**PRODUCTO TIPO:**

**PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**

**MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES**

**OBJETIVO:**

Brindar a las entidades del Orden Nacional y Territorial, un insumo base o plantilla, para la elaboración del Plan de Seguridad y Privacidad de la Información o Plan Estratégico de Seguridad de la Información (PESI) que permita cumplir con los requisitos del establecimiento de su estrategia de seguridad digital, de acuerdo con lo establecido en el artículo 5 de la resolución 500 de 2021.

**¿COMO USAR LA PLANTILLA?:**

1. Antes de empezar a utilizar la plantilla, se recomienda que la entidad diligencie el “**Instrumento de Autodiagnóstico del Modelo de Seguridad y Privacidad de la Información**”, además de tener presente el contexto interno y externo de la entidad, el tamaño y capacidades tanto de talento humano como capacidades económicas, ya que todos estos insumos son determinantes para poder elaborar de forma adecuada el PESI.
2. La presente plantilla contiene las secciones mínimas recomendadas que todas las entidades deberían tener en cuenta para estructurar un PESI adecuadamente, por tal motivo, no se recomienda eliminar ninguno de los puntos (a menos que la entidad así lo decida), sino que, por el contrario, de ser posible se añadan secciones adicionales para reforzar la estructura de este documento.
3. Revisar cada una de las secciones y completar la plantilla con base a lo que la entidad desea establecer.
4. Una vez diligenciada la plantilla con los lineamientos que la entidad quiere establecer, se deberá realizar la socialización, aprobación y publicación de dicho plan, de acuerdo con lo indicado por el decreto 612 de 2018 y la resolución 500 de 2021 establecida por MinTIC.

**PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**

**(NOMBRE DE LA ENTIDAD)**

**2024**

**Control de Versiones**

|  |  |  |
| --- | --- | --- |
| Versión | Fecha | Modificación |
| 2.0 |  | Versión inicial del documento |
|  |  |  |
|  |  |  |

**TABLA DE CONTENIDO**

[PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 6](#_Toc89670488)

[1. OBJETIVO 6](#_Toc89670489)

[1.1 OBJETIVOS ESPECÍFICOS 6](#_Toc89670490)

[2. ALCANCE 6](#_Toc89670491)

[3. DOCUMENTOS DE REFERENCIA 6](#_Toc89670492)

[4. ESTADO ACTUAL DE LA ENTIDAD RESPECTO AL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN 7](#_Toc89670493)

[5. ESTRATEGIAS 7](#_Toc89670494)

[5.1 DESCRIPCIÓN DE LAS ESTRATEGIAS 8](#_Toc89670495)

[5.2 PORTAFOLIO DE PROYECTOS / ACTIVIDADES: 9](#_Toc89670496)

[5.3 CRONOGRAMA DE ACTIVIDADES / PROYECTOS: 11](#_Toc89670497)

[5.4 ANÁLISIS PRESUPUESTAL: 12](#_Toc89670498)

[6. RESPONSABLES 13](#_Toc89670499)

[7. APROBACIÓN 13](#_Toc89670500)

# PLAN ESTRATEGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

# OBJETIVO

Fortalecer la integridad, confidencialidad y disponibilidad de los activos de información de la Entidad, para reducir los riesgos a los que está expuesta la información en la organización hasta niveles aceptables, a partir de la implementación de las estrategias de seguridad digital definidas en este documento para las vigencias 202x-202x.

## 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 ejecutar 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.

# ALCANCE

El Plan Estratégico de seguridad y privacidad de la Información al buscar la implementación del Sistema de Gestión de Seguridad y privacidad 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. (***Ajustar según el contexto de cada entidad***).

# 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.
* ***Relacionar otros documentos que el PESI tiene o toma como referencia para su definición.***

# ESTADO ACTUAL DE LA ENTIDAD RESPECTO AL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

*(En esta sección, se debe indicar y documentar de la forma más estratégica posible el estado actual de la entidad respecto a la implementación de los lineamientos de seguridad de la información requeridos por el MSPI.*

*Esto permitirá a la entidad establecer la línea base de donde se encuentra la entidad y así proyectar hacía que punto desea llegar con base a las actividades definidas dentro del PESI.*

*Para esto, la entidad puede tomar como base la sección* ***PORTADA*** *del* ***INSTRUMENTO DE EVALUACIÓN MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN****. También podrá emplear insumos como el* ***AUTODIAGNÓSTICO DE GOBIERNO DIGITAL*** *o la* ***MEDICIÓN FURAG*** *para los temas de* ***SEGURIDAD DE LA INFORMACIÓN****).*

# ESTRATEGIA DE SEGURIDAD DIGITAL

LA ENTIDAD 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 y privacidad 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 y debidamente articularse al habilitador de seguridad y privacidad de la Política de Gobierno Digital. (*Ver Resolución 500 de 2021*).

Por tal motivo, ***LA ENTIDAD*** define las siguientes 5 estrategias específicas, que permitirán establecer en su conjunto una estrategia general de seguridad digital:

**Nota: Es fundamental que las entidades hagan la lectura de la resolución 500 de 2021 y del Anexo 1, que contiene la actualización del Modelo de Seguridad y Privacidad de la Información.**

Estrategia de seguridad digital.

## 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 y privacidad 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 | 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 y apropiando al interior de la entidad 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. |

## PORTAFOLIO DE PROYECTOS / ACTIVIDADES:

Para cada estrategia específica, **(*LA ENTIDAD)*** define los siguientes proyectos y productos esperados, que tienen por objetivo lograr la implementación y mejoramiento continuo del Sistema de Gestión de Seguridad de la Información (SGSI). Los proyectos deben estar relacionados tanto con el Manual de políticas como con la política de seguridad definida en la entidad, además estos proyectos deben corresponder a la implementación de controles que permita mitigar riesgos de seguridad de la información que la entidad haya identificado

| ESTRATEGIA / EJE | PROYECTO | PRODUCTOS ESPERADOS |
| --- | --- | --- |
| Liderazgo de seguridad de la información | PROYECTO 1:  Desarrollar e implementar una política de seguridad  PROYECTO 2:  Definición de Roles y Responsabilidades de Seguridad de la Información.  PROYECTO 3 … | Política de Seguridad Formalizada e Implementada.  Definición de los Roles y Responsabilidades en Seguridad de la Información formalizados dentro de las políticas de seguridad. |
| Gestión de riesgos | PROYECTO 1:  Identificar, valorar y clasificar los riesgos asociados a los activos de información  PROYECTO 2:  Definir planes de tratamiento de riesgos de seguridad  ***PROYECTO 3 …*** | Matriz de riesgos de seguridad digital  Definir planes de tratamiento de riesgos |
| Concientización | PROYECTO 1:  Establecer desde el inicio de cada año la planeación de sensibilización para todo el año.  PROYECTO 2:  Realizar jornadas de sensibilización a todo el personal.  PROYECTO 3:  Realizar trasferencia de conocimiento a colaboradores de la Entidad a través de cursos especializados en diferentes temas.  PROYECTO 4:  Medir el grado de sensibilización a toda la Entidad. | 1 plan de cambio, cultura y apropiación que describa las estrategias que se implementarán en la vigencia.  2. Evidencias de las actividades desarrolladas  3. Certificaciones de cursos  4. Resultado de las encuestas de medición |
| Implementación de controles | CONTROL 1  Política de respaldos de información.  CONTROL 2  Procedimiento de Gestión de Cambios.  CONTROL 3  Clasificación de la información.  CONTROL 4  Políticas de Desarrollo Seguro  CONTROL 5  Implementación de solución WAF  ***CONTROL 6 …***  ***CONTROL 7 …*** | Política de respaldos de información.  Procedimiento de Gestión de Cambios.  Clasificación de la información.  Políticas de Desarrollo Seguro  WAF desplegado y funcional. |
| Gestión de incidentes | **PROYECTO 1:**  Definir y formalizar un procedimiento de Gestión de Incidentes de seguridad de la información.  **PROYECTO 2:**  Capacitar al personal en la gestión de incidentes de seguridad de la información.  **PROYECTO 3: …**  **PROYECTO 4: …** | 1. Procedimiento de gestión de incidentes de seguridad formalizado. 2. Sesiones de capacitación desarrolladas. |

## 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.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **AÑO 202X** | | | | | | **AÑO 202X** | | | |
|  | **TRIMESTRE 1** | **TRIMESTRE 2** | **TRIMESTRE 3** | **TRIMESTRE 4** | **RESPONSABLE** | **FECHA** | **TRIMESTRE 1** | **TRIMESTRE 2** | **RESPONSABLE** | **FECHA** |
| **ACTIVIDADADES** | **Realizar diagnóstico seguridad y privacidad** | | Definir y formalizar un procedimiento de Gestión de Incidentes de seguridad de la información. | Capacitar al personal en la gestión de incidentes de seguridad de la información. |  |  | Actualización Diagnóstico de Seguridad |  |  |  |
| **Identificación de activos procesos misionales** | Implementación de solución WAF | | Gestión de Riesgos de Seguridad |  |  | Adquisición e Implementación IPS | |  |  |
| **Desarrollo Plan de Sensibilización 2023** | Adquisición e implementación Sistema de Análisis de Vulnerabilidades | |  |  |  | Desarrollo Sensibilización 2024 | Implementación Estrategias de Capacitación en Seguridad |  |  |

**(Esta tabla solo muestra proyectos de ejemplo, cada entidad debe realizar la identificación de los posibles proyectos a plantear según lo establecido en la sección 5.2 o también con base a los controles o planes de tratamiento de riesgos para mitigar los riesgos de seguridad de la información, con base a la dimensión y necesidades específicas de cada entidad).**

**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.

## 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 | | |
| PROYECTO | **Inversión** | **PROYECTO** | **Inversión** | **PROYECTO** | | **Inversión** |
| Construir los lineamientos técnicos e implementación de controles que se definan en el plan operacional de seguridad y privacidad de la información. | $ 470.000.000 | Implementar el 100% del Modelo de Seguridad y Privacidad de la Información y gestionar la auditoría interna de cumplimiento. | $ 527.280.000 | Mantener el funcionamiento del Modelo de seguridad y privacidad de la Información | | $ 200.000.000 |
| Implementación de solución WAF | $ 150.000.000 | Adquisición y despliegue de soluciones de IPS | $ 200.000.000 | Adquisición Servicio Ethical Hacking | | $ 250.000.000 |
| Adquisición Sistema de Análisis de Vulnerabilidades | $ 100.000.000 | Renovación WAF y Sistema de Análisis de Vulnerabilidades | $ 125.000.000 | Renovación WAF, IPS y Análisis de Vulnerabilidades | | $ 225.000.000 |
| TOTAL PRESUPUESTO AÑO 2022 | **$720,000,000** | **TOTAL PRESUPUESTO AÑO 2023** | **$852,280,000** | **TOTAL PRESUPUESTO AÑO 2024** | | **$274,500,000** |

**(Esta tabla solo muestra valores de referencia, cada entidad debe realizar los estudios de mercado correspondientes para tener plenamente identificados los costos aproximados de cada solución o proyecto, con base a la dimensión y necesidades específicas).**

# RESPONSABLES

1. Alcalde / Gobernador / Ministerio o Representante Legal de la Entidad: Aprobar los documentos de Alto Nivel
2. Secretario (a) General y de Gobierno: Velar por la implementación del MSPI y garantizar los recursos requeridos.
3. Responsable de Seguridad Digital / CIO / Enlace TIC: Coordinar las actividades de implementación del MSPI
4. ***Añadir más responsables o responsabilidades según la entidad considere pertinente.***

# APROBACIÓN

El presente plan ha sido sometido a consideración y conocimiento de la alta dirección, el comité de gestión y desempeño institucional (***ajustar con base al esquema que maneje LA ENTIDAD***) con el objetivo de ser aprobado y aplicado conforme a lo que aquí se define.

|  |  |  |
| --- | --- | --- |
| **ELABORÓ** | **REVISÓ** | **APROBÓ** |
| Nombre:  **Cargo:** | Nombre:  **Cargo:** | Nombre:  **Cargo:**  Fecha: |