



PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN – PESI

**MINISTERIO DE JUSTICIA Y DEL
DERECHO**

2024



Tabla de contenido

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.....	3
1. OBJETIVO	3
1.1 OBJETIVOS ESPECÍFICOS.....	3
2. ALCANCE	3
3. DEFINICIONES.....	5
4. DOCUMENTOS DE REFERENCIA	6
5. ESTADO ACTUAL DE LA ENTIDAD RESPECTO AL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	6
6. ESTRATEGIA DE SEGURIDAD DIGITAL.....	11
6.1 DESCRIPCIÓN DE LAS ESTRATEGIAS ESPECÍFICAS (EJES)	11
6.2 PORTAFOLIO DE PROYECTOS / ACTIVIDADES:	12
6.3 CRONOGRAMA DE ACTIVIDADES / PROYECTOS:	17
6.4 ANÁLISIS PRESUPUESTAL:	18
7. RESPONSABLES	20
8. APROBACIÓN.....	20
9. Control de Versiones.....	20



PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

1. OBJETIVO

Fortalecer la integridad, confidencialidad y disponibilidad de los activos de información del Ministerio de Justicia y del Derecho, en adelante MJD, para reducir los riesgos a los que está expuesta la Entidad, hasta niveles aceptables, a partir de la implementación de las estrategias de seguridad digital definidas en este documento para las vigencias 2024-2026.

1.1 OBJETIVOS ESPECÍFICOS

- Promover 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 el correcto desarrollo 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.
- Promover y mantener la cultura de seguridad de la información en el Ministerio de Justicia y del Derecho.
- Realizar detección y seguimiento a los eventos e incidentes de seguridad de la información, con el fin de mitigarlos y obtener lecciones aprendidas que permitan mejorar periódicamente el Sistema de Gestión de Seguridad de la Información.

2. ALCANCE

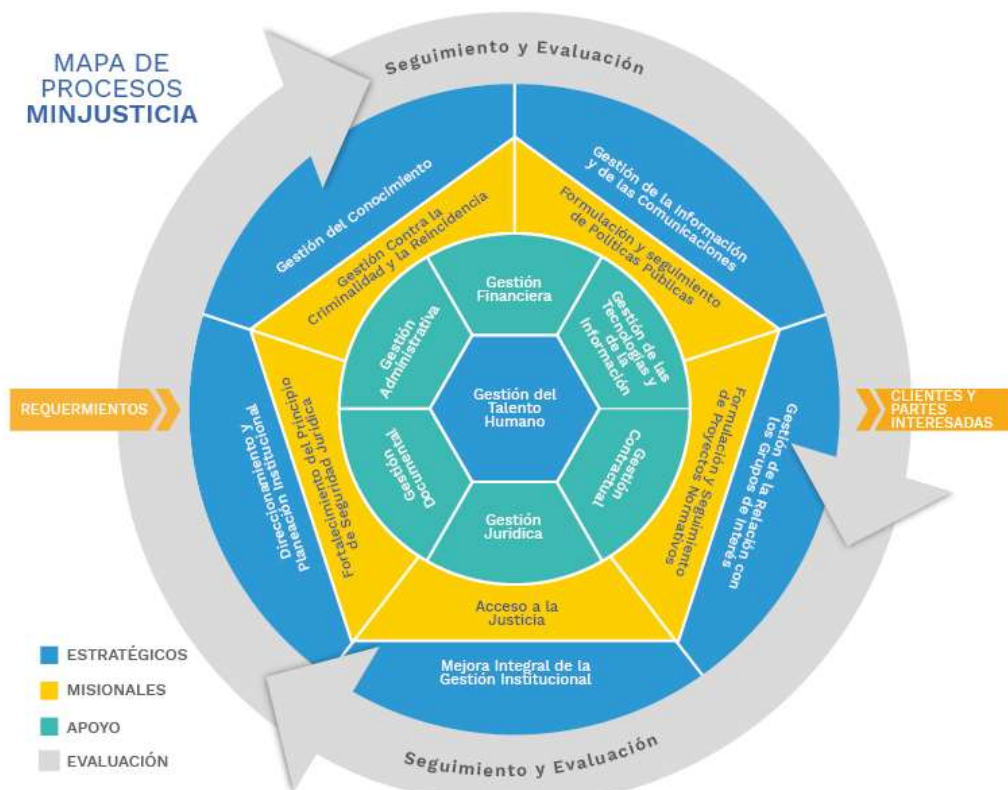
El Plan Estratégico de Seguridad de la Información se posiciona como el marco que impulsa la implementación del Sistema de Gestión de Seguridad de la Información y la estrategia de seguridad del MJD. En su esencia, este plan actúa como el enlace primordial entre los diversos componentes de la Política General

de Seguridad de la Información, la cual no solo establece lineamientos, sino que también constituye un pilar fundamental en la protección de la integridad, confidencialidad y disponibilidad de la información dentro del MJD.

En su esencia, este plan estratégico se orienta hacia la identificación y protección de nuestros activos críticos, así como hacia la implementación de controles y la gestión proactiva de los riesgos de seguridad. Su enfoque holístico y propositivo nos sitúa en una posición de fortaleza frente a las amenazas emergentes en el ámbito de la seguridad digital.

este plan no solo busca establecer estándares y protocolos, sino que aspira a crear una cultura organizacional arraigada en la importancia y la responsabilidad compartida en la protección de activos de TI y de la información sensible de la entidad.

En la siguiente ilustración se muestra el mapa de procesos del MJD que hacen parte del alcance del SGSI:





3. DEFINICIONES

- **Activo:** En cuanto a la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de ésta (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización. (ISO/IEC 27000).
- **Confidencialidad:** La información no se expone de manera desatendida ni se revela a personas, entidades o procesos no autorizados.
- **Control:** Las directrices, políticas, los procedimientos, las prácticas y las estructuras organizacionales diseñadas para mantener los riesgos de seguridad de la información por debajo del umbral de riesgo aceptado. Control es también un sinónimo de protección o medida preventiva. En términos más sencillos, es una acción que mitiga el riesgo.
- **Disponibilidad:** Garantizar que la información y los sistemas de procesamiento estén accesibles y utilizables por las personas, entidades o procesos autorizados en el momento en que los necesiten.
- **Integridad:** Preservar la precisión y la totalidad de la información, así como de los métodos utilizados para procesarla.
- **Política de Seguridad y Privacidad de la Información:** Declaración explícita de respaldo y compromiso por parte de la alta dirección en relación con la seguridad de la información.
- **Seguridad de la información:** Procesos, procedimientos, controles, guías y medidas preventivas y correctivas que las personas, entidades y las organizaciones adoptan para resguardar y proteger la información y los activos de información, buscando mantener la confidencialidad, disponibilidad e Integridad de los mismos. (ISO/IEC 27000).
- **MSPI:** Modelo de Seguridad y Privacidad de la Información del Ministerio de Tecnologías y Sistemas de Información. Recopilación de mejores prácticas nacionales e internacionales, para suministrar requisitos para el diagnóstico, planificación, implementación, gestión y mejoramiento continuo del SGSI, en el marco de la Política de Gobierno Digital, del gobierno nacional.



- **Riesgo:** Probabilidad de que una amenaza específica aproveche una vulnerabilidad, causando pérdida o daño a un activo de información. Esto generalmente se considera como una combinación de la probabilidad de que ocurra un evento y sus consecuencias. (ISO/IEC 27000).

4. 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".
- Manual de Gobierno Digital – MINTIC.
- Modelo de Seguridad y Privacidad de la Información – MINTIC.
- NTC/ISO 27001:2013 - NTC/ISO 27001:2022 – NTC/ISO 27005:2009 - GTC/ISO 27002:2015 - GTC/ISO 27002:2022.

5. ESTADO ACTUAL DE LA ENTIDAD RESPECTO AL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

El Ministerio de Justicia y del Derecho ha avanzado en la implementación del Modelo de seguridad y privacidad de la información MSPI, establecido por MinTic, a través de los planes que para tal fin se han llevado a cabo en la Entidad en vigencias anteriores, igualmente se han venido realizando ejercicios de medición y diagnóstico con el fin de fortalecer el Sistema de Gestión de Seguridad de la Información definido por MINTIC, denominado como Modelo de Seguridad y Privacidad de la Información – MSPI.

RIESGOS CRÍTICOS DE SEGURIDAD.

Riesgos identificados en el proceso de la definición del mapa de riesgos de seguridad por cada uno de los procesos o áreas de la Entidad, donde se identifica su criticidad según el valor de la evaluación del riesgo bajo los valores de Alto y Extremo.

RIESGO	AMENAZA	EVALUACIÓN	PLAN DE TRATAMIENTO
Pérdida de integridad	Daño físico de activos por polvo, corrosión, incendio, temperaturas elevadas, fenómenos meteorológicos o desastre natural	Extremo	Implementar la digitalización de los activos de información DMASC para su almacenamiento seguro.
	Acceso no autorizado a los activos de información por externos		
Pérdida de integridad	Daño físico de activos por polvo, corrosión, incendio, temperaturas elevadas, fenómenos meteorológicos o desastre natural	Alto	La DPC implementará un plan para asegurar el almacenamiento seguro de los activos con información reservada en formato electrónico y físico. Los activos electrónicos deben ser almacenados en los repositorios oficiales de la entidad y los activos físicos deberán estar protegidos contra accesos no autorizados, en el archivo de gestión.
	Acceso no autorizado a los activos de información por externos		
Pérdida de integridad	Daño físico de activos por polvo, corrosión, incendio, temperaturas elevadas, fenómenos meteorológicos o desastre natural	Extremo	Implementación del Plan de Conservación Documental del Sistema Integrado de Conservación para la mejora de las condiciones de los archivos de gestión de la entidad. Implementación del proceso de digitalización y conformación del expediente electrónico para las dependencias que aún manejan activos en papel.
Pérdida de confidencialidad	Acceso no autorizado a los activos de Información por externos	Alto	Plan de implementación de mejora en los controles de acceso en los archivos de gestión de la entidad.
Pérdida de integridad	Ataque físico malicioso (explosivos, químicos, vandalismo, radiación electromagnética, entre otros)	Alto	Implementación del Plan de Conservación Documental del Sistema Integrado de Conservación para la mejora de las condiciones del archivo central de la entidad.
	Hurto, falla o sabotaje de activos de información		
Pérdida de disponibilidad	Hurto, falla o sabotaje de activos de información	Extremo	Solicitar realización de pruebas de análisis de vulnerabilidades periódicas sobre MICC, por parte de la STSI. Implementar medición y seguimiento de indicadores de desempeño del software.
	Acceso no autorizado a los activos de información por externos		
	Ciberataques, piratería, acceso abusivo a sistemas informáticos, malware		

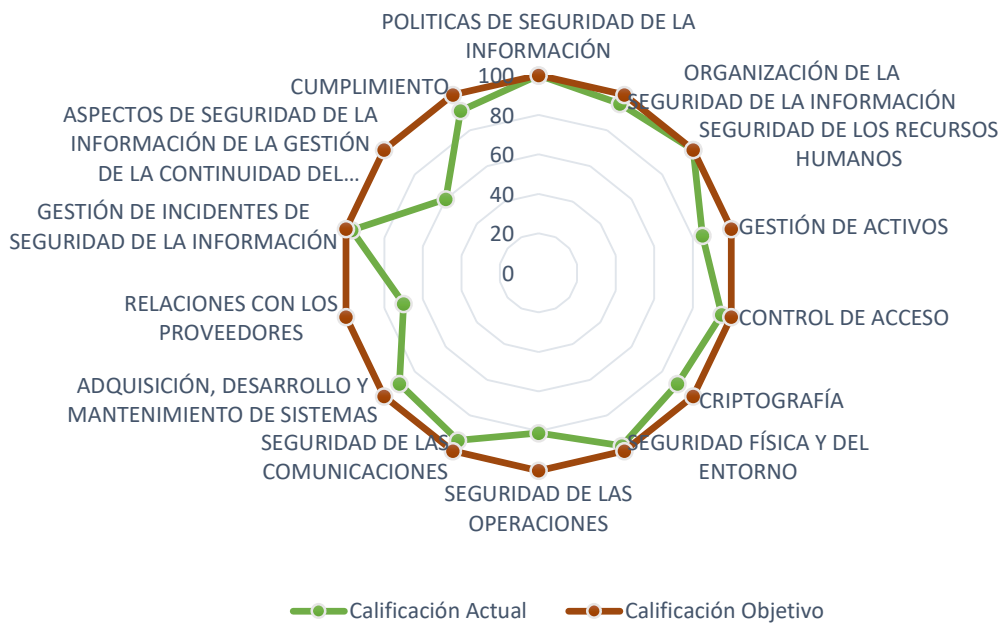
RIESGO	AMENAZA	EVALUACIÓN	PLAN DE TRATAMIENTO
Pérdida de disponibilidad	Hurto, falla o sabotaje de activos de información	Alto	Adquisición de herramienta de control de acceso con MFA (Múltiple Factor de Autenticación)
	Ciberataques, piratería, acceso abusivo a sistemas informáticos, malware		
	Interceptación de comunicaciones por medios digitales		
Pérdida de disponibilidad	Hurto, falla o sabotaje de activos de información	Alto	Plan de trabajo de la Fábrica de Software, con la implementación de mejoras, gestión de vulnerabilidades, logs de sistemas de información.
	Ciberataques, piratería, acceso abusivo a sistemas informáticos, malware		
	Acceso no autorizado a los activos de información por externos.		

ANÁLISIS DE BRECHAS DE SEGURIDAD, EVALUACIÓN DE CONTROLES Y MEJORA CONTINUA.

El análisis de brechas realizado y la evaluación de controles respecto al Anexo A de la ISO 27001:2013 en el MSPI, ha identificado áreas que requieren atención para mejorar la seguridad de la información. Las brechas destacadas afectan directamente la capacidad de la Entidad para proteger los activos de información y gestionar los riesgos de seguridad. Implementar las recomendaciones obtenidas del autodiagnóstico del MSPI ayudará a cerrar brechas de seguridad, fortalecer la postura de seguridad de la Entidad y cumplir con los requisitos de la ISO 27001:2013.

Se realizará revisión periódica y una mejora continua con el fin de mantener un nivel adecuado de seguridad de la información. A continuación, se presenta el análisis de brechas y evaluación de controles, resultado del autodiagnóstico del MSPI.

BRECHA ANEXO A ISO 27001:2013



No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	100	100	OPTIMIZADO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	95	100	OPTIMIZADO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	100	100	OPTIMIZADO
A.8	GESTIÓN DE ACTIVOS	85	100	OPTIMIZADO
A.9	CONTROL DE ACCESO	95	100	OPTIMIZADO
A.10	CRIPTOGRAFÍA	90	100	OPTIMIZADO
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	97	100	OPTIMIZADO
A.12	SEGURIDAD DE LAS OPERACIONES	81	100	OPTIMIZADO
A.13	SEGURIDAD DE LAS COMUNICACIONES	94	100	OPTIMIZADO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	90	100	OPTIMIZADO
A.15	RELACIONES CON LOS PROVEEDORES	70	100	GESTIONADO
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	97	100	OPTIMIZADO
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	60	100	EFFECTIVO
A.18	CUMPLIMIENTO	91	100	OPTIMIZADO
PROMEDIO EVALUACIÓN DE CONTROLES		89	100	OPTIMIZADO

Se presenta el nivel de madurez que se tiene actualmente en la Entidad y sobre el cual se trabaja de manera continua.



El estado actual del Modelo de Seguridad y Privacidad de la Información permitirá a la entidad establecer la línea base de donde se encuentra la entidad y así proyectar hacia que punto desea llegar con base a las actividades definidas dentro del PESI.

Optimizado	En este nivel se encuentran las entidades, en donde existe un mejoramiento continuo del MSPI, retroalimentando cualitativamente el modelo
-------------------	---

Año	AVANCE PHVA		
	COMPONENTE	% de Avance Actual Entidad	% Avance Esperado
2023	Planificación	39%	40%
	Implementación	18%	20%
	Evaluación de desempeño	20%	20%
	Mejora continua	20%	20%
TOTAL		98%	100%

El autodiagnóstico de gobierno digital ha sido un proceso mediante el cual la Entidad ha evaluado su capacidad para implementar y gestionar tecnologías digitales en las operaciones y servicios. Este proceso ha implica la revisión de varios aspectos de la Entidad incluyendo la infraestructura tecnológica, la gestión de datos, la ciberseguridad, la interoperabilidad de los sistemas, y la capacitación del personal. Esto ha permitido obtener una visión clara del estado actual sobre la política de gobierno digital y desarrollar un plan estratégico para alcanzar los objetivos de transformación digital.

La medición del FURAG ha Permitido recopilar información sistemática sobre el cumplimiento de los objetivos estratégicos, los planes de acción y los resultados de gestión. A través de esta herramienta, la entidad ha podido evaluar su desempeño en áreas claves como la gestión administrativa, la transparencia, la eficiencia operativa y el cumplimiento normativo.

6. ESTRATEGIA DE SEGURIDAD DIGITAL

El MJD 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, **EI MJD** define las siguientes 5 estrategias específicas, que permitirán establecer en su conjunto una estrategia general de seguridad digital:



6.1. DESCRIPCIÓN DE LAS ESTRATEGIAS ESPECÍFICAS (EJES)

A continuación, se describe el objetivo de cada una de las estrategias específicas a implementar, alineando las actividades 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.
Gestión de riesgos	Evaluar los riesgos de seguridad de la información mediante una planificación y evaluación detalladas, con el objetivo de prevenir o mitigar los efectos adversos. El elemento central de este proceso es la implementación de controles de seguridad efectivos para gestionar y tratar los riesgos identificados.
Concientización	Fomentar una cultura organizacional centrada en la seguridad de la información, integrando esta práctica en los hábitos diarios. Esto implica promover y adherirse a políticas, procedimientos, normas, buenas prácticas y directrices, además de facilitar la transferencia de conocimiento. Es esencial asignar y comunicar claramente las responsabilidades de todo el personal en materia de seguridad y privacidad de la información.
Implementación de controles	Desarrollar y aplicar las medidas necesarias para alcanzar los objetivos de seguridad y privacidad de la información, asegurando así la confianza en los procesos de la Entidad. Estas medidas pueden clasificarse 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.

6.2. PORTAFOLIO DE PROYECTOS / ACTIVIDADES:

Para cada estrategia específica, el MJD define los siguientes proyectos y productos esperados, que tienen por objetivo lograr el fortalecimiento y mejoramiento continuo del Sistema de Gestión de Seguridad de la Información (SGSI):



ESTRATEGIA / EJE	PROYECTO	PRODUCTOS ESPERADOS
<p>Liderazgo de seguridad de la información</p>	<p>PROYECTOS / ACTIVIDADES 1: Mejora continua y fortalecimiento de la política de Seguridad de la información, así como el Modelo de Seguridad y Privacidad de la Información.</p> <p>PROYECTOS / ACTIVIDADES 2: Llevar a cabo la implementación de un equipo de trabajo con funciones de primeros respondientes ante incidentes de seguridad, denominado CSIRT_Justicia</p> <p>PROYECTOS / ACTIVIDADES 3: Renovación de servicios de mantenimiento, soporte y garantía de infraestructura de seguridad (WAF nube y Firewall).</p> <p>PROYECTOS / ACTIVIDADES 4: Actualización y renovación de aseguramiento de conexiones remotas y teletrabajo.</p> <p>PROYECTOS / ACTIVIDADES 5: Actualización y renovación de aseguramiento de conexiones remotas y teletrabajo.</p> <p>PROYECTOS / ACTIVIDADES 6: Adquisición e implementación de sistemas de seguridad (DLP - Data Loss Prevention) el cual permita llevar a cabo la prevención de la pérdida de datos e información crítica.</p>	<p>actualizar la política de seguridad de la información y aumentar la madurez del Modelo de Seguridad y Privacidad de la Información (MSPI). Revisión y verificación de Roles y Responsabilidades</p> <p>Definición del equipo de trabajo como primer respondiente ante incidentes de Seguridad de la Información.</p> <p>Renovación y adquisición de servicios de seguridad y ciberseguridad.</p>

	<p>PROYECTOS / ACTIVIDADES 7: Adquirir una solución de seguridad EDR (ENDPOINT DETECTION AND RESPONSE) licenciada que a través de una plataforma unificada brinde una eficaz detección de amenazas y ciberataques a la infraestructura del Ministerio de Justicia y del Derecho.</p>	
<p>Gestión de riesgos</p>	<p>PROYECTOS / ACTIVIDADES 1: Identificar, valorar, actualizar y clasificar los riesgos asociados a los activos de información</p> <p>PROYECTOS / ACTIVIDADES 2: Definir planes de tratamiento de riesgos de seguridad.</p> <p>PROYECTOS / ACTIVIDADES 3: Adquisición de servicios/infraestructura de redundancia para continuidad de TI (DRP).</p> <p>PROYECTOS / ACTIVIDADES 4: Actualización e Implementación de solución de respaldos de información para el fortalecimiento de los procesos de Backup y aseguramiento de la información.</p>	<p>Matriz de riesgos de seguridad digital revisada y actualizada.</p> <p>Definir planes de tratamiento de riesgos.</p> <p>Renovación y adquisición de servicios de seguridad y ciberseguridad.</p>
<p>Concientización</p>	<p>PROYECTOS / ACTIVIDADES 1: Establecer desde el inicio de cada año la planeación de sensibilización para todo el año.</p> <p>PROYECTOS / ACTIVIDADES 2: Realizar jornadas de sensibilización a todo el personal de la Entidad.</p>	<p>1. Plan de Sensibilización</p> <p>2. Evidencias de las actividades desarrolladas</p>

	<p>PROYECTOS / ACTIVIDADES 3: Medir el grado de sensibilización a toda la Entidad.</p> <p>PROYECTOS / ACTIVIDADES 4: Contratación de servicios orientados a actividades de uso y apropiación</p>	<p>3. Resultado de las encuestas de medición.</p> <p>4. Capacitación sobre seguridad de la Información y ciberseguridad, ejercicios de ingeniería social, Stand Comedy de y transformación digital y seguridad.</p>
<p>Implementación de controles</p>	<p>CONTROL 1 Política de respaldos de información.</p> <p>CONTROL 2 Control Contra el uso y Bloqueo de USB.</p> <p>CONTROL 3 Clasificación de la información (Publica, Publica clasificada, Publica reservada).</p> <p>CONTROL 4 Políticas de Desarrollo Seguro</p> <p>CONTROL 5 Fortalecimiento de la configuración de la solución WAF</p> <p>CONTROL 6 Implementación de doble factor de autenticación.</p> <p>CONTROL 7 Fortalecimiento de la Implementación de la protección contra Malware.</p> <p>CONTROL 8 Control de acceso físico Centro de datos y bodega de archivos.</p>	<p>1. Actualización de la Política de respaldos de información, pruebas periódicas de restauración.</p> <p>2. Implementación de controles contra el uso de medios extraíbles.</p> <p>3. Clasificación de los activos de información.</p> <p>4. Revisión y actualización de la Política de Desarrollo Seguro.</p> <p>5. WAF funcional el cual de alcance al monitoreo de todos los activos críticos de la Entidad.</p> <p>6. Implementación de doble factor de autenticación a todos los usuarios dela Entidad.</p>

		<p>7. Llevar a cabo las configuraciones e implementaciones pendientes a mitigar los riesgos de contaminación por Malware.</p> <p>8. Controles de acceso a áreas protegidas o áreas seguras.</p>
<p>Gestión de incidentes</p>	<p>PROYECTOS / ACTIVIDADES 1: Revisión de seguimiento y mejoramiento del procedimiento de Gestión de Incidentes.</p> <p>PROYECTOS / ACTIVIDADES 2: Capacitar al personal en la gestión de incidentes de seguridad de la información.</p> <p>PROYECTOS / ACTIVIDADES 3: Contratación de servicios de SOC y Ethical Hacking.</p>	<ol style="list-style-type: none"> 1. Procedimiento de gestión de incidentes formalizado si este presentara cambio o actualizaciones. 2. Desarrollar Sesiones de capacitación. 3. Contratación de servicios profesionales de SOC y Ethical Hacking.



AÑO 2024				AÑO 2025				AÑO 2026			
TRIMESTRE1	TRIMESTRE2	TRIMESTRE3	TRIMESTRE4	TRIMESTRE1	TRIMESTRE2	TRIMESTRE3	TRIMESTRE4	TRIMESTRE1	TRIMESTRE2	TRIMESTRE3	TRIMESTRE4
		Adquirir una solución de seguridad EDR (ENDPOINT DETECTION AND RESPONSE) licenciada que a través de una plataforma unificada brinde una eficaz detección de amenazas y ciberataques a la infraestructura del Ministerio de Justicia y del Derecho. 157.726.187									
Proyección Plan de Sensibilización 2024		Contratación de servicios orientados a actividades de uso y apropiación y sensibilización. 60.000.000									

Nota: Al finalizar cada vigencia, LA ENTIDAD, realizará una actualización del cronograma, incorporando el estado del avance de los proyectos formulados y si en efecto se cumplieron o se plantean aplazamientos para las vigencias posteriores. Así mismo, el cronograma podrá ser modificado o ajustado de acuerdo con las necesidades o situaciones que surjan en la entidad.

6.4. 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 2024		AÑO 2025		AÑO 2026	
PROYECTO	Inversión	PROYECTO	Inversión	PROYECTO	Inversión
Contratación de servicios profesionales de SOC y Ethical Hacking.	\$ 660.000.000,00	Adquisición de servicios/infraestructura de redundancia para continuidad de TI (DRP)	\$ 1.662.251.256	Actualización e Implementación de solución de respaldos de información para el fortalecimiento de los procesos de Backups y aseguramiento de la información.	\$ 335.000.000
Renovación de servicios de mantenimiento, soporte y garantía de infraestructura de seguridad (WAF nube y Firewall)	\$ 135.529.267,00	Adquisición e implementación de sistemas de seguridad (DLP - Data Loss Prevention) el cual permita llevar a cabo la prevención de la pérdida de datos e información crítica.	\$ 152.289.733	Actualización y renovación de aseguramiento de conexiones remotas y teletrabajo.	\$ 300.000.000
Adquirir una solución de seguridad EDR (ENDPOINT DETECTION AND RESPONSE) licenciada que a través de una plataforma unificada brinde una eficaz detección de amenazas y ciberataques a la infraestructura del Ministerio de Justicia y del Derecho.	\$ 157.726.187,00				
Contratación de servicios orientados a actividades de uso y apropiación y sensibilización.	\$ 60.000.000,00				
TOTAL PRESUPUESTO AÑO 2024	\$ 1.013.255.454	TOTAL PRESUPUESTO AÑO 2025	\$ 1.814.540.989	TOTAL PRESUPUESTO AÑO 2026	\$ 635.000.000
\$ 3.462.796.443					



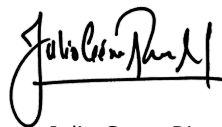


7. RESPONSABLES

1. Dirección de Tecnología DTGIJ: Aprobar los documentos de Alto Nivel
2. Subdirección de Tecnología de Sistemas de Información STSI: Velar por la implementación del MSPI y garantizar los recursos requeridos.
3. Responsables de Seguridad Digital – CIO - Enlace TIC: Coordinar las actividades de implementación del MSPI

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: Jair Caicedo Cortés Cargo: Oficial de Seguridad.	 Nombre: José Eliberto Fonseca Ruíz Cargo: Subdirector de Tecnología y Sistemas de Información.	 Nombre: Julio Cesar Rivera Morato Cargo: Director de Tecnología y Gestión de la Información en Justicia. Fecha:

9. Control de Versiones

Versión	Fecha	Modificación
1.0		Versión inicial del documento