PLAN DE SEGURIDAD DE LA INFORMACIÓN

SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Lineamientos GD

MINTIC vive digital Colombia TODOS POR UN NUEVO PAÍS PAZ EQUIDAD EDUCACIÓN

HISTORIA

VERSIÓN	FECHA	CAMBIOS INTRODUCIDOS
1.0.0		Versión inicial del documento

TABLA DE CONTENIDO

PÁG

1. DERECHOS DE AUTOR

2. AUDIENCIA

Este documento está elaborado para las entidades públicas de orden nacional y territorial con el objetivo de servir como guía para el cumplimiento de los requerimientos emitidos mediante el **Decreto 612 de 2018**, específicamente para la generación de los siguientes planes institucionales y estratégicos:

12. Plan de Seguridad y Privacidad de la Información

3. JUSTIFICACIÓN

Este documento se elabora con el objetivo de orientar a las entidades públicas para dar cumplimiento con lo solicitado en el **Decreto 612 de 2018** y todas las consideraciones expuestas, dentro de las cuáles se encuentra el decreto 1078 de 2015 y los instrumentos para implementar la Estrategia de Gobierno en Línea (Ahora **Gobierno Digital**), dentro de los cuales se exige la elaboración por parte de cada entidad, de un ***Plan de Seguridad y Privacidad de la Información***

4. LINEAMIENTOS PARA LA ELABORACIÓN DEL PLAN DE SEGURIDAD DE LA INFORMACIÓN (PESI)

El Plan de Seguridad de la Información (PSI), es un documento que tiene por objetivo trazar y planificar la manera como la entidad realizará o continuará con la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI).

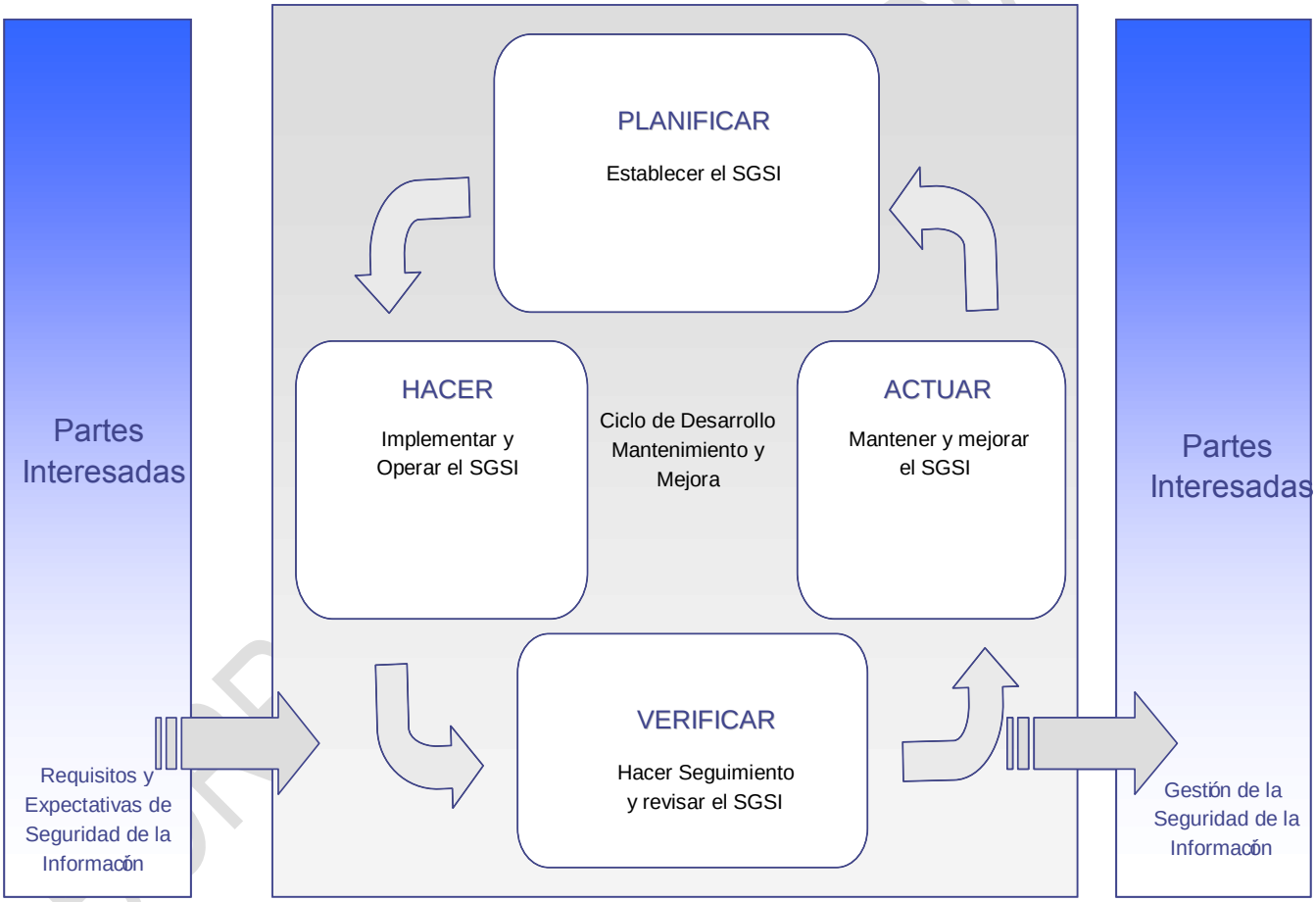
Este documento deberá indicar, definiendo plazos anuales, cuáles serán las labores que realizará la entidad con el objetivo de lograr el 100% de la implementación del MSPI al interior de todos los procesos de la entidad y debería contener como mínimo lo siguiente:

- **REQUISITOS GENERALES**
- **ESTABLECIMIENTO Y GESTION DEL MSPI**
  - ✓ Establecimiento del MSPI
  - ✓ Implementación y operación del MSPI
  - ✓ Seguimiento y revisión del MSPI
  - ✓ Mantenimiento y mejora del MSPI
- **REQUISITOS DE DOCUMENTACION**
  - ✓ Generalidades
  - ✓ Control de Documentos
  - ✓ Control de Registros
- **RESPONSABILIDAD DE LA DIRECCION**
  - ✓ Compromiso de la Dirección
  - ✓ Gestión de Recursos
    - ✓ Provisión de Recursos
    - ✓ Formación, toma de conciencia y competencia
- **AUDITORIAS INTERNAS DEL MSPI**
- **REVISION DEL MSPI POR LA DIRECCION**
  - ✓ Generalidades
  - ✓ Información para la revisión
  - ✓ Resultados de la revisión
- **MEJORA DEL MSPI**
  - ✓ Mejora continua
  - ✓ Acción correctiva
  - ✓ Acción preventiva
- **COMPATIBILIDAD DEL MSPI CON LOS OTROS SISTEMAS DE GESTION**

REQUISITOS GENERALES

Las entidades, a través de **los comités de gestión y desempeño institucional,** impulsarán la implementación del Modelo de Seguridad y Privacidad de la Información **MSPI**, en el contexto de las actividades globales de la entidad y de los riesgos que enfrenta.

Para llevar a cabo este propósito, se basará en el modelo **PHVA**.



Modelo **PHVA aplicado al MSPI**

PLANIFICAR (establecer el MSPI)	Establecer la política, los objetivos, procesos y procedimientos de seguridad pertinentes para gestionar los activos y el riesgo buscando mejorar la seguridad de la información, con el fin de entregar resultados acordes con las políticas y objetivos globales de una organización.
HACER (implementar y operar el MSPI)	Implementar y operar la política, los controles, procesos y procedimientos del MSPI
VERIFICAR (hacer seguimiento y revisar el MSPI)	Evaluar, y, en donde sea aplicable, medir el desempeño del proceso contra la política y los objetivos de seguridad y la experiencia práctica, y reportar los resultados a la dirección, para su revisión.
ACTUAR (mantener y mejorar el MSPI)	Emprender acciones correctivas y preventivas con base en los resultados de la auditoría interna del MSPI y la revisión por la dirección, para lograr la mejora continua del MSPI.

ESTABLECIMIENTO Y GESTION DEL MSPI

Establecimiento del MSPI

La entidad debe;

- Definir el **alcance y límites del MSPI** en términos de las características del servicio que presta el organismo, su estructura interna, su ubicación, sus activos de información, tecnología, e incluir los detalles y justificación de cualquier exclusión del alcance.

- Definir **una política de MSPI** en términos de las características del servicio que presta el organismo, su estructura interna, sus activos de información y tecnología; que:
    - **Incluya un marco de referencia** para fijar objetivos y establezca un sentido general de dirección y principios para la acción con relación a la seguridad de la información.
    - **Tenga en cuenta los requisitos del organismo**, los legales o reglamentarios y las obligaciones de seguridad contractuales
    - **Este alineada con el contexto organizacional** estratégico de gestión del riesgo en el cual tendrá lugar el establecimiento y mantenimiento del MSPI.
    - **Establezca los criterios** contra los cuales se evaluará el riesgo
    - **Haya sido aprobada por la dirección.**

- Definir **el enfoque organizacional** para la valoración del riesgo.
    - **Identificar una metodología de valoración del riesgo** que sea adecuada al MSPI y a los requisitos reglamentarios, legales y de seguridad de la información de la organización, identificados.
    - **Desarrollar criterios para la aceptación de riesgos**, e identificar los niveles de riesgo aceptables.

  La metodología seleccionada para la valoración de riesgos debe asegurar que dichas valoraciones producen resultados comparables y reproducibles.

- Identificar los riesgos
    - Identificar los activos dentro del alcance del MSPI y los propietarios de estos activos de información.
    - Identificar las amenazas a estos activos.
    - Identificar las vulnerabilidades que podrían ser aprovechadas por las amenazas.
    - Identificar los impactos que la perdida de confidencialidad, integridad y disponibilidad puede tener sobre estos activos.
- Analizar y evaluar los riesgos.
    - Valorar el impacto que podría causar una falla en la seguridad, sobre el organismo, teniendo en cuenta las consecuencias de la perdida de confidencialidad, integridad o disponibilidad de los activos.
    - Valorar la posibilidad realista de que ocurra una falla en la seguridad, considerando las amenazas, las vulnerabilidades, los impactos

asociados con estos activos, y los controles implementados actualmente.
    - Estimar los niveles de los riesgos.
    - Determinar la aceptación del riesgo o la necesidad de su tratamiento a partir de los criterios previamente establecidos.
- Identificar y evaluar las opciones para el tratamiento de los riesgos.
  Las posibles acciones incluyen:
    - Aplicar los controles apropiados
    - Aceptar los riesgos con conocimiento y objetividad, siempre y cuando satisfagan claramente la política y los criterios de la organización para la aceptación de riesgos.
    - Evitar riesgos
    - Transferir a otras partes los riesgos asociados con el negocio ej. Aseguradoras, proveedores, etc.
- Seleccionar los objetivos de control y los controles para el tratamiento de los riesgos.

Los objetivos de control y los controles se deben seleccionar e implementar de manera que cumplan los requisitos identificados en el proceso de valoración y tratamiento de riesgos

- Obtener la aprobación de la dirección sobre los riesgos residuales propuestos.
- Obtener autorización de la dirección para implementar y operar el **MSPI**
- Elaborar una declaración de aplicabilidad.

La declaración de aplicabilidad debe incluir;

    - Los objetivos de control y los controles.
    - Los objetivos de control y los controles que ya se hayan implementado.
    - La exclusión de cualquier objetivo de control y controles y la justificación para su exclusión.

- Elaborar un plan de sensibilización y apropiación del MSPI para toda la entidad.

Implementación y operación del MSPI

La entidad debe;

- Formular un plan para el tratamiento de riesgos que identifique la acción de gestión apropiada, los recursos, responsabilidades y prioridades para manejar los riesgos de seguridad de la información.

- Implementar el plan de tratamiento de riesgos para lograr los objetivos de control identificados, que incluye considerar la financiación y la asignación de funciones y responsabilidades.
- Implementar los controles seleccionados, para cumplir los objetivos de control.
- Definir cómo medir la eficacia de los controles o grupos de controles seleccionados y especificar cómo se van a usar estas mediciones con el fin de valorar la eficacia de los controles para producir resultados comparables y reproducibles.
- Implementar programas de formación y de toma de conciencia.
- Gestionar la operación del MSPI.
- Gestionar los recursos del MSPI.
- Implementar procedimientos y otros controles para detectar y dar respuesta oportuna a los incidentes de seguridad.

Seguimiento y revisión del MSPI

La entidad debe;

- Ejecutar procedimientos de seguimiento, revisión y otros controles para;
  - Detectar rápidamente errores en los resultados del procesamiento
  - Identificar con prontitud los incidentes e intentos de violación a la seguridad, tanto los que tuvieron éxito como los que fracasaron.
  - Posibilitar que la dirección determine si las actividades de seguridad delegadas a las personas o implementadas mediante tecnología de la información se están ejecutando en la forma esperada.
  - Ayudar a detectar eventos de seguridad, y de esta manera impedir incidentes de seguridad mediante el uso de indicadores.
  - Determinar si las acciones tomadas para solucionar un problema de violación a la seguridad fueron eficaces.
- Emprender revisiones regulares de la eficacia del MSPI (que incluyen el cumplimiento de la política y objetivos del MSPI, y la revisión de los controles de seguridad) teniendo en cuenta los resultados de las auditorías de seguridad, incidentes, medición de la eficacia sugerencias y retroalimentación de todas las partes interesadas.
- Medir la eficacia de los controles para verificar que se han cumplido los requisitos de seguridad.

- Revisar las valoraciones de los riesgos a intervalos planificados, y revisar el nivel de riesgo residual y riesgo aceptable identificado, teniendo en cuenta los cambios en;
    - La entidad
    - La tecnología
    - Los objetivos y procesos de la entidad
        - Las amenazas identificadas
        - La eficacia de los controles implementados
        - Eventos externos, tales como cambios en el entorno legal o reglamentario, en las obligaciones contractuales, y en el clima social.
- Realizar auditorías internas del MSPI a intervalos planificados
- Emprender una revisión del MSPI, realizada por la dirección, en forma regular para asegurar que el alcance siga siendo suficiente y que se identifiquen mejoras al proceso de MSPI.
- Actualizar los planes de seguridad para tener en cuenta las conclusiones de las actividades de seguimiento y revisión.
- Registrar acciones y eventos que podrían tener impacto en la eficacia o el desempeño del MSPI.

Mantenimiento y mejora del MSPI

La entidad debe, regularmente;

- Implementar las mejoras identificadas en el MSPI
- Emprender las acciones correctivas y preventivas adecuadas, aplicando las lecciones aprendidas de las experiencias de seguridad de otras organizaciones y las de la propia organización.
- Comunicar las acciones y mejoras a todas las partes interesadas, con un nivel detalle apropiado a las circunstancias y en donde sea pertinente, llegar a acuerdos sobre cómo proceder.
- Asegurar que las mejoras logran los objetivos previstos.

REQUISITOS DE DOCUMENTACION

Generalidades

La documentación del MSPI debe incluir registros de las decisiones de la dirección, asegurar que las acciones sean trazables a las decisiones y políticas de la alta dirección, y que los resultados registrados sean reproducibles.
Es importante estar en capacidad de demostrar la **relación** entre los **controles** seleccionados y los **resultados** del proceso de valoración y tratamiento de riesgos al igual que con la **política** y **objetivos** del MSPI.

La documentación del MSPI debe incluir;

- Declaraciones documentadas de la política y objetivos del MSPI.
- El alcance del MSPI.
- Los procedimientos y controles que apoyan el MSPI.
- Una metodología de Gestión de Activos
- Una descripción de la metodología de valoración de riesgos.
- El informe de valoración de riesgos.
- El plan de tratamiento de riesgos.
- Los procedimientos documentados que necesita la organización para asegurar la eficacia de la planificación, operación y control de sus procesos de seguridad de la información, y para describir como mediar la eficacia de los controles.
- Los registros exigidos por la norma ISO 27001 y el MSPI, ej. Un libro de visitantes, informes de auditoría y formatos de autorización de acceso diligenciados.
- La declaración de la aplicabilidad (Opcional para el MSPI)

Control de documentos

Los documentos exigidos por el MSPI se deben proteger y controlar. Se debe establecer un procedimiento documentado para definir las acciones de gestión necesaria para:

- Aprobar los documentos en cuanto a su suficiencia antes de su publicación.
- Revisar y actualizar los documentos según sea necesario y reprobarlos
- Asegurar que los cambios y el estado de actualización de los documentos estén identificados.
- Asegurar que las versiones más recientes de los documentos pertinentes están disponibles en los puntos de uso.
- Asegurar que los documentos permanezcan legibles y fácilmente identificables.

- Asegurar que los documentos estén disponibles para quienes lo necesiten, y que se apliquen los procedimientos pertinentes, de acuerdo con su clasificación, para su transferencia, almacenamiento y disposición final.
- Asegurar que los documentos de origen externo estén identificados.
- Asegurar que la distribución de documentos este controlada.
- Impedir el uso no previsto de los documentos obsoletos.
- Aplicar la identificación adecuada a los documentos obsoletos, si se retienen para cualquier propósito.

Control de registros

- Se deben establecer y mantener registros para brindar evidencia de la conformidad con los requisitos y la operación eficaz del MSPI.
- Los registros deben estar protegidos y controlados.
- El MSPI debe tener en cuenta cualquier requisito legal o reglamentario y las obligaciones contractuales pertinentes.
- Los registros deben permanecer legibles, fácilmente identificables y recuperables.
- Se deben documentar e implementar los controles necesarios para la identificación, almacenamiento, protección, recuperación, tiempo de retención y disposición de registros.
- Se deben llevar registros del desempeño del proceso y de todos los casos de incidentes de seguridad significativos relacionados con el MSPI.

RESPONSABILIDADES DE LA DIRECCION

Compromiso de la dirección

La dirección de la entidad debe bridar evidencia de su compromiso con el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora del MSPI:

- Mediante el establecimiento de una política del MSPI.
- Asegurando que se establezcan los objetivos y planes del MSPI.
- Estableciendo funciones y responsabilidades de seguridad de la información.
- Comunicando a la organización la importancia de cumplir los objetivos de seguridad de la información y de la conformidad con la política de seguridad de la información, sus responsabilidades bajo la ley, y la necesidad de la mejora continúa.

- Brindando los recursos suficientes para establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar un MSPI.
- Decidiendo los criterios para aceptación de riesgos y los niveles de riesgo aceptables.
- Asegurando que se realizan auditorías internas del MSPI.
- Efectuando las revisiones por la dirección, del MSPI.

Gestión de recursos

Provisión de recursos

La entidad debe determinar y suministrar los recursos necesarios para:

- Establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar el MSPI.
- Asegurar que los procedimientos de seguridad de la información brindan apoyo a los requisitos del Instituto.
- Identificar y atender los requisitos legales y reglamentarios, así como las obligaciones de seguridad contractuales.
- Mantener la seguridad suficiente mediante la aplicación correcta de todos los controles implementados.
- Llevar a cabo revisiones cuando sea necesario, y reaccionar apropiadamente a los resultados y en donde se requiera mejorar la eficacia del MSPI.

Formación, toma de conciencia y competencia.

La entidad debe asegurar que todo el personal al que se asigne responsabilidades definidas en el MSPI sea competente para realizar las tareas exigidas, mediante:

- La determinación de las competencias necesarias para el personal que ejecute el trabajo que afecta el MSPI.
-
- El suministro de formación o realización de otras acciones (ej. Contratación de personal competente) para satisfacer las necesidades.
- La evaluación de la eficacia de las acciones emprendidas

- El mantenimiento de registros de la educación, formación, habilidades, experiencia y calificaciones.

AUDITORIAS INTERNAS DEL MSPI

La entidad debe llevar a cabo auditoria internas del MSPI a intervalos planificados, para determinar si los objetivos de control, controles, procesos y procedimientos del MSPI:

- Cumplen los requisitos de la presente norma y de la legislación o reglamentaciones pertinentes.
- Cumplen los requisitos identificados de seguridad de la información.
- Están implementados y se mantienen eficazmente.
- Tienen un desempeño acorde con lo esperado.

La norma NTC-ISO 19011:2002, Directrices para la auditoria de los sistemas de gestión de la calidad y/o ambiente puede brindar orientación útil para la realización de auditorías internas del MSPI.

REVISION DEL MSPI POR LA DIRECCION

Generalidades

La dirección de La entidad debe revisar el MSPI de la organización a intervalos planificados (por lo menos una vez al año), para asegurar su conveniencia, suficiencia y eficacia. Esta revisión debe incluir la evaluación de las oportunidades de mejora y la necesidad de cambios del MSPI, incluidos la política de seguridad y los objetivos de seguridad. Los resultados de las revisiones se deben documentar claramente y se deben llevar registros.

Información para la revisión

Las entradas para la revisión por la dirección deben incluir:

- Resultados de las auditorias y revisiones del MSPI.
- Retroalimentación de las partes interesadas.
- Técnicas, productos o procedimientos que se pueden usar en la organización para mejorar el desempeño y eficacia del MSPI.
- Estado de las acciones correctivas y preventivas

- Vulnerabilidades o amenazas no tratadas adecuadamente en la valoración previa de los riesgos.
- Resultados de las mediciones de eficacia.
- Acciones de seguimiento resultante de revisiones anteriores por la dirección.
- Cualquier cambio que pueda afectar el MSPI.
- Recomendaciones para mejoras.

Resultados de la revisión

Los resultados de la revisión por la dirección deben incluir cualquier decisión y acción relacionada con:

- La mejora de la eficacia del MSPI.
- La actualización de la evaluación de riesgos y del plan de tratamiento de riesgos.
- La modificación de los procedimientos y controles que afectan la seguridad de la información, según sea necesario, para responder a eventos internos o externos que pueden tener impacto en el MSPI, incluidos cambios a:
  - Los requisitos de la organización
  - Los requisitos de seguridad
  - Los procesos del organismo que afectan los requisitos del negocio existentes.
  - Los requisitos reglamentarios o legales.
  - Las obligaciones contractuales.
  - Los niveles de riesgo y/o niveles de aceptación de riesgos.
- Los recursos necesarios.
- La mejora a la manera en que se mide la eficacia de los controles.

MEJORA DEL MSPI

Mejora continua

La entidad debe mejorar continuamente la eficacia del MSPI mediante;

- El uso de la política de seguridad de la información.
- Los objetivos de seguridad de la información.
- Los resultados de la auditoría.
- El análisis de los eventos a los que se les ha hecho seguimiento.
- Las acciones correctivas y preventivas y la revisión por la dirección.

Acción correctiva

La entidad debe emprender acciones para eliminar la causa de no conformidades asociadas con los requisitos del MSPI, con el fin de prevenir que ocurran nuevamente.
El procedimiento documentado para la acción correctiva debe definir requisitos para:

- Identificar las no conformidades
- Determinar las causas de las no conformidades.
- Evaluar la necesidad de acciones que aseguren que las no conformidades no vuelven a ocurrir.
- Determinar e implementar la acción correctiva necesaria.
- Registrar los resultados de la acción tomada.
- Revisar la acción tomada.

Acción preventiva

La entidad debe determinar acciones para eliminar la causa de no conformidades potenciales con los requisitos del MSPI y evitar que ocurran. Las acciones preventivas tomadas deben ser apropiadas al impacto de los problemas potenciales.
El procedimiento documentado para la acción preventiva debe definir requisitos para:

- Identificar no conformidades potenciales y sus causas.
- Evaluar la necesidad de acciones para impedir que las no conformidades ocurran.
- Determinar e implementar la acción preventiva necesaria.
- Registrar los resultados de la acción tomada.
- Revisar la acción preventiva tomada.

COMPATIBILIDAD DEL MSPI CON OTROS SISTEMAS DE GESTION

El MSPI está alineado con la norma NTC/IEC ISO 27001 y con la NTC-ISO 9001:2000, con el fin de apoyar la implementación y operación, consistentes e integradas con sistemas de gestión relacionados.