UNIVERSIDAD FUCS

MANUAL DE SEGURIDAD DE LA INFORMACIÓN

Tabla de contenido

UNIVERSIDAD FUCS

MANUAL DE SEGURIDAD DE LA INFORMACIÓN

I. INTRODUCCIÓN

La evolución de las tecnologías de la información y la implementación de herramientas, productos, software y servicios destinados a apoyar los procesos misionales y administrativos de la Universidad FUCS generan nuevas necesidades y riesgos relacionados con la protección de la información.

En este contexto, el presente Manual establece los lineamientos y controles aplicables a los sistemas, redes, dispositivos, aplicaciones, servicios y demás activos de información utilizados por la Universidad FUCS, con el propósito de preservar su confidencialidad, integridad y disponibilidad, proteger los datos personales y asegurar el cumplimiento de los requisitos legales, regulatorios e institucionales aplicables.

II. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

De conformidad con el Documento de Políticas Institucionales de la Universidad FUCS aprobado por el Consejo Superior, se estableció como política general en materia de seguridad de la información la siguiente:

1. Declaración.

La Universidad FUCS reconoce la información como uno de los principales activos para el desarrollo de las operaciones y cumplimiento de los objetivos institucionales, de esta manera se compromete con su protección, gestión transparente, efectiva y segura, protegiéndola de riesgos que afecten su confidencialidad, Integridad y disponibilidad para el continuo desarrollo de las funciones sustantivas y de apoyo.

2. Generalidades.

La implementación, seguimiento y mejora continua del Manual de Seguridad de la Información, como también la aplicación de los controles establecidos en el presente Manual, están enfocados en minimizar los riesgos asociados al manejo de la información que administran o consultan directivos, colaboradores, estudiantes, proveedores y personal externo de la Universidad FUCS.

El Consejo Superior tendrá la potestad de modificar el Manual de Seguridad de la Información, según los resultados de revisión y las necesidades identificadas, establecidas o según la aplicabilidad de estas.

Los proyectos que sean implementados en la Universidad FUCS deben cumplir con el Manual de Seguridad de la información descrita en este documento. El cumplimiento es de carácter obligatorio, esencial y legalmente requerido para que la Universidad FUCS tenga una adecuada protección y respuesta en seguridad.

Así mismo, la Política general de Seguridad y Privacidad de la Información, en su desarrollo facilita las siguientes premisas:

- Minimizar y/o mitigar los riesgos asociados a Seguridad de la Información en los procesos o áreas de la Universidad FUCS.
- Cumplir con los principios de seguridad de la información: Confidencialidad, Integridad y Disponibilidad.
- Fortalecer la cultura de seguridad de la información de los colaboradores, estudiantes y terceros que tengan vínculo contractual con la Universidad FUCS, con el fin de proteger los activos de información de la Universidad FUCS.
- Proteger los activos de información de la Universidad FUCS y la implementación de proyectos que se requieran acorde con los recursos dispuestos para tal fin.

3. Lineamientos.

- Promueve la protección y resguardo de los activos de información de la Universidad a fin de asegurar la confidencialidad, Integridad y disponibilidad de la información.
- Define controles en los diferentes niveles de la institución, para el manejo de los activos de información y los sistemas de información, enfocados en mitigar los riesgos asociados al manejo de la información.
- Promueve la cultura de uso seguro de la información, con el fin de evitar el riesgo de fuga de la misma.
- Define la clasificación de la información a fin de establecer los controles necesarios para su protección.
- Dispone de los recursos para la implementación y cumplimento de la normatividad vigente respecto a la seguridad de la información.
- Promueve la revisión permanente para la actualización de los mecanismos que permitan el cumplimiento de los pilares de la seguridad de la información.
- Define los estándares institucionales para garantizar la seguridad de la información.
- Regula el uso institucional de herramientas de inteligencia artificial, servicios en la nube, aplicaciones y dispositivos tecnológicos mediante controles de autorización, acceso, trazabilidad, supervisión humana y gestión de incidentes de seguridad.

4. Alcance

El presente manual tiene por objeto establecer lineamientos para gestionar la seguridad de la información en los activos de información, los sistemas de información institucionales y en general el ambiente tecnológico de la Universidad FUCS.

Deberá ser conocido y cumplido por todos los colaboradores (directivos, administrativos, docentes, practicantes, aprendices), estudiantes y terceros vinculados (contratistas y/o proveedores) de la Universidad FUCS.

El presente Manual toma como referencia los requisitos generales de la norma ISO/IEC 27001:2022 para el establecimiento, implementación, mantenimiento y mejora continua de un Sistema de Gestión de Seguridad de la Información, así como las orientaciones y controles previstos en la norma ISO/IEC 27002:2022.

Los lineamientos y controles se organizan de acuerdo con la estructura y las necesidades institucionales de la Universidad FUCS.

5. Contexto y partes interesadas

La Universidad FUCS determinará y revisará las condiciones internas y externas que puedan afectar el logro de los resultados del Sistema de Gestión de Seguridad de la Información.

Para lo anterior podrá tener en cuenta, entre otros aspectos, la identificación de sus grupos de interés y los requisitos aplicables a cada grupo, su naturaleza como institución de educación superior, sus funciones sustantivas, la infraestructura y servicios tecnológicos de que dispone, las condiciones especiales a seguir en el tratamiento de información académica, administrativa, financiera, laboral, investigativa y de salud, la interacción con los escenarios de práctica y demás aliados institucionales, la contratación de proveedores, así como los cambios jurídicos, tecnológicos, sociales y ambientales que puedan generar riesgos para la seguridad de la información.

Los requisitos pertinentes a cada grupo de interés se incorporarán en la gestión de riesgos, los controles, los contratos, los procedimientos y las evaluaciones del Sistema.

La Universidad podrá incluir en la revisión respectiva, el análisis sobre si el cambio climático constituye una condición relevante para el Sistema de Gestión de Seguridad de la Información o para las necesidades de sus partes interesadas, particularmente cuando pueda afectar la infraestructura física o tecnológica, la disponibilidad de servicios, la continuidad de las operaciones o la prestación de servicios por parte de terceros a favor de la Universidad FUCS.

6. Marco Normativo

Para la estructuración e implementación del presente Manual de Seguridad de la información, la

Universidad FUCS ha tomado como referencia los requisitos generales de la norma ISO/IEC 27001:2022, las orientaciones y controles de la norma ISO/IEC 27002:2022 y las demás normas, guías y disposiciones aplicables que se relacionan a continuación:

- Ley 1712 de 2014 – Ley de Transparencia y Acceso a la Información Pública
- Ley 1581 de 2012 – Ley de Protección de Datos Personales
- Ley 2300 de 2023 – Ley Dejen de Fregar
- Decreto 1074 de 2015 - Decreto Único Reglamentario del Sector Comercio, Industria y Turismo, en sus disposiciones sobre protección de datos personales.
- Decreto 1081 de 2015.
- Resolución 1519 de 2020 - Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos.
- ISO/IEC 27001:2022 – Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de seguridad de la información. Requisitos. ISO/IEC 27001:2022/Amd 1:2024 – Enmienda 1. Cambios relativos a la acción climática. ISO/IEC 27002:2022 – Seguridad de la información, ciberseguridad y protección de la privacidad. Controles de seguridad de la información.
- ISO 31000:2018 – Gestión del riesgo. Directrices
- ISO 22301:2019 – Seguridad y resiliencia. Sistemas de gestión de continuidad del negocio. Requisitos.
- Ley 30 de 1992 - Organización del servicio público de la Educación Superior
- Guías para el fortalecimiento del SGSI de MINTIC–Ministerio de Tecnologías de la Información y la Comunicación.
- Guía para la implementación del principio de responsabilidad demostrada de la Superintendencia de Industria y Comercio.
- Guía sobre el tratamiento de datos personales en el contexto universitario de la Superintendencia de Industria y Comercio.

7. Objetivo General

Establecer directrices y lineamientos generales que permitan proteger los activos de información de la Universidad FUCS, garantizando la confidencialidad, integridad y disponibilidad, protegiendo los datos personales y dando cumplimiento a los requisitos legales, regulatorios, contractuales e institucionales aplicables, tomando como referencia las normas ISO/IEC 27001:2022 e ISO/IEC 27002:2022 y otros estándares de ciberseguridad aplicables.

8. Objetivos Específicos

- Administrar, preservar y proteger la información de la Universidad FUCS, así como los recursos tecnológicos utilizados para su operación, almacenamiento y procesamiento; frente a amenazas internas o externas, garantizando el cumplimiento de los principios de seguridad de la información: Confidencialidad, Integridad y Disponibilidad de la información.
- Mantener actualizado, vigente y operativo el Manual de Seguridad de la Información de

manera que pueda ser auditada de acuerdo a los riesgos identificados por la Universidad FUCS, con el fin de conservar su nivel de eficacia y aplicabilidad.

- Determinar los lineamientos para una identificación y definición de riesgos con criterios que permitan la medición de su impacto y las alternativas de tratamiento que mantengan la operatividad de sus servicios dentro de los acuerdos de continuidad de la Universidad FUCS.
- Generar cultura de uso seguro de los sistemas de información.
- Fortalecer la Seguridad de la Información, mediante la implementación de mecanismos de control que permitan mitigar los riesgos.
- Gestionar a la mayor brevedad los eventos o incidentes de seguridad de la información, identificados y originados por el incumplimiento del Manual de Seguridad de la Información.
- Dar cumplimiento a los requisitos normativos y regulatorios aplicables en materia de protección de datos personales y seguridad de la información y atender los requerimientos de las autoridades y órganos de control competentes.
- Identificar eventos de fraude y establecer acciones, para la protección del buen nombre de la Universidad FUCS.

9. Compromiso de la Alta Dirección

El Consejo Superior y la Rectoría, en el marco de sus respectivas competencias, se comprometen a apoyar el desarrollo, implementación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información mediante las siguientes actuaciones:

- Revisar y aprobar el presente Manual de Seguridad de la Información y sus actualizaciones.
- Incentivar la cultura de Seguridad de la Información.
- Incentivar la divulgación del presente manual a la comunidad universitaria y a los terceros a los que resulte aplicable.
- Asignar los recursos necesarios para implementar y mantener las iniciativas de seguridad de la información.
- Revisar el desempeño del Sistema de Gestión de Seguridad de la Información, teniendo en cuenta los resultados de las auditorías institucionales y las oportunidades de mejora que se presenten.

10. Roles, Responsabilidades y Autoridades

En el organigrama de la Universidad FUCS, se encuentra definida la estructura de primer nivel, donde se observan todos los procesos, los cuales deberán dar cumplimiento al presente Manual de Seguridad de la Información.

Los lineamientos y controles aquí mencionados aplican para todos colaboradores (directivos, administrativos, docentes, practicantes, aprendices), estudiantes y terceros (contratistas y/o proveedores) que mantengan relación con el desarrollo de la misión de la Universidad FUCS y por tanto es responsabilidad de la Alta Dirección, velar por su cumplimiento.

Controles

No.	Responsable	Actividades
1	Consejo Superior	● Aprobar la creación de los cargos relacionados con las funciones de seguridad de la información. ● Asignar los recursos pertinentes para la aplicación eficaz del Manual de Seguridad de la Información de la Universidad FUCS.
2	Comité de Seguridad de la Información	● Revisar y proponer la actualización del Manual de Seguridad de la Información, de las funciones y de los controles asociados al Sistema de Gestión de Seguridad de la Información. ● Definir las necesidades de capacitación que se presenten en la Universidad FUCS. ● Aprobar roles relacionados con la seguridad de la información en los diferentes niveles jerárquicos. ● Definir planes de acción para subsanar debilidades en controles.
3	Profesional de Seguridad de la Información	● Actuar como oficial de protección de datos personales de la Universidad FUCS. ● Gestionar, coordinar y hacer seguimiento al Programa Integral de Gestión de Datos Personales de la Universidad FUCS, en el marco del Sistema de Gestión de Seguridad de la Información. ● Actualizar, documentar, sensibilizar y aplicar las normas y/o estándares aplicables para el mantenimiento del Sistema de Gestión de Seguridad de la Información. ● Gestionar en conjunto con la División de Desarrollo Tecnológico los controles para mitigar los riesgos asociados a la Seguridad de la Información y a la protección de datos personales, bajo su ámbito o alcance. ● Brindar acompañamiento especializado a los líderes de las dependencias, facultades, procesos y procedimientos en la identificación de amenazas, vulnerabilidades, impactos y controles relacionados con la seguridad de la información y la protección de datos personales, de conformidad con el Procedimiento de Gestión de Riesgos Institucionales. ● Monitorear la aplicación y cumplimiento de los controles definidos e informar al Comité de Seguridad de la Información los resultados correspondientes. ● Ejercer la secretaría del Comité de Seguridad de la Información, custodiar sus actas y hacer seguimiento a la ejecución de sus decisiones.
4	División de Desarrollo Tecnológico	● Asignar las funciones, roles y responsabilidades a los colaboradores encargados de la gestión y operación de la plataforma tecnológica de la institución. ● Gestionar en conjunto con Seguridad de la Información los controles para

		mitigar los riesgos asociados a la Seguridad de la Información.
5	División de Gestión del Talento Humano	• Notificar a los nuevos colaboradores, sobre la obligación de cumplir con el presente Manual de Seguridad de la Información. • Definir y aplicar los procesos disciplinarios a que haya lugar por las faltas identificadas a el Manual de Seguridad de la Información.
6	División de Auditoría	• Auditar el cumplimiento del presente Manual de Seguridad de la Información, dentro de la programación de auditorías institucionales. • Auditar el cumplimiento de la Política de Protección de Datos Personales y de los controles asociados al Programa Integral de Gestión de Datos Personales, dentro de la programación de auditorías institucionales.
7	Todos los Usuarios	• Cumplir el presente Manual de acuerdo con su rol dentro de la institución, así como, personal externo que realice labores en o para la Universidad FUCS. • Recibir las capacitaciones y sensibilizaciones sobre Seguridad de la Información, de tal forma que tenga conocimiento respecto al presente Manual.

III. ORGANIZACIÓN PARA LA SEGURIDAD DE LA INFORMACIÓN

La Universidad FUCS adopta el presente Manual de Seguridad de la Información, en el cual se establecen los roles, responsabilidades, controles y actividades necesarios para la administración, operación, evaluación, mejoramiento y gestión de la seguridad de la información.

La Universidad FUCS, es la responsable del Sistema de Gestión de Seguridad de la Información. Es un asunto de gran relevancia para los directivos, en consecuencia, apoyan la creación del Comité de Seguridad de la Información, integrado por delegados de las instancias administrativas y académicas.

El comité debe encargarse de velar por brindar el soporte manifiesto al Sistema de Gestión de Seguridad de la Información.

1. Funciones del Comité de Seguridad de la Información.

a. Revisar y proponer la actualización del Manual de Seguridad de la Información, de las funciones y de los controles asociados al Sistema de Gestión de Seguridad de la Información.

b. Conocer los resultados de la gestión de los riesgos de seguridad de la información y protección de datos personales, sus cambios significativos, materializaciones y planes de tratamiento, y

formular recomendaciones sobre la priorización de controles y cambios internos necesarios para su mitigación.

c. Conocer los eventos, incidentes y/o riesgos relativos a la seguridad de la información y las acciones de mitigación establecidas, así como proponer y aprobar acciones de mejora que se consideren pertinentes frente a los mismos.

d. Revisar y aprobar las iniciativas tendientes a mejorar la seguridad de la información.

e. Acordar y aprobar las metodologías y procesos específicos de Seguridad de la Información.

f. Solicitar a los responsables de los procesos de gestión que se alineen con el Manual de Seguridad de la Información, cuando se detecten actividades o controles que no se ajusten a lo descrito en el presente documento.

g. Coordinar, evaluar y promover la implementación de los controles específicos de seguridad de la información para nuevos servicios tecnológicos o sistemas, o procesos en los que se evidencie su necesidad de implementación.

h. Respaldar e impulsar la difusión del Manual de Seguridad de la información y la Política de Protección de Datos personales, así como su importancia, dentro de la comunidad universitaria.

i. Coordinar el proceso relacionado con la atención y gestión de las estrategias de continuidad del negocio, de los servicios tecnológicos institucionales frente a desastres o interrupciones imprevistas.

j. Aprobar la matriz de roles y perfiles de los Sistemas de información.

k. Revisar las actualizaciones anuales y modificaciones necesarias que requiera la Política de tratamiento de datos personales de la Institución, para su aprobación por el Consejo Superior.

l. Las demás establecidas en el Manual de Seguridad de la Información

2. Organización Interna.

Todos los colaboradores (directivos, administrativos, docentes, practicantes, aprendices), estudiantes y terceros (contratistas y/o proveedores), deben actuar de acuerdo con el Manual de Seguridad de la Información y los controles aquí establecidos, participando en las revisiones de seguridad que se lleven a cabo. Adicionalmente, presentarse en las distintas capacitaciones y/o jornadas de sensibilización lideradas por la División de Desarrollo Tecnológico y Seguridad de la Información.

Los propietarios, administradores, usuarios y custodios de la información de la Universidad FUCS deben:

- Aceptar y cumplir el Manual de Seguridad de la Información y los controles que se establezcan en la Universidad FUCS.

- Aceptar la responsabilidad de proteger la información de la Universidad FUCS contra pérdida, modificaciones y accesos no autorizados de terceras personas.
- Entender claramente su rol y responsabilidad frente al acceso y uso de los sistemas de información.
- Todas las áreas de la Universidad FUCS y los terceros que interactúan con la Institución (contratistas o proveedores), deben cumplir con los términos estipulados en las licencias de uso de software y en los contratos de adquisición de estas.
- Los colaboradores deben utilizar la información de la Universidad FUCS exclusivamente para fines laborales, quedando prohibido explícitamente el uso o divulgación para fines comerciales y/o privados no autorizado.
- Los terceros (contratistas o proveedores) que interactúan con la Universidad FUCS no deben hacer copias del software suministrado, ni podrán transferirlo a otro equipo por medio de la red, sin la autorización escrita de la Universidad FUCS.
- Debe existir un responsable para cada uno de los recursos de tecnología y activos de información usados en la Universidad FUCS. Las responsabilidades deben estar delimitadas de tal manera que no existan varios responsables de un mismo recurso.
- Se deberá informar a la división tecnológica cualquier incidente presentado ante protección de datos y seguridad de la información

3. Gestión de riesgos de seguridad de la información

La identificación, análisis, evaluación, tratamiento, seguimiento y comunicación de los riesgos de seguridad de la información se realizará de conformidad con el Procedimiento de Gestión de Riesgos Institucionales del Sistema de Gestión Organizacional de la Universidad FUCS, y demás normas internas sobre la materia.

Los líderes de las dependencias, facultades, procesos y procedimientos, con el acompañamiento del Profesional de Seguridad de la Información, serán responsables de identificar, valorar, tratar y hacer seguimiento a los riesgos de seguridad de la información asociados con las actividades y activos a su cargo, así como de implementar los controles y planes de acción correspondientes, mantener actualizada la información y reportar las evidencias y materializaciones en los sistemas institucionales definidos para tal fin.

La División de Planeación y Gestión Organizacional orientará la aplicación de la metodología institucional, verificará la adecuada documentación de las matrices y realizará el seguimiento y evaluación de los controles de acuerdo con sus competencias.

El Profesional de Seguridad de la Información brindará acompañamiento especializado a los líderes de las dependencias, de los procesos y procedimientos para identificar amenazas, vulnerabilidades, impactos y controles relacionados con la confidencialidad, integridad y disponibilidad de la información.

La valoración deberá revisarse con la periodicidad establecida institucionalmente y cuando se presenten cambios sustanciales en los procesos, activos, sistemas, infraestructura, servicios

tecnológicos, proveedores, requisitos aplicables o modalidades de operación, así como después de la materialización de riesgos, incidentes relevantes o la identificación de nuevas amenazas o vulnerabilidades.

El seguimiento y evaluación del diseño, ejecución y efectividad de los controles de seguridad de la información se realizará de acuerdo con el Procedimiento de Gestión de Riesgos Institucionales. Los hallazgos, controles ineficaces, riesgos materializados y oportunidades de mejora deberán incorporarse en las matrices, planes de acción y procedimientos institucionales que correspondan.

4. Manejo de equipos portátiles, equipos de escritorio y dispositivos móviles.

La Universidad FUCS debe garantizar que los colaboradores se comprometan a hacer uso adecuado de los dispositivos móviles para el acceso a los servicios corporativos de movilidad proporcionados por la Universidad FUCS, tales como aplicaciones, escritorio remoto y aplicaciones virtuales, correo electrónico, comunicaciones unificadas, redes virtuales privadas (VPN), entre otros.

Controles

Responsable	Actividades
División de Desarrollo Tecnológico	● Instalar las actualizaciones de software y seguridad de forma regular. ● En caso de robo la división de desarrollo tecnológico podrá realizar borrado remoto de la información almacenada en el dispositivo móvil con el fin de evitar que la información quede expuesta. ● Generar acceso a conexiones por VPN para conexión correcta para uso laboral y acceso correcto a aplicaciones que usa la institución
Seguridad de la Información	● Monitorear el cumplimiento de los lineamientos relacionadas con el buen uso de los equipos portátiles y dispositivos móviles. ● Garantizar que los dispositivos móviles que tienen acceso a información institucional estén autorizados y cumplen con los requisitos para su uso como antivirus y contraseñas seguras. ● Realizar capacitaciones y/o sensibilizaciones con el fin de dar a conocer la importancia de utilizar los equipos portátiles y dispositivos móviles de forma segura.
Todos los Usuarios	● Usar los dispositivos móviles, escritorio y portátiles de forma responsable. ● Proteger la información confidencial. ● Reportar cualquier incidente de seguridad a soporte@fucsalud.edu.co o al correo seguridaddelainformacion@fucsalud.edu.co

	● No abrir o aceptar mensajes de correo electrónico, SMS, MMS entre otros que vengan de origen desconocido. ● Mantener actualizado el sistema operativo de su dispositivo móvil, con las últimas actualizaciones disponibles previniendo que el dispositivo móvil sea expuesto a posibles vulnerabilidades. ● Evitar conexiones a redes públicas (Aeropuertos, hoteles, centros comerciales y terminales de transportes) ● Informar a la división de desarrollo tecnológico de la pérdida o robo de su dispositivo móvil con el fin de que el área tome las medidas para evitar que la información quede expuesta a terceros no autorizados. ● Contar con la configuración de algún patrón de seguridad para el bloqueo del dispositivo. ● Generar uso adecuado en navegaciones mediante conexiones VPN

5. Trabajo Remoto

La Universidad FUCS debe establecer, implementar y mantener lineamientos, controles y medidas de seguridad que garanticen la confidencialidad, integridad, disponibilidad y protección de la información institucional durante el desarrollo de actividades bajo modalidades de trabajo remoto (trabajo remoto, trabajo en casa y teletrabajo) garantizando la protección de dispositivos y gestión de riesgos cibernéticos asociados a conexiones externas y entornos remotos

Controles

Responsable	Actividades
División de Gestión del Talento Humano	● Verifica que la solicitud de trabajo remoto, este aprobada por el jefe de área.
División de Desarrollo Tecnológico	● Evaluar las solicitudes de permisos de VPN, aprobarlas o denegarlas, previa autorización por Gestión Humana y la Dependencia de la cual depende el colaborador que solicita el acceso. ● Configurar las conexiones remotas a los servicios tecnológicos al colaborador autorizado y por periodos de tiempo establecidos, de conformidad con las tareas asignadas.
Todos los Usuarios	● Contar con las autorizaciones necesarias para establecer una conexión remota (VPN) con los dispositivos de la plataforma tecnológica de la Universidad FUCS y cumplir con las instrucciones de acceso establecidas para las conexiones remotas descritas en este Manual.

	● Establecer conexiones remotas únicamente a través de la VPN y utilizar computadores que brinda la Universidad FUCS y, en ninguna ocasión, en computadores públicos, como hoteles o cafés internet, entre otros. ● Realizar la solicitud de conexiones VPN a través de la Mesa de Ayuda de la División de Desarrollo Tecnológico la cual deberá contar con la debida autorización del jefe inmediato. ● Cumplir con los requisitos estipulados acerca de escritorio y pantalla limpia. ● Permitir la ejecución de actividades de mantenimiento preventivo y correctivo para garantizar la seguridad del equipo esto se establecerá en los tiempos definidos por la División de Desarrollo Tecnológico.

6. Seguridad de la Información en la Gestión de Proyectos de TI

La Universidad FUCS debe integrar la seguridad de la información y la protección de datos personales desde la planeación, diseño, adquisición, desarrollo, configuración, prueba, implementación, operación, actualización y retiro de los proyectos, productos, servicios, sistemas y soluciones tecnológicas.

Los controles deberán definirse de acuerdo con la naturaleza de la información, las finalidades del tratamiento, los riesgos para los titulares y el impacto que una pérdida de confidencialidad, integridad o disponibilidad pueda generar.

Implementar controles de seguridad específicos en las áreas responsables puede proteger la información confidencial, prevenir fugas de información y asegurar el cumplimiento de las normas y regulaciones.

Los proyectos institucionales que puedan generar un riesgo elevado para los derechos de los titulares de datos personales deberán contar, antes de su implementación, con una evaluación de impacto en privacidad, en la que se deberá analizar el tratamiento proyectado, su necesidad y proporcionalidad, los riesgos para los titulares de datos personales, las medidas de mitigación y controles que realmente puede implementar la Universidad FUCS, el riesgo residual, los responsables de su implementación y la decisión de aprobar, modificar, suspender o descartar el proyecto.

La evaluación deberá efectuarse por el líder del proyecto, acompañado de la División de Desarrollo Tecnológico y el profesional de Seguridad de la Información, y deberá presentarse ante el Comité de Seguridad de la Información para su análisis y aprobación.

Esta evaluación será obligatoria, entre otros eventos, cuando se traten datos sensibles o de menores de edad, se realice monitoreo sistemático, se utilicen datos biométricos o de

geolocalización y/o perfilamiento, se adopten decisiones automatizadas con efectos relevantes, se integren múltiples bases de datos, se implementen tecnologías emergentes, o se transfiera o transmita información a terceros o a otros países en condiciones que incrementen el riesgo.

Controles

Responsable	Actividades
Líderes de Procesos	● Antes de aprobar un proyecto que implique tratamiento de datos personales, revisar en conjunto con Seguridad de la Información, el flujo de los datos personales, los mecanismos de recolección, la autorización de tratamiento de datos, la guarda de la autorización, las finalidades de recolección, los terceros que acceden a la misma y los riesgos para los titulares, para establecer las configuraciones y controles necesarios que permitan garantizar un adecuado tratamiento de datos en el nuevo proyecto. ● Implementar la seguridad de la información en la administración de los proyectos de la Universidad FUCS, independientemente de su origen, con el propósito de asegurar que los riesgos de seguridad de la información sean identificados, evaluados y tratados como parte integral del proyecto. ● Garantizar que la seguridad de la información se integre en todas las etapas de la metodología del proyecto.
Seguridad de la Información	● Evaluar si los objetivos, actividades y condiciones del proyecto se ajustan al presente Manual y a los requisitos aplicables de seguridad de la información y protección de datos personales, y formular recomendaciones para el tratamiento de los riesgos identificados. ● Brindar recomendaciones donde se identifique riesgos para los activos tecnológicos de la Universidad FUCS
División de Desarrollo Tecnológico	● Implementar en todo nuevo proyecto de TI o herramienta tecnológica, mecanismos de minimización, seudonimización, anonimización, cifrado, segregación de ambientes, registro de accesos, trazabilidad, gestión de privilegios y eliminación segura, según la categoría de los datos y el nivel de riesgo del tratamiento.

IV. GESTIÓN DE ACTIVOS DE INFORMACIÓN

La Universidad FUCS como propietaria de la información física y digital; generada, procesada y/o almacenada por diferentes instancias institucionales y transmitida a través de su plataforma tecnológica, otorgará responsabilidad sobre sus activos de información a los líderes de procesos, encargados de asegurar el cumplimiento de las directrices sobre el uso adecuado de la misma.

Los recursos de procesamiento de información de la Universidad FUCS están sujetos a revisión por parte de la Oficina de Auditoría de Gestión, y de los entes externos de supervisión (determinados por el Consejo Superior), por lo que, los propietarios de los activos de información deberán ser facilitadores en los procesos de revisión interna o externa, que la institución determine pertinentes.

Los activos de información deben ser identificados y clasificados acordes con la criticidad del activo. El inventario de activos de información se revisará y actualizará cada dos años, identificando; responsable de los activos, custodios, ubicación, amenazas, vulnerabilidades, usuarios y los controles que se tienen implementados para garantizar la Confidencialidad, Integridad y Disponibilidad de la información.

Los activos de información deberán ser identificados y clasificados por el líder del proceso, con el acompañamiento de Seguridad de la Información. La clasificación deberá atender, de manera diferenciada y complementaria, la naturaleza de la información, el régimen jurídico aplicable, las finalidades del tratamiento, los titulares involucrados, los riesgos asociados y los niveles de confidencialidad, integridad y disponibilidad requeridos.

Cuando el activo contenga datos personales, su clasificación deberá identificar si se trata de datos públicos, semiprivados, privados o sensibles, de conformidad con la ley vigente. Esta clasificación será paralela a las categorías de información pública, pública clasificada o pública reservada previstas en el régimen de transparencia y acceso a la información pública, las cuales se aplicarán únicamente cuando resulten jurídicamente procedentes.

Un mismo activo podrá estar sujeto simultáneamente a criterios de clasificación de seguridad de la información, protección de datos personales, reserva legal, gestión documental y acceso a la información. En estos casos deberán aplicarse los controles correspondientes al nivel de protección más elevado, sin perjuicio del análisis jurídico particular que resulte necesario.

1. Clasificación de la Información.

La Universidad FUCS define los diferentes niveles de clasificación de la información teniendo en cuenta el grado de confidencialidad, importancia y sensibilidad; basados en la guía de clasificación de la información generada por Seguridad de la Información, así como los controles necesarios para su protección.

Los líderes de las dependencias quienes para el efecto son los responsables de la información, deberán identificar los activos de información de las áreas a su cargo, con el fin de elaborar el inventario de activos de información y velar por mantenerlo actualizado con una periodicidad de 24 meses o cuando sea necesario.

La clasificación de la información debe realizarse teniendo en cuenta los principios de Seguridad de la Información y protección de datos personales, así:

- ✓ Confidencialidad

Para la Universidad FUCS la información que sea confidencial no deberá estar disponible ni ser revelada a individuos, entidades o procesos no autorizados, la cual será determinada bajo los siguientes niveles:

- *Alta*: información que al estar disponible o revelada puede tener un impacto significativo legal o económico. Puede generar reprocesos, pérdida de imagen o reputación de la institución.
- *Media:* información que al estar disponible o revelada puede tener un impacto legal y/o económico. Puede generar reprocesos en las actividades o pérdida moderada de la imagen reputacional.
- *Baja:* información que al estar disponible o revelada conlleva un impacto no significativo para la institución o entes externos.

✓ Integridad

La integridad de la información se define de acuerdo a la exactitud y completitud de la misma, permitiendo que tenga coherencia y esté disponible en su ciclo de vida. Se clasificará bajo los siguientes niveles:

- *Alta:* Información cuya incompletitud puede generar pérdidas severas de imagen reputacional, legal o económicas para la institución.
- *Media*: Información cuya inexactitud o falta de completitud puede generar impactos negativos moderados de imagen reputacional, económicos o legales.
- *Baja:* Información cuya pérdida de exactitud o que se encuentre incompleta, puede generar un impacto no significativo en la imagen reputacional, aspectos jurídicos o económicos.

✓ Disponibilidad

Para la Universidad FUCS la información se encontrará disponible para el acceso por solicitud de un colaborador, institución y/o procesos previamente autorizados, en el momento y en el medio requerido, así como los recursos necesarios para su uso. Los niveles de clasificación para esta propiedad están sujetos a la no disponibilidad de la información teniendo en cuenta lo siguiente:

- *Alta*: La información que no esté disponible puede generar un impacto negativo y severo de índole legal, económica, genera reprocesos y pérdida de imagen.
- *Media*: La información que no se encuentre disponible puede generar un impacto negativo moderado de índole legal, económica, reputacional y reprocesos en las actividades.
- *Baja:* La información que no se encuentre disponible, puede afectar la operación cotidiana de la institución, no genera pérdidas económicas, legales o reputaciones.

✓ Protección de datos personales

Para la Universidad FUCS, la información deberá identificar si contiene datos personales, de forma tal que, si el activo de información los contiene, el inventario deberá registrar, como mínimo:

a) El proceso y el área responsable;
b) Las categorías de titulares y de datos tratados;
c) La clasificación de los datos como públicos, semiprivados, privados o sensibles;
d) Las finalidades específicas del tratamiento;
e) El fundamento jurídico que habilita el tratamiento;
f) Los usuarios, cargos, dependencias y terceros autorizados para acceder a la información;
g) Las fuentes de obtención y los destinatarios de la información;
h) Las transferencias o transmisiones nacionales o internacionales que se realicen;
i) Los sistemas, repositorios y lugares de almacenamiento;
j) Los términos de conservación y las reglas de supresión, anonimización o archivo;
k) Los riesgos asociados al tratamiento; y
l) Las medidas jurídicas, administrativas, físicas y tecnológicas aplicables.

Esta información deberá mantenerse actualizada cuando cambien las finalidades, los sistemas utilizados, los sujetos autorizados, los terceros intervinientes o cualquier otra condición relevante del tratamiento.

De acuerdo con los principios de Seguridad de la Información, la Universidad FUCS realizará el etiquetado de la información conforme a la siguiente descripción:

Clasificación de la Información	Sigla para el Etiquetado	Descripción
Información Pública Reservada	IPR	El acceso a la información o revelación de la información a individuos, instituciones o procesos no autorizados tiene un impacto negativo de índole legal, económica, operativa o genera pérdida de imagen.
Información Pública Clasificada	IPC	Esta información es de acceso a varios colaboradores de la Universidad FUCS para realizar labores propias del área. No podrá ser utilizada por terceros sin autorización previa del administrador de la información.
Información Pública	IP	Información que puede ser entregada o publicada en la página web sin restricciones a cualquier persona dentro y fuera de la institución, sin que esto implique daños a terceros ni a las actividades de los procesos de la Universidad FUCS.

La información (pública clasificada y pública reservada) deberá estar protegida por contraseña y/o cifrada. De igual manera, deberá protegerse en caso de ser transmitida o en el medio de almacenamiento en el que se encuentre.

Una vez clasificada la información, la Universidad FUCS proporcionará los recursos tecnológicos necesarios para la aplicación de controles que preserven su confidencialidad, integridad y disponibilidad, promoviendo el uso adecuado por parte de los colaboradores y personal provisto por terceros que se encuentre autorizados y requieran el uso de información institucional para la ejecución de sus actividades.

Controles

Responsable	Actividades
Seguridad de la Información	● Diseñar y producir la guía de clasificación de la información. ● Monitorear la aplicación de los controles definidos para la actualización de activos de información de cada unidad o proceso. ● Socializar y publicar la guía de clasificación de la información a la comunidad universitaria de la Universidad FUCS. ● Monitorear que la depuración y la eliminación de la información se realice de una manera efectiva a través de los mecanismos necesarios. ● Aplicar los mecanismos de control necesarios, que garanticen los principios de Seguridad de la Información de los recursos tecnológicos bajo su custodia. ● Monitorear la supervisión sobre el cumplimiento de los ANS - Acuerdos de Niveles de Servicio y de intercambio de información establecidos con el proveedor de custodia externa de los documentos de la institución (en caso de presentarse la situación de almacenamiento externo).
División de Desarrollo Tecnológico	● Proveer los métodos de cifrado de la información y gestionar la contratación y actualización de las herramientas tecnológicas usadas para este fin.
Gestión Documental	● Velar por la destrucción de información física, cuando se ha cumplido su ciclo de almacenamiento. ● Mantener actualizadas las tablas de retención documental y velar por su aplicación
Propietarios de los Activos de Información	● Deben utilizar la guía de clasificación de la información para clasificar la información que gestionan. ● Son responsables por el monitoreo periódico de la información y la correcta clasificación o reclasificación de los activos de información a su cargo.

Todos los Usuarios	● Deben cumplir con los lineamientos establecidos por la Universidad FUCS sobre: el acceso, divulgación, almacenamiento, copia, transmisión, identificación y eliminación de la información de origen tecnológico (sistemas de información, archivos digitales) y medio físico propiedad de la Universidad FUCS. ● La información en medio físico y digital de la Universidad FUCS, debe tener un periodo de almacenamiento que puede ser establecido por el cumplimiento de normas legales o misionales; el período hace parte de la información contenida en las tablas de retención documental. Una vez se finalice el periodo de conservación, se debe garantizar la destrucción adecuada de la información. ● Los usuarios deben tener en cuenta: que cuando imprimen, escanean, saquen copias y comparten información: verificar las áreas adyacentes a impresoras, escáneres, fotocopiadoras y medios electrónicos para que no queden documentos relacionados o adicionales; de igual forma, se debe recoger los documentos de las máquinas de impresión para evitar la divulgación no autorizada. ● Los colaboradores de la Universidad FUCS y el personal provisto por terceras partes deben garantizar qué, al no estar en su puesto de trabajo los escritorios se encuentran libres de documentos y medios de almacenamiento, utilizados en el desarrollo de sus actividades; también deben asegurar la protección de los documentos de acuerdo con su nivel de clasificación. ● La Universidad FUCS y sus colaboradores, deben garantizar las condiciones adecuadas de almacenamiento, custodia, restricción y acceso físico a la información que se encuentra en documentos físicos.

2. Manejo de Medios Removibles.

La Universidad FUCS debe garantizar que la información almacenada en cualquier medio removible, que vaya a ser entregada a un colaborador o ente externo, sea removida de tal forma que no se pueda recuperar.
Todos los medios removibles que contengan información de la Universidad FUCS deben estar ubicados en un ambiente protegido y seguro, de acuerdo con las especificaciones del fabricante.

Controles

Responsable	Actividades

Comité de Seguridad de la Información	● Analizar de acuerdo con su criterio experto, qué cargos por la naturaleza de sus funciones requieren manejar este tipo de dispositivos; los cuales deben ser aprobados en dicho comité. Para los cargos excepcionales, el líder de proceso realizará la solicitud formal a Seguridad de la Información, con el fin de solicitar y justificar el otorgamiento de estos permisos, los cuales serán presentados a título informativo en Comité de Seguridad de la Información
División de Desarrollo Tecnológico	● Implementar las acciones establecidas en el comité de Seguridad de la Información, tendientes a mitigar cualquier riesgo relacionado con medios ● Realizar oportunamente una copia de respaldo que mitigue la pérdida de información.
Todos los Usuarios	● Deberán asegurar que la información allí contenida, no esté expuesta a ningún riesgo. ● La información considerada como "Información Pública Clasificada" o "Información Pública Reservada"; deberá estar bajo los controles establecida ● Reportar inmediatamente cualquier incidente, pérdida, robo o conexión sospechosa relacionada con medios removibles.

V. SEGURIDAD DEL TALENTO HUMANO

1. Vinculación de Colaboradores.

Para la Universidad FUCS el factor humano es fundamental para el cumplimiento de sus objetivos misionales, por ello se debe contar con personal calificado, así como también se debe garantizar que la vinculación de los nuevos colaboradores se realice mediante un proceso adecuado de selección, orientado a la asignación de actividades y roles de acuerdo con las funciones que se encuentran descritas en sus funciones de cargo.

Controles

Responsable	Actividades

División de Gestión del Talento Humano	• Verificar los antecedentes de todos los candidatos a convertirse en colaboradores de la Universidad FUCS esto debe llevarse a cabo antes de incorporarse a la organización y de forma continuada, tomando en consideración las leyes. • Garantizar que los colaboradores de la institución conozcan, acepten y firmen los documentos de confidencialidad, seguridad de la información y tratamiento de datos personales; estos documentos deben estar anexos y hacer parte integral del proceso de contratación. • Ejecutar un plan de capacitación y actualización periódica en temas de seguridad de la información para el personal de la Universidad FUCS y cuando sea pertinente para los terceros que desempeñen funciones en la Institución.
Directivos, Supervisores de Contratos	• Antes de otorgar el acceso a la información de la Universidad FUCS, confirmar la aceptación de los acuerdos y/o cláusulas de confidencialidad por parte de los contratistas.
Contratistas	• Deben firmar un acuerdo y/o cláusula de confidencialidad, con el fin de administrar correctamente los usuarios y roles otorgados. • Garantizar que se cumpla lo descrito en los documentos relacionados con la de seguridad de la información de la Universidad FUCS.

2. Procesos disciplinarios por incumplimiento de seguridad de la información

La Universidad FUCS investigará y sancionará conforme a sus reglamentos internos, todas aquellas conductas realizadas por estudiantes, docentes y colaboradores, que conlleven al incumplimiento de las normas de seguridad de la información, protección de los datos personales y uso correcto de los recursos tecnológicos de la Universidad FUCS.

De igual manera, la Universidad ejercerá las acciones administrativas, civiles y penales que sean pertinentes contra contratistas, proveedores, vinculados y terceros frente al incumplimiento en los contratos de prestación de servicios tecnológicos u otros en los que se generen afectaciones a las normas de seguridad de la información, protección de los datos personales y uso correcto de los recursos tecnológicos de la Universidad FUCS.

Así mismo, cuando se presente incumplimiento en los acuerdos de confidencialidad, acuerdos de transmisión de datos personales y contratos de transferencia de datos personales suscritos, de conformidad con lo dispuesto en las normas vigentes.

Controles

Responsable	Actividades
División de Gestión de Talento Humano.	● Efectuar el correspondiente proceso disciplinario, cuando se evidencie el incumplimiento de las normas de seguridad de la información, protección de los datos personales y uso correcto de los recursos tecnológicos de la Universidad FUCS.
División Jurídica	● Reportar de manera oportuna las novedades a la División de Gestión del Talento Humano, cuando se visualice el incumplimiento de las normas de seguridad de la información, protección de los datos personales y uso correcto de los recursos tecnológicos de la Universidad FUCS, por parte de colaboradores docentes y administrativos. ● Ejercer las acciones administrativas, civiles y penales que sean pertinentes contra contratistas, proveedores, vinculados y terceros frente al incumplimiento de las normas de seguridad de la información, protección de los datos personales y uso correcto de los recursos tecnológicos de la Universidad FUCS.
Líderes de área	● Reportar cualquier incidente de seguridad de la información o situación que conlleve o pueda conllevar al incumplimiento de las normas de seguridad de la información, protección de los datos personales y uso correcto de los recursos tecnológicos de la Universidad FUCS. ● Socializar con su grupo de trabajo, las acciones de mejora derivadas de la gestión de incidentes de seguridad de la información, para fortalecer los lineamientos incumplidos del presente Manual. ● Colaborar de manera proactiva y oportuna, en todo proceso de investigación interna o externa que sea adelantado por incumplimientos en las normas de seguridad de la información, protección de los datos personales y uso correcto de los recursos tecnológicos de la Universidad FUCS.
Todos los usuarios	● Cumplir con lo establecido en el presente manual, implementando los respectivos controles. ● Colaborar de manera proactiva y oportuna, en todo proceso de investigación interna o externa que sea adelantado por incumplimientos en las normas de seguridad de la información, protección de los datos personales y uso correcto de los recursos tecnológicos de la Universidad FUCS. ● Realizar el buen uso de los activos de información de la institución
Seguridad de la Información	● Reportar, documentar e investigar los eventos donde se incumplieron las buenas prácticas en seguridad de la información y todo incidente de seguridad de la información que se presente en la institución. ● Recopilar evidencias para el análisis del incidente

3. Desvinculación, Licencias, Vacaciones, o Traslados de Colaboradores y Personal Provisto por

Terceros.

La Universidad FUCS asegurará que el proceso de desvinculación o reasignación de colaboradores y el personal externo se realice de una forma adecuada y segura.

Controles

Responsable	Actividades
División de Gestión de Talento Humano	● Debe ejecutar los controles concernientes a la seguridad de la información para realizar los procesos de novedades de personal (ingreso, reasignación, desvinculación, vacaciones, licencias), de acuerdo con los procedimientos establecidos para este fin. ● Verificar los reportes de novedades de personal (ingreso, reasignación, desvinculación, vacaciones, licencias), y seguidamente solicitar de manera oportuna la respectiva gestión de usuarios a la División de Desarrollo Tecnológico con copia a Seguridad de la Información.
Directivos, Supervisores de Contrato	● Monitorear y reportar de manera oportuna las novedades contractuales de contratistas (persona natural) a la División de Gestión del Talento Humano.
Oficina de Auditoría de Gestión	● Auditar el cumplimiento de los controles establecidos.
División de Desarrollo Tecnológico	● Realizar las asignaciones y los cambios de roles y permisos. ● La División de Desarrollo Tecnológico garantizará la modificación o inhabilitación de usuarios cuando así sea requerido por la División de Gestión de Talento Humano y/o líderes de área, así mismo, garantizará la inactivación temporal.
Seguridad de la Información	● Monitorear el cumplimiento de los procedimientos de activación/inactivación de usuarios.

VI. SEGURIDAD FÍSICA Y DEL ENTORNO

1. Áreas Seguras.

La Universidad FUCS debe proveer mecanismos de seguridad física y controles que eviten problemas de acceso a todas las instalaciones, de igual forma vigilará las amenazas internas y externas y las circunstancias medioambientales de todas las oficinas.

Las áreas que gestionen información crítica o que alberguen activos tecnológicos deberán implementar controles de seguridad física y lógica que permitan proteger la información, los equipos, la infraestructura tecnológica y demás activos institucionales frente a accesos no autorizados.

Controles

Responsable	Actividades
División de Desarrollo Tecnológico	• Aprobar todo acceso a los datacenter o centros de cableado de la Universidad FUCS; de igual forma todo visitante deberá estar siempre acompañado por un colaborador de la División de Desarrollo Tecnológico mientras realice la visita a dichos espacios físicos. • Llevar una bitácora visible en la entrada de los datacenter y centros de cableado con el fin de registrar el acceso de visitantes a estos espacios, el cual debe ser obligatorio. • Desactivar o modificar de manera oportuna los permisos de acceso físico en la data center o centros de cableado a los usuarios previamente autorizados que se retiren o cambien sus labores en la institución. • Aprovisionar y monitorear los espacios físicos teniendo en cuenta las condiciones medioambientales para la protección y operación de los recursos de la infraestructura tecnológica ubicados en la data center; se debe contar con los sistemas de: control de temperatura y humedad, detección y extinción de incendios, alertas, monitoreo y alarmas en caso de detección de cambios en la temperatura y/o en las condiciones ambientales, de la data center. • Confirmar que el cableado estructurado tenga las medidas de protección necesarias de acuerdo con la norma ANSI/TIA/EIA/TSB-75 con el objetivo de reducir las interceptaciones o daños. • Realizar los respaldos de los recursos de la infraestructura tecnológica de la Universidad FUCS ubicados en la data center permitiendo protegerlos contra algún tipo de falla o interrupción. • Garantizar que las áreas designadas para el centro de cómputo y cableado se encuentren en un espacio alejado de líquidos inflamables o de amenazas de inundaciones y/o incendios. • Avalar y revisar que las labores de mantenimiento de redes eléctricas, redes de datos y voz, sean realizadas por colaboradores capacitados y autorizados; así como, realizar seguimiento del cumplimiento de la programación de los mantenimientos preventivos.

Líderes de Procesos	• Los Vicerrectores, Decanos, Gerente, directores y jefes de Oficina que se encuentren en áreas restringidas, deben velar por el buen uso de los sistemas de control de acceso físico y por los equipos de vigilancia instalados en su área. Los Vicerrectores, Decanos, Gerente, directores y jefes de Oficina ubicados en áreas restringidas son responsables, de autorizar el ingreso temporal de personal a estas áreas, evaluando la pertinencia del ingreso; de igual manera se debe realizar el registro y supervisión de estos ingresos. • Los Vicerrectores, Decanos, Gerente, directores y jefes de Oficina deben velar porque todos los mecanismos de Seguridad de acceso a sus áreas sólo sean utilizados por los colaboradores autorizados. Las contraseñas de los sistemas de alarma, las cajas fuertes, las llaves y cualquier otro elemento de seguridad será de acceso restringido y sólo será disponible para personal autorizado, salvo situaciones de emergencia o eventos que por su naturaleza requieran un manejo diferente, siempre con la supervisión de personal interno de la Universidad FUCS
División de Infraestructura	• Proveer los requerimientos necesarios para apoyar, resguardar y velar por el perfecto estado de los controles físicos establecidos en los diferentes espacios de la Universidad FUCS. • Implementar nuevos mecanismos que permitan la mejora de la seguridad física de todas las áreas de la institución, reconociendo los mecanismos actuales y perfeccionándolos. • Asegurar que se cumplan a cabalidad los mecanismos implantados en la seguridad física y en los controles de acceso a los centros de datos y de cableado, así como todas las áreas de la Universidad FUCS que procesen información.
División de Servicios Administrativos	• Validar que se encuentra monitoreado el Circuito Cerrado de Televisión (CCTV) que graba el perímetro de la Universidad FUCS.

Usuarios	• Portar el carnet visible durante su visita a las áreas de la institución, si lo pierden deben reportarlo inmediatamente a División de Gestión del Talento Humano. • Contar con un distintivo que permita su identificación es obligatorio para todo personal externo o tercero que, por el servicio brindado, ingrese a la Universidad FUCS con autorización de los colaboradores. Evitar el acceso a áreas no autorizadas también es un requisito para estos visitantes. • Evitar fumar o consumir alimentos cerca de los equipos es una obligación para todos los colaboradores y proveedores que tengan acceso a las instalaciones de la Universidad FUCS. • No está permitido el uso del PC por otro usuario diferente al que ha sido asignado, salvo casos excepcionales en los cuales la operación de la Universidad FUCS lo requiera. • Bloquear la sesión del equipo cada vez que se interrumpan las actividades o se abandone el puesto de trabajo es una obligación para los colaboradores que tengan a su cargo uno o más equipos de cómputo, con el fin de prevenir el acceso no autorizado a la información. Cerrar las sesiones activas y apagar los equipos al finalizar la jornada laboral también es responsabilidad de todos los empleados, salvo en situaciones excepcionales en las que se haya autorizado el acceso remoto. • Mantener la información sensible o crítica de la Universidad FUCS protegida y evitar pérdidas, daños o accesos no autorizados es una responsabilidad de todos los colaboradores. Guardar la información bajo llave o en la cajonera de trabajo cuando no se encuentren presentes o fuera del horario laboral es esencial. Además, recoger de inmediato toda la información impresa, escaneada o copiada tras autenticar en las impresoras es igualmente necesario. • Todos los equipos de cómputo deben tener lineamientos de protector de pantalla corporativo, con un tiempo de activación automática de cinco minutos.
Seguridad de la Información	• Monitorear el cumplimiento de los lineamientos relacionadas con el buen uso de los equipos de cómputo, así como el manejo de información en áreas seguras.

2. Lineamiento de Escritorio Limpio y Pantalla Limpia

La Universidad FUCS adopta un lineamiento de escritorio limpio para los papeles y un lineamiento de pantalla en las instalaciones de procesamiento de información.

Todos los colaboradores, estudiantes, contratistas y terceros deberán garantizar que la

información impresa, documentos físicos, dispositivos de almacenamiento, equipos de cómputo y demás activos de información permanezcan protegidos cuando no estén siendo utilizados para evitar actos mal intencionados.

Controles

Responsable	Actividades
Todos los Usuarios	• Conservar su escritorio libre de información propia de la Universidad FUCS papeles y conservar la pantalla del equipo de cómputo despejada de archivos office, pdf, correos electrónicos entre otros que contengan información, los cuales podrían ser copiados, utilizados o estar al alcance de terceros o por personal que no tengan autorización para su uso o conocimiento. • Bloquear la pantalla de su equipo de cómputo cuando no esté haciendo uso de este, o cuando por algún motivo deba ausentarse de su puesto de trabajo. • Salir de todas las aplicaciones y apagar los equipos de cómputo que se encuentren en su puesto de trabajo al finalizar sus actividades diarias. • Después de imprimir documentos de carácter CONFIDENCIAL, evitar reutilizarlos. • Antes de desechar documentos que contengan información confidencial, se debe destruir papel que contenga información CONFIDENCIAL.
Seguridad de la Información	• Realizar inspecciones para verificar que se esté cumpliendo el lineamiento de escritorio y pantalla limpia.

VII. SEGURIDAD EN LAS OPERACIONES

1. Asignación de Responsabilidades Operativas.

La División de Desarrollo Tecnológico, es el área encargada de la gestión de los recursos tecnológicos que apoyan los procesos de la Universidad FUCS, el director del área se encarga de asignar las funciones específicas a sus colaboradores, quienes deben garantizar la adecuada operación y administración de los recursos tecnológicos, mantener actualizada la documentación de los procesos operativos en pro de la adecuada ejecución de las actividades.

La División de Desarrollo Tecnológico garantizará una capacidad de procesamiento adecuada en

los sistemas de información de la Universidad FUCS, efectuando las proyecciones de crecimiento y las provisiones necesarias sobre la plataforma tecnológica con una periodicidad definida.

De igual manera debe velar por la eficiencia de los controles establecidos en los procesos operativos relacionados con los recursos tecnológicos, para garantizar así la confidencialidad, integridad y disponibilidad de la información gestionada a nivel institucional.

El profesional de Seguridad de la Información apoyará en las recomendaciones de seguridad sobre las soluciones para la infraestructura tecnológica de la Universidad FUCS.

Los instructivos o manuales de hardware/software deberán detallar como mínimo, las instrucciones para llevar a cabo cada actividad, incluyendo el procesamiento y manejo de la información, las restricciones en el uso de herramientas del sistema, la protección de la información, la gestión de eventos o incidentes de seguridad de la información, y el uso del correo electrónico. y de las aplicaciones de la Universidad FUCS.

Controles

Responsable	Actividades
División de Desarrollo Tecnológico	• Garantizar oportunamente la documentación, actualización y suministro de los procedimientos de operación y gestión de la plataforma tecnológica, a los colaboradores adscritos al área. • Gestionar los recursos necesarios para la implantación de controles, con el propósito de contar con ambientes de desarrollo/calidad, pruebas y producción, teniendo en cuenta los controles requeridos para el paso de información entre los diferentes ambientes. • Garantizar periódicamente la gestión de la demanda permitiendo realizar proyecciones de crecimiento de los recursos administrados (dimensionamiento), que permita asegurar el desempeño y capacidad de la plataforma tecnológica. Incluyendo: procesamiento de memorias volátil, almacenamiento, servicios de impresión, y tráfico de las redes de datos internas y ancho de banda de internet. • Los cambios estructurales que se planteen realizar sobre la plataforma crítica deben ser informados a Seguridad de la Información.
Seguridad de la Información	• Apoyar en las recomendaciones de seguridad sobre las soluciones para la infraestructura tecnológica de la Universidad FUCS.

Supervisores de contratos	• Controlar, gestionar y autorizar adecuadamente todos los cambios en cualquier componente de tecnología, ya sea por requerimientos de usuario, solución de incidentes o actualizaciones, es esencial. Estos cambios deben ser sometidos a una evaluación para identificar los riesgos asociados que podrían afectar la operación.

2. Restricción de equipos personales

La Universidad FUCS define el prohibido uso de equipos personales para uso laborales, teniendo en cuenta que no están parametrizados en aspectos de seguridad y puede afectar la confidencialidad, integridad disponibilidad de los activos que tenga la institución, los colaboradores usaran únicamente los computadores autorizados y dispuestos por la Universidad FUCS esto previniendo fugas de información y accesos no autorizados para evitar compromisos a nivel de información

Controles

Responsable	Actividades
División de Desarrollo Tecnológico	• Brindar acceso y soporte a los equipos autorizados de la Universidad FUCS para su uso correcto • Implementar controles de seguridad a los equipos autorizados a nivel de endpoints y de red
Usuarios	• No almacenar información y datos personales y credenciales correspondiente de la Universidad FUCS. • Cumplir los lineamientos del Manual de Seguridad de información • Generar el uso correcto de los equipos autorizados solo para fines laborales
Seguridad de la Información	• Monitorear que los equipos cumplan con los estándares a nivel de seguridad • Evaluar riesgos que puedan representar con exposición de información

3. Protección frente a software malicioso.

La Universidad FUCS deberá implementar controles preventivos y correctivos a los recursos tecnológicos de la institución deben contar con la adecuada protección de la información adoptando los controles necesarios para evitar que se vea afectada la integridad, confidencialidad

y disponibilidad, ocasionados por software malicioso. Además, se deben realizar campañas de concientización acerca de la cultura de seguridad entre sus colaboradores y personal provisto por terceros acerca de técnicas de hacking amenazas de software malicioso.

La Universidad FUCS cuenta con herramientas de seguridad como antivirus, antispam, antispyware y otras aplicaciones las cuales brindan protección contra código malicioso, con el fin de evitar la divulgación, modificación o daño por virus o eventos maliciosos afectando la operación de la Universidad FUCS.

Controles

Responsable	Actividades
División de Desarrollo Tecnológico	• Proveer, actualizar y licenciar las herramientas tales como; antivirus, antimalware, antispam, antispyware, entre otras, que permitan mitigar el riesgo de posibles eventos o incidentes de seguridad como, por ejemplo; contagio de software malicioso a la plataforma tecnológica de la Universidad FUCS y a los diferentes servicios que se ejecutan en la misma. • Garantizar que la información contenida en la plataforma tecnológica cuente con un escaneo periódico con el software de antivirus, así como la información que se encuentra alojada y transmitida por el servicio de correo electrónico. • A través de sus colaboradores, debe garantizar que la plataforma posea las últimas actualizaciones y aplicación de los correspondientes parches de seguridad, para atenuar las vulnerabilidades de la plataforma tecnológica. • Mantener instalado, actualizado y activo el software antivirus en todo el parque computacional de la Universidad FUCS. • Validar que los equipos autorizados no se ejecute aplicaciones o software no autorizados que afecte los equipos de la Universidad FUCS.

Usuarios	• Deben conservar la configuración del software de seguridad (antivirus, antispyware, antimalware, antispam) instalado por la División de Desarrollo Tecnológico, así como ejecutar escaneo sobre los archivos y/o documentos que provienen del correo electrónico, medios de almacenamiento externos y que son abiertos o ejecutados por primera vez. • Deben verificar la fuente de los archivos adjuntos, descargados o copiados de correos, internet o cualquier medio de almacenamiento, con el fin de garantizar que provienen de fuentes conocidas y seguras, para así mitigar el riesgo por virus o contagio por eventos que afecten la seguridad de la información. • No instalar ningún tipo de software o programa. • Notificar de forma inmediata a Soporte Técnico y a Seguridad de la Información, cuando se detecte o sospeche alguna infección por software malicioso. • Si el usuario desea descargar algún archivo, debe validar que sea un archivo confiable y de un sitio seguro para evitar descarar un virus y afecte la operación de la Universidad FUCS
Seguridad de la Información	• Monitorear mínimo una vez al mes la actualización de las bases de datos del software antivirus y su activación en todo el parque computacional de la Universidad FUCS.

Así mismo, la Universidad FUCS define los siguientes lineamientos que no son permitidos:

- Inactivar o desinstalar las aplicaciones que permiten la Seguridad de los equipos y Sistemas de Información.
- Modificar el código de programación de la infraestructura tecnológica.
- Descargar información de sitios no seguros

4. Copias de Respaldo de la Información.

La Universidad FUCS garantizara la protección de la información institucional que pertenezca a los procesos operativos y de misión crítica de la Universidad FUCS se le debe garantizar, la ejecución de copias de respaldo y almacenamiento de acuerdo con los procedimientos y mecanismos definidos por las áreas propietarias de la información y el apoyo de la División de Desarrollo Tecnológico, unidad encargada de la generación y custodia de los respaldos.

Esto facilitará la recuperación de la información ante incidentes de seguridad, fallas tecnológicas, errores operativos, pérdida de información o ataques de RAMSOMWARE mitigando la perdida de información.

Controles

Responsable	Actividades
División de Desarrollo Tecnológico	• Generar e implantar procedimientos para la generación, almacenamiento y restauración de las copias de respaldo de la información, garantizando su integridad, disponibilidad y confidencialidad. • Realizar pruebas de recuperación de las copias, para así garantizar su confiabilidad al momento de su restauración. • Definir las condiciones de custodia, transmisión y transporte de las copias de respaldo de la información generadas y sobre las que se prevea almacenamiento externo. • Generar campañas que permitan conocer los procedimientos de respaldo de información.
Propietarios de los Activos de Información	• Definir la estrategia en conjunto con la División de Desarrollo Tecnológico para la generación y tiempo de retención de las copias y de los demás activos de información generados por su área.
Usuarios	• Identificar y clasificar la información crítica que debe ser respaldada y almacenada.
Seguridad de la información	• Generar campañas que permitan conocer los procedimientos de respaldo de información. • Monitorear la aplicación de los procedimientos para la generación, almacenamiento y restauración de las copias de respaldo de la información, garantizando su integridad, disponibilidad y confidencialidad.

5. Eventos y Monitoreos a los Recursos Tecnológicos y Sistemas de información.

La Universidad FUCS, a través de la División de Desarrollo Tecnológico debe realizar el monitoreo constante de todos los recursos de la plataforma tecnológica aplicativos de la institución, redes para evitar con el fin de identificar oportunamente fallas operativas, incidentes de seguridad, accesos no autorizados.

Controles

Responsable	Actividades
División de Desarrollo Tecnológico	• Debe establecer e implementar los tipos de eventos que deben registrar los logs o registros de auditoría, y garantizar la obtención de los mismos, tanto de recursos tecnológicos como de sistemas de información. • Debe habilitar los registros o logs de auditoría y actividad de usuarios, así como aplicar los sistemas de monitoreo de la plataforma tecnológica de misión crítica y operacional, teniendo en cuenta los lineamientos y seguimiento establecidos, así como debe velar por su custodia y protección. • Determinar el tiempo de retención de los registros (logs) de recursos tecnológicos y de los sistemas de información de la Universidad FUCS para efectos de auditoría. • Monitorear disponibilidad de los servicios tecnológicos
Desarrolladores, consultores, analistas entre otros (Internos y Externos)	• Informar sobre eventos de los sistemas de información y/o plataforma tecnológica relacionados con interrupciones, acceso, modificación de acuerdo con los lineamientos establecidos por la División de Desarrollo Tecnológico.
Seguridad de la Información.	• Monitorear la gestión de usuarios en los Sistemas de Información. • Verificar el reporte de análisis de vulnerabilidades realizado por la División de Desarrollo Tecnológico y/o el tercero contratado; y verificar la ejecución de los planes de remediación.

6. Seguridad Para los Equipos Institucionales.

La Universidad FUCS debe proveer los recursos necesarios que aseguren la mitigación de riesgos para prevenir la pérdida, daño, robo o puesta en peligro de los activos de la infraestructura tecnológica de la institución, así mismo, debe garantizar que se realicen seguimientos de control que demuestren la custodia de estos mismos.

Controles

Responsable	Actividades
División de Desarrollo Tecnológico	• Implementar estrategias y desarrollar mecanismos que garanticen la seguridad de la información sobre la información contenida en los recursos de la infraestructura tecnológica, dentro y fuera de la institución (en caso de almacenamientos externos). • Asegurar la realización de los mantenimientos preventivos y correctivos de los activos de la infraestructura tecnológica de la Universidad FUCS. • Definir, implementar y asegurar el cumplimiento de los estándares de seguridad/configuración fiable para los equipos asignados a los empleados de la Universidad FUCS. • Establecer las condiciones de cumplimiento que deben tener los equipos de cómputo de personal externo y que se encuentren conectados a la red de datos de la Universidad FUCS, así como exigir el estricto cumplimiento antes de dar acceso a la red de la institución. • Establecer zonas aisladas y/o accesos de red restringidos para los equipos en los que se efectúan operaciones financieras o información sensible para evitar accesos no autorizados. • Establecer y aplicar lineamientos para una disposición final segura o traslado de usuarios, de los equipos de cómputo de los colaboradores de la Universidad FUCS. • Verificar periódicamente los equipos de cómputo de la Universidad FUCS, especialmente aquellos que se encuentran ubicados en áreas sensibles. • Realizar la asignación de recursos tecnológicos. • Acompañar los movimientos de recursos tecnológicos.
Seguridad de la Información	• Monitorear periódicamente el cumplimiento de las configuraciones en los equipos de cómputo, con base en el estándar de seguridad definido.
Oficina de Activos Fijos	• Validar la aprobación de entrada y salida de las instalaciones de la Universidad FUCS de equipos de cómputo y otros recursos de tecnología pertenecientes a la institución, verificando la autorización documentada y aprobada y además contar con sus respectivas pólizas según corresponda.
Servicios administrativos	• Monitorear que la empresa de seguridad revise los accesos físicos en horas no hábiles a las áreas donde se procesa información.

Usuarios	• No realizar movimientos de equipos tecnológicos. • Acoger las instrucciones técnicas proporcionadas por la División de Desarrollo Tecnológico cuando se asignen puestos de trabajo, equipos móviles y/o Sistemas de Información a personal provisto por terceras partes. • Reportar a Soporte Técnico para su respectiva gestión y solución las fallas o problemas de hardware o software que se presenten sobre los equipos de cómputo o algún recurso tecnológico que sea de propiedad de la Universidad FUCS. No está permitido que el usuario intente solucionar el problema en los puestos de trabajo, equipos móviles y/o Sistemas de Información. Estas actividades sólo pueden ser realizadas por los colaboradores de la División de Desarrollo Tecnológico, o en determinados casos por personal de terceras partes autorizado por dicha área. • Bloquear la sesión de red (usuarios) al levantarse de su puesto de trabajo, así como apagar los equipos en horarios no laborales.

7. Uso Responsable de Tecnologías de Inteligencia Artificial

La Universidad FUCS promueve y regula el uso responsable y seguro de las herramientas de inteligencia artificial, garantizando la protección de la información institucional, los datos personales, la propiedad intelectual y el cumplimiento de la normativa y de las disposiciones institucionales aplicables.

La Universidad FUCS gestionará los riesgos de seguridad, privacidad, confidencialidad, integridad, propiedad intelectual y continuidad asociados al uso, adquisición, desarrollo e integración de sistemas y herramientas de inteligencia artificial.

Su utilización deberá responder a una finalidad académica, investigativa o administrativa legítima, realizarse mediante herramientas autorizadas y mantener la supervisión y responsabilidad de las personas competentes.

Estos lineamientos se aplicarán a los sistemas, herramientas, modelos, plataformas, funcionalidades, extensiones, interfaces y servicios de inteligencia artificial que sean adquiridos, desarrollados, integrados o utilizados por la Universidad, así como a los datos de entrada, instrucciones, registros y resultados generados mediante estos. Igualmente aplicará a todas las herramientas de inteligencia artificial de uso público, respecto del uso que los usuarios realicen en su interacción usando o explotando de cualquier forma, información institucional de la Universidad FUCS, para la Universidad FUCS o para terceros en nombre de la Universidad FUCS.

Criterios mínimos

7.1. Autorización e inventario: La Universidad FUCS contará con un registro de las herramientas de IA autorizadas, su finalidad, área responsable, proveedor, tipo de información que pueden procesar y condiciones de uso.

7.2. Clasificación de usos: La Universidad FUCS clasificará el tipo de uso que podrá darse a las herramientas de inteligencia artificial teniendo en cuenta las siguientes categorías:

- Uso general: consultas y generación de borradores con información pública, ficticia, anonimizada o de libre circulación.
- Uso institucional restringido: tratamiento de información interna mediante herramientas previamente evaluadas y autorizadas.
- Uso prohibido: incorporación de información reservada, datos sensibles, credenciales, secretos, bases de datos o información institucional en herramientas no autorizadas.

7.3. Evaluación proporcional del riesgo.

- Los proyectos de IA deberán evaluarse antes de su adquisición, desarrollo o implementación, considerando la información tratada, los efectos sobre las personas, la dependencia tecnológica, la intervención de terceros y la necesidad de supervisión humana.
- Los proyectos piloto que incorporen inteligencia artificial deberán documentar su finalidad, alcance, responsable, fuentes de información, riesgos, controles, mecanismos de validación humana y condiciones para su suspensión, ajuste o retiro definitivo.
- Antes de adquirir, desarrollar o integrar una solución de inteligencia artificial, la Universidad evaluará sus condiciones de seguridad, privacidad, confidencialidad, propiedad intelectual, acceso, conservación de información, interoperabilidad, soporte, continuidad y gestión de cambios.
- Las soluciones de inteligencia artificial deberán ser probadas con información ficticia, anonimizada, sintética o expresamente autorizada, antes de su uso con información institucional o de su incorporación a procesos productivos.

7.4. Validación humana y trazabilidad. Todo resultado utilizado para producir comunicaciones, informes, actuaciones o decisiones institucionales debe ser revisado por una persona responsable. Cuando el resultado pueda producir efectos académicos, administrativos, jurídicos, laborales, financieros o sobre terceros, deberá conservarse evidencia de la herramienta utilizada, su finalidad, el responsable de la validación y la versión final aprobada, de acuerdo con las directrices institucionales de gestión documental.

7.5. Gestión de riesgos. La Universidad FUCS gestionará los riesgos derivados del uso de inteligencia artificial mediante controles de autorización, clasificación de la información, acceso, validación humana, trazabilidad, contratación, monitoreo y respuesta a incidentes.

7.6. Gestión de incidentes. Los usuarios deberán suspender la actividad o utilización afectada y reportar inmediatamente a Seguridad de la Información y a la División de Desarrollo Tecnológico cualquier evento relacionado con exposición o divulgación inadecuada de información, accesos indebidos, uso no autorizado de credenciales, suplantación, alteración de contenidos, generación de resultados fraudulentos o manifiestamente incorrectos utilizados institucionalmente, fallas de integridad, disponibilidad o cualquier funcionamiento anómalo que pueda afectar a la Universidad o a terceros, en los servicios dispuestos por la Institución. La continuidad o restablecimiento del uso estará sujeto a la evaluación y medidas adoptadas por las instancias correspondientes.

7.7. Activos de información. Las herramientas de inteligencia artificial, sus integraciones, configuraciones, datos de entrada, registros y resultados que tengan valor para la Universidad FUCS deberán identificarse y gestionarse como activos de información, de acuerdo con su propietario, clasificación, finalidad y ciclo de vida.

7.8. Capacitación. La Universidad FUCS incluirá dentro de sus actividades de inducción, capacitación y sensibilización continua y permanente, contenidos que permitan desarrollar las competencias de estudiantes, docentes y personal administrativo para el uso crítico, ético y seguro de las herramientas de inteligencia artificial.

7.9. Restricciones al uso de información institucional para entrenamiento de modelos. Los proveedores de servicios de inteligencia artificial no podrán utilizar información de la Universidad FUCS para fines propios, entrenamiento de modelos, perfilamiento, publicidad o mejora general de sus servicios. Excepcionalmente, podrá autorizarse el uso de información pública, anonimizada o expresamente habilitada para dicha finalidad, previa evaluación jurídica, técnica y de seguridad y autorización del Comité de Seguridad de la Información. En ningún caso podrá autorizarse para estos fines el uso de datos personales sensibles, información reservada o confidencial, credenciales, secretos, bases de datos institucionales ni información protegida por derechos de terceros.

7.10. Uso y explotación de herramientas de inteligencia artificial.

7.10.1. El uso de inteligencia artificial por parte de los estudiantes y docentes se sujetará a lo establecido en los reglamentos internos, las directrices y reglas de gobernanza e integridad académica establecidas por la Universidad FUCS, así como a las instrucciones impartidas para cada actividad.

7.10.2. Los usuarios no podrán utilizar herramientas de inteligencia artificial de cualquier manera que atente contra el uso ético y responsable.

7.10.3. Los usuarios no deberán, cargar, procesar o divulgar información confidencial de la Universidad FUCS, información financiera institucional,

información sensible bajo custodia de la Universidad FUCS, información reservada institucional o datos personales cuyo responsable o encargado sea la Universidad FUCS, en herramientas de Inteligencia Artificial no autorizadas por la Universidad FUCS, o para fines no autorizados previamente por la Universidad FUCS.

7.10.4. Los usuarios no deberán compartir credenciales institucionales de acceso, cadenas de conexión, instancias, direcciones IP, ni cualquier otro dato o metodología que permita el acceso directo o remoto a plataformas o repositorios de información institucional, en herramientas de Inteligencia Artificial.

7.10.5. El acceso a herramientas institucionales de inteligencia artificial deberá gestionarse mediante cuentas individualizadas, perfiles autorizados y, cuando sea técnicamente posible, autenticación institucional y registro de actividad. Las credenciales, llaves API y demás mecanismos de acceso serán personales o asignados formalmente por la División de Desarrollo Tecnológico y no podrán compartirse.

7.10.6. Los usuarios no podrán conectar cuentas institucionales, repositorios, correos electrónicos, servicios en la nube o sistemas de información de la Universidad a herramientas de inteligencia artificial, complementos o extensiones no autorizadas.

7.10.7. La instalación de asistentes, extensiones o complementos con funcionalidades de inteligencia artificial en navegadores, correos, plataformas educativas o sistemas institucionales requerirá autorización previa de la División de Desarrollo Tecnológico, mediante un caso gestionado por mesa de ayuda.

7.10.8. El uso de inteligencia artificial por cualquier usuario de la Universidad FUCS, deberá respetar los derechos de autor, la propiedad intelectual, la confidencialidad de los trabajos académicos y de investigación y los derechos de terceros. La información ingresada en una herramienta de inteligencia artificial externa será considerada una transferencia o comunicación de información a un tercero y deberá cumplir los controles aplicables según su clasificación.

7.10.9. El tratamiento de datos personales mediante herramientas de inteligencia artificial deberá responder a una finalidad autorizada, aplicar los principios de necesidad, finalidad, acceso restringido y seguridad, y contar con las autorizaciones, condiciones contractuales y medidas técnicas que correspondan.

7.10.10. Los datos personales sensibles, de menores de edad, o relacionados con salud, biométricos, genéticos y demás bajo dicha categoría, únicamente podrán ser procesados mediante herramientas expresamente autorizadas para esa categoría de información y para la finalidad específica

correspondiente, cuando su utilización sea necesaria y se hayan implementado las condiciones jurídicas, contractuales, técnicas y de seguridad aplicables. Su tratamiento estará prohibido en los demás casos.

Controles

Responsable	Actividades
División de Desarrollo Tecnológico	• Definir lineamientos técnicos para el uso seguro de herramientas de Inteligencia Artificial dentro de la institución. • Evaluar las condiciones técnicas, de acceso, integración, almacenamiento, transmisión, trazabilidad, disponibilidad y respuesta a incidentes de las herramientas de inteligencia artificial propuestas para uso institucional. • Validar los riegos por uso de las herramientas de inteligencia artificial que sean propuestas por la comunidad. • Validar las herramientas de inteligencia artificial adecuadas para uso institucional
Usuarios	• Utilizar exclusivamente las herramientas de inteligencia artificial autorizadas, conforme a la clasificación de usos que establezca la Universidad, y previo cumplimiento de lo establecido en los reglamentos internos, el presente manual, las directrices y reglas de gobernanza e integridad académica establecidas, así como a las instrucciones impartidas para cada actividad.
Seguridad de la Información	• Generar campañas de sensibilización sobre uso ético y responsable, así como riesgos asociados al uso de herramientas de Inteligencia Artificial. • Generar recomendaciones sobre el uso de inteligencia artificial • Llevar el inventario de herramientas de inteligencia artificial autorizadas por la Universidad FUCS, dentro del cual se indique, entre otros, su finalidad, área responsable, proveedor, tipo de información que pueden procesar y condiciones de uso. • Efectuar el monitoreo a las herramientas de inteligencia artificial autorizadas.
Comité de Seguridad de la Información	• Aprobar los criterios técnicos y de seguridad para la autorización de herramientas de inteligencia artificial. • Conocer los usos institucionales de mayor riesgo y proponer controles para mitigación, implementación y seguimiento. • Realizar seguimiento al monitoreo ejecutado a las herramientas de inteligencia artificial autorizadas.
División Jurídica	• Evaluar, cuando corresponda, las condiciones contractuales del proveedor de una herramienta de inteligencia artificial autorizada, a fin de verificar el cumplimiento en materia de tratamiento de

	datos personales, confidencialidad, propiedad intelectual, transferencia de información y responsabilidad del proveedor.
Líderes de área	• Definir la finalidad y necesidad del uso de herramientas de inteligencia artificial en sus procesos internos. • Identificar y clasificar la información institucional que será tratada mediante el uso de herramientas de inteligencia artificial. • Garantizar la revisión y validación de los resultados en su equipo de trabajo, antes de su utilización institucional. • Conservar las evidencias requeridas de acuerdo con la relevancia y nivel de riesgo del uso.

VIII. SEGURIDAD EN LAS COMUNICACIONES.

1. Gestión y Aseguramiento de las Redes de Datos.

La Universidad FUCS provee, a través de la División de Desarrollo Tecnológico, los mecanismos de control necesarios para garantizar la operación de las redes de los servicios tecnológicos; debe proveer también, los mecanismos de seguridad que protejan la integridad, disponibilidad y la confidencialidad de la información que utilizan las redes de datos institucionales.

Controles

Responsable	Actividades
División de Desarrollo Tecnológico	• Adoptar medidas para garantizar la estabilidad de los recursos y servicios de red de la Universidad FUCS. • Definir y aplicar los controles necesarios para mitigar los riesgos de seguridad de la información que viajan a través de las de las redes de datos de la Universidad FUCS. • Realizar la segmentación de la red de datos, de acuerdo con la clasificación de usuarios, tipo de datos, servicios y demás características que se determine según criterios de la institución. • Identificar y negociar con los proveedores de servicio de red externos, los respectivos acuerdos de servicio necesarios para la operación de la institución. • Realizar endurecimiento de las políticas para garantizar la seguridad y la configuración de los dispositivos, de acuerdo con los estándares de buenas prácticas para la plataforma tecnológica de la Universidad FUCS • Habilitar únicamente los servicios, protocolos y puertos de comunicación necesarios para la operación de las redes de datos FUCS y bloquear los puertos o servicios no necesarios

	para evitar robo de información y/o ataques cibernéticos. • Instalar plataformas de protección entre las redes internas de la Universidad FUCS y redes externas que representen una amenaza para la plataforma tecnológica de la Universidad FUCS. • Documentar y mantener la configuración de la Universidad FUCS.

2. Seguridad y uso del Correo Electrónico.

El servicio de correo electrónico es una herramienta muy importante para la comunicación digital de la institución, la cual debe garantizar confidencialidad, integridad, disponibilidad y autenticidad de su contenido para el desarrollo de las actividades entre colaboradores y/o personal externo que hacen uso de este medio.

La Universidad FUCS promoverá el uso seguro del correo electrónico institucional mediante mecanismos tecnológicos, campañas de concientización y monitoreo continuo que permitan reducir el riesgo asociado a ataques de ingeniería social y compromiso de credenciales institucionales.

Controles

Responsable	Actividades
División de Desarrollo Tecnológico	• Generar y divulgar el instructivo y las directrices para la gestión de cuentas de correo electrónico. • Diseñar e implementar la estrategia que proporcione un ambiente seguro y controlado que incluya los mecanismos de protección y detección para el buen funcionamiento de la plataforma de correo electrónico.
Usuarios	• Verificar la legitimidad de los correos electrónicos antes de abrir enlaces, descargar archivos adjuntos o suministrar información institucional. • No compartir credenciales institucionales mediante correos electrónicos o sitios no autorizados. • Reportar inmediatamente correos sospechosos, intentos de phishing o mensajes fraudulentos a Seguridad de la Información o Soporte Técnico soporte@fucsalud.edu.co o al correo seguridaddelainformacion@fucsalud.edu.co. • No realizar el envío de cadenas de mensajes que contengan información no institucional (político, religioso, comercial, contenido discriminatorio, pornografía, etc.) • Cumplir el uso individual y responsable de la cuenta de correo

	electrónico asignada por la Universidad FUCS, para el desarrollo de las funciones asignadas por la institución y no hacer uso del correo institucional para actividades personales. • Usar el correo con fines únicamente laborales, con el fin de evitar filtración de información y prevenir ataques de correos sospechosos (registro a redes sociales y demás)
Seguridad de la Información	• Realizar campañas de sensibilización y concientización sobre riesgos asociados a phishing, ingeniería social y fraude digital. • Monitorear eventos e incidentes relacionados con correos electrónicos sospechosos o intentos de suplantación de identidad. • Gestionar el análisis y seguimiento de incidentes asociados a compromiso de cuentas institucionales o correos maliciosos.

3. Seguridad a nivel de almacenamiento nube

La Universidad FUCS deberá establecer medidas de seguridad a nivel de almacenamiento de la nube esto con el fin de garantizar el uso adecuado para el almacenamiento de información crítica y evitar su divulgación no autorizada y accesos no autorizados.

Controles

Responsable	Actividades
División de Desarrollo Tecnológico	• Garantizar la disponibilidad del almacenamiento de la nube • Configurar controles de acceso, y autenticación sobre los servicios de almacenamiento institucional solo con fines institucionales. • Valida métodos seguros de autenticación
Usuarios	• No utilizar cuentas personales de almacenamiento en la nube para almacenar o compartir iinformación Pública Reservada. • Validar permisos y accesos para que no se comprometa la información • No compartir los archivos que son de manera confidencial de manera pública o de fácil acceso
Seguridad de la Información	• Validar y monitorear riesgos relacionados con fuga de información inadecuada de archivos en plataformas de almacenamiento en la nube • generar campañas de sensibilización sobre el uso seguro de servicios de almacenamiento y uso compartido de información. • Brindar recomendaciones para la protección de información

4. Uso Adecuado de Internet

La Universidad FUCS reconoce la importancia del uso de Internet como apoyo para el desempeño de labores, así como soporte al proceso de enseñanza y aprendizaje.

Controles

Responsable	Actividades
División de Desarrollo Tecnológico	• Proporcionar la prestación segura del servicio de Internet, mediante la implementación, administración y mantenimiento, conforme a los perfiles de acceso definidos. • Diseñar e implementar el plan de continuidad y/o recuperación del servicio de internet en caso requerido, así como realizar el monitoreo constante del servicio. • Establecer e implementar controles que garanticen el óptimo funcionamiento del servicio de internet (red interna), que restringa el acceso y/o descarga de software, malware o sitios que representen una amenaza para la Seguridad de la Información. • Mantener los registros de la navegación y acceso de los usuarios a internet, que permitan generar reportes sobre el uso de este servicio. • Generar campañas con el apoyo de impresos y publicaciones, para concientizar sobre el uso adecuado del servicio de internet
Usuarios	• Hacer uso adecuado del servicio de internet de acuerdo con las actividades que se desarrollan. Está prohibido la descarga e instalación de software no autorizado en las estaciones de trabajo o dispositivos móviles institucionales.
Seguridad de la Información	• Realizar monitoreo de acceso a páginas prohibidas de internet, que permitan evidenciar el uso inapropiado del servicio. • Realizar monitoreo sobre el uso de internet y verificar las configuraciones de restricciones definidas.

5. Intercambio de Información.

La Universidad FUCS garantiza que cuando se transfiera información hacia otras entidades utilizando canales autorizados por la Universidad FUCS (medios removibles, canales de internet, medio impreso), la información debe ser protegida cumpliendo los procedimientos y controles establecidos de acuerdo con su clasificación. Se deben establecer acuerdos de confidencialidad, y de intercambio de información con los terceros involucrados en el proceso.

Controles

Responsable	Actividades
División Jurídica	• Definir los modelos de los acuerdos de confidencialidad e intercambio de información con terceros, en donde estén descritos tanto los acuerdos como las penalidades por incumplimiento, esta labor debe ser coordinada con Seguridad de la Información. • Elaborar y/o revisar aquellos contratos que se realicen con terceros y que incluyan acuerdos de confidencialidad o de intercambio de información, especificando las condiciones contractuales legales para los terceros en caso de divulgación no autorizada de la información entregada por la Universidad FUCS. • Definir los procedimientos, servicios y herramientas para proteger con controles la información transmitida a los terceros que tienen relación con la Universidad FUCS.
División de Desarrollo Tecnológico	• Definir e implementar los procedimientos, servicios y herramientas para proteger con controles la información transmitida a los terceros que tienen relación con la Universidad FUCS. • Vigilar que el intercambio de información de la Universidad FUCS con externos, se encuentren alineadas con el Manual de Seguridad de la Información.
Propietarios de los Activos de Información	• Proteger los activos de información contra divulgación inapropiada, velando por el cumplimiento de cláusulas y/o acuerdos definidos por la Universidad FUCS. • Registrar el intercambio de información, en donde se especifique el tipo de información intercambiada, así como los datos del emisor, del receptor y fecha de entrega/recepción. • Verificar que las terceras partes realicen el procedimiento de destrucción de la información, una vez no se requiera para su función.
Gestión Documental	• Definir los procedimientos, servicios y herramientas para proteger con controles la información transmitida a los terceros que tienen relación con la Universidad FUCS. • Acoger los procedimientos de intercambio de información con terceros en medio físico o digital, así como garantizar la restricción de acceso al personal no autorizado, para evitar la divulgación no autorizada, destrucción, alteración y/o pérdida de la información.
Terceros con quienes se intercambia	• Dar manejo adecuado a la información que intercambia con la Universidad FUCS cumpliendo con procedimientos, controles, condiciones contractuales establecidos por la Universidad FUCS

información de la Universidad FUCS	para el manejo de la información, así como realizar de manera segura, la destrucción o eliminación de la información suministrada cuando ya no se requiera. • Garantizar que la información que se use sea con fines laborales e institucionales
Seguridad de la Información	• Definir los procedimientos, servicios y herramientas para proteger con controles la información transmitida a los terceros que tienen relación con la Universidad FUCS.
Usuarios	• Hacer uso de medios adecuados para enviar o recibir información confidencial, no se debe compartir la información, sin previo contrato de transmisión de datos, no se debe utilizar el correo electrónico personal y/o medios no autorizados por la Universidad FUCS para enviar o recibir información confidencial de la Universidad FUCS.

IX. CONTROL DE ACCESO

1. Acceso a Redes y Recursos de Red

La División de Desarrollo Tecnológico, como responsable de las redes y los recursos que las conforman, debe garantizar que estas redes cuenten con la protección y actualización adecuadas para evitar accesos no autorizados, con la aplicación de mecanismos de control de acceso lógico.

Controles

Responsable	Actividades
División de Desarrollo Tecnológico	• Establecer e implementar el procedimiento de autorización y control de acceso a las redes y recursos tecnológicos de la Universidad FUCS, con el fin de proteger el ingreso indebido de terceros. • Establecer e implementar controles de autenticación y autenticidad de los usuarios internos y externos a las redes y/o recursos de red de la Universidad FUCS. • Se debe tratar las redes inalámbricas "WIFI" como redes externas y separarlas de las redes internas, para garantizar de esta manera el cumplimiento de los principios de Seguridad de la Información de la Universidad FUCS. • Disponer métodos de identificación automática para los equipos

	en la red, dando cumplimiento con la autenticación de conexiones, desde segmentos de red específicos, hacia las plataformas donde operan los sistemas de información.
Seguridad de la Información	• Realizar revisiones periódicas de los accesos de los usuarios internos y externos verificando los controles que garanticen que sólo los usuarios que se encuentren autorizados están activos en las plataformas tecnológicas.
Todos los Usuarios	• Cumplir con el procedimiento de creación de usuarios, así como aceptar el acuerdo de confidencialidad, garantizar que los equipos con los que se acceden a la red cumplan con los requisitos o controles necesarios para que no representen una amenaza para la plataforma tecnológica de la Universidad FUCS. • Los visitantes que requieran conectarse a la red local cableada pueden hacerlo con acceso limitado (solo conexión a internet), según lo establecido por la División de Desarrollo Tecnológico. En caso de requerir acceso a servicios adicionales, debe contar con la autorización del líder de proceso, quien debe gestionar el requerimiento mediante solicitud registrada en Soporte Técnico. El acceso a la red wifi para visitantes se realiza a través de la red definida para tal fin y con uso de la clave establecida que será suministrada por el líder de proceso y/o la División de Desarrollo Tecnológico.

2. Gestión de identidades y accesos IAM

La Universidad FUCS establecerá controles de accesos y de privilegios para el acceso recursos tecnológicos, sistemas de información y redes todo limitado a los controles establecidos.

Los accesos otorgados a usuarios internos y externos deberán encontrarse debidamente autorizados, controlados y revisados periódicamente para prevenir accesos no autorizados y proteger la confidencialidad, integridad y disponibilidad de la información institucional.

Controles

Responsable	Actividades
División de Desarrollo Tecnológico	● Establecer e implementar el procedimiento formal para la administración del acceso lógico de los usuarios en las redes de datos, sistemas de información de la institución y demás recursos tecnológicos. ● Verificar que las solicitudes de creación, modificación o bloqueo de cuentas de usuarios cuenten con la respectiva aprobación de los líderes de proceso. ● Establecer el proceso para la eliminación y reasignación de los permisos de acceso dados en los recursos o Sistemas de Información para garantizar una gestión oportuna de las novedades de usuarios de acuerdo con la información suministrada por la División de Gestión del Talento Humano. ● Garantizar la inhabilitación o eliminación de los usuarios creados o asignados por defecto en los diferentes recursos de la plataforma tecnológica de la institución. ● Definir lineamientos de utilización de Internet para los usuarios (estudiantes/ colaboradores/directivos/terceros), que permitan optimizar y proteger el acceso a internet de los usuarios. ● Participar en la definición de controles para los recursos informáticos como sistemas operativos, servicios de red, enrutadores, etc. y realizar su validación periódicamente. ● Controlar la asignación de privilegios a roles y a usuarios, establecidos por el Comité de Seguridad de la Información. ● Garantizar que los aplicativos soliciten contraseñas con una longitud mínima de 8 caracteres que contengan: números, letras mayúsculas, letras minúsculas y caracteres especiales o símbolos. ● Garantizar que los aplicativos se bloqueen después de 3 intentos fallidos y solo podrá ser desbloqueado por el administrador. ● Administrar el ciclo de vida de las cuentas de usuario institucionales, garantizando la creación, modificación, suspensión y eliminación de accesos conforme a las autorizaciones establecidas. ● Mantener trazabilidad de creación, modificación y eliminación de usuarios.
Seguridad de la Información	● Establecer los perfiles de usuario (roles, funcionalidades y permisos), junto con los líderes de los activos de información y el Comité de Seguridad de la Información. ● Realizar monitoreo a los accesos lógicos, creación, modificación o bloqueo de cuentas de usuarios para validar que cuenten con la respectiva aprobación de los líderes de proceso.

	● Validar el cumplimiento de los procedimientos de creación de usuarios, modificación y eliminación
Líderes de Procesos	● Verificar y ratificar con una periodicidad semestral o cuando se requiera, las autorizaciones de acceso sobre los recursos tecnológicos y sistemas de información a cargo de cada área. ● Solicitar y autorizar las novedades de gestión de usuarios de los colaboradores que pertenecen a cada área cumpliendo los procesos y formatos de solicitud vigentes.
Comité de Seguridad de la Información.	● Definir las actividades pertinentes para la administración de roles y perfiles.
División de Gestión del Talento Humano	● Informar oportunamente, de acuerdo con el procedimiento institucional, a la División de Desarrollo Tecnológico y a Seguridad de la Información las novedades relacionadas con el ciclo de vida del personal (ingresos, cambios de cargo, traslados, licencias, suspensiones, vacaciones, retiros o terminación del vínculo), con el fin de gestionar la creación, modificación, suspensión o eliminación de cuentas, accesos y privilegios de los usuarios.

3. Responsabilidades de Acceso de los Usuarios.

Los usuarios con accesos otorgados deben realizar el uso adecuado y responsable de los recursos tecnológicos y de los sistemas de información de la Universidad FUCS protegiendo la información a la que tienen acceso.

Controles

Responsable	Actividades
Todos los Usuarios	● Responder por las acciones realizadas en los sistemas de la plataforma tecnológica de la Universidad FUCS, así como por el buen uso de las credenciales asignadas para dichos accesos. ● Los colaboradores y personal provisto por terceras partes que, por la naturaleza de su función, tengan acceso a los sistemas de la plataforma tecnológica de la Universidad FUCS, deben acogerse a los lineamientos establecidos para la configuración de cuentas de usuario y contraseñas implementados por la Universidad FUCS.

4. Uso de Altos Privilegios y Utilitarios de Administración.

La División de Desarrollo Tecnológico es la encargada de velar porque la operación y administración de los recursos de la plataforma tecnológica se encuentren en condiciones controladas y seguras; permitiendo así la trazabilidad de las acciones realizadas por usuarios administradores, responsables por los más altos privilegios sobre las plataformas y servicios.

Controles

Responsable	Actividades
División de Desarrollo Tecnológico	• Otorgar privilegios y cuentas separadas para la administración de recursos tecnológicos, solamente a colaboradores idóneos y responsables de estas funciones. • Garantizar el acceso sólo de consulta a sistemas de información en ambientes productivos a los administradores de los recursos tecnológicos. • Definir y evaluar las conexiones seguras remotas sobre los recursos de la plataforma tecnológica institucional y por ningún motivo permitir que los usuarios finales tengan accesos privilegiados sobre los sistemas de asignación. • Realizar el aseguramiento de los recursos mediante la inhabilitación de funcionalidades o servicios no utilizados. Establecer el mínimo de funcionalidades, servicios y utilitarios requeridos. • Generar y revisar periódicamente los listados de cuentas con privilegios sobre los recursos de la plataforma tecnológica. • Restringir el acceso a programas utilitarios solo a los perfiles administradores en los equipos de cómputo.
Seguridad de la Información	• Revisar con una periodicidad definida el registro de actividad de usuarios y privilegiados sobre los servicios de la plataforma tecnológica.

5. Control de Accesos a Sistemas y Aplicativos.

Los líderes de proceso como propietarios de los sistemas de información y aplicativos de apoyo, serán los encargados de velar por la gestión de novedades de acceso a los sistemas o aplicativos. La División de Desarrollo Tecnológico, como responsable de la gestión de los aplicativos, garantiza que el control de acceso lógico cuente con controles que eviten accesos no autorizados. Por otra parte, debe propender por que se adopten buenas prácticas de desarrollo de software que permita implementar control de acceso lógico de los sistemas de información.

Controles

Responsable	Actividades
Propietarios de los Activos de Información	• Autorizar de acuerdo con los procedimientos los accesos según los perfiles establecidos y necesidades de uso, a los sistemas de información o aplicativos. • Establecer niveles de autorización y controles para: usuarios que tienen permiso de ingreso a cargue o actualización de datos dentro de los aplicativos, usuarios que tienen permiso para consulta de la información, indicando nivel, mínimos privilegios, restricciones de acceso únicamente a las funcionalidades y datos requeridos para proteger el acceso a los sistemas y aplicativos de la Universidad FUCS. • Verificar, antes de comunicar datos personales a padres, acudientes, empleadores u otros terceros, la autorización previa y expresa del titular para acceder a su información personal.
División de Desarrollo Tecnológico	• Debe establecer los controles de acceso a los ambientes productivos de los aplicativos, así mismo, debe garantizar que los desarrolladores internos o externos, cuenten con acceso limitado y controlado tanto a los datos como a toda información que se encuentre en los ambientes de producción. • Suministrar el repositorio de archivos con acceso controlado y definición de privilegios para almacenar el código fuente de los Sistemas de información propios.
Desarrolladores (Internos y Externos	• Implementar módulos de autenticación preferiblemente integrados con la base de datos de usuarios, en los sistemas de información desarrollados de acuerdo con la clasificación de la información. • Adoptar controles de integridad sobre las contraseñas, evitando el almacenamiento y/o recordación de las mismas. • Evitar que durante el proceso de autenticación se muestren errores del sistema revelando información que permita realizar ataques y en su lugar se deben mostrar mensajes personalizados de acuerdo con la falla en la autenticación incluyendo la inhabilitación de cuentas por número de intentos fallido-definidos. • Implementar medidas que restrinjan el acceso a otros recursos internos donde se alojan las aplicaciones, así como garantizar que se valida la autenticación en cada recurso con información sensible. • Todos los sistemas de información crítica de la Universidad FUCS deben tener filtros y controles de acceso, con el fin de tener segregación de funciones de usuarios y administradores.
Usuarios	• Los usuarios que tengan acceso a la infraestructura tecnológica y/o los sistemas de información, deben tener una definición clara de roles y responsabilidades, así como, los niveles de acceso y

	funcionalidades, para mitigar el riesgo de uso no autorizado o modificaciones sobre los activos de información de la Universidad FUCS. • Para los distintos aplicativos, sistemas de información y medios, los propietarios deben definir qué información sensible puede ser eliminada y tener soporte de la eliminación de dicha información, como es el caso de los datos personales, datos sensibles o financieros, cuando estos ya no son requeridos. Para lo anterior, es necesario contar con el acompañamiento de la División Jurídica y Seguridad de la Información.
Seguridad de la Información	• Realizar verificaciones periódicas y aleatorias a las actividades ejecutadas con el usuario administrador de los sistemas de información críticos de la Universidad FUCS. • Monitorear periódicamente la definición de perfiles y asignación de privilegios a los usuarios que acceden en los sistemas de información, así mismo, notificar al Comité de Seguridad de la Información.

6. Controles criptográficos.

La Universidad FUCS garantizará el cifrado de la información, en cualquier tipo de almacenamiento de información clasificada, como pública reservada o pública clasificada.

Controles

Responsable	Actividades
División de Desarrollo Tecnológico	• Gestionar los recursos necesarios para la adquisición y mantenimiento del sistema de cifrado que la institución requiere para la protección de la información. • Garantizar el cifrado de la información en cualquier tipo de almacenamiento o transmisión de información clasificada como reservada con el propósito de proteger sus principios de seguridad. • Desarrollar y establecer el procedimiento y los estándares para la gestión de llaves de cifrado y controles criptográficos.
Desarrolladores (Internos o Externos)	• Adoptar los controles de cifrado de la información pública reservada o pública clasificada y seguir los estándares establecidos por la División de Desarrollo Tecnológico.

7. Uso de Conexiones Remotas.

La División de Desarrollo Tecnológico evaluará y autorizará de acuerdo con la necesidad, el uso de conexiones remotas a la plataforma tecnológica de la Universidad FUCS, así mismo,

suministrará y garantizará que estas conexiones se realicen de manera segura mediante el uso de las herramientas y controles necesarios.

Controles

Responsable	Actividades
División de Desarrollo Tecnológico	• Implementar los controles para el uso de conexiones remotas hacia la plataforma tecnológica de la Universidad FUCS, así como su monitoreo permanente. • Autorizar sólo a determinados colaboradores y por periodos de tiempo limitados, previo análisis de riesgo, el uso de conexión remota.
Todos los Usuarios	• Registrar la solicitud de conexión remota en la cuenta de Soporte Técnico, y luego de la aprobación cumplir con las condiciones de uso definidas para dicha conexión. • Garantizar que la conexión remota se realice mediante el uso de equipos de cómputo privados y/o personales que cuenten con los requisitos mínimos de seguridad, como lo son software antivirus y sistema operativo actualizados.

8. Uso de multifactor de autenticación MFA

La División de Desarrollo Tecnológico mantendrá su buen uso garantizando que todas las cuentas de correo electrónico contengan MFA esto para garantizar una doble validación para accesos a las cuentas corporativas, garantizando los accesos de manera segura.

Controles

Responsable	Actividades
División de Desarrollo Tecnológico	• Implementar y administrar mecanismos de autenticación multifactor (MFA) en las cuentas institucionales y servicios tecnológicos definidos por la Universidad FUCS. • Garantizar la correcta configuración, activación y funcionamiento del MFA • Gestionar los procesos de soporte para garantizar el uso adecuado con el multifactor
Seguridad de la información	• Monitoreo de incidentes para evitar accesos no autorizados en los correos de la Universidad FUCS • Realizar capacitaciones y/o sensibilizaciones con el fin de que la comunidad FUCS conozca la importancia de tener contraseñas seguras.

Todos los usuarios	• Utilizar de manera obligatoria los mecanismos de autenticación definidos por la Universidad FUCS • Reportar de manera inmediata a los correos autorizados por cualquier intento de autenticación de las cuentas. • No compartir ningún Código o elemento de acceso para evitar accesos no autorizados

9. Creación de Contraseñas.

La División de Desarrollo Tecnológico mantendrá estándares, en el uso de contraseñas que permiten la autenticación en los equipos de cómputo, sistemas de información y/o aplicaciones de la Universidad FUCS, así mismo, garantizará que estas cumplan con unos estándares para el uso y la creación.

Controles

Responsable	Actividades
División de Desarrollo Tecnológico	• Implementar un sistema de gestión de contraseñas el cual cumpla con lo siguiente (Estándares para el uso y creación de contraseñas - La longitud de la contraseña debe ser igual o superior a 8 caracteres. - Utilizar en la misma contraseña números, letras mayúsculas, letras minúsculas y caracteres especiales o símbolos. - Alternar las letras mayúsculas y letras minúsculas dentro de la contraseña. - Utilizar caracteres especiales o símbolos). • Forzar el cambio periódico de contraseñas cada 90 días en el dominio y correo electrónico. • Bloquear cuentas después de cinco intentos fallidos de autenticación. • Implementar medidas de seguridad para evitar el acceso no autorizado a las contraseñas
Seguridad de la información	• Verificar que se cumplan los estándares de configuración de contraseñas en los diferentes sistemas de la institución. • Realizar capacitaciones y/o sensibilizaciones con el fin de que la comunidad FUCS conozca la importancia de tener contraseñas seguras.

10. Administración y Uso de Tokens de Seguridad

La Universidad FUCS vigilará un uso responsable de los tokens por parte de los colaboradores que por su función requieran el uso de los mismos.

Controles

Responsable	Actividades
Áreas Usuarias de Tokens de Seguridad	• Delegar la autorización del uso de tokens de seguridad a un colaborador administrador.
Administradores de los Tokens de Seguridad	• Gestionar las solicitudes de los tokens y su activación de acuerdo con los requerimientos de cada entidad, en cada portal o sistema de información, incluyendo la documentación necesaria para la gestión. • Controlar los dispositivos token entregados a cada colaborador, mediante bases de datos y actas de entrega que permitan procedimientos ágiles de desactivación en caso de pérdida, robo o cuando presenten falla o mal funcionamiento.
Usuarios de Tokens de Seguridad	• Usar de manera responsable los tokens de seguridad y las cuentas asociadas al uso de los mismos, las cuentas son de carácter personal e intransferible. Los tokens hacen parte del inventario físico asignado a cada colaborador, por lo que se deben devolver cuando el vínculo laboral con la Universidad FUCS se termine o se presente cambio de cargo, es necesario emitir su respectivo paz y salvo con la institución. • Salvaguardar los tokens en lugares seguros que eviten el acceso o visualización de las claves a terceras personas, deben mantenerse en buen estado, se debe reportar de manera inmediata la pérdida o robo al administrador, con el fin de notificar a las entidades emisoras para iniciar el proceso de bloqueo y reposición. • Responder por transacciones electrónicas realizadas con la cuenta asociadas al token, asumiendo la responsabilidad administrativa, disciplinaria y económica a la que haya lugar. • Cumplir con las disposiciones y procedimientos de seguridad establecidos por las diferentes entidades emisoras de los dispositivos acatando las disposiciones que para tal fin emitan.

X. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN.

1. Establecimiento de Requisitos de Seguridad.

La Universidad FUCS garantiza que el software adquirido y de desarrollo propio cumple con los lineamientos de seguridad y calidad establecidos por la institución. Las áreas propietarias de sistemas de información, la División de Desarrollo Tecnológico y Seguridad de la Información

serán los responsables de definir los requerimientos necesarios para la evaluación y aval de compra o desarrollo de software.

Controles

Responsable	Actividades
División de Desarrollo Tecnológico	• Establecer metodologías para el desarrollo/contratación de software, donde se incluyan los requerimientos de seguridad y el desarrollo seguro mediante buenas prácticas con estándares internacionales que permita contar con el aseguramiento del software.
Propietarios de los Sistemas de Información.	• Establecer los requerimientos que incluyan las necesidades propias de los sistemas de información.
Desarrolladores (Internos o Externos)	• Documentar los requerimientos solicitados, definir la arquitectura de software más conveniente, que incluya herramientas de desarrollo licenciado y con gran trayectoria en el mercado. • Incluir en el desarrollo funcionalidades que contribuyan con la seguridad; funciones de autocompletar formularios, límites de tiempos de duración de las sesiones, conexiones paralelas de un mismo usuario, entre otras funcionalidades. • Garantizar que la transmisión de información relacionada con pagos/transacciones en línea se realice por medio de canales y protocolos seguros.

2. Desarrollo Seguro, Realización de Pruebas y Soporte de Sistemas.

La Universidad FUCS vigila que los desarrollos realizados internamente o por proveedores contratados para este fin, cumplan con los requerimientos de seguridad necesarios, así como que contemplen buenas prácticas de desarrollo (especialmente en lo relacionado con la seguridad), deben contar con la documentación y metodología para la aplicación de pruebas de seguridad y deben garantizar el respectivo soporte tecnológico requerido por la Universidad FUCS.

Controles

Responsable	Actividades
Propietarios de los Sistemas de Información	• Realizar metódicamente las pruebas de funcionalidad que aseguren el cumplimiento de los requerimientos y realizar la documentación de las pruebas. • Aprobar el paso a producción de los desarrollos/ajustes/cambio de versiones, luego de la revisión del cumplimiento de los requerimientos.
División de Desarrollo Tecnológico	• Realizar metódicamente las pruebas que aseguren el cumplimiento de los requerimientos de seguridad, realizar la documentación de las pruebas y correcciones realizadas necesarias antes del paso a producción. Llevar un control de de las migraciones/ajustes/versiones entre los diferentes ambientes de desarrollo, pruebas, calidad y producción de los productos entregados. • Implementar controles que garanticen los procedimientos y aprobaciones de migraciones entre los ambientes de desarrollo, de acuerdo con la gestión del cambio incluyendo el control de versiones. • Asegurar las condiciones contractuales y acuerdos de licenciamiento, para que los desarrollos por parte de proveedores cumplan los derechos de propiedad intelectual. • Generar los protocolos para la fase de pruebas al software desarrollado, teniendo en cuenta los lineamientos de manejo de datos y ambientes. • Realizar el aseguramiento tecnológico de la plataforma utilizada para el desarrollo de software mediante la aplicación de parches a los sistemas operativos y versiones de los IDE (entorno de desarrollo integrado). • Cuando la adquisición, desarrollo, contratación o integración involucre funcionalidades de inteligencia artificial, aplicar y documentar la evaluación de riesgos, pruebas, autorizaciones y demás criterios establecidos en el acápite de uso responsable de tecnologías de inteligencia artificial del presente manual, antes de su implementación o paso a producción.

Desarrolladores (Internos o Externos)	• Realizar su trabajo bajo los lineamientos de desarrollo seguro y las buenas prácticas recomendadas en cada fase del ciclo de vida del software, pasando desde el diseño hasta la operación y soporte. • Proporcionar un nivel adecuado de soporte con acuerdos de servicio que asegure la solución de problemas generados en el software o aplicativo de la Universidad FUCS. • Realizar las configuraciones que permitan la validación y generación de los datos de entrada y de salida de manera confiable, mediante el uso de rutinas de validación centralizadas y estandarizadas, así como garantizar el cierre de sesión oportuno optimizando el uso de recursos de máquina. • Incluir métodos de autenticación de doble factor cuando se realicen operaciones críticas en los aplicativos desarrollados. • Usar controles seguros que eviten la divulgación de información almacenada en cookies y complementos, estructura de datos, encabezados de respuesta o cualquier información sensible en respuestas, así como reemplazar los mensajes de error genéricos, remover archivos o funciones innecesarias. • Evitar incluir la información de cadenas de conexión a bases de datos en el código en texto plano. Las cuales deben estar en archivos de configuración independientes y cifrados. • Desarrollar los controles necesarios en la conexión a las bases de datos y transferencia de archivos, ésta última debe realizarse en repositorios o bases de datos seguros que eviten la ejecución de sentencias desde estos archivos. • Proteger el código fuente de los aplicativos contra las descargas o edición. • Se deben separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados. • Realizar análisis de vulnerabilidades y pruebas a nivel de seguridad antes de generar PAP • Generar buenas prácticas en desarrollo seguro (OWASP/BURP SUITE) • Documentar e implementar autorizaciones para PAP desde estado de pruebas a PAP
Seguridad de la Información	• Monitorear las pruebas funcionales y de seguridad realizadas a los aplicativos con el fin de validar si cumplen con los requisitos mínimos de seguridad. • Verificar los estándares de seguridad en los aplicativos según lo descrito por los desarrolladores

3. Protección de los Datos de Pruebas.

La División de Desarrollo Tecnológico debe proteger los datos utilizados en las diferentes pruebas realizadas por los desarrolladores.

Esta información solo se usará para ambiente de pruebas y no se debe utilizar información clasificada en ambientes de pruebas que no cuenten con los controles de seguridad

Controles

Responsable	Actividades
División de Desarrollo Tecnológico	• Asegurar que la información usada en ambientes de pruebas sea eliminada cuando se culminen las pruebas. • Implementar controles de acceso que permitan que únicamente el personal autorizado acceda a los ambientes de pruebas.
Desarrolladores	• Garantizar la confidencialidad y protección de la información utilizada en ambientes de pruebas. • Utilizar únicamente la información autorizada para las actividades de desarrollo y pruebas.

4. Inclusión de condiciones de seguridad en la relación con terceras partes.

La Universidad FUCS establecerá mecanismos de control con respecto a las relaciones estratégicas con terceras partes, que permitan garantizar que se tengan condiciones mínimas de seguridad con respecto al acceso a la información de la Universidad FUCS.

Los colaboradores de la Universidad FUCS encargados de establecer estas relaciones son los responsables de comunicar la documentación, procedimiento y lineamientos de Seguridad de la Información establecidos en el presente manual y demás normas internas de la Universidad FUCS.

Controles

Responsable	Actividades
División de Desarrollo Tecnológico y División Jurídica	• Establecer ANS y requisitos mínimos de seguridad de la información, que deben cumplir las terceras partes o proveedores de servicios tecnológicos. • Diseñar los acuerdos de confidencialidad y los acuerdos de intercambio de información que incluyan responsabilidad tanto civil como penal de las terceras partes que hayan sido contratadas. • Incluir en los contratos con proveedores de inteligencia artificial en los que sean procedentes, las condiciones aplicables que

	desarrollen la finalidad del servicio, tratamiento y localización de la información, prohibición o limitaciones para el entrenamiento de modelos, confidencialidad, propiedad intelectual, conservación, devolución y eliminación de la información, notificación de incidentes, continuidad, soporte, cambios significativos del servicio y terminación de la relación contractual, y demás aspectos relevantes para el uso y explotación de la herramienta.
División de Desarrollo Tecnológico	• Definir condiciones de conexión y comunicación segura para los equipos de cómputo y dispositivos móviles utilizados por terceras partes para conectarse a la red de datos de la institución, así como mecanismos de cifrado y transmisión con terceras partes. • Monitorear, identificar y mitigar los riesgos de accesos a la información de la Universidad FUCS mediante una constante evaluación y aprobación de los accesos requeridos por terceras partes.
Supervisores de Contratos con Terceros	• Velar por el buen cumplimiento de las políticas, lineamientos y procedimientos establecidos por la Universidad FUCS con respecto al acceso a la información, recursos tecnológicos de terceras partes, así como realizar la divulgación oportuna de estas medidas y procedimientos de seguridad de la información. • Validar el cumplimiento de los ANS (acuerdos de niveles de servicio) anexos al contrato.
Seguridad de la Información	• Validar el cumplimiento de estándares, normatividad y controles necesarios para la protección de los principios de seguridad (Confidencialidad, Integridad y Disponibilidad).

5. Gestión de la Prestación de Servicios de Terceras Partes.

La Universidad FUCS propenderá por cumplir y mantener durante el tiempo necesario los niveles acordados con respecto a la prestación de los servicios de los proveedores, así como también velará por el cumplimiento del proceso de gestión de cambios para los servicios y productos modificados por proveedores y los acuerdos aplicables con respecto a la seguridad de la información.

Controles

Responsable	Actividades
División de Desarrollo Tecnológico	• Verificar que los equipos de cómputo, dispositivos móviles que establezcan conexiones a los recursos y redes de datos de la Universidad FUCS cumplan con las condiciones de seguridad establecidas para terceras partes. • Verificar que existan las condiciones de conexión y comunicación segura para los equipos de cómputo y dispositivos móviles que terceras partes utilizan para conectarse a la red de datos de la institución, así como mecanismos de cifrado y transmisión con terceras partes.
Seguridad de la Información	• Realizar monitoreos con el ánimo de evaluar el cumplimiento del acuerdo de confidencialidad y de intercambio de información, así como los requisitos de seguridad de la información establecida hacia los terceros.
Supervisores de Contratos con Terceros	• Monitorear periódicamente el cumplimiento de acuerdos de niveles de servicio. • Identificar posibles situaciones anómalas que representen riesgo para la institución en la ejecución del contrato y reportarlas a la Gerencia y a la División Jurídica.

XI. RELACIÓN CON LOS PROVEEDORES

La Universidad FUCS tiene identificado y bajo mecanismos de control de acceso a los distintos proveedores que por la naturaleza de la prestación de sus servicios requiere acceso a las instalaciones.

Se tienen establecidos mecanismos de control en la relación con los proveedores y terceros, de tal forma que se dé cumplimiento a el Manual de Seguridad de la información.

Controles

Responsable	Actividades
Líderes de Proceso	• Como responsables de los activos de información o supervisores de contrato no deben brindar acceso a la información de la Universidad FUCS o de los activos de información, a proveedores o terceros hasta no tener firmados y formalizados contratos o acuerdos de confidencialidad, integridad y disponibilidad.

Proveedores y/o Terceros	• Todos los proveedores y terceros que vayan a tener acceso a información confidencial de la Universidad FUCS deberán firmar acuerdos de confidencialidad y/o acuerdos de transmisión de datos personales. • Deben cumplir con los controles y lineamientos establecidos en el Manual de Seguridad de la Información de la Universidad FUCS. • Considerar y aplicar buenas prácticas para el desarrollo seguro. • Desarrollar los controles necesarios para la transferencia de archivos, así como solicitar autenticaciones. • Monitorear la transferencia de archivos.
Colaboradores	• Los colaboradores responsables de la supervisión de contratos o convenios con proveedores y terceros deben dar a conocer los lineamientos y normas de Seguridad de la Información de la Universidad FUCS a dichas partes, así mismo, debe velar porque se otorguen accesos correctos y de almacenamiento de forma segura a los recursos de la Universidad FUCS.
Seguridad de la Información	• Realizar monitoreos y seguimientos a los proveedores que tengan acceso a información confidencial de la Universidad FUCS.

XII. GESTIÓN DE INCIDENTES DE SEGURIDAD

1. Reporte y Tratamiento de Eventos o Incidentes de Seguridad.

El personal interno y provisto por terceras partes debe reportar con prontitud los eventos o incidentes relacionados con la violación de seguridad de la información y sus recursos de procesamiento y almacenamiento de información de la plataforma tecnológica, los sistemas de información y las personas.

Definir una adecuada capacidad de respuesta a incidentes abordando su gestión de manera versátil y flexible facilitando la adopción y/o aprendizaje de las medidas adecuadas, minimizando el riesgo de pérdida de información digital o la interrupción de los servicios de la infraestructura tecnológica expuesta en el ciberespacio.

Controles

Responsable	Actividades
Propietarios de los Activos de Información y Usuarios	• Reportar los eventos o incidentes de seguridad inmediatamente sean identificados, a Seguridad de la Información y a Soporte Técnico de la División de Desarrollo Tecnológico, proporcionando toda la información necesaria, sin ocultar, corregir unilateralmente o destruir las evidencias del incidente.

División de Desarrollo Tecnológico	• Mantener actualizada la documentación de infraestructura tecnológica de la Universidad FUCS permitiendo establecer criticidad impacto y consecuencias de materialización de incidentes de seguridad. • Asignar personal calificado, para realizar las pesquisas necesarias de los eventos o incidentes de seguridad reportados, con el fin de identificar sus causas y que permita proporcionar soluciones, así como prevenir su recurrencia. • Establecer en conjunto con Seguridad de la Información, responsabilidades y procedimientos que permitan una respuesta rápida y efectiva a los eventos o incidentes de seguridad de la información. • Implementar un sistema de gestión de conocimiento que permita tener respuesta rápida a eventos o incidentes conocidos, así como la documentación de los nuevos incidentes.
Comité de Seguridad de la Información	• Apoyar las iniciativas de comunicación y sensibilización frente a los eventos de seguridad de la información.
Seguridad de la Información	• Evaluar los eventos o incidentes de Seguridad de la Información, así como realizar el escalamiento al Comité de Seguridad de la Información para los casos que requieran evaluación conjunta. • Realizar capacitaciones y/o sensibilizaciones con el fin de mitigar los riesgos que puedan estar asociados a eventos o incidentes de Seguridad de la Información y frente a los eventos o incidentes que ya han sido reportados y atendidos • Mantener registro de todos los eventos reportados por los colaboradores, proveedores y/o terceros, sobre aquellas anomalías o debilidades que afectan la seguridad de la información, asegurando el registro de todos los factores que permitan tener estadísticas anuales de comportamiento de respuesta ante incidentes, aprender de lo ocurrido y establecer mejoras en las acciones de control y en el contenido del presente Manual cuando sea necesario.
Usuarios	• Reportar oportunamente cualquier evento que pueda ser clasificado como incidente para la seguridad de la información, así como la pérdida o divulgación no autorizada de información, comunicando lo correspondiente a Seguridad de la Información y a la División de Desarrollo Tecnológico para la gestión respectiva.

2. Desarrollo de Gestión de Vulnerabilidades.

La Universidad FUCS, a través de la División de Desarrollo Tecnológico y Seguridad de la Información, ejecutará procedimientos que permitan conocer nuevas vulnerabilidades del software y sistemas de información de la plataforma tecnológica, con el objetivo de realizar remediación

de los hallazgos encontrados en las pruebas realizadas.

La priorización de la remediación deberá considerar la criticidad de los activos, la gravedad de la vulnerabilidad, la posibilidad de explotación, el impacto potencial sobre la Universidad y los cambios relevantes en la infraestructura tecnológica.

Controles

Responsable	Actividades
División de Desarrollo Tecnológico	• Coordinar y realizar directamente o a través de un tercero especializado, una vez al año, el análisis de vulnerabilidades técnicas a la infraestructura tecnológica de la Universidad FUCS. • Liderar las tareas de remediación oportuna, así como establecer los planes de acción para ser ejecutadas por parte de desarrolladores y terceras partes que permita la mitigación de vulnerabilidades generadas por las pruebas realizadas.
Seguridad de la Información	• Monitorear los resultados del análisis de vulnerabilidades, hacking ético, así como la remediación de las vulnerabilidades detectadas. • Realizar seguimiento a los planes de acción para la remediación de las vulnerabilidades detectadas.

3. Gestión de parches de seguridad

La Universidad FUCS identificará los activos tecnológicos que requieran actualizaciones y parches de seguridad y establecerá su priorización de acuerdo con su criticidad, las vulnerabilidades identificadas, el nivel de exposición y el impacto potencial sobre la operación. Antes de su implementación deberán realizarse, cuando resulte necesario, las validaciones y pruebas correspondientes.

Controles

Responsable	Actividades
División de Desarrollo Tecnológico	• Clasificar los activos críticos que disponga la Universidad FUCS y realizar su debido proceso de actualización • Mantener registros de actualizaciones realizadas donde se exprese versión, responsable fecha y hora de la actividad • Realizar el proceso de actualizaciones sin afectar la operación de la Universidad FUCS • Realizar validaciones y pruebas después de ejecución de la

	actividad de actualización.
Seguridad de la Información	• Identificar los activos más críticos para su actualización de seguridad • Realizar seguimiento a las actualizaciones y parches de seguridad aplicados.

XIII. INCLUSIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

1. Continuidad, Contingencia, Recuperación y Retorno a la Normalidad con Consideraciones de Seguridad de la Información.

La Universidad FUCS establecerá procedimientos que permitan a través de recursos tecnológicos y humanos garantizar la puesta en marcha de los planes de contingencia y continuidad en caso de presentarse fallas en la plataforma, eventos catastróficos ataques cibernéticos y eventos de perdida de información que puedan afectar la continuidad de la operación de la Universidad FUCS.

Se debe responder de manera oportuna y de acuerdo con la magnitud de afectación del servicio, el restablecimiento de las operaciones considerando el menor costo y pérdidas posibles, garantizando la seguridad de la información cuando se presenten este tipo de incidentes

Controles

Responsable	Actividades
Consejo Superior	• Identificar y formalizar los procesos críticos en la Institución, como eje y punto de partida para orientar los recursos en caso de eventos que afectan la continuidad del servicio. • Aceptar y reconocer las situaciones identificadas como emergencia o desastre para los procesos o áreas de la Universidad FUCS y apoyar los planes de acción para atender dichas situaciones, así como liderar los planes de continuidad del negocio y la recuperación ante desastres. • Aprobar el análisis de impacto al negocio (BIA) y los análisis de riesgos de continuidad que permitan desarrollar estrategias de recuperación en las situaciones y que se active el plan de contingencia o continuidad. • Aprobar los planes de contingencia, recuperación y regreso a la normalidad, que incluyan las medidas para garantizar la seguridad de la información, así como la documentación de las pruebas de dichos planes.

División de Desarrollo Tecnológico	• Elaborar el plan de continuidad y recuperación para la infraestructura tecnológica de la Universidad FUCS, así como los procedimientos de contingencia, recuperación y regreso a la normalidad para cada uno de los servicios prestados.
Líderes de Proceso	• Identificar y documentar al interior de las áreas los procedimientos de continuidad que podrían ser ejecutados en caso de presentarse situaciones adversas y que afecten la seguridad de la información. Es fundamental realizar pruebas sobre los procedimientos propuestos, para evaluar su efectividad. • Realizar el análisis BIA (Business Impact Analysis) con el fin de identificar procesos críticos, tiempos mínimos de atención en las actividades del proceso, responsables, cargos, backups, ubicación de información relevante para el cumplimiento de las actividades críticas, con el acompañamiento de Seguridad de la Información. • Mantener actualizada la información de contactos con sus respectivos responsables • Identificar los procesos críticos que dependan de herramientas de inteligencia artificial y establecer procedimientos alternativos que permitan mantener la operación cuando estas no estén disponibles, presenten errores, sean modificadas por el proveedor o deban ser suspendidas por razones de seguridad.
Seguridad de la Información	• Elaborar el Plan de Continuidad con las estrategias de recuperación frente a un evento de interrupción. • Realizar capacitaciones y/o sensibilizaciones frente al plan de continuidad y el análisis BIA (Business Impact Analysis). • Realizar una vez al año una prueba al plan de continuidad con el fin de evaluar su efectividad e identificar nuevos escenarios • Mantener actualizado el directorio para canales de emergencia cuando se surja un incidente incluyendo responsables de área

2. Redundancias.

La Universidad FUCS propenderá por que la plataforma tecnológica sea redundante cumpliendo los requisitos de disponibilidad adecuados y tolerados por la operación de la Universidad.

Controles

Responsable	Actividades
División de Desarrollo Tecnológico	• Analizar y construir los requisitos de redundancia para los aplicativos de misión crítica, para la Universidad FUCS y la plataforma tecnológica que los soporta, realizando una constante evaluación que permita la mejora continua de estos procedimientos. • Delegar la administración de los recursos destinados para la redundancia tecnológica, realizando la evaluación periódica que permita establecer el grado de disponibilidad de los servicios tecnológicos de la Universidad FUCS.
Seguridad de la Información	• Documentar en el Plan de Continuidad, el lineamiento de redundancia de los aplicativos de misión crítica de la Universidad FUCS, así como la plataforma tecnológica que los soporta.

XIV. CUMPLIMIENTO

1. Cumplimiento de Requisitos Legales y Contractuales.

La Universidad FUCS es responsable del licenciamiento y requisitos legales aplicables que den cumplimiento a las leyes, condiciones contractuales de cualquier requisito de seguridad de la información y de los derechos de autoría.

La Universidad FUCS establece que la información personal de los titulares de los datos personales, cuyo responsable del tratamiento es la Universidad FUCS, es de carácter confidencial, por lo cual se implementarán los controles necesarios para su protección y en ningún momento puede ser divulgada a terceras partes a menos que cuente con la autorización formal del titular, o en los casos en que la normatividad lo permita.

Es responsabilidad de Seguridad de la Información, propender por el cumplimiento de los lineamientos establecidos en este documento, registrar los procesos, procedimientos, manuales, instructivos y formatos específicos, alineados al estándar internacional ISO/IEC 27001 y sus normas derivadas y otros marcos generalmente aceptados, así como, liderar la implementación de los controles exigidos por la ley y la regulación.

En las revisiones periódicas se deben tener en cuenta factores como: incidentes de seguridad, nuevas vulnerabilidades detectadas, cambios dentro de la infraestructura organizacional o tecnológica, cambios en los procesos, en los objetivos del sistema o de la Universidad FUCS, normatividad vigente, entre otros.

Los documentos, matrices, registros y evidencias derivados de la aplicación del presente Manual deberán elaborarse, actualizarse, conservarse y protegerse de conformidad con los procedimientos institucionales de gestión documental y del Sistema de Gestión Organizacional, atendiendo su clasificación, responsable, versión, periodo de conservación y condiciones de acceso.

Controles

Responsable	Actividades
División Jurídica	• Documentar, actualizar e identificar los requisitos legales, reglamentados y aplicados a contratos y a la seguridad de la información de la Universidad FUCS. • Asesorar a la Universidad FUCS sobre los requisitos normativos y regulatorios dados por entes de control, así como de las obligaciones con terceros y colaboradores, siempre enmarcados dentro del cumplimiento de la legislación colombiana vigente. • Identificar normatividad de cumplimiento frente a propiedad intelectual y derechos de autor, con el fin de establecer de manera adecuada en los contratos que se realicen con proveedores.
División de Desarrollo Tecnológico	• Verificar que todo software y hardware que forme parte de los recursos tecnológicos de la Universidad FUCS, cuenten con el licenciamiento y estén custodiados por las normas y leyes de derechos de autor, o en su defecto sea licencia pública de libre distribución. • Elaborar el inventario de software, de sistemas de información y de recursos digitales, que estén autorizados para ser usados en los computadores o recursos de la infraestructura tecnológica de la Universidad FUCS. De igual forma debe hacer revisiones periódicas para corroborar que el software instalado coincida con el autorizado. • Los derechos de propiedad intelectual incluyen licencias de software, documentos generados como parte del conocimiento de la Universidad FUCS, propuestas comerciales y comercial que involucre la imagen de la institución. • Todos los programas de software usados para el desarrollo de las actividades de la Universidad FUCS, deben incluir los avisos de información de derechos de autor correspondiente y estos deben aparecer cuando el usuario inicie la aplicación.

Seguridad de la Información	• Garantizar la definición y cumplimiento de los requerimientos de seguridad de la Información y en conjunto con la División Jurídica establecer estos aspectos con las obligaciones contractuales específicas. • Reportar a la División de Desarrollo Tecnológico cualquier aplicación ilegal, así como registrarlo en los eventos de Seguridad de la información. • Identificar normatividad de cumplimiento frente a Seguridad de la Información.
Todos los Usuarios	• Cumplir y obedecer con los acuerdos de licenciamiento de software y las leyes de derechos de autor. No están autorizados para instalar software o sistema de información en los computadores de trabajo o recursos de la infraestructura tecnológica de la Universidad FUCS suministrado para sus actividades. • Los colaboradores de la Universidad FUCS no podrán acceder a páginas de internet relacionadas con contenidos diferentes a los que sean requeridos para el cumplimiento de sus funciones; así mismo, no está permitido la descarga, intercambio o instalación de aplicaciones de entretenimiento personal como; música, juegos, protectores de pantalla o aplicaciones sin costo, documentos o carpetas que contengan archivos ejecutables, que afecten los principios de Seguridad de la Información en la infraestructura tecnológica. • En caso de requerir alguna descarga o software, debe ser solicitado a la División de Desarrollo Tecnológico, con previa autorización de Seguridad de la Información.
Proveedores	• Deben existir acuerdos contractuales claramente definidos entre la Universidad FUCS y cualquier proveedor que realice actividades de desarrollo de software, en los cuales se especifiquen los compromisos de preservación de los derechos de propiedad intelectual.

2. Privacidad y Protección de Datos Personales.

La Universidad FUCS como responsable del manejo de datos personales, propenderá por la protección de la información de todos los titulares de los cuales gestione información personal, dando cumplimiento a la Ley 1581 de 2012, el Decreto 1074 de 2015 y demás normas vigentes sobre la materia que regulen el tratamiento de datos personales, y a su Política de Tratamiento de Datos Personales, en desarrollo de su Programa Integral de Gestión de Datos Personales, en el marco del Sistema de Gestión de Seguridad de la Información de la Universidad FUCS.

Se establecerán los términos, condiciones y finalidades para que la Universidad FUCS, como

responsable de los datos personales recibidos por medio de sus distintos puntos de atención, realice la gestión correcta de los datos personales que recolecta en todo momento y de conformidad con las actividades derivadas de las funciones sustantivas.

Cuando se realice la contratación de un tercero para desarrollar o prestar algún servicio, se debe garantizar que cumpla con los deberes de encargado del tratamiento de la información, de acuerdo con lo establecido en las normas vigentes, así mismo, deberá implementar las medidas de Seguridad y Privacidad para la custodia de los datos personales.

La información y datos personales de los titulares de la Universidad FUCS no podrán divulgarse ni entregarse a terceros, salvo que el tercero acredite que cuenta con autorización previa y expresa del titular, o fundamente su acceso en una excepción legal en la cual no sea necesario contar con tal autorización, según se definen en el artículo 10 de la Ley 1581 de 2012 y demás normas aplicables.

Cuando una solicitud de acceso, entrega o divulgación de información personal genere una tensión entre el derecho al habeas data y otros derechos fundamentales, el área que custodia la información con el acompañamiento de Seguridad de la Información y de la División Jurídica, deberán analizar la solicitud y determinar si se puede acceder a la solicitud o debe abstenerse de efectuar la entrega de los datos personales solicitados, explicando las razones para ello. Para dicho análisis podrán tenerse en cuenta las recomendaciones establecidas en la Guía sobre el tratamiento de datos personales en el contexto universitario de la Superintendencia de Industria y Comercio, así como la jurisprudencia y normas que sean aplicables.

La Universidad FUCS evaluará y establecerá los mecanismos y controles necesarios para la protección de los datos personales almacenados en sus bases de datos, teniendo en cuenta el nivel de protección que cada categoría de datos requiere, los controles de acceso requeridos y las finalidades asociadas, conforme al siguiente esquema:

Categoría de dato	Nivel de Protección
Dato personal público	Bajo
Dato personal semiprivado	Intermedio
Dato privado	Elevado
Dato personal sensible	Reforzado

No obstante lo anterior, la Universidad FUCS podrá adoptar un esquema de clasificación homogéneo, aplicable a todos sus procesos, sistemas y unidades académico administrativas.

Tratamiento de datos personales de niños, niñas y adolescentes

El tratamiento de datos personales de menores de edad deberá responder a su interés superior, asegurar el respeto de sus derechos prevalentes y ser necesario y proporcional para una finalidad legítima, especialmente para garantizar el acceso y permanencia en el servicio educativo, la protección de su vida, su salud e integridad, así como el cumplimiento de las obligaciones legales de la Universidad FUCS.

La autorización de tratamiento de datos deberá ser otorgada por el padre, madre o representante legal del niño, niña o adolescente menor de edad, previa información al menor de edad (comprensible de forma clara para su edad y madurez), pues la participación obligatoria del padre, madre o representante legal no excluye el derecho del menor a conocer, comprender y participar en las decisiones relacionadas con el tratamiento de sus datos personales, en reconocimiento de su autonomía progresiva.

Controles

Responsable	Actividades
Áreas que procesan datos personales	• Para el procesamiento de datos personales de los titulares identificados en la Política de Protección de Datos Personales de la Universidad FUCS, se debe contar con la respectiva autorización del titular de la información para poder tratarla en el desarrollo de las acciones que se lleven a cabo por la Universidad FUCS. • Asegurar el acceso a datos personales a cargo de su área, sólo para aquellas personas de su área, que tengan una necesidad laboral legítima. • Asegurar el acceso a datos personales a cargo de su área, sólo por terceros debidamente autorizados. o La calidad de padre, madre, acudiente de un estudiante o pagador de la matrícula, no le otorga por sí sola derecho a conocer la información académico administrativa de un estudiante mayor de edad, por lo cual este debe contar con autorización previa y expresa del estudiante para el acceso a su información. o La calidad de empleador, ex empleador o futuro empleador, asegurador u otros terceros, no le otorga por sí sola el derecho a conocer información académico administrativa o laboral de un estudiante o colaborador de la Universidad FUCS, por lo cual este debe contar con autorización previa y expresa del titular para el acceso a su información. • Recolectar únicamente los datos que sean indispensables para el desarrollo de la labor que realiza. • No realizar la recolección de datos personales sensibles, salvo cuando estos sean estrictamente necesarios para el desarrollo de la actividad o labor en específico que realiza. En tal caso, deberá informarse al titular su carácter facultativo y las finalidades específicas, obtenerse la autorización explícita y aplicarse medidas reforzadas de acceso, confidencialidad y seguridad a los datos personales entregados. • Aplicar controles reforzados de acceso y confidencialidad, respecto de la información y datos personales de menores de edad. • Establecer condiciones contractuales, de seguridad y

	confidencialidad para aquellas entidades vinculadas o aliadas que tengan acceso a los datos. • Acoger las instrucciones técnicas y procedimientos establecidos para el intercambio de datos, así mismo, con proveedores y terceros para el envío de información por cualquier medio. • Conocer y aplicar la Política de Protección de Datos Personales publicada en la página web de la Universidad FUCS.
Seguridad de la Información	• Gestionar, coordinar y hacer seguimiento al Programa Integral de Gestión de Datos Personales, en el marco del Sistema de Seguridad de la Información de la Universidad FUCS. • Dar acompañamiento a los controles de tratamiento de datos personales de los titulares identificados en la Política de Protección de Datos Personales de la Universidad FUCS. • Supervisar y monitorear el cumplimiento de los controles establecidos en la Política de Protección de Datos Personales de la Universidad FUCS. • Documentar y actualizar la Política de Protección de Datos personales de la Universidad FUCS cuando se requiera, y todos los documentos y procedimientos que conforman el Programa Integral de Gestión de Datos Personales. • Capacitar a los colaboradores sobre la protección de datos personales en la Universidad FUCS. • Responder a las consultas y reclamaciones presentadas por titulares y terceros, en materia de tratamiento de datos personales. • Apoyar técnica y documentalmente la atención de solicitudes judiciales o administrativas que involucren datos personales, previa validación de la División Jurídica sobre la competencia de la autoridad, el alcance de la solicitud y la información que resulte procedente entregar.
División de Desarrollo Tecnológico	• Implementar controles que permitan proteger los datos personales de los titulares identificados en la Política de Protección de Datos Personales de la Universidad FUCS, almacenados en las bases de datos y demás repositorios institucionales y prevenir su acceso, consulta, uso, divulgación, alteración, pérdida o eliminación no autorizados o contrarios a la finalidad autorizada.
Todos los Usuarios	• Guardar la reserva absoluta de la información y bases de datos a cargo de la Universidad FUCS que por cualquier motivo conozcan. • Remitir inmediatamente a la División Jurídica cualquier solicitud judicial, administrativa o de autoridad que requiera datos personales y abstenerse de entregar directamente la información.

Usuarios de los Portales de la Universidad FUCS	• Asumir la responsabilidad personal sobre la contraseña de acceso a los portales que les es suministrada, así mismo, es necesario cambiar periódicamente esta contraseña. • Tener controles de seguridad en sus dispositivos móviles, computadores o redes privadas para acceder a los portales de la Universidad FUCS. • Remitir inmediatamente a la División Jurídica cualquier solicitud judicial, administrativa o de autoridad que requiera datos personales y abstenerse de entregar directamente la información.
Estudiantes, docentes, colaboradores	• Tratar los datos personales recolectados en actividades académicas, prácticas, e investigativas, únicamente para las finalidades previamente autorizadas y conforme a las instrucciones, protocolos y condiciones aprobadas por la Universidad FUCS. • Abstenerse de acceder, copiar, descargar, utilizar o divulgar bases de datos, historias clínicas, expedientes académicos o disciplinarios, u otra información institucional de la Universidad FUCS o de sus escenarios de práctica, sin autorización del área responsable y sin el cumplimiento de los requisitos legales y de seguridad de la información aplicables. • Utilizar información anonimizada en sus actividades académicas, prácticas e investigativas, cuando la finalidad pueda alcanzarse sin identificar a los titulares. • Abstenerse de divulgar datos personales en los resultados, informes o publicaciones científicas derivadas de sus actividades académicas, prácticas e investigativas. • Reportar inmediatamente a Seguridad de la Información cualquier pérdida, acceso, envío, publicación o uso no autorizado de datos personales, ya sean datos bajo responsabilidad de la Universidad FUCS como de sus escenarios de práctica.

XV. TÉRMINOS Y DEFINICIONES

Para los propósitos de este manual, se utilizarán los siguientes términos y definiciones:

- **Aceptación del riesgo:** Decisión informada de aceptar las consecuencias y probabilidad de un riesgo en particular.
- **Activo:** Cualquier cosa que tiene valor para la organización. (NORMA TÉCNICA NTC- ISO/IEC COLOMBIANA 27002.TECNOLOGÍA DE LA INFORMACIÓN. TÉCNICAS DE SEGURIDAD. CÓDIGO DE PRÁCTICA PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN).
- **Amenaza:** Es una causa potencial de un incidente no deseado que puede causar daño a un sistema u organización. Una amenaza tecnológica, en particular, se refiere a crisis o escenarios

de riesgo originados por fallos o acciones humanas en la tecnología, especialmente en sistemas complejos donde los errores pueden resultar en accidentes.

- **Análisis de riesgos:** Elemento de control que permite establecer la probabilidad de ocurrencia de los eventos positivos o negativos y el impacto de sus consecuencias, calificándolos y evaluándolos a fin de determinar la capacidad de la institución para su aceptación y manejo.
- **Anonimización:** Proceso mediante el cual los datos personales se transforman de manera irreversible para impedir que el titular pueda ser identificado directa o indirectamente mediante medios razonablemente disponibles.
- **Autenticidad:** Busca asegurar la validez de la información en tiempo, forma y distribución. Así mismo, se garantiza el origen de la información, validando el emisor con el fin de evitar la suplantación.
- **Auditabilidad:** Define que todos los eventos de un sistema deben poder ser registrados para su control posterior.
- **Adquisición, Mantenimiento y Desarrollo de Sistemas de Información**: Define controles con el fin de racionalizar gastos integrales de los sistemas de información institucionales.
- **Confidencialidad**: Es la propiedad que asegura que la información no esté disponible ni sea revelada a personas, entidades o procesos no autorizados. La confidencialidad garantiza que la información personal se mantenga protegida y no sea divulgada sin el consentimiento explícito de la persona involucrada.
- **Control de Acceso:** Definir controles para limitar el acceso lógico a la información y a los espacios donde se procese información.
- **Continuidad tecnológica de la Universidad FUCS:** Dirigido a contrarrestar las interrupciones de las actividades basadas en la tecnología, resguardar los procesos críticos, de cualquier efecto generado por fallas significativas o desastres y determinar los planes de recuperación.
- **Cumplimiento de requisitos legales:** Pretende impedir infracciones y violaciones de cualquier ley, obligación, reglamento establecidas en contratos y de cualquier requisito de seguridad.
- **Dato personal:** cualquier información vinculada o que pueda asociarse a una o a varias personas naturales determinadas o determinables. Estos datos se pueden categorizar de la siguiente manera:
- **Dato personal privado:** es un dato personal que por su naturaleza íntima o reservada sólo interesa a su Titular. Para su tratamiento requiere de autorización expresa del Titular. Por ejemplo: libros de los comerciantes, entre otros.
- **Dato personal semiprivado:** son aquellos datos que no tienen una naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular, sino a un grupo de personas o a la sociedad en general. En este caso, para su tratamiento se requiere la autorización expresa del Titular de la información. Por ejemplo: datos de carácter financiero, crediticios, actividades comerciales o de servicios, datos relativos a las relaciones con las entidades de seguridad social (EPS, AFP, ARL, Cajas de Compensación), entre otros.

- **Dato personal público:** es aquel tipo de dato personal que las normas y la Constitución han determinado expresamente como públicos y, para cuya recolección y tratamiento, no es necesaria la autorización del Titular de la información. Por ejemplo: estado civil de las personas, datos contenidos en el RUNT, datos contenidos en sentencias judiciales ejecutoriadas, los datos contenidos en documentos públicos, entre otros.
- **Dato personal sensible:** son aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual, los datos biométricos y aquellos datos que se puedan obtener de un menor de edad. Para su tratamiento se requiere la autorización expresa del Titular de la información y en caso del menor de edad, de su representante legal.
- **Declaración de aplicabilidad**: Documento que describe los objetivos de control y los controles pertinentes y aplicables para el SGSI de la organización.
- **DDT:** División de Desarrollo Tecnológico – FUCS.
- **Disponibilidad:** Es la propiedad que asegura que la información, los datos o los sistemas sean accesibles y utilizables por entidades o procesos autorizados cuando lo requieran. La disponibilidad garantiza que los recursos necesarios estén operativos y se puedan recuperar en el momento en que se necesiten, evitando su pérdida o bloqueo.
- **Evento de seguridad de la información:** Es la presencia identificada de un estado en el sistema, servicio o red que indica un posible incumplimiento del Manual de Seguridad, una falla en los controles, o una situación previamente desconocida que puede ser relevante para la seguridad. Un evento de seguridad puede señalar una amenaza potencial, como una filtración de información, infección por malware o acceso no autorizado, y requiere monitoreo para determinar su impacto y responder adecuadamente.
- **Evaluación del riesgo**: Proceso utilizado para verificar los resultados obtenidos en el análisis de riesgos, con el propósito de establecer el grado de exposición que tiene la institución ante los riesgos identificados y de esta forma determinar la zona de riesgo inicial (Riesgo inherente) y distinguir entre los riesgos tolerables, bajos, medios, altos o intolerables.
- **Evaluación de impacto en privacidad:** proceso documentado destinado a identificar y valorar los riesgos que una actividad de tratamiento puede generar para los derechos de los titulares y a definir las medidas necesarias para mitigarlos antes de iniciar o modificar sustancialmente el tratamiento.
- **Entrada o prompt:** instrucción, consulta, archivo, dato o información suministrada a una herramienta de inteligencia artificial, para obtener un resultado.
- **Gestión del riesgo:** Conjunto de elementos de control que, al interrelacionarse, permiten a la institución evaluar aquellos eventos negativos, tanto internos como externos, que puedan

Impactar o impedir el logro de sus objetivos institucionales o los sucesos positivos que posibilitan la identificación de oportunidades para un mejor cumplimiento de su función. Se encuentra dentro del elemento de control que, al interactuar con sus diversos elementos, posibilita a la institución controlar aquellos sucesos que pueden afectar el cumplimiento de sus objetivos.

- **Gestión de Comunicaciones y Operaciones**: Establece controles para garantizar el correcto funcionamiento de los equipos de procesamiento de la información.
- **Gestión de Activos de Información:** Permite proteger los activos de información institucional.
- **Gestión de incidentes de seguridad de la información:** Actividades orientadas a gestionar los incidentes presentados y tomar las acciones necesarias de prevención y corrección.
- **Herramientas de inteligencia artificial:** sistemas basados en tecnología que, a partir de datos e instrucciones, generan resultados como predicciones, recomendaciones, clasificaciones, contenidos o decisiones que pueden influir en entornos físicos o digitales.
- **Herramienta de IA autorizada:** solución evaluada y habilitada por la Universidad para finalidades y condiciones determinadas.
- **Incidente de seguridad de la información**: Es un evento o una serie de eventos inesperados o no deseados que tienen una probabilidad elevada de comprometer las operaciones del negocio y comprometer la seguridad de la información. Un incidente de seguridad puede incluir accesos, intentos de acceso, uso, divulgación, modificación o destrucción no autorizada de información, impedimentos en la operación normal de redes y sistemas, o violaciones del Manual de Seguridad de la información de la organización.
- **Información:** Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, (textos, numéricas, gráficas, narrativas o audiovisuales) y en cualquier medio, ya sea magnético, en papel, audiovisual u otro.
- **Integridad:** Propiedad de salvaguardar la exactitud y estado completo de los activos.
- **Legalidad:** Se refiere al cumplimiento de las leyes, medidas, reglamentaciones o disposiciones a las que está sujeta la Institución.
- **Monitorear:** Verificar, supervisar, observar de forma crítica, o registrar el progreso de una actividad, acción o sistema, en forma regular, a fin de identificar cambios. (NORMA TÉCNICA NTC COLOMBIANA 5254 – GESTIÓN DEL RIESGO).
- **No repudio:** Se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.
- **Riesgo:** Posibilidad de que suceda algún evento que tendrá un impacto sobre los objetivos institucionales o del proceso. Se expresa en términos de probabilidad y consecuencias.
- **Riesgo residual**: Nivel restante de riesgo después de que se han tomado medidas de tratamiento del riesgo. (NORMA TÉCNICA NTC COLOMBIANA 5254 – GESTIÓN DEL RIESGO).

- **Seguridad de la información**: Es la preservación de la confidencialidad, integridad y disponibilidad de la información, así como de otras propiedades como autenticidad, responsabilidad, no-repudio y confiabilidad. Se refiere al conjunto de medidas preventivas y reactivas implementadas por organizaciones y sistemas tecnológicos para proteger la información en diferentes formatos y medios, asegurando su resguardo y protección. La seguridad de la información abarca más allá de la seguridad informática, incluyendo la protección de datos en todos los tipos de medios.
- **Seudonimización:** Tratamiento mediante el cual los datos personales no pueden atribuirse a un titular sin utilizar información adicional que se conserva separada y sometida a medidas de seguridad. La información seudonimizada continúa siendo dato personal.
- **Sistema de Información:** Es un conjunto integrado de recursos diseñados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información, mediante procedimientos automatizados y manuales. Incluye agentes, códigos y procesos que interactúan de manera coordinada para cumplir un propósito común. En informática, los sistemas de información gestionan, recolectan, procesan, almacenan y distribuyen información relevante, facilitando la toma de decisiones, mediante la gestión y correlación eficiente de datos.
- **Seguridad del Talento Humano**: Define la adecuada segregación de funciones y de reducir los riesgos de error humano y/o comisión de ilícitos, se deben considerar tanto colaboradores internos como personal de terceros que tengan relación con la Universidad FUCS.
- **Seguridad física y del entorno**: Permite definir controles que eviten accesos no autorizados tanto a instalaciones e información.
- **Supervisión humana:** Revisión y validación realizada por una persona competente antes de utilizar un resultado producido por una herramienta de inteligencia artificial, en un proceso institucional.
- **Organización de la Seguridad:** Facilita la gestión de la seguridad de la información dentro de la institución.
- **Protección a la duplicación**: Consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario.
- **Tecnología de la Información:** Se refiere al hardware y software operados por la institución o por un tercero que procese información en su nombre, para llevar a cabo una función propia de la Universidad FUCS, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otros.
- **Tercera parte:** Persona u organismo reconocido por ser independiente de las partes involucradas, con relación al asunto en cuestión. (NORMA TÉCNICA NTC-ISO/IEC COLOMBIANA 27002.TECNOLOGÍA DE LA INFORMACIÓN. TÉCNICAS DE SEGURIDAD. CÓDIGO DE PRÁCTICA PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN)
- **Tratamiento del riesgo**: Selección e implementación de las opciones apropiadas para ocuparse del riesgo. (NORMA TÉCNICA NTC COLOMBIANA 5254 – GESTIÓN DEL RIESGO).

- **Tratamiento:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.
- **Transferencia:** La transferencia de datos tiene lugar cuando el responsable y/o Encargado del Tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es Responsable del Tratamiento y se encuentra dentro o fuera del país.
- **Transmisión:** Tratamiento de datos personales que implica la comunicación de estos dentro o fuera del territorio de la República de Colombia cuando tenga por objeto la realización de un Tratamiento por el Encargado por cuenta del responsable.
- **Valoración del riesgo:** Proceso general de análisis del riesgo y evaluación del riesgo. (NORMA TÉCNICA NTC COLOMBIANA 5254 – GESTIÓN DEL RIESGO).
- **Vulnerabilidad:** Es una debilidad en el diseño, implementación, gestión u operación de un sistema o entorno de información que puede ser explotada por amenazas. Las vulnerabilidades representan puntos débiles que pueden ser aprovechados por fuentes maliciosas para comprometer la seguridad o privacidad del sistema.

XVI. APROBACIÓN DEL MANUAL Y ENTRADA EN VIGOR

Versión	Fecha Aprobación	Descripción del cambio
1	2019	El Manual fue aprobado por el Consejo Superior en sesión No. 516 del 24 de septiembre de 2019, mediante Acuerdo No. 4476 de la misma fecha.
2	2023	El Manual fue modificado por el Consejo Superior en sesión No. 603 de 2023 mediante Acuerdo No. 5807 de 2023 que derogó al Acuerdo No. 4476 de 2019. Se efectúan cambios adicionales con base en lo definido en el Acuerdo 5674 del Consejo Superior, del 13 de diciembre de 2022, Declaración de Políticas Institucionales.
3	2026	El documento ha sido nuevamente expedido integralmente por el Consejo Superior en sesión No. 690 de 18 de agosto de 2026 mediante Acuerdo No. 7252 de 2026, para su adaptación al nuevo carácter como Universidad, y otras actualizaciones necesarias para su mejora. Rige a partir de la fecha de su expedición.

SECRETARIA GENERAL
UNIVERSIDAD FUCS