FUNDACIÓN DE EDUCACIÓN SUPERIOR
SANJOSÉ
INSTITUCIÓN TECNOLÓGICA

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Fundación De Educación Superior San José

FUNDACIÓN DE EDUCACIÓN SUPERIOR
SANJOSÉ
INSTITUCIÓN TECNOLÓGICA

CONSEJO DIRECTIVO

Francisco Alfonso Pareja González.
Fundador

Dra. Romelia Ñuste.
Rectora

EdD. Luis C. Gutiérrez M.
Secretario General

Dra. Stefanny Camacho.
Vicerrectoría Académica

FUNDACIÓN DE EDUCACIÓN SUPERIOR

SANJOSÉ

INSTITUCIÓN TECNOLÓGICA

Nombre de Gobierno actual al momento de emisión de la política

Fundador
FRANCISO ALFONSO FERNANDO PAREJA GONZANALEZ

Rector
ROMELIA ÑUSTE

Vicerrectora
LEIDY STEFANNY CAMACHO GALINDO

Secretario General
LUIS CARLOS GUTIERREZ MARTINEZ

Comité de TIC

Gerente General:
FRANCISO ALFONSO FERNANDO PAREJA GONZANALEZ

Rectora:
ROMELIA ÑUSTE

Vicerrectora:
LEIDY STEFANNY CAMACHO GALINDO

Director de Planeación:
LUIS CARLOS GUTIERREZ MARTINEZ

Jefe Oficina de Infraestructura Física y Tecnologica:
JUAN DAVID MARTINEZ BOHORQUEZ

Contenido

Reconocimiento

El Comité de TIC agradece por cada una de las dependencias y a las autoridades académicas que le permitieron realizar esta política y expresan su reconocimiento a todas y cada una de las personas que hicieron posible llevar a cabo la elaboración de esta política institucional

Introducción

La información es vital para un correcto desempeño dentro de una empresa, sin importar qué tipo de información se trate dentro de ella, ésta es parte primordial en el cumplimiento de sus objetivos, es por ello que resguardar todo tipo de Información de cualquier posibilidad de alteración, mal uso, pérdida, entre otros muchos eventos, puede significar un respaldo para el normal desarrollo de las actividades.

Realizando una gestión amplia y suficiente de los siguientes ítems:

- Minimizar el riesgo de los procesos misionales de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de comunidad académica.
- Apoyar la innovación tecnológica.
- Proteger los activos de información.
- Garantizar la continuidad del servicio frente a incidentes.

Esta política deberá ser conocida y cumplida por toda la comunidad académica, tanto se trate de personas administrativas y técnicas, como estudiantes y la planta de docentes, ya sea cual fuere su nivel jerárquico dentro de la institución.

Marco General de la Política

Esta policita es de carácter institucional, de acuerdo a diferentes estándares en pro de la seguridad de la información.

- **Ley 1581 de 2012**: Esta ley establece el régimen general de protección de datos personales en Colombia y regula la recolección, almacenamiento, uso y circulación de la información personal. Las IES están obligadas a cumplir con esta normativa y contar con medidas de seguridad que protejan la información personal de los estudiantes, docentes y demás personal de la institución.

- **Decreto 1377 de 2013:** Este decreto reglamenta la Ley 1581 de 2012 y establece las obligaciones específicas para el manejo de datos personales en Colombia. En el ámbito de las IES, se exige la implementación de medidas técnicas y organizativas para garantizar la seguridad de la información personal.

- **Ley 1273 de 2009:** Esta ley establece el régimen de protección de la información y los datos en Colombia y regula los delitos informáticos. Las IES están obligadas a tomar medidas de seguridad para proteger la información de la institución y prevenir la comisión de delitos informáticos.

- **Resolución 20141200555425 de 2014:** Esta resolución establece los requisitos mínimos de seguridad de la información para las entidades públicas y privadas en Colombia. Las IES están obligadas a cumplir con estos requisitos para proteger la información de la institución.

- **Circular Externa 003 de 2015 de la Superintendencia de Industria y Comercio:** Esta circular establece los lineamientos para el reporte de incidentes de seguridad informática en Colombia. Las IES deben reportar cualquier incidente de seguridad que afecte la información personal de sus estudiantes, docentes y demás personal.

- **ISO 27001:** es una norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan.

  El estándar ISO 27001:2013 para los Sistemas Gestión de la Seguridad de la Información permite a las organizaciones la evaluación del riesgo y la aplicación de los controles necesarios para mitigarlos o eliminarlos.

- **ISO 27002:** (anteriormente denominada estándar 17799:2005), norma internacional que establece el código de mejores prácticas para apoyar la implantación del Sistema de Gestión de Seguridad de la Información (SGSI) en las organizaciones.

  A través del suministro de una guía completa de implementación, esa norma describe cómo se pueden establecer los controles. Dichos controles, a su vez, deben ser elegidos en base a una evaluación de riesgos de los activos más importantes de la empresa.

- **ISO 27005:** La norma ISO 27005 reemplaza a la norma ISO 13335-2 "Gestión de Seguridad de la Información y la tecnología de las comunicaciones". La norma fue publicada por primera vez en junio de 2008, aunque existe una versión mejorada del año 2011.

  El riesgo se define como una amenaza que explota la vulnerabilidad de un activo pudiendo causar daños. El riesgo se encuentra relacionado con el uso, propiedad, operación, distribución y la adopción de las tecnologías de la información de la empresa. Aunque no existe un método concreto de cómo gestionar riesgos, se recomienda utilizar un proceso estructurado, sistemático y riguroso de análisis de riesgos para la creación del plan de tratamiento de riesgo.

- **ISO 27017:** Es una norma perteneciente a la familia ISO/IEC 27000 que fue publicada en 2015. Incluye pautas y directrices sobre los controles de seguridad de la información relacionadas con servicios en la nube.

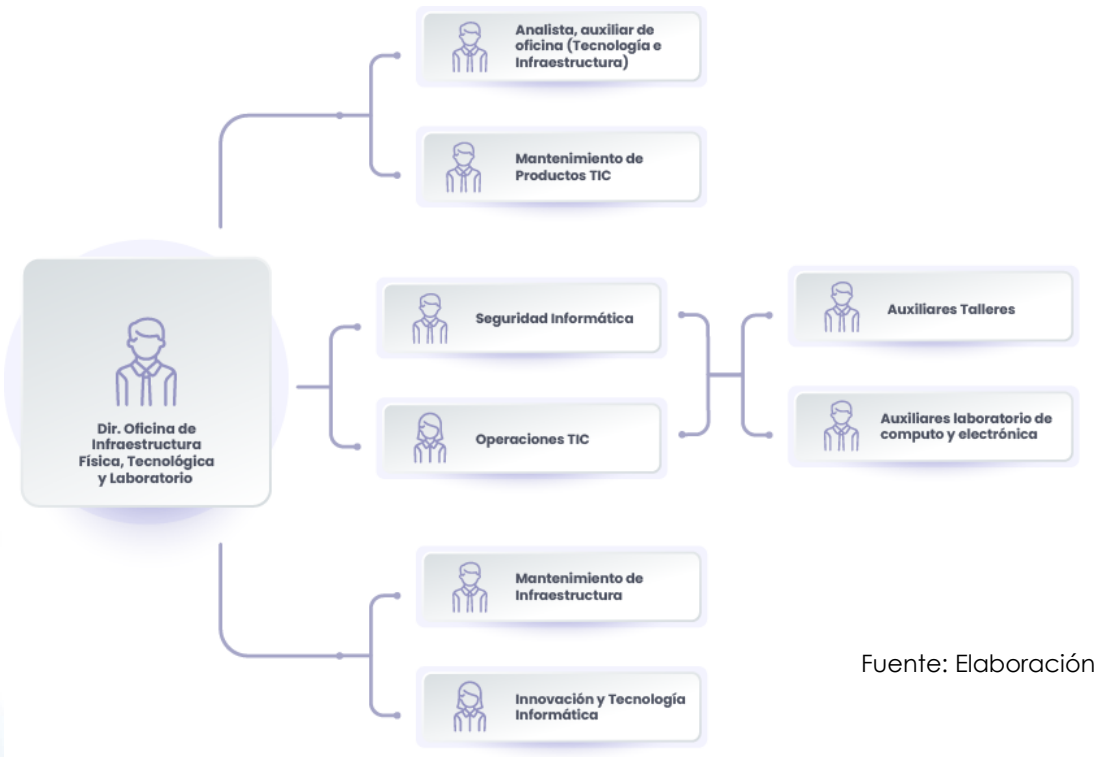
  Esta norma favorece que los datos usados por un cliente en una determinada plataforma (que haga uso de la nube) queden a salvo de posibles riesgos. Por parte del proveedor de dicho servicio, éste deberá proporcionar

información sobre la arquitectura y tecnología empleadas, así como de las medidas implementadas.

- **ITIL:** Desarrollada durante los años 1980, ITIL no fue ampliamente adoptada hasta mediados de los años 1990, La Biblioteca de Infraestructura de Tecnologías de Información (o ITIL, por sus siglas en inglés), es una metodología que involucra una serie de buenas prácticas en la gestión de TI. Abarca la infraestructura del área, el mantenimiento y la operación de los servicios de TI. Su aplicabilidad incluye tanto a los sectores operativos como a los estratégicos. El ITIL sirve para construir un entorno de TI estable y escalable, promoviendo una mejor prestación de servicios y atención al cliente.

COBIT: En 1992 comenzó la actualización de los objetivos de control de ISACA y, en 1996, ISACA proporcionó a los profesionales de TI un marco de prácticas control de la TI generalmente aplicables y aceptadas, llamadas COBIT (Control Objectives for Information and Related Technologies) en español significa Objetivos de Control para Tecnología de Información y Tecnologías Relacionadas. Es un marco de gobierno de TI que ayuda a las

Organigrama Departamento



Fuente: Elaboración Propia.

Alcance

Esta política busca garantizar la confidencialidad, integridad y disponibilidad de la información y los sistemas de información de la FUNDACION DE EDUCACION SUPERIOR SAN JOSE, mediante la implementación de medidas de seguridad técnicas y organizativas adecuadas, la promoción de la cultura de la seguridad de la información y la realización de auditorías y revisiones periódicas para evaluar la efectividad de las medidas implementadas.

Esta Política se aplica a toda la información y datos administrados en las bases de datos almacenadas en la institución.

Con el fin de ejercer este derecho, la persona debe presentar una solicitud de habeas data ante la FUNDACION DE EDUCACION SUPERIOR SAN JOSE correspondiente. En la solicitud, deberá indicar qué información desea conocer, actualizar o rectificar y acreditar su identidad como titular de los datos

Asimismo, se aplica al personal técnico que define, instala, administra y mantiene los permisos de acceso y las conexiones de red, y a los que administran su seguridad.

Glosario De Términos

Para el entendimiento de este documento se describen las siguientes definiciones:

Seguridad de la Información

La seguridad de la información se entiende como la preservación de las siguientes Características:

- **Confidencialidad**: Principio de seguridad de la información que se refiere a la protección de la información contra el acceso no autorizado. La confidencialidad implica que la información solo puede ser accesible por aquellos usuarios o entidades que tienen autorización para ello.

- **Integridad**: Principio de seguridad de la información que se refiere a la protección de la información contra la alteración no autorizada. La integridad implica que la información debe ser exacta y completa y que solo debe ser modificada por usuarios autorizados y mediante procesos controlados y seguros.

- **Disponibilidad**: Principio de seguridad de la información que se refiere a la capacidad de acceder a la información cuando se necesita. La disponibilidad implica que la información debe estar siempre disponible para los usuarios autorizados y que los sistemas y servicios que la manejan deben funcionar correctamente y sin interrupciones.

Adicionalmente, deberán considerarse los conceptos de:

- **Autenticidad**: Principio de seguridad de la información que se refiere a la verificación de la identidad de los usuarios y a la autenticidad de la información. La autenticidad implica que los usuarios deben ser autenticados y verificados antes de ser autorizados a acceder a la información, sistemas de gestión y bases de datos, adicional esta información debe ser auténtica y no haber sido alterada.

  La autenticidad se aplica a toda la información crítica o sensible que se maneja en una organización, incluyendo información financiera, datos de los clientes, información personal de los empleados, información de propiedad intelectual y cualquier otra información que pueda ser valiosa o importante para la organización.

- **Auditabilidad**: Principio de seguridad de la información que se refiere a la capacidad de registrar y monitorear las acciones realizadas por los usuarios y los sistemas en relación a la información y los recursos de la organización. La auditabilidad implica que se deben mantener registros detallados de las acciones realizadas para permitir la identificación y el seguimiento de cualquier actividad sospechosa o no autorizada.

- **No repudio**: Principio de seguridad de la información que se refiere a la capacidad de asegurar que una parte no pueda negar haber realizado una acción o transacción. En otras palabras, se asegura que las partes involucradas en una transacción no puedan negar su participación o responsabilidad en esa transacción.

- **Legalidad**: Principio de seguridad de la información que se refiere a la obligación de cumplir con las leyes, normas y regulaciones aplicables a la protección de la información. La legalidad implica que toda la información debe ser manejada de acuerdo con las leyes y regulaciones vigentes, y que los usuarios deben cumplir con las políticas y procedimientos de seguridad de la información establecidos.

- **Confiabilidad de la Información**: Principio de seguridad de la información que se refiere a la garantía de que la información es exacta, completa y actualizada. La confiabilidad es esencial para asegurar que la información sea útil y precisa para la toma de decisiones, la planificación y la ejecución de operaciones y actividades en una organización.

A los efectos de una correcta interpretación de la presente Política, se realizan las siguientes definiciones:

- **Información**: Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

- **Sistema de Información**: Se refiere a un 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 del Institución, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.

Evaluación de Riesgos

Se entiende por evaluación de riesgos a la evaluación y proceso fundamental para identificar y mitigar los riesgos asociados a la seguridad de la información, con el fin de garantizar su disponibilidad, integridad, confidencialidad y proteger los activos de información de la IES
.

Administración de Riesgos

Se entiende por administración de riesgos al proceso de identificación, control y minimización o eliminación, a un costo aceptable, de los riesgos de seguridad que podrían afectar a la información. Dicho proceso es cíclico y debe llevarse a cabo en forma periódica.

Comité de Tecnologías de la Información y Comunicación – CTIC -

El Comité de tecnologías de la información y Comunicación, es un grupo de trabajo que se encarga de asesorar y tomar decisiones relacionadas con la gestión de las tecnologías de la información y comunicación de una organización. La seguridad de la información es una de las áreas clave que debe ser considerada dentro de las responsabilidades del comité.

Incidente de Seguridad

Un incidente de seguridad es un evento adverso en un sistema de computadoras, o red de computadoras, que compromete la confidencialidad, integridad o disponibilidad, la legalidad y confiabilidad de la información. Puede ser causado mediante la explotación de alguna vulnerabilidad o un intento o amenaza de romper los mecanismos de seguridad existentes.

I. Política de Seguridad de la Información

Generalidades

La seguridad de la información se refiere a la protección de la información mediante accesos no autorizados, pérdidas, daños o alteraciones. La información es un recurso valioso para cualquier organización, por lo que es importante protegerla para garantizar su integridad, confidencialidad y disponibilidad.

Por ende, la implementación de medidas de seguridad efectivas es esencial para garantizar la integridad, confidencialidad y disponibilidad de la información, así como para protegerla contra accesos no autorizados, pérdidas, daños o alteraciones.

Objetivo

Establecer una serie normas y procedimientos necesarios para garantizar que la información sea manejada de forma segura en la FUNDACION DE EDUCACION SUPERIOR SAN JOSE. Esto incluye la autenticidad, confiabilidad e integridad de la información, la identificación de los datos críticos, la clasificación de la información, el control de acceso a los sistemas bases de datos y aplicaciones, la gestión de contraseñas, el monitoreo y la detección de posibles amenazas y la implementación de medidas de seguridad física y lógica para proteger los activos de información.

Responsabilidad

La política de seguridad de la información en FUNDACION DE EDUCACION SUPERIOR SAN JOSE, cuenta con diferentes roles y responsabilidades para garantizar que se cumpla con los objetivos de seguridad de la información establecidos. A continuación, se mencionan algunos de los responsables de la política de seguridad de la información:

- El **Comité de Tecnologías de la Información y Comunicación - CTIC -** de la institución, procederá a revisar y proponer a la máxima autoridad para su aprobación la política de seguridad de la información y las funciones generales en materia de seguridad de la información; monitorear cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes; tomar conocimiento y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad; aprobar las principales iniciativas para incrementar la seguridad de la información , de acuerdo a las competencias y responsabilidades asignadas a cada área, así como acordar y aprobar metodologías y procesos específicos relativos a seguridad de la información;

garantizar que la seguridad sea parte del proceso de planificación de la información; evaluar y coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios; promover la difusión y apoyo a la seguridad de la información dentro de la institución y coordinar el proceso de administración de la continuidad de las actividades.

- Los **Propietarios de la Información** son responsables de clasificarla de acuerdo con el grado de sensibilidad y criticidad de la misma, de documentar y mantener actualizada la clasificación efectuada, y de definir qué usuarios deberán tener permisos de acceso a la información de acuerdo a sus funciones y competencia.

- La **Oficina de Talento Humano** o quién desempeñe esas funciones, cumplirá la función de notificar a todo el personal que ingresa de sus obligaciones llamase (estudiantes, profesores, administrativos y otros) respecto del cumplimiento de la Política de Seguridad de la Información y de todas las normas, procedimientos y prácticas que de ella surjan. Asimismo, tendrá a su cargo la notificación de la presente Política a todo el personal, de los cambios que en ella se produzcan, la implementación de la suscripción de los Compromisos de Confidencialidad (entre otros) y las tareas de capacitación continúan en materia de seguridad.

- La **Oficina de Infraestructura Fisica, Tecnológica y Laboratorios** cumplirá la función de cubrir los requerimientos de seguridad informática establecidos para la operación, administración y comunicación de los sistemas y recursos de tecnología. Por otra parte, tendrá la función de efectuar las tareas de desarrollo y mantenimiento de sistemas, siguiendo una metodología de ciclo de vida de sistemas apropiada, y que contemple la inclusión de medidas de seguridad en los sistemas en todas las fases.

- El **Responsable del Área Legal** verificará el cumplimiento de la presente Política en la gestión de todos los contratos, acuerdos u otra documentación, con sus empleados y con terceros. Asimismo, asesorará en materia legal, en lo que se refiere a la seguridad de la información.

- La **Oficina de Control Interno**, o en su defecto quien sea propuesto por el Comité de Seguridad de la Información es responsable de practicar auditorías periódicas sobre los sistemas y actividades vinculadas con la tecnología de información, debiendo informar sobre el cumplimiento de las especificaciones y medidas de seguridad de la información establecidas por esta Política y por las normas, procedimientos y prácticas que de ella surjan.

Política

Aspectos Generales

Esta Política se conforma de una serie de pautas sobre aspectos específicos de la Seguridad de la Información, que incluyen lo siguiente:

- **Organización de la Seguridad:** Orientado a administrar la seguridad de la información dentro de la institución y establecer un marco gerencial para controlar su implementación.

- **Tratamiento de Datos Personales:** Orientado a garantizar derecho fundamental que busca proteger la privacidad y la autodeterminación informativa de la comunidad académica.

- **Clasificación y Control de Activos:** Destinado a mantener una adecuada protección de los activos.

- **Seguridad del Personal:** Orientado a reducir los riesgos de error humano, actividades ilícitas o uso inadecuado de infraestructura tecnológica.

- **Seguridad Física y Ambiental:** Destinado a impedir accesos no autorizados, daños e interferencia a las sedes e información de la institución.

- **Gestión de las Comunicaciones y las Operaciones:** Dirigido a garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información y medios de comunicación.

- **Control de Acceso:** Orientado a controlar el acceso lógico a la información.

- **Desarrollo y Mantenimiento de los Sistemas:** Orientado a garantizar la incorporación de medidas de seguridad en los sistemas de información desde su desarrollo y/o implementación y durante su mantenimiento.

- **Administración de la Continuidad de las Actividades:** Orientado a contrarrestar las interrupciones de las actividades y proteger los procesos críticos de los efectos de fallas significativas o desastres.

Cumplimiento

Destinado a impedir infracciones y violaciones de las leyes del derecho civil y penal; de las obligaciones establecidas por leyes, estatutos, normas, reglamentos o contratos; y de los requisitos de seguridad.

A fin de asegurar la implementación de las medidas de seguridad comprendidas en esta Política, la institución identificará los recursos necesarios e indicará formalmente las partidas presupuestales correspondientes, como anexo a la presente Política.

Lo expresado anteriormente no implicará necesariamente la asignación de partidas presupuestarias adicionales.

El Comité de Tecnologías de la Información y Comunicación revisará (indicar periodicidad no mayor a un año) la presente Política, a efectos de mantenerla actualizada. Asimismo, efectuará toda modificación que sea necesaria en función a posibles cambios que puedan afectar su definición, como ser, cambios tecnológicos, variación de los costos de los controles, impacto de los incidentes de seguridad, etc.

Sanciones Previstas por Incumplimiento

El incumplimiento de la Política de Seguridad de la Información tendrá como resultado la aplicación de diversas sanciones, conforme a la magnitud y característica del aspecto no cumplido.

II. Organización de la Seguridad

Generalidades

La presente Política de Seguridad establece la administración de la seguridad de la información, como parte fundamental de los objetivos y actividades de la Institución.

Por ello, se definirá formalmente un ámbito de gestión para efectuar tareas tales como la aprobación de la Política, la coordinación de su implementación y la asignación de funciones y responsabilidades.

Asimismo, se contemplará la necesidad de disponer de fuentes con conocimiento y experimentadas para el asesoramiento, cooperación y colaboración en materia de seguridad de la información.

Por otro lado, debe tenerse en cuenta que ciertas actividades la Institución pueden requerir que terceros accedan a información interna, o bien puede ser necesaria la tercerización de ciertas funciones relacionadas con el procesamiento de la información.

En estos casos se considerará que la información puede ponerse en riesgo si el acceso de dichos terceros se produce en el marco de una inadecuada administración de la seguridad, por lo que se establecerán las medidas adecuadas para la protección de la información.

Objetivo

Administrar la seguridad de la información dentro de la Institución y establecer un marco gerencial para iniciar y controlar su implementación, así como para la distribución de funciones y responsabilidades.

Fomentar la consulta y cooperación con entidades especializados para la obtención de asesoría en materia de seguridad de la información.

Garantizar la aplicación de medidas de seguridad adecuadas en los accesos de terceros a la información de la Institución.

Responsabilidad

El Comité de Tecnologías de la Información y Comunicación será el ente responsable de impulsar la implementación de la presente Política.

El Comité de Tecnologías de la Información y Comunicación tendrá a cargo el mantenimiento y la presentación para la aprobación de la presente Política, ante la máxima autoridad del organismo, el seguimiento de acuerdo a las incumbencias propias de cada área de las actividades relativas a la seguridad de la información (**análisis de riesgos, monitoreo de incidentes, supervisión de la investigación, implementación de controles, administración de la continuidad, impulsión de procesos de concientización, etc**.) y la proposición de asignación de funciones.
.

Los **Jefes o Directores de Área** cumplirán la función de autorizar la incorporación de nuevos recursos de procesamiento de información a las áreas de su incumbencia.

La **Oficina de Control Interno** o en su defecto quien sea propuesto por el Comité de Tecnologías de la Información y Comunicación, será responsable de realizar revisiones independientes sobre la vigencia y el cumplimiento de la presente Política.

El **La Oficina de Talento Humano** cumplirá la función de incluir en los contratos con proveedores de servicios de tecnología y cualquier otro proveedor de bienes o servicios cuya actividad afecte directa o indirectamente a los activos de información, la obligatoriedad del cumplimiento de la Política de Seguridad de la Información y de todas las normas, procedimientos y prácticas relacionadas.

El **Responsable del Área Legal** participará en dicha tarea. Asimismo, notificará a los proveedores sobre las modificaciones que se efectúen a la Política de Seguridad de la Información del Organismo.

Infraestructura de la Seguridad de la Información

Comité de Tecnologías de la Información y Comunicación

La seguridad de la información es una responsabilidad de la Institución, compartida con toda la comunidad académica, por lo cual se crea el Comité de Tecnologías de la Información y Comunicación, integrado por Rector, Vicerrector, Director de Planeación, Director de Talento Humano, Director de Infraestructura Física y Tecnologica, Asesor Jurídico; son esencial para garantizar que la organización esté alineada con las tendencias y tecnologías actuales, que se cumplan los objetivos estratégicos de la organización y que se gestione adecuadamente la seguridad de la información expuesta en esta política.

Conformación del Comité de Seguridad de la Información FUNDACION DE EDUCACION SUPERIOR SAN JOSE

Área / Dirección
Rector
Vicerrector
Director de Planeación
Director de Talento Humano
Director de Infraestructura Física y Tecnologica
Asesor Jurídico

Fuente: Elaboración Propia.

Este Comité tendrá entre sus funciones:

- Desarrollar políticas y estrategias que aborden el uso de la tecnología en la organización, incluyendo la adquisición, el mantenimiento y la actualización de los sistemas de TI.
- Revisar y aprobar los proyectos de TI, lo que puede incluir la implementación de nuevos sistemas, la actualización de los sistemas existentes, y la compra de nuevos equipos y software.
- Supervisar el presupuesto de TI, asegurándose de que los fondos se utilicen de manera efectiva y eficiente para apoyar las necesidades de la organización.
- Evaluar los riesgos de TI para la organización, lo que puede incluir la seguridad de la información y la gestión de desastres.
- Comunicarse regularmente con el personal de TI de la organización para

asegurarse de que se estén cumpliendo los objetivos y las metas de la organización en cuanto a tecnología y para mantener a los empleados informados sobre los proyectos y las políticas de TI.

- Desarrollar planes de formación y capacitación de TI para el personal de la organización, lo que puede incluir el desarrollo de habilidades técnicas y la educación sobre la política de TI de la organización.

- Promover la comunicación, divulgación y aplicación de las normativas planteadas.

- Coordinar el proceso de administración de la continuidad de la operatoria de los sistemas de tratamiento de la información de la institución frente a interrupciones imprevistas.

Asignación de Responsabilidades en Materia de Seguridad de la Información

Desde el consejo superior se asignan las funciones relativas a la Seguridad Informática de la institución a los administradores de tecnología (Director Oficina de Infraestructura Fisica, Tecnológica y / Web Master), estos administradores, serán los que se encarguen de la seguridad de los sistemas de información de la institución los cuales deberán supervisar todos los aspectos relacionados con la seguridad informática mencionados en la Política actual.

El Comité de Tecnologías de la Información y Comunicación presentará una propuesta a la autoridad competente para su aprobación, en la que se establecerán las responsabilidades que resulten del actual modelo.

A continuación, se detallan los procesos de seguridad, indicándose en cada caso el/los responsables(s) del cumplimiento de los aspectos de esta Política aplicables a cada caso:

Proceso	Responsable
Seguridad en las Comunicaciones y las Operaciones	Jefe Oficina de Infraestructura Fisica, Tecnológica y Laboratorios
Control de Accesos de Estudiante y Profesores presencial	Jefe Oficina de Infraestructura Fisica, Tecnológica y Laboratorios
Análisis de Seguridad en los Desarrollos y Mantenimiento de Sistemas Académicos	Jefe Oficina de Infraestructura Fisica, Tecnológica y Laboratorios / Proveedor
Página WEB Institucional y Derivados	Web Master tercerizado

Fuente: Elaboración Propia.

De igual forma, seguidamente se detallan los propietarios de los Sistemas de información, quienes serán los responsables de las Unidades Organizativas a cargo del manejo de la misma:

Información	Propietario	Recursos Asociados	Procesos Involucrados	Administrador
Mecosoft	Softland	Aplicación Cliente - Servidor , De Uso Interno Basado En Autenticación Adds, Departamentos De Contabilidad Y Recursos Humanos. Servidor Hp Proliant Ml 115 G5: • Windows 2003 • Base De Datos : Sql Server 2005 Enterprise Clientes: 12 Con Sistema Operativos Windows Xp , 7,	• Contables • Facturación • Recursos Humanos • Pagos • Cobros • Contratación	IT Fundación: Oficina de Infraestructura Fisica, Tecnología y Laboratorios Procesos: Copias De Seguridad Restauración Soporte Técnico
Pagos	Fessj	Sistema Desarrollo A partir De La Necesidad De Una Aplicación De Recaudo Y Facturación, De Uso Institucional En Los Departamentos De: • Tesorería • Admisiones • Biblioteca	• Recaudo Por <> Conceptos • Reportes De Recaudos • Asignación Examen De Admisión • Ayudas Educativas	IT Fundación: Oficina de Infraestructura Fisica, Tecnología y Laboratorios Procesos: Copias De Seguridad Restauración Soporte Técnico
Sifesj	Fessj	Aplicación Desarrollada Para La Academia, Usada Por Los Departamentos De: Registro Y Control Dirección Es De Carrera Departamentos (Investigaciones, Matemáticas, Biblioteca, Bienestar, Servicio Médico, Laboratorio Clínico, Entre Otros)	• Información Académica • Registro Académico • Horarios • Reportes • Docentes • Estudiantes	IT Fundación: Oficina de Infraestructura Fisica, Tecnología y Laboratorios Procesos: Copias De Seguridad Restauración Soporte Técnico
Honorarios	Fessj	Sistema Desarrollo A Partir De La Necesidad De Una Aplicación De Liquidación De Honorarios: • Dpto. De Recursos Humanos	• Contratos • Horas Laboradas Para Liquidación • Cuentas De Cobro • Prestamos	IT Fundación: Oficina de Infraestructura Fisica, Tecnología y Laboratorios Procesos: Copias De Seguridad Restauración Soporte Técnico
Q10	Q10 Soluciones	Sistema Académico y Financieros	• Admisiones • Información Financieros	IT Fundación: Oficina de Infraestructura Fisica,

				• Información Académica • Registro Académico • Horarios • Reportes • Docentes • Estudiantes	Tecnología y Laboratorios Procesos: Contacto Directo Q10: Mesa de Ayuda Procesos: Copias De Seguridad Restauración Soporte Técnico
Moodle		FESSJ	Plataforma Virtual	• Información Académica • Docentes • Estudiantes	IT Fundación: Dirección Virtual Proceso: Copias De Seguridad Restauración Soporte Técnico
Pagos Online		**Pagos online**	**Tesorería**	• **Recaudo Por Transacciones Electrónicas**	**IT Pagos Online** **Proceso: Transacciones Soporte**
Soportes Tickets	**X**	eTicket	It , Helpdesk	• Reporte De Incidentes • Seguimiento De Tickets • Soluciones Finales	IT Fundación: Oficina Virtual Proceso: Copias De Seguridad Restauración Soporte Técnico

Fuente: Elaboración Propia.

Cabe aclarar que, si bien los propietarios pueden delegar la administración de sus funciones a personal idóneo a su cargo, conservarán la responsabilidad del cumplimiento de las mismas. La delegación de la administración por parte de los propietarios de la información será documentada por los mismos y proporcionada al Responsable de Seguridad Informática.

III. Tratamiento de Datos Personales:

Generalidades

En Colombia, el habeas data es un derecho fundamental consagrado en la Constitución Política este se refiere al derecho que tienen todas las personas a conocer, actualizar y rectificar toda la información que se haya recogido sobre ellas en bases de datos o archivos, tanto públicos como privados, así como también velar por la privacidad, el buen uso, la intimidad y el buen nombre, garantizando principios de buena fe, legalidad, autodeterminación informática, libertad y transparencia.

Este derecho es especialmente importante en el ámbito de las Instituciones de Educación Superior (FUNDACION DE EDUCACION SUPERIOR SAN JOSE), por medio de sus diferentes canales de información suele recopilar y almacenar gran cantidad de información personal de sus estudiantes, docentes y demás personal.

Objetivo

Establecer que cualquier persona que haya suministrado información personal a FUNDACION DE EDUCACION SUPERIOR SAN JOSE, tenga derecho a:

- Solicitar el acceso a esa información y a pedir que se corrijan posibles errores o inexactitudes en ella.
- Velar por la privacidad, legalidad, libertad y transparencia de la misma.

Política

- **Acceso a la información:** Cualquier persona que haya suministrado información personal a FUNDACION DE EDUCACION SUPERIOR SAN JOSE, tiene derecho a solicitar el acceso a esa información. Esto significa que puede pedir que se le informe qué datos personales tiene la institución sobre él o ella, así como los fines para los que se han recopilado esos datos.

- **Actualización y rectificación de la información:** Si la persona comprueba que los datos personales que tiene FUNDACION DE EDUCACION SUPERIOR SAN JOSE, son incorrectos, inexactos o incompletos, puede solicitar que se actualicen o rectifiquen. Esto garantiza que la información sea precisa y esté actualizada.

- **Eliminación de la información:** Si la persona comprueba que FUNDACION DE

EDUCACION SUPERIOR SAN JOSE, está almacenando información personal que no debería tener, puede solicitar que se elimine. Esto garantiza que la información se use de forma justa y legal.

- **Protección de datos personales:** FUNDACION DE EDUCACION SUPERIOR SAN JOSE tiene la obligación de proteger los datos personales de sus estudiantes, docentes y demás personal, garantizando que se usen de forma justa y legal. En caso de que la IES incumpla esta obligación, la persona puede utilizar el habeas data para exigir el cumplimiento de sus derechos.

Responsabilidad

Los propietarios de la información son los encargados de clasificarla de acuerdo con su grado de sensibilidad y criticidad, de documentar y mantener actualizada la clasificación efectuada, y de definir las funciones que deberán tener permisos de acceso a la información.

El Responsable de Seguridad Informática es el encargado de asegurar que los lineamientos para la utilización de los recursos de la tecnología de información contemplen los requerimientos de seguridad establecidos según la criticidad de la información que procesan.

Cada Propietario de la Información supervisará que el proceso de clasificación y rótulo de información de su área de competencia sea cumplimentado de acuerdo a lo establecido en la presente Política.

IV. Clasificación y Control de Activos

La Institución debe tener conocimiento sobre los activos que posee como parte importante de la administración de riesgos. Algunos ejemplos de activos son:

Recursos de información: bases de datos y archivos, documentación de sistemas, manuales de usuario, material de capacitación, procedimientos operativos o de soporte, planes de continuidad, información archivada, etc.

Recursos de software: software de aplicaciones, sistemas operativos, herramientas de desarrollo, utilitarios, etc.

Activos físicos: equipamiento informático (Servidores, computadores de escritorio, portátiles, tablets), equipos de comunicaciones (routers, switchs, PBX, máquinas de fax, contestadores automáticos, teléfonos), medios magnéticos (cintas, discos, NAS, SAN), otros equipos técnicos (relacionados con el suministro eléctrico, unidades de aire acondicionado), mobiliario, entre otros

Servicios: servicios informáticos y de comunicaciones, sistema de comunicación y colaboración, plataforma virtual, página web, sistema eléctrico, sistema hidráulico, entre otros.

Es necesario categorizar los activos de información en función de su grado de sensibilidad y su importancia, o según el rol que desempeñan, y etiquetarlos en consecuencia para indicar el nivel de tratamiento y protección que deben recibir.

Es común que la información pierda su importancia o confidencialidad después de un tiempo determinado, especialmente cuando se ha vuelto pública. Esto es importante tenerlo en cuenta, ya que clasificar la información como excesivamente confidencial puede resultar en gastos innecesarios para la institución.

Las pautas de clasificación deben prever y contemplar el hecho de que la clasificación de un ítem de información determinado no necesariamente debe mantenerse invariable por siempre, y que ésta puede cambiar de acuerdo con una Política predeterminada. Se debe considerar la cantidad de categorías a definir para la clasificación dado que los esquemas demasiado complejos pueden tornarse engorrosos y antieconómicos o resultar poco prácticos.

La información adopta muchas formas, tanto en los sistemas informáticos como fuera de ellos. Puede ser almacenada (en dichos sistemas o en medios portátiles), transmitida (a través de redes o entre sistemas) e impresa o escrita en papel. Cada una de estas formas debe contemplar todas las medidas necesarias para asegurar la confidencialidad, integridad y disponibilidad de la información.

Por último, la información puede pasar a ser obsoleta y, por lo tanto, ser necesario eliminarla. La destrucción de la información es un proceso que debe asegurar la confidencialidad de la misma hasta el momento de su eliminación.

Objetivo

- Garantizar que los activos de información reciban un apropiado nivel de protección.
- Clasificar la información para señalar su sensibilidad y criticidad.
- Definir niveles de protección y medidas de tratamiento especial acordes a su clasificación.

Responsabilidad

Los propietarios de la información son los encargados de clasificarla de acuerdo con su grado de sensibilidad y criticidad, de documentar y mantener actualizada la clasificación efectuada, y de definir las funciones que deberán tener permisos de acceso a la información.

El Responsable de Seguridad Informática es el encargado de asegurar que los lineamientos para la utilización de los recursos de la tecnología de información

contemplen los requerimientos de seguridad establecidos según la criticidad de la información que procesan.

Cada Propietario de la Información supervisará que el proceso de clasificación y rótulo de información de su área de competencia sea cumplimentado de acuerdo a lo establecido en la presente Política.

Política

Inventario de activos

Activos	Ubicación	Propietario
SISTEMAS DE INFORMACIÓN		
Sistema de Aprendizaje en Línea		
Cursos	Servidor de Hosting dedicada	Dirección de Virtualidad
Aportes en Foros	Servidor de Hosting dedicada I	Dirección de Virtualidad
Notas de los Estudiantes	Servidor de Hosting dedicada	Dirección de Virtualidad
Envió de Tareas	Servidor de Hosting dedicada	Dirección de Virtualidad
Campus Virtual		
Contenido	Servidor de Hosting dedicada	Dirección de Virtualidad
Sistema de Helpdesk		
Ticket	Servidor de Hosting dedicada	Dirección de Virtualidad
Informes	Servidor de Hosting dedicada	Dirección de Virtualidad
SIFES		
Historia Académica x Estudiante		Departamento de Registro y Control
Horarios del Estudiante		Departamento de Registro y Control
Notas del Estudiante		Departamento de Registro y Control
Horario de los Docentes		Departamento de Registro y Control
Evaluación Docente		Departamento de Registro y Control
HONORARIOS		
Contratos		Departamento de Recursos Humanos y Contabilidad.
Cuentas de cobros		Departamento de Recursos Humanos y Contabilidad.
Prestamos		Departamento de Recursos Humanos y Contabilidad.
SNIES(Sistema Nacional de		

Información de la Educación Superior)		
Información Académica y Financiera del Estudiante.		Registro y Control.
Información Administrativa de la Institución		Rectoría y Dirección de Planeación
Q10 (Sistema de Información Académica y Financiera)		Admisiones
		Tesorería
		Crédito y Cartera
		Registro y Control
		Departamento de Recursos Humanos y Contabilidad
		Docentes
		Estudiantes
MECOSOFT		
Contabilidad		Departamento de Recursos Humanos y Contabilidad.
Facturación		Departamento de Recursos Humanos y Contabilidad.
Recursos humanos		Departamento de Recursos Humanos y Contabilidad.
Pagos		Departamento de Recursos Humanos y Contabilidad.
Cobros		Departamento de Recursos Humanos y Contabilidad.
BIBLIOTECA VIRTUAL		
Biblioteca Virtual		Departamento de Biblioteca
SERVIDOR DE CORREO		
Correos de Estudiantes Administrativos, Docentes y Terceros	Google y Microsoft	Oficina de Infraestructura Fisica, Tecnológica y Laboratorios
INFRAESTRUCTURA		
SALAS		
14 Salas de Computo con 283 Equipos	Distribuidos en toda las planta física de las 3 sedes cll 67 y Cll 63	Oficina de Infraestructura Fisica, Tecnológica y Laboratorios
ZONA DE SERVIDORES		
5 servidores	Sede principal Cll 67 Bloque D Piso 5	Oficina de Infraestructura Fisica, Tecnológica y Laboratorios
TELECOMUNICACIONES		
2 Plantas Panasonic	Admisiones y Centro de Telecomunicaciones	Colombiana de Telecomunicaciones

	sede Cll 67	
23 Swich 1 GB Capa 1	Distribuidos en toda las planta física de las 3 sedes cll 67 y Cll 63	Oficina de Infraestructura Fisica, Tecnológica y Laboratorios
12 Router Wifi	Distribuidos en las 3 sedes cll 67 y Cll 63	Oficina de Infraestructura Fisica, Tecnológica y Laboratorios
BIBLIOTECA		
Libros	Sede Principal Cll 67 Bloque D primer piso.	Departamento de Biblioteca
Artículos	Sede Principal Cll 67 Bloque D primer piso.	Departamento de Biblioteca
Tesis	Sede Principal Cll 67 Bloque D primer piso.	Departamento de Biblioteca
Revistas	Sede Principal Cll 67 Bloque D primer piso.	Departamento de Biblioteca
Videos	Sede Principal Cll 67 Bloque D primer piso.	Departamento de Biblioteca
EXTENSION y PROYECCIÓN SOCIAL		
Contratos de Convenios con el Gobiernes, Empresas Publicas y Privadas	Sede Cll 63 Piso 6 OFC 501	Departamento de Extensión y Proyección Social.
REGISTRO y CONTROL- ADMISIONES		
Documentación Personal, Académica y Financiera de Estudiante	Sede Principal Cll 67 Bloque A Primer Piso	Departamento de Registro y Control
BIENESTAR UNIVERSITARIO		
Historia Médica, Psicológica y Deportiva del Estudiante y Profesores	Sede Principal Cll 67 Bloque H Segundo Piso	Oficina de Bienestar Universitario. Servicio Medico
RECURSOS HUMANOS y CONTABILIDAD		
Contratos de Docente y Terceros	Sede Principal Cll 67 Bloque A segundo Piso	Departamento de Recursos Humanos
Hojas de Vida	Sede Principal Cll 67 Bloque A segundo Piso	Departamento de Recursos Humanos
Desprendibles de Pagos	Sede Principal Cll 67 Bloque A segundo Piso	Departamento de Recursos Humanos
Cuentas de Cobros y Pagos	Sede Principal Cll 67 Bloque A segundo Piso	Departamento de Recursos Humanos

Fuente: Elaboración Propia.

El mismo será actualizado ante cualquier modificación de la información registrada y revisado con una periodicidad de 2 meses.

El encargado de elaborar el inventario y mantenerlo actualizado es cada Responsable de Unidad Organizativa.

Clasificación de la información

Para clasificar un Activo de Información, se evaluarán las tres características de la información en las cuales se basa la seguridad: confidencialidad, integridad y disponibilidad.

A continuación, se establece el criterio de clasificación de la información en función a cada una de las mencionadas características:

Confidencialidad

Publico	Reservada – uso Interno	Reservada - confidencial	Reservada secreta
Comunidad Académica	Libros, Artículos, Tesis, Videos entre otros servicios de Biblioteca.	Historia Académica del Estudiante.	Contratos.
	Historia Médica, Psicológica y Cultural	Cursos Virtuales	Información Financiera de la Institución.
	Convenios	Aportes en Foros.	Cuentas de Cobro y Pagos
	Bibliotecas Virtuales		Correos

Integridad

Información cuya modificación no autorizada puede repararse fácilmente, o no afecta la operatoria del Organismo.	**Información cuya modificación no autorizada puede repararse aunque podría ocasionar pérdidas leves para el Organismo**	**Información cuya modificación no autorizada es de difícil reparación y podría Ocasionar pérdidas significativas para el Organismo**	**Información cuya modificación no autorizada no podría repararse, ocasionando pérdidas graves al Organismo**
Comunidad Académica	Libros, Artículos, Tesis, Videos entre otros servicios de Biblioteca.	Historia Académica y Financiera del Estudiante.	
	Historia Médica, Psicológica y Cultural.	Cursos Virtuales	
	Convenios.	Correos	
	Información Financiera de la Institución.	Cuentas de Cobros y Pagos.	
	Bibliotecas Virtuales	Sistema Contable y Financiero	
	Aportes de los Estudiantes en Foros del LMS.		

Disponibilidad

Información cuya inaccesibilidad no afecta la operatoria del Organismo.	Información cuya inaccesibilidad permanente durante 5 días podría ocasionar pérdidas significativas para el Organismo	Información cuya inaccesibilidad permanente durante 1 día podría ocasionar pérdidas significativas al Organismo	Información cuya inaccesibilidad permanente 5 horas podría ocasionar pérdidas significativas al Organismo.
Libros, Artículos, Tesis, Videos entre otros servicios de Biblioteca.	Contenido del Campus Virtual	Historia Académica y Financiera del Estudiante.	Cursos Virtuales
Historia Médica, Psicológica y Cultural.	Aportes de los Estudiantes en Foros del LMS.	Ingreso de Notas.	Correos
Convenios.			
Información Financiera de la Institución.			

V. Seguridad Física y Ambiental Generalidades

La seguridad física y ambiental brinda el marco para minimizar los riesgos de daños e interferencias a la información y a las operaciones de la institución. Asimismo, pretende evitar al máximo el riesgo de accesos físicos no autorizados, mediante el establecimiento de perímetros de seguridad.

Se distinguen tres conceptos a tener en cuenta: la protección física de accesos, la protección ambiental y el transporte, protección y mantenimiento de equipamiento y documentación.

El establecimiento de perímetros de seguridad y áreas protegidas facilita la implementación de controles tendientes a proteger las instalaciones de procesamiento de información crítica o sensible, de accesos físicos no autorizados.

El control de los factores ambientales permite garantizar el correcto funcionamiento de los equipos de procesamiento y minimizar las interrupciones de servicio. Deben contemplarse tanto los riesgos en las instalaciones como en instalaciones próximas a las sedes del mismo que puedan interferir con las actividades.

El equipamiento donde se almacena información es susceptible de mantenimiento periódico, lo cual implica en ocasiones su traslado y permanencia fuera de las áreas protegidas. Dichos procesos deben ser ejecutados bajo estrictas normas de seguridad y de preservación de la información almacenada en los mismos. Así también se tendrá en cuenta la aplicación de dichas normas en equipamiento perteneciente a la institución, pero situado físicamente fuera del mismo ("housing") así como en equipamiento ajeno que albergue sistemas y/o preste servicios de procesamiento de información al Organismo ("hosting").

La información almacenada en los sistemas de procesamiento y la documentación contenida en diferentes medios de almacenamiento, son susceptibles de ser recuperadas mientras no están siendo utilizados. Es por ello que el transporte y la disposición final presentan riesgos que deben ser evaluados.

Gran cantidad de información manejada en las oficinas se encuentra almacenada en papel, por lo que es necesario establecer pautas de seguridad para la conservación de dicha documentación.

Objetivo

Prevenir e impedir accesos no autorizados, daños e interferencia a las sedes, instalaciones e información.

Proteger el equipamiento de procesamiento de información crítica ubicándolo en áreas protegidas y resguardadas por un perímetro de seguridad definido, con medidas de seguridad y controles de acceso apropiados. Asimismo, contemplar la protección del mismo en su traslado y permanencia fuera de las áreas protegidas, por motivos de mantenimiento u otros.

Controlar los factores ambientales que podrían perjudicar el correcto funcionamiento del equipamiento informático que alberga la información.

Implementar medidas para proteger la información manejada por el personal en las oficinas, en el marco normal de sus labores habituales.

Proporcionar protección proporcional a los riesgos identificados.

Responsabilidad

El **Responsable de Seguridad Informática** definirá junto con el Propietarios de Información, según corresponda, las medidas de seguridad física y ambiental para el resguardo de los activos críticos, en función a un análisis de riesgos, y controlará su implementación. Asimismo, verificará el cumplimiento de las disposiciones sobre seguridad física y ambiental indicadas en el presente Capítulo.

La **Oficina de Infraestructura Fisica, Tecnológica y Laboratorios**, asistirá al Responsable de Seguridad Informática en la definición de las medidas de seguridad a implementar en áreas protegidas, y coordinará su implementación. Asimismo, controlará el mantenimiento del equipamiento tecnológico de acuerdo a las indicaciones de proveedores tanto dentro como fuera de las instalaciones.

Los **Jefes o Directores de Área** definirán los niveles de acceso físico del personal a las a las áreas restringidas bajo su responsabilidad.

Los Propietarios de la Información autorizarán formalmente el trabajo fuera de las instalaciones con información de su incumbencia a los empleados cuando lo crean conveniente.

La **Oficina de Control Interno** o en su defecto quien sea propuesto por el Comité de Tecnologías de la Información y Comunicación revisará los registros de acceso a las áreas protegidas.

Todo el personal es responsable del cumplimiento de la política de pantallas y escritorios limpios, para la protección de la información relativa al trabajo diario en las oficinas.

Política

Controles de Acceso Físico

Las áreas protegidas se resguardarán mediante el empleo de controles de acceso físico como puertas, tarjetas de acceso y claves de acceso, a fin de permitir el acceso sólo al personal autorizado. Estos controles de acceso físico tendrán, por lo menos, las siguientes características:

- Supervisar o inspeccionar a los visitantes a áreas protegidas y registrar la fecha y horario de su ingreso y egreso. Sólo se permitirá el acceso mediando propósitos específicos y autorizados e instruyéndose al visitante en el momento de ingreso sobre los requerimientos de seguridad del área y los procedimientos de emergencia.

- Controlar y limitar el acceso a la información clasificada y a las instalaciones de procesamiento de información, exclusivamente a las personas autorizadas. Se utilizarán los siguientes controles de autenticación para autorizar y validar todos los accesos: personal de guardia con listado de personas habilitadas o por tarjeta magnética o inteligente y número de identificación personal. Se mantendrá un registro protegido para permitir auditar todos los accesos.

- Implementar el uso de una identificación unívoca visible para todo el personal del área protegida e instruirlo acerca de cuestionar la presencia de desconocidos no escoltados por personal autorizado y a cualquier persona que no exhiba una identificación visible.

- Revisar y actualizar cada mes los derechos de acceso a las áreas protegidas, los que serán documentados y firmados por el Responsable de la Unidad Organizativa de la que dependa.

- Revisar los registros de acceso a las áreas protegidas. Esta tarea la realizará la Oficina de Control Interno o en su defecto quien sea propuesto por el Comité de Seguridad de la Información.

Protección de Oficinas, Recintos e Instalaciones

Para la selección y el diseño de un área protegida se tendrá en cuenta la posibilidad de daño producido por incendio, inundación, explosión, agitación civil, y otras formas de desastres naturales o provocados por el hombre. También se tomarán en cuenta las disposiciones y normas (estándares) en materia de sanidad y seguridad. Asimismo, se considerarán las amenazas a la seguridad que representan los edificios y zonas aledañas, por ejemplo, filtración de agua desde otras instalaciones.

Se definen los siguientes sitios como áreas protegidas.

Área Restringida	Ubicación
Zona de Servidores y Comunicaciones	Sede Principal
Ubicación de los Dispositivos para Acceso a Internet.	Sede Principal y Cll 63

Fuente: Elaboración Propia.

Se establecen las siguientes medidas de protección para áreas protegidas:

- Ubicar las instalaciones críticas en lugares a los cuales no pueda acceder personal no autorizado.
- Establecer que los edificios o sitios donde se realicen actividades de procesamiento de información serán discretos y ofrecerán un señalamiento mínimo de su propósito, sin signos obvios, exteriores o interiores.
- Ubicar las funciones y el equipamiento de soporte, por ejemplo: impresoras, fotocopiadoras, máquinas de fax, adecuadamente dentro del área protegida para evitar solicitudes de acceso, el cual podría comprometer la información.
- Establecer que las puertas y ventanas permanecerán cerradas cuando no haya vigilancia. Se agregará protección externa a las ventanas, en particular las que se encuentran en planta baja o presenten riesgos especiales.

Desarrollo de Tareas en Áreas Protegidas

Para incrementar la seguridad de las áreas protegidas, se establecen los siguientes controles y lineamientos adicionales. Esto incluye controles para el personal que trabaja en el área protegida, así como para las actividades de terceros que tengan lugar allí:

- Dar a conocer al personal la existencia del área protegida, o de las actividades que allí se llevan a cabo, sólo si es necesario para el desarrollo de sus funciones.
- Evitar la ejecución de trabajos por parte de terceros sin supervisión.
- Bloquear físicamente e inspeccionar periódicamente las

áreas protegidas desocupadas.

- Limitar el acceso al personal del servicio de soporte externo a las áreas protegidas o a las instalaciones de procesamiento de información sensible. Este acceso, como el de cualquier otra persona ajena que requiera acceder al área protegida, será otorgado
- solamente cuando sea necesario y se encuentre autorizado y monitoreado. Se Mantendrá un registro de todos los accesos de personas ajenas.
- Pueden requerirse barreras y perímetros adicionales para controlar el acceso físico entre áreas con diferentes requerimientos de seguridad, y que están ubicadas dentro del mismo perímetro de seguridad.
- Impedir el ingreso de equipos de computación móvil, fotográficos, de vídeo, audio o cualquier otro tipo de equipamiento que registre información, a menos que hayan sido formalmente autorizadas por el Responsable de dicho área o el Responsable del Área Informática y el Responsable de Seguridad Informática.
- Prohibir comer, beber y fumar dentro de las instalaciones de procesamiento de la información.

Ubicación y Protección del Equipamiento y Copias de Seguridad

El equipamiento será ubicado y protegido de tal manera que se reduzcan los riesgos ocasionados por amenazas y peligros ambientales, y las oportunidades de acceso no autorizado, teniendo en cuenta los siguientes puntos:

a) Ubicar el equipamiento en un sitio donde se minimice el acceso innecesario y provea un control de acceso adecuado.
b) Ubicar las instalaciones de procesamiento y almacenamiento de información que manejan datos clasificados, en un sitio que permita la supervisión durante su uso.
c) Aislar los elementos que requieren protección especial para reducir el nivel general de protección requerida.
d) Adoptar controles adecuados para minimizar el riesgo de amenazas potenciales, por:

Amenazas Potenciales	Controles
Robo o hurto, Derrumbes, Incendio o Inundaciones	1. Servidores y Componentes de Comunicación: A nivel de los Servidores se tendrá un cuarto exclusivo para la ubicación de los servidores donde solo podrá acceder las personas autorizadas por medio de llave o tarjeta de acceso, dicho sistema supervisará todos los accesos y tendrá las diferentes alarmas. Adicional cada uno de los servidores y UPS estarán en su respectivo RACK en candado donde se tendrá 2 copias que tendrá el Director de TIC y el director de Planeación. 2. Salas de Computo: Cada vez que un usuario llamase Estudiantes, Profesores y Administrativo solicite el

	uso de algún computador de la sala deberá de realizar 1° Mostrara su carnet que lo identifique donde el monitor hará su respectiva verificación en el sistema Q10, 2° el Monitor deberá de llenar el registro de prestamo con la información del usuario donde estarán los siguientes campos Nombre y Apellido, código, Hora de Ingreso, Computador asignado y el usuario deberá firmar aceptando la información registrada por el monitor. Adicional Cada Computador tendrá un candado con llaves que estarán ubicadas en la OFC de Infraestructura. 3. Cursos Virtuales: Durante la producción de cada uno de los cursos, los profesores tendrán unos computadores que actualmente son 10 para realizar dicha actividad donde cada uno tendrá su clave de acceso y su carpeta que solo podrán acceder ellos, dichos computadores tendrán deshabilitado el ingreso de USB y quemado de CD, adicional estos computadores en su Caja de CPU tendrán candados para poder acceder a ellos internamente. También el grupo de Operación de la Dirección de Infraestructura hará backup como se define en las políticas de Backup. 4. Claves de Acceso: Las claves de acceso el usuario tendrá que realizar la renovación de dichas claves de acceso cada 60 días. 5. Historia Académica del Estudiantes: Toda la información de la Institución estará digitalizada para una recuperación de la información en casa de que haya un robo de la información.
Interferencia en el suministro de energía eléctrica (cortes de suministro, variación de tensión)	1. Servidores: Todos los Servidores y Dispositivo estarán conectado a una UPS que tiene una duración entre 10 ha 15 min y se activara se existe algún apagón dentro de la institucional, adicional cada componente como servidores, swith, router, PBX, Computadoras de Escritorio tendrán su estabilizador de voltaje. 2. Componentes de Comunicación: 3. Salas de Computo: 4. Información de los Departamentos:

Fuente: Elaboración Propia.

e) Revisar regularmente las condiciones ambientales para verificar que las mismas no afecten de manera adversa el funcionamiento de las instalaciones de procesamiento de la información. Esta revisión se realizará cada: 3 meses.

f) Considerar asimismo el impacto de las amenazas citadas en el punto que tengan lugar en zonas próximas a las sedes.

Mantenimiento de Equipos

Se realizará el mantenimiento del equipamiento para asegurar su disponibilidad e integridad permanentes. Para ello se debe considerar:

- Someter el equipamiento tecnológico a tareas de mantenimiento preventivo, de acuerdo con los intervalos de servicio y especificaciones recomendados por el proveedor y con la autorización formal de la Oficina de Infraestructura Fisica, Tecnológica y Laboratorios.

- La Oficina de Infraestructura Fisica, Tecnológica y Laboratorios mantendrá un listado actualizado del equipamiento con el detalle de la frecuencia en que se realizará el mantenimiento preventivo

- Establecer que sólo el personal de mantenimiento autorizado puede brindar mantenimiento y llevar a cabo reparaciones en el equipamiento.

- Registrar todas las fallas supuestas o reales y todo el mantenimiento preventivo y correctivo realizado.

- Registrar el retiro de equipamiento de la sedes para su mantenimiento o dada de baja.

- Eliminar la información confidencial que contenga cualquier equipamiento que sea necesario retirar, realizándose previamente las respectivas copias de resguardo.

Para la implementación del Mantenimiento se deberá cumplir las siguientes políticas.

1. Salas de Computo
    a. Todos los viernes los PC de las diferentes salas se limpiarán toda la información.

2. Zona de Servidores y Comunicaciones:
    a. Todos los Sábados se limpiaran todos los Logs de Eventos registrado sobre el sistema operativos solo se dejaran los logs de cada aplicativos que tendrán una duración de 1 mes.
3. Centro de Producción.
    a. Todos los Lunes, Miércoles y Viernes se hará backup de cada uno de estos equipos con el sistema de Windows Backup Recovery Automáticamente y los días
    b. Se creara una carpeta con el nombre del tutor para su información de las

asignaturas solo tendrá acceso él ya que si le asigna permisos a su usuario sobre la máquina.

c. Toda información que este por fuera de dichas carpeta será eliminadas todos los sábados en su respectivos mantenimiento de las maquinas.
d. Todo archivo Mayor a 100MB será eliminado de las maquinas.

4. Computadores Administrativos
   a. Todos los Lunes, Miércoles y Viernes se hará backup de cada uno de estos equipos con el sistema de Windows Backup Recovery Automáticamente y los días
   b. Se creara una carpeta con el nombre del tutor para su información de las asignaturas solo tendrá acceso él ya que si le asigna permisos a su usuario sobre la máquina.
   c. Toda información que este por fuera de dichas carpeta será eliminadas todos los sábados en su respectivos mantenimiento de las maquinas.
   d. Todo archivo Mayor a 100MB será eliminado de las maquinas.

5. Hosting Dedicados.
   a. Todos los Sábados se limpiaran todos los Logs de Eventos registrado sobre el sistema operativos solo se dejaran los logs de cada aplicativos que tendrán una duración de 1 mes.

Políticas de Escritorios y Pantallas Limpias

Se adopta una política de escritorios limpios para proteger documentos en papel y dispositivos de almacenamiento removibles y una política de pantallas limpias en las instalaciones de procesamiento de información, a fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información, tanto durante el horario normal de trabajo como fuera del mismo.

Se aplicarán los siguientes lineamientos:

- Almacenar bajo llave, cuando corresponda, los documentos en papel y los medios informáticos, en gabinetes y/u otro tipo de mobiliario seguro cuando no están siendo utilizados, especialmente fuera del horario de trabajo.
- Guardar bajo llave la información sensible o crítica (preferentemente en una caja fuerte o gabinete a prueba de incendios) cuando no está en uso, especialmente cuando no hay personal en la oficina.
- Desconectar de la red / sistema / servicio las computadoras personales, terminales e impresoras asignadas a funciones críticas, cuando están desatendidas. Las mismas deben ser protegidas mediante cerraduras de seguridad, contraseñas u otros controles cuando no están en uso (como por ejemplo la utilización de protectores de pantalla con contraseña). Los responsables de cada área mantendrán un registro de las contraseñas o copia de las llaves de seguridad utilizadas en el sector a su cargo. Tales elementos se encontrarán protegidos en

sobre cerrado o caja de seguridad para impedir accesos no autorizados, debiendo dejarse constancia de todo acceso a las mismas, y de los motivos que llevaron a tal acción.
- Proteger los puntos de recepción y envío de correo postal y las máquinas de fax no atendidas.
- Bloquear las fotocopiadoras (o protegerlas de alguna manera del uso no autorizado fuera del horario normal de trabajo.
- Retirar inmediatamente la información sensible o confidencial, una vez impresa.

VI. Control de Accesos

Generalidades

El acceso por medio de un sistema de restricciones y excepciones a la información es la base de todo sistema de seguridad informática. Para impedir el acceso no autorizado a los sistemas de información se deben implementar procedimientos formales para controlar la asignación de derechos de acceso a los sistemas de información, bases de datos y servicios de información, y estos deben estar claramente documentados, comunicados y controlados en cuanto a su cumplimiento.

Los procedimientos comprenden todas las etapas del ciclo de vida de los accesos de los usuarios de todos los niveles, desde el registro inicial de nuevos usuarios hasta la privación final de derechos de los usuarios que ya no requieren el acceso.

La cooperación de los usuarios es esencial para la eficacia de la seguridad, por lo tanto es necesario concientizar a los mismos acerca de sus responsabilidades por el mantenimiento de controles de acceso eficaces, en particular aquellos relacionados con el uso de contraseñas y la seguridad del equipamiento.

Objetivo

- Impedir el acceso no autorizado a los sistemas de información, bases de datos y servicios de información.
- Implementar seguridad en los accesos de usuarios por medio de técnicas de autenticación y autorización.
- Controlar la seguridad en la conexión entre la red y otras redes públicas o privadas.
- Registrar y revisar eventos y actividades críticas llevadas a cabo por los usuarios en los sistemas.
- Concientizar a los usuarios respecto de su responsabilidad frente a la utilización de contraseñas y equipos.
- Garantizar la seguridad de la información cuando se utiliza computación móvil e instalaciones de trabajo remoto.

Responsabilidad

El Responsable de Seguridad Informática estará a cargo de:

Definir normas y procedimientos para: la gestión de accesos a todos los sistemas, bases de datos y servicios de información multiusuario; el monitoreo del uso de las instalaciones de procesamiento de la información; la solicitud y aprobación de accesos a Internet; el uso de computación móvil, trabajo remoto y reportes de incidentes relacionados; la respuesta a la activación de alarmas silenciosas; la revisión de registros de actividades; y el ajuste de relojes de acuerdo a un estándar preestablecido.

- Definir pautas de utilización de Internet para todos los usuarios.
- Participar en la definición de normas y procedimientos de seguridad a implementar en el ambiente informático (ej.: sistemas operativos, servicios de red, enrutadores o gateways, etc.) y validarlos periódicamente.
- Controlar la asignación de privilegios a usuarios.
- Analizar y sugerir medidas a ser implementadas para efectivizar el control de acceso a Internet de los usuarios.
- Verificar el cumplimiento de las pautas establecidas, relacionadas con control de accesos, registración de usuarios, administración de privilegios, administración de contraseñas, utilización de servicios de red, autenticación de usuarios y nodos, uso controlado de utilitarios del sistema, alarmas silenciosas, desconexión de terminales por tiempo muerto, limitación del horario de conexión, registro de eventos, protección de puertos, subdivisión de redes, control de conexiones a la red, control de ruteo de red, etc.
- Concientizar a los usuarios sobre el uso apropiado de contraseñas y de equipos de trabajo.
- Verificar el cumplimiento de los procedimientos de revisión de registros de auditoría.
- Asistir a los usuarios que corresponda en el análisis de riesgos a los que se expone la información y los componentes del ambiente informático que sirven de soporte a la misma.

Los Propietarios de la Información estarán encargados de:

- Evaluar los riesgos a los cuales se expone la información con el objeto de:
  - determinar los controles de accesos, autenticación y utilización a ser implementados en cada caso.
  - definir los eventos y actividades de usuarios a ser registrados en los sistemas de procesamiento de su incumbencia y la periodicidad de revisión de los mismos.
- Aprobar y solicitar la asignación de privilegios a usuarios.
- Llevar a cabo un proceso formal y periódico de revisión de los derechos de acceso a la información.
- Definir un cronograma de depuración de registros de auditoría en línea.

Los Propietarios de la Información junto con la Oficina de Control Interno o en su defecto

quien sea propuesto por el Comité de Seguridad de la Información, definirán un cronograma de depuración de registros en línea en función a normas vigentes y a sus propias necesidades.

Los **Jefes o Directores de Área**, junto con el Responsable de Seguridad Informática, autorizarán el trabajo remoto del personal a su cargo, en los casos en que se verifique que son adoptadas todas las medidas que correspondan en materia de seguridad de la información, de modo de cumplir con las normas vigentes. Asimismo, autorizarán el acceso de los usuarios a su cargo a los servicios y recursos de red y a Internet.

La **Oficina de Infraestructura Fisica, Tecnológica y Laboratorios** cumplirá las siguientes funciones:

- Implementar procedimientos para la activación y desactivación de derechos de acceso a las redes.
- Analizar e implementar los métodos de autenticación y control de acceso definidos en los sistemas, bases de datos y servicios.
- Evaluar el costo y el impacto de la implementación de "enrutadores" o "gateways" adecuados para subdividir la red y recomendar el esquema apropiado.
- Implementar el control de puertos, de conexión a la red y de ruteo de red.
- Implementar el registro de eventos o actividades de usuarios de acuerdo a lo definido por los propietarios de la información, así como la depuración de los mismos.
- Definir e implementar los registros de eventos y actividades correspondientes a sistemas operativos y otras plataformas de procesamiento.
- Evaluar los riesgos sobre la utilización de las instalaciones de procesamiento de información, con el objeto de definir medios de monitoreo y tecnologías de identificación y autenticación de usuarios (Ej.: biometría, verificación de firma, uso de autenticadores de hardware).
- Definir e implementar la configuración que debe efectuarse para cada servicio de red, de manera de garantizar la seguridad en su operatoria.
- Analizar las medidas a ser implementadas para efectivizar el control de acceso a
- Internet de los usuarios.
- Otorgar acceso a los servicios y recursos de red, únicamente de acuerdo al pedido formal correspondiente.
- Efectuar un control de los registros de auditoría generados por los sistemas operativos y de comunicaciones.

La **Oficina de Control Interno** o en su defecto quien sea propuesto por el Comité de Tecnologías de la Información y Comunicación, tendrá acceso a los registros de eventos a fin de colaborar en el control y efectuar recomendaciones sobre modificaciones a los aspectos de seguridad.

Comité de Tecnologías de la Información y Comunicación aprobará el análisis de riesgos de la información efectuado. Asimismo, aprobará el período definido para el mantenimiento de los registros de auditoría generados.

Política

Administración de Accesos de Usuarios

Las políticas de Control de Acceso a Nivel Institucional son las siguientes:

Registro de Usuarios

- Se concede el acceso a equipos administrativos de acuerdo a solicitud de credenciales por parte de jefe de área, incluyendo horario, días laborales, tipos de permisos entre otros.
- Los equipos de uso general como salas de docentes y computo, contaran con contraseña genéricas, sin embargo se debe registrar en planilla el uso del equipo.

Administración de Contraseñas de Usuario

- Requerir que los usuarios firmen una declaración por la cual se comprometen a mantener sus contraseñas personales en secreto y las contraseñas de los grupos de trabajo exclusivamente entre los miembros del grupo
- Garantizar que los usuarios cambien las contraseñas iniciales que les han sido asignadas la primera vez que ingresan al sistema. Las contraseñas provisorias, que se asignan cuando los usuarios olvidan su contraseña, sólo debe suministrarse una vez
- Identificado el usuario.
- Generar contraseñas provisorias seguras para otorgar a los usuarios. Se debe evitar la participación de terceros o el uso de mensajes de correo electrónico sin protección (texto claro) en el mecanismo de entrega de la contraseña y los usuarios deben dar acuse de recibo cuando la reciban.
- Las contraseñas Generadas no deberán ser inferior a 8 caracteres. Deberá contener letra minúscula, Mayúsculas, números y un carácter especial.
- Los Usuarios se bloquearan después de 3 Intentos erróneos sobre la misma IP o Usuario.
- Para Desbloquear un usuario deberán de hacer una solicitud por nuestro sistema e Ticket donde su solución será en 48 horas.
- Cada Contraseña tendrá una vigencia de 45 días.

Control de Acceso a la Red

Política de Utilización de los Servicios de Red

Las conexiones no seguras a los servicios de red pueden afectar a toda la comunidad, por lo tanto, se controlará el acceso a los servicios de red tanto internos como externos. Esto es necesario para garantizar que los usuarios que tengan acceso a las redes y a sus servicios, no comprometan la seguridad de los mismos.

La **Oficina de Infraestructura Fisica, Tecnológica y Laboratorios**, tendrá a cargo el otorgamiento del acceso a los servicios y recursos de red, únicamente de acuerdo al pedido formal del titular del área que lo solicite para personal de su incumbencia.

Este control es particularmente importante para las conexiones de red a aplicaciones que procesen información clasificada o aplicaciones críticas, o a usuarios que utilicen el acceso desde sitios de alto riesgo, por ejemplo áreas públicas o externas que están fuera de la administración y del control de seguridad.

Para ello, se desarrollarán procedimientos para la activación y desactivación de derechos de acceso a las redes, los cuales comprenderán:

- Identificar las redes y servicios de red a los cuales se permite el acceso.
- Realizar normas y procedimientos de autorización para determinar las personas y las redes y servicios de red a los cuales se les otorgará el acceso.
- Establecer controles y procedimientos de gestión para proteger el acceso a las conexiones y servicios de red.

Acceso a Internet

El acceso a Internet será utilizado con propósitos autorizados o con el destino por el cual fue provisto.

El Responsable de Seguridad Informática definirá procedimientos para solicitar y aprobar accesos a Internet.

A continuación, se definirán los diferentes procedimientos para acceso a Internet.

- La Institución tendrá acceso Wifi en las diferentes sedes para que el usuario pueda acceder a internet, el usuario deberá ingresar el mismo usuario y contraseña que tiene sobre todos los servicios de la Institución, este medio compartirá el mismo internet de las salas que es de 50 MB en cada uno de sus canales.

- Todas las salas de institución saldrán por medio de un firewall a internet donde para salir a internet deberán ingresar su usuario y contraseña que

utilizarán en todos los servicios de la institución.

- Los Usuarios Administrativo para acceder a cualquiera de los servicios deberán estar autenticado sobre el directorio Administrativo y tendrán un acceso de 50MB a internet que será controlado por el servicio firewall de la Zona de servidores.

Identificación y Autenticación de los Usuarios

Todos los usuarios (incluido el personal de soporte técnico, como los operadores, administradores de red, programadores de sistemas y administradores de bases de datos) tendrán un identificador único (ID de usuario) solamente para su uso personal exclusivo, de manera que las actividades puedan rastrearse con posterioridad hasta llegar al individuo responsable. Los identificadores de usuario no darán ningún indicio del nivel de privilegio otorgado.

En circunstancias excepcionales, cuando existe un claro beneficio para la institución, podrá utilizarse un identificador compartido para un grupo de usuarios o una tarea específica. Para casos de esta índole, se documentará la justificación y aprobación del Propietario de la Información de que se trate.

Si se utilizará un método de autenticación, deberá implementarse un procedimiento que incluya:

- Asignar la herramienta de autenticación.
- Registrar los poseedores de autenticadores.
- Rescatar el autenticador al momento de la desvinculación del personal al que se le otorgó.
- Revocar el acceso del autenticador, en caso de compromiso de seguridad.

Desconexión de Usuario y Terminales por Tiempo Muerto

El Responsable de Seguridad Informática, junto con los Propietarios de la Información de que se trate definirán cuáles se consideran terminales de alto riesgo, por ejemplo áreas públicas o externas fuera del alcance de la gestión de seguridad, o que sirven a sistemas de alto riesgo. Las mismas se apagarán después de un periodo definido de inactividad, tiempo muerto, para evitar el acceso de personas no autorizadas.

Esta herramienta de desconexión por tiempo muerto deberá limpiar la pantalla de la terminal y deberá cerrar tanto la sesión de la aplicación como la de red. El lapso por tiempo muerto responderá a los riesgos de seguridad del área y de la información que maneje la terminal.

Por otro lado, si un estudiante, profesor o personal administrativo debe abandonar su puesto de trabajo momentáneamente, activará protectores de pantalla con contraseñas, a los efectos de evitar que terceros puedan ver su trabajo o continuar con

la sesión de usuario habilitada.

Control de Acceso a las Aplicaciones

Aislamiento de los Sistemas Sensibles

Los sistemas sensibles podrían requerir de un ambiente informático dedicado (aislado). Algunos sistemas de aplicación son suficientemente sensibles a pérdidas potenciales y requieren un tratamiento especial. La sensibilidad puede señalar que el sistema de aplicación debe ejecutarse en una computadora dedicada, que sólo debe compartir recursos con los sistemas de aplicación confiables, o no tener limitaciones. Los siguientes sistemas van estar aislados ya que por seguridad es mejor que solo se acceda de una forma local

- MECOSOFT: Sistema que realiza un manejo de los procesos a nivel de Contables, Facturación, Recursos Humanos, Pagos, Cobros Y Contratación
- Académica: Sistema Académico (1998 a 2005)
- Tesorero: Sistema Financiero (1998 a 2005)
- SIFES: Sistema Académico (2005 a 2015)
- SIFES: Sistema Financiero (2005 a 2015)

Monitoreo del Acceso y Uso de los Sistemas

Registro de Eventos

Se generarán registros de auditoría que contengan excepciones y otros eventos relativos a la seguridad.

Los registros de auditoría deberán incluir:

- Identificación del usuario.
- Fecha y hora de inicio y terminación.
- Identidad o ubicación de la terminal, si se hubiera dispuesto identificación automática para la misma.
- Registros de intentos exitosos y fallidos de acceso al sistema.
- Registros de intentos exitosos y fallidos de acceso a datos y otros recursos.
- En todos los casos, los registros de auditoría serán archivados preferentemente en un equipo diferente al que los genere y conforme los requerimientos de la Política de Retención de Registros.

Los Propietarios de la Información junto con la Oficina de Control Interno o en su defecto quien sea propuesto por el Comité de Seguridad de la Información, definirán un cronograma de depuración de registros en línea en función a normas vigentes y a sus

propias necesidades.

VII. Desarrollo y Mantenimiento de Tecnologías

Generalidades

El desarrollo y mantenimiento de las aplicaciones es un punto crítico de la seguridad.

Durante el análisis y diseño de los procesos que soportan estas aplicaciones se deben identificar, documentar y aprobar los requerimientos de seguridad a incorporar durante las etapas de desarrollo e implementación. Adicionalmente, se deberán diseñar controles de validación de datos de entrada, procesamiento interno y salida de datos.

Dado que los analistas y programadores tienen el conocimiento total de la lógica de los procesos en los sistemas, se deben implementar controles que eviten maniobras dolosas por parte de estas personas u otras que puedan operar sobre los sistemas, bases de datos y plataformas de software de base (por ejemplo, operadores que puedan manipular los datos y/o atacantes que puedan comprometer / alterar la integridad de las bases de datos) y en el caso de que se lleven a cabo, identificar rápidamente al responsable.

Asimismo, es necesaria una adecuada administración de la infraestructura de base, Sistemas Operativos y Software de Base, en las distintas plataformas, para asegurar una correcta implementación de la seguridad, ya que en general los aplicativos se asientan sobre este tipo de software.

Objetivo

- Asegurar la inclusión de controles de seguridad y validación de datos en el desarrollo de los sistemas de información.
- Definir y documentar las normas y procedimientos que se aplicarán durante el ciclo de vida de los aplicativos y en la infraestructura de base en la cual se apoyan.
- Definir los métodos de protección de la información crítica o sensible.

Responsabilidad

El Responsable de Seguridad Informática junto con el Propietario de la Información y/o la Oficina de Control Interno, definirán los controles a ser implementados en los sistemas desarrollados internamente o por terceros, en función de una evaluación previa de riesgos.

El Responsable de Seguridad Informática, junto con el Propietario de la Información, definirá en función a la criticidad de la información, los requerimientos de protección mediante métodos criptográficos. Luego, el Responsable de Seguridad Informática definirá junto con el Responsable del Área de Sistemas, los métodos de encriptación a ser utilizados.

Asimismo, el Responsable de Seguridad Informática cumplirá las siguientes funciones:

- Definir los procedimientos de administración de claves.
- Verificar el cumplimiento de los controles establecidos para el desarrollo y mantenimiento de sistemas.
- Garantizar el cumplimiento de los requerimientos de seguridad para el software.

Política

Mantenimiento y Actualización Tecnológica

Para la actualización de la plataforma se deberán aplicar las siguientes políticas.

- Toda Actualización de los sistemas se hará los sábados después de las 4 pm hasta las 5 am del domingo.
- Siempre se hará un Backup de todo el sistema que se va actualizar si hay alguna posible falla en la actualización.
- Se deberá informar a todos los usuarios que utilicen el sistema con la información de cuando se hará la inactividad del Sistema.

Restricción del Cambio de Paquetes de Software

En caso de considerarlo necesario la modificación de paquetes de software suministrados por proveedores, y previa autorización del Responsable del Área Informática, se deberá:

- Analizar los términos y condiciones de la licencia a fin de determinar si las modificaciones se encuentran autorizadas.
- Determinar la conveniencia de que la modificación sea efectuada por el Organismo, por el proveedor o por un tercero.
- Evaluar el impacto que se produce.
- Retener el software original realizando los cambios sobre una copia perfectamente identificada, documentando exhaustivamente por si fuera necesario aplicarlo a nuevas versiones.

Evaluación y Mejora de la Política

- Esta política y cada uno de sus componentes son sujetos a mejora continua.
- Esta mejora parte de los procesos de cada política en miras a un Sistema educativo integral de Calidad.
- Este proceso auto evaluativo involucra el comité de TIC