PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN

AGENCIA DE DESARROLLO RURAL

2023 - 2026

Fecha actualización 10 de enero de 2024

Clasificación de la Información: Publica ☒ Reservada ☐ Clasificada ☐

Tabla de contenido

Clasificación de la Información: Publica ☒ Reservada ☐ Clasificada ☐

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

1. OBJETIVO DEL PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Fortalecer la confidencialidad, integridad y disponibilidad de los activos de información de la Agencia de Desarrollo Rural, para reducir los riesgos a los que está expuesta la organización hasta niveles aceptables, a partir de la implementación de las estrategias y/o proyectos de seguridad digital definidas en este documento para las vigencias 2023-2026.

1.1 OBJETIVOS ESPECÍFICOS

- Definir y establecer la estrategia de seguridad digital de la entidad.
- Definir y establecer las necesidades de la entidad para la implementación del Sistema de Gestión de Seguridad de la Información.
- Priorizar los proyectos a implementar para la correcta implementación del SGSI.
- Planificar la evaluación y seguimiento de los controles y lineamientos implementados en el marco del Sistema de Gestión de Seguridad de la Información.
- Definir, establecer e implementar las actividades de arquitectura de seguridad de la información.

2. ALCANCE

El Plan Estratégico de Seguridad de la Información al buscar la implementación del Sistema de Gestión de Seguridad de la Información y la estrategia de seguridad digital de la entidad, comparte el alcance definido dentro de la Política General de Seguridad de la Información, donde se indica que se tendrán en cuenta todos los procesos de la entidad.

3. DOCUMENTOS DE REFERENCIA

El Plan Estratégico de Seguridad de la Información se basa en los siguientes documentos, normas y lineamientos para su estructura y funcionamiento:

- 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*", donde se encuentra el presente Plan Estratégico de Seguridad de la Información (PESI) como uno de los requisitos a desarrollar para cumplir con esta normativa.
- Resolución 500 de 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*".
- Decreto 767 de 2022 - Política de Gobierno Digital.

- Manual de Gobierno Digital – MINTIC.
- Modelo de Seguridad y Privacidad de la Información – MINTIC.
- Resolución 1978 DE 2023 “por la cual se adopta la Versión 3 del Marco de Referencia de Arquitectura Empresarial para el Estado Colombiano como el instrumento para implementar el habilitador de arquitectura de la Política de Gobierno Digital y se dictan otras disposiciones” – Donde se establece la guía general MAE.G.AS - DOMINIO DE ARQUITECTURA DE SEGURIDAD.

4. ESTADO ACTUAL DE LA AGENCIA DE DESARROLLO RURAL RESPECTO AL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

La Agencia de Desarrollo Rural, ha realizado ejercicios de medición y diagnóstico respecto a la implementación del Sistema de Gestión de Seguridad de la Información, específicamente frente al Modelo de Seguridad y Privacidad de la Información (MSPI) del Ministerio de Tecnologías de la información y las Comunicaciones.

4.1 RIESGOS CRÍTICOS A LA SEGURIDAD Y LA CONTINUIDAD DE LA ENTIDAD

De acuerdo con el diagnóstico en sitio efectuado, en el 2023 se identificaban riesgos críticos, dentro de estos, en el 2023 se superaron algunos riesgos. Sin embargo, algos persisten y se recomienda, ser tratados con prioridad dentro de los planes de adquisiciones para la vigencia 2024, estos riesgos están incluidos dentro del diagnóstico detallado dentro de la sección 4.2, sin embargo, se considera pertinente priorizarlos dado el impacto crítico que podrían llegar a causar a la Agencia de Desarrollo Rural en caso de no tratarse en el menor tiempo posible:

RIESGO	AMENAZAS	NIVEL DE RIESGO	PLAN DE TRATAMIENTO PROPUESTO	ESTADO Y VIGENCIA TRATAMIENTO
AFECTACIÓN DE LA DISPONIBILIDAD DE LOS SERVICIOS	**DEFICIENCIAS ELÉCTRICAS EN EL CENTRO DE DATOS (PLANTA ELÉCTRICA INSUFICIENTE E INOPERANTE).** **DAÑO DE LA INFRAESTRUCTURA TECNOLÓGICA** **DEFICIENCIAS DE REFRIGERACIÓN EN EL CENTRO DE**	**CRÍTICO**	**TRASLADO DE INFRAESTRUCTURA TECNOLÓGICA A DATACENTER ESPECIALIZADO (COLOCATION)**	**Abierto**

Clasificación de la Información: Publica ☒ Reservada ☐ Clasificada ☐

RIESGO	AMENAZAS	NIVEL DE RIESGO	PLAN DE TRATAMIENTO PROPUESTO	ESTADO Y VIGENCIA TRATAMIENTO
	DATOS			
AFECTACIÓN DE LA DISPONIBILIDAD DE LOS SERVICIOS	**AUSENCIA DE CONTRATOS DE SOPORTE, GARANTÍA Y MANTENIMIENTO DE EQUIPOS** **FALLAS ELÉCTRICAS QUE PUEDAN AVERIAR LA INFRAESTRUCTURA SIN SOPORTE**	**CRÍTICO**	**RENOVACIÓN URGENTE DE CONTRATOS DE SOPORTE, GARANTÍA O MANTENIMIENTO.** **TRASLADO DE INFRAESTRUCTURA TECNOLÓGICA A DATACENTER ESPECIALIZADO (COLOCATION)**	**Abierto** **(Resolución parcial en el 2023 con la renovación de contratos de soporte y garantía de infraestructura tecnológica, el mismo proceso debe ser ejecutado en el 2024)** **(Se requiere tratamiento de los riesgos del Datacenter)**
AFECTACIÓN DE LA INTEGRIDAD Y DISPONIBILIDAD DE LOS SERVICIOS	**AUSENCIA DE ESQUEMAS DE BACKUP (RESPALDOS) DE SISTEMAS DE INFORMACIÓN** **ATAQUES Y/O INFECCIONES POR RANSOMWARE, MALWARE Y DENEGACIÓN DE SERVICIOS**	**CRÍTICO**	**ADQUISICIÓN DE PLATAFORMA DE BACKUP (RESPALDO) PARA REALIZAR RECUPERACIÓN DE LOS SERVIDORES.**	**Abierto** **(En la vigencia 2023 se adquirió infraestructura para gestión de respaldos, se requiere afinamiento y generación de nuevo procedimiento de backups)**

Clasificación de la Información: Publica ☒ Reservada ☐ Clasificada ☐

RIESGO	AMENAZAS	NIVEL DE RIESGO	PLAN DE TRATAMIENTO PROPUESTO	ESTADO Y VIGENCIA TRATAMIENTO
AFECTACIÓN DE LA INTEGRIDAD Y DISPONIBILIDAD DE LOS SERVICIOS	AUSENCIA DE CONTROLES DE SEGURIDAD DE CORREO ELECTRÓNICO PARA ATAQUES DE INGENIERÍA SOCIAL PERSONAL SIN CONOCIMIENTOS EN SEGURIDAD DE LA INFORMACIÓN	CRÍTICO	ADQUISICIÓN DE PLATAFORMA PARA PROTECCIÓN DE BUZONES DE CORREO ORIENTADOS A BUSINESS EMAIL COMPROMISE (BEC).	Abierto
AFECTACIÓN DE LA CONFIDENCIALIDAD INTEGRIDAD Y DISPONIBILIDAD DE LOS SERVICIOS	AUSENCIA DE GESTIÓN DE VULNERABILIDADES EN LOS SISTEMAS DE INFORMACIÓN EN LA NUBE Y LOCALES	CRÍTICO	ADQUISICIÓN DE SERVICIOS DE ETHICAL HACKING	Abierto

4.2 DIAGNÓSTICO DE SEGURIDAD DE LA INFORMACIÓN

Con base además las evaluaciones y diagnósticos efectuados, se encuentra la siguiente línea base establecida en la vigencia 2023, manejando como premisa los dominios de la norma ISO 27001 y el modelo de seguridad y privacidad de la información del MINTIC.

Así mismo, Teniendo en cuenta que el Marco de arquitectura Empresarial V3.0 donde se incluye el nuevo dominio de arquitectura de seguridad fue liberado a finales del 2023. Se establece una nueva necesidad de establecimiento de documentación adicional, la cual será incluida como parte del Sistema de Gestión de Seguridad de la Información (SGSI).

Acorde a lo anterior, inicialmente para establecer el diagnóstico del estado del Sistema de Gestión de Seguridad y Privacidad de la información, se está empleando el "Instrumento de Autodiagnóstico de Seguridad y Privacidad de la Información", siendo el resultado de calificación de implementación de controles para la entidad tomados como punto base en el 2023 el siguiente:

Clasificación de la Información: Publica ☒ Reservada ☐ Clasificada ☐

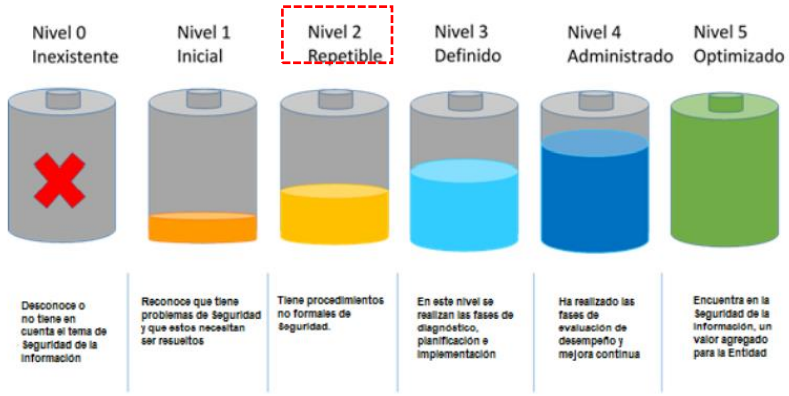
No.	Evaluación de Efectividad de controles	
	DOMINIO	Calificación Actual
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	50
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	11
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	56
A.8	GESTIÓN DE ACTIVOS	37
A.9	CONTROL DE ACCESO	49
A.10	CRIPTOGRAFÍA	20
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	54
A.12	SEGURIDAD DE LAS OPERACIONES	35
A.13	SEGURIDAD DE LAS COMUNICACIONES	35
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	21
A.15	RELACIONES CON LOS PROVEEDORES	20
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	26
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	4
A.18	CUMPLIMIENTO	34
PROMEDIO EVALUACIÓN DE CONTROLES		**32**

Año	AVANCE PHVA		
	COMPONENTE	% de Avance Actual Entidad	% Avance Esperado
2022	Planificación	21%	40%
	Implementación	8%	20%
	Evaluación de desempeño	9%	20%
	Mejora continua	10%	20%
TOTAL		48%	100%

En la gráfica anterior, donde se encuentra la calificación de cada uno de los controles por dominio de la norma ISO 27001, se evidencian que la mayoría de los puntos deben ser fortalecidos para cumplimiento de estándares internacionales de seguridad, como lo es la ISO 27001. Así como, dar cumplimiento a lo establecido en el Modelo de Seguridad y Privacidad del MINTIC, como parte del Modelo Integrado de Planeación y Gestión (MIPG) y el cumplimiento a la política de Gobierno Digital.

Así mismo, de conformidad a la metodología establecida por el MINTIC, para evaluar el nivel de madurez del Sistema de Gestión de Seguridad de la Información y con los resultados del instrumento de autodiagnóstico, el SGSI de la Agencia se encuentra actualmente en el siguiente nivel.

Clasificación de la Información: Publica ☒ Reservada ☐ Clasificada ☐



	NIVEL DE CUMPLIMIENTO
Inicial	SUFICIENTE
Repetible	INTERMEDIO
Definido	CRÍTICO
Administrado	CRÍTICO
Optimizado	CRÍTICO

Con base a la gráfica anterior, el **nivel 2 Repetible** con avance intermedio, traduce la siguiente descripción.

Repetible	En este nivel se encuentran las entidades, en las cuales existen procesos procesos básicos de gestión de la seguridad y privacidad de la información. De igual forma existen controles que permiten detectar posibles incidentes de seguridad, pero no se encuentra gestionados dentro del componente planificación del MSPI.

Con base a los resultados del autodiagnóstico, y el nivel de madurez donde se encuentra la entidad. A continuación, se detallan los aspectos más relevantes por cada uno de los dominios del sistema, en los que se deben realizar acciones de mejora, con el fin de que la entidad llegue a un nivel mínimo aceptable en su sistema:

DOMINIO	SITUACIÓN ACTUAL	SITUACIÓN DESEADA
POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	- La entidad cuenta con una Política de Seguridad y Privacidad de la Información, que no año sido actualizada desde el año 2021, y que plantea una estructura definida para los diferentes dominios de la norma y el modelo de seguridad y privacidad de la información. Sin embargo, en la mayoría de estos dominios la Política plantea a futuro que los procesos deban establecer mecanismos para seguridad de la información, no siendo claro en los lineamientos a cumplir y dando ambigüedad, en la implementación de los	- Política General de Seguridad y Privacidad de la información actualizada para la vigencia 2033 que incluya: - Mecanismos claros de aplicación, como los nombres de manuales de políticas, procedimientos, instructivos, y demás documentación, que permita la implementación adecuada de los dominios y sus controles, de tal forma que no se de ambigüedad a los procesos del cómo se deben ejecutar las

DOMINIO	SITUACIÓN ACTUAL	SITUACIÓN DESEADA
	controles a implementar por parte de los procesos. - No está definida la organización de seguridad de la información, que es un requisito mínimo con el que debe contar la Política General de Seguridad de la Información. Así mismo se observa que las políticas para gestión de activos de seguridad, se encuentran inmersas en el documento de Política General de Seguridad y Privacidad, haciendo denso el documento y dificultando la búsqueda e identificación y entendimiento para los usuarios, por lo cual es recomendable, el retiro de estas políticas de este documento, e individualizarlas en un documento como manual de políticas.	actividades en sus procesos con respecto a los controles del Sistema de Gestión de Seguridad de la Información. - Estructura definida de organización de la seguridad de la información en la entidad. - Retiro de temas no asociados a lineamiento generales de seguridad de la información de tal forma que allá una segregación adecuada de los dominios de la norma, y un fácil manejo y entendimiento, por los usuarios. - Objetivos de seguridad de la información, actualizados y que sean medibles y aporten a la mejora continúa del sistema.
ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	- No se cuenta con una estructura de organización de seguridad de la información para un esquema de decisión o definición de responsabilidades de funcionario, terceros, dirección, procesos o comités. - La oficina de tecnología no cuenta con un esquema de roles conforme a las buenas prácticas ITIL para gestión de servicios de tecnologías de la información (TI), lo que impide la identificación de una adecuada segregación de funciones en la entidad.	- Política general de seguridad y privacidad de la información, con las responsabilidades de cada una de las partes con respecto a los sistemas de seguridad de la información. Así como, un esquema jerárquico de decisión en los temas asociados al sistema. - Esquema de roles de gestión de servicios TIC conforme a las buenas prácticas ITIL. - Inclusión de política general para control de dispositivos

DOMINIO	SITUACIÓN ACTUAL	SITUACIÓN DESEADA
	Adicional en los aspectos de seguridad del teletrabajo y uso de dispositivos móviles internos y externos, la entidad no cuenta con un lineamiento general o manual de políticas, ocasionando gran exposición de la infraestructura tecnológica de la Entidad.	móviles, BYOD y Teletrabajo.
SEGURIDAD DE LOS RECURSOS HUMANOS	- Se cuentan documentos por parte del área de talento humano con los controles de selección, ejecución y desvinculación de usuarios. Sin embargo, a pesar de que desde el proceso de Tecnologías de la Información se cuenta con un plan de comunicación y concientización, no hay un apoyo por parte del área de talento humano, en los temas relacionados con la toma de conciencia, educación y formación en la seguridad de la información, brindando lineamientos para los funcionarios con respecto a la asistencia de los funcionarios a las inducciones o capacitaciones de seguridad de la información.	- Cumplimiento de los procedimientos de talento humano, en el reporte continuo de desvinculación de personal, que permita evitar brechas de seguridad por falta de retiro de derechos de acceso a los funcionarios. - Establecimiento de lineamientos por parte del área de talento humano en la obligatoriedad de asistir a los cursos, charlas, inducciones y reinducciones del Sistema de Gestión de Seguridad de la información.
GESTIÓN DE ACTIVOS	- Se cuenta con lineamientos para el buen uso de los activos de información, que están inmersas en la Política General de Seguridad de la Información y las cuales se recomienda dejarlas en un documento independiente, para facilidad de consulta y entendimiento de los funcionarios.	- Documento de Manual de Políticas para el buen uso de los activos de información independiente y con lineamientos robustecidos respecto a la gestión de medios removibles. Liberado y divulgado para la aplicación de la Entidad.

Clasificación de la Información: Publica ☒ Reservada ☐ Clasificada ☐

DOMINIO	SITUACIÓN ACTUAL	SITUACIÓN DESEADA
	- No se cuenta con lineamientos o procedimientos para la gestión de inventario de activos de seguridad de la información. Así mismo, no se cuenta con lineamientos para el mantenimiento reutilización o baja de estos. Así como no se cuentan con lineamientos para la gestión de medios removibles. Lo anterior ocasiona que no haya una planificación de mantenimientos ocasionando riesgos asociados a la falta de renovaciones de mantenimientos de la infraestructura tecnológica.	- Documentos de Procesos de gestión de inventario de activos de información, mantenimiento, reutilización y baja de equipos, liberado y apropiado.
CONTROL DE ACCESO	- No se cuenta con procedimientos de segregación de roles. Sin embargo, se cuenta con documento de clasificación de la información que permita dar manejo a la información. - Se cuenta con lineamientos genéricos de acceso a la red. Lo cual implica que, al no tener lineamientos o procedimientos específicos de control de acceso lógico, se encuentran varias debilidades en la red. - Se evidencia que el área de Talento Humano reporta periódicamente la desvinculación de personal. Sin embargo, se evidencio debilidad en el reporte desde la Oficina de Gestión Contractual, con el reporte de desvinculación de contratistas.	- Lineamientos establecidos para el control de segregación, con el fin de mitigar los riesgos asociados al conflicto de interés o responsabilidades. - Procedimientos establecidos de control de acceso lógico, para una adecuada segmentación y asignación de permisos en la red. - Oficinas de Talento Humano y Oficina de Contractual reportando los cambios en contratos y desvinculación de personal en tiempos mínimos aceptables.
CRIPTOGRAFÍA	- No se cuenta con procedimientos sobre la gestión de los controles	- Registro de control de llaves criptográficas debidamente diligenciado y definición de

Clasificación de la Información: Publica ☒ Reservada ☐ Clasificada ☐

DOMINIO	SITUACIÓN ACTUAL	SITUACIÓN DESEADA
	criptográficos. Se evidencia que la entidad cuenta con controles como firmas, certificados SSL y conexiones VPN. Pero no s controlan los mismos.	estándares mínimos para algoritmos de llaves criptográficas.
SEGURIDAD FÍSICA Y DEL ENTORNO	- Se cuentan con controles adecuados a las instalaciones, sin embargo, se debe verificar los aspectos relacionados con áreas seguras. - Se evidenciaron debilidades en las instalaciones, con respecto a la capacidad de recuperación de fallas eléctricas, y falta de gestión de mantenimientos y contratos de soporte y garantía.	- Áreas seguras identificadas y aplicando todos los controles de seguridad. - Infraestructura cubierta por UPS y plantas eléctrica con capacidad para sostenimiento de equipos tecnológicos. - Procedimientos y planificación para gestión de plan de mantenimiento anual de infraestructura con cubrimiento de soporte y garantía para todos los equipos.
SEGURIDAD DE LAS OPERACIONES	- Se evidencio que la entidad cuenta con algunos procedimientos liberados de gestión de cambios y capacidad, sin embargo los mismos no han sido apropiados, por lo cual son cumplidos o conocidos por el personal. - No se evidencia procedimiento para monitoreo gestión de logs o herramientas de la plataforma tecnológica de tal forma que se pueda realizar una detección temprana de eventos de seguridad, que mitiguen la posibilidad de materialización de riegos que puedan ocasionar incidentes de seguridad de la información.	- Procedimientos de seguridad de la información aprobados en el SGI, divulgados y apropiados, con un responsable asignado para seguimiento y gestión - Procedimientos establecidos y liberados para monitoreo y gestión de logs de la infraestructura tecnológica periódica por parte de los responsables de las plataformas.

Clasificación de la Información: Publica ☒ Reservada ☐ Clasificada ☐

DOMINIO	SITUACIÓN ACTUAL	SITUACIÓN DESEADA
	- No se cuenta con controles para gestión de licenciamiento y control del software dentro de la entidad. - No se evidencia la ejecución de procedimientos o infraestructura necesaria para la ejecución de copias de respaldos de los sistemas de información. - No se cuenta con procedimientos de gestión de vulnerabilidades técnicas.	- Procedimientos establecidos y liberados para control de software (licenciamiento) dentro de la entidad. - Procedimientos e infraestructuras de gestión de copias de respaldos implementados, para la generación de bakups, según las necesidades de la entidad. - Procedimientos de gestión de vulnerabilidades técnicas implementado, y ejecuciones periódicas de Ethical Hacking a los sistemas de información de la entidad.
SEGURIDAD DE LAS COMUNICACIONES	- No se cuenta con procedimientos de control de acceso lógico. Así mismo, se evidencia que la red no cuenta con restricción para conexión de equipos. o limitación de privilegios. - No se cuenta con procedimientos para protección de medios o información en transito	- Procedimiento de control de acceso lógico, liberado, apropiado, y aplicados los diferentes controles a la infraestructura de la Entidad. - Procedimientos de información en transito liberados, divulgados y apropiados al personal de la entidad.
ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	- No se cuenta con procedimientos para Adquisición, desarrollo y mantenimiento de software. Donde se involucren los requisitos mínimos de	- Procedimientos para adquisición, mantenimiento y desarrollo de software. Con definición de metodología unificada para todos los desarrollos y con

Clasificación de la Información: Publica ☒ Reservada ☐ Clasificada ☐

DOMINIO	SITUACIÓN ACTUAL	SITUACIÓN DESEADA
	seguridad para los sistemas de información. - No se cuenta con lineamientos para enmascaramiento o autorización de datos de uso de prueba.	estándares de desarrollo seguro de software, liberados y apropiados. - Procedimientos definidos para enmascaramiento de información o generación de autorizaciones para uso de datos de prueba en los diferentes ambientes de desarrollo.
RELACIONES CON LOS PROVEEDORES	- No se cuenta con una política de seguridad de la información para la relación con los proveedores. Únicamente se indica que la Oficina de contractual, deberá generar protocolos.	- Política de Seguridad de la Información, para la relación con los proveedores definida e implementada, con lineamientos para la protección de la cadena de suministro, cumplimiento de acuerdos de niveles de servicio y aspectos de seguridad de la información a ser cumplidos por los proveedores o terceros.
GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	- Se cuenta con procedimiento de gestión de incidentes. Sin embargo, se evidencio desconocimiento o falta de apropiación del mismo en el grupo TIC - Se evidencio confusión y falta de apropiación de los términos relacionados con debilidades y eventos de seguridad de la información. Así mismo no es claro para los usuarios la gestión a realizar con los mismos.	- Procedimientos de gestión de incidentes actualizado, divulgado y apropiado para ser cumplido por el personal del Ministerio. - Personal de la entidad capacitados en la gestión y reporta de debilidades, eventos e incidentes de seguridad de la información.
ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	- Se cuenta con documento Análisis de Impacto al Negocio BIA, Pero no se tiene establecido un plan de continuidad de negocio o DRP, teniendo en cuenta que no existe infraestructura de	- Estrategia de continuidad de negocio con alcance tecnología (Plan de Recuperación Tecnológica) definida y con infraestructura de redundancia necesaria para

DOMINIO	SITUACIÓN ACTUAL	SITUACIÓN DESEADA
	redundancia. Así mismo no se evidencia, la ejecución de procedimientos de gestión de copias de respaldo.	su implementación.
CUMPLIMIENTO	- La entidad cuenta con un normograma. Sin embargo, no se evidencia algunos lineamientos relacionados con seguridad de la información. Ley 1712 de 2014	- Normograma establecido y con identificación de todos los lineamientos relacionados con seguridad de la información y con actividades establecidas para el cumplimiento de toda la normatividad.
SEGURIDAD EN LA NUBE	- Los procedimientos de la entidad, no cuenta con alcance, donde se incluya los aspectos relacionados a seguridad en nube.	- Procedimientos de seguridad de la información, alineados para brindar protección a la infraestructura y actividades desarrolladas en nube.

Para la vigencia 2023, con el objetivo de apoyar los puntos anteriores, se estableció una base de documentos borradores para estandarización de controles y políticas de la Agencia de Desarrollo Rural. Esta documentación se encuentra en proceso de revisión, aprobación y publicación en el SIG (Sistema Integrado de Gestión).

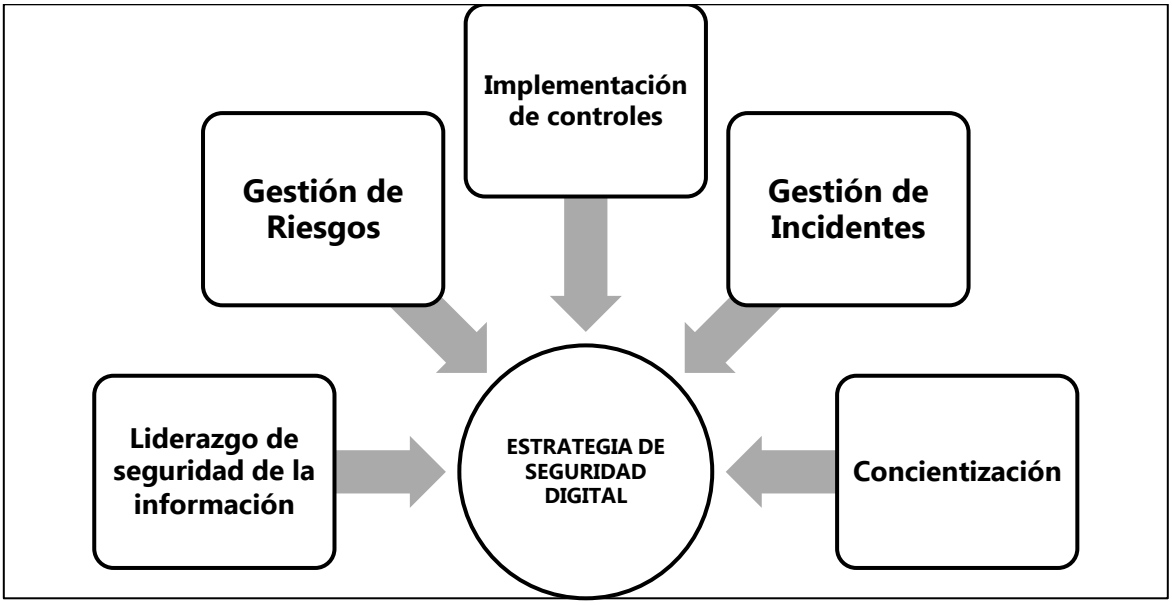
Una vez se surtan los pasos anteriores se iniciará el proceso de apropiación, lo que permitirá el aumento en la calificación de controles y madurez del sistema en la vigencia 2024.

5. ESTRATEGIA DE SEGURIDAD DIGITAL

La Agencia de Desarrollo Rural establecerá una estrategia de seguridad digital en la que se integren los principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información, teniendo como premisa que dicha estrategia gira entorno a la implementación del Modelo de Seguridad y Privacidad de la Información -MSPI, así como de la guía de gestión de riesgos de seguridad de la información y del procedimiento de gestión de incidentes que debe establecerse.

Por tal motivo, la Agencia de Desarrollo Rural define las siguientes 5 estrategias, que permitirán establecer en su conjunto una estrategia integral de seguridad digital:

Clasificación de la Información: Publica ☒ Reservada ☐ Clasificada ☐



Ejes Estrategia de Seguridad Digital

5.1 DESCRIPCIÓN DE LAS ESTRATEGIAS ESPECÍFICAS (EJES)

A continuación, se describe el objetivo de cada una de las estrategias específicas a implementar, alineando las actividades a lo descrito dentro del MPSI y la resolución 500 de 2021:

ESTRATEGIA / EJE	DESCRIPCIÓN/OBJETIVO
Liderazgo de seguridad de la información	Asegurar que se establezca el Modelo de Seguridad y Privacidad de la Información (MSPI) a través de la aprobación de la política general y demás lineamientos que se definan buscando proteger la confidencialidad, integridad y disponibilidad de la información teniendo como pilar fundamental el compromiso de la alta dirección y de los líderes de las diferentes dependencias y/o procesos de la Entidad a través del establecimiento de los roles y responsabilidades en seguridad de la información.

Clasificación de la Información: Publica ☒ Reservada ☐ Clasificada ☐

ESTRATEGIA / EJE	DESCRIPCIÓN/OBJETIVO
Gestión de riesgos	Determinar los riesgos de seguridad de la información a través de la planificación y valoración que se defina buscando prevenir o reducir los efectos indeseados tendiendo como pilar fundamental la implementación de controles de seguridad para el tratamiento de los riesgos.
Concientización	Fortalecer la construcción de la cultura organizacional con base en la seguridad de la información para que convierta en un hábito, promoviendo las políticas, procedimientos, normas, buenas prácticas y demás lineamientos, la transferencia de conocimiento, la asignación y divulgación de responsabilidades de todo el personal de la entidad en seguridad y privacidad de la información.
Implementación de controles	Planificar e implementar las acciones necesarias para lograr los objetivos de seguridad y privacidad de la información y mantener la confianza en la ejecución de los procesos de la Entidad, se pueden subdividir en controles tecnológicos y/o administrativos.
Gestión de incidentes	Garantizar una administración de incidentes de seguridad de la información con base a un enfoque de integración, análisis, comunicación de los eventos e incidentes y las debilidades de seguridad en pro de conocerlos y resolverlos para minimizar el impacto negativo de estos en la Entidad.

5.2 PORTAFOLIO DE PROYECTOS / ACTIVIDADES:

Para cada estrategia específica, la **AGENCIA DE DESARROLLO RURAL** define las siguientes actividades/proyectos y productos esperados, que tienen por objetivo lograr la implementación y mejoramiento continuo del Sistema de Gestión de Seguridad de la Información (SGSI):

ESTRATEGIA/ EJE	ACTIVIDADES/PROYECTOS	PRODUCTOS ESPERADOS

Clasificación de la Información: Publica ☒ Reservada ☐ Clasificada ☐

ESTRATEGIA/ EJE	ACTIVIDADES/PROYECTOS	PRODUCTOS ESPERADOS
LIDERAZGO EN SEGURIDAD DE LA INFORMACIÓN	Reestructurar e implementar una política de seguridad totalmente alineada a la entidad, que defina objetivos y lineamientos claros.	Política de Seguridad Actualizada, Implementada y Socializada en la entidad.
	Reestructar el Manual de Políticas de Seguridad de la Información que funcione acorde a las necesidades de la Agencia de Desarrollo Rural.	Manual de Políticas de Seguridad debidamente alineado con la entidad, formalizado y socializado.
	Definición de Roles y Responsabilidades de Seguridad de la Información a nivel institucional.	Definición de los Roles y Responsabilidades en Seguridad de la Información formalizados dentro de las políticas de seguridad y comunicados a través del comité de gestión y desempeño institucional.
	Definir la estructura de roles dentro de la Oficina de Tecnologías de la Información y las Comunicaciones.	Roles debidamente definidos, establecidos y designados dentro de la Oficina de Tecnologías de la Información y las Comunicaciones para cada una de las actividades del SGSI.

Clasificación de la Información: Publica ☒ Reservada ☐ Clasificada ☐

ESTRATEGIA/ EJE	ACTIVIDADES/PROYECTOS	PRODUCTOS ESPERADOS
GESTIÓN DE RIESGOS	Verificar y alinear la política institucional de gestión de riesgo de la entidad con los lineamientos vigentes emitidos por el Departamento Administrativo de la Función Pública en la Guía de Administración de Riesgo y Administración de controles en la versión vigente.	Política de Administración de Riesgo que incluya las tipologías de riesgo de Gestión, Corrupción y Seguridad Digital, debidamente alineada con lo indicado con DAFP.
	Definir la metodología para identificación y clasificación de activos de información para el SGSI	Manual de identificación y clasificación de activos de información formalizado y aplicado.
	Realizar las actividades de apoyo para que los procesos puedan identificar, clasificar y valorar los activos de información.	Inventario de activos de información generado por cada líder de proceso.
	Realizar las actividades de apoyo para que los procesos puedan identificar, clasificar y valorar los riesgos de seguridad de la información.	Matriz de riesgos de seguridad digital elaborado por cada líder de proceso.
	Realizar las actividades de apoyo para que los procesos definan sus planes de tratamiento de riesgos de seguridad de la Información (PTR).	Planes de tratamiento de riesgo (PTR) incluidos en cada matriz de riesgo de seguridad de la información en cada proceso.

Clasificación de la Información: Publica ☒ Reservada ☐ Clasificada ☐

ESTRATEGIA/ EJE	ACTIVIDADES/PROYECTOS	PRODUCTOS ESPERADOS
	Actualizar el Plan Estratégico de Seguridad de la Información con base a los PTR encontrados.	Plan Estratégico de Seguridad de la Información (PESI) actualizado.
CONCIENTIZACIÓN	Establecer el Plan de Sensibilización en Seguridad de la Información Anual junto al Grupo u Oficina de Comunicaciones.	Plan de Sensibilización anual debidamente socializado y aprobado para cada vigencia.
	Realizar jornadas de sensibilización en seguridad de la información para el personal de la Agencia sobre temáticas como (Correos Maliciosos, Buenas prácticas en seguridad, políticas de seguridad y lineamientos vigentes).	Jornadas de sensibilización en seguridad con alta tasa de participación.
	Realizar ejercicios de ingeniería social (ataques controlados) a los funcionarios y contratistas de la agencia.	Resultados de los ejercicios de ingenieria social que permitan identificar debilidades en el personal de la entidad.
	Realizar evaluación de conocimientos en seguridad de la información al final de la vigencia.	Resultados de la evaluación que permitan establecer el nivel de conocimiento del personal de la entidad en seguridad de la información.
IMPLEMENTACIÓN DE CONTROLES	Definición de lineamientos para respaldos de información eficiente para la entidad.	Definición del rol de Gestor de Respaldos de Información. Manual de Gestión de Respaldos de Información Formalizado y Socializado.
	Adquisición e Implementación de solución de respaldos de información para gestión de copias de respaldos de los sistemas de información de la Agencia.	Sistema de respaldos de información desplegado y administrado por el Gestor de Respaldos de información.

Clasificación de la Información: Publica ☒ Reservada ☐ Clasificada ☐

ESTRATEGIA/ EJE	ACTIVIDADES/PROYECTOS	PRODUCTOS ESPERADOS
	Definición de lineamientos para gestión de cambios en los sistemas de información en la entidad.	Definición del rol de Gestor de Cambios del SGSI. Manual de Gestión de Cambios Formalizado y Socializado.
	Implementación de Sistema WAF para plataforma On-Premise de la Agencia.	Sistema WAF debidamente desplegado e implementado en ambiente productivo on-premise.
	Adquisición e implementación de solución de seguridad avanzada para buzones de correo electrónico críticos en la entidad.	Sistema avanzado de seguridad para correo electrónico debidamente desplegado, protegiendo cuentas sensibles para la entidad.
	Actualización de Endpoint de Seguridad Avanzado	Sistema de Endpoint de seguridad avanzado debidamente desplegado en toda la infraestructura tecnológica de la entidad.
	Adquisición y ejecución de Ethical Hacking	Vulnerabilidades identificadas debidamente remediadas por el personal de la Oficina TIC.
	Definir y formalizar lineamientos para (Controles criptográficos, Control de acceso lógico, Información en tránsito, control de acceso físico, gestión de proveedores de TI, adquisición desarrollo y mantenimiento de software, gestión de vulnerabilidades técnicas, monitoreo y gestión y monitoreo de logs).	Lineamientos para Controles criptográficos, Control de acceso lógico, Información en tránsito, control de acceso físico, gestión de proveedores de TI, adquisición desarrollo y mantenimiento de software, gestión de vulnerabilidades técnicas y gestión y monitoreo de logs debidamente formalizados y socializados.
	Adquisición y parametrización de servicio SOC para monitoreo de la seguridad de la entidad.	Implementación de servicio SOC que permita a la entidad identificar brechas de seguridad y monitorear su infraestructura crítica 24/7.

Clasificación de la Información: Publica ☒ Reservada ☐ Clasificada ☐

ESTRATEGIA/ EJE	ACTIVIDADES/PROYECTOS	PRODUCTOS ESPERADOS
	Realización/Actualización de Análisis de riesgos de disponibilidad – Etapa 1 Continuidad de Negocio	Análisis de riesgos de continuidad efectuado a todos los procesos de la entidad.
	Realización/Actualización de Análisis BIA – Etapa 2 continuidad de negocio	Análisis BIA efectuado a todos los procesos de la entidad.
	Realización de Plan de Continuidad de TI (DRP) – Etapa 3 continuidad de negocio	Plan de continuidad de TI (DRP) establecido con base a los resultados del análisis BIA y ARD.
	Adquisición de servicios/infraestructura de redundancia para continuidad de TI (DRP) para la Agencia.	Infraestructura de redundancia implementada que permita restablecer los servicios de la agencia en eventos críticos.
	Definir lineamientos para control de dispositivos móviles y BYOD.	Lineamientos adecuados para el control de dispositivos móviles y BYOD dentro de la Agencia.
GESTIÓN DE INCIDENTES	Actualizar el procedimiento de Gestión de Incidentes de seguridad de la información y realizar proceso de apropiación y divulgación.	Manual y procedimiento de gestión de incidentes formalizado, implementado y socializado dentro del equipo de TI, con roles definidos. Rol de gestor de incidentes de seguridad designado.
	Aprovisionar la plataforma para gestionar incidentes dentro de la agencia.	Plataforma para gestión de incidentes configurada y apropiada.
	Capacitar al personal de la Agencia en la gestión de incidentes de seguridad de la información y el rol de cada funcionario en este aspecto.	Personal de la agencia debidamente capacitado en la gestión de incidentes de seguridad.

Clasificación de la Información: Publica ☒ Reservada ☐ Clasificada ☐

ESTRATEGIA/ EJE	ACTIVIDADES/PROYECTOS	PRODUCTOS ESPERADOS
	Realizar simulacro de incidente de seguridad para verificar respuesta por parte del equipo de TICs.	Simulacro de incidente debidamente documentado.

5.3 CRONOGRAMA DE ACTIVIDADES / PROYECTOS:

El responsable de seguridad de la información, con base a los proyectos definidos en la sección anterior, deberá establecer un cronograma de actividades donde se evidencie como se llevarán a cabo cada uno de los proyectos previstos. Las actividades podrán desarrollarse de forma secuencial o paralela según se considere.

<table>
<tr><th colspan="2">AÑO 2023</th><th colspan="2">AÑO 2024</th><th colspan="2">AÑO 2025</th><th></th></tr>
<tr><th>SEMESTRE 1</th><th>SEMESTRE 2</th><th>SEMESTRE 1</th><th>SEMESTRE 2</th><th>SEMESTRE 1</th><th>SEMESTRE 2</th><th>SEMESTRE 1</th></tr>
<tr><td>Realizar diagnóstico de seguridad y privacidad de la información</td><td colspan="6">Mantener actualizado el diagnóstico de seguridad y privacidad de la información y mantener in
dirección del estado y avance del sistema.</td></tr>
<tr><td>Reestructurar e implementar una política de seguridad totalmente alineada a la entidad, que defina objetivos y lineamientos claros y que incluya organización de la seguridad.</td><td>Divulgación y apropiación de lineamientos y políticas de seguridad al personal de la entidad.</td><td colspan="3">Implementación y apropiación de los manuales, procedimientos y políticas del Sistema de Gestión de Seguridad de la Información.</td><td>Ejecución de preauditoria Sistema de Gestión de Seguridad de la Información (NTC – ISO 27001)</td><td>Impleme
ación d
planes d
acción pa
preparac
n audito
certifica
n.</td></tr>
<tr><td colspan="3">Reestructuración de la documentación del sistema acorde a las necedades de la entidad y la norma ISO 27001. (Procedimientos, manuales, Políticas)</td><td>Mantenimiento y mejora continua del SGSI</td><td colspan="3" rowspan="2">Mantenimiento y mejora continua de</td></tr>
<tr><td>Definir la estructura de roles dentro de la Oficina de Tecnologías de la Información y las Comunicaciones.</td><td colspan="3">Apropiación de roles del Sistema de Gestión de Seguridad de la Información</td></tr>
<tr><td>Verificar y alinear la política institucional de gestión de riesgo de la entidad con los lineamientos vigentes emitidos por el Departamento Administrativo de la Función Pública en la Guía de</td><td>Realizar capacitación y apropiación de metodología de riesgos y gestión de activos de seguridad digital

Realizar las actividades de apoyo para que los procesos puedan identificar, clasificar y valorar los activos de información.</td><td colspan="5">Realizar las actividades de apoyo para que los procesos puedan i
y valorar los riesgos de seguridad de la informaci</td></tr>
</table>

AÑO 2023		AÑO 2024		AÑO 2025		
SEMESTRE 1	SEMESTRE 2	SEMESTRE 1	SEMESTRE 2	SEMESTRE 1	SEMESTRE 2	SEMESTRE 1
Administración de Riesgo y Administración de controles en la versión vigente.						
Definir la metodología para identificación y clasificación de activos de información para el SGSI						
Adquisición de servicios e infraestructura básica para gestión de copias de respaldo		Realización/Actualización de Análisis de riesgos de disponibilidad – Etapa 1 Continuidad de Negocio Realización/Actualización de Análisis BIA – Etapa 2 continuidad de negocio		Adquisición de servicios/infraestructura de redundancia para continuidad de TI (DRP) para la Agencia. Realización de Plan de Continuidad de TI (DRP) – Etapa 3 continuidad de negocio	Ejecución de pruebas de continuidad de negocio (DRP)	Esta actividad
ACTIVIDADES PERIÓDICAS						
Establecer el Plan de Sensibilización en Seguridad de la Información Anual junto al Grupo u Oficina de Comunicaciones.	Realizar evaluación de conocimientos en seguridad de la información al final de la vigencia.	Establecer el Plan de Sensibilización en Seguridad de la Información Anual junto al Grupo u Oficina de Comunicaciones.	Realizar evaluación de conocimientos en seguridad de la información al final de la vigencia.	Establecer el Plan de Sensibilización en Seguridad de la Información Anual junto al Grupo u Oficina de Comunicaciones.	Realizar evaluación de conocimientos en seguridad de la información al final de la vigencia.	Establecer el Plan de Sensibilización en Seguridad de la Información Anual junto al Grupo u Oficina de Comunicaciones.
Actualizar el Plan Estratégico de Seguridad de la	-	Actualizar el Plan Estratégico	-	Actualizar el Plan Estratégico de Seguridad de la	-	Actualizar el Plan Estratég

Clasificación de la Información: Publica ☒ Reservada ☐ Clasificada ☐

AÑO 2023		AÑO 2024		AÑO 2025		
SEMESTRE 1	SEMESTRE 2	SEMESTRE 1	SEMESTRE 2	SEMESTRE 1	SEMESTRE 2	SEMESTRE 1
Información con base a los PTR encontrados.		de Seguridad de la Información con base a los PTR encontrados.		Información con base a los PTR encontrados.		o de Seguridad de la Información con base a los PTR encontrados.
-	Realizar ejercicios de ingeniería social (ataques controlados) a los funcionarios y contratistas de la agencia.	-	Realizar ejercicios de ingeniería social (ataques controlados) a los funcionarios y contratistas de la agencia.	-	Realizar ejercicios de ingeniería social (ataques controlados) a los funcionarios y contratistas de la agencia.	-
Renovación de servicios de mantenimiento, soporte y garantía de infraestructura de seguridad.	-	Renovación de servicios de mantenimiento, soporte y garantía de infraestructura de seguridad.	-	Renovación de servicios de mantenimiento, soporte y garantía de infraestructura de seguridad.	-	Renovación de servicios de mantenimiento, soporte y garantía de infraestructura de seguridad.
Realizar jornadas de sensibilización en seguridad de la información para el personal de la Agencia sobre temáticas Maliciosos, Buenas prácticas en seguridad, políticas de seguridad y lineamientos vigentes).						
Ejecución de pruebas de vulnerabilidades técnicas de los sistemas de información						
NUEVOS PROYECTOS INFRAESTRUCTURA						
Adquisición e Implementación de solución de respaldos de			Adquisición servicio AntiDDoS para plataforma On-	Adquisición servicio para análisis de comportamiento y tráfico de Red.		Por defin

AÑO 2023		AÑO 2024		AÑO 2025		
SEMESTRE 1	SEMESTRE 2	SEMESTRE 1	SEMESTRE 2	SEMESTRE 1	SEMESTRE 2	SEMESTRE 1
información para gestión de copias de respaldos de los sistemas de información de la Agencia.			Premise y nube			
Implementación de Sistema WAF para plataforma On-Premise de la Agencia.			Adquisición e implementación de solución de seguridad avanzada para buzones de correo electrónico críticos en la entidad.	Adquisición escritorios virtuales para teletrabajo		Por defin
			Actualización de Endpoint de Seguridad Avanzado	Adquisición de servicios/infraestructura de redundancia para continuidad de TI (DRP) para la Agencia.		Por defin
		Adquisición y parametrización de servicio SOC para monitoreo de la seguridad de la entidad.				
		Adquisición servicio ethical hacking y remediación		Adquisición servicio ethical hacking y remediación		Adquisic n servic ethical hacking remediac ón
			Adquisición de software para código estático.		Adquisición de solución para protección y monitoreo de base de datos	

5.4 ANÁLISIS PRESUPUESTAL:

Con base a los proyectos definidos en el cronograma de actividades, se debe generar el presupuesto aproximado por cada vigencia según los proyectos establecidos y presentarlo a la Alta Dirección para las consideraciones y viabilidad pertinentes:

AÑO 2023		AÑO 2024		AÑO 2025		AÑO 2
PROYECTO	Inversión	PROYECTO	Inversión	PROYECTO	Inversión	PROYECTO
Adquisición e Implementación de solución de respaldos de información para gestión de copias de respaldos de los sistemas de información de la Agencia.	$700.000.000	Renovación de servicio de mantenimiento, soporte y garantía de solución de respaldos	$175.000.000	Renovación de servicio de mantenimiento, soporte y garantía de solución de respaldos	$185.000.000	Renovación de servicio de mantenimiento, soporte y garantía de solución de respaldos
		Adquisición e implementación de solución de seguridad avanzada para buzones de correo electrónico críticos en la entidad.	$200.000.000	Renovación de servicio de mantenimiento, soporte y garantía de solución protección buzones	$60.000.000	Renovación de servicio de mantenimiento, soporte y garantía de solución protección buzones
		Actualización de Endpoint de Seguridad Avanzado	$230.000.000	Renovación de servicio de mantenimiento, soporte y garantía de EndPoint	$240.000.000	Renovación de servicio de mantenimiento, soporte y garantía de EndPoint
		Adquisición y parametrización de servicio SOC para monitoreo de la seguridad de la entidad.	$275.000.000	Adquisición y parametrización de servicio SOC para monitoreo de la seguridad de la	$302.500.000	Adquisición y parametrización de servicio SOC para monitoreo de la seguridad de la entidad.

Clasificación de la Información: Publica ☒ Reservada ☐ Clasificada ☐

AÑO 2023		AÑO 2024		AÑO 2025		AÑO 2
PROYECTO	Inversión	PROYECTO	Inversión	PROYECTO	Inversión	PROYECTO
				entidad.		
Implementación de Sistema WAF para plataforma On-Premise de la Agencia.	$320.000.000	Implementación de Sistema WAF para plataforma On-Premise de la Agencia.	$85.600.000	Renovación de servicio de mantenimiento, soporte y garantía WAF	$91.592.000	Renovación de servicio de mantenimiento, soporte y garantía WAF
Renovación servicio protección WAF en nube	$120.000.000	Renovación servicio protección WAF en nube	$ 128.400.000,00	Renovación servicio protección WAF en nube	$ 137.388.000,00	Renovación servicio protección WAF en nube
				Adquisición de servicio de escritorios virtuales para teletrabajo	$300.000.000	Renovación de servicio de mantenimiento, soporte y garantía escritorios virtuales
-	-			Adquisición de servicios/infraestructura de redundancia para continuidad de TI (DRP) para la Agencia.	$1.100.000.000	Renovación de servicio de mantenimiento, soporte y garantía infraestructura DRP
		Adquisición servicio ethical hacking y remediación	$90.000.000	Adquisición servicio ethical hacking y remediación	$95.000.000	Adquisición servicio ethical hacking y remediación
Renovación de servicios de mantenimiento, soporte y garantía de	$330.000.000	Renovación de servicios de mantenimiento, soporte y	$340.000.000	Renovación de servicios de mantenimiento, soporte	$350.000.000	Renovación de servicios de mantenimiento, soporte y garantía de infraestructura de seguridad

Clasificación de la Información: Publica ☒ Reservada ☐ Clasificada ☐

AÑO 2023		AÑO 2024		AÑO 2025		AÑO 2
PROYECTO	**Inversión**	**PROYECTO**	**Inversión**	**PROYECTO**	**Inversión**	**PROYECTO**
infraestructura de seguridad (Firewall)		garantía de infraestructura de seguridad		y garantía de infraestructura de seguridad		
				Ejecución de preauditoria Sistema de Gestión de Seguridad de la Información (NTC – ISO 27001)	$60.000.000	Ejecución de auditoría de certificación del Sistema de Gestión de Seguridad de la Información (NTC – ISO 27001)
		Adquisición de software para código estático.	$70.000.000			
TOTAL	**1.470.000.000**		**$1.594.000.000**		**$2.921.480.000**	
$ 8.243.238.600						

6. RESPONSABLES

Respecto al Plan Estratégico de Seguridad de la Información (PESI), se indican los siguientes responsables:

1. Representante Legal de la Entidad y Comité de Gestión y Desempeño Institucional: Aprobar los documentos de Alto Nivel
2. Alta dirección: Velar por la implementación del MSPI y garantizar los recursos requeridos.
3. Responsable de Seguridad Digital (CISO)/ CIO / Enlace TIC: Coordinar las actividades de implementación del MSPI.

7. CONTROL DE CAMBIOS

VERSIÓN	FECHA	RAZÓN DE LA ACTUALIZACIÓN
01	Enero-2023	Versión inicial del documento
02	Enero-2024	Actualización proyectos y estado actual

Clasificación de la Información: Publica ☒ Reservada ☐ Clasificada ☐

8. APROBACIÓN

El presente plan ha sido sometido a consideración y conocimiento de la alta dirección, el comité de gestión y desempeño institucional con el objetivo de ser aprobado y aplicado conforme a lo que aquí se define.

ELABORÓ	REVISÓ	APROBÓ
Nombre: Hugo Alejandro Casallas Larrotta **Cargo:** Contratista profesional	**Nombre:** Olga Lucía Rivera Rodríguez **Cargo:** Jefe Oficina de Tecnología de la Información **Nombre:** Oscar Luis Felipe Pedraza Quintero **Cargo:** Contratista profesional	**Nombre:** Comité de Gestión y Desempeño Institucional: