ESCUELA
COLOMBIANA
DE INGENIERÍA
JULIO GARAVITO

Manual de Políticas

SEGURIDAD
& PRIVACIDAD
DE LA INFORMACIÓN

PRESENTACIÓN

Consejo Directivo
Presidente
Ingeniero Ricardo Rincón Hernández

Vocales
Ingeniera Sandra Ximena Campagnoli Martínez
Ingeniero Manuel García López
Ingeniera María del Rosario Montejo Perry
Ingeniero Armando Palomino Infante
Ingeniero Héctor Alfonso Rodríguez Díaz
Ingeniero Luis Guillermo Aycardi Barrero
Doctor Germán Ricardo Santos Granados
Ingeniero Ricardo Quintana Sighinolfi

Representante de los Profesores
Ingeniero Henry Moreno Mosquera

Representante de los Estudiantes
Jhon Édgar Herrera Díaz

Rectora
Ingeniera Myriam Astrid Angarita Gómez

Vicerrectora Académica
Ingeniera Claudia Ríos Reyes

Vicerrector Administrativo
Ingeniero Mauricio Vela Prieto

Secretario General
Ingeniero Ricardo López Cualla

MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
Publicación Institucional
Bogotá, D.C., abril de 2018

Elaborado por: Oficina de Sistemas y Recursos Informáticos OSIRIS

Diseño y diagramación: Dirección de Mercadeo y Comunicaciones Internas

CONTENIDO

1. Introducción

Manual de Políticas

SEGURIDAD & PRIVACIDAD DE LA INFORMACIÓN

Conforme a la Política General de Seguridad y Privacidad de la Información de la Escuela Colombiana de Ingeniería Julio Garavito, en adelante la Escuela, y en cumplimiento a los objetivos de seguridad de la información definidos en dicha política, en el presente documento se definen el conjunto de políticas de dominio específico.

El presente manual cubre los siguientes dominios de seguridad de la información:

1. Gestión sobre las políticas de seguridad de la Información
2. Organización de seguridad de la Información
3. Seguridad de los Recursos Humanos
4. Gestión de Activos
5. Control de Acceso
6. Seguridad Física y Ambiental
7. Cifrado
8. Seguridad de las operaciones
9. Seguridad de las comunicaciones
10. Adquisición, desarrollo y mantenimiento de sistemas
11. Relaciones con los proveedores
12. Gestión de incidentes de seguridad de la información
13. Cumplimiento

2. Gestión sobre las políticas de seguridad de la información

Manual de Políticas

SEGURIDAD & PRIVACIDAD DE LA INFORMACIÓN

- El manual de políticas de seguridad de la información vigente será el elaborado por la dirección de la Oficina de Sistemas y Recursos Informáticos (Osiris), en compañía del comité técnico y aprobado por el comité de políticas de seguridad de la información.
- La Oficina de Sistemas y Recursos Informáticos (Osiris) realizará las gestiones requeridas para que el manual de políticas de seguridad de la información o las políticas de dominio específico contenidas en él, sean comunicadas a todos los miembros de la comunidad universitaria.
- La Oficina de Sistemas y Recursos Informáticos (Osiris) deberá revisar y actualizar las políticas de seguridad de la información contenidas en el presente documento una vez al año o cuando los cambios en el entorno lo exijan.
- La Oficina de Sistemas y Recursos Informáticos Osiris) deberá diseñar, definir y realizar un programa de auditoría para el Sistema de Gestión de Seguridad de la Información de la Escuela, en el cual se contemplen los diferentes dominios de seguridad cubiertos en el presente manual.

3. Organización de Seguridad de la Información

Manual de Políticas

SEGURIDAD & PRIVACIDAD DE LA INFORMACIÓN

3.1 Organización Interna

- La Escuela debe definir y mantener un esquema de seguridad de la información en donde existan roles y responsabilidades que consideren actividades de administración, operación y gestión de la seguridad de la información.
- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe identificar las autoridades pertinentes hacia quienes pueda acudir en el caso de que un incidente de seguridad lo amerite. La Oficina de Sistemas y Recursos Informáticos (Osiris) debe mantener contacto con grupos de interés especial del ámbito de la seguridad de la información que aporten a la gestión de los riesgos de seguridad identificados en la Escuela.
- Los proyectos que desarrolle la Escuela deben contemplar una gestión de los riesgos de seguridad asociados a la información del proyecto, lo cual incluye una identificación de los riesgos y la definición de la forma como serán gestionados.
- En cualquier caso, los proyectos desarrollados por la Escuela deben estar alineados a las políticas de seguridad contenidas en el presente manual.
- Las actividades y proyectos encaminados a la gestión de la seguridad de la información deben estar enmarcados en la estrategia de la Escuela y alineados al cumplimiento de las funciones misionales de la institución.

3.1.1 Roles y Responsabilidades

ROL	RESPONSABLES	RESPONSABILIDADES
PROPIETARIO	Directivos institucionales	Serán los responsables de clasificar la información, establecer el nivel de criticidad y disponibilidad de la misma.
RESPONSABLE	Directores o Jefes de área, Decanos y Directores de Programas	Tendrán como responsabilidad asegurar la información de su área, controlando que se cumplan los requerimientos de seguridad de acuerdo con lo indicado por los propietarios de la información y las medidas implementadas por el Custodio.

ROL	RESPONSABLES	RESPONSABILIDADES
CUSTODIO	Osiris	Será responsable de implementar las medidas y controles necesarios para salvaguardar los activos de información de acuerdo con la clasificación establecida por los propietarios.
USUARIO	Personas que utilizan el activo de información de manera directa en el día a día dentro de sus funciones laborales o académicas.	Tendrán como responsabilidad hacer buen uso del acceso a la información suministrada para el cumplimiento de sus funciones diarias.

3.2 DISPOSITIVOS MÓVILES Y TELETRABAJO

- Los dispositivos móviles que hagan uso de información de la Escuela o que se conecten a su red se deben acoger a las políticas de seguridad de la información definidas en el presente manual.
- Al conectar un dispositivo a la red de la Escuela, el propietario del dispositivo acepta las políticas definidas en el presente manual y así mismo, las disposiciones que estas determinen.
- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe disponer de un mecanismo de conexión seguro que garantice que las conexiones de teletrabajo autorizadas por la Escuela se realizan de forma segura y se protegen los activos de información en uso.

4. Seguridad de los recursos humanos

Manual de Políticas

SEGURIDAD & PRIVACIDAD DE LA INFORMACIÓN

4.1 Antes de asumir el empleo

La Oficina de Recursos Humanos es la encargada de realizar las siguientes actividades relacionadas a la selección del personal administrativo para la Escuela y que son fundamentales para la seguridad de la información:

- Verificar los antecedentes de todos los candidatos a un empleo, de acuerdo con:
  - Las leyes, reglamentos y ética vigentes en la Escuela y el país
  - La clasificación de la información a la cual se va a tener acceso
  - Los riesgos percibidos.
- Confirmar la información de referencias personales, familiares y comerciales, para los casos en los que el candidato vaya a tener acceso a información considerada sensible.
- Realizar una verificación completa de la hoja de vida del solicitante.
- Solicitar una confirmación de las calificaciones académicas y profesionales entregadas en la hoja de vida, en caso de sospecha sobre su legitimidad.
- Realizar una verificación de identidad independiente (pasaporte o documento similar).
- Realizar todas las verificaciones necesarias para confirmar la veracidad de la información suministrada por el candidato a ocupar un cargo antes de su vinculación definitiva
- Certificar que los funcionarios de la institución que en razón de su cargo deban tener acceso a información de la Escuela, firmen en calidad de aceptación un Acuerdo de Seguridad, en el cual se les informe de la existencia de las políticas contenidas en el presente manual, documento que deberá ser adjuntado a los demás documentos relacionados con la ocupación del cargo.

Las Oficinas de compras, Jurídica, decanaturas, Vicerrectoría Académica y la Unidad de Gestión Externa (UGE), serán las encargadas de realizar las siguientes actividades fundamentales para la seguridad de la información, según corresponda en cada caso:

Certificar que el personal provisto por terceros (conferencistas, profesores, profesores temporales, etc.), que en razón de sus funciones deban tener acceso a información de la Es-

cuela firmen en calidad de aceptación un Acuerdo de Seguridad, antes de otorgar acceso a las instalaciones o a la plataforma tecnológica.

4.2 Durante la ejecución del empleo

La alta dirección (Rectoría, Vicerrectoría Académica, Vicerrectoría Administrativa, y Secretaría General), en razón de proteger la información y los recursos de procesamiento de la Escuela, y como demostración de apoyo a la implementación del Sistema de Gestión de Seguridad de la Información, promoverá la cultura de seguridad de la información entre los miembros de la comunidad universitaria, y por lo tanto define lo siguiente:

- El grupo directivo debe mostrar su compromiso con la seguridad de la información por medio de la aprobación y apoyo a la implantación del presente manual de políticas de seguridad de la información.
- La Escuela debe promover la importancia de la seguridad de la información entre los miembros de la comunidad universitaria, así como motivar el entendimiento, la toma de conciencia y el cumplimiento de las políticas, normas, procedimientos y estándares establecidos.
- El grupo directivo debe definir y establecer los procesos disciplinarios y el tratamiento que se le dará a los casos de incumplimiento al presente manual de políticas de seguridad de la información.
- Para el caso de estudiantes estará basado en el Régimen Estudiantil, para los profesores por medio del Estatuto de Profesores y Reglamento de Trabajo, para los Administrativos el Reglamento de Trabajo se deben aplicar los respectivos procesos disciplinarios cuando se identifiquen violaciones o incidentes de seguridad que así lo ameriten.
- La Oficina de Recursos Humanos en conjunto con la Oficina de Sistemas y Recursos Informáticos – Osiris, serán los encargados de convocar a los profesores y administrativos a las charlas y eventos programados como parte del programa de sensibilización en seguridad de la información que se realizará de manera anual y deben proveer los recursos para su ejecución y controlar la asistencia.

- La Vicerrectoría académica en conjunto con la Oficina de Sistemas y Recursos Informáticos – Osiris, serán los encargados de convocar a la comunidad universitaria (estudiantes), a las charlas y eventos programados como parte del programa de sensibilización en seguridad de la información que será anual y así mismo deben proveer los recursos para su ejecución y controlar la asistencia.
- Los miembros de la comunidad universitaria que por su cargo hagan uso de información de la Escuela o custodiada por ésta, deben dar cumplimiento a lo indicado en el presente manual de políticas de seguridad de la información y asistir a las charlas y eventos a los cuales sean convocados como parte del programa de sensibilización en seguridad de la información.
- Todos los miembros de la comunidad universitaria deben ser cuidadosos de no divulgar información confidencial de la Escuela ni por escrito ni en forma verbal. Igualmente, esto aplica para situaciones donde la revelación de información pueda causar un impacto operativo, reputacional o legal para la Escuela.

4.3 Terminación y cambio de empleo

La Escuela asegurará que sus funcionarios serán desvinculados o reasignados para la ejecución de nuevas labores de una forma ordenada, controlada y segura, por lo tanto, define lo siguiente:

- La Oficina de Recursos Humanos debe realizar el procedimiento de desvinculación, otorgamiento de licencias, incapacidades, vacaciones o cambio de labores de los empleados de la Escuela llevando a cabo los procedimientos que dicha oficina haya establecido.
- Cada Director y Jefe de Oficina deben reportar de manera inmediata a la Oficina de Recursos Humanos, la desvinculación o cambio de labores de los funcionarios o del personal provisto por terceras partes, con el fin que se tomen las medidas pertinentes y a su vez se informe a las oficinas interesadas.

5. Gestión de Activos

Manual de Políticas

SEGURIDAD & PRIVACIDAD DE LA INFORMACIÓN

5.1 Política de responsabilidad por los activos de información

La información, los sistemas, los servicios y los equipos (estaciones de trabajo, equipos portátiles, impresoras, redes, Internet, Servidores, aplicaciones, teléfonos, entre otros) de la Escuela, son activos de la institución y se proporcionan a los funcionarios y a terceros autorizados, para cumplir con los propósitos institucionales.

Todos los activos de información de la Escuela, deben ser asignados a un responsable, inventariados y posteriormente clasificados, de acuerdo con los requerimientos y los criterios que se parametrizaron en la GUÍA DE CLASIFICACIÓN DE LA INFORMACIÓN.

5.1.1 Responsabilidad por los activos de la información

- Cada Director y Jefe de oficina, debe actuar como responsable de la información física y electrónica de la dependencia a cargo, ejerciendo así la facultad de aprobar o revocar el acceso a su información con los perfiles adecuados para tal fin.
- Cada Director y Jefe de oficina como responsable de los activos de información debe generar un inventario de dichos activos para las áreas o procesos que lideran, acogiendo las indicaciones de la guía de clasificación de la información con el apoyo del coordinador(a) de seguridad informática.
- Cada Director y Jefe de oficina como responsable de los activos de información debe monitorear periódicamente la validez de los usuarios y sus perfiles de acceso a la información cada seis meses.
- La Oficina de Sistemas y Recursos Informáticos (Osiris) puede realizar monitoreo sobre los activos de información de la Escuela sin que esto identifique a usuarios particulares. Este procedimiento se podrá llevar a cabo siempre y cuando se tengan indicios de su vinculación a un incidente de seguridad, de igual manera esta labor debe realizarse bajo a autorización del involucrado.
- Los activos de información de la Escuela deben ser utilizados por toda la comunidad universitaria de acuerdo con las políticas contenidas en el presente manual y según la

normatividad vigente nacional. Esto con el fin de evitar un impacto operativo, legal o reputacional para la Escuela.

- Los profesores y administrativos deben utilizar los recursos tecnológicos de la Escuela, con el único objetivo de llevar a cabo las labores asignadas al cargo; por consiguiente, no deben ser utilizados para fines ajenos a este.
- Los Estudiantes deben utilizar los recursos tecnológicos de la Escuela, como son los laboratorios de cómputo, con el único fin de sacar provecho a las herramientas para la formación en el ámbito educativo; por consiguiente, no deben ser utilizados para fines ajenos a este.
- Si los profesores y administrativos necesitan utilizar equipos propios diferentes a los proporcionados por la institución, deben solicitar la autorización, verificación y registro de la Oficina de Sistemas y Recursos Informáticos (Osiris).
- Todos los miembros de la comunidad y terceros deben cumplir con los controles mínimos de seguridad establecidos (antivirus, sistema operativo con ciertos parches de seguridad), por la Oficina de Sistemas y Recursos Informáticos (Osiris), para poder conectarse a la red de la Escuela.
- Si los profesores, administrativos, estudiantes y terceros, necesitan instalar, hacer uso o compartir software (libre o propio) en los recursos proporcionados por la Escuela, deben solicitar la autorización, verificación y registro de la Oficina de Sistemas y Recursos Informáticos (Osiris).
- Los profesores y administrativos en el momento de desvinculación o cambio de labores, deben realizar la entrega de su puesto de trabajo al Director o Jefe de Oficina o a quien este delegue; así mismo, deben encontrarse a paz y salvo con la entrega de los recursos tecnológicos y otros activos de información suministrados en el momento de su vinculación.
- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe establecer un inventario con el software y sistemas de información que se encuentran permitidos en las estaciones de trabajo de la institución para el desarrollo de las actividades laborales, así como

verificar periódicamente que el software instalado en dichas estaciones de trabajo o equipos móviles corresponda únicamente al permitido.

5.2 Clasificación de la información

La Escuela definirá los niveles más adecuados para clasificar su información, de acuerdo con su sensibilidad y la Oficina de Sistemas y Recursos Informáticos (Osiris) generará una Guía de Clasificación de la Información para que los propietarios de la misma la cataloguen y determinen los controles requeridos para su protección.

Toda la información debe ser identificada, clasificada y documentada de acuerdo con la Guía de Clasificación de la Información establecida por el Comité de Seguridad de la Información.

La Guía de Clasificación de la Información define los controles técnicos y administrativos que se implantarán en la Escuela con el fin de preservar la confidencialidad, integridad y disponibilidad de los activos en función de su nivel de clasificación.

5.2.1 Normas para la clasificación y manejo de la información

- Los profesores y administrativos deben cumplir con los lineamientos establecidos en el manual de clasificación de la Información para el acceso, divulgación, almacenamiento, copia, transmisión, etiquetado y eliminación de la información contenida en los recursos tecnológicos, así como de la información física de la institución.
- El área de documentación debe tener un periodo de almacenamiento para la información física y digital, el cual puede ser dictaminado por requerimientos legales o misionales; este período debe ser indicado previamente por el propietario de la información y cuando se cumpla el periodo de expiración, toda la información debe ser eliminada adecuadamente.
- Los profesores y administrativos deben tener en cuenta estas consideraciones cuando impriman, escaneen, saquen copias y envíen faxes:

  - Verificar las áreas vecinas a impresoras, escáneres, fotocopiadoras y máquinas de fax para asegurarse que no quedaron documentos relacionados o adicionales.
  - Recoger de las impresoras, escáneres, fotocopiadoras y máquinas de fax, inmediatamente los documentos confidenciales para evitar su divulgación no autorizada.
- Los profesores y administrativos deben asegurar que los documentos y medios de almacenamiento que contengan información sensible, no queden de forma desprotegida en el momento de ausentarse de su puesto de trabajo.
- Los profesores y administrativos deben proteger la información física de la Escuela, utilizando los medios de almacenamiento y resguardo de los que dispongan.

Para cumplir con la clasificación a continuación se presentan los tipos de prioridad para la información:

  - Pública: estará la información que se puede compartir.
  - Uso interno: estará la información de interés para la institución, en general.
  - Información confidencial: estará la información de interés solo para un área en particular o por disposición de la ley (datos sensibles, privados, menores de edad, etc.).
- El Director o Jefe de área debe realizar la entrega de la información conveniente a quien lo suceda en el cargo.
- El Director o Jefe de área debe resguardar la información almacenada en medios magnéticos, de carácter histórico, está quedará documentada como activo del área.
- Ningún miembro de la comunidad o tercero deberá poseer material o información confidencial de la Institución, para usos no propios de su responsabilidad.

5.2.2 Etiquetado de la información

La información almacenada en medios magnéticos se deberá inventariar, anexando la descripción y las especificaciones de la misma, clasificándola y etiquetándola en los mismos niveles establecidos en clasificación de la información.

- Los directores o jefes de área responsables de la información contenida en las unidades a su cargo deben delimitar las responsabilidades de sus subordinados y determinar quién está autorizado a efectuar operaciones emergentes con dicha información tomando las medidas de seguridad pertinentes.

5.3 Manejo de los soportes de almacenamiento

La Escuela evitará la divulgación no autorizada, la modificación, eliminación o destrucción de la información almacenada en los medios de almacenamiento dispuestos para tal fin.

5.3.1 Gestión de soporte extraíbles

La Oficina de Sistemas y Recursos Informáticos (Osiris), como responsable de proporcionar los medios, mecanismos o herramientas tecnológicas realizará la gestión de medios extraíbles de acuerdo a las necesidades de cada usuario respecto a las labores desempeñadas.

- Los equipos de cómputo tienen autorizado el manejo de USB y unidades reproductoras de CD/DVD, por lo tanto, deben cumplir con los siguientes requisitos:
  - Tener habilitado el escaneo automático de virus.
  - Tener configurado en el software de antivirus el bloqueo de la reproducción automáticas de archivos ejecutables.

5.3.2 Eliminación de soportes

La Oficina de Sistemas y Recursos Informáticos (Osiris) debe velar porque la información será eliminada de los medios de almacenamiento de forma segura cuando ya no sea necesaria, utilizando procedimientos y herramientas de borrado seguro, garantizando que no queden rastros de esta.

5.3.3 Soportes físicos e información en tránsito

La Oficina de Sistemas y Recursos Informáticos (Osiris) debe garantizar que los medios que contienen información confidencial estén protegidos contra acceso no autorizado, mal uso o corrupción durante el transporte.

La Oficina de Sistemas y Recursos Informáticos (Osiris) debe garantizar que la información que transita a través de la red cuenta con los protocolos de seguridad necesarios, asegurado su confidencialidad, disponibilidad e integridad.

La Oficina de Sistemas y Recursos Informáticos (Osiris) debe implementar la utilización de protocolos de seguridad para el cifrado de las claves.

6. Control de acceso

Manual de Políticas

SEGURIDAD & PRIVACIDAD DE LA INFORMACIÓN

6.1 Política de control de acceso

La Escuela garantizará entornos con controles de acceso idóneos, los cuales aseguren el perímetro, tanto en oficinas, aulas de clase, salas de cómputo y laboratorios, así como en entornos abiertos para evitar el acceso no autorizado a ellos.

Así mismo, controlará las amenazas físicas externas y velará por proveer las condiciones medioambientales requeridas para el funcionamiento de la plataforma tecnológica y para la preservación de sus activos de información digitales y físicos.

La Oficina de Sistemas y Recursos Informáticos (Osiris) debe asegurar la implantación y efectividad de mecanismos de seguridad física, controles de acceso físico y condiciones medioambientales con los que se debe contar.

Los proveedores responsables de las áreas seguras tienen la obligación de vigilar y garantizar que se cumplan las siguientes medidas de seguridad:

- Las áreas que se catalogan como seguras deben permanecer cerradas y custodiadas
- El acceso a áreas seguras donde se procesa o almacena información confidencial, de uso interno y público, es limitado únicamente a personas autorizadas.

6.1.1 Acceso a redes y a servicios en red

La Oficina de Sistemas y Recursos Informáticos (Osiris) como responsable de las redes de datos y los recursos de red de la institución, debe velar porque dichas redes sean debidamente protegidas contra accesos no autorizados por medio de mecanismos de control de acceso lógico.

- La oficina de Sistemas y recursos Informáticos (Osiris) debe establecer un procedimiento de autorización y controles para proteger el acceso a las redes de datos y los recursos de red de la institución.

- La oficina de Sistemas y recursos Informáticos (Osiris) debe asegurar que las redes inalámbricas cuenten con mecanismos de autenticación que evite los accesos no autorizados.
- La oficina de Sistemas y recursos Informáticos (Osiris) debe establecer controles para la identificación y autenticación de los usuarios provistos por terceras partes a las redes o recursos de red del a Escuela, así como velar por la aceptación de las responsabilidades de dichos terceros en cuanto a las Políticas de Seguridad de la Información.
- La oficina de Sistemas y recursos Informáticos (Osiris)debe suministrar una herramienta para realizar conexiones remotas a la red de área local de la Escuela de manera segura para los profesores y administrativos que por su labor así lo requiera, la cual debe ser aprobada, registrada y auditada.
- La oficina de Sistemas y recursos Informáticos (Osiris)debe contar con un procedimiento de creación de cuentas, donde estén definidas las condiciones de autorización y acuerdos de confidencialidad respectivos.
- Los profesores y administrativos deben contar con el Acuerdo de Seguridad firmado, otorgado por recursos humanos y la autorización de creación de cuentas otorgado por el jefe inmediato, para tener acceso lógico a los sistemas de información de la institución, según sea el caso.
- Los profesores, administrativos y terceros que deseen que los equipos de cómputo personales accedan a la red de datos de la institución deben cumplir con todos los requisitos o controles para autenticarse en ésta y únicamente podrán realizar las tareas para las que fueron autorizados.

6.1.2 Control de accesos remotos

Los profesores, administrativos, estudiantes y terceros deben contar con una autorización y con los mecanismos permitidos por la Oficina de Sistemas y Recursos Informáticos (Osiris), para realizar una conexión remota a equipos conectados a la red interna desde fuera de la misma.

6.2 Gestión de acceso de usuarios

6.2.1 Política de administración de acceso de usuarios

La Escuela, establecerá privilegios para el control de acceso lógico de cada usuario o grupo de usuarios a las redes de datos, los recursos tecnológicos y los sistemas de información de la institución. Así mismo, velará porque los profesores, administrativos y el personal provisto por terceras partes tengan acceso únicamente a la información necesaria para el desarrollo de sus labores y la asignación de los derechos de acceso esté regulada por normas y procedimientos establecidos para tal fin.

- La oficina de Sistemas y Recursos Informáticos (Osiris) debe establecer un procedimiento formal para la administración de los usuarios en las redes de datos, los recursos tecnológicos y sistemas de información de la institución; que contemple la creación, modificación, bloqueo o eliminación de las cuentas de usuario.
- Los directores o jefes de área deben gestionar la creación, modificación, bloqueo o eliminación de los usuarios y permisos a los diferentes sistemas de información y recursos tecnológicos ante la Oficina de Sistemas y Recursos Informáticos(Osiris) quien será el encargado de ejecutar las labores a nivel tecnológico.
- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe definir los lineamientos para las características que deben contener las contraseñas que se aplicarán sobre la plataforma tecnológica, los servicios de red y los sistemas de información.
- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe establecer un procedimiento que asegure la eliminación, reasignación o bloqueo de los privilegios de acceso otorgados sobre los recursos tecnológicos, los servicios de red y los sistemas de información de manera oportuna.
- La oficina de Sistemas y recursos Informáticos (Osiris) debe asegurarse que los usuarios o perfiles de usuario, que tienen asignados por defecto los diferentes recursos de la plataforma tecnológica, sean inhabilitados o eliminados.

- La Oficina de Sistemas y Recursos Informáticos (Osiris) en conjunto con los propietarios de los activos de información deben autorizar la creación o modificación de las cuentas de acceso de los recursos tecnológicos y sistemas de información de la institución, según sea el caso.
- Los propietarios de los activos de información (directores de área, decanatura, dirección o dependencia) deben verificar y ratificar periódicamente (cada seis meses) todas las autorizaciones sobre sus recursos tecnológicos y sistemas de información.

6.2.2 Política de responsabilidades de acceso de los usuarios

Los usuarios, de los recursos tecnológicos y los sistemas de información, realizarán un uso adecuado y responsable de dichos recursos y sistemas, salvaguardando la información a la cual se les ha permitido el acceso.

Normas de responsabilidad de acceso

- Los estudiantes, profesores, administrativos y terceros que hacen uso de la plataforma tecnológica, los servicios de red y los sistemas de información de la Escuela, deben hacerse responsables de las acciones realizadas en los mismos, así como del usuario y contraseña asignados para el acceso a estos.
- Ninguna persona debe compartir sus cuentas de usuario y contraseñas asignados para el ingreso a los servicios de red y los sistemas de información con otros miembros de la comunidad institucional o terceros.
- Los estudiantes, administrativos, profesores y terceros que posean acceso a la plataforma tecnológica, los servicios de red y los sistemas de información que la institución ofrece, deben acogerse a las normas establecidas para la configuración de contraseñas designadas por la institución.

6.2.3 Registro y cancelación del registro de usuarios

- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe registrar todos los usuarios en la Base de Datos de Usuarios y Roles.

- La creación de un nuevo usuario o solicitud para la asignación de otros roles dentro de cualquier sistema de información, deberá acompañarse por el reporte debidamente firmado por el Jefe de área, de lo contrario no se le dará trámite a la requisición.

6.3 Control de acceso a sistemas y aplicaciones

6.3.1 Restricción de acceso a información

- Todos los miembros de la comunidad y terceros serán responsables por las credenciales (usuario y contraseña) que le sean asignadas y que reciben para el uso y acceso de los recursos.
- Ningún usuario (profesor, administrativo, estudiante, graduado o tercero) recibirá credenciales de acceso a la plataforma tecnológica, los servicios de red y los sistemas de información o aplicaciones, hasta que no acepte formalmente la Política de Seguridad de la Información e Informática vigente.
- Todos los estudiantes, profesores, administrativos, graduados, visitantes y terceros, deberán autenticarse en los mecanismos de control de acceso provistos por la Oficina de Sistemas y Recursos Informáticos (Osiris) antes de poder usar la infraestructura tecnológica de la Escuela.
- Los administrativos y profesores no deben proporcionar información de los mecanismos de control de acceso en las instalaciones e infraestructura tecnológica de la Escuela a personal externo, a menos que se tenga el visto bueno del dueño de la información, de Osiris y de su Jefe inmediato.
- Todo estudiante, administrativo y profesor, que acceda a la infraestructura tecnológica de la Escuela, debe contar con un identificador de usuario (ID) único y personalizado.

6.3.2 Procedimiento de inicio de sesión segura

- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe asegurarse que el acceso a los servicios de información solo sea posible con un proceso de conexión segura.

- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe implementar los controles necesarios para proteger los servicios de información de intentos de inicio de sesión mediante ataques de fuerza bruta.
- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe generar mensajes de advertencia general indicando que solo los usuarios autorizados pueden acceder al equipo de cómputo.
- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe validar la información de ingreso solamente al completar todos los datos de entrada.Si presenta una condición de error, el sistema no debe indicar qué parte de los datos es correcta o incorrecta.
- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe habilitar el registro de los intentos exitosos y fallidos de acuerdo a los perfiles de los usuarios en los sistemas de información necesarios.
- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe garantizar la transmisión segura de contraseñas sobre la red.
- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe asegurar la terminación de sesiones inactivas después de un período de inactividad de cinco minutos, teniendo especial cuidado con lugares de alto riesgo, tales como áreas públicas o externas por fuera de la organización o en dispositivos móviles.

6.3.3 Sistema de gestión de contraseñas

- Los profesores, administrativos y estudiantes deben recibir junto con el nombre de usuario una contraseña o clave para acceder a los recursos informáticos de la institución, la cual es de cambio obligatorio en el primer uso, garantizando así su responsabilidad y único conocimiento sobre la misma.
- Los profesores, administrativos y estudiantes deben establecer una contraseña que debe tener una longitud mínima de ocho caracteres alfanuméricos (mayúsculas, minúsculas, números, símbolos), diferentes a nombres propios o cualquier otra palabra de fácil identificación.

- Los profesores, administrativos y estudiantes deben cambiar las contraseñas o claves de acceso a la red, a los sistemas de información y demás con una periodicidad de seis meses.
- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe cambiar las contraseñas o claves de Administrador de los diferentes sistemas con una periodicidad de 90 días.
- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe establecer los controles necesarios para que después de tres intentos no exitosos al digitar la contraseña del usuario, esta se bloquee de manera inmediata y se deberá solicitar el desbloqueo en la plataforma destinada para este fin.
- Los profesores, administrativos y estudiantes deben realizar su cambio de contraseña exclusivamente en la plataforma destinada para tal fin. No se podrán modificar por ningún otro medio.
- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe asegurar que el número de sesiones concurrentes de un mismo usuario sea limitado.
- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe asegurar que el usuario sea usado en el equipo asignado al profesor o administrativo respectivo.
- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe establecer mecanismos para que las contraseñas o claves no sean iguales al nombre de usuario o cualquier variación (al revés, mayúsculas, etc.), alias o sobrenombre de la persona.
- Los profesores, administrativos y estudiantes deben asegurarse que la contraseña o clave no contiene palabras frecuentemente usadas y que se puedan asociar de manera rápida con su vida personal (nombre de hijos, fecha de nacimiento, número de cédula y número de celular, entre otros), no usa patrones como secuencias de números o caracteres y cadena repetidas.
- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe proporcionar los mecanismos necesarios para que los profesores, administrativos o estudiantes que olviden, bloqueen o extravíen su contraseña, puedan restablecerla de forma segura.

- Los profesores, administrativos y estudiantes deben asegurarse que las contraseñas no se encuentren de forma legible en cualquier medio impreso o dejarlos en un lugar donde personas no autorizadas puedan descubrirlos.
- Los estudiantes, administrativos y profesores deben cambiar inmediatamente la contraseña si tiene la sospecha de que esta es conocida por otra persona.
- Los profesores y administrativos no deben almacenar las contraseñas en ningún programa o sistema que proporcione esta facilidad a menos que sea aprobada por la Oficina de Sistemas y Recursos Informáticos (Osiris).

6.3.4 Control de acceso a códigos fuente de aplicaciones

- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe implementar los controles necesarios para asegurar que el acceso al código fuente de los aplicativos desarrollados sea limitado. Solamente el personal del grupo de desarrollo podrá contar con acceso a esta información y hará un uso moderado de la misma.
- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe proporcionar las herramientas necesarias para realizar control de cambios sobre el código fuente de los aplicativos desarrollados por la misma, las cuales permitirán retroceder a una versión anterior del código.
- La oficina de Sistemas y Recursos Informáticos (Osiris) debe ser responsable por la aprobación, supervisión y modificación de los códigos fuente de los aplicativos.

7. Cifrado

Manual de Políticas

SEGURIDAD & PRIVACIDAD DE LA INFORMACIÓN

7.1 Controles criptográficos

La Escuela, asegurará el uso adecuado y efectivo de la criptografía para proteger la confidencialidad, autenticidad o integridad de la información confidencial de la institución al momento de almacenarse o transmitirse.

7.1.1 Política de uso de los controles criptográficos

La Oficina de Sistemas y Recursos Informáticos (Osiris) debe proporcionar los mecanismos o herramientas necesarias para asegurar la protección de claves de acceso a la red de datos, los sistemas de información, datos y servicios de la institución.

La Oficina de Sistemas y Recursos Informáticos (Osiris) debe proporcionar los mecanismos de cifrado necesarios para asegurar que la transmisión de información confidencial de forma interna o externa se realice de forma segura.

La Oficina de Sistemas y Recursos Informáticos (Osiris) debe proporcionar los mecanismos o herramientas necesarias para cifrar la información confidencial de la institución, resguardada por los propietarios de la información (directores de área, decanatura, dirección o dependencia).

La Oficina de Sistemas y Recursos Informáticos (Osiris) debe contar con una política para garantizar la privacidad de la información que se respalda en medios de almacenamiento secundarios. Por lo tanto, se recomienda cifrar dicha información para mayor seguridad.

8. Seguridad Física y Ambiental

Manual de Políticas

SEGURIDAD & PRIVACIDAD DE LA INFORMACIÓN

8.1 Áreas seguras

La Escuela proveerá la implantación y velará por la efectividad de los mecanismos de seguridad física y control de acceso que aseguren el perímetro de sus instalaciones. Así mismo, controlará de amenazas físicas externas e internas y las condiciones medioambientales de sus oficinas.

Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se consideran áreas de acceso restringido.

8.1.1 Controles físicos de entrada

- Cualquier persona (estudiante, administrativo, docente, tercero), que tenga acceso a las instalaciones de la Escuela, deberá registrar los equipos de cómputo que no sean de propiedad de la institución, en la plataforma web establecida y de acuerdo a los procedimientos definidos por la Oficina de Sistemas y Recursos Informáticos (Osiris).
- Los profesores, administrativos, estudiantes o terceros, que requieran ingresar a los centros de cómputo y a los centros de cableado, deben realizar las solicitudes de acceso a la Oficina de Sistemas y Recursos Informáticos (Osiris). En el caso de los centros de cómputo de la Decanatura de Ingeniería de Sistemas al Laboratorio de Informática y si existiesen otros centros similares, a la dependencia responsable del mismo. Adicional, los responsables deben realizar un registro del ingreso de los visitantes en una bitácora ubicada en la entrada de estos lugares de forma visible.
- Los profesores, administrativos, estudiantes y terceros que deseen ingresar a los centros de cómputo y a los centros de cableado deben realizar el ingreso acompañados de un funcionario de la dependencia responsable de los mismos.
- Los profesores, administrativos, estudiantes y terceros deben cumplir completamente con los controles físicos implantados por la institución, ya que los ingresos y salidas a las instalaciones de la Escuela deben ser registrados.

- Todos los miembros de la comunidad y terceros deben portar el carné que los identifica como tales en un lugar visible, mientras se encuentren en las instalaciones de la institución; en caso de pérdida del carné, deben reportarlo a la mayor brevedad posible.
- Los profesores, administrativos, estudiantes y terceros no deben intentar ingresar a áreas a las cuales no tengan autorización.
- Las dependencias que tienen bajo su custodia centros de cómputo y centros de cableado deben modificar de manera inmediata los privilegios de acceso físico a estos sitios, en situaciones de desvinculación o cambio en las labores de una persona autorizada.
- Las dependencias que tienen bajo su custodia centros de cómputo y centros de cableado deben velar por las condiciones físicas y medioambientales necesarias para certificar la protección y correcta operación de los recursos de la plataforma tecnológica ubicados en estos sitios. Para cumplir con esto deben existir:
  - Sistemas de control ambiental de temperatura y humedad
  - Sistemas de extinción de incendios
  - Sistemas de vigilancia y monitoreo
  - Alarmas en caso de detectarse condiciones ambientales inapropiadas.
- Las dependencias que tienen bajo su custodia centros de cómputo y centros de cableado, en conjunto con la Dirección de Planta Física, deben velar porque los recursos de la plataforma tecnológica, ubicados en estos sitios, se encuentren protegidos contra fallas o interrupciones eléctricas.
- Las dependencias que tienen bajo su custodia centros de cómputo y centros de cableado, en conjunto con la Dirección de Planta Física, deben certificar que estos sitios se encuentren separados de áreas que tengan líquidos inflamables o que corran riesgo de inundaciones e incendios.
- Las dependencias que tienen bajo su custodia centros de cómputo y centros de cableado, en conjunto con la Dirección de Planta Física, deben asegurar que las labores de mantenimiento de redes eléctricas, de voz y de datos, sean realizadas por personal idóneo y previamente autorizado e identificado.

- Las dependencias que tienen bajo su custodia centros de cómputo y centros de cableado deben llevar control de la programación de los mantenimientos preventivos a estos sitios, teniendo en cuenta los niveles de servicio acordados con los responsables de los servicios particulares y acorde a la operación de la institución.
- Las dependencias que tienen bajo su custodia centros de cómputo y centros de cableado deben velar porque los niveles de temperatura y humedad relativa en estos sitios estén dentro de los límites requeridos por la infraestructura de cómputo allí instalada, para lo cual se deben usar sistemas de aire acondicionado según sea el caso.
- Las dependencias que tienen bajo su custodia centros de cómputo y/o centros de cableado deben solicitar mantenimientos preventivos y pruebas de funcionalidad del sistema de UPS y plantas eléctricas, de los sistemas de detección de incendios y del sistema de aire acondicionado.

8.1.2 Protección sobre amenazas externas o ambientales

- Las dependencias que tienen en custodia centros de cómputo y/o centros de cableado deben monitorear las variables de temperatura y humedad de las áreas de procesamiento de datos.
- La Escuela debe designar y aplicar protección física para desastres como: fuego, inundación, terremoto, explosión, malestar civil y otras formas de desastre natural o humano.
- Las dependencias que tienen bajo su custodia centros de cómputo y/o centros de cableado deben velar por el ambiente adecuado para los activos informáticos como ventilación, iluminación, regulación de corriente, etc.

8.1.3 Trabajo en áreas seguras

La Escuela debe mantener áreas seguras para la gestión, almacenamiento y procesamiento de información en la institución. Las áreas deben contar con:

- Protecciones físicas y ambientales, acordes con el valor y la necesidad de aseguramiento de los activos que se protegen.
- Definición de perímetros de seguridad
- Controles de acceso físicos
- Seguridad para protección de los equipos
- Seguridad en el suministro eléctrico y cableado
- Condiciones ambientales adecuadas de operación
- Sistemas de contención, detección y extinción de incendios.

8.2 Equipos

8.2.1 Ubicación y protección de los equipos

- Los estudiantes, administrativos, profesores y terceros no deben mover o reubicar los equipos de cómputo pertenecientes a la Escuela, instalar o desinstalar dispositivos, ni retirar marcas, logotipos ni hologramas de los mismos sin la autorización de la Oficina de Sistemas y Recursos Informáticos (Osiris).
- La Dirección de Compras y Suministros debe resguardar los activos de información que se le asignan a los profesores y administrativos mediante la firma del usuario como responsable de estos.
- Los profesores, administrativos y estudiantes deben conservar los equipos de cómputo en la ubicación autorizada por la oficina de Sistemas y Recursos Informáticos (Osiris).
- Los profesores y administrativos deben utilizar los equipos de cómputo asignados para uso exclusivo de las funciones del cargo que desempeñan en la Escuela.
- Los estudiantes deben utilizar los equipos de cómputo destinados como herramientas de apoyo (salas de cómputo y laboratorios) a las labores académicas o de investigación, sin vulnerar las políticas establecidas por la institución y por las leyes vigentes del país.

- Los profesores y administrativos deben solicitar la capacitación necesaria para el correcto manejo de las herramientas informáticas que requieren para realizar sus labores, a fin de evitar riesgos por mal uso y para aprovechar al máximo los recursos proporcionados por la institución.
- Los profesores, administrativos, estudiantes y terceros no deben consumir alimentos o ingerir líquidos mientras utilizan los equipos de cómputo.
- Los profesores y administrativos deben informar a la Oficina de Sistemas y Recursos Informáticos (Osiris) cuando se requiera realizar cambios múltiples de los equipos de cómputo derivado de reubicación de lugares físicos de trabajo o cambios locativos, con tres días de anticipación y un plan detallado.
- Los profesores, administrativos, estudiantes y terceros no deben abrir o destapar los equipos de cómputo de la Escuela. Solo el personal de la Oficina de Sistemas y Recursos Informáticos (Osiris) está autorizado para realizar esta labor.

8.2.2 Seguridad del cableado

- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe mantener los cables de red de los centros de datos claramente marcados para identificar fácilmente los elementos conectados y evitar desconexiones erróneas.
- La Oficina de Sistemas y Recursos Informáticos (Osiris) y la Dirección de Planta Física deben contar con los planos que describan las conexiones del cableado.
- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe mantener el acceso a los centros de cableado solo para el personal autorizado.

8.2.3 Mantenimiento de equipos

- La Oficina de Sistemas y Recursos Informáticos (Osiris) es la responsable de llevar a cabo los servicios de mantenimiento y reparaciones al equipo informático, por medio de personal idóneo para la labor.

- La Oficina de Sistemas y Recursos Informáticos (Osiris) es la única autorizada para realizar la labor descrita en el punto anterior.
- Los profesores, administrativos y estudiantes deben respaldar con copias de seguridad toda la información personal o confidencial que se encuentre en el equipo de cómputo asignado, previniendo así la pérdida involuntaria de la misma, derivada del proceso de reparación.
- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe realizar procedimientos de borrado seguro en los equipos que se dan de baja y los equipos que son asignados a usuarios diferentes por temas de rotación.

8.2.4 Equipos de usuario desatendidos

- Los profesores y administrativos deben bloquear la sesión de sus equipos de cómputo cuando no se encuentren en su lugar de trabajo. Esto con el fin que la sesión del usuario no quede activa con los privilegios a la mano. (Procedimiento de cierre por inactividad)
- Los estudiantes deben cerrar sesión en los equipos de cómputo luego de terminar de usarlos para evitar el uso inadecuado de terceros.

8.2.5 Política de escritorio limpio y pantalla limpia

- Los profesores y administrativos de la Escuela deben conservar el escritorio del equipo libre de información de uso interno o confidencial propia de la institución, que pueda ser alcanzada, copiada o utilizada por terceros o por personal que no tenga autorización para su uso o conocimiento.
- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe garantizar que los usuarios tengan la pantalla del equipo limpia o libre de archivos confidenciales por medio de mecanismos adecuados para este fin.
- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe aplicar un protector estándar en todas las estaciones de trabajo y equipos portátiles de la Escuela, de forma que se active luego de diez minutos sin uso.

- Los profesores y administrativos deben guardar en un lugar seguro cualquier documento, medio magnético u óptico removible que contenga información confidencial o de uso interno.
- Los profesores y administrativos no deben dejar en el escritorio físico documentos de uso confidencial sin custodia.
- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe establecer las medidas de control necesarias que permitan comprobar el correcto cumplimiento de los puntos anteriores.

9. Seguridad de las operaciones

Manual de Políticas

SEGURIDAD & PRIVACIDAD DE LA INFORMACIÓN

9.1 Procedimientos operacionales y responsabilidades

- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe realizar la documentación y actualización de los procedimientos relacionados con la operación y administración de los sistemas de información de la institución.
- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe proporcionar a sus funcionarios manuales de configuración y operación de los servicios de red, bases de datos y sistemas de información que conforman las diferentes plataformas.
- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe proveer los recursos necesarios para la implantación de controles que permitan la separación de ambientes de desarrollo, pruebas y producción, teniendo en cuenta consideraciones como:
  - Controles para el intercambio de información entre los ambientes de desarrollo y producción.
  - La inexistencia de compiladores, editores o fuentes en los ambientes de producción.
  - Acceso diferente para cada uno de los ambientes.

9.1.1 Gestión de Cambios

- La Escuela con el apoyo de la Oficina de Sistemas y Recursos Informáticos (Osiris) establecerá los mecanismos para las solicitudes de cambios. De igual manera, coordinará y controlará los cambios realizados en los activos de información tecnológicos y los recursos informáticos.
- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe garantizar que todo cambio realizado a un componente de la plataforma tecnológica, los cuales conlleve modificación de accesos, modificación o mantenimiento de software, actualización de versiones o modificación de parámetros, certifica y mantiene los niveles de seguridad existentes no afecta la correcta operación de la misma ni de otros servicios.
- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe garantizar que todo cambio realizado sobre la plataforma tecnológica de la Escuela, quedará formalmente documentado desde su solicitud hasta su implementación.

- Los responsables de los activos de información tecnológicos y recursos informáticos (directores de área, decanatura, dirección o dependencia) deben solicitar formalmente los requerimientos de nuevas funcionalidades, servicios o modificaciones sobre sus sistemas de información.
- La Oficina de Sistemas y Recursos Informáticos (Osiris), como Administradores de los activos de información tecnológicos y recursos informáticos, deben garantizar que las modificaciones o adiciones en las funcionalidades de los sistemas de información están soportadas por las solicitudes realizadas por los usuarios.

9.1.2 Gestión de capacidades

- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe supervisar continuamente el uso de los recursos con el fin de realizar los pertinentes ajustes, mirar las proyecciones para las futuras necesidades de capacidad y asegurar el rendimiento del sistema requerido.
- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe realizar estudios sobre las proyecciones de crecimiento de los recursos administrados de manera periódica, con el fin de asegurar el desempeño y capacidad de la plataforma tecnológica. Aspectos a considerar:
  - Consumo de recursos de procesadores, memorias, discos.
  - Servicios de impresión
  - Ancho de banda, internet y tráfico de las redes de datos.

9.1.3 Separación de entornos de desarrollo, prueba y producción

- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe separar los ambientes de desarrollo, pruebas y producción con el fin de reducir los riesgos de acceso no autorizado o cambios en el entorno operativo.
- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe garantizar los recursos necesarios que permitan la separación de los ambientes de desarrollo, pruebas y producción.

- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe garantizar la independencia de los usuarios que usan los ambientes de desarrollo, pruebas y producción.

9.2 Protección contra códigos maliciosos

9.2.1 Controles contra códigos maliciosos

Teniendo en cuenta que cada uno de los equipos de la institución cuenta con una licencia de antivirus y un agente instalado en cada una de ellas.

- Los profesores, administrativos, estudiantes y terceros deben contar con un antivirus actualizado en sus dispositivos personales tales como: portátiles o celulares, si desean ingresar a la red de datos de la institución.
- Los profesores, administrativos, estudiantes y terceros deben verificar que la información y los medios de almacenamiento, estén libres de cualquier tipo de código malicioso, para lo cual deben ejecutar el software antivirus instalado por la Oficina de Sistemas y Recursos Informáticos (Osiris)en los equipos de cómputo de la Institución.
- Los profesores y administrativos deben verificar, mediante el uso del software de antivirus, que todo archivo, independiente de su procedencia, esté libre de virus antes de ser accedido.
- Ningún profesor, administrativo, estudiante o tercero debe descargar software desde sistemas de correo electrónico, de mensajería instantánea y redes de comunicaciones externas, sin la debida autorización de la Oficina de Sistemas y Recursos Informáticos (Osiris).
- Los profesores, administrativos y terceros que sospechen de alguna infección por virus deben dejar de usar inmediatamente el equipo de cómputo y notificar a la Oficina de Sistemas y Recursos Informáticos (Osiris), para la revisión y eliminación del virus.
- Los profesores, administrativos, estudiantes y terceros no deben realizar modificaciones o eliminar las configuraciones de seguridad en Antivirus, Outlook, office, navegadores u otros programas, para detectar y prevenir la propagación de virus.

- Los profesores, administrativos, estudiantes y terceros no deben intentar eliminar los virus de los equipos, a menos que sean personal autorizado por la Oficina de Sistemas y Recursos Informáticos (Osiris), para garantizar la limpieza total de los equipos.

9.3 Copias de respaldo

9.3.1 Copias de respaldo de la información

- La Escuela, tiene el compromiso de la generación de copias de respaldo y almacenamiento de su información confidencial, proporcionando los recursos necesarios y estableciendo los procedimientos y mecanismos para la realización de estas actividades.
- Las áreas propietarias de la información, con el apoyo de Osiris, serán las encargadas de la generación de las copias de respaldo, se definirá la estrategia a seguir y los periodos de retención para el respaldo y almacenamiento de la información.
- Así mismo, se velará porque los medios magnéticos que contienen información de la Escuela sean almacenados en una ubicación diferente a las instalaciones donde se encuentra disponible. El sitio externo donde se resguarden las copias de respaldo debe contar con los controles de seguridad física y medioambiental apropiados.

9.3.1.1 Política para realizar copias de respaldo

Para una correcta realización y seguridad de backups se deberán tener en cuenta estos puntos:

- La Oficina de Sistemas y Recursos Informáticos (Osiris)(Osiris) debe contar con un procedimiento de respaldo de los sistemas operativos y de la información de los usuarios, para poder realizar una reinstalación en caso de sufrir un percance.
- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe determinar los medios y herramientas correctos para realizar los backups, teniendo en cuenta los espacios necesarios, tiempos de lectura escritura, tipo de backup a realizar, etc.
- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe realizar el almacenamiento de los backups en lugares diferentes de donde reside la información principal. De

este modo se evita la pérdida total si hay un desastre que afecte todas las instalaciones de la institución.

- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe verificar la integridad de los backups que se están almacenando, de acuerdo con el procedimiento de revisión periódica de estos, con el fin de asegurar que al momento de requerir restaurar alguno de ellos funcione como se espera.
- Los directores o jefes de área deben identificar la información que debe ser respaldada y almacenarla de acuerdo con su nivel de clasificación.
- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe contar con un procedimiento adecuado para garantizar la integridad física de los respaldos, en previsión de robo, destrucción o pérdida.
- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe contar con un procedimiento previamente definido para borrar físicamente la información de los medios de almacenamiento, antes de desecharlos.
- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe provisionar equipos de hardware con características similares a los utilizados para el proceso normal de la operación de la Escuela, en condiciones necesarias para entrar en funcionamiento en caso de desastres físicos.
- Los directores o jefes de área, para el caso de la información confidencial, deben realizar el respaldo diario de las modificaciones efectuadas y guardar respaldos históricos semanalmente de dicha información mediante los mecanismos o herramientas proporcionadas por la Oficina de Sistemas y Recursos Informáticos (Osiris).
- Los directores o jefes de área para el caso de la información de uso interno deben respaldar con una frecuencia mínima de una semana y guardar los respaldos históricos mensualmente de la información mediante los mecanismos o herramientas proporcionadas por la Oficina de Sistemas y Recursos Informáticos (Osiris).
- Los directores o jefes de área para el caso de la información pública deben realizar el respaldo de ésta a criterio propio.

- Los directores o jefes de área como propietarios de los recursos tecnológicos y sistemas de información deben definir en conjunto con la Oficina de Sistemas y Recursos Informáticos (Osiris), las estrategias para la generación, retención y rotación de las copias de respaldo de los activos de información.
- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe asegurar reproducir toda la información necesaria para la posterior recuperación sin pasos secundarios, esto para tener un plan de contingencia y poner en práctica, de alguna manera, la continuidad del negocio.

Roles y Responsabilidades

La Oficina de Sistemas y Recursos Informáticos (Osiris) debe determinar los roles de usuario, según su responsabilidad y tareas asignadas dentro de la Escuela, que intervienen dentro del proceso de backups:

- Administrador de backups: persona encargada de realizar los backups.
- Transportador: encargado de llevar los backups fuera de las instalaciones de la institución.
- Probador: Encargado de probar backups cada cierto período de tiempo.

9.4 Registro y seguimiento DE EVENTOS DE LOS SISTEMAS DE INFORMACIÓN

La Escuela, realizará monitoreo permanente del uso que dan los funcionarios a los recursos de la plataforma tecnológica y los sistemas de información de la institución. Además, velará por la custodia de los registros de auditoria cumpliendo con los periodos de retención establecidos para dichos registros.

La Oficina de Sistemas y Recursos Informáticos (Osiris), en conjunto con los responsables de los servicios, definirán la realización de monitoreo de los registros de auditoría sobre los aplicativos donde se opera los procesos de la institución.

- La oficina de Sistemas y Recursos Informáticos (Osiris) debe determinar los eventos que generarán registros de auditoría en los recursos tecnológicos y los sistemas de información.
- La oficina de Sistemas y Recursos Informáticos (Osiris) debe habilitar los registros de auditoría y sistemas de monitoreo de la plataforma tecnológica administrada, acorde con los eventos a auditar establecidos.
- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe certificar la integridad y disponibilidad de los registros de auditoría generados en la plataforma tecnológica y los sistemas de información. Estos registros deben ser almacenados y sólo deben ser accedidos por personal autorizado.

9.5 Control de software operacional

9.5.1 Instalación de software en sistemas operativos

La Escuela, por medio de la Oficina de Sistemas y Recursos Informáticos (Osiris), designará responsables y establecerá procedimientos para controlar la instalación de software en los equipos informáticos, se cerciorará de contar con el soporte de los proveedores de dicho software y asegurará la funcionalidad de los sistemas de información que operan sobre la plataforma tecnológica cuando el software sea actualizado.

- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe establecer responsabilidades y procedimientos para controlar la instalación del software en los equipos de cómputo.
- La Oficina de Sistemas y Recursos Informáticos (Osiris)debe asegurarse que tanto las aplicaciones desarrolladas in-house como las de terceros, realicen las respectivas pruebas antes de salir a producción.
- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe asegurarse que el software instalado en la plataforma tecnológica cuenta con soporte preciso en caso de ser necesario y con los proveedores según sea requerido.

- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe conceder accesos temporales y controlados a los proveedores para realizar las actualizaciones sobre el software, así como monitorear dichas actualizaciones.
- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe validar los riesgos que genera la migración hacia nuevas versiones del software.
- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe asegurar el correcto funcionamiento de sistemas de información y herramientas de software que se ejecutan sobre la plataforma tecnológica cuando el software es actualizado.
- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe establecer las restricciones y limitaciones para la instalación de software en los equipos de cómputo.

9.6 Gestión de vulnerabilidades

La Escuela, por intermedio de la Oficina de Sistemas y Recursos Informáticos (Osiris), revisará periódicamente la aparición de vulnerabilidades técnicas sobre los recursos de la plataforma tecnológica por medio de la realización periódica de pruebas de vulnerabilidades (cada seis meses), con el objetivo de realizar la corrección sobre los hallazgos arrojados por dichas pruebas.

- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe revisar cada tres meses o según se requiera, la aparición de nuevas vulnerabilidades técnicas y reportarlas a los administradores de la plataforma tecnológica y los desarrolladores de los sistemas de información, con el fin de prevenir la exposición al riesgo de estos.
- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe generar, ejecutar y monitorear planes de acción para la mitigación de las vulnerabilidades técnicas detectadas en la plataforma tecnológica cada tres meses.

9.6.1 Restricciones sobre la instalación de software

La Oficina de Sistemas y Recursos Informáticos (Osiris) debe realizar la instalación de software en los computadores suministrados por la Escuela, como función exclusiva de esta o a quienes ellos deleguen.

La Oficina de Sistemas y Recursos Informáticos (Osiris) debe autorizar el software adicional que se requiera instalar en equipos de cómputo específicos de la Escuela.

Osiris tendrá que mantener una lista actualizada del software autorizado para instalar en los computadores.

9.7 Consideraciones sobre auditorías de sistemas de información

9.7.1 Controles sobre auditorías de sistemas de información

- La Escuela, apoyada en la Oficina de Sistemas y Recursos Informáticos (Osiris), apoyada en el Procedimiento de Auditoria Interna, verificará el cumplimiento de los requisitos las normas ISO aplicables, la normatividad legal vigente y los requisitos propios de la organización cada año o según sea necesario.
- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe verificar que las auditorías concluyan la eficacia y eficiencia de los sistemas de información implementados en la institución.
- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe planificar para reducir al mínimo las interrupciones de los procesos, de acuerdo a los requisitos de auditoría y las actividades relacionadas con la verificación de los sistemas operativos.

10. Seguridad de las comunicaciones

Manual de Políticas

SEGURIDAD & PRIVACIDAD DE LA INFORMACIÓN

10.1 Políticas de Gestión de la seguridad de redes

La Escuela establecerá, con la Oficina de Sistemas y Recursos Informáticos (OSIRIS), los mecanismos de control necesarios para proveer la disponibilidad de las redes de datos y de los servicios tecnológicos que soportan la operación de la misma; así mismo, velará para que se tengan los mecanismos de seguridad que protejan la integridad y la confidencialidad de la información que se envía a través de dichas redes de datos.

De igual manera, proporcionará el aseguramiento de las redes de datos, el control del tráfico en dichas redes y la protección de la información interna y confidencial de la institución.

- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe adoptar medidas para asegurar la disponibilidad de los recursos y servicios de red.
- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe implantar controles para minimizar los riesgos de seguridad de la información transportada por medio de las redes de datos.
- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe mantener las redes de datos segmentadas por dominios, grupos de servicios, grupos de usuarios y ubicación.
- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe identificar los mecanismos de seguridad y los niveles de servicio de red requeridos e incluirlos en los acuerdos de nivel de servicios de red.
- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe establecer los estándares técnicos de configuración de los dispositivos de seguridad y de red de la institución, acogiendo buenas prácticas de configuración segura.
- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe identificar, justificar y documentar los servicios, protocolos y puertos permitidos en la red de datos de la Escuela e inhabilitar o eliminar el resto de los servicios, protocolos y puertos.
- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe instalar protección entre las redes internas y cualquier red externa, que esté fuera de la capacidad de control y administración de la institución.

- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe velar por la confidencialidad de la información del direccionamiento y el enrutamiento de las redes de datos.

10.2 Política de uso del mensajería electrónica

La Escuela Colombiana de Ingeniería Julio Garavito, entendiendo la importancia del correo electrónico como herramienta para facilitar la comunicación entre funcionarios y terceras partes, proporcionará un servicio idóneo y seguro para la ejecución de las actividades que requieran el uso del correoelectrónico, respetando siempre los principios de confidencialidad, integridad, disponibilidad y autenticidad de quienes realizan las comunicaciones por medio de este medio.

- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe generar y divulgar un procedimiento para la administración de cuentas de correo electrónico.
- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe diseñar y divulgar las normas para el uso de los servicios de correo electrónico.
- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe garantizar que la plataforma de correo tenga los procedimientos y controles necesarios que permitan detectar y proteger la integridad de la información que viaja a través de esta plataforma.
- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe asegurar que los mensajes electrónicos están protegidos contra código malicioso y pudiera ser transmitido a través de estos.
- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe generar campañas de concientización a todos sus usuarios (profesores, administrativos, estudiantes, etc.), respecto a las precauciones que deben adoptar en el intercambio de información confidencial y de uso interno por medio del correo electrónico.
- Los profesores y administrativos deben saber que la cuenta de correo electrónico asignada es de carácter individual; por consiguiente, ningún funcionario, bajo ninguna circunstancia debe utilizar una cuenta de correo que no sea la suya.
- Los directores y jefes de área deben designar responsables para la administración de las cuentas institucionales, donde estas personas responderán por las mismas.

- Los profesores y administrativos deben utilizar el correo electrónico para envío de mensajes e información relacionada con el desarrollo de las labores y funciones asignadas a cada usuario.

Ningún miembro de la comunidad universitaria debe utilizar el correo electrónico institucional para actividades personales de ninguna índole, entre otras, el envío de cadenas de mensajes de cualquier tipo, ya sea comercial, político, religioso, contenido discriminatorio, pornografía y demás condiciones que degraden la condición humana y resulten ofensivas para los miembros de la institución.

- Los profesores y administrativos deben mantener solamente los mensajes relacionados con el desarrollo de sus funciones, puesto que los mensajes e información contenida en los buzones de correo son propiedad de la Escuela.
- Los profesores, administrativos, estudiantes y terceros no deben enviar archivos que contengan extensiones ejecutables con contenido malicioso, bajo ninguna circunstancia.
- Los profesores y administrativos deben respetar el estándar de formato e imagen corporativa definidos por el la Escuela para los mensajes electrónicos y deben conservar en todos los casos el mensaje legal corporativo de confidencialidad.

10.3 Política de uso adecuado de internet

La Escuela, consciente de la importancia de internet como una herramienta para el desempeño de las labores diarias, proporcionará los recursos necesarios para asegurar su disponibilidad a los usuarios que así lo requieran para el desarrollo de sus actividades en la institución.

- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe proporcionar los recursos necesarios para la implementación, administración y mantenimiento requeridos para la prestación segura del servicio de internet, bajo las restricciones de los perfiles de acceso establecidos.

- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe diseñar e implementar mecanismos que permitan la continuidad o restablecimiento del servicio de internet en caso de contingencia interna.
- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe monitorear continuamente el canal o canales del servicio de internet, en cuanto a carga y tráfico.
- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe establecer procedimientos e implementar controles para evitar la descarga de software no autorizado, evitar código malicioso proveniente de internet y evitar el acceso a sitios catalogados como restringidos.
- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe generar registros de la navegación y los accesos de los usuarios a internet, así como establecer e implantar procedimientos de monitoreo sobre la utilización del servicio de internet.
- La Oficina de Sistemas y Recursos Informáticos (Osiris) en acompañamiento con Recursos Humanos y la Vicerrectoría Académica deben generar campañas para concientizar tanto a los profesores, administrativos, estudiantes y terceros, respecto a las precauciones que deben tener en cuenta cuando utilicen el servicio de internet.
- Los profesores, administrativos, estudiantes y terceros deben hacer uso del servicio de internet que provee la Escuela para las actividades que guarden relación con su labor dentro de la Escuela.
- Los profesores, administrativos, estudiantes y terceros deben abstenerse de descargar no autorizado desde internet, así como su instalación en las estaciones de trabajo asignados para el desempeño de sus labores, a menos que sean autorizados por la Oficina de Sistemas y Recursos Informáticos (Osiris).
- Los profesores, administrativos, estudiantes y terceros no deben acceder a páginas relacionadas con pornografía, drogas, alcohol, webproxys, hacking y cualquier otra página que vaya en contra de la ética y la moral, las leyes vigentes del país o las políticas establecidas en este documento, a menos que la labor que tiene en la Escuela, así lo demande.

- Los profesores y administrativos no deben utilizar el servicio de internet para el acceso y uso de servicios interactivos o mensajería instantánea como Facebook y otros similares, con el fin de intercambiar información confidencial o de uso interno de la institución o para actividades que no corresponden con el desempeño de las funciones asignadas.
- Los profesores, administrativos, estudiantes y terceros no deben descargar, usar, intercambiar o instalar juegos, música, películas, información que de alguna manera atenten contra la propiedad intelectual de sus autores.
- Los profesores, administrativos, estudiantes y terceros no deben ejecutar archivos o herramientas que atenten contra la integridad, disponibilidad o confidencialidad de la infraestructura tecnológica de la institución.
- Los profesores, administrativos, estudiantes y terceros deben asegurarse que la información audiovisual (videos e imágenes) descargada y utilizada para las labores diarias no atenten contra la propiedad intelectual de sus autores.
- Los profesores y administrativos no deben intercambiar de ninguna forma, información confidencial para la institución sin la debida autorización.

10.4 Transferencia de información

La Escuela, asegurará la protección de la información en el momento de ser transferida o intercambiada con otras entidades y establecerá los procedimientos y controles necesarios para el intercambio de información; así mismo, se establecerán Acuerdos de Confidencialidad o de Intercambio de Información con las terceras partes con quienes se realice dicho intercambio. La institución velará por el uso de tecnologías informáticas y de telecomunicaciones para llevar a cabo el intercambio de información; sin embargo, establecerá directrices para el intercambio de información en medio físico.

10.4.1 Políticas y procedimientos de transferencia de información

- La oficina Jurídica, en acompañamiento con la Oficina de Sistemas y Recursos Informáticos (Osiris)(Osiris), debe definir los modelos de Acuerdos de Confidencialidad y de intercambio de información entre la institución y terceras partes incluyendo los com-

promisos adquiridos y las penalidades civiles o penales por el incumplimiento de dichos acuerdos.

- Entre los aspectos a considerar se debe incluir:
  - La prohibición de divulgar la información entregada por parte de la Escuela a los terceros con quienes se establecen estos acuerdos.
  - La destrucción de dicha información una vez cumpla su cometido.
- La oficina Jurídica debe establecer en los contratos que se constituyan con terceras partes, los Acuerdos de Confidencialidad o Acuerdos de intercambio dejando explícitas las responsabilidades y obligaciones legales asignadas a dichos terceros por la divulgación no autorizada de información de la institución que les ha sido entregada.
- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe velar porque el intercambio de información con entidades externas se realice en cumplimiento de este Manual de Políticas de Seguridad, los Acuerdos de Intercambio de Información y el procedimiento definido para dicho intercambio de información.
- Los profesores y administrativos deben utilizar únicamente los mecanismos y herramientas proporcionadas por la Oficina de Sistemas y Recursos Informáticos (Osiris) para el envío o recepción de información confidencial para la institución.
- Los profesores y administrativos no deben revelar o intercambiar información confidencial de la institución por ningún medio, sin contar con la debida autorización.

11. Adquisición, desarrollo y mantenimiento de sistemas

Manual de Políticas

SEGURIDAD & PRIVACIDAD DE LA INFORMACIÓN

11.1 Políticas para establecer los requisitos de seguridad de los sistemas de información

La Escuela, asegurará que el software adquirido y desarrollado tanto al interior de la institución como por terceras partes, cumplirá con los requisitos de seguridad y calidad establecidos por él. Las áreas propietarias de sistemas de información y la Oficina de Sistemas y Recursos Informáticos (Osiris), incluirán requisitos de seguridad en la definición de requerimientos y posteriormente se asegurarán que estos se encuentren generados a cabalidad durante las pruebas realizadas sobre los desarrollos del software construido.

- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe aprobar la compra de los aplicativos o el software en concordancia con la política de adquisición de bienes de la institución.
- La oficina de Sistemas y Recursos Informáticos (Osiris) debe establecer metodologías para el desarrollo de software, que incluyan la definición de requerimientos de seguridad y las buenas prácticas de desarrollo seguro.
- Las áreas propietarias de los sistemas de información, en acompañamiento con la Oficina de Sistemas y Recursos Informáticos (Osiris), deben establecer las especificaciones de adquisición o desarrollo de sistemas de información, considerando los requerimientos de seguridad de la información.
- Las áreas propietarias de los sistemas de información deben definir qué información confidencial puede ser eliminada de sus sistemas y solicitar que estos soporten la eliminación de dicha información, como es el caso de los datos personales o financieros, cuando estos ya no son requeridos.
- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe liderar la definición de requerimientos de seguridad de los sistemas de información, teniendo en cuenta aspectos como la estandarización de herramientas de desarrollo, controles de autenticación, controles de acceso y arquitectura de aplicaciones, entre otros.
- Los desarrolladores deben documentar los requerimientos establecidos y definir la arquitectura de software más conveniente para cada sistema de información que se

quiera desarrollar, de acuerdo con los requerimientos de seguridad y los controles deseados.

- Los desarrolladores deben certificar que todo sistema de información adquirido o desarrollado utilice herramientas de desarrollo licenciadas y reconocidas en el mercado.
- Los desarrolladores deben deshabilitar las funcionalidades de completar automáticamente en formularios de solicitud de datos que requieran información sensible.
- Los desarrolladores deben cerrar las sesiones activas de las aplicaciones luego que pasen tres minutos sin actividad, terminándolas una vez se cumpla este tiempo.
- Los desarrolladores deben asegurar que no se permitan conexiones recurrentes a los sistemas de información con el mismo usuario.
- Los desarrolladores deben utilizar usar los protocolos sugeridos por la Oficina de Sistemas y Recursos Informáticos (Osiris) en los aplicativos desarrollados.
- Los desarrolladores deben realizar la transmisión de información relacionada con pagos o transacciones en línea a los operadores encargados, por medio de canales seguros y utilizando mecanismos o herramientas de cifrado.
- Los profesores, administrativos, terceros que desarrollen un sistema de información deben proporcionar los respectivos manuales, como son:
- Manual del usuario que describa los procedimientos de operación.
- Manual técnico que describa su estructura interna, programas, catálogos y archivos.

11.2 Seguridad en los procesos de desarrollo y de soporte

11.2.1 Política de desarrollo seguro

- La Escuela velará porque el desarrollo interno o externo de los sistemas de información cumpla con los requerimientos de seguridad esperados, con las buenas prácticas para desarrollo seguro de aplicativos, así como con metodologías para la realización de pruebas de aceptación y seguridad al software desarrollado. Además, se asegurará que todo software desarrollado o adquirido, interna o externamente cuenta con el nivel de soporte requerido por la institución.

- La Oficina de Sistemas y Recursos Informáticos (Osiris) en conjunto con los propietarios de los aplicativos deben realizar las pruebas necesarias para asegurar que los sistemas de información desarrollados cumplen con los requerimientos de seguridad establecidos antes del paso a producción.
- La Oficina de Sistemas y Recursos Informáticos (Osiris) en conjunto con los propietarios de los aplicativos deben realizar las pruebas de los sistemas de información utilizando metodologías establecidas para este fin, documentado las pruebas realizadas y aprobando los pasos a producción.
- La Oficina de Sistemas y Recursos Informáticos (Osiris) en conjunto con los propietarios de los aplicativos deben realizar las pruebas por entrega de funcionalidades nuevas, por ajustes de funcionalidad o por cambios sobre la plataforma tecnológica en la cual funcionan los aplicativos.
- La Oficina de Sistemas y Recursos Informáticos (Osiris) en conjunto con los propietarios de los aplicativos deben aprobar las migraciones entre los ambientes de desarrollo, pruebas y producción de sistemas de información nuevos y de cambios o nuevas funcionalidades.
- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe implantar los controles necesarios para asegurar que las migraciones entre los ambientes de desarrollo, pruebas y producción han sido aprobadas, de acuerdo con el procedimiento de control de cambios.
- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe contar con sistemas de control de versiones para administrar los cambios de los sistemas de información.
- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe asegurase que los sistemas de información adquiridos o desarrollados por terceros, cuenten con un acuerdo de licenciamiento el cual debe especificar las condiciones de uso del software y los derechos de propiedad intelectual.
- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe generar metodologías para la realización de pruebas al software desarrollado, que contengan pautas para la

selección de escenarios, niveles, tipos, datos de pruebas y sugerencias de documentación.

- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe asegurar que la plataforma tecnológica, las herramientas de desarrollo y los componentes de cada sistema de información estén actualizados con todos los parches generados para las versiones en uso y que estén ejecutando la última versión aprobada del sistema.
- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe incluir dentro del procedimiento y los controles de gestión de cambios el manejo de los cambios en el software aplicativo y los sistemas de información de la institución.
- Los desarrolladores de los sistemas de información deben considerar las buenas prácticas y lineamientos de desarrollo seguro durante el ciclo de vida de los mismos, pasando desde el diseño hasta la puesta en marcha.
- Los desarrolladores deben proporcionar un nivel adecuado de soporte para solucionar los problemas que se presenten en el aplicativo; dicho soporte debe contemplar tiempos de respuesta aceptables.
- Los desarrolladores deben construir los aplicativos de tal manera que efectúen las validaciones de datos de entrada y la generación de los datos de salida de manera confiable, utilizando rutinas de validación centralizadas y estandarizadas.
- Los desarrolladores deben asegurar que los sistemas de información construidos validen la información suministrada por los usuarios antes de procesarla, teniendo en cuenta aspectos como:
  - Tipos de datos
  - Rangos válidos
  - Longitud
  - Listas de caracteres aceptados
  - Caracteres considerados peligrosos
  - Caracteres de alteración de rutas.

- Los desarrolladores deben suministrar opciones de desconexión o cierre de sesión de los aplicativos (logout) que permitan terminar completamente con la sesión o conexión asociada, las cuales deben encontrarse disponibles en todas las páginas protegidas por autenticación.
- Los desarrolladores deben asegurar el manejo de operaciones sensibles o críticas en los aplicativos desarrollados permitiendo el uso de dispositivos adicionales como parámetros adicionales de verificación.
- Los desarrolladores deben asegurar que los aplicativos proporcionen la mínima información de la sesión establecida, almacenada en cookies y complementos.
- Los desarrolladores deben garantizar que no se divulgue información confidencial en respuestas de error, incluyendo detalles del sistema, identificadores de sesión o información de las cuentas de usuarios; así mismo, deben implementar mensajes de error genéricos.
- Los desarrolladores deben remover todas las funcionalidades y archivos que no sean necesarios para los aplicativos, previo a la puesta en producción.
- Los desarrolladores deben prevenir la revelación de la estructura de directorios de los sistemas de información construidos.
- Los desarrolladores deben remover información innecesaria en los encabezados de respuesta que se refieran a los sistemas operativos y versiones del software utilizado.
- Los desarrolladores deben evitar incluir las cadenas de conexión a las bases de datos en el código de los aplicativos. Dichas cadenas de conexión deben estar en archivos de configuración independientes, los cuales se recomienda que estén cifrados.
- Los desarrolladores deben certificar el cierre de la conexión a las bases de datos desde los aplicativos tan pronto como estas no sean requeridas.
- Los desarrolladores deben desarrollar los controles necesarios para la transferencia de archivos, como:
  - Exigir autenticación
  - Vigilar los tipos de archivos a transmitir

  - Almacenar los archivos transferidos en repositorios destinados para este fin o en bases de datos.
  - Eliminar privilegios de ejecución a los archivos transferidos
  - Asegurar que dichos archivos sólo tengan privilegios de lectura.
- Los desarrolladores deben proteger el código fuente de las aplicaciones construidas, de tal forma de que no pueda ser descargado ni modificado por los usuarios.
- Los desarrolladores deben asegurar que no se permite que los aplicativos desarrollados ejecuten comandos directamente en el sistema operativo.

11.3 Datos de prueba

11.3.1 Protección de datos de prueba

Osiris protegerá los datos de prueba que se entregarán a los desarrolladores, asegurando que no revelan información confidencial de los ambientes de producción.

- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe certificar que la información entregada a los desarrolladores para realizar sus pruebas no revelará información confidencial de los ambientes de producción.
- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe eliminar la información de los ambientes de pruebas, una vez estas han concluido. Relaciones con los proveedores

12. Seguridad de la información en las relaciones con los proveedores

Manual de Políticas

SEGURIDAD & PRIVACIDAD DE LA INFORMACIÓN

La Escuela, establecerá mecanismos de control en sus relaciones con los proveedores, con el objetivo de asegurar que la información a la que tengan acceso o servicios que sean provistos por las mismas, cumplan con las políticas, normas y procedimientos de seguridad de la información.

Los funcionarios responsables de la realización o firma de contratos o convenios con terceras partes se asegurarán de la divulgación de las políticas, normas y procedimientos de seguridad de la información a dichas partes.

12.1 Política de seguridad de la información para las relaciones con proveedores

- La Oficina de Sistemas y Recursos Informáticos (Osiris) y la Oficina Jurídica deben generar un modelo base para los Acuerdos de Niveles de Servicio y requisitos de Seguridad de la Información, con los que deben cumplir los proveedores de servicios; dicho modelo debe ser divulgado a todas las áreas que adquieran o supervisen recursos o servicios tecnológicos.
- La Oficina de Sistemas y Recursos Informáticos (Osiris) y la Oficina Jurídica deben elaborar modelos de Acuerdos de Confidencialidad y Acuerdos de Intercambio de Información con terceras partes. De dichos acuerdos deberán derivarse una responsabilidad tanto civil como penal para la tercera parte contratada.
- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe establecer las condiciones de conexión adecuada para los equipos de cómputo y dispositivos móviles de los terceros en la red de datos de la institución.
- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe mitigar los riesgos relacionados con terceras partes que tengan acceso a los sistemas de información y la plataforma tecnológica.

12.2 Gestión de la prestación de servicios de proveedores

La Escuela velará por mantener los niveles acordados de seguridad de la información y de prestación de los servicios de los proveedores, en concordancia con los acuerdos estable-

cidos con estos. Así mismo, velará por la adecuada gestión de cambios en la prestación de servicios de dichos proveedores.

- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe verificar el momento pertinente para que el proveedor realice la conexión, apegándose a las condiciones de conexión de los equipos de cómputo y dispositivos móviles de los terceros en la red de datos de la institución.

13. Gestión de incidentes de seguridad de la información

Manual de Políticas

SEGURIDAD & PRIVACIDAD DE LA INFORMACIÓN

13.1 Gestión de incidentes y mejoras en la seguridad de la información

La Oficina de Sistemas y Recursos Informáticos (Osiris) presentará un reporte de incidentes relacionado con la seguridad de la información a la directiva institucional.

De igual manera, asignará responsables para el tratamiento de los incidentes de seguridad de la información, quienes tendrán la responsabilidad de investigar y solucionar los incidentes reportados, tomando las medidas necesarias para evitar su reincidencia y escalando los incidentes de acuerdo con su criticidad.

La directiva institucionales será la única autorizada para reportar incidentes de seguridad ante las autoridades; así mismo, son los únicos canales de comunicación autorizados para hacer pronunciamientos oficiales ante entidades externas.

13.1.1 Responsabilidades y procedimientos

- Los directores o jefes de área como propietarios de los activos de información deben reportar a la Oficina de Sistemas y Recursos Informáticos (Osiris) los incidentes de seguridad que identifiquen o que reconozcan su posibilidad de materialización.
- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe establecer responsabilidades y procedimientos para asegurar una respuesta rápida, ordenada y efectiva frente a los incidentes de seguridad de la información.
- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe evaluar todos los incidentes de seguridad de acuerdo a sus circunstancias particulares y escalar aquellos en los que se considere pertinente.
- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe designar personal calificado, para investigar adecuadamente los incidentes de seguridad reportados, identificando las causas, realizando una investigación exhaustiva, proporcionando las soluciones y finalmente previniendo su ocurrencia nuevamente.
- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe crear bases de conocimiento para los incidentes de seguridad presentados con sus respectivas soluciones,

con el fin de reducir el tiempo de respuesta para los incidentes futuros, partiendo de dichas bases de conocimiento.

- Los profesores, administrativos, estudiantes y terceros deben reportar cualquier evento o incidente relacionado con la seguridad de la información y los recursos tecnológicos con la mayor prontitud posible.
- Los profesores, administrativos, estudiantes y terceros deben informar, en caso de conocer la pérdida o divulgación no autorizada de información clasificada como uso interno o confidencial, a la Oficina de Sistemas y Recursos Informáticos (Osiris), para que se registre y se le dé el trámite necesario.

14. Cumplimiento

14.1 Cumplimiento de requisitos legales y contractuales

La Escuela velará por la identificación, documentación y cumplimiento de la legislación relacionada con la seguridad de la información, entre ellas la referente a derechos de autor y propiedad intelectual, razón por la cual estará pendiente que el software instalado en los recursos de la plataforma tecnológica cumpla con los requerimientos legales y de licenciamiento aplicables.

14.1.1 Identificación de la legislación aplicable y de los requisitos contractuales

- La Oficina Jurídica y la Oficina de Sistemas y Recursos Informáticos (Osiris) deben identificar, documentar y mantener actualizados los requisitos legales, reglamentarios o contractuales aplicables a la institución y relacionados con seguridad de la información.
- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe certificar que todo el software que se ejecuta en la institución esté protegido por derechos de autor y requiera licencia de uso o, en su lugar sea software de libre distribución y uso.
- Los profesores y administrativos no deben instalar software en sus estaciones de trabajo suministrados para el desarrollo de sus actividades sin la autorización de la Oficina de Sistemas y Recursos Informáticos (Osiris), a menos que su labor así lo requiera, acogiéndose al buen uso y licenciamiento del software que se está utilizando.
- Los profesores, administrativos, estudiantes y terceros deben cumplir con las leyes de derechos de autor y acuerdos de licenciamiento de software. Es ilegal duplicar software sin la autorización del propietario de los derechos de autor y su reproducción no autorizada es una violación de ley; no obstante, puede distribuirse un número de copias bajo una licencia otorgada.

14.1.2 Privacidad y protección de información de datos personales

En cumplimiento de la de Ley 1581 de 2012, por la cual se dictan disposiciones para la protección de datos personales, la Escuela velará por la protección de los datos personales de

sus empleados, estudiantes, graduados, proveedores y demás terceros de los cuales reciba y administre información.

Se establecerán los términos, condiciones y finalidades para las cuales la Escuela como responsable de los datos personales obtenidos en sus distintos canales, tratará la información de todas las personas que, en algún momento, por razones de la actividad que desarrolla la institución, hayan suministrado datos personales.

Así mismo, buscará proteger la privacidad de la información personal de sus funcionarios, estableciendo los controles necesarios para preservar aquella información que la institución conozca y almacene de ellos, velando porque dicha información sea utilizada únicamente para funciones propias del negocio y no sea publicada, revelada o entregada a funcionarios o terceras partes sin autorización.

- Las áreas que procesan datos personales de estudiantes, profesores, administrativos y terceros deben obtener la autorización para el tratamiento de estos datos con el fin de recolectar, transferir, almacenar, usar, suprimir, compartir, actualizar y transmitir dichos datos personales en el desarrollo de las actividades de la institución.
- Las áreas que procesan datos personales de estudiantes, profesores, administrativos y terceros deben asegurar que solo aquellas personas que tengan una relación laboral legítima puedan tener acceso a dichos datos.
- Las áreas que procesan datos personales de estudiantes, profesores, administrativos y terceros deben acoger las directrices técnicas y procedimientos establecidos para enviar mensajes por correo electrónico a dichos usuarios.
- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe establecer los controles para el tratamiento y protección de los datos personales de los estudiantes, profesores, administrativos y terceros de los cuales reciba y administre información almacenada en bases de datos o cualquier otro repositorio y evitar su divulgación, alteración o eliminación, sin la autorización requerida.

- Los profesores y administrativos deben guardar la discreción correspondiente o la reserva absoluta con respecto a la información de la institución o de sus funcionarios de la cual tengan conocimiento en el ejercicio de sus funciones.
- Los profesores y administrativos deben verificar la identidad de todas aquellas personas a quienes se les entrega información por teléfono, por correo electrónico o certificado, entre otros.
- Los usuarios que se registren en los sistemas de información de la Escuela, deben aceptar el suministro de datos personales que pueda hacer la institución a los terceros delegados para el tratamiento de datos personales, a entidades judiciales y demás entes del Estado que, en ejercicio de sus funciones, solicitan esta información.

14.2 Revisiones de seguridad de la información

14.2.1 Cumplimiento con las políticas de seguridad de la Información

La Oficina de Sistemas y Recursos Informáticos (Osiris) tiene como una de sus funciones proponer y revisar el cumplimiento de normas y políticas de seguridad, que garanticen acciones preventivas y correctivas para salvaguardar la información digital y física, los equipos de cómputo e instalaciones de cómputo, así como de las bases de datos de información automatizada en general.

14.2.1.1 Cláusulas de Cumplimiento

- La Oficina de Sistemas y Recursos Informáticos (Osiris) debe gestionar la verificación del cumplimiento del Manual de Políticas de Seguridad de la Información.
- La Oficina de Sistemas y Recursos Informáticos (Osiris) puede implantar mecanismos de control que permitan identificar tendencias en el uso de recursos informáticos del personal interno o externo. El mal uso de los recursos informáticos que sea detectado será reportado.

- Los directores o jefes de área como dueños de los procesos establecidos en la Escuela deben apoyar las revisiones del cumplimiento de las políticas de seguridad de la información que les competa y cualquier otro requerimiento de seguridad.

14.2.1.2 Violaciones de seguridad Informática

Los profesores, administrativos, estudiantes y terceros no deben hacer uso de herramientas de hardware o software para violar los controles de seguridad de la Información, a menos que se autorice por la Oficina de Sistemas y Recursos Informáticos (Osiris).

- Ningún profesor, administrativo, estudiante o tercero, debe probar o intentar probar fallas de la Seguridad Informática conocidas, a menos que estas pruebas sean controladas y aprobadas por la Oficina de Sistemas y Recursos Informáticos (Osiris).
- Ningún profesor, administrativo, estudiante o tercero debe intencionalmente escribir, generar, compilar, copiar, coleccionar, propagar, ejecutar o intentar introducir cualquier tipo de código (programa) como virus, gusanos o caballos de Troya, diseñado para auto replicarse, dañar o afectar el desempeño o acceso a los equipos de cómputo, redes o información de la Escuela.
- Ningún profesor, administrativo, estudiante o tercero debe hacer uso de los recursos asignados para actividades no relacionadas con el propósito de la institución, o bien con la extralimitación en su uso.
- Ningún profesor, administrativo, estudiante o tercero debe realizar actividades como: traer equipos o ejecutar aplicaciones que no estén directamente especificados como parte del software, hardware o de los estándares de los recursos informáticos propios de la institución educativa.
- Ningún profesor, administrativo, estudiante o tercero debe introducir en los Sistemas de Información o la Red Corporativa contenidos obscenos, amenazadores, inmorales u ofensivos.
- Ningún profesor, administrativo, estudiante o tercero debe introducir voluntariamente programas, virus, macros, applets, controles ActiveX o cualquier otro dispositivo lógico

o secuencia de caracteres que causen o sean susceptibles de causar cualquier tipo de alteración o daño a la información o los recursos informáticos.

- Ningún docente, administrativo, estudiante o tercero debe intentar destruir, alterar, inutilizar o cualquier otra forma de dañar los datos, programas o documentos electrónicos.
- Ningún profesor, administrativo, estudiante o tercero debe albergar datos de carácter personal en carpetas diferentes a la asignada para este fin, en los computadores de trabajo.
- Cualquier archivo introducido en la red corporativa o en el puesto de trabajo del usuario a través de soportes automatizados, internet, correo electrónico o cualquier otro medio, deberá cumplir los requisitos establecidos en estas normas y, en especial, las referidas a propiedad intelectual y control de virus.

Manual de Políticas

SEGURIDAD & PRIVACIDAD DE LA INFORMACIÓN

VIGILADA MINEDUCACIÓN

AK. 45 N.° 205-59 (autopista Norte)
Línea nacional gratuita 01 8000 112 668
Contact center: 57(1) 668 36 00
Bogotá, D.C., Colombia
www.escuelaing.edu.co

Escuela Colombiana de Ingeniería Julio Garavito

Escuelaing

Personería Jurídica 086 del 19 de enero de 1973