

Código	1313-SIG-MC-05
Versión	2
Fecha	16-12-2025
Página	1 de 33

**MANUAL DEL SISTEMA
DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.**

Norma 27001:2022
Modelo de Seguridad y Privacidad de
la Información (MSPI) 2025.



Código	1313-SIG-MC-05
Versión	2
Fecha	16-12-2025
Página	2 de 33

Manual del Sistema de Gestión de Seguridad de la Información.

El presente manual sirve de guía para la implementación, mantenimiento y mejoramiento continuo del Sistema de Gestión de Seguridad de la Información, adoptado por la Universidad Tecnológica de Pereira.

TABLA DE CONTENIDO.

Objetivo.....	3
Alcance.....	3
Capítulo 1: Requisitos de la norma ISO/IEC 27001 en su versión vigente y el modelo de Seguridad y Privacidad de la Información	4
Capítulo 2: Protección datos personales cumplimiento ley 1581 de 2012	22
Capítulo 3: Seguridad Digital Web, cumplimiento Resolución 1519 de 2020, Anexo 3.....	29

Código	1313-SIG-MC-05
Versión	2
Fecha	16-12-2025
Página	3 de 33

Objetivo

Presentar el Manual del Sistema de Gestión de Seguridad de la Información (SGSI), como el documento guía para el cumplimiento de los requisitos establecidos en la implementación, mantenimiento y mejoramiento continuo del Sistema de Gestión de Seguridad de la Información, adoptado por la Universidad Tecnológica de Pereira, describe, el alcance, los objetivos, la política y las directrices principales en relación a seguridad de la información, mantenimiento y mejora del SGSI y articulado al Modelo de Seguridad y Privacidad de la Información (MSPI)

Alcance

Este manual aplica para dar cumplimiento a los requisitos de la norma ISO/IEC 27001 en su versión vigente, al modelo de seguridad y privacidad de la información, ley 1581 de 2012, de protección de datos personales y a la Resolución 1519 de 2020.

Código	1313-SIG-MC-05
Versión	2
Fecha	16-12-2025
Página	4 de 33

CAPITULO 1.

Norma ISO/IEC 27001 y modelo de seguridad y privacidad de la información (MSPI)

TABLA DE CONTENIDO.

1. OBJETIVO	6
2. ALCANCE	6
3. DEFINICIONES / ABREVIATURAS	6
3.1 Contenido	7
3.2 Exclusiones Norma ISO/IEC 27001	7
3.3 Alcance de implementación	7
4. CONTEXTO DE LA ORGANIZACIÓN.	8
4.1 Comprensión de la organización y su contexto.	8
4.2 Comprensión de las necesidades y expectativas de las partes interesadas	9
4.3 Determinación del alcance del sistema de gestión de seguridad de la Información	9
4.4 Sistema de gestión de la Seguridad de la información.	10
5. LIDERAZGO.	11
5.1 Liderazgo y compromiso.	11
5.2 Política:	12
5.3 Roles, responsabilidades y autoridades en la organización	12
6. PLANIFICACIÓN	13
6.1 Acciones para abordar los riesgos y las oportunidades.	13
6.2 Objetivos de seguridad de la información y planificación para alcanzarlos.	14
6.3 Planificación de los cambios.....	14
7. APOYO.....	15
7.1 Recursos	15
7.2 Competencia.	15

Código	1313-SIG-MC-05
Versión	2
Fecha	16-12-2025
Página	5 de 33

7.3 Toma de conciencia	16
7.4 Comunicación	16
7.5 Información documentada	17
8. OPERACIÓN	18
8.1 Planificación y control de la operación.....	18
8.2 Evaluación de los riesgos para la seguridad de la información.	18
8.3 Tratamiento de los riesgos para la seguridad de la información.	19
9.0 EVALUACIÓN DEL DESEMPEÑO	19
9.1 Seguimiento, medición, análisis y evaluación	20
9.2 Auditoría interna	20
9.3 Revisión por la dirección.	21
10. MEJORA.	21
10.1 Mejora continua.....	21
10.2 No conformidad y acción correctivas.....	21
11. DOCUMENTOS DE REFERENCIA	21

Código	1313-SIG-MC-05
Versión	2
Fecha	16-12-2025
Página	6 de 33

1. OBJETIVO

Servir de guía para mostrar el cumplimiento de los numerales de la norma ISO/IEC 27001:2022, así como los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) en la Universidad Tecnológica de Pereira.

2. ALCANCE

Este capítulo da alcance al cumplimiento a los requisitos de la norma ISO/IEC 27001 en su versión vigente y al Modelo de Seguridad y Privacidad de la información (MSPI).

3. DEFINICIONES /ABREVIATURAS

- **Objetivo de Calidad:** Lo que se busca, o pretende relacionado con el sistema integral de gestión.
 - **Política de Calidad:** Intenciones y dirección global de una organización, relativas a la calidad tal como se expresan formalmente por la alta dirección.
<https://www.utp.edu.co/gestioncalidad/sin-categoría/277/terminos-ydefiniciones>
 - **Modelo de Seguridad y Privacidad de la Información (MSPI):** Es el modelo fijado por el Ministerio de las Tecnologías Informáticas y comunicaciones que permite fijar los criterios para proteger la privacidad de la información y los datos, así como de los procesos y las personas vinculadas con dicha información



3.1 CONTENIDO

El Sistema de Gestión de seguridad de la información, contiene:



- El Manual del Sistema de Gestión de Seguridad de la Información donde se establecen los requisitos del Sistema de Gestión de Seguridad de la información y referencia los procedimientos técnicos y de gestión.
- Los procedimientos que contienen la información técnica y de gestión administrativa para la implementación, mantenimiento y mejoramiento continuo del Sistema de Gestión de Seguridad de la Información.
- El cumplimiento de cada uno de los controles del Anexo A de la norma 27001, por parte de la Universidad Tecnológica de Pereira.
- El cumplimiento del Modelo de Seguridad y Privacidad de la Información (MSPI).

3.2 EXCLUSIONES NORMA ISO/IEC 27001

No hay exclusiones para la norma.

3.3 ALCANCE DE IMPLEMENTACIÓN

El alcance de la aplicación de la norma ISO/IEC 27001 y el Modelo de privacidad y Seguridad de la información (MSPI) es para:

Gestión de Tecnologías Informáticas y Sistemas de Información, específicamente:

- Arquitectura de Software.
- Administración de Servidores Especializados y Bases de Datos.

Código	1313-SIG-MC-05
Versión	2
Fecha	16-12-2025
Página	8 de 33



- Administración de Servicios Informáticos.
- Implementación del Sistema de Información Institucional.
- Renovación Tecnológica Institucional.

Centro de Recursos Informáticos y Educativos:

- Administración de Redes y seguridad de la información.
- Administración del sitio Web Institucional.

Gestión de documentos:

- Custodio de la información

Sistema Integral de Gestión:

- Articulador e integrador de modelos de gestión.

4. CONTEXTO DE LA ORGANIZACIÓN.

4.1 Comprensión de la organización y su contexto

MSPI: 7.1. Contexto - 7.1.1. Comprensión de la Organización y de su contexto

La Universidad Tecnológica de Pereira, determina sus cuestiones internas y externas a través de la Matriz de partes interesadas del Sistema de Gestión de Seguridad de la Información documento, con código 1313-SIG-F23.

El logro de los resultados previstos del sistema de gestión de la seguridad de la información y que puedan verse afectados tanto para las cuestiones internas y externas se tratan a partir del análisis de riesgos.

- El modelo de gestión aplicado es el de la norma ISO 27001, establecido en este manual.



Código	1313-SIG-MC-05
Versión	2
Fecha	16-12-2025
Página	9 de 33

- La Universidad dirige la planeación estratégica a través del PDI, el cual puede consultarse en <https://pdi.utp.edu.co/wp-content/uploads/2021/05/Documento-PDI-2020-2028-Aqui-construimos-futuro.pdf>
- Se cuenta con la política de aseguramiento de la calidad,
<https://gestioncalidad.utp.edu.co/sin-categoría/37/politica-integral-de-gestion/>

4.2 Comprensión de las necesidades y expectativas de las partes interesadas

MSPI: 7.1.2. Necesidades y expectativas de los interesados.



La universidad Tecnológica de Pereira, identifica sus partes interesadas a través de la Matriz de partes interesada del Sistema de Gestión de Seguridad de la Información, documento con código 1313-SIG-F23.

A través del Proyecto Educativo Institucional (PDI), se evalúa las necesidades y expectativas que se incluyen dentro de cada pilar de gestión.

4.3 Determinación del alcance del sistema de gestión de seguridad de la Información

MSPI: 7.1.3. Definición del alcance del MSPI

El alcance del Sistema de Gestión de la seguridad de la información de la Universidad Tecnológica de Pereira está definido en el numeral 3.3 de este manual.

Este alcance se encuentra disponible en la página web de la institución, específicamente en la página del sistema integral de gestión, en el enlace:

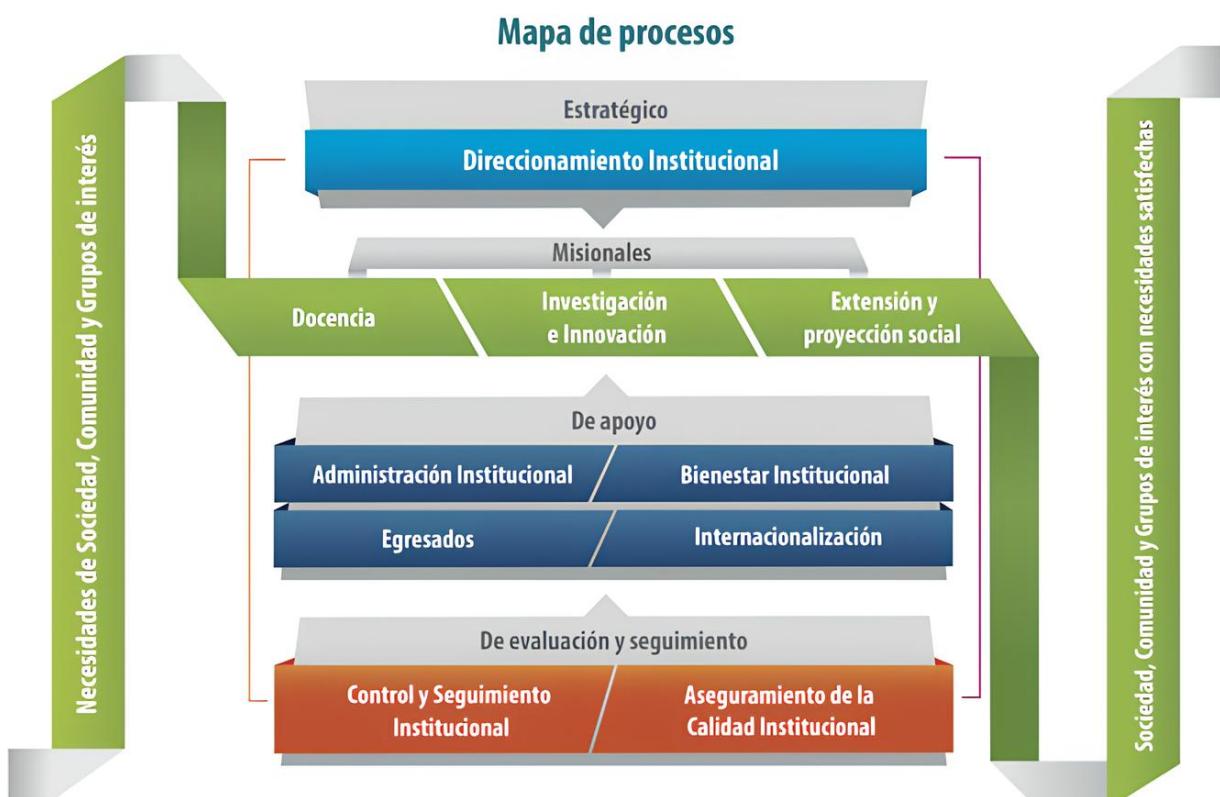
<https://www.utp.edu.co/gestioncalidad/sincategoria/284/alcance>.

Código	1313-SIG-MC-05
Versión	2
Fecha	16-12-2025
Página	10 de 33

4.4 Sistema de gestión de la Seguridad de la información.

MSPI: 7.1. Contexto - 7.1.1. Comprensión de la Organización y de su contexto

Los procesos establecidos en la Universidad Tecnológica de Pereira representan los diferentes servicios que se prestan en el cumplimiento de la misión institucional, el Sistema de Gestión de Seguridad de la Información se ubica en el proceso de Administración institucional al cual pertenecen tanto la Unidad Organizacional de Gestión de Tecnologías Informáticas y Sistemas de Información, Recursos Informáticos y Educativos y Gestión de documentos, se observan gráficamente mediante el siguiente Mapa Institucional de Procesos código SGC-MC-FOR-01:



Código	1313-SIG-MC-05
Versión	2
Fecha	16-12-2025
Página	11 de 33

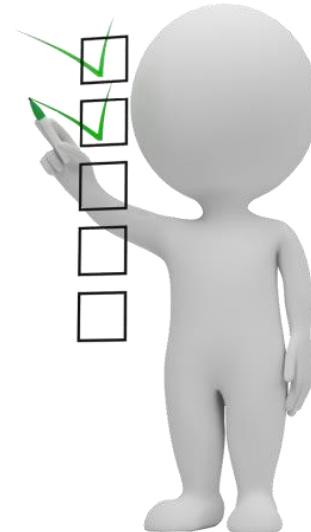
5. LIDERAZGO.

5.1 Liderazgo y compromiso.

MSPI: 7.2. Liderazgo - 7.2.1. Liderazgo y Compromiso.

La alta dirección asegura el compromiso con el Sistema de Gestión de Seguridad de la información y el compromiso de sus funcionarios, a través de:

- Estableciendo el comité del Sistema Integral de Gestión a través de la resolución de Rectoría No 4329 del 25 de abril de 2022.
- Estableciendo y divulgando la Política Institucional de Aseguramiento de la Calidad y las directrices contenidas en 1313-MGD-01 Manual General de Directrices de Seguridad de la Información.
- Definiendo objetivos de seguridad de la información compatibles con la dirección estratégica de la universidad Tecnológica de Pereira, los cuales pueden ser consultados en la página de la universidad, en el enlace: <https://www.utp.edu.co/gestioncalidad/sin-categoría/275/objetivos>
- Definiendo el presupuesto para el sistema de gestión de seguridad de la información.
- Estableciendo la Resolución de Rectoría No 1762 del 19 de febrero de 2024 por medio de la cual se conforma el equipo técnico de Seguridad de la Información en la Universidad Tecnológica de Pereira.
- Definiendo el plan de trabajo anual, con el fin de alcanzar los resultados previstos en cuanto a seguridad y privacidad de la información de la universidad.
- Precisando TIPS de buenas prácticas que contribuyan a la eficacia del SGSI. Asignando responsabilidades a las áreas de alcance del SGSI.
- Realizando revisiones por la dirección.
- Cumpliendo el Modelo de Seguridad y Privacidad de la Información (MSPI).



Código	1313-SIG-MC-05
Versión	2
Fecha	16-12-2025
Página	12 de 33



5.2 Política

MSPI: 7.2.2. Política de seguridad Manual de políticas de seguridad y privacidad de la información.

La política integral de gestión, establecida por la Universidad Tecnológica de Pereira, se encuentra disponible para ser consultada por cualquiera de las partes interesadas en la página institucional, específicamente en el enlace:

<https://www.utp.edu.co/gestioncalidad/sin-categoría/37/politicaintegral-de-gestión>.

Para el SGSI se complementa la política integral de gestión con el Manual General de directrices de seguridad de la información. Ver Anexo 1, 1313-MGD-01 Manual General de Directrices de Seguridad de la Información., ubicado en el siguiente enlace:

<https://media2.utp.edu.co/oficinas/8/1313-MGD-01%20V7%20Manual%20General%20de%20Directrices%20del%20SGSI.pdf>

5.3 Roles, responsabilidades y autoridades en la organización

MSPI: 7.2.3. Roles y responsabilidades

- a. La Universidad Tecnológica de Pereira cuenta con una estructura orgánica definida en el acuerdo 14 de 2014, donde se establecen funciones y responsabilidades, y ha conformado el grupo técnico de seguridad de la información por medio de la Resolución de Rectoría No 1762 del 19 de febrero de 2024.
- b. El desempeño del Sistema de gestión de seguridad de la información, se revisa a través de las revisiones por la dirección del comité del Sistema Integral de Gestión siguiendo el procedimiento “Revisiones por la Dirección al Sistema Integral de Gestión (SIG-PRO-004)”.

6 PLANIFICACIÓN

6.1 Acciones para abordar los riesgos y las oportunidades.



6.1.1 Generalidades

MSPI: 7.3.1 Identificación de activos de información e infraestructura crítica cibernética.

La Universidad Tecnológica de Pereira tiene establecido el procedimiento “Administración de Riesgos (SIG-PRO-11)”, donde se identifican los riesgos relacionados con la operación de las áreas del alcance del SGSI, lo anterior se realiza realizando un adecuado inventario de activos de información, los cuales son la materia prima para definir los riesgos asociados a estos.

El Manual General de Directrices de Seguridad de la Información tiene controles que ayudan a mitigar riesgos en esta materia.

6.1.2 Evaluación de riesgos de seguridad de la información

MSPI: 7.3.2 Valoración de los riesgos de seguridad de la información.

La Universidad Tecnológica de Pereira tiene establecido el procedimiento “Administración de Riesgos (SIG-PRO-11)”, donde se valoran los riesgos relacionados con la operación de las áreas de alcance del SGSI. La valoración de los riesgos de la seguridad de la información se verifica con relación a los controles de la norma ISO/IEC 27001 en su versión vigente.

6.1.3 Tratamiento de los riesgos de seguridad de la información

MSPI: 7.3.3 Plan de tratamiento de los riesgos de seguridad de la información.

La Universidad Tecnológica de Pereira tiene establecido el procedimiento “Administración de Riesgos (SIG-PRO-11)”, donde se tratan los riesgos relacionados con la operación de las áreas de alcance del SGSI.

Código	1313-SIG-MC-05
Versión	2
Fecha	16-12-2025
Página	14 de 33

6.2 Objetivos de seguridad de la información y planificación para alcanzarlos.

MSPI: 7.2. Liderazgo - 7.2.1. Liderazgo y Compromiso (ítem 1)

Los objetivos de calidad se indican en el formato SGC-MC2-FOR-02, estos son definidos anualmente por el Equipo Técnico de Seguridad de la Información, aprobados a través de acta de reunión del equipo y publicados en el link: <https://www.utp.edu.co/gestioncalidad/sin-categoría/275/objetivos>

6.3 Planificación de Cambios.

MSPI: 7. Fase 1: Planificación

Los cambios que se realizan en el Sistema de Gestión de Seguridad de la Información, de acuerdo al Procedimiento Administración de la Información Documentada (SIG-PRO-002), considerando la normatividad interna o externa que es aplicable a los diferentes procesos de la institución, generando planes, programas, proyectos y responsabilidades necesarias para su ejecución en cada caso. Las decisiones relacionadas con la aprobación, ajustes y actualización de cambios en el Sistema de Gestión de Seguridad de la Información, son gestionadas en los diferentes niveles de autoridad y gobierno con los que cuente la Institución, teniendo en cuenta la integralidad y disponibilidad de la información.

La planificación de los cambios está alineada al plan de mejoramiento, allí también se soporta:

- a) el propósito del cambio
- b) consecuencias potenciales del cambio.
- c) la integridad del sistema de gestión de la calidad.
- d) la disponibilidad de recursos.
- e) la asignación o reasignación de responsabilidades y autoridades
- f) Declaración de aplicabilidad.
- g) Plan de cambio, cultura y apropiación.

7 APOYO

7.1 Recursos

MSPI: 7.4. Soporte - 7.4.1. Recursos

El Sistema de Gestión de Seguridad de la Información cuenta con los recursos humanos, financieros, infraestructura física, tecnológica y el ambiente necesario para el establecimiento, implementación, mantenimiento y mejora continua.

Gestión del Talento Humano, provee el personal administrativo necesario para cada uno de los procesos; la infraestructura física se define en la Plan de Ordenamiento Territorial del Campus Universitario, gestionado y actualizado en Planeación. La infraestructura tecnológica se planifica en Gestión de Tecnologías Informáticas y Sistemas de Información y Recursos Informáticos y Educativos. El mantenimiento de la infraestructura física de la institución y la prestación de servicios tales como vigilancia, transporte, aseo, entre otros se planifican y ejecutan en Gestión de Servicios Institucionales.



7.2 Competencia.

MSPI: 7.4.2. Competencia, toma de conciencia y comunicación

La Universidad Tecnológica de Pereira tiene en cada uno de los manuales de funciones y responsabilidades (MFR), descripción de requisitos y responsabilidades (DRR) de sus colaboradores, un ítem referente a la seguridad de la información, para los MFR como función y para los DRR como responsabilidad, pueden ser consultados en la página del sistema integral de gestión de la institución, ingresando a la dependencia o área específica; de igual manera la universidad se asegura que el personal

Código	1313-SIG-MC-05
Versión	2
Fecha	16-12-2025
Página	16 de 33



docente y administrativo sea competente a través de la evaluación del desempeño docente y la evaluación de competencias del personal administrativo, generándose los planes de mejoramiento y acuerdos de desempeño necesarios según los resultados obtenidos.

7.3 Toma de conciencia.

MSPI: 7.4.2. Competencia, toma de conciencia y comunicación.

La Universidad Tecnológica de Pereira, promueve el Sistema de Gestión de seguridad de la información a través de diferentes actividades de socialización y sensibilización como brigadas de Calidad, TIPS informativos, publicación en la página web de las directrices de SI; así se toma conciencia del papel que cada uno de los involucrados desempeña y la manera en que aporta al cumplimiento de los requisitos y mejoramiento continuo.



7.4 Comunicación

MSPI: 7.4.2. Competencia, toma de conciencia y comunicación



La comunicación institucional se realiza a través de la página Web www.utp.edu.co, específicamente para el SGSI, reposa información en: <https://www.utp.edu.co/gestioncalidad/sin-categoría/801/seguiradadelainformacion-iso-27001-2013-y-gobierno-en-linea>, la emisora Universitaria Estéreo 88.2 FM, el correo electrónico, el informativo UTP en tu correo, el link de Peticiones, Quejas, Reclamos, Sugerencias y Denuncias por corrupción (PQRS), vía telefónica, correspondencia interna, aplicativos, TIPS de calidad, brigadas de calidad, contamos con matriz de comunicaciones y el plan de comunicaciones establecido por esta área con el fin de sensibilizar y dar a conocer la normatividad interna y las buenas

prácticas relacionadas a la seguridad de la información, así como 1313-MGD-01 Manual General de Directrices de Seguridad de la Información, definido por la Universidad Tecnológica de Pereira y la respuesta ante incidentes.

7.5 Información documentada

MSPI: 7.4.3. Información documentada

MSPI: 7.3. Planeación - 7.3.1. Identificación de activos de información e infraestructura crítica cibernética



La documentación necesaria que respalda el SGSI, se da a través de este manual, política, procedimientos, 1313-MGD-01 Manual General de Directrices de Seguridad de la Información, registros, identificación de activos de información y mapa de riesgos.

Mediante el procedimiento – “Administración de la información documentada SIG-PRO-002”, se establecen los criterios para la administración de la información documentada (documentos y registros), asegurándose el control en la creación, identificación, idoneidad, actualización, revisión, aprobación, disponibilidad, protección, almacenamiento, distribución, acceso, conservación, preservación, recuperación y disposición final. Así mismo, en este procedimiento se definen los criterios para controlar los documentos tanto internos como externos (regulaciones, normas, etc.).

Para la identificación de los activos de información de la Universidad, se cuenta con el formato 1313-SIG-F62 - Activos de información donde se realiza el inventario de activos y se clasifica de acuerdo los principios de Integridad, confidencialidad y disponibilidad, para los activos de las áreas del alcance se realiza el ejercicio en el formato 1313-SIG-F64 - Riesgos Seguridad de la Información áreas del alcance.

Código	1313-SIG-MC-05
Versión	2
Fecha	16-12-2025
Página	18 de 33

8. OPERACIÓN.

8.1 Planificación y Control de la operación.

MSPI: 8.1. Control y planeación operacional

La planificación estratégica de la institución se determina a través del Plan de Desarrollo Institucional, el Proyecto Educativo Institucional y la planificación y control de los procesos en cada una de las unidades organizacionales se da a través de:

- Los documentos que hacen parte del Sistema de Gestión de Seguridad de la Información (SGSI).
- El plan de tratamiento de riesgos. (Mapa de riesgos de seguridad de la información).
- Plan de trabajo del equipo Técnico de Seguridad de la Información.
- Programa Integral en Protección de datos personales.
- Cumplimiento de controles que se encuentran dentro del Manual general de directrices de Seguridad de la información y en el anexo A de la ISO 27001.
- Los activos de información.

8.2 Evaluación de los riesgos para la seguridad de la información.

MSPI: 8.2. Plan de tratamiento de riesgos

Para la valoración de los riesgos de seguridad de la información se utiliza la metodología de riesgos definida por la Universidad, documentada en el Procedimiento de Administración de riesgos SGC-PRO-011, el formato 1313-F12 Riesgos Seguridad de la Información áreas del alcance, la evaluación de los



riesgos de la seguridad de la información se verifica con relación al inventario de activos, incidentes de seguridad, pruebas de vulnerabilidad y los controles de la norma ISO/IEC 27001 en su versión vigente.

El Manual General de Directrices de Seguridad de la Información tiene controles que mitigan riesgos.

8.3 Tratamiento de riesgos para la seguridad de la información (ISO 27001).

MSPI: 7.3.3. Plan de tratamiento de los riesgos de seguridad de la información.

MSPI: 8.2. Plan de tratamiento de riesgos.

Se implementa la metodología de riesgos definida por la Universidad, documentada en el Procedimiento de Administración de riesgos SGC-PRO-011, el formato 1313-F12 Riesgos Seguridad de la Información áreas del alcance, se publica en la página del Sistema Integral de Gestión (SIG), el inventario de activos y los riesgos vigentes de seguridad de la información.

MSPI: 8.3 Definición de indicadores de gestión.

A través de los objetivos del Sistema de Gestión de Seguridad de la Información (SGSI) se definen los indicadores para cada vigencia.

9. EVALUACIÓN DEL DESEMPEÑO.

MSPI: 9. Fase 3: Evaluación de desempeño.

Se evalúa la efectividad de las acciones tomadas a través de los indicadores y la implementación de:

- Modelo de Seguridad y Privacidad de la Información (MSPI)

Código	1313-SIG-MC-05
Versión	2
Fecha	16-12-2025
Página	20 de 33

- Modelo Integrado de Planeación y Gestión (MIPG) en las políticas de Gobierno Digital y política de Seguridad Digital.
- Ley 1581 de 2012

9.1 Seguimiento, medición, análisis y evaluación

MSPI: 9.1. Seguimiento, medición, análisis y evaluación

El equipo técnico de seguridad de la información, conformado según Resolución de Rectoría No 1762 del 19 de febrero de 2024, realiza seguimiento, medición, análisis y evaluación a planes de trabajo interno, indicadores, riesgos, controles, pruebas de vulnerabilidad, que permiten el planteamiento de planes de mejora para garantizar el cumplimiento de los requerimientos de los usuarios y la mejora continua.

Los resultados del seguimiento, medición y el desempeño de la Seguridad de la Información son analizados para la definición de acciones y fortalecimiento de planes de mejoramiento.



9.2 Auditoría interna

MSPI 9.2. Auditoría Interna

Para la realización de las auditorías internas al Sistema de Gestión de Seguridad de la Información, se sigue el procedimiento “Auditorías Internas y Externas para la Revisión de Procesos y OEC (SIG-PRO-007)”, para los hallazgos de estas se dará trámite al procedimiento Toma de acciones (SIG-PRO-006)”.

9.3 Revisión por la dirección.

MSPI: 9.3. Revisión por la dirección

Para la revisión por la dirección al Sistema de Gestión de Seguridad de la Información se sigue el procedimiento “Revisiones por la Dirección al Sistema Integral de Gestión (SIG-PRO-004)”.



10. MEJORA.

10.1 Mejora continua.

MSPI: 10. Fase 4: Mejoramiento continuo - 10.1. Mejora continua

La gestión de la mejora continua del Sistema de Gestión de seguridad de la información se realiza mediante la aplicación de planes de mejoramiento desarrollados por las áreas de alcance de la norma 27001 en la Universidad Tecnológica de Pereira, siguiendo el procedimiento “Toma de Acciones (SIG-PRO-006)”.



10.2 No conformidades y acciones correctivas.

MSPI: 10.2. Acciones Correctivas y no conformidades



Para dar tratamiento a las no conformidades, acciones correctivas, oportunidades de mejora, al Sistema de Gestión de Seguridad de la Información se sigue el procedimiento para “Toma de Acciones (SIG-PRO-006)”, se da tratamiento mediante el formato plan de mejoramiento (1313-F10).

11 DOCUMENTOS DE REFERENCIA

- Norma ISO/IEC 27001- Requisitos.
- Modelo de Seguridad y Privacidad de la Información (MSPI)

Código	1313-SIG-MC-05
Versión	2
Fecha	16-12-2025
Página	22 de 33

CAPITULO 2.

Protección datos personales cumplimiento ley 1581 de 2012.

El proceso de protección de datos en Colombia inició con la Ley 1266 de 2008 como norma especial y luego con la expedición de una ley general y específica: la Ley 1581 de 2012, mediante la cual se regula el derecho fundamental de habeas data con la finalidad de proteger los datos personales registrados en cualquier base de datos que permita realizar operaciones como recolección, almacenamiento, uso y tratamiento por parte de entidades de naturaleza pública y privada.

Esta Ley fue parcialmente reglamentada por Decreto Reglamentario parcial 1377 de 2013. El fenómeno de la protección de datos personales se ha venido trabajando en Colombia en aras de hacer efectivo el goce pleno de los derechos fundamentales de titulares de los datos.

Para la aplicación de la ley 1581 de 2012, sobre protección de datos personales, la Universidad tecnológica de Pereira tiene definido:

TABLA DE CONTENIDO.

1. Objetivo.....	23
2. Alcance.....	23
3. Definiciones / Abreviaturas.....	23
4. Aviso de privacidad.....	24
5. Ciclo de los datos personales en la Universidad Tecnológica de Pereira	25
6. Programa Integral sobre Protección datos Personales UTP.....	28
7. Registro Nacional de Base De Datos (RNBD).....	28

Código	1313-SIG-MC-05
Versión	2
Fecha	16-12-2025
Página	23 de 33

1. Objetivos.

Servir de guía para cumplir con las disposiciones de la ley 1581 de 2012, en la Universidad Tecnológica de Pereira (UTP), con el fin de garantizar la protección de los datos personales que han sido suministrados y que se han incorporado en distintas bases o bancos de datos, o en repositorios electrónicos de todo tipo con que cuenta la Universidad, garantizando con ello, el derecho constitucional que tienen todas las personas a conocer, actualizar, rectificar y eliminar su información.

2. Alcance.

Este capítulo da alcance al cumplimiento de las disposiciones de la Ley 1581 de 2012, sobre protección de datos personales.

3. Definiciones / Abreviaturas.

- **Ley 1581 de 2012:** Por el cual se dictan disposiciones generales para la protección de datos personales. Aplicable a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento.
- **Autorización:** Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales.
- **Aviso de privacidad:** Comunicación verbal o escrita generada por el responsable, dirigida al Titular para el Tratamiento de sus datos personales, mediante la cual se le informa acerca de la

Código	1313-SIG-MC-05
Versión	2
Fecha	16-12-2025
Página	24 de 33

existencia de las políticas de Tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las finalidades del Tratamiento que se pretende dar a los datos personales.

- **Consentimiento:** Es toda manifestación de voluntad, libre, específica, informada y explícita, mediante la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.
- **Dato Personal:** Es cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables o que puedan asociarse con una persona natural o jurídica.
- **Responsabilidad Demostrada:** Probar a los entes de control y vigilancia como a los titulares de la información el cumplimiento de la entidad ante el diseño, implementación y ejecución del Programa Integral de Gestión de Datos Personales.
- **Titular:** Persona natural cuyos datos personales sean objeto de Tratamiento.
- **Titular de la información:** Es la persona natural o jurídica a quien se refiere la información que reposa en un banco de datos y sujeto del derecho de hábeas data y demás derechos y garantías de la normatividad aplicable.

4. Aviso de privacidad.

La Universidad Tecnológica de Pereira implementará un Aviso de Privacidad para informar a los Titulares sobre el tratamiento y uso dado a sus datos personales y la existencia de la presente directriz. Este aviso deberá ser remitido al momento de solicitar la información al Titular.

Aviso de Privacidad:

La Universidad Tecnológica de Pereira, con domicilio en la Ciudad de Pereira, Risaralda Colombia, quien es Responsable del Tratamiento de los Datos Personales informa que sus datos personales

Código	1313-SIG-MC-05
Versión	2
Fecha	16-12-2025
Página	25 de 33

serán incluidos en nuestras bases o bancos de datos y/o repositorios electrónicos y estos serán utilizados de manera directa o a través de terceros debidamente designados para:

- a) Cumplir con la misión y los objetivos institucionales y demás funciones propias de la Universidad como Institución de Educación Superior.
- b) Lograr una efectiva comunicación en relación con nuestros servicios y actividades de docencia, extensión, investigación y administración; así mismo, sobre alianzas, estudios
- c) Lograr una adecuada gestión, administración, mejora de los distintos servicios de nuestra Universidad que puedan contribuir con el bienestar de la comunidad Universitaria.
- d) Dar cumplimiento a obligaciones contraídas con nuestros estudiantes, docentes, empleados, contratistas, contratantes, clientes y proveedores.
- e) Informar sobre los cambios de los procesos, trámites y servicios de la Universidad.
- f) Dar cumplimiento a las obligaciones contraídas en razón a convenios firmados con instituciones internacionales, siempre y cuando se cumpla lo establecido en la Ley 1581 de 2012.
- g) Dar cumplimiento a las normas legales en cuanto a los requerimientos de los entes de control y/o otras entidades públicas, en el ejercicio de sus funciones.

El aviso de privacidad de la universidad tecnológica de Pereira puede ser consultado en: 1313-MGD-01 Manual General de Directrices de Seguridad de la Información.

5. Ciclo sobre Protección datos Personales.

Es importante mencionar que la Universidad Tecnológica de Pereira, tiene definido un ciclo en el uso de los datos personales, con el cual logra el cumplimiento de la ley 1581 en la institución y sirve de guía a toda la comunidad universitaria en el correcto uso de sus datos personales y de sus partes interesadas, dicho ciclo comienza con la necesidad de recolectar información la cual debe de estar enmarcada dentro del aviso de privacidad de la institución y finaliza con la puntualidad de evitar sanciones por incumplimiento por parte de la Superintendencia de industria y comercio (SIC).



- a. **Necesidad de recolectar información personal:** Toda base de datos se construye con un propósito principal, que puede ir desde dejar evidencias de una actividad, participación o asistencia hasta formar un gran banco de datos que puede ser usado para múltiples finalidades, es por esto que el ciclo de los datos personales en la Universidad tecnológica parte de esta misma necesidad o premisa, cuando se requiera crear una base de datos por parte de las Unidades Organizacionales, Facultades u Organismos Evaluadores de la Conformidad (OEC), se diligencia el formato 1313-F15 Formato De Creación Base De Datos (B.D) Personales, donde se registra los aspectos más relevantes de la base de datos, entre estos nombre del Responsable, tiempo de retención, finalidad, entre otros.

Una vez diligenciado el formato de creación de base de datos, se envía al oficial de datos personales o quien haga sus veces en la institución para que este registre la información en el formato 1313-F16 Documentos maestro Base de Datos Personales, para llevar el control de las bases de datos con información personal existentes en la Universidad Tecnológica de Pereira.

Código	1313-SIG-MC-05
Versión	2
Fecha	16-12-2025
Página	27 de 33

- b. **UTP aplica la ley 1581 de 2012:** Continuando con el ciclo de los datos personales en la institución, es importante mencionar que la Universidad en virtud de su quehacer diario recoge, procesa y custodia un gran volumen de información, la cual tiene el debido tratamiento indicado en la ley 1581 de 2012.
- c. **Solicitar autorización al titular de la información:** De acuerdo al numeral anterior donde se enuncia la aplicación de la ley 1581 en la Universidad Tecnológica, en concordancia es requisito solicitar una autorización previa, expresa e informada al titular de la información para que sus datos puedan ser recolectados e incluidos en las bases de datos de la institución, tal y como lo indica la ley de habeas data.
- d. **Explicar Usos y fines de la Información:** Cuando se va a recolectar información, de acuerdo a los lineamientos de la ley 1581 de 2012, es deber de quien realiza este ejercicio, informar cuáles serán los usos y finalidades de dicha información, para lo cual el titular indicará la autorización o no de esta, dicha información única y exclusivamente podrá ser utilizada para los usos y fines autorizados por el titular, la Universidad Tecnológica de Pereira informa los usos y finalidades de la información recolectada, de manera verbal o escrita y deja evidencia de esto, en los formatos diseñados para recoger la información.
- e. **La UTP cuenta con aviso de privacidad:** La Universidad Tecnológica de Pereira cuenta con un Aviso de Privacidad para informar a los Titulares sobre el tratamiento y uso dado a sus datos personales y la existencia de la directriz sobre protección de los datos personales que se encuentra en 1313-MGD-01 Manual General de Directrices de Seguridad de la Información. Este aviso deberá ser remitido al momento de solicitar la información al Titular.
- f. **Sanciones por incumplimiento:** El ciclo sobre protección de datos personales en la Universidad Tecnológica, es concebido con la firme intención de evitar sanciones por incumplimiento de

Código	1313-SIG-MC-05
Versión	2
Fecha	16-12-2025
Página	28 de 33

alguno de los lineamientos de la ley 1581 de 2012, por parte de la Superintendencia de Industria y Comercio (SIC), objetivo que se logrará aplicando fielmente cada uno de los pasos del presente ciclo enunciados anteriormente.

6. Programa Integral sobre Protección datos Personales UTP

La Universidad Tecnológica de Pereira, tiene diseñada dentro de sus directrices de Seguridad de la Información, los lineamientos necesarios para garantizar la protección de los datos personales de sus partes interesadas, directriz que soporta y fundamenta el programa integral de protección de datos personales de la institución, Ver anexo 3, SGC-MC5-FOR-02 Programa Integral de protección de datos personales, en el cual se pueden encontrar todas las indicaciones de la guía de responsabilidad demostrada de la Superintendencia de Industria y Comercio (SIC) y la manera como da cumplimiento la UTP.

7. Registro Nacional de Base De Datos (RNBD)

La Universidad Tecnológica de Pereira, registra sus bases de datos de acuerdo a lo establecido por la Superintendencia de Industria y Comercio (SIC) y conforme a lo dispuesto por la Ley 1581 de 2012. Para la recolección de la información que será reportada ante la SIC, se utiliza el formato 1313-F17, donde se consolida la información para posteriormente reportarla a la plataforma de la Superintendencia de Industria y Comercio, actividad que realiza el Oficial de Protección de Datos Personales o quien haga sus veces en la institución.

Código	1313-SIG-MC-05
Versión	2
Fecha	16-12-2025
Página	29 de 33

CAPITULO 3.

Seguridad Digital Web, cumplimiento Resolución 1519 de 2020, Anexo 3.

La Resolución 1519 de 2020 del Ministerio de las Tecnologías Informáticas y comunicaciones MinTic, establece los criterios para la estandarización de contenidos e información, accesibilidad, seguridad, datos abiertos, y PQRS, para los obligados a dar cumplimiento a datos señalados en la Ley de Acceso a la Información Pública, en el presente capítulo nos centraremos únicamente al cumplimiento del anexo 3 de dicha resolución, correspondiente a la Seguridad Digital Web.

TABLA DE CONTENIDO.

1. Objetivo.....	30
2. Alcance.....	30
3. Definiciones / Abreviaturas.....	30
4. Autodiagnóstico de condiciones mínimas técnicas y de seguridad digital web.....	32

Código	1313-SIG-MC-05
Versión	2
Fecha	16-12-2025
Página	30 de 33

1. Objetivo.

Servir de guía para mostrar el grado de cumplimiento de los controles que señala la Resolución 1519 de 2020 en su Anexo 3, del Ministerio de las Tecnologías Informáticas y las Comunicaciones MinTic, referente a las condiciones mínimas técnicas y de Seguridad digital Web, en la Universidad Tecnológica de Pereira.

2. Alcance.

Este capítulo da alcance al cumplimiento de las disposiciones de la Resolución 1519 de 2020 en su Anexo 3, del Ministerio de las Tecnologías Informáticas y las Comunicaciones MinTic, sobre las condiciones mínimas técnicas y de Seguridad digital Web, en la Universidad Tecnológica de Pereira.

3. Definiciones / Abreviaturas.

- **MinTic:** El Ministerio de Tecnologías de la Información y las Comunicaciones, según la Ley 1341 o Ley de TIC, es la entidad que se encarga de diseñar, adoptar y promover las políticas, planes, programas y proyectos del sector de las Tecnologías de la Información y las Comunicaciones.
- **Resolución 1519 de 2020:** Contiene cuatro anexos, el primero desarrolla las directrices de accesibilidad web; el segundo incorpora nuevos estándares de transparencia y divulgación de contenidos; el tercero dispone medidas en materia de seguridad digital; y el cuarto dispone condiciones sobre datos abiertos, con la publicación de la Resolución, MinTIC desarrolla las

Código	1313-SIG-MC-05
Versión	2
Fecha	16-12-2025
Página	31 de 33

bases para impulsar la transformación digital de las entidades públicas, a partir de cambios en los sitios web y las nuevas sedes electrónicas de las entidades.

- Accesibilidad web: Son las condiciones y características de los contenidos dispuestos en medios digitales por parte de los sujetos obligados para que puedan ser utilizados por la mayoría de ciudadanos independientemente de sus condiciones tecnológicas o del ambiente, e incluyendo a las personas con discapacidad.
- Seguridad digital web: El avance de la digitalización también implica que los sujetos obligados deban garantizar la disponibilidad de los sitios web y, en especial, la seguridad digital, la seguridad de la información y la privacidad de los datos.
- Trasparencia y Acceso a la información pública: La prerrogativa que tiene toda persona para acceder a la información generada, administrada o en poder de los Entes Públicos. Puede definirse como el conjunto de las normas jurídicas que regulan el acceso ciudadano a la información de interés público, particularmente la que general los órganos del Estado.
- Condiciones mínimas técnicas y de seguridad digital: Son las condiciones mínimas técnicas que deben de cumplir los sujetos obligados referente a la seguridad digital, estas se definen en el Anexo 3 de la resolución 1519 de 2020.
- Discapacidad: Conforme la Convención Interamericana para la Eliminación de todas las formas de discriminación contra las Personas con discapacidad, aprobada en Colombia por medio de la Ley [762](#) de 2002, es la deficiencia física (consiste en falta, deterioro o alteración funcional de una o más partes del cuerpo, y que provoque inmovilidad o disminución de movilidad), mental (consiste en alteraciones o deficiencias en las funciones mentales, específicamente en el pensar, sentir y relacionarse) o sensorial (consiste en el deterioro o falta de la función sensorial de oír o de ver, principalmente), que limita la capacidad de ejercer una o más actividades esenciales de la vida diaria, que puede ser causada o agravada por el entorno económico y social. Recientemente, también se ha reconocido la discapacidad intelectual/cognitiva, que consiste en limitaciones significativas en el funcionamiento intelectual y en la conducta adaptativa, que se manifiesta en habilidades adaptativas conceptuales, sociales y prácticas.

Código	1313-SIG-MC-05
Versión	2
Fecha	16-12-2025
Página	32 de 33

- **Usabilidad Web:** Es una medida que comprende un conjunto de principios que son utilizados para optimizar la navegación, de forma que sea sencilla, intuitiva, agradable y segura.
- **Principios que orientan la accesibilidad Web:** Serán principios que orienten la accesibilidad web, los siguientes:
 - a. **Perceptible:** La información y los componentes de la interfaz de usuario deben ser puestas a disposición de los usuarios de manera que puedan percibirlos, incluyendo alternativas de texto, subtítulos, contenido distingible, uso del color, entre otros aspectos.
 - b. **Operable:** Los componentes de interfaz de usuario y la navegación deben facilitar el acceso, uso y operación por parte de los usuarios, incluyendo teclado accesible, ordenes mediante voz, pantallas táctiles, entre otros aspectos.
 - c. **Comprensible:** La información/textos deben ser legibles y claros (lenguaje claro), y el funcionamiento de la interfaz facilite que el contenido sea predecible para los usuarios.
 - d. **Robusto:** El contenido web debe permitir ser interpretado por una amplia gama de los usuarios y las tecnologías de asistencia para la accesibilidad al usuario, incluyendo las ayudas técnicas.
- **Criterios generales de accesibilidad web para contenidos audiovisuales web:** Los sujetos obligados tendrán que adecuar los contenidos audiovisuales de sus sitios web bajo los siguientes requerimientos:
 - a. **Subtítulos o Closed Caption:** A partir del 1 de enero del 2022, todos los sujetos obligados deberán incluir en el 100% de los contenidos audiovisuales (vídeos) nuevos la opción de subtítulos incorporados o texto escondido (closed caption) auto activable por los usuarios. Esta disposición no aplica para transmisiones en vivo y en directo.

4. Autodiagnóstico de condiciones mininas técnicas y de seguridad digital web

La Universidad Tecnológica de Pereira, en materia del cumplimiento de la Resolución 1519 del año 2020 del Ministerio de las Tecnologías Informáticas y las comunicaciones MINTIC, realizó un diagnóstico donde se verificó las condiciones mininas técnicas y de seguridad digital web, ejercicio

Código	1313-SIG-MC-05
Versión	2
Fecha	16-12-2025
Página	33 de 33

con el cual se validó el porcentaje de cumplimiento de los 26 controles de seguridad digital, así como de las 6 condiciones de seguridad digital en relación a la programación del código fuente.

El diagnóstico fue realizado en conjunto por miembros de las oficinas de Gestión de las Tecnologías informáticas y Sistemas de Información (GTISI), Centro de Recursos Informáticos y Educativos (CRIE), Gestión del Sistema Integral de Calidad y El Equipo Técnico de Seguridad de la información, allí se revisaron cada uno de los controles y se identificaron los porcentajes de implementación de estos en la institución así como los recursos necesarios para aquellos en los cuales no se cumplía totalmente con el requisito.

El resultado del Diagnóstico de las condiciones mínimas técnicas y de seguridad digital, se encuentra en el Anexo 4, SGC-MC5-FOR-03 Diagnóstico Seguridad Digital Web.

Elaborado por:	Revisado por:	Aprobado por:
Personal UTP	Profesional Especializado III Gestión del Sistema Integral de Calidad	Directivo 21 Vicerrectoría Administrativa y Financiera

***** Fin del Documento *****