PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

Tecnología e Informacion

Fecha de elaboración: Cali, Enero 2025

INTRODUCCION

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.

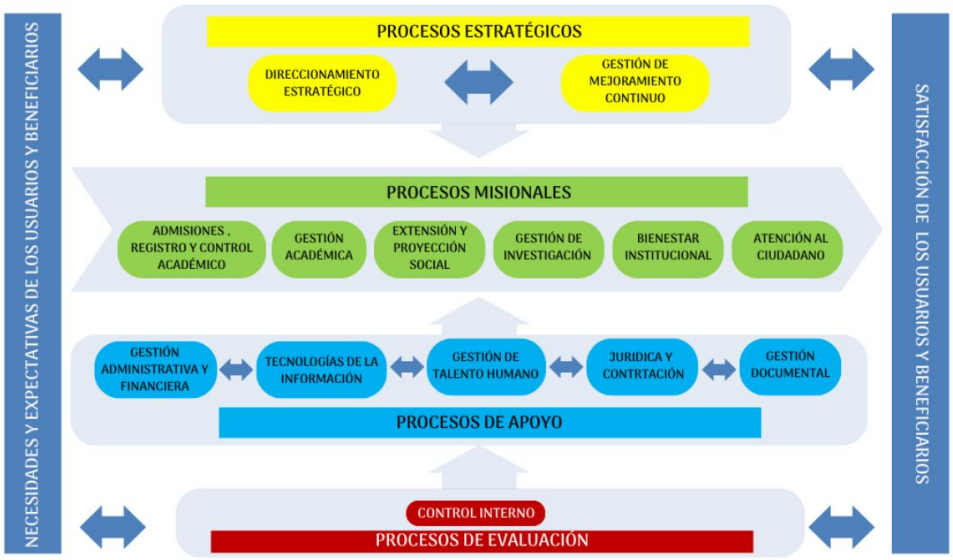
La necesidad de Proteger la Confidencialidad, Integridad y Disponibilidad de la información

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.

MAPA DE PROCESOS



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.

OBJETIVO

Establecer y aplicar los controles necesarios para mitigar los riesgos que afecten la

confidencialidad, integridad y disponibilidad de los activos de información de INTENALCO, especialmente en los sistemas SIGA, Q10, SIESA, ADVISER y TURNERO, asegurando la continuidad de la operación académica.

MARCO LEGAL Y NORMATIVO

El presente Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de INTENALCO se fundamenta en el cumplimiento de las disposiciones legales vigentes en materia de seguridad digital y protección de datos en Colombia. Además de la Resolución 500 de 2021 del MinTIC, que establece los lineamientos para el Modelo de Seguridad y Privacidad de la Información (MSPI), este plan incorpora:

- Ley 1581 de 2012: Marco general para la protección de datos personales (Habeas Data).
- Ley 2157 de 2021: Actualización del tratamiento de datos financieros y comerciales, aplicable a los procesos de recaudo y gestión financiera.
- CONPES 3995 de 2020: Política Nacional de Confianza y Seguridad Digital, que orienta la gestión de riesgos ante amenazas cibernéticas.
- Guía de Gestión de Riesgos de Seguridad Digital (MinTIC, actualización 2022): Documento técnico que define la metodología para la identificación de amenazas y la implementación de controles en las entidades públicas.
- Decreto 1263 de 2022: Por el cual se establecen los lineamientos y estándares para la transformación digital y seguridad de la información en el Estado Colombiano.

METODOLOGIA

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.

POLITICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

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)

IDENTIFICACIÓN Y TRATAMIENTO DE RIESGOS CRÍTICOS (ACTUALIZACIÓN 2026)

Escenario de Riesgo	**Activo / Sistema Afectado**	**Impacto**	**Control / Acción de Mitigación (Hitos 2026)**
Indisponibilidad o caída del servicio por fallos de infraestructura.	**SIGA, Q10 y ADVISER**	Interrupción de matrículas y registro académico.	Implementación de **Backups en la nube** y monitoreo proactivo con **Zabbix/GLPI**.

Escenario de Riesgo	**Activo / Sistema Afectado**	**Impacto**	**Control / Acción de Mitigación (Hitos 2026)**
Acceso no autorizado o fuga de datos personales de la comunidad.	**Bases de Datos (SIGA/Q10)**	Sanciones legales (Superintendencia) y pérdida de confianza.	Fortalecimiento del MSPI y control de identidades (según Res. 500/2021).
Secuestro de información (Ransomware) o ataques dirigidos.	**SIESA (Financiero) y Servidores**	Parálisis financiera y pérdida de registros históricos.	**Transición a IPv6** para mejorar la seguridad de red y escaneos de vulnerabilidades semestrales.
Uso inadecuado o pérdida de integridad en la atención al usuario.	**TURNERO (Mercadeo)**	Mala imagen institucional y desorden en procesos de admisión.	Auditorías de acceso y mantenimiento preventivo al hardware del sistema de turnos.
Alteración de registros de graduación y certificaciones.	**Software de Graduandos**	Fraude académico y riesgos legales ante el MEN.	Centralización del software y copias de seguridad automáticas diarias.

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	01/06/26	30/11/26
	Validar la actualización realizada	Archivo -OTI	01/06/26	30/11/26
Evaluación de Riesgos	Identificar posibles amenazas internas y externas que puedan afectar la seguridad y privacidad de la información.	OTI	01/06/26	30/11/26
	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	Calidad y OTI	01/06/25	30/11/25

	de acceso, roles y responsabilidades			
	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 evaluación de la efectividad de los controles y pruebas de penetración para identificar vulnerabilidades.	Tercero - OTI	01/06/25	30/11/25
	Acciones correctivas	Tercero -OTI	01/06/26	30/11/26
Revisión y Aprobación	Realizar una evaluación anual del plan, actualizándolo basado en cambios en el entorno operativo	Control Interno - Planeacion	01/06/26	30/11/26

	o regulaciones.			
	Obtención de aprobación formal de la alta dirección	Comité de seguridad	01/06/26	30/11/26
Cumplimiento Normativo	Asegurarse de que todas las políticas y procedimientos estén alineados con las normativas establecidas por el MinTic.	Comité de Seguridad y OTI	01/06/26	30/11/26
Capacitación Continua	Implementar programas regulares de capacitación para el personal en aspectos de seguridad y privacidad de la información.	Talento Humano - OTI	01/06/26	30/11/26
Documentación y Archivo	Mantener una documentación actualizada y archivar los registros de auditorías, revisiones y incidentes.	Archivo - OTI	01/06/26	30/11/26
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	01/06/26	30/11/26

Fortalecimiento de Backups	Implementar respaldo externo/nube 100%.	Oficina TI	15/07/26	30/11/26
Transición Segura a IPv6	Reducir vulnerabilidades de escaneo de red.	Oficina TI	----	---
Gestión de Vulnerabilidades	Realizar 2 escaneos de seguridad al año.	Oficina TI	01/04/26	30/11/26
Implementación GLPI	Registro del 100% de incidentes de seguridad.	Oficina TI	15/01/26	28/02/26

SEGUIMIENTO Y MONITOREO

El proceso de seguimiento garantiza que los controles implementados para mitigar los riesgos en los sistemas misionales sean efectivos. INTENALCO aplicará el siguiente esquema:

Mesas de Trabajo Semestrales

Se realizarán reuniones de seguimiento lideradas por la Oficina de TI y el Comité de Seguridad, con el fin de:

Revisar la efectividad de los controles aplicados a los sistemas SIGA, Q10, SIESA, ADVISER y TURNERO.

Validar el estado de la Transición a IPv6 y la integridad de los Backups en la nube.

Identificar nuevos riesgos emergentes producto de cambios en la infraestructura o normativa.

Monitoreo Técnico Automatizado

Para garantizar la disponibilidad y seguridad en tiempo real, se utilizarán las siguientes herramientas:

Zabbix / GLPI: Monitoreo constante de la disponibilidad de los servidores y gestión de incidentes de seguridad reportados.

Logs de Auditoría: Revisión mensual de los registros de acceso a las bases de datos académicas para detectar intentos de ingreso no autorizados.

Indicadores de Gestión de Riesgo

Para medir el éxito de este plan, se establecen los siguientes indicadores:

Indicador	**Descripción**	**Meta 2026**	**Periodicidad**
Eficacia de Mitigación	(Riesgos mitigados / Riesgos identificados) * 100	90%	Semestral
Frecuencia de Incidentes	Número de incidentes de seguridad reportados en GLPI.	< 5 críticos	Trimestral
Disponibilidad de Backups	Porcentaje de copias de seguridad exitosas y verificadas.	100%	Mensual