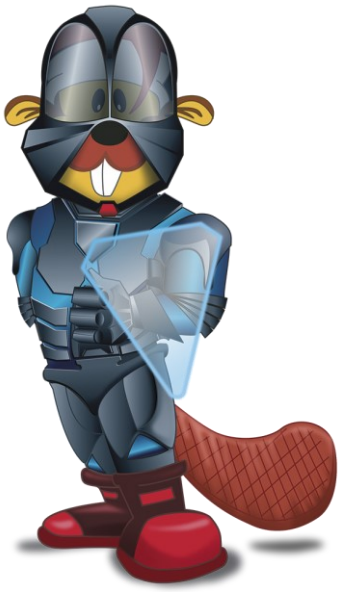
MANUAL DE CALIDAD:

GESTIÓN DEL SISTEMA INTEGRAL DE CALIDAD

SEGURIDAD DE LA INFORMACIÓN

Norma 27001:2013



ORIGINAL
2021-05-21

TABLA DE CONTENIDO.

1. OBJETIVO

Presentar el Manual del Sistema de Gestión de Seguridad de la Información (SGSI), es 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.

2. ALCANCE

Este Manual aplica para dar cumplimiento a los requisitos de la norma ISO/IEC 27001 en su versión vigente.

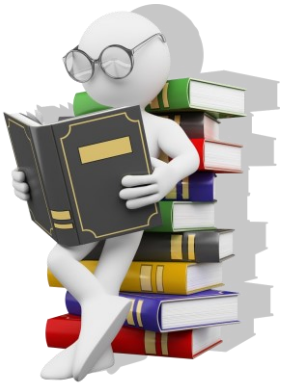
3. DEFINICIONES / ABREVIATURAS

- **Manual de Calidad:** Documento que especifica el Sistema de Gestión de una organización.

- **Objetivo de Calidad:** Lo que se busca, o pretende relacionado con el Sistema 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-categoria/277/terminos-y-definiciones

3.1 CONTENIDO

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



- El Manual de Calidad 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.

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 es para:

Gestión de Tecnologías Informáticas y Sistemas de Información, específicamente:

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

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

Cetro de Recursos Informáticos y Educativos:

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

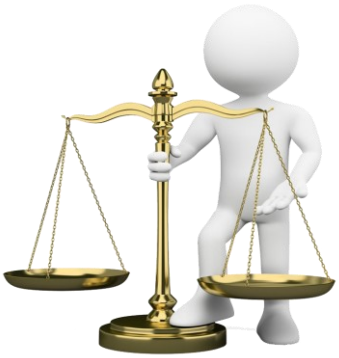
Gestión de documentos:

- Custodio de la información

4. CONTEXTO DE LA ORGANIZACIÓN.

4.1 Conocimiento de la organización y de su contexto.

La Universidad Tecnológica de Pereira, determina las cuestiones externas a través de:



- Normatividad de tipo legal por el ministerio de las TICS.
- Gobierno digital, gobierno en línea.
- Ley 1581 de 2012 - Protección de datos personales.
- Ley 1712 de 2014 - Transparencia y acceso a la información.

Las cuestiones internas a través de:

Resoluciones de rectoría y del consejo superior- dependencias de TICS.

4.2 Comprensión de las necesidades y expectativas de las partes interesadas

La universidad Tecnológica de Pereira, identifica como sus partes interesadas a la comunidad universitaria y a los entes gubernamentales tanto locales como nacionales, acatando las normatividades de tipo legal definidas por el ministerio de las TICS, Gobierno digital, gobierno en línea, protección de datos personales, ley de transparencia y acceso a la información pública.

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

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 de Gestión del Sistema Integral de Calidad, en el enlace: https://www.utp.edu.co/gestioncalidad/sin-categoria/284/alcance.

4.4 Sistema de gestión de la Seguridad de la información.

La Universidad Tecnológica de Pereira, cuenta con procedimientos para la implementación, mantenimiento y mejoramiento continuo del Sistema, así:

CRIE.

- Administración del sistema de copias de seguridad (Backups)
- Administración servicios correo electrónico, aplicaciones de Google, recursos IP y dominio.
- Gestión de incidentes.

GTI&SI.

- Administración de cuentas de usuarios y permisos.

- Diseño y desarrollo de software.
- Gestión para la conectividad con entidades bancarias.
- Mantenimiento preventivo equipos de cómputo.

GESTIÓN DE DOCUMENTOS

- Custodio de la información

5. LIDERAZGO.

5.1 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:

- Establecimiento y divulgación de la política integral de gestión
- Definiendo objetivos de seguridad de la información compatibles con la dirección estratégica de la universidad Tecnológica de Pereira, los cuales pueden ser consultados en el la página de la universidad, en el enlace: https://www.utp.edu.co/gestioncalidad/sin-categoria/275/objetivos

- Contando con el presupuesto para el sistema de gestión de seguridad de la información.
- Definiendo el plan de acción anual, con el fin de alcanzar los resultados previstos en cuanto a seguridad de la información de la universidad.
- Precisar TIPS de buenas prácticas que contribuyan a la eficacia del SGSI.
- Dando tratamiento a las acciones: Plan de mejoramiento-Oportunidades de mejora con el fin de promover la mejora continua del SGSI.
- Asignando responsabilidades a las áreas de alcance del SGSI.

5.2 Política:

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-categoria/37/politica-integral-de-gestion.

5.3 Roles, responsabilidades y autoridades en la organización

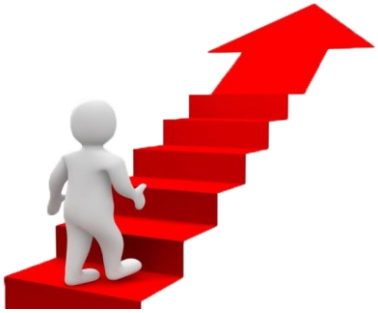
La Universidad Tecnológica de Pereira cuenta con una estructura orgánica definida en el acuerdo 14 de 2015, donde se establecen funciones y responsabilidades, y ha conformado el grupo técnico de seguridad de la información por medio de la Resolución de Rectoría No. 2096 del 24 de septiembre del 2014, el desempeño del Sistema de gestión de seguridad de la información, se revisa por medio del procedimiento “Revisiones por la Dirección al Sistema Integral de Gestión (SIG-PRO-004)”.

6. PLANIFICACIÓN

6.1 Acciones para tratar riesgos y oportunidades.

Se tiene establecido el procedimiento "Administración de Riesgos (SIG-PRO-11)", donde se identifican y valoran los riesgos relacionados con la operación de las áreas de alcance del SGSI específicamente en el numeral 4.2.C. El tratamiento de los riesgos de la seguridad de la información se verifica con relación a los controles existentes en el manual general de directrices y los presentes en el mapa de riesgos de la universidad.

6.2 Objetivos de seguridad de la información y planes para lograrlos.



Los objetivos de calidad se indican en el formato SGC-MC2-FOR-02, son definidos anualmente y publicados en el link: https://www.utp.edu.co/gestioncalidad/sin-categoria/275/objetivos

7. SOPORTE

7.1 Recursos

El Sistema de Gestión de seguridad de la información, cuenta con recursos humanos, financieros y de infraestructura física y tecnológica, necesarios para la operación de cada una de los procesos y la implementación de la norma ISO/IEC 27001.

Los recursos necesarios para la operación de los procesos (talento humano e infraestructura) y mejoramiento continuo del Sistema de Gestión de seguridad de la información, se establecen en el presupuesto de cada vigencia y son gestionados por cada uno de los procesos.

7.2 Competencia.

La Universidad Tecnológica de Pereira tiene contemplado 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, dichos manuales pueden ser consultados en la página de Gestión del Sistema Integral de Calidad de la institución, ingresando a la dependencia o área específica; de igual manera la universidad se asegura que el personal 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.

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; con los cuales se pretende la toma de conciencia en el 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

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-categoria/801/seguridad-de-la-informacion-iso-27001-2013-y-gobierno-en-linea, TIPS de calidad, brigadas de calidad periódicas con el fin de sensibilizar y dar a conocer la normatividad interna de las buenas prácticas relacionadas a la seguridad de la información, así como el manual general de directrices definida por la Universidad Tecnológica de Pereira.

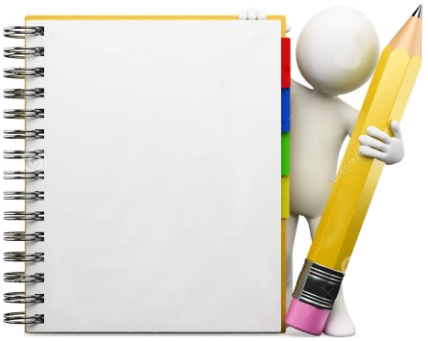
7.5 Información documentada

La documentación necesaria que respalda el SGSI, se da a través de procedimientos, manual general de directrices de seguridad de la información, formatos y registros como autorización de tratamiento de datos personales y activos de información.

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.).

8. OPERACIÓN

8.1 Planificación y control operacional



La planificación y control operacional del Sistema de Gestión de Seguridad de la información se determina a través del plan de acción anual definido por el grupo técnico del SGSI; se mantiene información documenta referente a la ejecución del mismo.

8.2 Valoración de riesgos de la seguridad de la información.

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 V5.

8.3 Tratamiento de riesgos de la seguridad de la información.

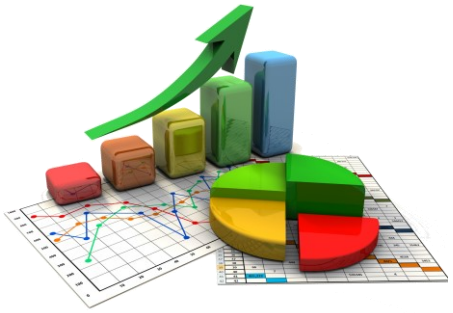
Para el tratamiento de los riesgos de seguridad de la información se utiliza la metodología de riesgos definida por la Universidad documentada en el Procedimiento de Administración de riesgos SGC-PRO-011 V5.

9.0 EVALUACIÓN DEL DESEMPEÑO

9.1 Seguimiento, medición, análisis y evaluación

El grupo técnico de seguridad de la información, conformado por representantes de Control Interno, Jurídica, Gestión del Sistema Integral de Calidad, Centro De Recursos Informáticos Y Educativos (CRIE)

y de Gestión De Tecnologías Informáticas y Sistemas De Información (GTI&SI), realiza seguimiento, medición, análisis y evaluación a planes de trabajo interno, indicadores, identificación de riesgos, entre otros, 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 y medición son analizados por las dependencias involucradas para la definición de acciones y fortalecimiento de planes de mejoramiento.

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)”.

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 a Gestión del Sistema Integral de Calidad (SIG-PRO-004)”.

10. MEJORA.

10.1 No conformidades y acciones correctivas.

Para dar tratamiento a las no conformidades y acciones correctivas al Sistema de Gestión de Seguridad de la Información se sigue el procedimiento para "Toma de Acciones (SIG-PRO-006)".

10.2 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)".

11. DOCUMENTOS DE REFERENCIA

- Norma ISO/IEC 27001- Requisitos.

Elaborado por:	**Revisado por:**	**Aprobado por:**
Personal UTP	Profesional I Gestión del Sistema Integral de Calidad.	Profesional IV Gestión del Sistema Integral de Calidad.