SGSI

UNIVERSIDAD DISTRITAL
Francisco José de Caldas

SEGURIDAD DE LA INFORMACIÓN

Política para la Seguridad de la Información de la Universidad Distrital Francisco José de Caldas

TERMINOS Y CONDICIONES DE USO

Versión actual del documento: 0.0.0.11

El contenido de este texto es PRIVADO y la presente versión se considera un documento interno de trabajo.

NO SE AUTORIZA LA REPRODUCCIÓN O DIFUSION POR NINGÚN MEDIO O MECANISMO SIN EL DEBIDO CONTROL Y AUTORIZACIÓN DE LA OFICINA ASESORA DE SISTEMAS.

Tabla de Contenido

1 Introducción

En la actualidad la información de la institución se ha reconocido como un activo valioso y a medida que los sistemas de información apoyan cada vez más los procesos de misión crítica se requiere contar con estrategias de alto nivel que permitan el control y administración efectiva de los datos. Nuestra institución, los sistemas y red de información enfrentan amenazas de seguridad que incluyen, entre muchas otras: el fraude por computadora, espionaje, sabotaje, vandalismo, fuego, robo e inundación. Las posibilidades de daño y pérdida de información por causa de código malicioso, mal uso o ataques de denegación de servicio se hacen cada vez más comunes.

Con la promulgación de la presente Política de Seguridad de la Información la Universidad Distrital Francisco José de Caldas formaliza su compromiso con el proceso de gestión responsable de información que tiene como objetivo garantizar la integridad, confidencialidad y disponibilidad de este importante activo, teniendo como eje el cumplimiento de los objetivos misionales.

2 Acerca de la Seguridad de la Información

La seguridad de la información se entiende como la preservación, aseguramiento y cumplimiento de las siguientes características de la información:
• **Confidencialidad:** los activos de información solo pueden ser accedidos y custodiados por usuarios que tengan permisos para ello.
• **Integridad:** El contenido de los activos de información debe permanecer inalterado y completo. Las modificaciones realizadas deben ser registradas asegurando su confiabilidad.
• **Disponibilidad:** Los activos de información sólo pueden ser obtenidos a corto plazo por los usuarios que tengan los permisos adecuados.

Para ello es necesario considerar aspectos tales como:

•**Autenticidad**: Los activos de información los crean, editan y custodian usuarios reconocidos quienes validan su contenido.
• **Posibilidad de Auditoría:** Se mantienen evidencias de todas las actividades y acciones que afectan a los activos de información.
• **Protección a la duplicación**: Los activos de información son objeto de clasificación, y se llevan registros de las copias generadas de aquellos catalogados como confidenciales.
• **No repudio:** Los autores, propietarios y custodios de los activos de información se pueden identificar plenamente.
• **Legalidad:** Los activos de información cumplen los parámetros legales, normativos y estatutarios de la institución.
• **Confiabilidad de la Información:** Es fiable el contenido de los activos de información que conserven la confidencialidad, integridad, disponibilidad, autenticidad y legalidad..
Datos o información propiedad de la Universidad que

3 Organización para la Seguridad de la Información

La Universidad Distrital Francisco José de Caldas garantiza el apoyo al proceso de establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora del Sistema de Gestión de la Seguridad de la Información, del cual hace parte integral la presente política, por medio de la creación de una comisión técnica denominada ***Comité de Seguridad de la Información*** cuya composición y funciones serán reglamentadas por una mesa de trabajo compuesta por:

- **Vicerrector académico** o un delegado especializado,
- **Vicerrector administrativo** o un delegado especializado**,**
- **Jefe de la oficina de Planeación** o un delegado especializado,
- **Jefe de la Oficina Asesora de Sistemas** o un delegado especializado**,**
- **Jefe de la Red de Datos** o un delegado especializado**,**
- **Asesor certificado en seguridad de la información**.

En todo caso, dicha comisión o la mesa de trabajo, deberá revisar y actualizar anualmente esta política presentando las propuestas a las directivas de la institución para su aprobación mediante

resolución o acto jurídico correspondiente.

Los jefes de dependencia, previa identificación y valoración de sus activos de información, hacen parte del grupo de responsable de Seguridad de la Información y por tanto ***deben*** seguir los lineamientos de gestión enmarcados en esta política y en los estándares, normas, guías y procedimientos recomendados por el Comité de Seguridad de la Información y aprobados por las directivas.

4 Política de Seguridad de la Información

4.1 Generalidades

La información es un recurso que, como el resto de los activos, tiene valor para la institución y por consiguiente debe ser debidamente protegida.

El establecimiento, seguimiento, mejora continua y aplicación de la Política de Seguridad de la Información garantiza un compromiso ineludible de protección a la misma frente a una amplia gama de amenazas. Con esta política se contribuye a minimizar los riesgos asociados de daño y se asegura el eficiente cumplimiento de las funciones sustantivas de la entidad apoyadas en un correcto sistema de información.

La institución establecerá los mecanismos para respaldar la difusión, estudio, actualización y consolidación tanto de la presente política como de los demás componentes del Sistema de Gestión de la Seguridad de la Información y alinearlos de forma efectiva con los demás sistemas de gestión.

4.2 Alcance

Esta política es de aplicación en el conjunto de dependencias que componen la institución, a sus recursos, a la totalidad de los procesos internos o externos vinculados a la universidad a través de contratos o acuerdos con terceros y a todo el personal de la Universidad Distrital Francisco José de Caldas, cualquiera sea su situación contractual, la dependencia a la cual se encuentre adscrito y el nivel de las tareas que desempeñe.

4.3 Objetivos

a) Proteger, preservar y administrar objetivamente la información de la Universidad Distrital Francisco José de Caldas junto con las tecnologías utilizada para su procesamiento, frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de los características de confidencialidad, integridad, disponibilidad, legalidad, confiabilidad y no repudio de la información.

b) Mantener la ***Política de Seguridad de la Información*** actualizada, vigente, operativa y auditada dentro del marco determinado por los riesgos globales y específicos de la Universidad para asegurar su permanencia y nivel de eficacia.

c) Definir las directrices de la ***Universidad Distrital Francisco José de Caldas*** para la correcta valoración, análisis y evaluación de los riesgos de seguridad asociados a la información y su impacto, identificando y evaluando diferentes opciones para su tratamiento con el fin de garantizar la continuidad e integridad de los sistemas de información.

4.4 Responsabilidad

La Política de Seguridad de la Información es de aplicación obligatoria para todo el personal de la Universidad Distrital Francisco José de Caldas, cualquiera sea su situación contractual, la dependencia a la cual se encuentre adscrito y el nivel de las tareas que desempeñe.

Las directivas institucionales aprueban esta Política y son responsables de la autorización de sus modificaciones.

El **Comité de Seguridad de la Información** de la institución es responsable de revisar y proponer a las directivas institucionales para su aprobación, el texto de la Política de Seguridad de la Información, las funciones generales en materia de seguridad de la información y la estructuración, recomendación, seguimiento y mejora del Sistema de Gestión de Seguridad de la institución. Es responsabilidad de dicho comité definir las estrategias de capacitación en materia de seguridad de la información al interior de la Universidad.

El **Coordinador del Comité de Seguridad de la Información** será el responsable de coordinar las acciones del Comité de Seguridad de la Información y de impulsar la implementación y cumplimiento de la presente Política.

El **grupo responsable de Seguridad Informática** será responsable de cumplir funciones relativas a la seguridad de los sistemas de información de la entidad, lo cual incluye la operación del SGSI y supervisión del cumplimiento, dentro de la dependencia, de aspectos inherentes a los temas tratados en la presente Política. El nivel de supervisión que pueda realizar cada grupo responsable de seguridad, está relacionado con el talento humano que lo conforma y en todo caso deberá ser aprobado por el Comité de Seguridad de la Información.

Los **propietarios de activos de información (ver su definición en el glosario)** son responsables de la clasificación, mantenimiento y actualización de la misma; así como de documentar y mantener actualizada la clasificación efectuada, definiendo qué usuarios deben tener permisos de acceso a la información de acuerdo a sus funciones y competencia. En general, tienen la responsabilidad de mantener íntegro, confidencial y disponible el activo de información mientras que es desarrollado, producido, mantenido y utilizado.

El **jefe de Recursos Humanos** cumplirá la función de notificar a todo el personal que se vincula contractualmente con la Universidad, de las obligaciones respecto del cumplimiento de la Política de Seguridad de la Información y de todos los estándares, procesos, procedimientos, prácticas y guías que surjan del Sistema de Gestión de la Seguridad de la Información. De igual forma, será responsable de la notificación de la presente Política y de los cambios que en ella se produzcan a todo el personal, a través de la suscripción de los *Compromisos de Confidencialidad* y de tareas de capacitación continua en materia de seguridad según lineamientos dictados por el Comite de Seguridad de la Información.

El **jefe de la Oficina Asesora de Sistemas** en coordinación con el **Director de la Red de Datos UDNET** deben seguir los lineamientos de la presente política y cumplir los requerimientos que en materia de seguridad informática se establezcan para la operación, administración, comunicación y

mantenimiento de los sistemas de información y los recursos de tecnología de la entidad.

Corresponde a dichas jefaturas determinar el inventario de activos de información y recursos tecnológicos de los cuales son propietarios o custodios, el cual será revisado y avalado por el **Jefe de Almacén** y el **Jefe de Recursos Físicos**.

El **jefe de la Oficina Jurídica** verificará el cumplimiento de la presente Política en la gestión de todos los contratos, acuerdos u otra documentación de la entidad con empleados y con terceros. Asimismo, asesorará en materia legal a la entidad en lo que se refiere a la seguridad de la información.

Los usuarios de la información y de los sistemas utilizados para su procesamiento son responsables de conocer y cumplir la Política de Seguridad de la Información vigente.

La O**ficina de Control Interno** es responsable de practicar auditorías periódicas sobre los sistemas y actividades vinculadas con la gestión de activos de información y la tecnología de información. Es su responsabilidad informar sobre el cumplimiento de las especificaciones y medidas de seguridad de la información establecidas por esta Política y por las normas, procedimientos y prácticas que de ella surjan.

5 Identificación, clasificación y valoración de activos de información.

Cada dependencia, bajo supervisión del Comité de Seguridad de la Información, debe elaborar y mantener un inventario de los activos de información que poseen (procesada y producida). Las características del inventario, donde se incorpore la clasificación, valoración, ubicación y acceso de la información, las especifica el **Comité de Seguridad de la Información,** correspondiendo a la **Oficina Asesora de Sistemas** brindar herramientas que permitan la administración del inventario por cada dependencia, garantizando la disponibilidad, integridad y confidencialidad de los datos que lo componen.
La **Red de Datos UDNET** en coordinación con la **División de Recursos Físicos** y la **Sección de Almacén** tienen la responsabilidad de mantener el inventario completo y actualizado de los recursos de hardware y software de la institución.

6 Seguridad de la información en el Recurso Humano

Todo el personal de la Universidad Distrital Francisco José de Caldas, cualquiera sea su situación contractual, la dependencia a la cual se encuentre adscrito y el nivel de las tareas que desempeñe debe tener asociado un perfil de uso de los recursos de información, incluyendo el hardware y software asociado. La **Oficina Asesora de Sistemas** en coordinación con la **Red de Datos UDNET** deben mantener un directorio completo y actualizado de tales perfiles.

El **Comité de Seguridad de la Información** determina cuales son los atributos que deben definirse para los diferentes perfiles.

El **Comité de Seguridad de la Información** debe elaborar, mantener, actualizar, mejorar y difundir el

manual de “Responsabilidades Personales para la Seguridad de la Información en la Universidad Distrital Francisco José de Caldas”.

La responsabilidad de custodia de cualquier archivo mantenido, usado o producido por el personal que se retira, o cambia de cargo, recae en el jefe de departamento o supervisor del contrato; en todo caso el proceso de cambio en la cadena de custodia de la información debe hacer parte integral del procedimiento de terminación de la relación contractual o de cambio de cargo.

6.1 Responsabilidades del personal de la Universidad

Todo el personal de la Universidad Distrital Francisco José de Caldas, cualquiera sea su situación contractual, la dependencia a la cual se encuentre adscrito y las tareas que desempeñe debe firmar un acuerdo que contenga los términos y condiciones que regulan el uso de recursos de TI y las reglas y perfiles que autorizan el uso de la información institucional.

Los procedimientos para obtener tales perfiles y las características de cada uno de ellos deben ser mantenidos y actualizados por cada dependencia, de acuerdo a los lineamientos dados por la **Oficina Asesora de sistemas**, en cuanto a la información y la **Red de Datos UDNET**, en cuanto a los dispositivos hardware y los elementos software.

El Estatuto General y el Estatuto Docente deben contemplar procesos y sanciones disciplinarias para los casos en que se presente usos de información y TI que violen los términos y condiciones.

La **Oficina de Recursos Humanos** junto con la **Oficina Asesora de Sistemas** se encargarán de crear, actualizar, mantener y ejecutar un plan de capacitación en seguridad de la información que propenda por el crecimiento continuo de la conciencia individual y colectiva en temas de seguridad de la información.

La **Oficina Asesora de Sistemas** en conjunto con la **Red de Datos UDNET** y la **Sección de Biblioteca** se encargarán de crear y mantener un centro documental de acceso general con información relacionada con temas de seguridad de la información tales como responsabilidad en la administración de archivos, buenas prácticas, amenazas de seguridad, entre otros.

6.2 Responsabilidades de los estudiantes.

Para poder usar los recursos de TI de la Universidad, los estudiantes deben leer y aceptar en cada matrícula de semestre un acuerdo con los términos y condiciones. La **Oficina Asesora de Sistemas** debe asegurar los mecanismos para la difusión y aceptación de dichas condiciones por medio de registros y manuales en línea.

El estatuto estudiantil debe contemplar procesos y sanciones disciplinarias para los casos en que se presente usos de información y TI que violen los términos y condiciones.

6.3 Responsabilidades de Usuarios Externos

Todos los usuarios externos y personal de empresas externas deben estar autorizados por un

miembro del personal de la Universidad quien será responsable del control y vigilancia del uso adecuado de la información y los recursos de TI institucionales. Los procedimientos para el registro de tales usuarios debe ser creado y mantenido por la Oficina Asesora de Sistemas en conjunto con la Red de Datos UDNET y la Oficina de Recursos Humanos.

Los usuarios externos deben aceptar por escrito los términos y condiciones de uso de la información y recursos de TI institucionales. Las cuentas de usuarios externos deben ser de perfiles específicos y tener caducidad no superior a ***tres (3) meses***, renovables de acuerdo a la naturaleza del usuario.

6.4 Usuarios invitados y servicios de acceso público.

El acceso de usuarios no registrados solo debe ser permitido al sitio web de información institucional. El acceso y uso a cualquier otro tipo de recurso de información y TI no es permitido a usuarios invitados o no registrados.

7 Seguridad Física y del entorno

7.1 Acceso

Se debe tener acceso controlado y restringido a los cuartos de servidores principales, subsidiarios y a los cuartos de comunicaciones. La Red de Datos UDNET en conjunto con la Oficina Asesora de Sistemas elaborarán y mantendrán las normas, controles y registros de acceso a dichas áreas.

7.2 Seguridad en los equipos

Los servidores que contengan información y servicios institucional deben ser mantenidos en un ambiente seguro y protegido por los menos con:

• Controles de acceso y seguridad física.
• Detección de incendio y sistemas de extinción de conflagraciones.
• Controles de humedad y temperatura.
• Bajo riesgo de inundación.
• Sistemas eléctricos regulados y respaldados por fuentes de potencia ininterrumpida (UPS).

Toda información institucional en formato digital debe ser mantenida en servidores aprobados por la **Oficina Asesora de Sistemas** o la **Red de Datos UDNET**. El **Comité de Informática** y Telecomunicaciones define el límite de responsabilidades de las dependencias. No se permite el alojamiento de información institucional en servidores externos sin que medie una aprobación por escrito del **Comité de Seguridad de la Información**.

Equipos claves de comunicaciones deben se alimentados por sistemas de potencia eléctrica regulados y estar protegidos por UPS.

La Red de Datos UDNET debe asegurar que la infraestructura de servicios de TI este cubierta por mantenimiento y soporte adecuados de hardware y software.

Las estaciones de trabajo deben estar correctamente aseguradas y operadas por personal de la institución el cual debe estar capacitado acerca del contenido de esta política y de las responsabilidades personales en el uso y administración de la información institucional.

Los medios que alojan copias de seguridad deben ser conservados de forma correcta de acuerdo a las políticas y estándares que para tal efecto elabore y mantenga el **Comité de Seguridad en la Información.**

Las dependencias tienen la responsabilidad de adoptar y cumplir las normas definidas para la creación y el manejo de copias de seguridad.

8 Administración de las comunicaciones y operaciones

8.1 Reporte e investigación de incidentes de seguridad

El personal de la Universidad debe reportar con diligencia, prontitud y responsabilidad presuntas violaciones de seguridad a través de su jefe de dependencia a la Oficina Asesora de Sistemas o la Red de Datos UDNET. En casos especiales dichos reportes podrán realizarse directamente a la **Oficina Asesora de Sistemas**, la cual debe garantizar las herramientas informáticas para que formalmente se realicen tales denuncias.

El **Comité de Seguridad de la Información** debe preparar, mantener y difundir las normas, procesos y guías para el reporte e investigación de incidentes de seguridad.

En conformidad con la ley, la Universidad podrá interceptar o realizar seguimiento a las comunicaciones por diferentes mecanismos previa autorización del **Comité de Informática** y Telecomunicaciones, y en todo caso notificando previamente a los afectados por esta decisión.

La **Oficina Asesora de Sistemas** en conjunto con la **Red de Datos** UDNET mantendrá procedimientos escritos para la operación de sistemas cuya no disponibilidad suponga un impacto alto en el desarrollo normal de actividades. A dichos sistemas se debe realizar seguimiento continuo del desempeño para asegurar la confiabilidad del servicio que prestan.

8.2 Protección contra software malicioso y hacking.

Todos los sistemas informáticos deben ser protegidos teniendo en cuenta un enfoque multi-nivel que involucre controles humanos, físicos técnicos y administrativos. El Comité de Seguridad de la Información elaborará y mantendrá un conjunto de políticas, normas, estándares, procedimientos y guías que garanticen la mitigación de riesgos asociados a amenazas de software malicioso y técnicas de hacking.

En todo caso y como control mínimo, las estaciones de trabajo de la Universidad deben estar protegidas por software antivirus con capacidad de actualización automática en cuanto a firmas de

virus. Los usuarios de la estaciones no están autorizados a deshabilitar este control.

La Universidad a través de la **Oficina Asesora de Sistemas** o la **Red de Datos** UDNET podrá hacer seguimiento al tráfico de la red cuando se tenga evidencias de actividad inusual o detrimentos en el desempeño. La dependencia que realice dicho seguimiento deberá informar a la comunidad universitaria a través de correo electrónico o noticias en el portal institucional de la ejecución de esta tarea.

La **Red de Datos** UDNET y la **Oficina Asesora de Sistemas** deben mantener actualizada una base de datos con alertas de seguridad reportadas por organismos competentes y actuar en conformidad cuando una alerta pueda tener un impacto considerable en el desempeño de los sistemas informáticos.

8.3 Copias de Seguridad

Toda información que pertenezca a la matriz de activos de información institucional o que sea de interés para un proceso operativo o de misión crítica debe ser respaldada por copias de seguridad tomadas de acuerdo a los procedimientos documentados por el **Comité de Seguridad de la Información**. Dicho procedimiento debe incluir las actividades de almacenamiento de las copias en sitios seguros.

Las dependencias de la Universidad debe realizar pruebas controladas para asegurar que las copias de seguridad pueden ser correctamente leídas y restauradas.

Los registros de copias de seguridad deben ser guardados en una base de datos creada para tal fin. La Oficina Asesora de Sistemas debe proveer las herramientas para que las dependencias puedan administra la información y registros de copias de seguridad. La Oficina de Control Interno debe efectuar auditorías aleatorias que permitan determinar el correcto funcionamiento de los procesos de copia de seguridad.

Las copias de seguridad de información crítica debe ser mantenida de acuerdo a cronogramas definidos y publicados por la **Oficina Asesora de Sistemas** en conjunto con la **Red de Datos UDNET**.

La creación de copias de seguridad de archivos usados, custodiados o producidos por usuarios individuales es responsabilidad exclusiva de dichos usuarios. Los usuarios deben entregar al respectivo jefe de dependencia las copias de seguridad para su registro y custodia.

8.4 Administración de Configuraciones de Red

La configuración de enrutadores, switches, firewall, sistemas de detección de intrusos y otros dispositivos de seguridad de red; debe ser documentada, respaldada por copia de seguridad y mantenida por la Red de Datos UDNET.

Todo equipo de TI debe ser revisado, registrado y aprobado por la Red de Datos UDNET antes de conectarse a cualquier nodo de la Red de comunicaciones y datos institucional. Dicha dependencia debe desconectar aquellos dispositivos que no estén aprobados y reportar tal conexión como un incidente de seguridad a ser investigado.

8.5 Intercambio de Información con Organizaciones Externas.

Las peticiones de información por parte de entes externos de control deben ser aprobadas por la Vicerrectoría Administrativa y Financiera, y dirigida por dichos entes a los responsables de su custodia.

Toda la información institucional debe ser manejada de acuerdo a la legislación. (*Sección 12 de esta Política*)

8.6 Internet y Correo Electrónico

Las normas de uso de Internet y de los servicios de correo electrónico serán elaboradas, mantenidas y actualizadas por el **Comité de Seguridad de la Información** y en todo caso este comité debe velar por el cumplimiento del código de ética institucional y el manejo responsable de los recursos de tecnologías de la información.

8.7 Instalación de Software

Todas las instalaciones de software que se realicen sobre sistemas de la Universidad deben ser aprobadas por la **Oficina Asesora de Sistemas** o la **Red de Datos UDNET,** de acuerdo a los procedimientos elaborados para tal fin por dichas dependencias. El **Comité de Informática y Telecomunicaciones** definirá el ámbito en el cual actuará cada dependencia.

No se permite la instalación de software que viole las leyes de propiedad intelectual y derechos de autor en especial la **ley 23 de 1982** y relacionadas. La **Oficina Asesora de Sistemas** y la **Red de Datos** UDNET deben desinstalar cualquier software ilegal y registrar este hecho como un incidente de seguridad que debe ser investigado.

Corresponde a la **Oficina Asesora de Sistemas** en conjunto con la **Red de Datos UDNET** mantener una base de datos actualizada que contenga un inventario del software autorizado para su uso e instalación en los sistemas informáticos institucionales.

9 Control de Acceso

9.1 Categorías de Acceso

El acceso a los recursos de tecnologías de información institucionales deben estar restringidos según los perfiles de usuario definidos por el **Comité de Seguridad de la Información**.

9.2 Control de Claves y Nombres de Usuario

El acceso a información restringida debe estar controlado. Se recomienda el uso de sistemas automatizados de autenticación que manejen credenciales o firmas digitales.

Corresponde a la **Oficina Asesora de Sistemas** en conjunto con la **Red de Datos UDNET** elaborar, mantener y publicar los documentos de *servicios de red que ofrece la institución* a su personal, estudiantes, docentes y terceros.

La **Oficina Asesora de Sistemas** en conjunto con la **Red de Datos UDNET** deben elaborar, mantener y publicar procedimientos de administración de cuentas de usuario para el uso de servicios de red.

El acceso a sistemas de cómputo y los datos que contienen es responsabilidad exclusiva del personal encargado de tales sistemas.

La Universidad debe propender por mantener al mínimo la cantidad de cuentas de usuario que el personal, los estudiantes, docentes y terceros deben poseer para acceder a los servicios de red.

El control de las contraseñas de red y uso de equipos es responsabilidad de la **Red de Datos UDNET**. Dichas contraseñas deben ser codificadas y almacenadas de forma segura.

Las claves de administrador de los sistemas deben ser conservadas por la dirección de la **Red de Datos UDNET** y deben ser cambiadas en intervalos regulares de tiempo y en todo caso cuando el personal adscrito al cargo cambie. Se exceptúa de lo anterior las claves de administrador de servidores y equipos de escritorio adscritos a la **Oficina Asesora de Sistemas** las cuales deben ser conservadas por la Jefatura de la **Oficina Asesora de Sistemas** y deben ser cambiadas en intervalos regulares de tiempo y en todo caso cuando el personal adscrito al cargo cambie.

La **Red de Datos UDNET** en coordinación con la **Oficina Asesora de Sistemas** deben elaborar, mantener y actualizar el procedimiento y las guías para la correcta definición, uso y complejidad de claves de usuario.

Como requisito para la terminación de relación contractual - o laboral - del personal de la Universidad, la **Red de Datos UDNET** debe expedir un certificado de cancelación de las cuentas de usuario asignadas para el uso de recursos de tecnologías de la información de la institución.

9.3 Computación Móvil

La Universidad reconoce el alto grado de exposición que presenta la información y los datos almacenados en dispositivos portátiles (computadores portátiles, notebooks, PDA, celulares, etc). Corresponde a la Oficina de Recursos Humanos en conjunto con la Oficina Asesora de Sistemas elaborar, mantener e implementar planes de capacitación que propendan por la formación y mantenimiento de la conciencia en cuestión de seguridad de la información.

Las redes inalámbricas potencialmente introducen nuevos riesgos de seguridad que deben ser

identificados, valorados y tratados de acuerdo a los lineamientos de la ***Política de Seguridad en redes inalámbricas*** que debe elaborar el **Comité de Seguridad de la Información..**

9.4 Auditoria y Seguimiento

Todo uso que se haga de los recursos de tecnologías de la información en la Universidad deben ser seguidos y auditados de acuerdo con los lineamientos del **Código de Ética** y del **Código de Uso de Recursos de Tecnologías de la Información,** el cual debe ser elaborado por el **Comité de Seguridad de la Información**.

9.5 Acceso Remoto

El acceso remoto a servicios de red ofrecidos por la Universidad debe estar sujeto a medidas de control definidas por la **Red de Datos UDNET**, las cuales deben incluir acuerdos escritos de seguridad de la información.

10 Adquisición, Desarrollo y Mantenimiento de Sistemas Software

Para apoyar los procesos operativos y estratégicos la Universidad debe hacer uso intensivo de las Tecnologías de la Información y las Comunicaciones. Los sistemas de software utilizados pueden ser adquiridos a través de terceras partes o desarrollados por personal propio.

La Oficina Asesora de Sistemas debe elegir, elaborar, mantener y difundir el "***Método de Desarrollo de Sistemas Software en la Universidad Distrital Francisco José de Caldas***" que incluya lineamientos, procesos, buenas prácticas, plantillas y demás artefactos que sirvan para regular los desarrollos de software internos en un ambiente de mitigación del riesgo y aseguramiento de la calidad.

Todo proyecto de desarrollo de software interno debe contar con un documento de I***dentificación y Valoración de Riesgos del proyecto***. La Universidad no debe emprender procesos de desarrollo – o mantenimiento – de sistemas software que tengan asociados riesgos altos no mitigados.

Los sistemas software adquiridos a través de terceras partes deben certificar el cumplimiento de estándares de calidad en el proceso de desarrollo.

11 Administración de Continuidad del Negocio

La Administración de Continuidad del Negocio debe ser parte integral del Plan de Administración de Riesgo de la Universidad.

12 Cumplimiento

Todo uso y seguimiento de uso a los recursos de TI en la Universidad Distrital Francisco José de Caldas debe estar de acuerdo a las normas y estatutos internos así como a la legislación nacional en la materia, incluido pero no restringido a:

Constitución Política de Colombia
Ley 527-1999 Ley de comercio electrónico.
NTC 27001:2006. Sistema de Gestión de Seguridad de la Información.
ISO/IEC 17799:2005 Information technology - Security techniques - Code of practice for information security management
Proyecto Universitario Institucional
Acuerdo 027 de diciembre 23 de 1993. Estatuto Estudiantil de la Universidad Distrital Francisco José de Caldas
Estatuto Docente de la Universidad Distrital Francisco José de Caldas
Código de ética de la Universidad Distrital Francisco José de Caldas
MECI 1000:2005 Lineamientos generales para la implementación del Modelo Estándar de Control Interno para el Estado Colombiano
NTCGP1000:2004 Norma Tecnica Colombiana de la Gestion Publica
PIGA – Plan Institucional de Gestión Ambiental

13 Referencias

[**1] ISO 27001:2005.** Sistemas de gestión de Seguridad en la Información– Requerimientos .

[2] ISO/IEC 13335-1:2004. Tecnología de la información – Técnicas de seguridad – Gestión de seguridad en tecnología de información y comunicaciones – Parte 1: Conceptos y modelos para la gestión de seguridad en la tecnología de la información y comunicaciones .

[3] ISO/IEC TR 13335-3:1998. Lineamientos para la Gestión de Seguridad TI – Parte 3: Técnicas para la gestión de la seguridad TI .

[4] ISO/IEC 13335-4:2000. Lineamientos para la Gestión de la Seguridad TI – Parte 4: Selección de

salvaguardas.

[5] ISO 14001:2004. Sistemas de gestión ambiental – Requerimientos con lineamiento para su uso

[6] ISO/IEC TR 18044:2004.Tecnología de la información – Técnicas de seguridad – Gestión de incidentes en la seguridad de la información .

[7] ISO/IEC 19011:2002. Lineamientos para la auditoría de sistemas de auditoría y/o gestión ambiental

[8] ISO/IEC Guía 62:1996. Requerimientos generales para los organismos que operan la evaluación y certificación/registro de sistemas de calidad.

[9] ISO/IEC Guía 73:2002. Gestión de riesgo –Vocabulario – Lineamientos para el uso en estándares .

[10] NIST SP 800-30. Guía de Gestión de Riesgo para los Sistemas de Tecnología de la Información.

[11] ISO 9001:2000. Sistemas de gestión de calidad – Requerimientos .

14 Términos y Definiciones

14.1 Información

Toda forma de conocimiento objetivo con representación física o lógica explícita.

14.2 Activo de Información

Datos o información propiedad de la Universidad que se almacena en cualquier tipo de medio y que es considerada por la misma como sensitiva o crítica para el cumplimiento de los objetivos misionales.

Definir información sensitiva o crítica...

14.3 Sistema de Información

Conjunto ordenado de elementos cuyas propiedades se relacionan e interaccionan permitiendo la recopilación, procesamiento, mantenimiento, transmisión y difusión de información utilizando diferentes medios y mecanismos tanto automatizados como manuales.

14.4 Propietario de Activos de Información

En el contexto de la norma NTC 27001, un propietario de activos de información es cualquier persona o entidad a la cual se le asigna la responsabilidad formal de custodiar y asegurar un activo de información o un conjunto de ellos.

14.5 Tecnología de la Información

Conjunto de hardware y software operados por la entidad - o por un tercero en su nombre, que componen la plataforma necesaria para procesar y administrar la información que requiere la entidad para llevar a cabo sus funciones.

14.6 Evaluación de Riesgos

Evaluación de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma, la probabilidad de que ocurran y su potencial impacto.

14.7 Administración de Riesgos

Proceso de identificación, control y reducción o eliminación, a un costo aceptable, de los riesgos de seguridad que podrían afectar a la información. Dicho proceso es cíclico y debe llevarse a cabo en forma periódica.

14.8 Comité de Seguridad de la Información

El Comité de Seguridad de la Información, es un cuerpo integrado por diferentes representantes de la Universidad, destinado a garantizar el apoyo manifiesto de las directivas a las iniciativas de seguridad. Su función principal es definir, estructurar, recomendar, hacer seguimiento y mejorar el Sistema de Gestión de Seguridad de la Información (SGSI) de la institución. Depende directamente de la Vicerrectoría Administrativa y Financiera, y complementa el trabajo del **Comité de Informática y Telecomunicaciones** sirviendo como consultor técnico en temas relacionados con la seguridad de la información.

14.9 Responsable de Seguridad Informática

Coordinador general del Comité de Seguridad de la Información. Su función principal es supervisar el cumplimiento de la presente Política y los lineamientos del SGSI.

14.10 Grupo responsable de Seguridad Informática

Grupos de apoyo creado en dependencias de la Universidad que manejan información sensible o crítica y que se encargan de velar por la operación del SGSI. Están conformados por funcionarios o contratistas de la dependencia que tengan formación en temas de seguridad de la información.

14.11 Incidente de Seguridad Informática

Un incidente de seguridad informática es un evento adverso en un sistema de computadoras, o red de computadoras, que compromete la confidencialidad, integridad, disponibilidad, legalidad o confiabilidad de la información.

Puede ser causado mediante la explotación de alguna vulnerabilidad o un intento o amenaza de romper los mecanismos de seguridad existentes.

14.12 Cadena de custodia

En el ámbito de la seguridad de la información La cadena de custodia es la aplicación de una serie de normas y procedimientos tendientes a asegurar, depositar y proteger cada activo de información para evitar la pérdida de integridad, disponibilidad o confidencialidad.