PLAN POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Oficina de Gestión Informática – Sistemas y Soporte Técnico

24Enero2026

1. INTRODUCCIÓN

La Universidad Tecnológica del Chocó considera la información como un recurso esencial para su gestión académica y administrativa y, por tanto, requiere asegurar su adecuada protección. Bajo este propósito, la Universidad avanza en la adopción de un Sistema de Gestión de Seguridad de la Información (SGSI), mediante el cual se establecen lineamientos y mecanismos orientados a preservar la confidencialidad, integridad y disponibilidad de la información institucional en todas las actividades donde sea generada, almacenada, procesada o transmitida.

El presente documento establece las políticas que estructuran el Sistema de Gestión de Seguridad de la Información de la Universidad Tecnológica del Chocó. Dichas políticas son de observancia obligatoria para directivos, docentes, personal administrativo, estudiantes, egresados y terceros que, por razón de sus funciones, actividades o vínculos contractuales, accedan, gestionen o utilicen información institucional.

2. JUSTIFICACIÓN

La Universidad Tecnológica del Chocó requiere contar con lineamientos claros que orienten la gestión de la seguridad de la información en todos sus procesos académicos, administrativos y misionales. La adopción de políticas institucionales en esta materia permite establecer un marco ordenado de actuación, indispensable para proteger los activos de información y asegurar la continuidad de las operaciones institucionales.

Este marco normativo busca promover una cultura de responsabilidad frente al tratamiento de la información institucional, sensibilizando a la comunidad universitaria sobre el valor de la información que manipula, los riesgos tecnológicos y humanos a los que está expuesta, y la necesidad de adoptar prácticas que reduzcan incidentes de seguridad o mitiguen su impacto cuando estos ocurran.

Asimismo, la definición de políticas de seguridad contribuye al cumplimiento de *obligaciones legales, contractuales y regulatorias aplicables a la* Universidad, especialmente en lo relacionado con la protección de datos personales, privacidad y manejo seguro de la información. De esta forma, la Universidad Tecnológica del Chocó fortalece su desempeño institucional y garantiza que la gestión de la información se realice en concordancia con las normas vigentes y con las expectativas de transparencia, confianza y seguridad que demanda la comunidad y el entorno.

3. MARCO NORMATIVO Y GENERAL

Para fortalecer la seguridad de la información, la Universidad Tecnológica del Chocó puede adoptar estándares internacionales que orienten el diseño, implementación y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI). Entre los más relevantes se encuentran:

3.1. ISO/IEC 27001 — Implementación del SGSI en la UTCH

La norma ISO/IEC 27001 proporciona un marco para implementar y gestionar un SGSI que permita proteger adecuadamente la información académica, administrativa y misional de la Universidad.

Su aplicación en la UTCH implica:

- Definir políticas y procedimientos de seguridad.
- Identificar activos de información institucional.
- Establecer controles para garantizar confidencialidad, integridad y disponibilidad.
- Monitorear y mejorar continuamente la seguridad tecnológica.

Esto contribuye a elevar la madurez institucional en ciberseguridad y a disminuir riesgos asociados a accesos no autorizados, pérdida de datos o fallas operativas.

3.2. ISO/IEC 27002 — Buenas prácticas y controles para la UTCH

La norma ISO/IEC 27002 complementa ISO/IEC 27001 definiendo los controles específicos que la Universidad puede implementar en materia de:

- Control de accesos.
- Seguridad en redes y comunicaciones.
- Gestión de incidentes.
- Protección de datos y privacidad.
- Seguridad en proveedores y terceros.
- Uso seguro de recursos tecnológicos.

Su adopción facilita la formalización de manuales, directrices y protocolos que deben ser aplicados por docentes, administrativos, estudiantes, egresados y contratistas que interactúen con la información institucional.

Código: 530

3.3. ISO/IEC 27005 — Gestión de riesgos para la UTCH

Este estándar proporciona las bases para analizar y gestionar riesgos que afecten los activos de información de la Universidad.

Su aplicación práctica en la UTCH implica:

- Identificar amenazas (ciberataques, fallas, errores humanos, etc.).
- Evaluar vulnerabilidades tecnológicas y operativas.
- Determinar impacto sobre procesos institucionales.
- Establecer planes de tratamiento y mitigación.

Con este enfoque, la Universidad puede priorizar recursos y tomar decisiones basadas en riesgo, alineadas con sus objetivos misionales y normativos.

Las ventajas institucionales aplicadas con la adopción del enfoque ISO 27000 conduce a beneficios como:

- Fortalecimiento de la gobernanza TI
- Reducción de incidentes de seguridad
- Protección de datos personales y cumplimiento legal
- Mejor gestión de la continuidad del servicio
- Mayor confianza institucional y reputacional

4. OBJETIVOS

Establecer un Sistema de Gestión de Seguridad de la Información en la Universidad Tecnológica del Chocó, orientado a proteger la confidencialidad, integridad y disponibilidad de la información institucional mediante la adopción de políticas, controles, estándares internacionales y prácticas de gestión del riesgo que fortalezcan la operación académica, administrativa y misional de la institución.

5. ALCANCE

El Sistema de Gestión de Seguridad de la Información de la Universidad Tecnológica del Chocó aplica a todos los procesos académicos, administrativos y misionales que involucren el uso, tratamiento, almacenamiento, transmisión o gestión de información institucional, incluyendo datos personales, operativos y estratégicos. Este alcance cubre a toda la comunidad universitaria (directivos, docentes, administrativos, estudiantes, egresados y

contratistas), así como a los sistemas de información, infraestructura tecnológica, servicios digitales y terceros que accedan o interactúen con la información bajo responsabilidad de la Universidad.

6. DESARROLLO

6.1. Política general de seguridad y privacidad de la información

La Política General de Seguridad y Privacidad de la Información expresa el compromiso de la Alta Dirección de la Universidad Tecnológica del Chocó frente a la protección y gestión adecuada de los activos de información institucional. Esta declaración refleja la responsabilidad de la Universidad en el establecimiento y fortalecimiento de un Sistema de Gestión de Seguridad de la Información (SGSI), así como su interés en promover buenas prácticas, asegurar su divulgación y garantizar un proceso de mejora continua.

En coherencia con su carácter de institución de educación superior, la Universidad Tecnológica del Chocó orienta la gestión de la seguridad y privacidad de la información mediante la aplicación de controles administrativos, técnicos y físicos, basados en la identificación y tratamiento de riesgos. Dichos controles buscan preservar la confidencialidad, integridad y disponibilidad de la información en todo su ciclo de vida, incluyendo aquella vinculada a procesos académicos, administrativos, investigativos, misionales y de extensión.

La Universidad asume este compromiso en armonía con los marcos regulatorios, legales y contractuales aplicables, especialmente en materia de protección de datos personales y seguridad digital, contribuyendo al fortalecimiento institucional, a la confianza de la comunidad universitaria y a la prestación segura y eficiente de los servicios que ofrece.

Este proceso de medición, seguimiento y monitoreo permitirá evaluar la eficacia de los controles, verificar el cumplimiento de los objetivos de seguridad establecidos y promover la mejora continua del SGSI, en coherencia con el enfoque de desempeño y mejora definido por la ISO/IEC 27001.

7. OBJETIVOS DE LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Los objetivos de la gestión de la seguridad de la información en la Universidad Tecnológica del Chocó son:

1. **Proteger los activos de información institucional**, garantizando la preservación de su confidencialidad, integridad, disponibilidad y trazabilidad en todos los procesos académicos, administrativos, investigativos y misionales.

2. **Implementar un enfoque de gestión de riesgos** que permita identificar, evaluar, tratar y monitorear amenazas que puedan afectar la información, la operación institucional y la prestación de servicios a la comunidad universitaria.
3. **Cumplir con la normatividad legal, regulatoria y contractual aplicable**, especialmente en materia de protección de datos personales, privacidad, seguridad digital y gestión documental.
4. **Promover una cultura de seguridad y privacidad** entre docentes, administrativos, estudiantes, egresados, contratistas y terceros, mediante procesos de formación, divulgación, sensibilización y buenas prácticas en el uso de la información.
5. **Establecer controles administrativos, físicos y tecnológicos** que mitiguen los riesgos asociados al uso de sistemas de información, redes, infraestructura tecnológica y servicios digitales utilizados por la Universidad.
6. **Garantizar la continuidad de las operaciones institucionales** ante incidentes de seguridad, fortaleciendo las capacidades de prevención, respuesta y recuperación a nivel tecnológico y organizacional.
7. **Fortalecer la gestión institucional** mediante la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) con enfoque de mejora continua que responda a las necesidades de la Universidad y su entorno.
8. **Proteger la imagen, reputación y confianza institucional** mediante prácticas de seguridad que resguarden los datos personales, la propiedad intelectual, los resultados de investigación y demás información estratégica.

8. POLÍTICAS ESPECÍFICAS PARA LA SEGURIDAD DE LA INFORMACIÓN

8.1. Política de control de acceso

La **Política de Control de Acceso** de la Universidad Tecnológica del Chocó establece las directrices y medidas requeridas para regular y asegurar el acceso adecuado a los sistemas de información, recursos tecnológicos y datos institucionales. Su objetivo principal es garantizar que únicamente las personas autorizadas puedan acceder, consultar, modificar o administrar la información, de acuerdo con sus funciones y responsabilidades, manteniendo la confidencialidad, integridad y disponibilidad de los activos de información institucional.

8.2. Política de uso de dispositivos móviles

La presente política establece los lineamientos para el uso adecuado y seguro de dispositivos móviles en la Universidad Tecnológica del Chocó, con el fin de proteger la información institucional y mitigar riesgos asociados a divulgación, pérdida, manipulación indebida o acceso no autorizado.
Se entenderán como dispositivos móviles los teléfonos inteligentes, tabletas, laptops, dispositivos portátiles de almacenamiento y cualquier equipo con capacidad de procesamiento y conectividad que sea utilizado para acceder, almacenar o transmitir información institucional.

8.3. Política de Teletrabajo

La presente política establece las directrices para el desarrollo de actividades laborales bajo la modalidad de teletrabajo en la Universidad Tecnológica del Chocó, definiendo las condiciones mínimas de seguridad, uso de recursos tecnológicos y protección de la información institucional, cuando por razones operativas, administrativas o de fuerza mayor se autorice la ejecución de funciones fuera de las instalaciones físicas de la Universidad.

Su implementación se encuentra condicionada a las necesidades institucionales y a la normatividad vigente, y no constituye obligación para la Universidad habilitar dicha modalidad de manera permanente.

8.4. Política sobre el Uso de Controles Criptográficos

La Universidad Tecnológica del Chocó establece la presente política con el fin de definir los criterios y lineamientos para el uso adecuado de controles criptográficos que protejan la información institucional durante su almacenamiento, transmisión y procesamiento. Estos controles serán utilizados para garantizar la confidencialidad, integridad, autenticidad y no repudio de la información, cuando así lo exijan los requisitos legales, contractuales, técnicos o de riesgo.

8.5. Política de escritorio y pantalla limpia

La presente política establece las directrices para la implementación de prácticas de **escritorio limpio** y **pantalla limpia** en la Universidad Tecnológica del Chocó, con el fin de reducir la exposición de la información institucional ante accesos y observaciones no autorizadas. Su finalidad es proteger la confidencialidad, la integridad y la disponibilidad

de los activos de información que se gestionan en espacios de trabajo, computadores y equipos utilizados por la comunidad universitaria.

8.6. Política para la Generación y Restauración de Copias de Respaldo

La presente política establece los lineamientos para la generación, almacenamiento, protección y restauración de copias de respaldo de la información institucional en la Universidad Tecnológica del Chocó, con el fin de asegurar la recuperación oportuna de datos ante incidentes que afecten la disponibilidad o integridad de los activos de información.

8.7. Política para la transferencia de información

La presente política establece los lineamientos que regulan la transferencia de información institucional entre sistemas, dependencias, usuarios internos, proveedores y terceros autorizados, con el fin de garantizar la seguridad, confidencialidad, integridad y disponibilidad de los datos durante su intercambio. Esta política aplica a cualquier tipo de transferencia física o digital que involucre información generada, almacenada o administrada por la Universidad Tecnológica del Chocó.

8.8. Política de Desarrollo Seguro de Software

La presente política establece los lineamientos, criterios y prácticas mínimas para el diseño, desarrollo, implementación, mantenimiento y retiro de software utilizado o producido por la Universidad Tecnológica del Chocó, con el fin de garantizar que las aplicaciones informáticas protejan la información institucional desde su concepción, durante su operación y a lo largo de todo su ciclo de vida. Su objetivo principal es reducir vulnerabilidades, prevenir incidentes de seguridad y promover un enfoque de desarrollo basado en riesgos y buenas prácticas.

8.9. Política de seguridad para la relación con proveedores

La presente política establece los lineamientos que regulan la relación de la Universidad Tecnológica del Chocó con proveedores, aliados estratégicos, contratistas y terceros que participen en procesos que involucren tratamiento, acceso, administración, custodia o soporte de información institucional, con el fin de garantizar que dichos actores cumplan con estándares mínimos de seguridad, protección de datos y confidencialidad.

9. ROLES Y RESPONSABILIDADES

- **Consejo Superior y Rectoría:** Definen la planeación estratégica y orientan la autoevaluación institucional.
- **Consejo Académico:** Desarrollan y realizan seguimiento a las políticas institucionales.
- **Rectoría + Dirección de TI + Responsable de Seguridad:** Implementan, acompañan, orientan y mejoran la política de seguridad de la información.
- **Vicerrectoría Académica y Vicerrectoría Administrativa:** Ejecutan y evalúan la política en procesos, programas y servicios bajo su gestión.
- **Dependencias Académicas y Administrativas:** Aplican la política en sus áreas y apoyan la gestión del riesgo y la información.
- **Comunidad Universitaria:** Es corresponsable del cumplimiento (estudiantes, docentes, administrativos, contratistas).

10. MEJORAS

- **Fortalecer la gobernanza TIC:** consolidar comités o instancias formales de seguridad y protección de datos que apoyen la toma de decisiones y el seguimiento institucional.
- **Actualizar políticas y manuales internos:** crear o actualizar las políticas de seguridad, privacidad, protección de datos y uso aceptable según estándares técnicos (ISO 27001, Ley 1581).
- **Estandarizar procesos TI:** establecer procedimientos documentados para acceso, respaldos, incidentes, transferencias y desarrollo seguro.
- **Optimizar infraestructura tecnológica:** incorporar herramientas de ciberseguridad, monitoreo, cifrado y control de accesos conforme a criticidad y riesgos.
- **Mejorar capacidades de continuidad y contingencia:** formalizar planes de respaldo, restauración, continuidad y recuperación ante incidentes.
- **Clasificar la información institucional:** identificar activos críticos, sistemas sensibles y bases de datos personales para definir prioridades y controles.
- **Potenciar la capacitación interna:** desarrollar programas permanentes de formación en seguridad y protección de datos para toda la comunidad universitaria.

11. RECOMENDACIONES

- **Alinear el SGSI con la Planeación Institucional:** asegurar que la seguridad apoye la misión académica, investigativa y administrativa de la Universidad.

- **Formalizar roles y responsabilidades:** definir claramente roles como Responsable del Tratamiento, Encargado, Oficial de Seguridad, Custodios y Dueños de la Información.
- **Establecer indicadores y métricas:** medir avances en incidentes, tiempos de respuesta, disponibilidad, cumplimiento y mejora continua.
- **Integrar la protección de datos en procesos académicos y administrativos:** aplicar la Ley 1581/2012 en matrículas, egresados, publicaciones, bienestar, talento humano, etc.
- **Fortalecer la relación con proveedores:** exigir cláusulas de seguridad y confidencialidad en servicios de software, nube, hosting, soporte y procesamiento de datos.
- **Documentar el ciclo de vida de software e información:** desde su creación hasta su disposición final, incorporando controles técnicos y legales.
- **Promover cultura de corresponsabilidad:** fomentar el uso adecuado de recursos tecnológicos entre estudiantes, docentes y administrativos.

12. CONCLUSIONES

- La **seguridad de la información** y la **protección de datos personales** son componentes esenciales para el cumplimiento misional de la Universidad Tecnológica del Chocó en los ámbitos académico, administrativo, científico y social.
- La implementación de un **Sistema de Gestión de Seguridad de la Información (SGSI)** permite gestionar riesgos tecnológicos y organizacionales, mejorar la continuidad operativa y fortalecer la confianza de la comunidad universitaria.
- El cumplimiento de la **Ley 1581 de 2012**, el **Decreto 1377 de 2013**, la **Ley 1273 de 2009**, así como de estándares como **ISO/IEC 27001**, garantiza un tratamiento adecuado de la información institucional y de los datos personales.
- La corresponsabilidad entre **Consejo Superior, Rectoría, Vicerrectorías, Dependencias académicas/administrativas, TI y usuarios** es clave para la correcta implementación del modelo.
- La consolidación de políticas, procedimientos, roles, capacitación y controles técnicos permitirá a la Universidad Tecnológica del Chocó avanzar en temas como **gobernanza digital**, **mejora continua**, **transformación tecnológica** y **protección de activos de información**.
- El fortalecimiento del SGSI y de los procesos de protección de datos contribuye a mejorar la **imagen institucional**, la **calidad de los servicios**, la **transferencia tecnológica** y la **competitividad académica y administrativa** de la Universidad.

Código: 530

La seguridad de la información en la Universidad Tecnológica del Chocó se entiende como el conjunto de principios, políticas, procedimientos, controles y prácticas orientadas a proteger los activos de información institucional frente a amenazas internas y externas, garantizando en todo momento su confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad. Este enfoque integral reconoce a la información como un recurso estratégico para la misión académica, investigativa y administrativa de la Universidad, y establece la necesidad de implementar un Sistema de Gestión de Seguridad de la Información (SGSI) que permita gestionar riesgos, fortalecer el cumplimiento normativo, promover la corresponsabilidad institucional y asegurar la continuidad operativa en beneficio de la comunidad universitaria y del entorno social que acompaña la labor de la institución.

Atentamente,

RAFAEL SANDOVAL MORALES
Jefe Gestión Informática – Sistemas y Soporte Técnico
a-rafael.sandoval@utch.edu.co

Realizó: Rafael Sandoval Morales Cargo: Jefe Oficina Gestión Informática – Sistemas y soporte técnico (e) Fecha: 24 de enero de 2026	**Revisó:** Deimer Stiwar Mena Murillo Cargo: Profesional Especializado - Oficina Gestión Informática – Sistemas y soporte técnico Fecha: 24 de enero de 2026	**Aprobó:** Rafael Sandoval Morales Cargo: Jefe Oficina Gestión Informática – Sistemas y soporte técnico (e) Fecha: 24 de enero de 2026