreto se pueden financiar gastos operativos y administrativos, entre los cuales, de acuerdo con lo aprobado por el Consejo Directivo de la Entidad se encuentra la línea de los Contratos de Estudio y Apoyos Transversales. De acuerdo con la cadena de valor del proyecto, estos gastos se incluyen transversalmente en el costo de los productos.

ANEXOS

Anexo 1 Cronograma actividades.

ANEXO 1. CRONOGRAMA DE ACTIVIDADES FONDO ADAPTACIÓN

Ítem	Gestión / Proyecto	Actividades	Responsables	Fechas Programación Tareas	
				Fecha Inicio	Fecha Final
1	Realiza diagnóstico de MSPI	Realizar actualización de autogiagnóstico anual, con el fin de identificar brechas y las acciones para su mitigación.	Profesional de Seguridad de la Información	abr-23	may-26
2	Políticas de Seguridad de la Información	Revisión y actualización del Manual de Políticas de Seguridad de la Información y Resolución de Seguridad de la Información anual	Profesional de Seguridad de la Información	abr-23	may-26
3	Activos de Información	Revisar la documentación frente a la normativa vigente	Profesional de Seguridad de la Información	feb-23	jul-26
		Realiza identificación de Activos de Información anual	Profesional de Seguridad de la Información		
		Socialización de activos de información anual	Profesional de Seguridad de la Información		
4	Gestión de Riesgos	Realizar identificación, valoración y definición de plan de tratamiento.	Profesional de Seguridad de la Información	jul-23	sept-26
5	Gestión de Incidentes de Seguridad de la Información	Revisar guía, procedimiento y formatos de gestión de incidentes de seguridad	Profesional de Seguridad de la Información	may-23	dic-26
		Gestionar los incidentes de Seguridad de la Información identificados	Profesional de Seguridad de la Información		
		Eventos/ vulnerabilidades	Profesional de Seguridad de la Información		
6	Plan de sensibilización y capacitación en seguridad de la información	Elaborar y ejecutar el plan de sensibilización y capacitación anual en seguridad de la información anual	Profesional de Seguridad de la Información	mar-23	dic-26
7	Requisitos Legales de Seguridad de la Información	Identificar la normativa vigente en materia de seguridad que aplica a la organización en cuanto a requisitos legales cuando sea requerido	Profesional de Seguridad de la Información	may-23	dic-26
8	Implementación de controles	Renovación de herramientas de seguridad adquiridas	Profesional de Seguridad de la Información	ago-23	dic-25
		Adquisición de pruebas de ingeniería social	Profesional de Seguridad de la Información		
		Adquisición de campañas de sensibilización	Profesional de Seguridad de la Información		
		Adquisición de herramienta de gestión del SGSI	Profesional de Seguridad de la Información		
9	Auditorías	Ejecución de Auditoría Interna anual al SGSI	Control Interno	nov-23	dic-26
		Elaborar plan de mejoramiento	Control Interno Profesional de Seguridad de la		
10	Indicadores SGSI	Revisión y evaluación de los indicadores de medición del SGSI semestralmente	Profesional de Seguridad de la Información	abr-23	may-26
11	Preparación para certificación ISO 27001:2022	Realizar revisiones de los procesos que se van a postular para la certificación.	Profesional de Seguridad de la Información	ene-24	mar-24
		Realizar diagnóstico de los procesos seleccionados	Profesional de Seguridad de la Información		
		Aplicar las acciones de mejora.	Profesional de Seguridad de la Información Proceso de la Entidad		
12	Solicitud de otorgamiento decertificación ISO 27001:2022	Realizar la gestión y atender la auditoría de otorgamiento del certificado de la Norma ISO 27001:2022	Control Interno Profesional de Seguridad de laInformación	mar-26	oct-26