INSTITUTO TOLIMENSE DE FORMACIÓN TÉCNICA PROFESIONAL
"ITFIP"

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2025

SC6793-1

CO-SC6793-1

“ITFIP”
INSTITUCIÓN DE EDUCACIÓN SUPERIOR

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

MARIO FERNANDO DÍAZ PAVA
Rector

DIANA MARILY RODRIGUEZ RICAURTE
Asesor de Planeación

Diseño y elaboración:
JUAN SEBASTIAN LAGUNA ALMARIO
RUBEN ANDRES GUALTERO GUZMAN.

Espinal – enero 21 de 2025

Contenido

1.Introducción 5
1.OBJETIVO…….. 6
2.ALCANCE……. 6
3.TÉRMINOS Y DEFINICIONES 6
4.1Activo:……. 6
4.2 Amenaza:…. 6
4.3 Confidencialidad: 6
4.4 Disponibilidad: 6
4.5 Integridad: 6
4.6 Riesgo:…….. 6
4.7 Evaluación de riesgos: 7
4.8 Tratamiento de riesgos: 7
4.9 Incidente de seguridad de la información: 7
4.10 Sistema de Gestión de Seguridad de la Información (SGSI): 7
4.Estado Actual del Sistema de Gestión de Seguridad de la Información (SGSI) 7
4.1 Política de Seguridad de la Información 7
4.2 Objetivo…….. 7
4.3 Alcance……. 7
5.Principios de Seguridad de la Información 7
5.1 Confidencialidad: 8
5.2Integridad:. 8
5.3Disponibilidad: 8
6. Responsabilidades 8
6.1 Planeación con la aprobación de rectoría: 8
6.2 responsable de Seguridad de la Información: 8
6.3 Empleados y Contratistas: 8
7. Directrices…… 8
7.1 Gestión de Riesgos: 8
7.2 Control de Acceso: 8
7.3 Protección de Datos: 8
7.4 Capacitación y Concienciación: 9
7.5 Monitoreo y Revisión: 9
8. Cumplimiento de La Política 9
9. Implementación de Controles Técnicos 9
9.1 Gestión de Accesos 9
9.2 Monitoreo y Auditoría 9
10. Recursos Necesarios 9
11. Indicadores de Éxito 10
12. Revisión y Mejora Continua 10
13. Identificación de Activos de Información 10

14 Categorías de Activos: 11
15. Clasificación y Valoración de Activos 11
15.1 Clasificación de Activos: 11
15.2 Valoración de Activos: 11
16. Protección de Activos de Información 11
16.1 Asignación de Propietarios de Activos: 11
16.2 Implementación de Controles de Seguridad: 12
17. Monitoreo y Revisión: 12
18. Documentación y Actualización 12
19. Revisión y Actualización: 12
20. gestión de Riesgos de Seguridad de la Información: 12
21. comunicación 13
22. Normatividad 13
23 MARCO LEGAL 14
24 . WEBGRAFIA 15

1. Introducción

En la actualidad la información digital se ha convertido en uno de los activos más valiosos para las organizaciones, la seguridad y privacidad de la información digital son aspectos críticos que se deben gestionar con el mayor profesionalismo. El Instituto Tolimense de Formación Técnica Profesional (ITFIP) reconoce la importancia de proteger la información de toda la comunidad que lo conforma (estudiantes, Docentes, Administrativos, contratistas etc.), así como de cumplir con las normativas y estándares de seguridad vigentes en materia de seguridad de la información.

El presente Plan de Seguridad y Privacidad de la Información 2025 tiene como objeto establecer un marco de referencia que permita identificar, evaluar y gestionar los posibles riesgos asociados a la seguridad y privacidad de la información en el ITFIP. Este plan se alinea con la norma ISO 27001, la cual proporciona un enfoque sistemático para la gestión de la seguridad de la información, asegurando la confidencialidad, integridad y disponibilidad de los datos.

El ITFIP se compromete a implementar y mantener un Sistema de Gestión de Seguridad de la Información (SGSI) que permita proteger sus activos de información frente a amenazas internas y externas, garantizando así la continuidad de sus operaciones y la confianza de sus partes interesadas. Para ello, se han definido una serie de políticas, procedimientos y controles que serán aplicados de manera consistente en toda la institución.

.

1. OBJETIVO

Describir las actividades que se llevarán a cabo como parte del Plan de Seguridad y Privacidad de la Información, con el fin de implementar el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información en el Instituto Tolimense de Formación Técnica Profesional (ITFIP), de acuerdo con la norma ISO 27001.

2. ALCANCE

El Plan de Seguridad y Privacidad de la Información se aplica a todas las dependencias y los procesos del Instituto Tolimense de Formación Técnica Profesional ITFIP, en concordancia con el Sistema Integrado de Gestión y la Política de Seguridad de la Entidad.

3. TÉRMINOS Y DEFINICIONES

4.1 Activo:

es cualquier información o dispositivo que tenga valor para la institución.

4.2 Amenaza:

cualquier incidente o acontecimiento no deseado para la organización, que pueda provocar daños a un sistema o a la información confidencial de la misma.

4.3 Confidencialidad:

vigilar y proteger que la información sea accesible solo a personas autorizadas por la organización.

4.4 Disponibilidad:

Garantizar que solo los usuarios autorizados tengan acceso a la información y a los activos asociados cuando lo requieran según su rol.

4.5 Integridad:

proteger que la información no sea alterada.

4.6 Riesgo:

Toda amenaza que se pueda materializar en la organización como lo son factores internos, externos.

4.7 Evaluación de riesgos:

es el medio por el cual se determina la naturaleza del riesgo y el nivel de riesgo.

4.8 Tratamiento de riesgos:

es un proceso donde se implementan medidas para modificar el riesgo, como lo son el evitar, compartir, aceptar o mitigar el riesgo.

4.9 Incidente de seguridad de la información:

es un evento o serie de eventos no deseados o inesperados que tienen una alta probabilidad de comprometer las operaciones comerciales y amenazar la seguridad de la información.

4.10 Sistema de Gestión de Seguridad de la Información (SGSI):

Conjunto de políticas, procedimientos, directrices y recursos asociados gestionados de manera coordinada para proteger la información.

4. Estado Actual del Sistema de Gestión de Seguridad de la Información (SGSI)

4.1 Política de Seguridad de la Información

4.2 Objetivo

El objetivo de esta política es proteger la información del ITFIP contra una amplia gama de amenazas, garantizando la continuidad del negocio, minimizando los riesgos empresariales y maximizando el retorno de las inversiones y oportunidades de negocio.

4.3 Alcance

Esta política se aplica a todos los 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.

5. Principios de Seguridad de la Información

5.1 Confidencialidad:

La información debe ser accesible solo a personas autorizadas.

5.2 Integridad:

La información debe ser precisa y completa.

5.3 Disponibilidad:

La información debe estar disponible para los usuarios autorizados cuando la necesiten.

6. Responsabilidades

6.1 Planeación con la aprobación de rectoría:

dependencias encargadas de aprobar **e** Impulsar la política de seguridad de la información.

6.2 responsable de Seguridad de la Información:

es la dependencia encargada de implementar y mantener el Sistema de Gestión de Seguridad de la Información (SGSI).

6.3 Empleados y Contratistas:

Deben cumplir con esta política y reportar cualquier incidente de seguridad.

7. Directrices

7.1 Gestión de Riesgos:

Identificar, evaluar y tratar los riesgos de seguridad de la información en la institución.

7.2 Control de Acceso:

Acceso a la información según los roles y responsabilidades de cada funcionario de esta manera asegurando que solo las personas autorizadas tengan acceso a la información.

7.3 Protección de Datos:

proteger los datos contra pérdida, alteración o acceso no autorizado.

7.4 Capacitación y Concienciación:

Realizar gestión de aprendizaje continuo en seguridad de la información a todos los empleados y contratistas de la institución.

7.5 Monitoreo y Revisión:

Realizar auditorías y revisiones periódicas para asegurar la efectividad de las medidas de seguridad.

8. 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.

9. Implementación de Controles Técnicos

Actividad: **Instalar y configurar herramientas de seguridad (firewalls, Fortiweb, fortianalyzer, fortisiem, antivirus, sistemas de detección de intrusos).**

Responsable: Dependencia de coordinación e Internet.

9.1 Gestión de Accesos

Actividad: Establecer controles de acceso y autenticación para sistemas críticos dependiendo de los Roles y Responsabilidades.

Responsable: Coordinación e Internet.

9.2 Monitoreo y Auditoría

Actividad: Implementar sistemas de monitoreo continuo y realizar auditorías periódicas con especialistas en seguridad de la información.

Responsable: Dependencia de Planeación.

10. Recursos Necesarios

Personal: Especialistas en seguridad de la información.

Tecnología: Herramientas de seguridad (software y hardware).

Presupuesto: Asignación de fondos para la adquisición de herramientas y formación del personal por parte de la organización.

11. Indicadores de Éxito

- Identificación y tratamiento de los riesgos.
- Mitigación de incidentes de seguridad.
- Mejora en las evaluaciones de seguridad y auditorías.

12. Revisión y Mejora Continua

Actividad: Revisar y actualizar el plan de implementación anualmente.

Responsable: Planeación.

Plazo: diciembre 2025.

Gestión de Activos de Información: Identificación y protección de los activos de información.

13. Identificación de Activos de Información

Inventario de Activos: activo digital donde se consignan todos los elementos importantes de la organización.

Actividad: Crear un inventario detallado de todos los activos de información.

Ejemplos de Activos: Datos almacenados en servidores, dispositivos de hardware, software, documentos en papel, bases de datos, redes, y personal que maneja la información.

Responsable: Planeación.

Plazo: enero 2025.

14 Categorías de Activos:

Actividad: Clasificar los activos de la organización en categorías como lo son hardware, software, datos, personas, y servicios.

Responsable: Coordinación e Internet.

Plazo: febrero 2025.

15. Clasificación y Valoración de Activos

15.1 Clasificación de Activos:

Actividad: Asignar una clasificación a cada activo según su valor, sensibilidad y criticidad.

Responsable: Coordinación e Internet.

Plazo: marzo 2025.

15.2 Valoración de Activos:

Actividad: 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 2025.

16. Protección de Activos de Información

16.1 Asignación de Propietarios de Activos:

Actividad: Designar un propietario para cada activo, responsable de su protección y mantenimiento.

Responsable: Dependencia de almacén.

Plazo: Mayo 2025.

16.2 Implementación de Controles de Seguridad:

Actividad: 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 2025.

17. Monitoreo y Revisión:

Actividad: Monitorear continuamente los activos y revisar periódicamente las medidas de seguridad implementadas.

Responsable: Planeación.

Plazo: Continuo.

18. Documentación y Actualización

Actividad: Mantener registros actualizados de todos los activos, sus propietarios, clasificaciones y medidas de protección.

Responsable: Planeación.

Plazo: Continuo.

19. Revisión y Actualización:

Actividad: 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.

20. gestión de Riesgos de Seguridad de la Información:

Evaluación y tratamiento de riesgos.

21. comunicación

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

Métodos: Informes, reuniones, boletines.

Responsable: Planeación.

Plazo: Continuo.

22. Normatividad

Listado de leyes, normas y regulaciones aplicables al SGSI del ITFIP.
ISO/IEC 27001: Norma internacional que proporciona los requisitos para establecer, implementar, mantener y mejorar continuamente un SGSI

ISO/IEC 27002: Norma que ofrece directrices para la implementación de controles de seguridad de la información basados en las mejores prácticas

Ley 1581 de 2012 (Colombia): Ley de Protección de Datos Personales que regula el tratamiento de datos personales en Colombia

Decreto 1377 de 2013 (Colombia): Reglamenta parcialmente la Ley 1581 de 2012, estableciendo disposiciones para la protección de datos personales

Reglamento General de Protección de Datos (RGPD): Reglamento de la Unión Europea que establece las reglas para la protección de los datos personales y la privacidad de los ciudadanos europeos

NIST (National Institute of Standards and Technology): Conjunto de estándares y directrices de seguridad informática establecidos por el Instituto Nacional de Estándares y Tecnología de los Estados Unidos

Esquema Nacional de Seguridad (ENS): Normativa española que regula la protección de la información en el sector público y en las entidades privadas que colaboran con él

VIII. Documentos de Referencia

Referencias a documentos y estándares utilizados para la elaboración del plan.
ISO/IEC 27001:2013: Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información - Requisitos

ISO/IEC 27002:2013: Tecnología de la información - Técnicas de seguridad - Código de

prácticas para controles de seguridad de la información

Ley 1581 de 2012 (Colombia): Ley de Protección de Datos Personales

Decreto 1377 de 2013 (Colombia): Reglamenta parcialmente la Ley 1581 de 2012

Reglamento General de Protección de Datos (RGPD): Reglamento de la Unión Europea sobre la protección de datos personales

NIST SP 800-53: Controles de seguridad y privacidad para sistemas de información federales y organizaciones

Esquema Nacional de Seguridad (ENS): Normativa española para la protección de la información en el sector público

Plan de Seguridad y Privacidad de la Información - MINTIC: Lineamientos para la elaboración del Plan de Seguridad y Privacidad de la Información

Modelo de Seguridad y Privacidad de la Información - MINTIC: Guía para la implementación del Modelo de Seguridad y Privacidad de la Información

23 MARCO LEGAL

Decreto 612 de 4 de abril de 2018, Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las Entidades del Estado.
Decreto 1008 de 14 de junio de 2018, Por el cual se establecen los lineamientos generales de la política de Gobierno Digital.
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 ESTATUTARIA 1581 DE 2012: Por la cual se dictan disposiciones generales para la protección de datos personales. Congreso de la República.
LEY 1474 DE 2011: Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública. DECRETO 4632 DE 2011 Por medio del cual se reglamenta parcialmente la Ley 1474 de 2011 en lo que se refiere a la Comisión Nacional para la Moralización y la Comisión Nacional Ciudadana para la Lucha contra la Corrupción y se dictan 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.
DECRETO 103 DE 2015: por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
LEY 1266 DE 2008: por la cual se dictan las disposiciones generales del hábeas data y

se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
LEY 23 DE 1982: sobre Derechos de Autor. Congreso de la República.
CONSTITUCIÓN POLÍTICA DE COLOMBIA 1991: Artículo 15. “Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar.

24 . 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/

ISO/IEC 27001:2013:
International Organization for Standardization. (2013). *ISO/IEC 27001:2013 - Information technology - Security techniques - Information security management systems - Requirements*. ISO.

ISO/IEC 27002:2013:
International Organization for Standardization. (2013). *ISO/IEC 27002:2013 - Information technology - Security techniques - Code of practice for information security controls*. ISO.

Ley 1581 de 2012 (Colombia):
Congreso de Colombia. (2012). *Ley 1581 de 2012*. Diario Oficial No. 48.587.

Decreto 1377 de 2013 (Colombia):
Presidencia de la República de Colombia. (2013). *Decreto 1377 de 2013*. Diario Oficial No. 48.834.

Reglamento General de Protección de Datos (RGPD):
Parlamento Europeo y del Consejo. (2016). *Reglamento (UE) 2016/679 del Parlamento*

Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Diario Oficial de la Unión Europea.

NIST SP 800-53:
National Institute of Standards and Technology. (2020). *Security and Privacy Controls for Information Systems and Organizations (NIST Special Publication 800-53, Revision 5)*. NIST.

Esquema Nacional de Seguridad (ENS):
Ministerio de la Presidencia. (2010). *Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica*. Boletín Oficial del Estado.

Plan de Seguridad y Privacidad de la Información - MINTIC:
Ministerio de Tecnologías de la Información y las Comunicaciones. (2021). *Plan de Seguridad y Privacidad de la Información*. MINTIC.

Modelo de Seguridad y Privacidad de la Información - MINTIC:
Ministerio de Tecnologías de la Información y las Comunicaciones. (2021). *Modelo de Seguridad y Privacidad de la Información*. MINTIC.