FUNDACIÓN UNIVERSITARIA DE CIENCIAS DE LA SALUD

FUCS

Vigilada Mineducación

Manual de Políticas de Seguridad de la Información

2019

CONTENIDO

INTRODUCCION 6
POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN 6
Generalidades 6
Alcance 7
Marco Normativo 7
Objetivo General 7
Objetivos específicos 7
Compromiso de la Alta Dirección 8
Roles, Responsabilidades y Autoridades 8
Controles 8
ORGANIZACIÓN PARA DE LA SEGURIDAD DE LA INFORMACION 9
Funciones del Comité de Seguridad de la Información: 9
Organización Interna 10
GESTION DE ACTIVOS DE INFORMACIÓN 11
Política de clasificación de la Información 11
Confidencialidad 11
Integridad 12
Disponibilidad 12
Controles 13
Política de Medios Removibles 14
Controles 14
POLÍTICAS DE SEGURIDAD DEL TALENTO HUMANO 15
Política relacionada con la vinculación de funcionarios 15
Controles 15
Política de desvinculación, licencias, vacaciones o traslados de los funcionarios y personal provisto por terceros 16
Controles 16
SEGURIDAD FÍSICA Y DEL ENTORNO 16
Política de áreas seguras 16
Controles 16

POLÍTICAS DE SEGURIDAD EN LAS OPERACIONES 19
Política de asignación de responsabilidades operativas 19
Controles 19
Política de protección frente a software malicioso 20
Controles 20
Política de copias de respaldo de la información 21
Controles 21
Política de eventos y monitoreos a los recursos tecnológicos y Sistemas de Información 22
Controles 22
Política de seguridad para los equipos institucionales 22
Controles 23
POLÍTICAS DE SEGURIDAD EN LAS COMUNICACIONES 24
Política de gestión y aseguramiento de las redes de datos 24
Controles 24
Política de uso del correo electrónico 25
Controles 25
Política de uso adecuado de internet 25
Controles 25
Política de intercambio de información 26
Controles 26
POLÍTICAS DE CONTROL DE ACCESO 27
Política de acceso a redes y recursos de red 27
Controles 27
Política para la administración de accesos de usuarios 28
Controles 28
Política de responsabilidades de acceso de los usuarios 29
Controles 29
Política de uso de altos privilegios y utilitarios de administración 30
Controles 30
Política de control de acceso a sistemas y aplicativos 30

Controles 30
Política de controles criptográficos 32
Controles 32
Política para uso de conexiones remotas 32
Controles 32
Política para uso de tokens de seguridad 33
Controles 33
ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN 34
Política para el establecimiento de requisitos de seguridad 34
Controles 34
Desarrollo seguro, realización de pruebas y soporte de los sistemas 34
Controles 34
Política para la protección de los datos de prueba 36
Controles 36
Política de inclusión de condiciones de seguridad en la relación con terceras partes 36
Controles 36
Política de gestión de la prestación de servicios de terceras partes 37
Controles 37
RELACIÓN CON LOS PROVEEDORES 37
Controles 38
POLÍTICAS DE GESTIÓN DE INCIDENTES DE SEGURIDAD 38
Política para el reporte y tratamiento de eventos o incidentes de seguridad 38
Controles 38
Política de gestión de vulnerabilidades 40
Controles 40
POLÍTICAS DE INCLUSIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO 40
Política de continuidad, contingencia, recuperación y retorno a la normalidad con consideraciones de seguridad de la información 40
Controles 40
Política de redundancia 41

Controles 41
POLÍTICAS DE CUMPLIMIENTO 42
Política de cumplimiento con requisitos legales y contractuales 42
Controles 42
Política de privacidad y protección de datos personales 43
Controles 44
TÉRMINOS Y DEFINICIONES 45
VIGENCIA 47
SANCIONES PARA EL INCUMPLIMIENTO A LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN 47

INTRODUCCION

La información es uno de los principales activos para el desarrollo de las operaciones y cumplimiento de los objetivos misionales y estratégicos de la FUCS. En consecuencia, la información debe ser protegida de riesgos que afecten su confidencialidad, integridad y disponibilidad.

Mediante la evolución de nuevas tecnologías de la información y la puesta a producción de servicios (Herramientas/productos y software) para el cubrimiento de las necesidades de la FUCS y la optimización de los procesos misionales, se incorpora el requerimiento de protección de información tratada; de igual forma, todo aquello que contemple en proporcionar seguridad a sistemas, redes, dispositivos, software y servicios que son utilizados en la Fundación Universitaria de Ciencias de la Salud, en adelante FUCS.

El objetivo de implementar una Política de Seguridad de la Información abarca los activos de la FUCS, relacionados con la protección de los principios de Seguridad de la Información (Confidencialidad, Integridad y Disponibilidad).

POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

Generalidades

La Política de Seguridad de la Información de la FUCS está basada en normas, y procedimientos específicos, los cuales propenden por el manejo adecuado de la información de la institución. Así también, se establecen políticas específicas de seguridad de la información, fundamentadas en la norma internacional ISO 27001:2013.

La implementación, seguimiento y mejora continua de la Política de Seguridad de la Información, como también la aplicación de los controles que minimicen los riesgos asociados al manejo de la información que administran o consultan los colaboradores, estudiantes, proveedores y personal externo.

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

Para la implementación de cualquier proyecto de la FUCS, se tienen en cuenta las Políticas de Seguridad y Privacidad de la Información.

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 FUCS.
- Cumplir con los principios de seguridad de la información: Confidencialidad, Disponibilidad e Integridad.
- Fortalecer la cultura de seguridad de la información para mantener la confianza de los estudiantes, funcionarios y terceros relacionados con la razón de ser de la FUCS.

- Proteger los activos de información de la FUCS y la implementación de proyectos que se requieran acorde con los recursos dispuestos para tal fin.

Alcance

La presente Política se enuncia con el objeto de gestionar la seguridad de la información, los sistemas de información institucional y en general el ambiente tecnológico de la FUCS y tiene como fin propender por que la comunidad universitaria cumpla las normas establecidas.

Debe ser conocida y cumplida por todos los colaboradores (directivos, administrativos y docentes) y estudiantes de la FUCS, la política también contempla el cumplimiento por parte de contratistas.

La estructura de la política está basada, en los dominios contemplados en la norma internacional ISO 27001:2013 y toma como referencia, los requisitos más relevantes y aplicables a la FUCS.

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

Marco Normativo

Para la implementación de la presente Política de Seguridad de la información, se establece en la FUCS tomar como insumo principal los dominios descritos en las normas ISO/IEC 27001:2013, observando las mejores prácticas y protocolos de seguridad. Sin perjuicio de lo anterior, se contemplan para el desarrollo de la presente política las principales normas que contextualizan el marco regulatorio:

- Ley 1712 de 2014 – Ley de Transparencia y Acceso a la Información Publica
- Ley 1581 de 2012 – Ley de Tratamiento de Datos Personales
- Decreto 1377 de junio 27 de 2013-Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
- ISO 31000:2009 de Gestión de Riesgos
- ISO 22301 Continuidad del Negocio
- 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.

Objetivo General

Establecer directrices generales que permitan proteger los activos de información de la Institución, garantizando la confidencialidad, integridad y disponibilidad de la misma; dando cumplimiento a las leyes regulatorias en cuanto a seguridad de información y protección de datos personales orientado bajo la norma ISO/IEC 27001-2013.

Objetivos específicos

- Administrar, preservar y proteger la información de la FUCS, así como los recursos tecnológicos utilizados para su operación, almacenamiento y procesamiento; frente a amenazas internas o externas, permitiendo garantizar el cumplimiento de las características de confidencialidad, integridad y disponibilidad de la información.

- Mantener actualizada, vigente y operativa la Política de Seguridad de la Información de manera que pueda ser auditada de acuerdo a los riesgos identificados por la 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 FUCS.
- Generar cultura de uso seguro de los sistemas de información y su manipulación.
- Fortalecer la Seguridad, mediante la implementación de mecanismos de control que permitan identificar y contener los ataques y su materialización.
- Crear el sistema de gestión de eventos y/o incidentes mediante el desarrollo de capacidades de prevención, detección, contención, erradicación y respuesta ante amenazas.
- Brindar cumplimiento normativo y regulatorio a entes de control internos y externos en termas de protección de datos y activos de información.
- Identificar eventos de fraude y establecer acciones, para la protección del buen nombre de la FUCS.

Compromiso de la Alta Dirección

El Consejo Superior de la FUCS, da aprobación a la presente Política de Seguridad de la Información, mediante sesión No. 516 del veinticuatro (24) de septiembre de 2019. Comprometiéndose y apoyando en el diseño e implementación de políticas que garanticen la mitigación de riesgos de Seguridad de la Información:

- Revisión y aprobación de las presentes Políticas de Seguridad de la Información.
- Incentivar la cultura de Seguridad.
- Aprobar la divulgación de esta Política a todos los funcionarios de la FUCS.
- Establecer los recursos para implementar y mantener las iniciativas de seguridad de la información
- Validación del correcto cumplimiento de las presentes Políticas de Seguridad de la Información.

Roles, Responsabilidades y Autoridades

La FUCS, cuenta con el organigrama definido donde se identifica la estructura de primer nivel. En la estructura se observan todos los procesos, los cuales deberán dar cumplimiento las Políticas de Seguridad de la Información.

Las políticas aquí mencionadas aplican para los funcionarios y terceros que mantengan relación con el desarrollo de la misión de la FUCS y por tanto es responsabilidad de la Alta Dirección, velar por su cumplimiento.

Controles

Responsable	Actividades
Todos los Usuarios	• Cumplir la presente política de acuerdo con su rol como colaboradores, así como, personal externo que realice labores en o para la FUCS.

	• Recibir las capacitaciones o sensibilizaciones sobre Seguridad de la Información, de tal forma que tenga conocimiento respecto a las Políticas de Seguridad de la Información.
División de Gestión Humana	• Notificar a los funcionarios que ingresan nuevos, sobre la obligación de darle cumplimiento a las Políticas de Seguridad de la Información descritas en el presente documento.
Consejo Superior	• Aprobar roles y funciones relacionadas con la seguridad de la información en los diferentes niveles jerárquicos. • Asignar los recursos pertinentes para la aplicación eficaz de las Políticas de Seguridad de la Información de la institución.
Oficina de Auditoria de Gestión	• Auditar la presente Política de Seguridad de la Información.
División de Desarrollo Tecnológico	• Asignar las funciones, roles y responsabilidades, a los funcionarios encargados de la gestión y operación de la plataforma tecnológica de la institución.
Comité de Seguridad de la Información	• Revisar y proponer la actualización de Políticas de Seguridad de la Información, funciones, controles y actualizaciones que se deriven del Sistema de Gestión de Seguridad de la Información. • Definir las necesidades de capacitación que se presenten en la FUCS.
Seguridad De La Información	• Actualizar, documentar, sensibilizar y aplicar las normas y estándares aplicables para el mantenimiento de Sistema de Gestión de Seguridad de la Información.

ORGANIZACIÓN PARA DE LA SEGURIDAD DE LA INFORMACION

La FUCS construye una Política de Seguridad de la Información en la que se establecen los roles y las responsabilidades dentro de las que deben quedar asignadas actividades para la administración, operatividad, mejoramiento y gestión de la seguridad de la información.

La FUCS, es la responsable del Sistema de Gestión de Seguridad de la Información. Es un asunto de gran relevancia para los directivos, que en consecuencia apoyan la creación del Comité de Seguridad de la Información, integrado por delegados de las instancias académicas y administrativas. El comité debe encargarse de garantizar el soporte manifiesto al sistema de gestión de la seguridad.

Funciones del Comité de Seguridad de la Información:

- Revisar y proponer mejoramiento a la Política de Seguridad de la Información frente a las responsabilidades de los diferentes actores institucionales.

- Estar atento a los riesgos, sus cambios significativos y afectación de los recursos de información, frente a las principales amenazas.
- Conocer y supervisar los eventos o incidentes relativos a la seguridad de la información.
- Revisar y aprobar las iniciativas tendientes a mejorar la seguridad de la información.
- Acordar y aprobar las metodologías y procesos específicos de Seguridad de la Información.
- Garantizar que todos los procesos de gestión se alineen con la Política de Seguridad de la Información.
- Coordinar, evaluar y promover la implementación de los controles específicos de seguridad de la información para nuevos servicios tecnológicos o sistemas.
- Respaldar e impulsar la difusión de la seguridad de la información y su importancia, dentro de comunidad universitaria.
- 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.

Organización Interna

Todos los funcionarios deben actuar de acuerdo con las Políticas de Seguridad de la Información participando en las revisiones de seguridad que se lleven a cabo. Adicionalmente, participar en las distintas capacitaciones y/o jornadas de sensibilización lideradas por División de Desarrollo Tecnológico y Seguridad de la Información.

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

- Aceptar y cumplir las Políticas de Seguridad de la Información que se establezcan en la FUCS.
- Aceptar la responsabilidad de proteger la información de la 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 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 las mismas.
- Los funcionarios deben utilizar la información de la FUCS exclusivamente para fines laborales, quedando prohibido explícitamente cualquier uso comercial y/o privado no autorizado.
- Los terceros (contratistas o proveedores) que interactúan con la 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 FUCS.
- Debe existir un responsable para cada uno de los recursos de tecnología y activos de información usados en la FUCS. Las responsabilidades deben estar delimitadas de tal manera que no existan varios responsables de un mismo recurso.

GESTION DE ACTIVOS DE INFORMACIÓN

La FUCS como propietaria de la información física y digital; generada, procesada, almacenada por diferentes instancias institucionales y transmitidas 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 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 realizará anualmente, identificando; responsable de los activos, custodios, ubicación, amenazas, vulnerabilidades, usuarios y los controles que se tienen implementados para garantizar la confidencialidad, disponibilidad e integridad de la información.

El inventario y clasificación que se otorga a los activos de información, debe ser reconocido por el líder del proceso o funcionario designado, con el acompañamiento de Seguridad de la Información durante el ejercicio de actualización o elaboración de activos de información.

De acuerdo a lo anterior, la FUCS establece la clasificación de los activos conforme a lo dispuesto en la ley 1712 de 2012 respecto a que la clasificación debe ser: publica, publica clasificada, publica reservada.

Política de clasificación de la Información

La 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 establecer 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 12 meses.

Confidencialidad

Para la 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 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 legar 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 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 perdida de exactitud o que se encuentre incompleta, puede generar un impacto no significativo en la imagen reputacional, aspectos jurídicos o económicos.

Disponibilidad
Para la FUCS la información se encontrará disponible para el acceso por solicitud de un proceso, institución o proceso autorizado, en el momento y en el medio requerido, así como los recursos necesarios para su uso. Los niveles de clasificación para ésta 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.

Clasificación de la Información	Sigla para el Etiquetado	Descripción
Información Publica 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 Publica Clasificada	IPC	Esta información es de acceso a varios funcionarios de la FUCS para realizar labores propias del área. No podrá ser utilizada por terceros sin autorización previa del administrador de la información.
Información Publica	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 FUCS.

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

La información (pública clasificada o reservada o dato sensible) 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 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 FUCS. • Proveer los métodos de cifrado de la información y gestionar la contratación y actualización de las herramientas tecnológicas usadas para este fin. • Garantizar que la depuración y la eliminación de la información se realice de una manera efectiva a través de los mecanismos necesarios en los casos de renovación de plataforma tecnológica o novedades de usuario. • Aplicar mecanismos de control necesarios, que garanticen los principios de Seguridad de la Información de los recursos tecnológicos bajo su custodia. • Debe garantizar la destrucción de información física, cuando se ha cumplido su ciclo de almacenamiento. • Debe verificar 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).
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 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 FUCS. • La información en medio físico y digital de la 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, toda la información debe ser apropiadamente eliminada. • 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 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 FUCS y sus funcionarios deben garantizar las condiciones adecuadas de almacenamiento, resguardo y acceso físico a la información que se encuentra en documentos físicos.

Política de Medios Removibles

La FUCS debe garantizar que la información almacenada en cualquier medio removible, que vaya a ser entregada a un ente externo; sea removida de tal forma que no se pueda recuperar.

Todos los medios removibles que contengan información de la 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	• Analizará 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	• Realizar oportunamente una copia de respaldo que mitigue la pérdida de información. • Implementar las acciones establecidas en el comité de Seguridad de la Información, tendientes a mitigar cualquier riesgo relacionado con medios removibles.
Todos los Usuarios	• Deberá asegurar que la información allí contenida, no esté expuesta a ningún riesgo. • La información considerada como "Información Publica Clasificada" o "Información Publica Reservada"; deberá estar bajo los controles establecidos.

POLÍTICAS DE SEGURIDAD DEL TALENTO HUMANO

Política relacionada con la vinculación de funcionarios

Para la 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 funcionarios se realice mediante un proceso adecuado de selección, orientado a la asignación de actividades y roles de acuerdo a las funciones que se encuentran descritas en sus funciones de cargo.

Controles

Responsable	Actividades
Gerencia – División de Gestión Humana	• Garantizar que los funcionarios de la Institución conozcan y acepten firmando los documentos de Confidencialidad; éstos 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 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 FUCS, confirmar la aceptación de los acuerdos y/o cláusulas de confidencialidad para los funcionarios provistos por terceras partes.
Funcionarios Provistos por Terceras Partes	• 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 FUCS.

Política de desvinculación, licencias, vacaciones o traslados de los funcionarios y personal provisto por terceros

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

Controles

Responsable	Actividades
División de Gestión Humana	• Debe ejecutar los controles concernientes a la seguridad de la información para realizar los procesos de novedades de personal (reasignación, retiro, desvinculación, vacaciones) y de acuerdo con los procedimientos establecidos para este fin. • Verificar los reportes de novedades y seguidamente solicitar 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 personal provisto por terceras partes a la División de Gestión Humana.
Oficina de Auditoría de Gestión	• Monitorear el cumplimiento de las políticas y 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 Humana y/o líderes de área, así mismo, garantizará la inactivación temporal.
Seguridad de la Información	• Realizar monitoreo a los cambios o modificaciones de estados de los usurarios en los aplicativos de acuerdo al reporte de novedades generado por División de Gestión Humana y/o líderes de área.

SEGURIDAD FÍSICA Y DEL ENTORNO

Política de áreas seguras

La 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.

Controles

Responsable	Actividades
División de Desarrollo Tecnológico	• Aprobar todo acceso a los datacenter o centros de cableado de la FUCS por funcionarios de la División de Desarrollo Tecnológico autorizados; de igual forma todo visitante deberá estar siempre acompañado por un

	funcionario 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 los 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 los data center; se debe contar con los sistemas de: control de temperatura y humedad, detección y extinción, incendios, alertas, monitoreo y alarmas en caso de detección de cambios de estas condiciones ambientales. • 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 FUCS ubicados en los 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 alejados 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 funcionarios 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 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 funcionarios autorizados. Las contraseñas de los sistemas de alarma, las cajas fuertes, las llaves y cualquier otro elemento de seguridad estará restringido a 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 FUCS.
Oficina Infraestructura Física	• Proveer los requerimientos necesarios para apoyar, resguardar y velar por el perfecto estado de los controles físicos establecidos en los diferentes espacios de la 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 al FUCS que procesen información.
División de Servicios Administrativos	• Validar que se encuentre monitoreado el Circuito Cerrado de Televisión (CCTV) que graba el perímetro de la FUCS.
Usuarios	• Todos los funcionarios y terceros deben portar el carné visible durante su visita a las áreas de la institución, si lo pierden deben reportarlo inmediatamente a División de Gestión Humana. • Todo personal externo o tercero que por su servicio brindado ingrese a la FUCS por autorización de funcionarios, debe contar con algún distintivo que permita identificarlo y no debe ingresar a lugares que no tenga autorización. • Los funcionarios y/o proveedores, que tengan acceso a las instalaciones de la FUCS, no pueden fumar o consumir alimentos cerca de los equipos. • 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 FUCS lo requiera. • Los funcionarios que tengan asignado uno o más equipos de cómputo, durante el tiempo en el cual cesan las actividades, será su responsabilidad bloquear la sesión del equipo para evitar que terceros no autorizados accedan a la información contenida. Es responsabilidad de todos los funcionarios una vez finalice la jornada laborar, cerrar las sesiones activas y dejar los equipos apagados. • Con el fin de velar por los principios de Seguridad de la Información de información sensible o crítica de la FUCS y evitar pérdidas, daños o accesos no autorizados, todos los funcionarios deben ser responsables de mantener la información custodiada bajo llave o en la cajonera de

	trabajo, cuando se encuentren desatendidos o en horas no laborales. Una vez el funcionario realice la autenticación en las distintas impresoras, se debe recoger de manera inmediata la información impresa, escaneada o copiada. • Todos los equipos de cómputo deben tener políticas de protector de pantalla corporativo, con un tiempo de activación automática de cinco minutos. • Los funcionarios que manejen información de la FUCS a través de dispositivos móviles deberán protegerla física y lógicamente con el fin de evitar el hurto, acceso o divulgación de información no autorizada.
Seguridad de la Información	• Monitorear el cumplimiento de las políticas relacionadas con el buen uso de los equipos de cómputo, así como el manejo de información en áreas seguras.

POLÍTICAS DE SEGURIDAD EN LAS OPERACIONES

Política de 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 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 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.

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

Los instructivos o manuales de hardware/software como mínimo deberán especificar las instrucciones para la ejecución de cada actividad, incluyendo el procesamiento y manejo de la información, restricciones en el uso de utilitarios del sistema, resguardo de información, gestión de evento o incidentes de seguridad de la información, así como el uso del correo electrónico y de las aplicaciones de la 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 funcionarios 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 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	• Emitir el concepto sobre las soluciones de seguridad adecuadas para la gestión sobre la plataforma tecnológica de la FUCS.
Supervisores de Contrato División de Desarrollo Tecnológico	• Los cambios que se generen sobre cualquier componente de tecnología, como consecuencia de un requerimiento de usuario, de la solución de un incidente o de una actualización deben ser controlados, gestionados y autorizados adecuadamente, y deben ser sometidos a una evaluación que permita identificar riesgos asociados que pueden afectar la operación.

Política de protección frente a software malicioso

Todos los recursos de la plataforma tecnológica FUCS 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, generar 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 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.

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 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.
Usuarios	• Deben conservar la configuración del software 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. • Notificar de forma inmediata a la mesa de ayuda cuando se detecte o sospeche alguna infección por software malicioso.

Así mismo, la 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.
- Utilizar otros medios de almacenamiento que no estén permitidos en la FUCS.

Política de copias de respaldo de la información

Sobre la información institucional, que pertenezca a los procesos operativos y de misión crítica de la 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.

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.
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, de la los activos información generados por su área.
Usuarios	• Identificar y clasificar la información crítica que debe ser respaldada y almacenada.

Política de eventos y monitoreos a los recursos tecnológicos y Sistemas de Información
La FUCS, a través de la División de Desarrollo Tecnológico debe realizar el monitoreo constante de todos los recursos de la plataforma tecnológica y los aplicativos de la institución. Seguridad de la Información verificará la custodia de los registros de auditoría de manera que se cumpla con las tablas de retención establecidas.

Controles

Responsable	Actividades
División de Desarrollo Tecnológico	• Debe establecer los tipos de eventos que deben registrar los logs o registros de auditoría, 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 FUCS para efectos de auditoría.
Desarrolladores (Internos y Externos)	• Registrar en los registros (logs) de actividad todos aquellos eventos relacionados con interrupciones, acceso, modificación de acuerdo con los lineamientos establecidos por la División de Desarrollo Tecnológico y evitar registrar datos innecesarios.

Política de seguridad para los equipos institucionales
La 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 los mismos.

Controles

Responsable	Actividades
División de Desarrollo Tecnológico	• Implementar estrategias y desarrollar mecanismos que certifiquen 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 FUCS. • Asegurar el cumplimiento de los estándares de configuración fiables para los equipos asignados a los empleados de la 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 FUCS, así como exigir el estricto cumplimiento antes de dar acceso a la red de la institución. • Establecer zonas aisladas para los equipos en los 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 funcionarios de la FUCS. • Verificar periódicamente los equipos de cómputo de la FUCS, especialmente aquellos que se encuentran ubicados en áreas sensibles.
Seguridad de la Información	• Evaluar y analizar los informes relacionados con listas de chequeo, prevista para la revisión del parque computacional de la FUCS, en particular de las áreas con información sensible.
Oficina de Activos Fijos	• Revisar los accesos físicos en horas no hábiles a las áreas donde se procesa información. • Validar la aprobación de entrada y salida de las instalaciones de la 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.
Usuarios	• Cumplir con los movimientos y asignación de recursos tecnológicos autorizados por la División de Desarrollo Tecnológico; por tal motivo se prohíbe la disposición por los funcionarios ajenos a esta dirección. • 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 la mesa de ayuda 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 FUCS. No está permitido que el usuario intente solucionar el problema. • Evitar la reparación, instalación o cambio de cualquier elemento de hardware o software de equipos de cómputo, puestos de trabajo, equipos móviles y o Sistemas de Información. Estas actividades sólo pueden ser realizadas por los funcionarios de la División de Desarrollo Tecnológico, o en determinados casos por personal de terceras partes autorizado por dicha área. • Bloquear las sesiones de usuarios de las estaciones de trabajo cuando no se encuentren frente a ellas, así como apagarlas en horarios no laborales.

POLÍTICAS DE SEGURIDAD EN LAS COMUNICACIONES

Política de gestión y aseguramiento de las redes de datos

La 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 FUCS. • Definir 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 FUCS. • Realizar la segmentación de la red de datos, de acuerdo con la clasificación de usuarios, tipo de datos, servicios y demás característica 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 FUCS. • Habilitar únicamente los servicios, protocolos y puertos de comunicación necesarios para la operación de las redes de datos FUCS restringiendo los demás que no se requieran para evitar intrusiones y ataques mal intencionados. • Instalar plataformas de protección entre las redes internas de la FUCS y redes externas que representen una amenaza para la plataforma tecnológica de la FUCS.

	• Mantener la confidencialidad de la información de configuración y funcionamiento de las redes de datos de la FUCS.

Política de 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 funcionarios y/o personal externo que hacen uso de este medio.

Controles

Responsable	Actividades
División de Desarrollo Tecnológico Seguridad de la Información	• Generar y divulgar el instructivo y las directrices para la gestión de cuentas de correo electrónico. • Diseñar 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. • Generar campañas que permitan la concientización de los usuarios acerca de las medidas de prevención que se deben tener en cuenta al momento de intercambiar información por este medio.
Usuarios	• Cumplir el uso individual y responsable de la cuenta de correo electrónico asignada por la FUCS. Para el desarrollo de las funciones asignadas por la institución y no hacer uso del correo institucional para actividades personales. • Evitar el envío de cadenas de mensajes que contengan información no institucional (político, religioso, comercial, contenido discriminatorio, pornografía, etc.) • Reportar correos electrónicos de procedencia sospechosa.

Política de uso adecuado de internet

La FUCS reconoce la importancia del uso de Internet como apoyo para el desempeño de labores, Así como soporte al proceso 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, evitando 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. Evitar 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.

Política de intercambio de información

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

Controles

Responsable	Actividades
Oficina 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. • Participar en la elaboración de 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 FUCS.
División de Desarrollo Tecnológico	• Definir los procedimientos, servicios y herramientas para proteger con controles la información trasmitida a los terceros que tienen relación con la FUCS. • Vigilar que el intercambio de información de la FUCS con externos, se encuentren alineadas con las Políticas 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 FUCS.

	• Registrar el intercambio de información, en donde se especifique el tipo de información intercambiada, así como los datos de 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	• Acoger los procedimientos de intercambio de información con terceros en medio físico o digital, así como cumplir que eviten la divulgación no autorizada, destrucción, perdida o alteraciones.
Terceros con Quienes se Intercambia Información de la FUCS	• Dar manejo adecuado a la información que intercambia con la FUCS cumplimiento con procedimientos, controles, condiciones contractuales de seguridad de la FUCS, así como realizar de manera segura, la destrucción o eliminación de la información suministrada cuando ya no se requiera.
Usuarios	• Hacer uso de medios adecuados para enviar o recibir información sensible, no se debe utilizar ni el correo electrónico personal ni medios telefónicos para enviar o recibir información sensible de la FUCS.

POLÍTICAS DE CONTROL DE ACCESO

Política de 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 el procedimiento de autorización y control de acceso a las redes y recursos tecnológicos de la FUCS, con el fin de proteger el ingreso indebido de terceros. • Establecer controles de autenticación y autenticidad de los usuarios internos y externos a las redes y/o recursos de red de la FUCS. • Se debe tratar las redes inalámbricas "WIFI" como redes externas y separarlas de las redes internas, garantizando de esta manera el cumplimiento de los principios de Seguridad de la Información de la 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 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 la mesa de ayuda. El acceso a la red wifi para visitantes se realiza a través de la red definida para el fin y con uso de la clave establecida que será suministrada por el líder de proceso y/o la División de Desarrollo Tecnológico.

Política para la administración de accesos de usuarios

La FUCS garantiza que se establezcan los tipos de privilegios para el control de acceso lógico de usuarios o grupos de usuarios internos y externos a las redes de datos y a los recursos de infraestructura tecnológica y a los sistemas de información de la institución. Es importante que el acceso del personal externo se encuentre claramente limitado y bajo los controles y procedimientos establecidos.

Controles

Responsable	Actividades
División de Desarrollo Tecnológico	• Establecer 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. El Comité de Seguridad de la Información definirá las actividades pertinentes para la administración de roles y perfiles. • 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 Humana. • 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 políticas de utilización de Internet para los usuarios (estudiantes/funcionarios/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 Accesos.
Líderes de los Activos de Información Seguridad de la Información	• Establecer los perfiles de usuario, junto con el Comité de Seguridad de la Información.
Líderes de Procesos	• Verificar y ratificar con una periodicidad definida 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 funcionarios que pertenecen a cada área cumpliendo los procesos y formatos de solicitud vigentes. • La División de Gestión Humana deberá mediante procedimiento informar a la División de Desarrollo Tecnológico y a Seguridad de la Información las novedades del personal, en las que se requiera modificación de cuentas accesos y privilegios de usuarios. • 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.

Política de 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 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 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 FUCS, deben acogerse a los lineamientos establecidos para la configuración de cuentas de usuario y contraseñas implementados por la FUCS.

Política de 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 funcionarios 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.
Seguridad de la Información	• Revisar con una periodicidad definida el registro de actividad de usuarios y privilegiados sobre los servicios de la plataforma tecnológica.

Política de control de acceso 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 Seguridad de la Información	• Autorizar de acuerdo con los procedimientos los accesos según los perfiles establecidos y necesidades de uso, el acceso a los sistemas de información o aplicativos. • Monitorear periódicamente la definición de perfiles y asignación de privilegios a los usuarios que acceden en los

	sistemas de información, así mismo, deberá notificar al Comité de Seguridad de la Información, aquellas inconsistencias. • 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 FUCS. • 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.
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 definido. • 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 FUCS, deben tener políticas 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 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.
Seguridad de la Información	• Seguridad de la Información realizará verificaciones periódicas y aleatorias a las actividades realizadas con el usuario administrador de los sistemas de información críticos de la FUCS.

Política de controles criptográficos

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

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 reservada o restringida y seguir los estándares establecidos por la División de Desarrollo Tecnológico

Política para 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 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 FUCS, así como su monitoreo permanente. • Autorizar sólo a determinados funcionarios 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 mesa de ayuda, y luego de la aprobación, debe 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 actualizado.

Política para uso de tokens de seguridad

La FUCS vigilará un uso responsable de los tokens por parte de los funcionarios 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 funcionario 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 funcionario, mediante bases de datos y actas de entrega que permitan, procedimientos agiles 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 asignados a cada colaborador por lo que se deben devolver, cuando el vínculo laboral con la 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.

ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

Política para el establecimiento de requisitos de seguridad

La 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
Propietarios de los Sistemas de Información División de Desarrollo Tecnológico	• Definir un área física designada y con las medidas de protección dentro de la FUCS para el desarrollo de sistemas de información o software. • 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. • Las áreas propietarias de los sistemas de información, deben apoyar a la División de Desarrollo Tecnológico con los requerimientos para la adquisición, desarrollo de software o sistemas de información, teniendo en cuenta los controles como; autenticación, acceso y diseño de aplicaciones que garanticen la seguridad de la 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.

Desarrollo seguro, realización de pruebas y soporte de los sistemas

La 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 FUCS.

Controles

Responsable	Actividades

Propietarios de los Sistemas de Información	• 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. • Aprobar mediante control de cambios las migraciones entre los diferentes ambientes de desarrollo, pruebas, calidad y producción de los productos entregados.
División De Desarrollo Tecnológico	• 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).
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 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 de 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.
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.

Política para la protección de los datos de prueba

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

Controles

Responsable	Actividades
División de Desarrollo Tecnológico	• Asegurar que la información usada en ambientes de pruebas sea eliminada cuando se culminen las pruebas.

Política de inclusión de condiciones de seguridad en la relación con terceras partes

La FUCS establece 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 FUCS.

Los funcionarios de la FUCS encargados de establecer estas relaciones son los responsables de comunicar la documentación; procedimiento y Políticas de Seguridad de la Información.

Controles

Responsable	Actividades
División de Desarrollo Tecnológico y Oficina Jurídica	• Establecer ANS y servicios requisitos 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.
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 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 y procedimientos establecidos por la 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.
Seguridad de la Información	• Validar el cumplimiento de los ANS acuerdos de niveles de servicio, cumplimiento de estándares, normatividad y controles necesarios para la protección de los principios de seguridad (Confidencialidad, Integridad y Disponibilidad).

Política de gestión de la prestación de servicios de terceras partes

La 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 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 de acuerdos de niveles de servicio, 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, de confidencialidad e intercambio de información, así como los requisitos de seguridad de la información establecida en relaciones con terceros. • Administrar y controlar las novedades y monitorear la aparición de nuevos riesgos en el suministro de servicios, de los proveedores.

RELACIÓN CON LOS PROVEEDORES

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

Se tienen establecidos mecanismos de control en la relación con proveedores y terceros, de tal forma que se dé cumplimiento a la Política 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 FUCS o de los activos de información, a proveedores o terceros hasta no tener firmados y formalizados contratos o acuerdos, confidencialidad, integridad y disponibilidad.
Proveedores y/o Terceros	• Todos los proveedores y terceros que vayan a tener acceso a información confidencial de la FUCS, deben cumplir con las medidas mínimas de Seguridad de la Información. • Dar cumplimiento a los controles, protocolos deseados por la 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.
Funcionarios	• Los funcionarios responsables de la supervisión de contratos o convenios con proveedores y terceros, deben dar a conocer las políticas y normas de Seguridad de la Información de la FUCS a dichas partes, así mismo, debe velar porque se dé accesos correctos y de almacenamiento de forma segura a los recursos de la FUCS.
Seguridad de la Información	• Realizar monitoreos y seguimientos a los proveedores que tengan acceso a información confidencial de la FUCS.

POLÍTICAS DE GESTIÓN DE INCIDENTES DE SEGURIDAD

Política para el 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	Reportar los eventos o incidentes de seguridad a Seguridad de la Información.

División de Desarrollo Tecnológico	• Mantener actualizada la documentación de infraestructura tecnológica de la FUCS permitiendo establecer criticidad impacto y consecuencias de materialización de incidentes de seguridad.
Comité de Seguridad de la Información	• Establecer responsabilidades y procedimientos que permitan una respuesta rápida y efectiva a los eventos o incidentes de 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. • 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. • 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. • Implementar planes de lecciones aprendidas donde se comunique y sensibilice respecto a los eventos o incidentes que ya han sido reportados y atendido, permitiendo así mayor sensibilización y menos tiempo de respuesta frente a un posible evento o incidente de Seguridad de la Información.
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 también se debe reportar a la División de Desarrollo Tecnológico para la gestión correspondiente.
Seguridad de la Información	• Documentar procedimientos, donde se establezcan responsables y actividades que permiten brindar respuestas oportunas a los eventos reportados. • 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. • Mantener registro de todos los eventos reportados por los funcionarios, 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 las políticas cuando sea necesario.

Política de gestión de vulnerabilidades

La FUCS, a través de la División de Desarrollo Tecnológico y Seguridad de la Información, ejecutarán 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.

Controles

Responsable	Actividades
División de Desarrollo Tecnológico	• Coordinará una vez al año, el análisis de vulnerabilidades técnico a la infraestructura tecnológica de la 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.

POLÍTICAS DE INCLUSIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

Política de continuidad, contingencia, recuperación y retorno a la normalidad con consideraciones de seguridad de la información

La 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 o eventos catastróficos y que afecten la continuidad de su operación de la 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	• Aceptar y reconocer las situaciones identificadas como emergencia o desastre para los procesos o áreas de la 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. • Aprueba 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. • Aprueba 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 recuperación para la infraestructura tecnológica de la FUSC, 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 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.
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. • Realizar una vez al año una prueba al plan de continuidad con el fin de evaluar su efectividad e identificar nuevos escenarios.

Política de redundancia

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

Controles

RESPONSABLE	ACTIVIDADES
División de Desarrollo Tecnológico	• Analizar y construir los requisitos de redundancia para los aplicativos de misión crítica, para la 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 FUCS.
Seguridad de la Información	• Documentar en el Plan de Continuidad la política de redundancia de los aplicativos de misión crítica de la FUCS, así como la plataforma tecnológica que los soporta.

POLÍTICAS DE CUMPLIMIENTO

Política de cumplimiento con requisitos legales y contractuales

La 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 FUCS establece que la información personal de los funcionarios y/o contratistas 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 funcionario y/o contratista o en los casos en que la normatividad lo permita.

Es responsabilidad de Seguridad de la Información, propender por el cumplimiento de las políticas establecidas en este documento, registrar los procesos, procedimientos, manuales, instructivos, formatos y políticas específicas alineados al estándar internacional ISO 27001:2013 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 FUCS, normatividad vigente entre otros.

Controles

Responsable	Actividades
Oficina Jurídica	• Documentar, actualizar e identificar los requisitos legales, reglamentados y aplicados a contratos y a la seguridad de la información de la FUCS. • Es la responsable de asesorar a la FUCS sobre los requisitos normativos y regulatorios dados por entes de control, así como de las obligaciones con terceros y funcionarios, siempre enmarcados dentro del cumplimiento de la legislación colombiana vigente.
División de Desarrollo Tecnológico	• Verificar que todo software y hardware que forme parte de los recursos tecnológicos de la FUCS, cuente 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 sistema de información y de recursos digitales, que estén autorizados para ser usados en los computadores o recursos de la infraestructura tecnológica de la 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 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 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	• 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. • Garantizar la definición y cumplimiento de los requerimientos de seguridad de la Información y en conjunto con la Unidad 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.
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 FUCS suministrado para sus actividades. • Los funcionarios de la 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 DDT con previa autorización de Seguridad de la Información.
Proveedores	• Deben existir acuerdos contractuales claramente definidos entre la 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.

Política de privacidad y protección de datos personales

La FUCS como responsables del manejo de datos personales, propenderá por la protección de la información de sus funcionarios, estudiantes, proveedores y terceros de los cuales gestione información, dando cumplimiento a la Ley 1581 de 2012, la cual establece los derechos y deberes del tratamiento de los datos personales.

Se establecerán los términos, condiciones y finalidades para los que la FUCS, como encargado 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 a las actividades de la FUCS.

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, der acuerdo a lo establecido a la Ley 1581 de 2012, así mismo, deberá implementar las medidas de Seguridad y Privacidad para la custodia de los datos personales.

Controles

Responsable	Actividades
Áreas que Procesan Datos Personales	• Para el procesamiento de datos personales de funcionarios, estudiantes, proveedores o terceros, 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 FUCS. • Asegurar el acceso a datos, sólo para aquellas personas que tengan una necesidad laboral legitima. • 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 mensajes por medio de correo electrónico y mensajes de texto. • Conocer y aplicar la Política de Protección de Datos Personales publicada en la página web de la FUCS.
Seguridad de la Información	• Dar acompañamiento a los controles de tratamiento de datos personales de los funcionarios, estudiantes, docentes, colaboradores o terceros de la FUCS. • Documentar y actualizar las Políticas de Protección de Datos personales de la FUCS. • Sensibilizar a los funcionarios sobre la protección de datos personales en la FUCS.
División de Desarrollo Tecnológico	• Crear controles que permitan proteger la información personal de los estudiantes, docentes, administrativos, directivos, proveedores y otras personas almacenada en las bases de datos o cualquier otro repositorio de información y evitar manejo (divulgación, alteración o eliminación) sin la previa autorización.
Todos los Usuarios	• Guardar la reserva absoluta de la información de la FUCS (sus estudiantes, docentes, administrativos, directivos, proveedores y otras personas).

	• Verificar la identidad de las personas, a quienes se les entrega datos o información vía telefónica, correo electrónico o correspondencia, etc.
Usuarios de los Portales de la 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 FUCS. • Atender las solicitudes judiciales y/o de entender de control que requieren datos personales de conformidad con la ley.

TÉRMINOS Y DEFINICIONES

Para los propósitos de esta política, se aplican los siguientes términos y definiciones:

- **Aceptación del riesgo:** decisión de asumir un riesgo. (NORMA TECNICA COLOMBIANA NTC-ISO/IEC 2701)
- **Activo:** cualquier cosa que tiene valor para la organización. (NORMA TECNICA COLOMBIANA NTC-ISO/IEC 2701)
- **Análisis de riesgo:** uso sistemático de la información para identificar las fuentes y estimar el riesgo. (NORMA TECNICA COLOMBIANA NTC-ISO/IEC 2701)
- **Autenticidad:** busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.
- **Auditabilidad:** define que todos los eventos de un sistema deben poder ser registrados para su control posterior.
- **Confidencialidad:** propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados. (NORMA TECNICA COLOMBIANA NTC-ISO/IEC 2701)
- **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:** propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.
- **Evaluación del riesgo:** proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo. (NORMA TECNICA COLOMBIANA NTC-ISO/IEC 2701).
- **Evento de seguridad de la información:** presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad. (NORMA TECNICA COLOMBIANA NTC-ISO/IEC 2701)

- **Gestión del riesgo:** actividades coordinadas para dirigir y controlar una organización en relación con el riesgo. (NORMA TECNICA COLOMBIANA NTC-ISO/IEC 2701)
- **Incidente de seguridad de la información:** un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información. (NORMA TECNICA COLOMBIANA NTC-ISO/IEC 2701)
- **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. (NORMA TECNICA COLOMBIANA NTC-ISO/IEC 2701)
- **Legalidad:** Se refiere al cumplimiento de las leyes, medidas, reglamentaciones o disposiciones a las que está sujeta la Institución.
- **Protección a la duplicación:** consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario.
- **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 residual:** nivel restante de riesgo después del tratamiento del riesgo. (NORMA TECNICA COLOMBIANA NTC-ISO/IEC 2701)
- **Seguridad de la información:** preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad (Accountability), no repudio y fiabilidad. (NORMA TECNICA COLOMBIANA NTC-ISO/IEC 2701)
- **Sistema de Información:** se refiere al conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.
- **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 FUCS, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otros.
- **Tratamiento del riesgo:** proceso de selección e implementación de medidas para modificar el riesgo. (NORMA TECNICA COLOMBIANA NTC-ISO/IEC 2701)
- **Valoración del riesgo:** proceso global de análisis y evaluación del riesgo. (NORMA TECNICA COLOMBIANA NTC-ISO/IEC 2701).
- **Organización de la Seguridad:** facilita la gestión de la seguridad de la información dentro de la institución.
- **Gestión de Activos de Información:** permite proteger los activos de información institucional.
- **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 FUCS.

- **Seguridad física y del entorno:** Permite definir controles que eviten accesos no autorizados tanto a instalaciones e información.
- **Gestión de Comunicaciones y Operaciones:** establece controles para garantizar el correcto funcionamiento de los equipos de procesamiento de la información.
- **Control de Acceso:** definir controles para limitar el acceso lógico a la información y a los espacios donde se procese información.
- **Adquisición, Mantenimiento y Desarrollo y de Sistemas de Información:** define controles con el fin de racionalizar gastos integrales de los sistemas de información institucionales.
- **Gestión de incidentes de seguridad de la información:** con el objetivo de gestionar los incidentes presentados y tomar las acciones necesarias de prevención y corrección.
- **Continuidad tecnológica de la 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.

VIGENCIA

Las políticas contenidas en el presente documento se encuentran vigentes y aprobadas por el Consejo Superior en la sesión No. 516 del veinticuatro (24) de septiembre de 2019.

SANCIONES PARA EL INCUMPLIMIENTO A LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

La Política de Seguridad de la información, pretende instituir y afianzar la cultura de información segura, en los funcionarios, estudiantes, personal externo y proveedores de la FUCS. La violación a la Política de Seguridad de la Información puede acarrear acciones disciplinarias.