Tecnológico de Antioquia Institución Universitaria
Acreditación Institucional de Alta Calidad
Res. MEN 13167 - 17 Jul 2020 - 8 años

GOBERNACIÓN DE ANTIOQUIA
República de Colombia

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (PSPI)

2022

Tecnológico de Antioquia Institución Universitaria

Contenido

1. OBJETIVO

Construir el plan de seguridad y privacidad de la información acorde a la misión y estrategia del Tecnológico de Antioquia acogiendo el Modelo de Seguridad y Privacidad de la Información - MSPI de la Estrategia de Gobierno en Línea – GEL del Ministerio de Tecnologías de la Información y las Comunicaciones (Min-TIC), para estar acorde con las buenas prácticas de seguridad y teniendo en cuenta las normas ISO 27001 del 2013, Transparencia y Acceso a la Información Pública (Ley 1712 de 2014), la ley de Protección de Datos Personales, entre otras. Este modelo busca preservar la confiabilidad, disponibilidad e integridad de la información, generando estrategias para garantizar la privacidad y el buen uso de los datos que genera y posee la Institución dentro de sus sistemas de información.

2. ALCANCE DEL DOCUMENTO

Este documento busca identificar la metodología, los documentos y procesos que permitan desarrollar el PSPI de la Institución, definiendo las tareas generales en cada una de las etapas de implementación.

De esta forma la institución puede comenzar a definir, implementar y documentar el PSPI de una forma ordenada y de acuerdo a una metodología establecida que garantice el logro de los objetivos establecidos dentro del PSPI.

3. RECURSOS

Aquí se definen los recursos tanto humanos, físicos y financieros que soportan la implementación del PSPI.

Humanos: La definición e implementación del PSPI será liderado por el coordinador de las TIC del TdeA, apoyado por los profesionales que lideran los procesos de los diferentes Sistemas de información, Seguridad de la Información, Telecomunicaciones, Soporte, Infraestructura y acompañados por la oficina de gestión de calidad de la institución.

Físicos: Para lograr los objetivos trazados dentro de la implementación del PSPI se hace necesario el acceso a los equipos de control perimetral con que cuenta la Institución (Firewall, IDS/IPS), al equipo de análisis de tráfico que permitirá una visión más real de lo que está pasando en el perímetro de la red de datos, además el acceso a los centros de cableado, switches CORE y de borde.

4. FASES DE IMPLEMENTACIÓN

Acogiendo lo planteado en el modelo de seguridad y privacidad de la información del MinTIC (MSPI), donde se plantean cinco (5) fases que sirven de ruta para el desarrollo de dicho modelo y permite gestionar de una forma adecuada la seguridad y la privacidad de la información como componente fundamental de los procesos institucionales, se definen las siguientes fases:

Diagnóstico: En esta fase se realiza un levantamiento de información que pretende identificar el estado actual de la seguridad y la privacidad de la información e identificar su nivel de madurez.

Planificación: Partiendo de los resultados de la fase de diagnóstico, se procede a la elaboración del PSPI alineado con el objetivo misional Institucional, definiendo las acciones a implementar y los alcances de dicho plan.

Implementación: Se implementan todas las acciones planteadas en la fase de planificación, teniendo en cuenta indicadores de gestión y tratamiento de la seguridad y privacidad de la información.

Evaluación de Desempeño: A través de auditorías internas, monitoreo, medición y evaluación de controles y los resultados que arrojan los indicadores de la seguridad de la información se puede verificar la efectividad, la eficiencia y la eficacia de las acciones implementadas.

Mejora continua: En esta fase se define el plan de mejoramiento continuo donde se toman acciones para mitigar las debilidades encontradas, de acuerdo a los resultados obtenidos en la fase de evaluación de desempeño.

5. CRONOGRAMA

Fase	Meta	Resultado	Fecha
Diagnostico	Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad.	Diligenciamiento de la herramienta.	En proceso
	Identificar el nivel de madurez de seguridad y privacidad de la información en la Entidad.	Diligenciamiento de la herramienta e identificación del nivel de madurez de la entidad.	Abril 2021
	Identificar vulnerabilidades técnicas y administrativas que sirvan como insumo para la fase de planificación.	Documento con los hallazgos encontrados en las pruebas de vulnerabilidad.	Mayo 2021

Fase	Meta	Resultado	
	Roles y responsabilidades de seguridad y privacidad de la información.	Acto administrativo a través del cual se crea o se modifica las funciones del comité gestión institucional (o el que haga sus veces), en donde se incluyan los temas de seguridad de la información en la entidad, revisado y aprobado por la alta Dirección, deberá designarse quien será el encargado de seguridad de la información dentro de la entidad.	Junio 2021
Planificación	Inventario de activos de información.	Documento con la metodología para identificación, clasificación y valoración de activos de información, validado por el comité de seguridad de la información o quien haga sus veces y revisado y aprobado por la alta dirección. Matriz con la identificación, valoración y clasificación de activos de información. Documento con la caracterización de activos de información, que contengan datos personales	Octubre 2021
Planificación	Política de Seguridad y Privacidad de la Información	Documento con la política de seguridad de la información, debidamente aprobado por la alta Dirección y socializada al interior de la Entidad.	Noviembre 2021
	Políticas de seguridad y privacidad de la información	Manual con las políticas de seguridad y privacidad de la información, debidamente aprobadas por la alta dirección y socializadas al interior de la Entidad.	Noviembre 2021

5.1 SEGUIMIENTO Y EVALUACIÓN

Como se establece en el cronograma todas las fases requieren un seguimiento, unas metas y evaluación que permiten definir las mejores prácticas en cada caso concreto. En reuniones periódicas con el grupo primario que lidera el coordinador de las TIC de la Institución, se socializan todas las actividades y eventos que afectan el PSPI y se hace entrega de documentos o avances asignados en cada fase. De todas estas reuniones se elaboran actas.

6. ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN - SGSI

6.1 Introducción:

El presente documento establece el alcance del Sistema de Gestión de Seguridad de la Información (en adelante SGSI) del Tecnológico de Antioquia – Institución Universitaria.

El SGSI se realiza acorde a la misión y estrategia del Tecnológico de Antioquia – Institución Universitaria acogiendo el Modelo de Seguridad y Privacidad de la Información - MSPI de la Estrategia de Gobierno en Línea – GEL del Ministerio de Tecnologías de la Información y las Comunicaciones (Min-TIC), para estar acorde con las buenas prácticas de seguridad y teniendo en cuenta las normas ISO 27001 del 2013, transparencia y acceso a la Información Pública (Ley 1712 de 2014), la ley de Protección de Datos Personales, entre otras. Este modelo busca preservar la confiabilidad, disponibilidad e integridad de la información, generando estrategias para garantizar la privacidad y el buen uso de los datos que genera y posee la Institución dentro de sus sistemas de información.

El alcance del SGSI permite a la institución definir los límites sobre los cuales se implementará la seguridad y privacidad de la información con un enfoque por procesos, el cual más adelante se extiende a toda la institución.

Mediante el aprovechamiento de las TIC y el modelo de seguridad y privacidad de la información, se trabaja en el fortalecimiento de la seguridad de la información en la institución, con el fin de garantizar la protección de la misma y la privacidad de los datos de los ciudadanos y funcionarios de la entidad, todo esto acorde con lo expresado en la legislación Colombiana.

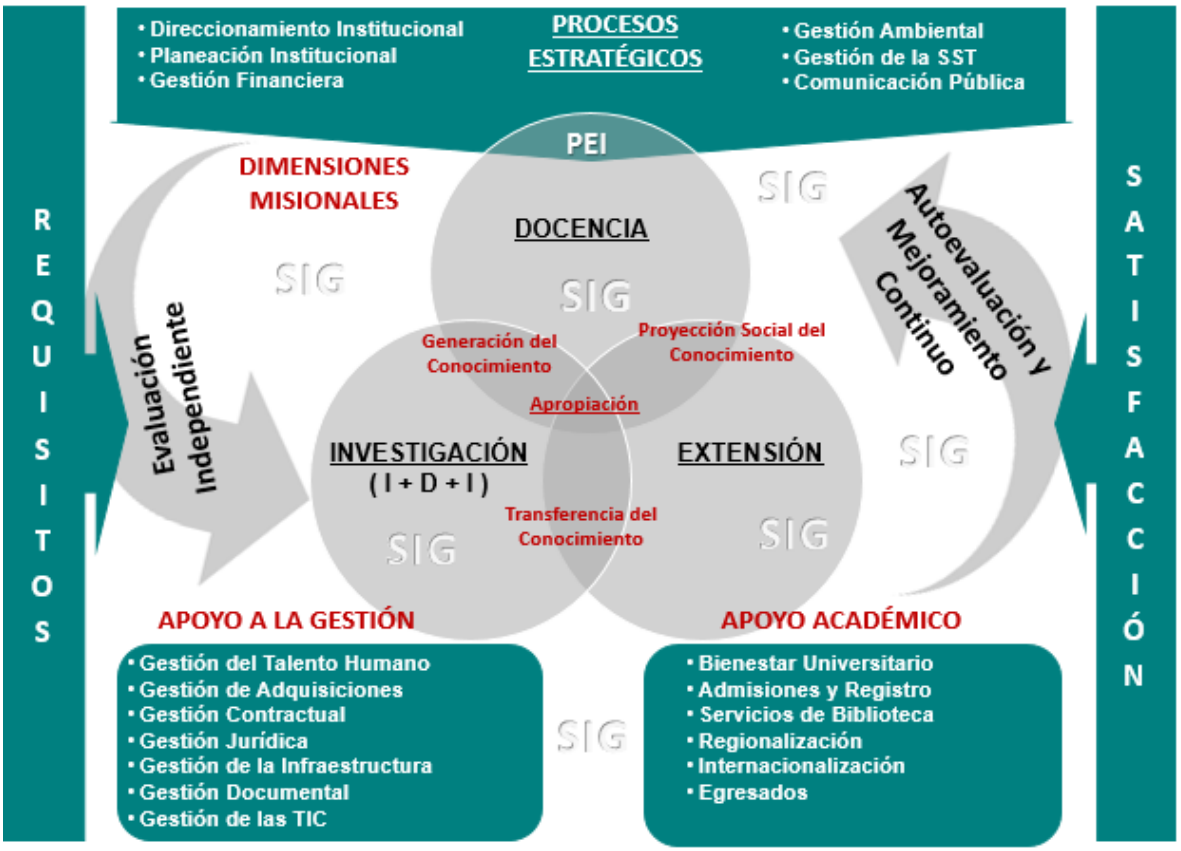
6.2 Objetivo:

Establecer el alcance inicial para la implementación del SGSI, de acuerdo a una valoración de los procesos la cual obedece a un contraste entre los requisitos de la norma ISO 27001, las disposiciones legales, y el impacto de los diferentes usuarios (Clientes, Directivos, Aliados, e

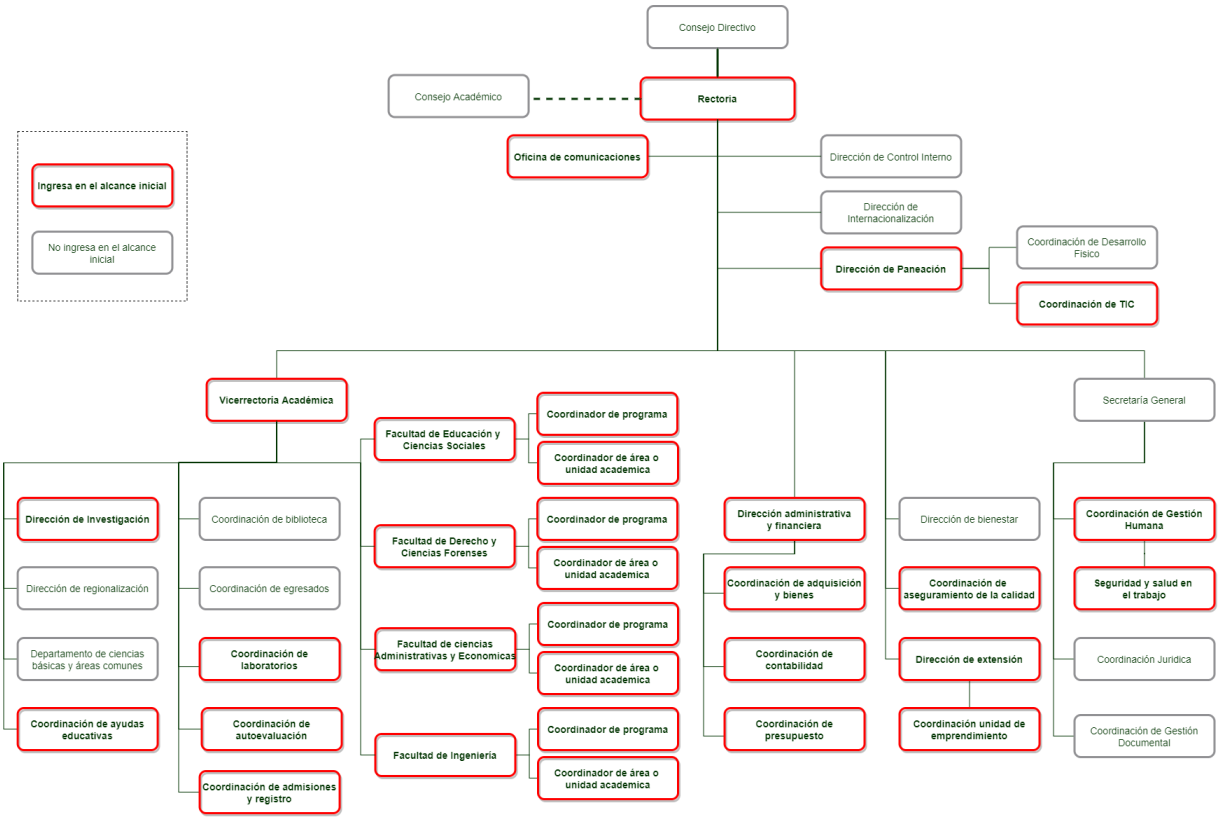
Internos) con los pilares de la seguridad de la información (Integridad, Confidencialidad, Disponibilidad).

6.3 Contexto de la institución:

En la siguiente ilustración se puede conocer el mapa de procesos del Tecnológico de Antioquia – Institución Universitaria, donde podemos identificar las dimensiones misionales, el apoyo a la gestión, el apoyo académico e identificar los procesos estratégicos.



En la siguiente ilustración se resaltan los procesos que hacen parte inicial del alcance del SGSI, estos son los procesos que se encuentran en un rango alto acorde a la valoración de los procesos la cual obedece a un contraste entre los requisitos de la norma ISO 27001, las disposiciones legales, y el impacto de los diferentes usuarios (Clientes, Directivos, Aliados, e Internos) con los pilares de la seguridad de la información (Integridad, Confidencialidad, Disponibilidad), donde cada uno obtiene un resultado numérico (siendo 1 el de menor impacto y 5 el de mayor impacto), y cuyos puntajes, finalmente se promedian y se obtiene un resultado final de valoración, por tal motivo serán los pioneros en la aplicación del SGSI.

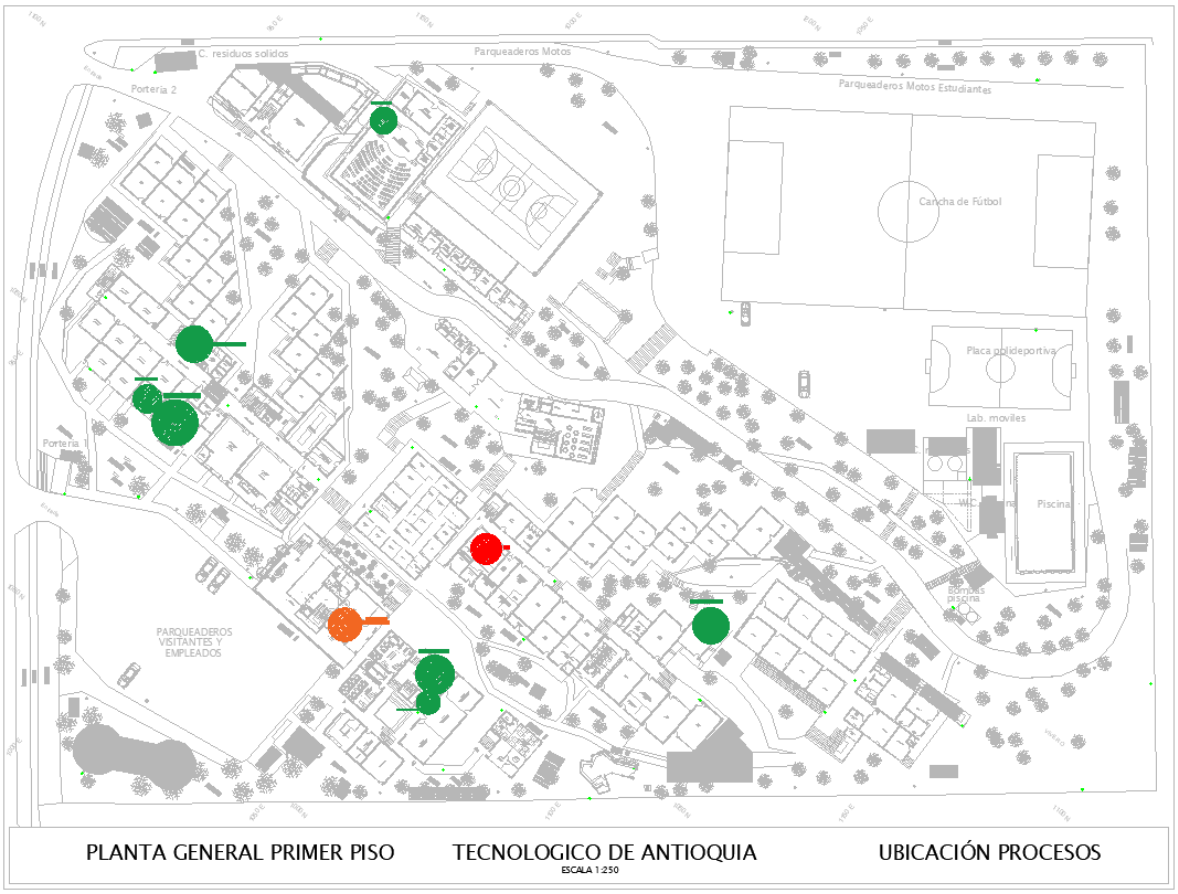


Los puntajes obtenidos por los diferentes procesos los podemos ver en la tabla siguiente, así como la línea de mando correspondiente.

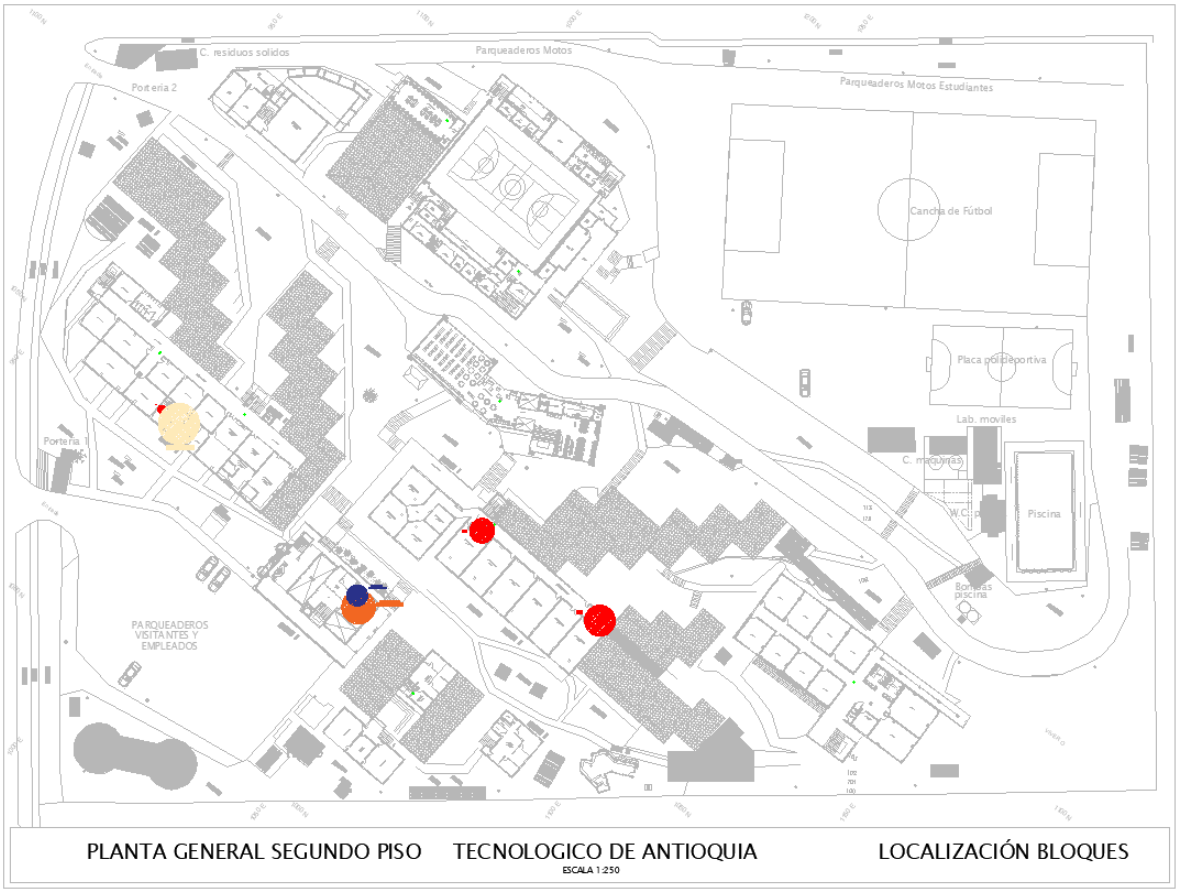
Puntaje	Proceso	Línea de mando
5	GTI - Gestión de las TIC	Rectoría Dirección de Planeación Coordinación de TIC
4	AMC - Autoevaluación y Mejoramiento Continuo	Rectoría Coordinación de Aseguramiento de la Calidad Rectoría Vicerrectoria Academica Coordinación de Autoevaluación
4	DIN - Direccionamiento Institucional	Rectoría Dirección de Planeación, Dirección de Control Interno, Dirección de Internacionalización
4	DOC - Docencia	Rectoría Vicerrectoria Académica Decanatura Coordinación de programa
4	EXT - Extensión	Rectoría Dirección de Extensión Vicerrectoria Académica Líder de la Unidad de Educación Continua, Líder de la Unidad de Proyectos Especiales, Coordinador de la Unidad de Emprendimiento, Líder de Responsabilidad Social Universitaria, Líder de Gestión del Relacionamiento
4	GSS - Gestión de la SST	Rectoría Secretaría General Coordinación de Gestión Humana Coordinador de Seguridad y Salud en el Trabajo, Coordinador de Laboratorios
4	GTH - Gestión del Talento Humano	Rectoría Secretaría General Coordinación de Gestión Humana

Puntaje	Proceso	Línea de mando
4	INV - Investigación	Rectoría Vicerrectoría Academica Dirección de Investigación
4	CPU - Comunicación Pública	Rectoría Profesional de Comunicaciones , Profesional de Ayudas Educativas
4	ADM - Admisiones y Registro	Rectoría Vicerrectoría Academica Coordinador de Admisiones y Registro
4	GFI - Gestión Financiera	Rectoría Dirección Administrativa y Financiera Profesional de Contabilidad, Profesional de Presupuesto

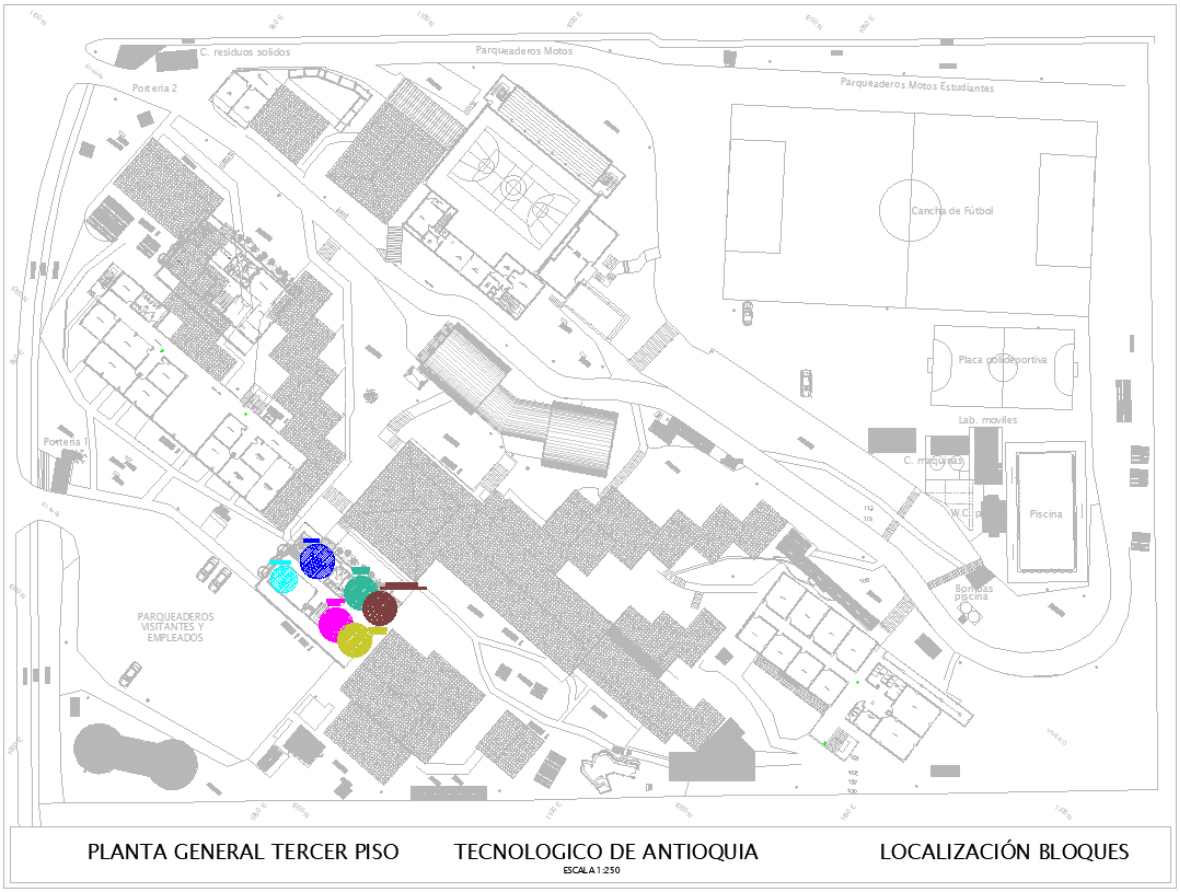
La ubicación de los procesos incluidos en el alcance los encontramos en las siguientes ilustraciones.



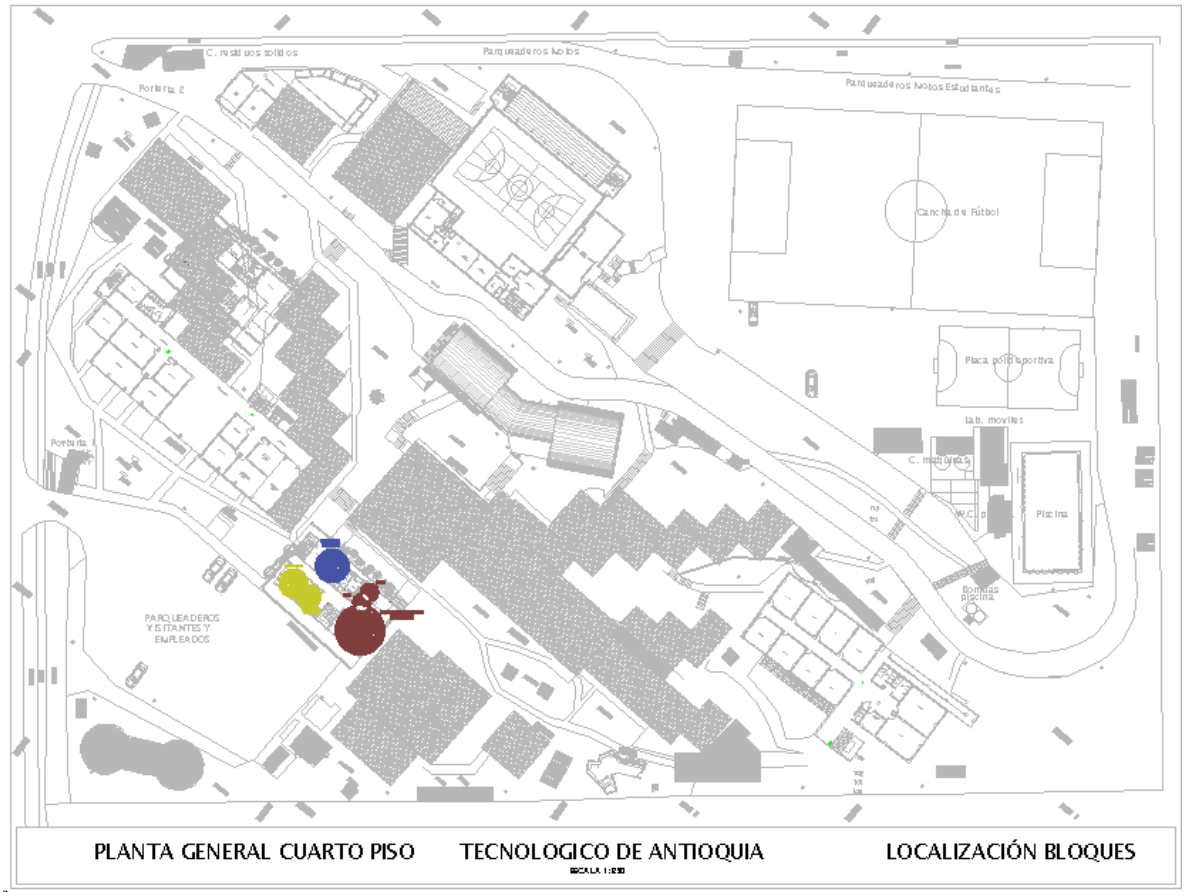
CPU – Comunicación pública
GTH - Gestión del Talento Humano
GTI - Gestión de las TIC



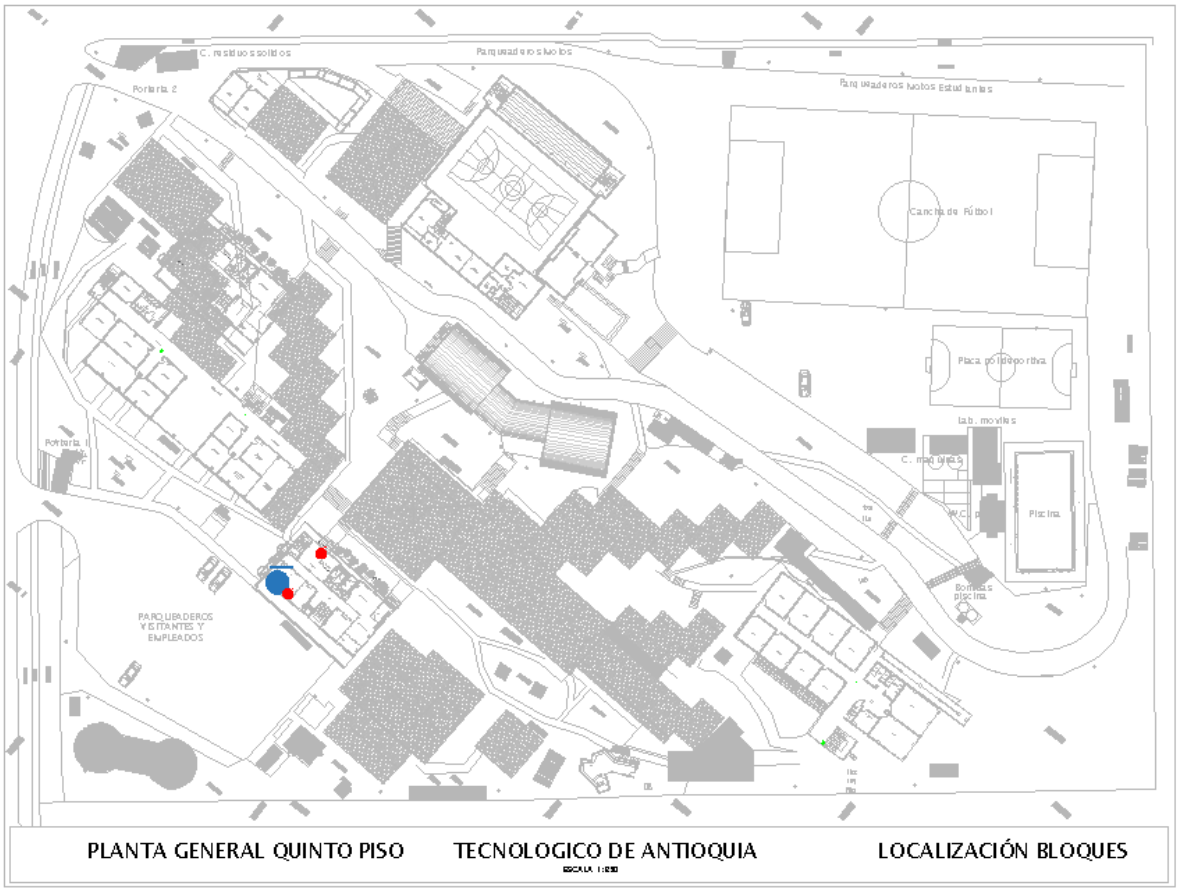
ADM - Admisiones y Registro
GTH - Gestión del Talento Humano
GSS - Gestión de la SST
GTI - Gestión de las TIC



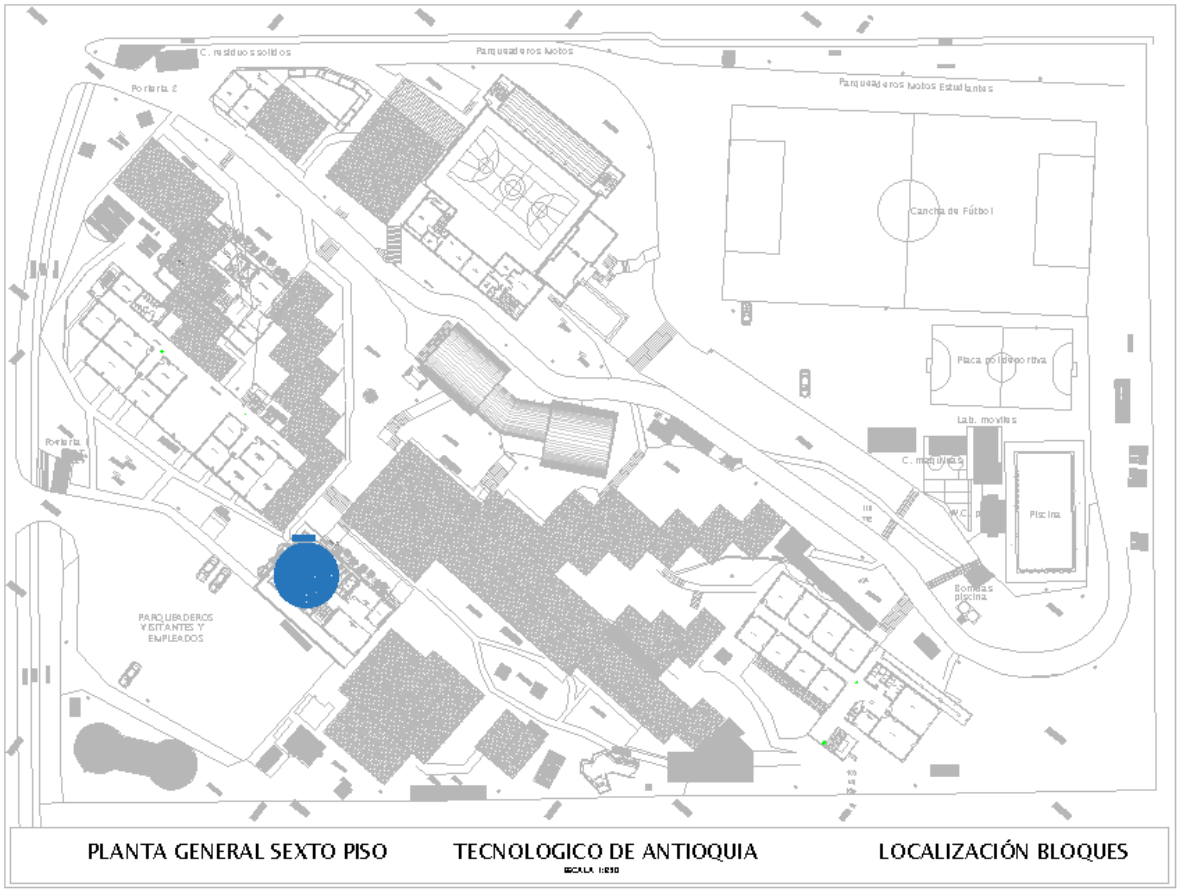
EXT – Extensión
INV – Investigación
DOC – Docencia - Facultad de Ciencias Administrativas y Economicas
DOC – Docencia - Facultad de Derecho
DOC – Docencia - Facultad de Ingenieria
DOC – Docencia - Facultad de Educación



GFI - Gestión Financiera
EXT – Extensión
AMC - Autoevaluación y Mejoramiento Continuo



DIN - Direccionamiento Institucional (PIN - Planeación Institucional)
GTI - Gestión de las TIC



DIN - Direccionamiento Institucional

Nota: El Tecnológico de Antioquia I.U. se encuentra desarrollando una sede en el municipio de Itagüí en el departamento de Antioquia, la cual requiere la integración del personal administrativo que se contemplan en el alcance inicial, es por ello que, a pesar de no contar aún con la planta física elaborada, los espacios físicos de dicho personal administrativo ya se contemplan en el alcance del SGSI.

Los siguientes son los procesos que se encuentran en un rango medio y bajo acorde a la valoración de los procesos la cual obedece a un contraste entre los requisitos de la norma ISO 27001, las disposiciones legales, y el impacto de los diferentes usuarios (Clientes, Directivos, Aliados, e Internos) con los pilares de la seguridad de la información (Integridad, Confidencialidad, Disponibilidad), donde cada uno obtiene un resultado numérico (siendo 1 el de menor impacto y 5 el de mayor impacto), y cuyos puntajes, finalmente se promedian y se obtiene un resultado final de valoración, por tal motivo no serán incluidos en la fase inicial del SGSI.

Rango	Puntaje	Proceso
Medio	3	EIN - Control Interno
	3	GCO - Gestión Contractual
	3	GAD - Gestión de Adquisiciones
	3	GOD - Gestión Documental
	3	GJU - Gestión Jurídica
Bajo	2	BUN - Bienestar Universitario
	2	EGR - Egresados
	2	GIN - Gestión de la Infraestructura Física
	1	GAM - Gestión Ambiental
	1	INT - Internacionalización
	1	PIN - Planeación Institucional
	1	REG - Regionalización
	1	SBB - Servicios de Biblioteca