PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

TECNOLOGÍA DE LA INFORMACIÓN

Fecha de elaboración: Cali, enero 2024

INTRODUCCIÓN

INTENALCO Educación Superior, es una Institución Educativa de carácter oficial nacional con aprobación del ICFES y el Ministerio de Educación Nacional (MEN) mediante la Resolución No. 2903 del 17 de noviembre de 1992, está comprometida con la implementación y cumplimiento de los lineamientos establecidos por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), según la Resolución 500 de 2021. Esta resolución establece los parámetros para la adopción de un Modelo de Seguridad y Privacidad de la Información (MSPI).

En concordancia con el artículo 3 de dicha resolución, INTENALCO se compromete a adoptar medidas técnicas, administrativas y de talento humano para integrar la seguridad digital en su Plan de Seguridad y Privacidad de la Información, con el objetivo de mitigar riesgos asociados a la protección y privacidad de la información, así como a incidentes de seguridad digital. La entidad se esfuerza por contar con políticas, procesos, procedimientos, guías, manuales y formatos que garanticen el cumplimiento del ciclo PHVA del MSPI.

Asimismo, según el artículo 4, INTENALCO implementará el Sistema de Gestión de Seguridad de la Información y Seguridad Digital, siguiendo los modelos, guías y documentos técnicos emitidos por el MinTIC a través del habilitador de seguridad y privacidad de la información, en el marco de la Política de Gobierno Digital. Se buscará la incorporación de estándares internacionales y sus actualizaciones, así como otros marcos de trabajo que definan mejores prácticas en la materia.

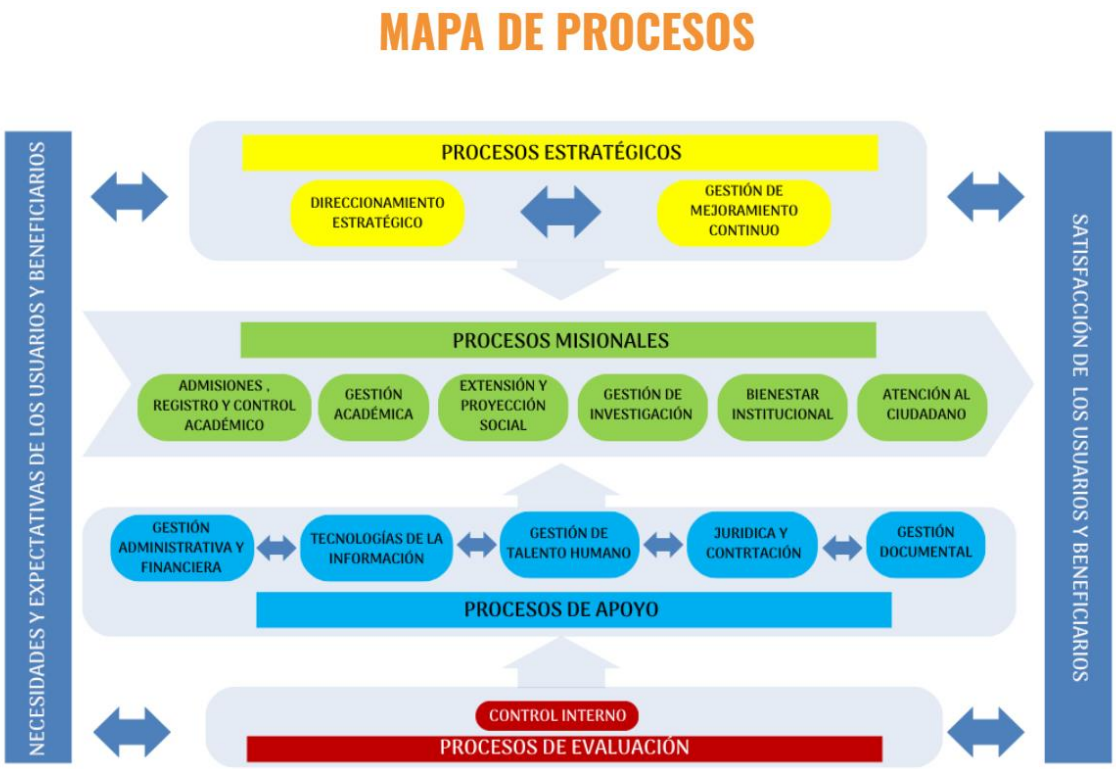
El artículo 5 destaca la importancia de adoptar una estrategia de seguridad digital que integre principios, políticas, procedimientos, guías, manuales, formatos y lineamientos en el Plan de Seguridad y Privacidad de la Información. Esta estrategia se incluirá en el Plan de Acción, conforme a lo establecido en el Decreto 1083 de 2015, Único Reglamentario del Sector de la Función Pública.

El Plan de Seguridad y Privacidad de la Información de INTENALCO aborda la protección de la información en sus formas digital, impresa y en medios físicos, digitales y no digitales, frente a los riesgos y amenazas potenciales.

En la implementación del MSPI, se considera esencial proteger la Confidencialidad, Integridad y Disponibilidad de la información. Esto se lleva a cabo mediante la guía de gestión de riesgos de seguridad de la información y el procedimiento de gestión de incidentes de seguridad digital, que están incorporados en el Anexo 1 de la resolución.

ALCANCE

Mejorar el desempeño de la seguridad digital para los 14 procesos de INTENALCO, buscando garantizar la confidencialidad, integridad y disponibilidad de los servicios de información.



Con el objetivo de salvaguardar la confidencialidad, integridad y disponibilidad de nuestros servicios de información, se emprenderán acciones concretas durante la ejecución de este plan. Al concluir este proceso, se anticipa contar con procesos y procedimientos considerablemente fortalecidos en el ámbito de la seguridad digital.

MARCO LEGAL Y NORMATIVO

La normatividad aplicable al Plan de Seguridad y Privacidad de la Información de INTENALCO incluye diversas leyes, decretos y resoluciones relevantes que abarcan distintos aspectos. A continuación, se destacan las más pertinentes para la implementación de medidas de seguridad digital y privacidad de la información:

- **Constitución Política de Colombia**:

  - Artículos 15, 20, 23 y 74.

Leyes:

- Ley 1581 de 2012: Protección de datos personales.
- Ley 1273 de 2009: Protección de la información y los datos.
- Ley 1712 de 2014: Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional.
- Ley 1437 de 2011: Código de Procedimiento Administrativo y de lo Contencioso Administrativo.
- Ley 527 de 1999: Acceso y uso de mensajes de datos, comercio electrónico y firmas digitales.
- Ley 1341 de 2009: Principios y conceptos sobre la sociedad de la información y TIC.

Decretos:

- Decreto 338 de 2022: Gobernanza de la seguridad digital.
- Decreto 767 de 2022: Política de Gobierno Digital.
- Decreto 88 de 2022: Digitalización y automatización de trámites.
- Decreto 1287 de 2020: Seguridad de documentos firmados durante el trabajo en casa.
- Decreto 620 de 2020: Uso y operación de servicios ciudadanos digitales.
- Decreto 2106 de 2019: Simplificación y reforma de trámites en la administración pública.

Resoluciones:

- Resolución 0448 de 2022: Política General de Seguridad y Privacidad de la Información.
- Resolución 1838 de 2022: Modalidades de teletrabajo y lineamientos de desconexión laboral.
- Resolución 746 de 2022: Fortalecimiento del Modelo de Seguridad y Privacidad de la Información.
- Resolución 500 de 2021: Lineamientos y estándares para la estrategia de seguridad digital.
- Resolución 1519 de 2020: Estándares y directrices para la publicación de información y requisitos de acceso a la información pública.

CONPES:

- CONPES 3995 de 2020: Confianza y Seguridad Digital.

- CONPES 3854 de 2017: Política Nacional de Seguridad Digital.
- CONPES 3701 de 2011: Lineamientos de Política para Ciberseguridad y Ciberdefensa.

Directiva:

- Directiva 26 de 2020: Diligenciamiento de información en el índice de transparencia y acceso a la información.

Esta normativa proporciona un marco legal robusto para la implementación de medidas de seguridad y privacidad de la información, asegurando el cumplimiento de estándares y la protección de datos en consonancia con las disposiciones gubernamentales y las mejores prácticas internacionales.

METODOLOGÍA

En términos del marco legal y normativo, la metodología aplicada sigue el enfoque de Planear, Hacer, Verificar y Actuar (PHVA) indicado por el MinTIC.

La entidad ha adoptado el MSPI, acogiendo buenas prácticas y estándares internacionales. Cada una de las fases se dará por completada, cuando se cumplan todos los requisitos definidos en cada una de ellas.

Ilustración 1 Ciclo del Modelo de Seguridad y Privacidad de la Información

INTENALCO cuenta con un conjunto de políticas entre las que se incluyen:

- ✓ Política de Gestión de Activos de la Información
- ✓ Política de Control de Acceso
- ✓ Política de Seguridad Física
- ✓ Política de Software
- ✓ Política de Integridad
- ✓ Política de Continuidad, contingencia, recuperación y retorno a la normalidad
- ✓ Política de Cumplimientos Requisitos Legales

Estas políticas se respaldan con procedimientos detallados como:

- ✓ Procedimiento de Respaldo de la Información
- ✓ Procedimiento de Activos de Información
- ✓ Procedimiento de Ingreso y egreso de Equipos Tecnológicos

Todas las políticas y procedimientos están sujetos a revisión continua para identificar áreas de mejora. La entidad realiza autodiagnósticos recomendados por el MinTIC para validar mejoras implementadas y fortalecer los controles con calificaciones más bajas. Además, se programa una revisión periódica, al menos una vez al año, para garantizar la efectividad del Plan de Seguridad y Privacidad de la Información.

En conclusión, el plan se lleva a cabo con actividades específicas que abarcan desde la identificación de activos hasta la gestión de incidentes, con el objetivo de fortalecer la seguridad digital de INTENALCO y garantizar la protección de la información.

Estos documentos entran en revisión 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, igualmente se debe programar una revisión periódicamente (mínimo una vez al año).

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El Plan de Seguridad y Privacidad de la información se llevará acabó mediante las siguientes actividades

ACTIVIDAD	TAREA	RESPONSABLE	INICIO	FIN
Identificación de activos de información	Realizar una revisión exhaustiva y actualización del inventario de activos de información, identificando activos críticos y clasificándolos adecuadamente.	Jefes de Área	01/06/24	30/11/24
	Validar la actualización realizada	Archivo -OTI	01/06/24	30/11/24
Evaluación de Riesgos	Identificar posibles amenazas internas y externas que puedan afectar la seguridad y privacidad de la información.	OTI	01/06/24	30/11/24
	Analizar los sistemas y procesos para identificar posibles vulnerabilidades que podrían ser explotadas.	OTI	01/06/24	30/11/24
Controles de Seguridad	Implementar controles técnicos, como actualizaciones de firewall, antivirus y cifrados	OTI	01/06/24	30/11/24
	Reforzar políticas de acceso, roles y responsabilidades	Calidad y OTI	01/06/24	30/11/24
	Realizar campañas de concienciación del personal	OTI	01/06/24	30/11/24
	Garantizar la seguridad en instalaciones y el control de acceso.	OTI	01/06/24	30/11/24
	Respaldos y almacenamiento seguro de datos	OTI	01/06/24	30/11/24
Gestión de Incidentes	Desarrollar procedimientos efectivos para notificar y manejar incidentes de seguridad.	OTI	01/06/24	30/11/24
Auditorias y Revisiones	Establecer un programa de auditorías regulares, incluyendo evaluación de la efectividad de los controles y pruebas de penetración para identificar vulnerabilidades.	Tercero - OTI	01/06/24	30/11/24
	Acciones correctivas	Tercero -OTI	01/06/24	30/11/24
Revisión y Aprobación	Realizar una evaluación anual del plan, actualizándolo basado en cambios en el	Control Interno - Planeación	01/06/24	30/11/24

	entorno operativo o regulaciones.			
	Obtención de aprobación formal de la alta dirección	Comité de seguridad	01/06/24	30/11/24
Cumplimiento Normativo	Asegurarse de que todas las políticas y procedimientos estén alineados con las normativas establecidas por el MinTic.	Comité de Seguridad y OTI	01/06/24	30/11/24
Capacitación Continua	Implementar programas regulares de capacitación para el personal en aspectos de seguridad y privacidad de la información.	Talento Humano - OTI	01/06/24	30/11/24
Documentación y Archivo	Mantener una documentación actualizada y archivar los registros de auditorías, revisiones e incidentes.	Archivo - OTI	01/06/24	30/11/24
Certificación y Aprobación Formal	Obtener la certificación y aprobación formal de la alta dirección para el Plan de Seguridad y Privacidad de la Información.	Comité de Seguridad	01/06/24	30/11/24