PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DIGITAL 2023

Versión 1

MINISTERIO DE EDUCACIÓN
NACIONAL

Tabla de contenido

I. INTRODUCCIÓN

El Ministerio de Educación Nacional de acuerdo con lo indicado por el Ministerio de Tecnologías de la Información y las Comunicaciones – MINTIC, en la resolución 500 de 2021[1] que indica los lineamientos a seguir para dar cumplimiento a un MSPI (Modelo de Seguridad y Privacidad de la Información) efectivo:

"ARTÍCULO 3. Lineamientos generales. Los sujetos obligados deben adoptar medidas técnicas, administrativas y de talento humano para garantizar que la seguridad digital se incorpore al plan de seguridad y privacidad de la información y así mitigar riesgos relacionados con la protección y la privacidad de la información e incidentes de seguridad digital. Las entidades deben contar con políticas, procesos, procedimientos, guías, manuales y formatos para garantizar el cumplimiento al ciclo PHVA del MSPI. En ese sentido, deben adoptar los lineamientos del MSPI, guía de riesgos y gestión de incidentes de seguridad digital que se relacionan en el Anexo 1 de la presente resolución.

Para todos los procesos, trámites, servicios de información, infraestructura tecnológica e infraestructura critica de los sujetos obligados, se deben adoptar medidas de seguridad eficientes alienadas al MSPI, para prestar servicios de confianza, generando protección de la información de los ciudadanos, gestionando los riesgos y los incidentes de seguridad digital.

ARTÍCULO 4. Sistema de gestión de seguridad de la información y seguridad digital. Los sujetos obligados deben aplicar los modelos, guías, y demás documentos técnicos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones a través del habilitador de seguridad y privacidad de la información en el marco de la Política de Gobierno Digital y propenderán por la incorporación de estándares internacionales y sus respectivas actualizaciones o modificaciones, al igual que otros marcos de trabajo que defina mejores prácticas en la materia.

ARTÍCULO 5. La estrategia de seguridad digital. Los sujetos obligados deben adoptar la 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 digital. Dicha estrategia se debe incluir en el Plan de Seguridad y Privacidad de la Información que se integra al Plan de Acción en los términos artículo 2.2.22.3.14. del capítulo 3 del Título 22 de la Parte 2 del Libro 2 del Decreto 1083 de 2015, Único Reglamentario del Sector de Función Pública, o la norma que la modifique, adicione, subrogue o derogue.

El Plan de Seguridad y Privacidad de la Información contempla la protección de la información digital, medios impresos y físicos digitales y no digitales.

[1] https://gobiernodigital.mintic.gov.co/692/articles-162625_recurso_2.pdf

La estrategia de seguridad digital debe definirse en 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 de seguridad digital, incorporadas en el Anexo 1 de la presente resolución y estar debidamente articulada al habilitador de seguridad y privacidad de la Política de Gobierno Digital.

Adicionalmente, la estrategia de seguridad digital debe:

1. Ser aprobada a través de un acto administrativo de carácter general.
2. Contar con un análisis y tratamiento de riesgos de seguridad digital e implementar controles que permitan gestionarlos.
3. Establecer los roles y responsabilidades al interior de la entidad asociados a la seguridad digital.
4. Establecer e implementar los principios, lineamientos y estrategias para promover una cultura para la seguridad digital y de la información que incluya actividades de difusión, capacitación y concientización tanto al interior de la entidad como frente a usuarios y terceros que ésta considere relevantes para mejorar habilidades y promover conciencia en la seguridad de la información. Estas actividades deben realizarse anualmente y pueden incluirse, adicionalmente, en el Plan Institucional de Capacitaciones PIC, o el que haga sus veces.
5. La estrategia debe incluir todas las tecnologías de la información y las comunicaciones que utiliza la organización, incluida la adopción de nuevas tecnologías o tecnologías emergentes.
6. Aplicar las demás consideraciones que a juicio de la entidad contribuyan a elevar sus estándares de seguridad digital.

Parágrafo 1. Los sujetos obligados deben adoptar el Modelo de Seguridad y Privacidad de la Información – MSPI señalado en el Anexo 1 de la presente resolución, como habilitador de la política de Gobierno Digital".

Dicho lo anterior, se construye un plan de trabajo de mejora continua para seguir fortaleciendo el modelo de seguridad y privacidad del Ministerio de Educación con el fin de generar confianza en el tratamiento de la información en todos los procesos de la entidad.

II. OBJETIVO

Realizar un proceso de mejora continua de acuerdo con el Modelo de Seguridad y Privacidad de la Información (https://gobiernodigital.mintic.gov.co/692/articles-162625_recurso_1.pdf), el cual, está alineado con la norma NTC/IEC ISO 27001:2013.

III. ALCANCE

El presente plan tiene como propósito mejorar el desempeño de seguridad digital para todos los procesos del Ministerio de Educación Nacional aplicándolo a todos los niveles funcionales y

organizacionales, propendiendo por la confidencialidad, integridad y disponibilidad de los servicios de información.

Al final de la ejecución de este plan, se contará con procesos y procedimientos más maduros a nivel de seguridad digital.

IV. DEFINICIONES [2]

Activo: en relación con 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).

Activos de Información y recursos: se refiere a elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo. (CONPES 3854 de 20116).

Archivo: conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o Entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3).

Amenazas: causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

Análisis de Riesgo: proceso para comprender la naturaleza del riesgo y determinar el nivel de dicho riesgo. (ISO/IEC 27000).

Auditoría: proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (ISO/IEC 27000).

Autorización: consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3)

Bases de Datos Personales: conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3)

[2] https://gobiernodigital.mintic.gov.co/692/articles-162625_recurso_1.pdf

Ciberseguridad: protección de activos de información, mediante el tratamiento de las amenazas que ponen en riesgo la información que se procesa almacena y transporta mediante los servicios de información que se encuentran interconectados.

Ciberespacio: es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

Control: las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

Datos Personales: cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

Datos Personales Públicos: es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3)

Datos Personales Privados: es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h)

Datos Personales Mixtos: para efectos de este documento es la información que contiene datos personales públicos junto con datos privados o sensibles.

Datos Personales Sensibles: se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3)

Derecho a la Intimidad: derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).

Encargado del Tratamiento de Datos: persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento. (Ley 1581 de 2012, art 3)

Gestión de incidentes de seguridad de la información: procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

Información Pública Clasificada: es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)

Información Pública Reservada: es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)

Ley de Habeas Data: se refiere a la Ley Estatutaria 1266 de 2008.

Ley de Transparencia y Acceso a la Información Pública: se refiere a la Ley Estatutaria 1712 de 2014.

Plan de continuidad del negocio: plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).

Plan de tratamiento de riesgos: documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

Responsable del Tratamiento de Datos: persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art. 3).

Riesgo: posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

Seguridad de la información: preservación de la confidencialidad, integridad, y disponibilidad de la información en cualquier medio: impreso o digital. (ISO/IEC 27000).

Seguridad digital: preservación de la confidencialidad, integridad, y disponibilidad de la información que se encuentra en medios digitales.

Titulares de la información: personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3)

Tratamiento de Datos Personales: cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).

Trazabilidad: cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o Entidad. (ISO/IEC 27000).

Vulnerabilidad: debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

V. NORMATIVIDAD Y METODOLOGÍA

El Ministerio de Educación ha desarrollado el modelo de seguridad y privacidad de la información de acuerdo con las siguientes resoluciones:

1. Resolución No. 017564 31 DIC 2019 en su Artículo 3. Modelos referenciales del Sistema Integrado de Gestión del Ministerio de Educación Nacional indica:
"Sistema de Gestión de Seguridad de la Información, recoge los lineamientos del Ministerio de las TIC para el desarrollo de la política de seguridad digital de MIPG, que busca gestionar adecuadamente la seguridad y privacidad de los activos de información, en el marco de la estrategia de «Gobierno Digital antes Gobierno en Línea» establecido en el Decreto 2573 del año 2014 y el Decreto 1078 de 2015".

"Política SIG: El Ministerio de Educación Nacional se compromete a implementar y mejorar continuamente el SIG, articulando sus procesos entre sí y con las políticas de gestión y desempeño de MIPG, cumpliendo los requisitos de los modelos referenciales y demás normas que le sean aplicables y garantizando la calidad de los servicios que ofrece, a través de la gestión de los riesgos que puedan afectar el logro de sus objetivos institucionales, la protección del medio ambiente, la seguridad de la información y el bienestar integral de los colaboradores. Asimismo, se compromete con la escucha y análisis de las necesidades y expectativas de los grupos de valor, como parte de la evaluación periódica del cumplimiento y del desempeño del sistema, rindiendo cuentas sobre las decisiones tomadas para asegurar su conveniencia, adecuación, eficacia y alineación con las metas estratégicas de la entidad"

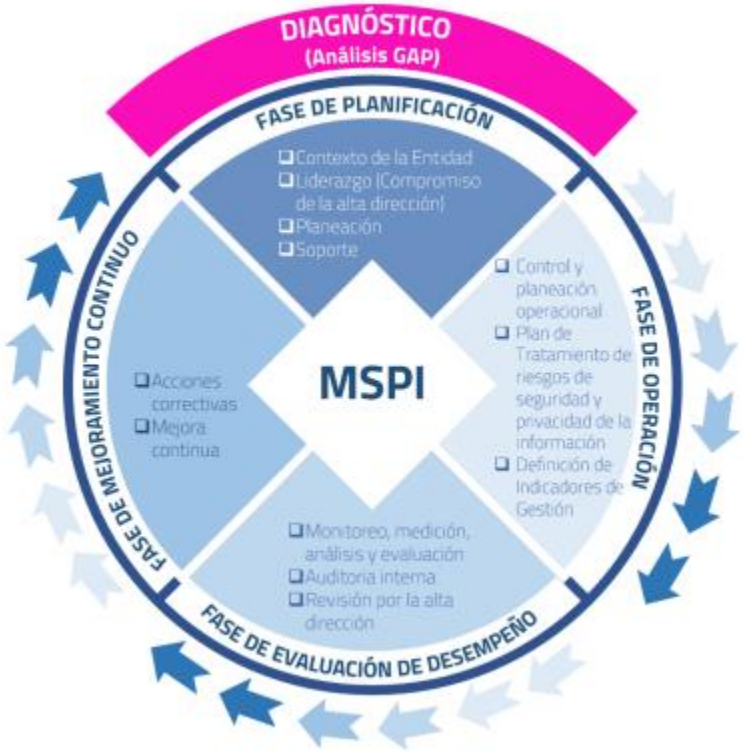
2. Resolución 10491 de 2021 Artículo 1. Adoptar las Políticas de Gestión y Desempeño Institucional. Adóptese como Políticas de Gestión y Desempeño Institucional las siguientes:

• Planeación Institucional
• Gestión presupuestal y eficiencia del gasto público
• Talento humano

- Integridad
- Transparencia, acceso a la información pública y lucha contra la corrupción
- Fortalecimiento organizacional y simplificación de procesos
- Servicio al ciudadano
- Participación Ciudadana en la gestión pública
- Racionalización de trámites
- Gestión documental
- Gobierno Digital, antes Gobierno en Línea
- **Seguridad Digital**
- Defensa jurídica
- Gestión de conocimiento y la innovación
- Control interno
- Seguimiento y evaluación de desempeño institucional
- Mejora normativa

METODOLOGÍA

La metodología que se aplicará para este plan corresponde a lo que se conoce como Planear, Hacer, Verificar y Actuar que en el nuevo modelo indicado por MinTIC corresponde a:



En el momento se cuenta con un manual de seguridad, un manual de gestión de incidentes de seguridad de la información, un manual de política de tratamiento de datos personales y 23 guías de política:

Guía de Política de adquisición desarrollo y mantenimiento de sistemas
Guía de Política seguridad en los procesos de desarrollo y soporte
Guía de Política de escritorio y pantalla limpios
Guía de Política de seguridad física y del entorno
Guía de Política de seguridad de las operaciones
Guía de Política de dispositivos móviles y teletrabajo
Guía de Política de seguridad de la información en los recursos humanos
Guía de Política de usos de controles criptográficos
Guía de Política de cumplimiento de requisitos legales y contractuales
Guía de Política de gestión de seguridad de las redes
Guía de Política de seguridad de la gestión de continuidad de negocio
Guía de Política de gestión de incidentes de seguridad de la información
Guía de Política de transferencia de información
Guía de Política de seguridad para proveedores
Guía de clasificación de la información MEN
Guía de Política de uso adecuado de los recursos tecnológicos
Guía de Política de control de acceso
Guía de Política de seguridad en la nube
Guía de Política de organización interna
Guía para despliegue de servicio de análisis forense digital
Guía de Política de gestión de activos de información
Lineamiento Activos de Software
Lineamientos para el plan de toma de conciencia del SGSI

Y siete procedimientos:

Procedimiento Gestión de Seguridad de la Información
Procedimiento Gestión De Activos De Información
Procedimiento Gestión de incidentes mayores
Procedimiento Gestión de incidentes de seguridad de la información
Procedimiento Activos - Software
Procedimiento - Backup y Restauración
Procedimiento gestión de acceso e identidades

Estos documentos son revisados periódicamente (mínimo una vez al año) con el fin de identificar puntos de mejora. Así mismo se realiza el autodiagnóstico recomendado por MinTIC que permite validar las mejoras implementadas y proceder con un plan para fortalecer los controles que tienen una menor calificación.

Como se puede observar el Ministerio de Educación se encuentra en la fase de mejoramiento continuo.

VI. CUMPLIMIENTO DE LA IMPLEMENTACIÓN

Con el fin de asegurar el cumplimiento del plan de trabajo que se describe en el presente documento, se llevará a cabo un seguimiento de manera mensual por parte de la Oficina Asesora de Planeación y Finanzas y a su vez serán un punto de apoyo para fortalecer las actividades que se estarán ejecutando.

VII. NIVEL DE MADUREZ DEL SGSI

Para identificar el nivel de madurez que se tiene en el Ministerio de Educación Nacional es necesario que se diligencie la herramienta de autodiagnóstico (Análisis GAP), la cual, permite ir evaluando las brechas y mejoras que se tienen sobre el modelo de seguridad y privacidad de la información, y seguir construyendo un plan de mejora, en cada vigencia.
Por lo anterior, es necesario validar al inicio de cada vigencia las actualizaciones al instrumento realizadas por parte de MinTIC, con el fin de adoptar las medidas correspondientes en el presente plan.

VIII. PLAN DE MEJORAMIENTO CONTINUO - CRONOGRAMA

A continuación, se detallan las actividades que se desarrollarán para fortalecer el modelo de seguridad y privacidad de la información actual del Ministerio de Educación Nacional.

IDENTIFICACIÓN DE ACTIVOS DE INFORMACIÓN

Al momento de generar controles es necesario conocer primero qué es lo que se va a proteger, por lo que se debe realizar, como mínimo, una capacitación con los enlaces (personas que conocen cada proceso del Ministerio y son designadas por el directivo de área) para identificar y/o actualizar los activos de información que aportan valor agregado al proceso y por tanto necesitan ser protegidos de potenciales riesgos.

Teniendo identificados los activos de información se realiza la respectiva clasificación de acuerdo con la triada: integridad, confidencialidad y disponibilidad para garantizar que la información recibe los niveles de protección adecuados. Una vez establecida la matriz de activos, ésta debe ser publicada en el Sistema Integrado de Gestión - SIG.

Para llevar a cabo la capacitación mencionada anteriormente, es necesario validar si existe alguna nueva reglamentación sobre el procedimiento que se está llevando actualmente en la entidad para realizar el ajuste y la publicación en el SIG.

Las tareas que se desarrollarán son:
Definir enlaces de cada área para identificación de activos

Actualizar metodología en caso de ser necesario
Capacitar a los enlaces sobre la metodología a aplicar
Actualizar activos de información
Validar la actualización realizada
Consolidar la información recopilada y cargarla en el SIG
Publicar los activos de información en los sistemas correspondientes

GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

La Subdirección de Desarrollo Organizacional será la encargada de validar y/o actualizar el procedimiento para la administración de riesgos de seguridad donde se incluye el apartado de seguridad de la información y seguridad digital. Es así como se brindará la capacitación preferiblemente al mismo equipo humano que participó en la identificación de activos de información permitiendo así, que se generen las salvaguardas correspondientes y, de ser necesario, la creación de planes de mejoramiento para la eliminación o mitigación de los riesgos, con el fin de llevarlo a valores aceptables por cada proceso de la entidad.

El seguimiento a las salvaguardas y a los planes de mejora serán realizados por la Subdirección de Desarrollo Organizacional y Control Interno, con el fin de asegurar el cumplimiento de las fechas establecidas.

Las tareas que se desarrollarán son:
Actualizar de ser necesario los lineamientos de tratamiento de riesgos
Capacitar a los enlaces sobre la metodología a aplicar
Identificar riesgos de seguridad digital para los activos de información identificados en la actividad anterior
Actualizar mapa de riesgos
Realizar seguimiento a los controles y planes de mejora

APROPIACIÓN DEL SISTEMA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Para que un modelo de seguridad y privacidad de la información tenga resultados exitosos es necesario que todos los lineamientos sean socializados con los colaboradores de la entidad, de tal manera que se promueva una cultura digital, con el fin de estar atentos a todos los riesgos de seguridad digital en las labores diarias, ya sea dentro de las instalaciones del Ministerio o en la modalidad de teletrabajo.

Por lo anterior es necesario definir, por medio del formato de toma de conciencia del Sistema Integrado de Gestión, las temáticas que serán socializadas por los diferentes medios dispuestos por el Ministerio, entre los cuales se encuentran el Pregonero y RadioMEN.

Es importante, así mismo, realizar ejercicios de ingeniería social para evaluar el nivel de conciencia de los usuarios finales con respecto a mensajes falsos con los cuales puede comprometer la seguridad de la información de los activos que maneja.

Las tareas que se desarrollarán son:
Definir temáticas a sensibilizar
Diligenciar formato de toma de conciencia
Crear piezas de sensibilización para enviar por los medios dispuestos
Enviar piezas de sensibilización
Realizar ejercicios de ingeniería social

PLAN DE RECUPERACIÓN DE DESASTRES

Con la finalidad de reducir las afectaciones que puedan llegar a existir ante la materialización de un riesgo de seguridad digital, es necesario actualizar la estrategia de recuperación de desastres, para lo cual, se debe iniciar con la actualización del BIA (Business Continuity Plan) para determinar los sistemas más críticos y los que se deben recuperar primero.

Con este insumo se actualizará la estrategia del DRP (Disaster Recovery Plan) y la manera en que periódicamente se deberá probar la efectividad de este.

Una vez cumplido con estos documentos se debe publicar la información sobre el SIG.

Las tareas que se desarrollarán son:
Actualizar documentación del Análisis de Impacto del Negocio
Actualizar la documentación de estrategias del plan de recuperación de desastres
Realizar pruebas de las estrategias del plan de recuperación
Ajustar documentación de la estrategia de ser necesaria de acuerdo con la tarea anterior

AUDITORÍAS

Una parte esencial para la mejora continua del MSPI es realizar auditorías a las políticas y controles definidos en la declaración de aplicabilidad; por consiguiente, desde la Oficina de Tecnología y Servicios de información se participará activamente en estas sesiones de trabajo y en los planes de mejoramiento, en caso de ser encontrada alguna oportunidad de mejora.

SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN

Participar en las sesiones de comités directivos para presentar los avances realizados al MSPI, planes de mejoramiento y los indicadores que se tienen definidos en el SIG y recibir la retroalimentación correspondiente por parte del comité.

ACTUALIZACIÓN Y CREACIÓN DE POLÍTICAS

Actualizar cuando se requiera la documentación sobre los manuales, políticas y procedimientos y publicarlas en el SIG.

Las tareas que se desarrollarán son:
Validar las políticas y procedimientos existentes
Actualizar políticas y procedimientos en caso de ser necesario
Publicar las políticas y/o procedimientos con los ajustes correspondientes

REVISIÓN DE CONTROLES

Validar el cumplimiento de los controles definidos en las políticas que se tienen implementadas en el Ministerio y que están en la declaración de aplicabilidad y ejecutar acciones de mejora, en caso de requerirse.
Las tareas que se desarrollarán son:
Validar la correcta implementación de los controles definidos
Realizar ajuste a los controles en caso de ser necesario

Actividad	Tarea	Responsable	Comienzo	Fin
Identificar de activos de información	Definir enlaces de cada área para identificación de activos	Jefes de Área	6/02/2023	28/02/2023
	Actualizar metodología en caso de ser necesario	Oficina de Tecnología y Servicios de información - OTSI	6/02/2023	6/03/2023
	Capacitar a los enlaces sobre la metodología a aplicar	OTSI - Enlaces de cada proceso	17/03/2023	31/03/2023
	Actualizar activos de información	Enlaces de cada proceso	3/04/2023	3/05/2023
	Validar la actualización realizada	OTSI	4/05/2023	18/05/2023
	Consolidar la información recopilada y cargarla en el SIG	OTSI - Subdirección de Desarrollo Organizacional (SDO)	19/05/2023	2/06/2023
	Publicar los activos de información en los sistemas correspondientes	OTSI – Oficina Asesora de Comunicaciones (OAC)	5/06/2023	9/06/2023
Gestionar riesgos de seguridad de la información	Actualizar, de ser necesario, los lineamientos de tratamiento de riesgos	Oficina de Control Interno (OCI) y SDO	6/02/2023	18/05/2023
	Capacitar a los enlaces sobre la metodología a aplicar	OTSI	13/06/2023	14/07/2023

	Identificar riesgos de seguridad digital para los activos de información identificados en la actividad anterior	OTSI - Enlaces de cada proceso	17/07/2023	14/08/2023
	Actualizar mapa de riesgos	OTSI - SDO	14/08/2023	31/08/2023
	Realizar seguimiento a los controles y planes de mejora	OCI y SDO	31/08/2023	15/12/2023
Apropiación del SGSI	Definir temáticas a sensibilizar	OTSI	6/02/2023	15/02/2023
	Diligenciar formato de toma de conciencia	OTSI	15/02/2023	15/02/2023
	Crear piezas de sensibilización para enviar por los medios dispuestos	OTSI	15/02/2023	1/11/2023
	Enviar piezas de sensibilización	OAC	1/03/2023	15/11/2023
	Realizar ejercicios de ingeniería social	OTSI	6/02/2023	30/11/2023
Crear plan de recuperación de desastres	Actualizar documentación del Análisis de Impacto del Negocio	OTSI - Enlaces de cada proceso	6/02/2023	14/04/2023
	Actualizar la documentación de estrategias del plan de recuperación de desastres	OTSI	14/04/2023	15/05/2023
	Realizar pruebas de las estrategias del plan de recuperación	OTSI - líderes funcionales	15/05/2023	15/11/2023
	Ajustar documentación de la estrategia, de ser necesaria, de acuerdo con la tarea anterior	OTSI	15/05/2023	15/11/2023
Participar en auditorias	Participar en las auditorías internas y externas que sean requeridas	OTSI	6/02/2023	29/12/2023
Seguimiento al SGSI	Participar en las sesiones de comités directivos para mostrar los avances sobre el SGSI	OTSI	6/02/2023	29/12/2023
Actualizar políticas	Validar las políticas y procedimientos existentes	OTSI	6/02/2023	30/11/2023
	Actualizar políticas y procedimientos en caso de ser necesario	OTSI	6/02/2023	30/11/2023
	Publicar las políticas y/o procedimientos con los ajustes correspondientes	SDO	6/02/2023	30/11/2023
Revisar controles	Validar la correcta implementación de los controles definidos	OTSI	6/02/2023	30/11/2023

	Realizar ajuste a los controles en caso de ser necesario	OTSI	6/02/2023	30/11/2023

IX. ANEXOS

Cronograma SGSI_ MEN 2023.xlsx

X. CONTROL DE CAMBIOS

Control de Cambios		
Versión	**Fecha**	**Observaciones**
1	Enero 2023	Se crea el documento de conformidad con los lineamientos institucionales establecidos y la normatividad vigente.

MINISTERIO DE EDUCACIÓN NACIONAL

Mineducacion

@Mineducacion

@Mineducacion

@Mineducacioncol