INSTITUCIÓN UNIVERSITARIA ANTONIO JOSÉ CAMACHO

RESOLUCIÓN No. 055
(enero 27 de 2025)

"Por medio de la cual se aprueba el Plan de seguridad y privacidad de la información 2025"

EL RECTOR

De la Institución Universitaria Antonio José Camacho, en ejercicio de sus atribuciones legales en especial las conferidas en el artículo 69 de la Constitución Nacional, en el artículo 29 de Ley 30 de 1992 y en el artículo 23 del Estatuto General de la INSTITUCION UNIVERSITARIA ANTONIO JOSE CAMACHO y

CONSIDERANDO

Que la Institución Universitaria Antonio José Camacho es un establecimiento público de Educación Superior del Orden Municipal, adscrito al Municipio de Santiago de Cali, creado por el Acuerdo No. 29 del 21 de diciembre de 1993 y modificado por el Acuerdo 0249 del 15 de diciembre de 2008, emitido por el Honorable Concejo Municipal de Santiago de Cali, como una unidad autónoma con régimen especial vinculado al Ministerio de Educación Nacional en lo referente a las políticas y planeación del sector educativo.

Que el artículo 29 literal **g** de la Ley 30 de 1992, reconoce a las Instituciones Universitarias las facultades de arbitrar y aplicar sus recursos para el cumplimiento de su misión social y de su función institucional.

Que los artículos 20 y 23 literales **e,** y **n** del Estatuto General de la INSTITUCION UNIVERSITARIA ANTONIO JOSE CAMACHO, facultan al rector para suscribir los contratos y expedir los actos que sean necesarios para el cumplimiento de los objetivos de la Institución, atendiéndose las disposiciones legales y estatutarias vigentes, y para las demás que le correspondan conforme a las leyes, al Estatuto General y los reglamentos de la Institución, y aquellas que no estén expresamente atribuidas a otra autoridad de la Institución.

Que, es necesario adoptar *Plan de seguridad y privacidad de la información 2025.*

En mérito de lo anterior,

RESUELVE:

Artículo Primero: Aprobar el *Plan de seguridad y privacidad de la información* de la Institución Universitaria Antonio José Camacho, versión 2025, así:

Introducción.

Hoy en día, la información está definida como uno de los activos más valiosos y primordiales para cualquier tipo de organización, la cual, sólo tiene sentido cuando está disponible y es utilizada de forma adecuada, integra, oportuna, responsable y segura, lo que implica, que es necesario que las organizaciones tengan una adecuada gestión de sus recursos y activos de información con el objetivo de asegurar y controlar el debido acceso, tratamiento y uso de la información. El aseguramiento y la protección de la seguridad de la información de las organizaciones y de los datos de carácter personal de los usuarios, representan un reto al momento de pretender garantizar su confidencialidad, integridad, disponibilidad y privacidad, razón por la cual, la

seguridad de la información se ha convertido en uno de los aspectos de mayor preocupación a nivel mundial. Cualquier tipo de organización independiente de su tamaño y naturaleza, debe ser consciente que la diversidad de amenazas existentes que actualmente atentan contra la seguridad y privacidad de la información, representan un riesgo que al materializarse no solo les puede acarrear costos económicos, sanciónales legales, afectación de su imagen y reputación, sino que pueden afectar la continuidad y supervivencia del negocio. Lo anterior, sumando a un entorno tecnológico en donde cada día se hace más complejo de administrar y asegurar, genera que cada vez más la seguridad de la información forme parte de los objetivos y planes estratégicos de las organizaciones. Por lo tanto, es indispensable que los responsables dentro de las organizaciones encargadas de velar por la protección y seguridad de sus recursos, infraestructura e información, constantemente estén adoptando, implementando y mejorando medidas de seguridad orientadas a prevenir y/o detectar los riesgos que pueden llegar a comprometer la disponibilidad, integridad y confidencialidad de los activos de información a través de los cuales se gestiona la información del negocio, independientemente si está es de carácter organizacional o personal, o de tipo pública o privada. En la medida que la organización tenga una visión general de los riesgos que pueden afectar la seguridad y privacidad de la información, podrán establecer controles y medidas efectivas, viables y transversales con el propósito de salvaguardar la disponibilidad, integridad y confidencialidad tanto de la información del negocio como los datos de carácter personal de sus empleados, usuarios y partes interesadas. Es indispensable que las organizaciones realicen una adecuada identificación, clasificación, valoración, gestión y tratamiento de los riegos que pueden afectar su seguridad, con el propósito de implementar medidas y controles efectivos que les permitan estar preparados ante situaciones adversas que puedan comprometer tanto la seguridad física y lógica de sus instalaciones, personas, recursos y sistemas, como la seguridad de su información. Las entidades del sector educación están en la obligación de garantizar la debida seguridad, protección y privacidad de la información de la comunidad Universitaria y personal de los usuarios que residen en sus bases de datos, lo que implica, que deben contar con los más altos estándares y niveles de seguridad con el propósito de asegurar la debida recolección, almacenamiento, respaldo, tratamiento, uso, intercambio y distribución de esta información. Debido a los múltiples riesgos y amenazas que hoy en día atentan contra la seguridad de la información y la protección y privacidad de los datos, es fundamental que las organizaciones establezcan, implementen, mantengan y mejoren continuamente un sistema de gestión de seguridad de la información basado en los riesgos y a su vez, alineado con los objetivos estratégicos y necesidades tanto del negocio como de sus partes interesadas. La oficina de Tic es consciente que la protección y aseguramiento de su información es fundamental para garantizar su debida gestión financiera, administrativa y operativa, razón por la cual debe establecer un marco normativo de Seguridad de la Información que contemple políticas, límites, responsabilidades y obligaciones frente a la seguridad y privacidad de la información de la entidad. El presente documento contiene el plan de seguridad y privacidad de la información para el establecimiento del Sistema de Gestión de Seguridad y Privacidad de la Información de la organización, el cual tomará como referencia el Modelo de Seguridad y Privacidad de la estrategia de Gobierno en Línea y la norma de seguridad, los cuales proporcionan un marco metodológico basado en buenas prácticas para llevar a cabo la implementación de un modelo de Gestión de Seguridad y Privacidad de la Información en cualquier tipo de organización, lo cual, permite garantizar su efectiva implementación y asegurar su debida permanecía y evolución en el tiempo.

RESOLUCIÓN No. 055
(enero 27 de 2025)

"Por medio de la cual se aprueba el Plan de seguridad y privacidad de la información 2025"

Marco de Referencia

Marco Normativo

Un listado de las diferentes leyes que son el punto de partida para la elaboración de planes, guías y documentos organizacionales.

En el contexto del Estado colombiano, las tecnologías de la información y las comunicaciones (TIC) han tomado un papel central en la modernización y digitalización de los servicios públicos. La Ley 1341 de 2009, actualizada por la Ley 1978 de 2019, establece las bases para regular el sector TIC, promoviendo el acceso equitativo a la tecnología y fomentando una sociedad más conectada e informada.

Por otro lado, la política de Gobierno Digital, regida por el Decreto 1008 de 2018, busca transformar las entidades públicas mediante la digitalización de procesos, la transparencia en la gestión y la adopción de herramientas tecnológicas que beneficien tanto a las instituciones como a los ciudadanos. Esta transformación también se apoya en el Decreto 2106 de 2019, que simplifica trámites y fomenta la eficiencia administrativa a través de soluciones tecnológicas.

En cuanto a la seguridad y protección de la información, la Ley 1581 de 2012 se centra en el manejo responsable de los datos personales, mientras que la Ley 1928 de 2018 y el Decreto 338 de 2022 refuerzan los lineamientos de ciberseguridad en las instituciones públicas, protegiendo la información frente a amenazas digitales.

Otro aspecto clave es la interoperabilidad entre las instituciones, promovida por el Conpes 4023 de 2021 y la Ley 2052 de 2020, que buscan facilitar el intercambio seguro de datos entre entidades, mejorando la eficiencia y confiabilidad de los servicios públicos. Adicionalmente, normativas como la Ley 1931 de 2018 integran criterios de sostenibilidad y eficiencia energética en el uso de tecnologías.

En resumen, el marco normativo colombiano refleja un esfuerzo por modernizar el Estado, fortalecer la seguridad digital, garantizar el acceso equitativo a las TIC y construir una administración pública más eficiente y transparente para todos los ciudadanos.

Gobernanza y Digitalización del Estado

- Ley 1341 de 2009 (Modificada por la Ley 1978 de 2019): Regula el sector TIC, promoviendo el acceso equitativo a la tecnología y el fortalecimiento de la sociedad de la información. Impulsa la modernización de las entidades públicas.
- Decreto 1008 de 2018: Establece la política de Gobierno Digital, orientada a mejorar la eficiencia estatal, la transparencia y la apropiación digital.
- Decreto 2106 de 2019: Simplifica trámites y promueve la digitalización de procesos administrativos en el sector público.

Protección de Datos y Ciberseguridad

- Ley 1581 de 2012: Marco general de protección de datos personales, regulando el manejo de información sensible por parte de entidades públicas y privadas.
- Ley 1928 de 2018: Define los lineamientos de ciberseguridad y ciberdefensa en Colombia, aplicable a todas las instituciones del Estado.
- Decreto 338 de 2022: Crea el sistema de gestión de riesgos cibernéticos para proteger la información en las entidades públicas.

Transparencia y Acceso a la Información

- Ley 1712 de 2014 (Ley de Transparencia): Obliga a las entidades públicas a publicar datos abiertos, promoviendo la transparencia y el acceso ciudadano a la información.
- Conpes 4023 de 2021: Fortalece la interoperabilidad y la confianza en el intercambio de datos entre instituciones públicas y privadas.

Comercio Electrónico e Interoperabilidad

- Ley 527 de 1999: Regula el comercio electrónico, las firmas digitales y el uso de mensajes de datos como prueba legal.
- Ley 2052 de 2020: Promueve la interoperabilidad entre entidades del Estado para mejorar la eficiencia administrativa.

Innovación y Modernización

- Ley 1955 de 2019 (Plan Nacional de Desarrollo 2018-2022): Fomenta la modernización digital y tecnológica en las entidades públicas.
- Ley 2039 de 2020: Impulsa la formación en competencias digitales para empleados públicos y ciudadanos, fortaleciendo la adopción tecnológica.

Sostenibilidad

- Ley 1931 de 2018: Promueve la sostenibilidad y la eficiencia energética en la implementación de infraestructuras tecnológicas.

Prioridades para el Estado Colombiano

- Digitalización de trámites: En línea con el Decreto 2106 de 2019.
- Interoperabilidad: Cumplimiento de las directrices de Gobierno Digital y el Conpes 4023.
- Seguridad y protección de datos: Asegurar el manejo responsable de datos personales (Ley 1581 de 2012) y fortalecer sistemas de ciberseguridad (Decreto 338 de 2022).
- Acceso y equidad tecnológica: A través de políticas basadas en la Ley 1341 de 2009 y su actualización.

RESOLUCIÓN No. 055
(enero 27 de 2025)

"Por medio de la cual se aprueba el Plan de seguridad y privacidad de la información 2025"

Contexto Histórico

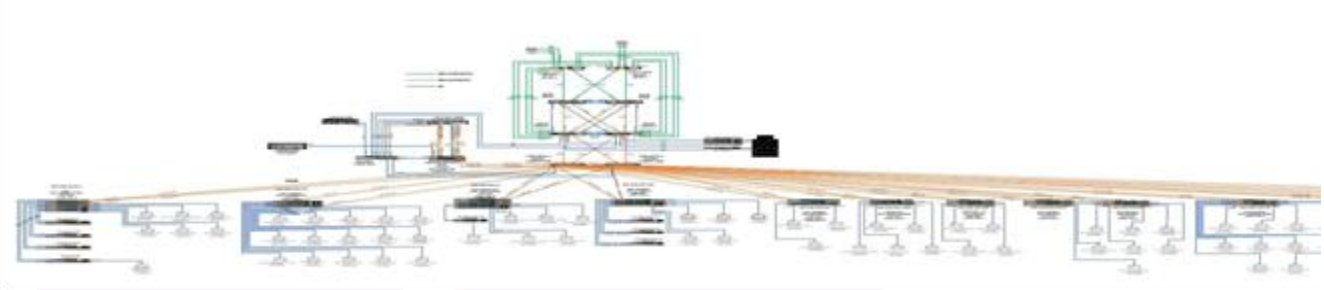
Los recursos informáticos y de telecomunicaciones de la Institución son administrados por la oficina de Tecnologías de Información y Comunicaciones (DTIC) adscrita a la Rectoría de la UNIAJC. Esta oficina contribuye en la gestión de actividades académicas, investigativas y administrativas de la Institución a través del diseño, el desarrollo y la prestación de servicios de informática y telecomunicaciones, alineado con el objetivo estratégico de "modernizar la infraestructura física y tecnológica que garantice el adecuado servicio educativo" y con los objetivos estratégicos por área de desempeño de "infraestructura y equipamiento", y cumplir con los objetivos de las políticas gubernamentales como lo son la política del gobierno digital, las directrices del Conpes (3701, 3854, 2018 incluyendo la directriz 2021, 2022) que incentiva la confianza en el comercio electrónico y la interoperabilidad de datos entre las instituciones.

Caracterización de la infraestructura tecnológica

La institución garantiza a la comunidad universitaria condiciones que favorezcan el acceso permanente a la información, experimentación y práctica docente, necesarios para apoyar los procesos misionales, docencia, investigación y proyección social.
Actualmente, la configuración de los canales de Internet de la Institución cuenta con las siguientes características:

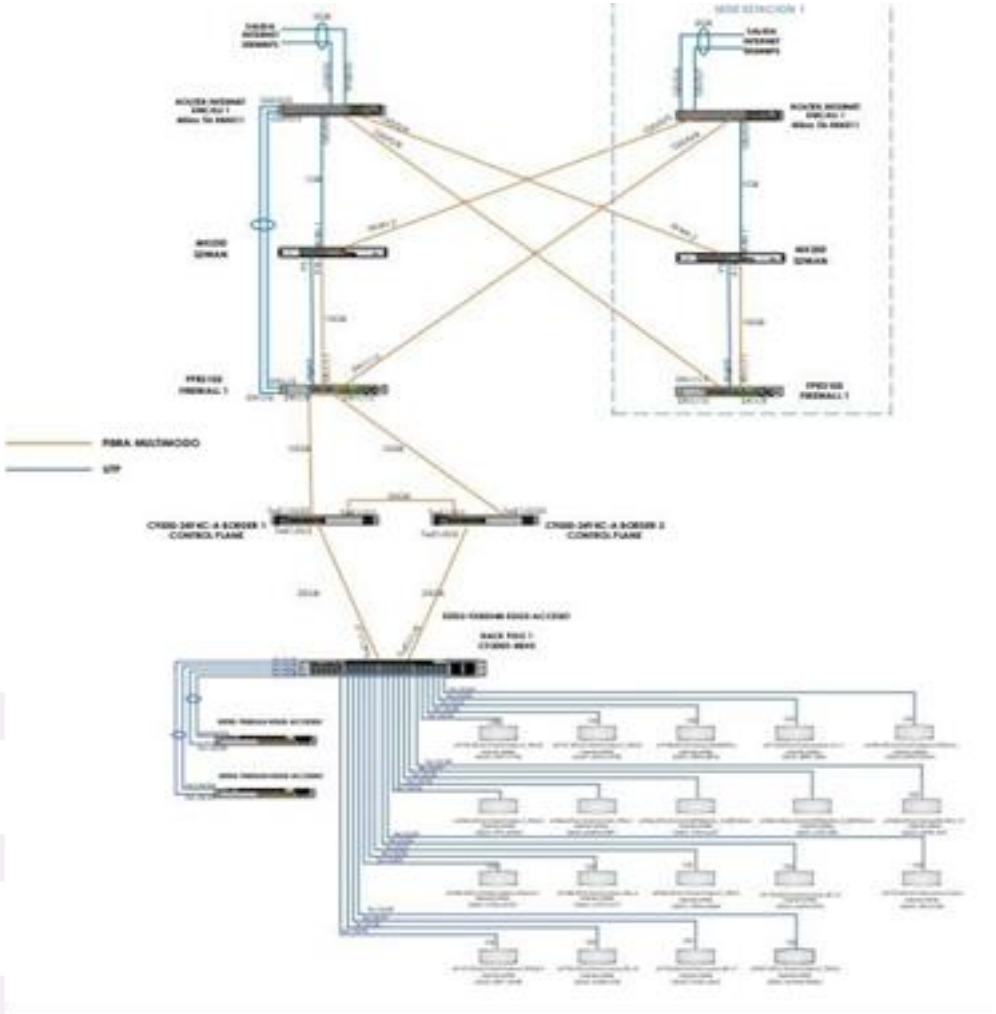
- Edificio principal Norte, Internet dedicado (2048 Megas)
- Edificio principal Norte, Enlace de respaldo redundante (1024 Megas)
- Salida al Nap Colombia 30 Megas
- Edificio Parquesoft (1024) Megas internet dedicado
- Edificios Sur Alameda Canal de datos (150) Megas
- Internet dedicado Casa Proyección Social, (100) Megas
- Conexión al Data Center 30 Megas Canal de datos
- Estación 1 (500) Megas
- Sede Yumbo (1000) Megas

Aquí observamos un diagrama de red donde un núcleo central compuesto por switches gestiona las conexiones hacia diferentes áreas de la infraestructura. Las líneas de colores representan rutas específicas (datos, administración, etc.), y las conexiones se distribuyen hacia servidores, switches de acceso y estaciones de trabajo. El diseño parece enfocado en centralizar y segmentar servicios para garantizar una comunicación eficiente en toda la red



Topología Física y lógica estación 1

Observamos el diagrama de red con un núcleo central compuesto por switches interconectados mediante fibra multimodo y enlaces UTP. Desde este núcleo, las conexiones se distribuyen hacia switches de acceso y, posteriormente, a estaciones de trabajo organizadas en una red segmentada. Este diseño parece optimizado para garantizar redundancia en el núcleo y una distribución eficiente hacia los dispositivos finales.

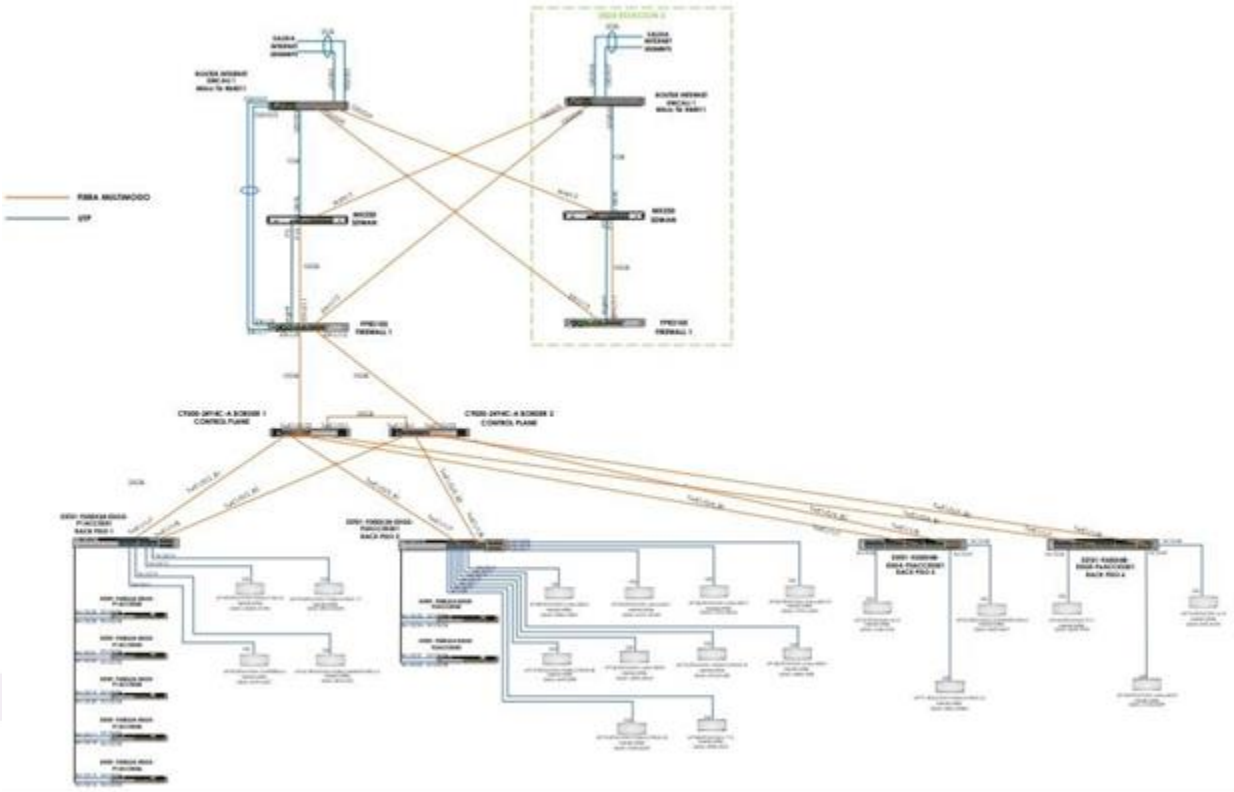


Topología física estación 3

Aquí observamos el diagrama de red con un núcleo central compuesto por switches conectados mediante enlaces de fibra multimodo y UTP. Este núcleo distribuye las conexiones hacia múltiples switches de acceso, organizados en diferentes áreas. Desde estos switches, se conectan estaciones de trabajo y otros dispositivos finales. El diseño muestra redundancia en el núcleo y una segmentación eficiente para garantizar estabilidad y buen rendimiento en la red.

RESOLUCIÓN No. 055
(enero 27 de 2025)

"Por medio de la cual se aprueba el Plan de seguridad y privacidad de la información 2025"

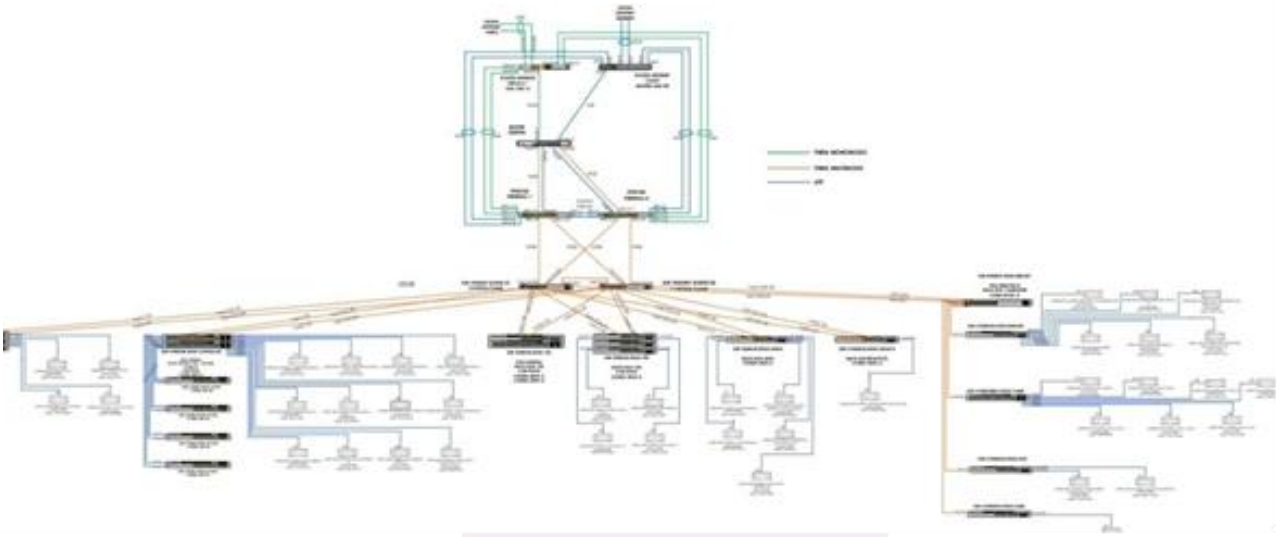


Topología Física sede sur

El diagrama de red representa una estructura jerárquica en la que el núcleo central está compuesto por switches interconectados mediante enlaces de fibra multimodo y cables UTP. Este núcleo actúa como el corazón del sistema, gestionando el tráfico de datos y distribuyendo las conexiones hacia los switches de acceso ubicados en distintas áreas de la red. Los switches de acceso, a su vez, facilitan la conexión de estaciones de trabajo y dispositivos finales. El diseño implementa redundancia en el núcleo para asegurar alta disponibilidad y segmenta las áreas de manera estratégica, optimizando el rendimiento y la confiabilidad de la red.

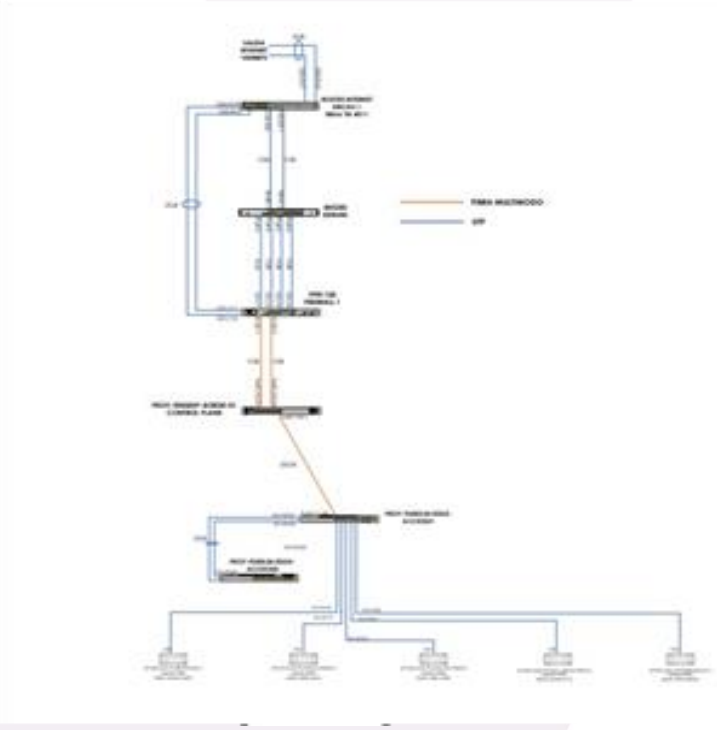
RESOLUCIÓN No. 055
(enero 27 de 2025)

"Por medio de la cual se aprueba el Plan de seguridad y privacidad de la información 2025"



Topología Física sede proyección UNIAJC

En estos switches observamos que se proporciona la conectividad directa a estaciones de trabajo y dispositivos finales. La redundancia en el núcleo garantiza continuidad operativa frente a fallos, mientras que la segmentación eficiente optimiza el manejo del tráfico y asegura un desempeño estable en toda la red.



RESOLUCIÓN No. 055
(enero 27 de 2025)

"Por medio de la cual se aprueba el Plan de seguridad y privacidad de la información 2025"

Objetivos

Objetivo General.

Establecer un Plan de Seguridad y Privacidad de la Información que apoye el establecimiento del Sistema de Gestión de Seguridad y Privacidad de la Información de UNIAJC, acorde a los requerimientos del modelo de seguridad de la estrategia de gobierno en línea, los requerimientos del negocio y en cumplimiento de las disposiciones legales vigentes.

Objetivos Específicos

- Definir las etapas para establecer la estrategia de seguridad de la información de la entidad.
- Apalancar la implementación del Sistema de Gestión de Seguridad de la Información de la entidad de acuerdo con los requerimientos establecidos en el modelo de seguridad de la estrategia de Gobierno en Línea.
- Establecer lineamientos para la implementación y/o adopción de mejores prácticas de seguridad en la entidad.
- Optimizar la gestión de la seguridad de la información al interior de la entidad.

Políticas actuales de seguridad de la información

Propósito: Proteger la información estratégica de la Institución y formar sus niveles de acceso y confidencialidad.

Exposición de la política

- Los dueños de la información nominados por autoridad competente deben ser funcionarios que estén completamente familiarizados con el segmento de información que les corresponde, así como con todos los procesos que interactúan con esta información.
- Los dueños de la información serán los responsables de verificar que existan procedimientos y procesos de seguridad para asegurar el manejo y la integridad de la información que reside en medios magnéticos o en documentos.
- El uso de los recursos lógicos de la institución deberá ser destinados para uso exclusivo de la UNIAJC.
- Toda información que viaje en un ambiente público deberá ser previamente encriptada.
- Los permisos de acceso a todos los sistemas de información, sean estos aplicativos del ERP y/o tendrán un tiempo de expiración de tres meses como mínimo y máximo cuatro meses.
- Se debe aplicar estándares y buenas prácticas de seguridad sobre el manejo de un modelo seguro de datos.
- Toda alta o baja del archivo maestro de personal debe ser oportuna y adecuadamente informado para una correcta administración de las claves de acceso.
- La entrega y/o acceso a la información de la institución, así como el acceso a su infraestructura tecnológica por parte de terceros se realizará en base a la suscripción de convenios de confidencialidad o a la existencia de cláusulas de confidencialidad en los contratos u órdenes de trabajo respectivos.
- Todos los funcionarios que manejan información sensible de la compañía deberán firmar un acuerdo de confidencialidad.

- Será responsabilidad de la Oficina de tecnologías de la información, mantener vigente y actualizado el licenciamiento de software para la institución, tal como antivirus, licencias de firewall, destinados a proteger las instalaciones y activos informáticos de la Institución, así como también procurar una operación sin sobre cargas en la red de datos.

Políticas de manejo de cuentas de correo y uso de la red

Propósito: Para el manejo del uso de red se ha establecido las siguientes políticas:

- La instalación de puntos de red LAN Y WAN se realizará con contratación externa y/o personal directo de la Institución Universitaria Antonio José Camacho.
- La Oficina de tecnologías de la información y Comunicaciones, tendrá la responsabilidad de llevar un control de inventario de los puntos de red instalados en todos los edificios y oficinas de la Institución. Esto incluye la certificación, rotulación de los mismos de acuerdo al estándar previamente establecido, y el uso de un sistema informático de control de este inventario.
- Todas las unidades de la institución que tengan necesidad de instalar puntos de red deberán canalizar y sustentar sus requerimientos ante su correspondiente responsable de área. Encontrar justificada la necesidad, cada responsable deberá hacer llegar a DTIC para ser atendidos.

Para el manejo del correo electrónico y el internet, la UNIAJC ha establecido las siguientes políticas:

- Para la utilización de los diferentes servicios de red a través de las cuentas creadas, se deben acatar las normas obligatorias, cuyo incumplimiento acarreará sanciones de acuerdo con el reglamento interno de trabajo, según sea el caso.
- La cuenta electrónica es personal e intransferible. El usuario es el único y directo responsable de todas las acciones y mensajes que se lleven a cabo en su nombre. La Institución Universitaria Antonio José Camacho no se hace responsable por lo que se haga o diga en nombre de una cuenta particular, y, por lo tanto, está prohibido el uso de cuentas por personas ajenas a su titular.
- La UNIAJC podrá suspender o cancelar cuentas por mal manejo, sin perjuicios de imponer las sanciones correspondientes, según la gravedad de la falla.

Se consideran como conductas de mal manejo de las cuentas personales: Usos inaceptables tales como:

- Exceder los servicios para la cual se creó la cuenta.
- Intentar apoderarse de claves de acceso de otros usuarios acceder y/o modificar archivos de otro usuario y en especial los pertenecientes a la UNIAJC.
- Enviar mensajes para la difusión de mensajes o correos electrónicos sin identificar plenamente a su autor o enviar anónimos.
- Usar los servicios de red para propósitos no investigativos o usuarios para propósitos fraudulentos, comerciales o publicitarios o para propagación de mensajes destructivos u obscenos.
- Difundir cadena de mensajes.
- Perturbar el trabajo de los demás enviando mensajes que pueden interferir con su trabajo.
- Violar o intentar violar los sistemas de seguridad de la red y servidores académicos y administrativos a los cuales se tenga acceso de manera local o externamente.

- Violar los derechos de privacidad de terceras partes.
- Violación de los derechos de propiedad intelectual de terceras partes.
- Usar la red para propósitos recreativos.
- Violar las reglas y restricciones impuestas por el administrador de red y la política de seguridad de la información de cualquier equipo que tenga una conexión a la red.
- No hacer uso racional del ancho de banda, espacio en disco, memoria, disco duro y unidades de almacenamiento.
- No salirse de una cuenta ajena cuando por circunstancia accidental se conecte a una.

Se consideran como conductas de buen manejo de las cuentas personales: Usos aceptables:

- Uso para propósitos educativos y de investigación.
- Uso para propósitos de administración de la infraestructura educativa y para investigación.
- Uso para acceso a bibliotecas.
- Uso para desarrollar proyectos de instituciones educativas o de un sector privado de proyectos de investigación.

Custodia y tenencia de activos informáticos.

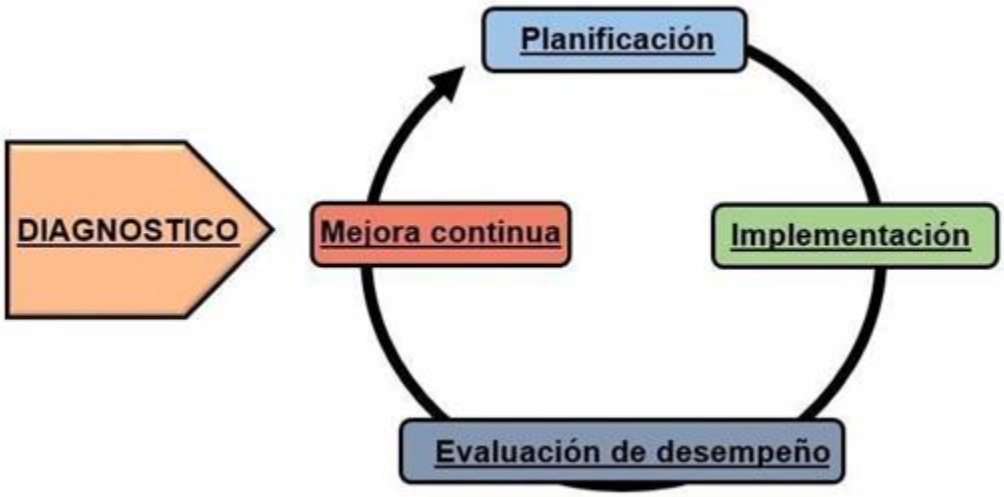
- Los activos informáticos corporativos y centralizados serán custodiados por DTIC En caso de que se requiere equipo especializado, estos serán custodiados por el área donde se encuentre la operación.
- Los activos informáticos de usuarios finales (Mouse, Teclado y Diademas, sonido), serán custodiados por el responsable de su operación.
- Los custodios deberán ser funcionarios nombrados por la institución, a quienes se asignan los activos informáticos y son responsables pecuniariamente de su buen uso e integridad. Los usuarios son quienes utilizan para su labor diaria o eventual el activo informático y pueden ser empleados regulares de la institución o no (empleados de outsourcing, contratistas externos, consultores, entre otros).
- Cuando el usuario es un empleado regular de la institución, es a su vez un custodio. Cuando el usuario no es un empleado regular, el equipo debe estar a cargo de un funcionario nombrado de la Institución.
- La asignación de equipos de cómputo se realiza por la DTIC a los funcionarios custodios, después de la solicitud del jefe de área, una vez asignado el recurso a un funcionario este no puede asignarse a ningún otro empleado.

Metodología e implementación del modelo de seguridad

Ciclo Operación.

El Modelo de Seguridad y Privacidad de la Información de la Estrategia de Gobierno en Línea contempla el siguiente ciclo de operación que contempla cinco (5) fases, las cuales permiten que las entidades puedan gestionar adecuadamente la seguridad y privacidad de sus activos de información.

Grafica 1. Ciclo operación



Fuente: (MinTIC, s.f.)

- Fase Diagnostico: Permite identificar el estado actual de la entidad con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información.
- Fase Planificación (Planear): En esta fase se establecen los objetivos a alcanzar y las actividades del proceso susceptibles de mejora, así como los indicadores de medición para controlar y cuantificar los objetivos.
- Fase Implementación (Hacer): En esta fase se ejecuta el plan establecido que consiste en implementar las acciones para lograr mejoras planteadas.
- Fase Evaluación de desempeño (Verificar): Una vez implantada la mejora, se establece un periodo de prueba para verificar el correcto funcionamiento de las acciones implementadas.
- Fase Mejora Continua (Actuar): Se analizan los resultados de las acciones implementadas y si estas no se cumplen los objetivos definidos se analizan las causas de las desviaciones y se generan los respectivos planes de acciones.

Alineación norma de seguridad vs ciclo de operación.

Aunque en la norma de seguridad no se determina un modelo de mejora continua (PHVA) como requisito para estructurar los procesos del Sistema de Gestión de Seguridad de la Información, la nueva estructura de esta versión se puede alinear con el ciclo de mejora continua de las modelos de gestión de la siguiente forma:

Grafica 2. Norma de seguridad alineado al Ciclo de mejora continua.

El siguiente cuadro muestra la relación entre las fases del ciclo de operación del Modelo de Seguridad y Privacidad de la Información (Diagnostico, Planificación, Implementación, Evaluación, Mejora Continua) y la estructura de capítulos y numerales de la norma de seguridad:

Tabla 1. Fases Ciclo Operación vs Estructura norma de seguridad

FASES	CAPITULO Norma de seguridad	CUMPLIMIENTO												
		2021	2022											
			01	02	03	04	05	06	07	08	09	10	11	12
Diagnostico	Contexto de la organización	50%	5%	5%	5%	5%	5%	5%	5%	5%	10%			

Fuente: (Gutiérrez, 2013)

Fase DIAGNÓSTICO en la norma de seguridad.

En el capítulo 4 - Contexto de la organización de la norma de seguridad, se determina la necesidad de realizar un análisis de las cuestiones externas e internas de la organización y de su contexto, con el propósito de incluir la necesidad, es y expectativas de las partes interesas de la organización en el alcance del SGSI.

- **Fase PLANEACIÓN en la norma de seguridad.**

En el capítulo 5 - Liderazgo, se establece las responsabilidades y compromisos de la Alta Dirección respecto al Sistema de Gestión de Seguridad de la Información y entre otros aspectos, la necesidad de que la Alta Dirección establezca una política de seguridad de la información adecuada al propósito de la organización asegure la asignación de los recursos para el SGSI y que las responsabilidades y roles pertinentes a la seguridad de la información se asignen y comuniquen. En el capítulo 6 - Planeación, se establece los requerimientos para la valoración y tratamiento de riesgos de seguridad y para la definición de objetivos viables de seguridad de la información y planes específicos para su cumplimiento.

En el capítulo 7 - Soporte se establece que la organización debe asegurar los recursos necesarios para el establecimiento, implementación y mejora continua Sistema de Gestión de Seguridad de la Información.

- **Fase IMPLEMENTACION en la norma de seguridad.**

En el capítulo 8 - Operación de la norma de seguridad, se indica que la organización debe planificar, implementar y controlar los procesos necesarios para cumplir los objetivos y requisitos de seguridad y llevar a cabo la valoración y tratamiento de los riesgos de la seguridad de la información.

- **Fase EVALUACION DEL DESEMPEÑO en la norma de seguridad.**

En el capítulo 9 - Evaluación del desempeño, se define los requerimientos para evaluar periódicamente el desempeño de la seguridad de la información y eficacia del sistema de gestión de seguridad de la información.

- **Fase MEJORA CONTINUA en la norma de seguridad.**

En el capítulo 10 - Mejora, se establece para el proceso de mejora del Sistema de Gestión de Seguridad de la Información, que a partir de las no-conformidades que ocurran, las organizaciones deben establecer las acciones más efectiva para solucionarlas y evaluar la necesidad de acciones para eliminar las causas de la no conformidad con el objetivo de que no se repitan.

Fases del ciclo operativo.

Fase I: diagnostico.

Identificar el estado de la Entidad con respecto a los requerimientos del SGSI.

Tabla 2. Metas VS Actividades, Instrumentos y Resultados.

Metas	Actividades \ Instrumentos \ Resultados	2021	CUMPLIMIENTO 2023												META
			01	02	03	04	05	06	07	08	09	10	11	12	
Perfilar la gestión de seguridad y privacidad de la información al interior de la Entidad, a la luz de la norma de seguridad	Recibir la asesoría de implementación de la norma de seguridad	50%													50%
Identificar el nivel de madurez de seguridad y privacidad de la información en la Entidad.	Valoración del nivel de madurez de la entidad frente a la seguridad de la información a la luz de la norma de seguridad.	50%													50%
	Valoración del nivel de madurez de la privacidad de la información en la entidad a la luz de la norma de seguridad.	50%													50%
Identificar vulnerabilidades técnicas y administrativas que sirvan como insumo para la fase de planificación.	Actualización con nuevas herramientas para la mitigación de vulnerabilidades.	50%													50%

Fuente: (Gutiérrez, 2013)

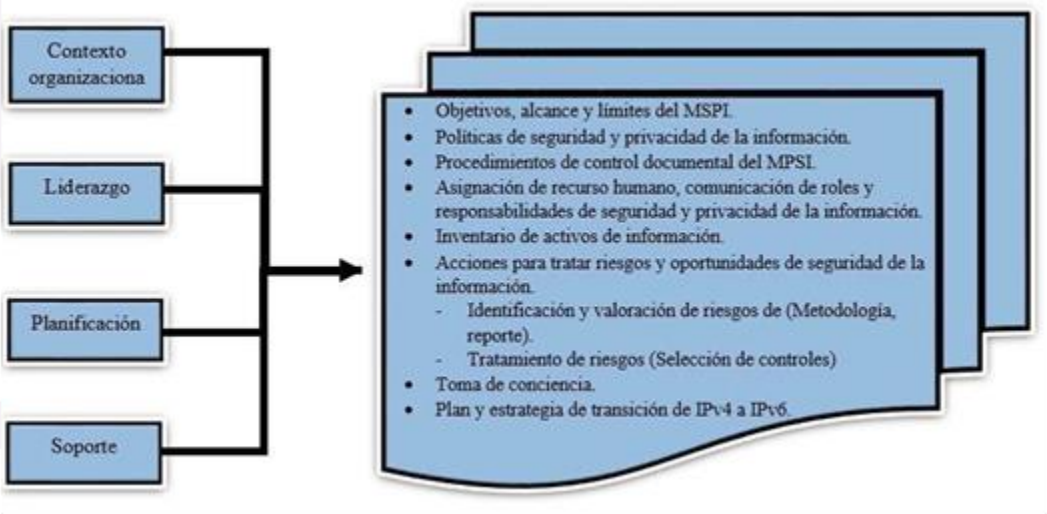
Para la recolección de la información, en esta fase se utilizarán mecanismo como:

- Diligenciamiento de cuestionarios con el objetivo de determinar el nivel de cumplimiento de la entidad con relación a los dominios de la norma de seguridad.
- Documentación existente en el sistema de calidad de la entidad relacionada con la información de las partes interesadas de la entidad y los roles y funciones asociados a la seguridad de la información.
- Fuentes externas, como las guías de autoevaluación, encuesta y estratificación dispuestas por la estrategia de gobierno en línea Ministerio de Tecnologías de la Información y las Comunicaciones.

Fase II: planificación.

Definir la estrategia metodológica, que permita establecer el alcance, objetivos, procesos y procedimientos, pertinentes a la mejora de seguridad de la información, en procura de los resultados.

Grafica 3. Planificación modelo de seguridad.



Fuente: (MinTIC)

Tabla 3. Metas VS Actividades, Instrumentos y Resultados

Metas	Actividades \ Instrumentos \ Resultados	CUMPLIMIENTO													
		2021	2022												
			01	02	03	04	05	06	07	08	09	10	11	12	
Realizar un análisis de Contexto y factores externos e internos de la Entidad en torno a la seguridad de la información junto con el asesor norma de seguridad.	Realizar un Análisis de Contexto de la entidad entorno a la seguridad	80%													85%
Definir Roles, Responsables y Funciones de seguridad y privacidad de la información	Adicionar las funciones de seguridad de la información al personal de la oficina de Tic.	80%													95%

con las modificaciones y nuevos activos de información.	Establecer nuevos Roles de Seguridad de la información a la luz de los nuevos cambios que traen los nuevos activos de información.	80%													80%
Elaborar los procedimientos, manuales de seguridad y privacidad de la información de la entidad.	Elaborar nuevos procedimientos generales para la seguridad, privacidad y buenas prácticas de la información al interior de la Entidad.	80%													80%
Identificar y valorar activos de información.	Realizar una actualización y valoración de los activos de información de la entidad de acuerdo con su	100%													100%
	nivel de criticidad de acuerdo con el alcance del SGSI.														
Establecer capacitaciones, y sensibilización de seguridad de la información.	Dictar mínimo dos capacitaciones al año, sobre sensibilización en el ámbito de seguridad de la información.	50%													50%

Fuente: (Gutiérrez, 2013)

Fase III: implementación.

Llevar a cabo la implementación de la fase de planificación del SGSI, teniendo en cuenta para esto los aspectos más relevantes en los de implementación del Sistema de Gestión de Seguridad.

Grafica 4. Fase de implementación modelo de seguridad.

Tabla 4. Metas VS Actividades, Instrumentos y Resultados.

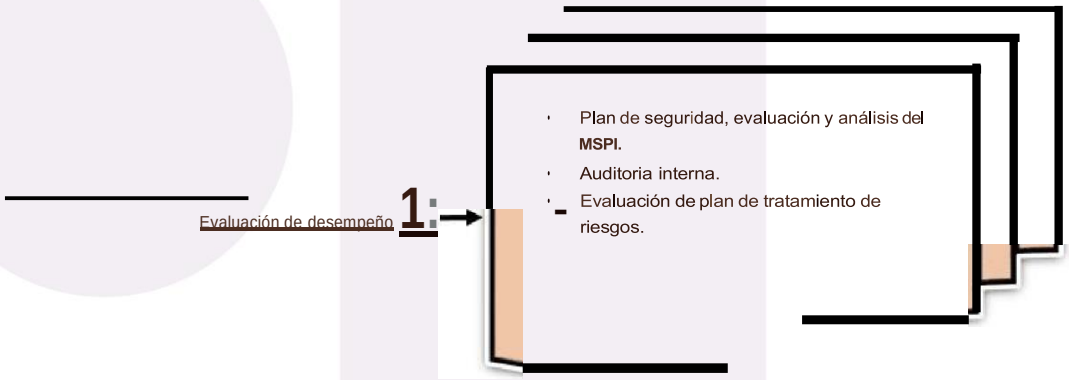
Metas	Actividades \ Instrumentos \ Resultados	2021	CUMPLIMIENTO 2022												META
			01	02	03	04	05	06	07	08	09	10	11	12	
Establecer controles a la seguridad de la información y los riesgos.	Realizar análisis exhaustivos con equipos de seguridad perimetral	100%													100%
Ejecutar pruebas anuales de vulnerabilidades e intrusión.	Ejecutar pruebas de vulnerabilidad e intrusión con el objetivo de identificar el nivel de protección de los activos de información de la entidad.	80%													80%

Fuente: (Gutiérrez, 2013)

1Fase IV: evaluación de desempeño.

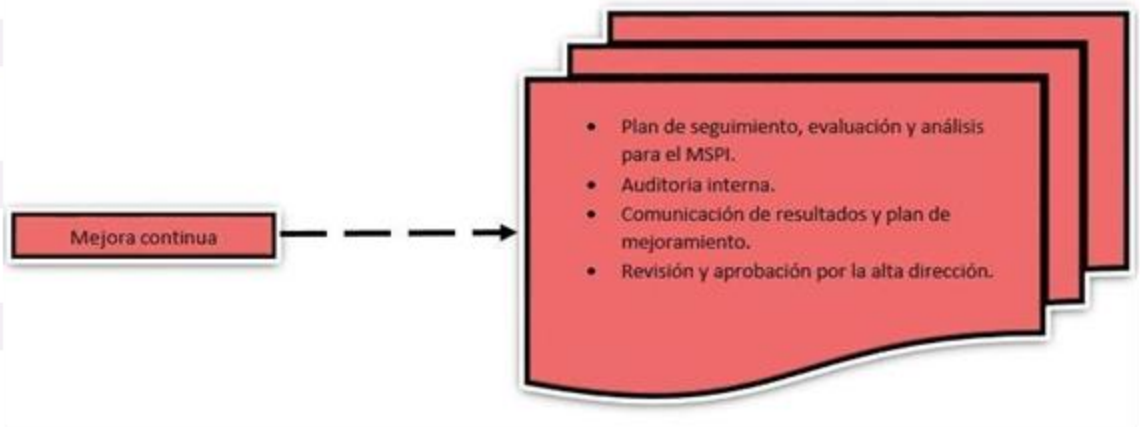
Fase IV: evaluación de desempeño.
Evaluar el desempeño y la eficacia del SGSI, a través de instrumentos.

Grafica 5. Fase Evaluación Desempeño modelo de seguridad.



Fase V: mejora continua.
Consolidar los resultados obtenidos del componente de evaluación de desempeño, para diseñar el plan de mejoramiento y privacidad de la información, que permita realizar el plan.

Grafica 6. Fase Mejora Continua modelo de seguridad.



Fuente: (MinTIC)

Tabla 6. Metas VS Actividades, Instrumentos y Resultados.

METAS	ACTIVIDADES \ INSTRUMENTOS \ RESULTADOS	CUMPLIMIENTO												META
		2023	2023											
			01	02	03	04	05	06	07	08	09	10	11	12	
Diseñar	Aplicar acciones													

plan de mejoramiento.	correctivas que permitan mejorar la seguridad perimetral de equipos, servidores y dispositivos.	90%													90%

Fuente: (Gutiérrez, 2013)

Mapa de Riesgos.

Una gran variedad de riesgos amenaza la infraestructura de tecnología de la información en la organización, por esta razón los riesgos de seguridad se clasifican en tres grandes tipos con diferentes consecuencias y probabilidades agrupados en la siguiente tabla:

Tabla 7. Tipo de riesgos.

TIPO DE RIESGO	DESCRIPCION
R. Estratégico	Este tipo de riesgo obedece a todo lo que la organización no puede controlar. Ej. Desastres naturales, redes eléctricas externas, asonadas.
R. Corrupción	Este tipo de riesgo está asociado con el indebido con personas dentro de la organización.
R. Digital	todas aquellas amenazas que afectan el buen funcionamiento de las tecnologías de información que soportan las actividades académico administrativos

Tabla 8. Mapa de riesgo.

MAPA DE RIESGOS						V - 3.0 - 2015 DIR-F-7
MEDIDAS DE MITIGACIÓN			ANÁLISIS			
TIPO DE RIESGO	AMENAZAS	CONSECUENCIA	PROBABILIDAD	CONTROLES	IMPACTO	ZONA RIESGO RESIDUAL
R. Seguridad Digital	Evadir los dispositivos y controles que cuidan la seguridad perimetral.	Perdida de la continuidad de negocio.	4	Generación periódica de los informes pertenecientes a los equipos y sistemas de seguridad perimetral.	1	Moderada
R. Seguridad Digital	Saltar controles de usuarios, roles, permisos, perfiles, restricciones y contraseñas.	Falla en el control de acceso a activos de información.	2	Generación periódica de los informes pertenecientes a los equipos y sistemas de seguridad perimetral.	3	Moderada
R. Estratégico	Sobrepasar la capacidad contingencia.	Atención parcial de los servicios de tecnología.	3	Actualización de contratos de tecnologías con diferentes proveedores tecnológicos.	3	Alta
R. Corrupción	Falta de normas, manuales y procedimientos.	Asumir el Riesgo	2	Capacitación y charlas permanentes al personal interno de la oficina.	2	Baja

R. Corrupción	Falta de normas, manuales y procedimientos .	Asumir el Riesgo	1	Actualización permanente en documentos del sistema de calidad institucional.	2	Baja
R. Corrupción	- Procedimientos formales aplicados - Dispositivos de seguridad física y electrónica.	Perdida o daños a la infraestructura tecnológica	5	Gestión periódica de los inventarios y activos.	4	Extrema

Seguimiento al Plan de Seguridad.

La tabla número 9 describe cada una de las actividades que soportan el plan de seguridad de la información, además se describe el presupuesto promediado mensual.
Tabla 9. Fuente de elaboración propia, matriz de seguimiento**.**

Tabla. Cronograma de Ejecución 2025

RESOLUCIÓN No. 055
(enero 27 de 2025)

"Por medio de la cual se aprueba el Plan de seguridad y privacidad de la información 2025"

Proyectos	DESCRIPCIÓN	01	02	03	04	05	06	07	08	09	10	11	12	Objetivo	Meta	%
Fortalecimiento de la Seguridad Perimetral	Gestión y actualización de los sistemas de seguridad perimetral para proteger la infraestructura tecnológica frente a posibles amenazas externas.	12.5 %											95 %	Proteger infraestructura digital.	95%	95%
Implementación de Sistemas de Prevención de Riesgos	Implementación de sistemas avanzados de detección y prevención para minimizar riesgos y responder a posibles-incidentes de seguridad.	12.5 %											95 %	Minimizar riesgos de vulnerabilidad.	95%	95%
Análisis y Mitigación de Vulnerabilidades Digitales	Realización de análisis periódicos de vulnerabilidades y generación de reportes para identificar y mitigar riesgos en el entorno digital.	12.5 %											95 %	Asegurar un entorno digital protegido.	95%	95%
Optimización del Rendimiento de Servidores	Administración y optimización de servidores en el centro de datos, garantizando un procesamiento eficiente de la información.	12.5 %											95 %	Optimizar recursos de procesamiento .	95%	95%
Configuración de Equipos de Seguridad Perimetral	Configuración de siete equipos especializados en seguridad perimetral para reforzar la protección de redes institucionales.	12.5 %											100 %	Proteger redes contra intrusiones.	100%	100%

RESOLUCIÓN No. 055
(enero 27 de 2025)

"Por medio de la cual se aprueba el Plan de seguridad y privacidad de la información 2025"

Términos y Referencias.

- Activo de información: aquello que es de alta validez y que contiene información vital de la empresa que debe ser protegida.
- Amenaza: Es la causa potencial de un daño a un activo de información.
- Anexo SL: Nuevo esquema definido por International Organización de estándares – norma de seguridad, para todos los Sistemas de Gestión acorde al nuevo formato llamado "Anexo SL", que proporciona una estructura uniforme como el marco de un sistema de gestión genérico.
- Análisis de riesgos: Utilización sistemática de la información disponible, para identificar peligros y estimar los riesgos.
- Causa: Razón por la cual el riesgo sucede.
- Ciclo de Deming: Modelo mejora continua para la implementación de un sistema de mejora continua.
- Colaborador: Es toda persona que realiza actividades directa o indirectamente en las instalaciones de la entidad, Trabajadores de Planta, Trabajadores Temporales, Contratistas, Proveedores y Practicantes.
- Confidencialidad: Propiedad que determina que la información no esté disponible a personas no autorizados.
- Controles: Son aquellos mecanismos utilizados para monitorear y controlar acciones que son consideradas sospechosas y que pueden afectar de alguna manera los activos de información.
- Disponibilidad: Propiedad se determina que la información sea accesible y utilizable por aquellas personas debidamente autorizadas.
- Dueño del riesgo sobre el activo: Persona responsable de gestionar el riesgo.
- Impacto: Consecuencias de que la amenaza ocurra. Nivel de afectación en el activo de información que se genera al existir el riesgo.
- Incidente de seguridad de la información: Evento no deseado o inesperado, que tiene una probabilidad de amenazar la seguridad de la información.
- Integridad: Propiedad de salvaguardar la exactitud y estado completo de los activos.
- Oficial de Seguridad: Persona encargada de administrar, implementar, actualizar y monitorear el Sistema de Gestión de Seguridad de la Información.
- Probabilidad de ocurrencia: Posibilidad de que se presente una situación o evento específico.
- Responsables del Activo: Personas responsables del activo de información.
- Riesgo: Grado de exposición de un activo que permite la materialización de una amenaza.
- Riesgo Inherente: Nivel de incertidumbre propio de cada actividad, sin la ejecución de ningún control.
- Riesgo Residual: Nivel de riesgo remanente como resultado de la aplicación de medidas de seguridad sobre el activo.
- PSE: Proveedor de Servicios Electrónicos, es un sistema centralizado por medio del cual las empresas brindan a los usuarios la posibilidad de hacer sus pagos por Internet.
- SARC: Siglas del Sistema de Administración de Riesgo Crediticio.
- SARL: Siglas del Sistema de Administración de Riesgo de Liquidez**.**
- SARLAFT: Siglas del Sistema de Administración del Riesgo de Lavado de Activos y Financiación del Terrorismo.
- SARO: Siglas del Sistema de Administración de Riesgos Operativos.

RESOLUCIÓN No. 055
(enero 27 de 2025)

"Por medio de la cual se aprueba el Plan de seguridad y privacidad de la información 2025"

- Seguridad de la Información: Preservación de la confidencialidad, la integridad y la disponibilidad de la información (norma de seguridad).
- SGSI: Siglas del Sistema de Gestión de Seguridad de la Información.
- Sistema de Gestión de Seguridad de la información SGSI: permite establecer, implementar, mantener y mejorar continuamente la gestión de la seguridad de la información de acuerdo con los requisitos de la norma de seguridad.
- Vulnerabilidad: Debilidad de un activo o grupo de activos de información que puede ser aprovechada por una amenaza. La vulnerabilidad se caracteriza por ausencia en controles de seguridad que permite ser explotada.

Artículo Segundo: Establecer como corresponde, la responsabilidad por la implementación y ejecución de este plan, a la Dependencia de Tecnologías de la Información.

Artículo Tercero: Publicar el siguiente plan en la página institucional.

COMUNÍQUESE, PUBLÍQUESE Y CÚMPLASE

Dada en Santiago de Cali a los veintisiete (27) días de enero de dos mil veinticinco (2025).

HUGO ALBERTO GONZÁLEZ LÓPEZ
Rector

LUIS GUILLERMO BETANCOURT MARADIAGA
Secretario General

Vo.Bo. LUIS GUILLERMO BETANCOURT M.