“ITFIP”

INSTITUCIÓN DE EDUCACIÓN SUPERIOR

PLAN DE PRESERVACION DE DOCUMENTOS ELECTRONICOS

MARIO FERNANDO DÍAZ PAVA
Rector

DIANA MARILY RODRIGUEZ RICAURTE
Asesor de Planeación

Diseño y elaboración:

JUAN SEBASTIAN LAGUNA ALMARIO
RUBEN ANDRES GUALTERO GUZMAN

Espinal – 2026

Contenido

INTRODUCCIÓN

En la actualidad, la información digital se ha consolidado como uno de los activos más valiosos para las organizaciones. Por ello, la seguridad y la privacidad de los datos se convierten en elementos críticos que deben gestionarse con rigor, responsabilidad y profesionalismo. El Instituto Tolimense de Formación Técnica Profesional (ITFIP) reconoce la importancia de proteger la información de toda su comunidad institucional —estudiantes, docentes, administrativos, contratistas, entre otros— y de garantizar el cumplimiento de las normativas, lineamientos y estándares vigentes en materia de seguridad de la información.

El Plan de Seguridad y Privacidad de la Información 2025 tiene como propósito establecer un marco de referencia que permita identificar, evaluar y gestionar los riesgos asociados a la protección de la información dentro del ITFIP. Este plan se encuentra alineado con los principios y requisitos de la norma ISO 27001, la cual proporciona un enfoque sistemático para la implementación y mejora continua de un Sistema de Gestión de Seguridad de la Información (SGSI), asegurando la confidencialidad, integridad y disponibilidad de los datos.

El ITFIP se compromete a implementar, fortalecer y mantener un SGSI que permita resguardar sus activos de información frente a amenazas internas y externas, garantizando la continuidad institucional y preservando la confianza de sus partes interesadas. Para ello, se han definido políticas, procedimientos y controles que serán aplicados de manera coherente y transversal en toda la institución.

1. OBJETIVO

Definir y detallar las actividades necesarias para la implementación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información del Instituto Tolimense de Formación Técnica Profesional (ITFIP), asegurando la adopción y aplicación de los controles, procedimientos y directrices establecidos por la norma ISO 27001, con el fin de fortalecer el Sistema de Gestión de Seguridad de la Información (SGSI) y garantizar la protección integral de los activos de información institucional.

2. ALCANCE

El presente Plan de Seguridad y Privacidad de la Información tiene alcance sobre todas las dependencias, procesos, servicios, activos de información y actores institucionales del Instituto Tolimense de Formación Técnica Profesional (ITFIP). Su aplicación es obligatoria en todo el ámbito organizacional y se desarrolla en coherencia con el Sistema Integrado de Gestión, la Política Institucional de Seguridad de la Información y los lineamientos normativos vigentes, garantizando la protección y el adecuado tratamiento de la información en cada etapa del ciclo de gestión.

3. MARCO NORMATIVO

- Ley 527 de 1999: Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

- Ley 1273 de 2009: Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

- Ley 1712 de 2014: Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.

- Ley 1581 de 2012, Principio de seguridad: "La información sujeta a Tratamiento por el responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente Ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento."

- Ley 1581 de 2012, Artículo 17, ítem d: "Conservar la información bajo las

condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento".

- Ley 1712 de 2014, "principio de transparencia": "Principio conforme al cual toda la información en poder de los sujetos obligados definidos en esta Ley se presume pública, en consecuencia, de lo cual dichos sujetos están en el deber de proporcionar y facilitar el acceso a la misma en los términos más amplios posibles y a través de los medios y procedimientos que al efecto establezca la Ley, excluyendo solo aquello que esté sujeto a las excepciones constitucionales y legales y bajo el cumplimiento de los requisitos establecidos en esta Ley."

- Decreto 1413 de 2017, "Seguridad de la información." "Los actores que traten información, en el marco del presente título, deberán adoptar medidas apropiadas, efectivas y verificables de seguridad que le permitan demostrar el correcto cumplimiento de las buenas prácticas consignadas en el modelo de seguridad y privacidad de la información emitido por el Ministerio de Tecnologías de la Información y las Comunicaciones, o un sistema de gestión de seguridad de la información certificable. Esto con el fin de salvaguardar la confidencialidad, integridad y disponibilidad de los activos de información."

4. DEFINICIONES

1. **Aceptación de riesgo**: Decisión de asumir un riesgo. Activo: Cualquier cosa que tiene valor para la organización. Adaptabilidad: Define los eventos y bajo qué criterios un sistema debe poder ser monitoreado y revisado para su control posterior.

2. **Amenazas**: es un ente o escenario interno o externo que puede hacer uso de una vulnerabilidad para generar un perjuicio o impacto negativo en la institución (materializar el riesgo).

3. **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.

4. **Autenticidad**: Busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidad. alimentación eléctrica y condiciones de temperatura y humedad.
5. **Centro de cómputo**: Es una zona específica para el almacenamiento de múltiples computadores para un fin específico, los cuales se encuentran

conectados entre sí a través de una red de datos.

6. **Ciberseguridad** : Capacidad del Estado para minimizar el nivel de riesgo aceptable al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética.
7. **Confiabilidad de la Información**: Garantiza que la fuente de la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.
8. **Control o Medida**: acciones o mecanismos definidos para prevenir o reducir el impacto de los eventos que ponen en riesgo, la adecuada ejecución de las actividades y tareas requeridas para el logro de objetivos de los procesos de una entidad.
9. **Custodio del activo de información**: Es la unidad organizacional o proceso, designado por los propietarios, encargado de mantener las medidas de protección establecidas sobre los activos de información confiados.
10. **Datos personales**: Es cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.
11. **Dato público**: 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.

12. **Datos 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.

13. **Disponibilidad:** Propiedad de que la información sea accesible y utilizable por solicitud de una entidad.

14. **Disponibilidad:** Propiedad de que la información sea accesible y utilizable por solicitud de una entidad. **Evaluación del riesgo**: Proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo.

15. **Incidente de seguridad de la información**: Un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer lasoperaciones del negocio y amenazar la seguridad de la información.

16. **Integridad**: Propiedad de salvaguardar la exactitud y estado completo de los activos.

17. **Impacto**: son las consecuencias que genera un riesgo una vez se materialice.

18. **Probabilidad**: es la posibilidad de que la amenaza aproveche la vulnerabilidad para materializar el riesgo.

19. **Recursos informáticos**: Todos aquellos componentes de hardware y programas (software) que son necesarios para el buen funcionamiento y la optimización del trabajo con computadores y periféricos, tanto a nivel Individual, como colectivo u organizativo, sin dejar de lado el buen funcionamiento de estos.

20. **Seguridad de la Información**: Preservación de la confidencialidad, integridad, y disponibilidad de la información.

21. **Sistema de Gestión de Seguridad de la Información**: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua.

22. **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.

23. **Tratamiento del riesgo**: Proceso de selección e implementación de acciones de mejora que permita gestionar el riesgo.

24. **Valoración del riesgo**: Proceso de análisis y evaluación del riesgo. Vulnerabilidad : es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos.

5. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

5.1. Objetivo:

Proteger la información del contra una amplia gama de amenazas garantizando la continuidad de la institución, minimizando los riesgos empresariales y maximizando el retorno de las inversiones y oportunidades de negocio.

5.2. Objetivo:

Aplica a todos lo empleados contratistas y terceros que tengan acceso a la información del ITFIP. Incluye todos los sistemas de información, redes, aplicaciones, datos y servicios de la institución.

6. PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN

6.1. Confidencialidad

La información debe ser accesible únicamente para las personas autorizadas, evitando su divulgación, uso o acceso no autorizado

6.2. Integridad

La información debe mantenerse precisa, completa y protegida contra modificaciones no autorizadas.

6.3. Disponibilidad

La información debe estar disponible para los usuarios autorizados cuando la requieran, garantizando la continuidad de la operación Institucionales.

7. RESPONSABILIDADES

7.1. Planeación con aprobación de Rectoría

Dependencias encargadas de aprobar y promover la Política de Seguridad de la Información, asegurando su alineación con los lineamientos institucionales

7.2. Responsable de Seguridad de la Información

Dependencia encargada de implementar, mantener y mejorar continuamente el Sistema de Gestión de Seguridad de la Información (SGSI).

7.3. Empleados y Contratistas

Deben cumplir con esta política, participar en actividades de sensibilización y reportar cualquier incidente de seguridad de manera oportuna.

8. DIRECTRICES

- **Gestión de Riesgos**

Identificar, evaluar y tratar los riesgos relacionados con la seguridad de la información en toda la institución**.**

- **Control de Acceso**

Aplicar controles de acceso basados en roles y responsabilidades, asegurando que únicamente el personal autorizado pueda acceder a la información.

- **Protección de Datos**

Proteger los datos institucionales frente a pérdida, alteración, divulgación o acceso no autorizado.

- **Capacitación y Concienciación**

Fortalecer una cultura de seguridad mediante procesos continuos de formación dirigidos a empleados y contratistas.

- **Monitoreo y Revisión**

Realizar auditorías, monitoreo y revisiones periódicas que permitan garantizar la efectividad de las medidas de seguridad implementadas.

9. CUMPLIMIENTO DE LA POLÍTICA

El incumplimiento de esta política puede resultar en medidas disciplinarias, incluyendo la terminación del contrato de trabajo o la relación contractual.

10. IMPLEMENTACIÓN DE CONTROLES TÉCNICOS

- **Actividad principal**

Instalar y configurar herramientas de seguridad (firewalls, Fortiweb, fortianalyzer, fortisiem, antivirus, sistemas de detección de intrusos).
Responsable: Coordinación e Internet.

Gestión de Accesos: Establecer controles de acceso y autenticación para sistemas críticos dependiendo de los Roles y Responsabilidades.
Responsable: Coordinación e Internet.

10.1. Monitoreo y Auditoría

Implementar sistemas de monitoreo continuo y realizar auditorías periódicas con apoyo de especialistas en seguridad de la información.
Responsable: Dependencia de Planeación.

10.2. Recursos Necesarios

Personal: Especialistas en seguridad de la información.

Tecnología: Herramientas de seguridad (software y hardware).

Presupuesto: Fondos para la adquisición de tecnología y capacitación del personal.

10.3. Indicadores de Éxito

- Identificación y tratamiento adecuado de los riesgos.
- Reducción y mitigación efectiva de incidentes de seguridad.
- Mejoras evidenciadas en auditorías internas y externas..

10.4. Revisión y Mejora Continua

Revisar y actualizar el plan de implementación anualmente.
Responsable: Planeación.
Plazo: diciembre 2026.

Gestión de Activos de Información Identificación, protección y control de los activos de información institucionales.

11. IDENTIFICACIÓN DE ACTIVOS DE INFORMACIÓN

11.1. Inventario de Activos

Desarrollar un inventario digital que registre todos los activos de información relevantes.
Ejemplos: Datos en servidores, hardware, software, documentos físicos, bases de datos, redes y personal que gestiona información.
Responsable: Planeación.
Plazo: enero 2026.

11.2. Categorías de Activos:

Clasificar los activos de la organización en categorías como lo son hardware, software, datos, personas, y servicios.
Responsable: Coordinación e Internet.
Plazo: febrero 2026

12. CLASIFICACIÓN Y VALORACIÓN DE ACTIVOS

12.1. Clasificación de Activos:

Asignar una clasificación a cada activo según su valor, sensibilidad y criticidad.
Responsable: Coordinación e Internet.
Plazo: marzo 2026.

12.2. Valoración de Activos:

Evaluar la importancia de cada activo para la organización y su impacto en caso de pérdida o compromiso.
Responsable: Dependencias y procesos de la organización liderados por planeación
Plazo: abril 2026.

13. PROTECCIÓN DE ACTIVOS DE INFORMACIÓN

13.1. Asignación de Propietarios de Activos:

Designar un propietario para cada activo, responsable de su protección y mantenimiento.
Responsable: Dependencia de almecen
Plazo: mayo 2026.

13.2. Implementación de Controles de Seguridad:

Aplicar controles de seguridad adecuados para proteger los activos según su clasificación y valoración.
Ejemplos de Controles: Encriptación de datos, control de acceso según su roles, copias de seguridad de la información, medidas físicas de seguridad.
Responsable: Coordinación e Internet
Plazo: Junio - Julio 2026.

13.3. Monitoreo y Revisión:

Monitorear continuamente los activos y revisar periódicamente las medidas de seguridad implementadas.
Responsable: Planeación.
Plazo: Continuo.

13.4. Documentación y Actualización

Mantener registros actualizados de todos los activos, sus propietarios, clasificaciones y medidas de protección.
Responsable: Planeación.
Plazo: Continuo.

13.5. Documentación y Actualización

Revisar y actualizar el inventario de hardware y software tecnológico y las medidas de protección de los activos de información regularmente.
Responsable: Coordinación e internet
Plazo: Anual

14. GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Evaluar y tratar los riesgos que afectan la seguridad de la información institucional conforme a metodologías establecidas.

14.1. Comunicación

Informar a todas las partes interesadas sobre los riesgos y las medidas de tratamiento implementadas.

Métodos: Informes, reuniones, boletines.
Responsable: Planeación.
Plazo: Continuo.

15. NORMAS INTERNACIONALES

- **ISO/IEC 27001**: Estándar internacional que establece los requisitos para implementar, mantener y mejorar continuamente un SGSI.
- **ISO/IEC 27002**: Código de buenas prácticas que proporciona directrices para la implementación de controles de seguridad de la información.
- **NIST (National Institute of Standards and Technology)**: Conjunto de estándares y guías

de seguridad, ampliamente utilizados como referencia internacional en gestión de riesgos y controles de seguridad.

- **Esquema Nacional de Seguridad (ENS) – España**: Marco normativo que establece requisitos mínimos para la protección de la información en entidades públicas y privadas que prestan servicios al Estado.

16. NORMATIVIDAD NACIONAL (COLOMBIA)

- **Ley 1581 de 2012**: Ley de Protección de Datos Personales que regula el tratamiento, almacenamiento y uso de datos personales en el territorio nacional.
- **Decreto 1377 de 2013**: Reglamenta parcialmente la Ley 1581 de 2012, estableciendo directrices para la recolección, uso, administración y protección de datos personales.

Documentos de referencia

Los siguientes documentos, estándares y lineamientos fueron utilizados como soporte técnico y metodológico para la elaboración del Plan de Seguridad y Privacidad de la Información del ITFIP:

Normas Técnicas y Estándares

- **ISO/IEC 27001:2013**: Tecnología de la información – Técnicas de seguridad – Requisitos para Sistemas de Gestión de Seguridad de la Información.
- **ISO/IEC 27002:2013**: Tecnología de la información – Técnicas de seguridad – Código de prácticas para controles de seguridad de la información.
- **NIST SP 800-53**: Controles de seguridad y privacidad para sistemas de información federales y organizaciones.
- **Esquema Nacional de Seguridad (ENS)**: Requisitos mínimos para la protección de la información en organizaciones del sector público.

Lineamientos y Guías Nacionales (Colombia)

- **Plan de Seguridad y Privacidad de la Información – MINTIC**: Lineamientos oficiales para la formulación del Plan de Seguridad y Privacidad en entidades públicas.
- **Modelo de Seguridad y Privacidad de la Información – MINTIC**: Guía metodológica para la implementación del Modelo de Seguridad y Privacidad de la Información en entidades del Estado.

17. WEBGRAFIA

https://www.bsigroup.com/globalassets/localfiles/es-es/normas/iso27001/iso-27001- features--benefits-guide-es.pdf
https://dni.gov.co/wp-content/uploads/2023/12/Plan-de-Seguridad-y-Privacidad-de-Informacion-2023-2026.pdf
https://renobo.com.co/sites/default/files/2025-01/6_PSPI%202025_%20V-Borrador.pdf https://mintic.gov.co/portal/715/articles-135830_plan_seguridad_privacidad_informacion_v1_20230124.pdf
https://www.cra.gov.co/sites/default/files/2024-01/Plan_de_Seguridad_y_privacidad_2024-2027.pdf
https://es.isms.online/iso-27001/https://www.impconsultores.com/que-es-la-norma-iso-27001-y-para-que-sirve/