PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Tecnología e Información

Fecha de elaboración: Cali, Enero 2025

INTRODUCCIÓN

INTENALCO Una Institución Educativa de carácter oficial nacional, Técnica Profesional aprobada por el ICFES y el Ministerio de Educación Nacional (MEN) mediante Resolución No. 2903 del 17 de noviembre de 1992. INTENALCO de acuerdo con lo indicado por el Ministerio de Tecnologías de la Información y las Comunicaciones – MINTIC, en la resolución 500 de 20211 que indica los lineamientos a seguir para dar cumplimiento a un MSPI (Modelo de Seguridad y Privacidad de la Información) donde:

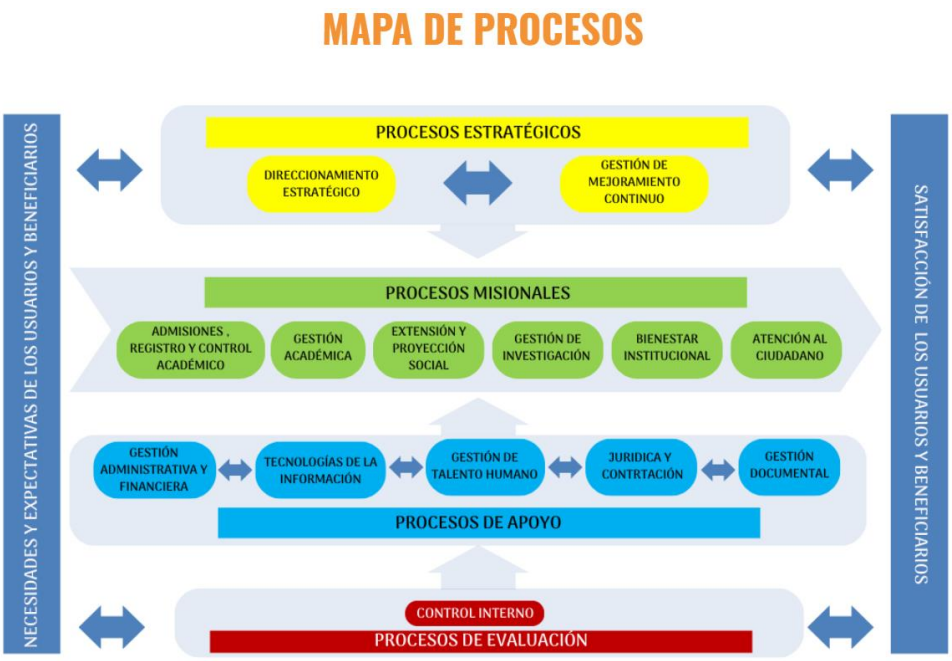
> *"ARTÍCULO 3. Lineamientos generales. Los sujetos obligados deben adoptar medidas técnicas, administrativas y de talento humano para garantizar que la seguridad digital se incorpore al plan de seguridad y privacidad de la información y así mitigar riesgos relacionados con la protección y la privacidad 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 de los riesgos y amenazas que se pueden presentar en la entidad.

La necesidad de Proteger la Confidencialidad, Integridad y Disponibilidad de la información de la entidad se define 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. Que esta aprobada por acto administrativo Resolución ######

ALCANCE

El presente plan tiene como propósito mejorar el desempeño de seguridad digital para los14 procesos de INTENALCO.



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.

MARCO LEGAL Y NORMATIVO

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:

–

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

Cada una de las fases se dará por completada, cuando se cumplan todos los requisitos definidos en cada una de ellas; La entidad en el momento se encuentra en la fase de Evaluación de desempeño.

POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La entidad INTENALCO desde que adopto El Modelo de Seguridad y Privacidad de la Información – MSPI ha implementado y acogiendo a las buenas prácticas, tomando como referencia estándares internacionales, con el objetivo de orientar la gestión e implementación adecuada del ciclo de vida de la seguridad de la información (Planeación, Implementación, Evaluación, Mejora Continua), permitiendo habilitar la implementación de la Política de Gobierno Digital.

INTENALCO cuenta con el manual de políticas de seguridad para tecnologías de la información, plan de tratamiento de riesgos de seguridad de la información, también contamos con las siguientes políticas:

- ✓ 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

Apoyamos en los procedimientos de Política de Seguridad

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

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 se lleva acabó con las siguientes actividades

Actividad	Tarea	Responsable	Inicio	Fin
Identificación de activos de informacion	Realizar una revisión exhaustiva y actualización del inventario de activos de información, identificando activos críticos y clasificándolos adecuadamente.	Jefes de Área	01/06/25	30/11/25
	Validar la actualización realizada	Archivo -OTI	01/06/25	30/11/25
Evaluación de Riesgos	Identificar posibles amenazas internas y	OTI	01/06/25	30/11/25

	externas que puedan afectar la seguridad y privacidad de la información.			
	Analizar los sistemas y procesos para identificar posibles vulnerabilidades que podrían ser explotadas.	OTI	01/06/25	30/11/25
Controles de Seguridad	Implementar controles técnicos, como actualizaciones de firewall, antivirus y cifrados	OTI	01/06/25	30/11/25
	Reforzar políticas de acceso, roles y responsabilidades	Calidad y OTI	01/06/25	30/11/25
	Realizar campañas de concienciación del personal	OTI	01/06/25	30/11/25
	Garantizar la seguridad en instalaciones y el control de acceso.	OTI	01/06/25	30/11/25
	Respaldos y almacenamiento seguro de datos	OTI	01/06/25	30/11/25
Gestión de Incidentes	Desarrollar procedimientos efectivos para notificar y manejar incidentes de seguridad.	OTI	01/06/25	30/11/25
Auditorias y Revisiones	Establecer un programa de auditorías regulares, incluyendo	Tercero - OTI	01/06/25	30/11/25

	evaluación de la efectividad de los controles y pruebas de penetración para identificar vulnerabilidades.			
	Acciones correctivas	Tercero -OTI	01/06/25	30/11/25
Revisión y Aprobación	Realizar una evaluación anual del plan, actualizándolo basado en cambios en el entorno operativo o regulaciones.	Control Interno - Planeacion	01/06/25	30/11/25
	Obtención de aprobación formal de la alta dirección	Comité de seguridad	01/06/25	30/11/25
Cumplimiento Normativo	Asegurarse de que todas las políticas y procedimientos estén alineados con las normativas establecidas por el MinTic.	Comité de Seguridad y OTI	01/06/25	30/11/25
Capacitación Continua	Implementar programas regulares de capacitación para el personal en aspectos de seguridad y privacidad de la información.	Talento Humano - OTI	01/06/25	30/11/25
Documentación y Archivo	Mantener una documentación actualizada y archivar los	Archivo - OTI	01/06/25	30/11/25

	registros de auditorías, revisiones y incidentes.			
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	01/06/25	30/11/25