Política de Seguridad de la Información

UniCatólica del Sur
FUNDACIÓN UNIVERSITARIA CATÓLICA DEL SUR

ACUERDO No. 003
(24 marzo 2021)

Por medio de la cual se aprueba la política de Seguridad de la Información en la Fundación Universitaria Católica del Sur

El Consejo Superior, en uso de sus facultades legales, estatutarias y reglamentarias y

CONSIDERANDO:

Que de acuerdo con el Artículo 15 de la Constitución Política de Colombia:

> "Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.
>
> En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.
>
> La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley (...)".

Que, la Fundación Universitaria Católica del Sur ha de establecer, implementar, operar y mantener un Sistema de Gestión Integrado bajo los lineamientos y aspectos de Seguridad y Privacidad de la información, basándose en la norma técnica ISO27001:2013, la Ley 1712 de 2014, Ley 1581 de 2012, Decreto 1330 de 2013 y demás normatividad vigente y aplicable en la materia.

Que, el Estatuto General de Unicatólica del Sur, artículo 22, establece como funciones del Consejo Superior: "Definir las políticas académicas, administrativas y la planeación de la Institución".

Que, en mérito de lo expuesto,

ACUERDA:

PRIMERO. Aprobar la Política de Seguridad de la Información en la Fundación Universitaria Católica del Sur.

SEGUNDO. El presente Acuerdo rige a partir de la fecha de su expedición.

COMUNÍQUESE Y CÚMPLASE

Dado en San Juan de Pasto, a los veinticuatro (24) días del mes de marzo de dos mil veintiuno (2021).

+Mons. JUAN CARLOS CARDENAS TORO
Presidente Consejo Superior

DARWIN HERRERA BENAVIDES
Secretario General

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

FUNDACIÓN UNIVERSITARIA CATÓLICA DEL SUR

Consejo Superior

Mons. Juan Carlos Cárdenas Toro
Presidente

Dra. Emma Guerra Nieto

Dra. Doris Sarasty Rodríguez

Dr. Gerardo León Guerrero Vinueza

Dr. Hernán Caicedo Bustos

Pbro. Carlos Santander Villarreal

Pbro. Germán Rosero Arce

Representantes Docentes a Consejos

Mg. Jimena Alexandra Ortega Ordoñez
Representante a Consejo Académico

Mg. Héctor Julio Villota Oviedo
Representante a Consejo Directivo

Esp. Oswaldo Fabian Sotto Pabón
Representante a Comité Curricular

Representantes Estudiantiles a Consejos

Jessica Eliana Díaz López
Representante a Consejo Académico

Daniela Alejandra Narváez Moncayo
Representante a Consejo Académico

Karol Elizabeth Minayo Quiñonez
Representante a Comité Curricular

Comité Rectoral

Mg. Sonia María Gómez Erazo
Rectora

PhD. Gerson Eraso Arciniegas
Vicerrector Académico y de Extensión

Mg. Víctor Iván Acosta Rodríguez
Vicerrector Administrativo y Financiero

Pbro. Jamer Adrián Bravo Díaz
Vicerrector de Proyección Social y Bienestar

Mg. Miriam Ruby Gamboa Coral
Asesora de Planeación y Desarrollo Institucional

Esp. María Antonia Cabrera Insuasty
Asesora de Sistema de Aseguramiento Interno de la Calidad

Ing. Oswaldo Ernesto Ruiz Quintero
Asesor Sistemas de Información y Comunicación

Pbro. Alexander Guillermo Ortega Rojas
Capellán y Coordinador del CAT

Elaborado por:
Ing. Oswaldo Ernesto Ruiz Quintero

Marzo 24 de 2021

TABLA DE CONTENIDO

PRESENTACIÓN

La Información, reconocida como un activo, representa hoy en día un valor de suma importancia para la Fundación Universitaria Católica del Sur. A medida que los sistemas informáticos penetran cada vez más los procesos de misión crítica de la Institución, es evidente contar con estrategias de alto nivel que permitan agregar control y administración adecuada a esta información representada en datos que se pueden procesar.

La fundación Universitaria Católica del Sur reconoce que los sistemas de información y la red de datos son susceptibles a enfrentar amenazas de seguridad generando un riesgo de daño y/o pérdida de información por lo cual se compromete a generar procesos de gestión responsable de la información, los cuales tienen como objetivo garantizar la integridad, confidencialidad y disponibilidad de los datos así como reducir el riesgo de que en forma accidental o intencional se divulgue, modifique, destruya o use en forma indebida la información de la institución, teniendo como eje el cumplimiento de los objetivos misionales.

1. GENERALIDADES

La Fundación Universitaria Católica del Sur busca la protección de sus activos de Información adoptando las siguientes directivas:

- Todos los estudiantes, profesores, administrativos, empleados, asesores, contratistas, consultores y personal temporal de la universidad, serán responsables de proteger la información a la cual accedan y procesen, para evitar su pérdida, alteración, destrucción o uso indebido.
- Es responsabilidad de todos los estudiantes, profesores, administrativos, empleados, asesores, contratistas, consultores o personal temporal de la universidad, reportar los Incidentes de Seguridad, eventos sospechosos y el mal uso de los recursos que identifique.
- Las violaciones a las Políticas y Controles de Infraestructura Tecnológica y Seguridad de la Información serán reportadas, registradas y monitoreadas.

1.1. ACUERDOS DE CONFIDENCIALIDAD

Todos los empleados de la Fundación Universitaria Católica del Sur deben aceptar los acuerdos de confidencialidad definidos por la entidad, los cuales reflejan los compromisos de protección y buen uso de la información de acuerdo con los criterios establecidos en ella.
Estos acuerdos deben aceptarse por cada uno de ellos como parte del proceso de contratación, razón por la cual dicha cláusula y/o acuerdo de confidencialidad hace parte integral de cada uno de los contratos.

1.2. OBJETIVOS DE LA POLÍTICA

La presente política tiene como objetivos los siguientes:

- Implementar y dar a conocer los lineamientos de seguridad de la información de la Fundación Universitaria Católica del Sur, para proteger, preservar y administrar objetivamente la información de la Institución junto con las tecnologías utilizadas para su procesamiento, frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de las características de confidencialidad, integridad, disponibilidad, legalidad, confiabilidad y no repudio de la información.
- 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 Institución para asegurar su permanencia y nivel de eficacia.

1.3. ALCANCE

Este documento aplica para la creación e implementación de todas las políticas de seguridad tanto de los recursos en red como de resguardo, copia y manejo de la información que se maneja dentro de la Institución. Busca estandarizar los procesos de la Oficina Asesora de Sistema de Información y Comunicaciones para su mejor funcionamiento.

1.4. DEFINICIONES

- **Activo de información:** Información representada en registros de tipo físico o digital que tienen valor para la Institución.

- **Amenaza:** Evento que puede ser la causa de un hecho que comprometa la confidencialidad, integridad o disponibilidad de algún activo de información de la Institución.
- **Análisis de riesgo:** Diagnóstico para identificar los riesgos de los mecanismos de protección de los activos de información con el fin de optimizar dichos mecanismos y facilitar su monitoreo.
- **Confidencialidad:** Garantía que la información no está disponible o es divulgada a personas, entidades o procesos no autorizados.
- **Continuidad:** Conjunto de actividades que permitan garantizar la operación cotidiana de la Institución.
- **Control:** Medida utilizada para garantizar la confidencialidad, integridad y disponibilidad de un activo de la información.
- **Cuenta de Usuario:** Una cuenta de usuario es la que permite la autenticación a los servicios de un sistema. Por lo general, autoriza el acceso. Aunque, la autenticación no implica autorización automática.
- **Custodio de la información:** Cargo o grupo de trabajo encargado de mantener las medidas de protección establecidas sobre los activos de información confiados.
- **Disponibilidad:** Garantizar que el personal autorizado podrá acceder a la información cuando lo requieran.
- **Evaluación del riesgo:** Determina el valor de los activos de información, identifica las amenazas aplicables y las vulnerabilidades que existen (o pueden existir), identifica los controles existentes y sus efectos en el riesgo identificado, determina los efectos potenciales y finalmente prioriza los riesgos derivados y los ordena contra el conjunto de criterios de valoración del riesgo en el contexto establecido.
- **Gestión de activos:** Conjunto de actividades que consisten en la clasificación de los activos identificados, gestión de riesgo y seguimiento de los controles aplicados con el fin de garantizar la confidencialidad, integridad de los activos de información que forman parte del SGSI.
- **Gestión de incidentes:** Conjunto de actividades y recursos con los que se manejan los eventos que afectan la confidencialidad, integridad y disponibilidad de la información de La Institución.
- **Gestión de vulnerabilidades:** Conjunto de actividades que consiste en detectar y controlar el riesgo generado por las vulnerabilidades mediante el uso de controles.
- **ICTUS:** Sistema de Información Académico de la Fundación Universitaria Católica del Sur.
- **Incidente de seguridad de la información:** Evento no deseado o inesperado con una probabilidad significativa de comprometer operaciones de negocio, divulgación de datos confidenciales o de uso interno de la Institución o datos personales de los cuales la Institución es responsable, tal que desencadene en repercusiones sobre aspectos financieros, operativos o en su reputación. Ejemplos de incidentes de seguridad de la información son: Pérdida de servicio en equipos, instalaciones o conexiones, incumplimiento de las políticas o directrices referentes a seguridad de la información, ataques de Phishing, infecciones de código malicioso (virus, malware, etc.), entre otros.
- **Impacto:** Grado en que se ve afectado un activo de información e incluso la Institución por la materialización de un riesgo.
- **Información:** Datos relacionados que tienen significado para la Institución. Estos datos pueden presentarse en formato digital o en documentos físicos.
- **Integridad:** Propiedad o atributo de la información que indica que la información no debe tener modificaciones por parte de personas o procesos que no cuenten con la debida

autorización.

- **Medio removible:** Componente extraíble de hardware utilizado para el almacenamiento de información. Por ejemplo, cintas, discos duros removibles, CDs, DVDs y unidades de almacenamiento USB.
- **Phishing:** Técnica utilizada para obtener información confidencial (nombres de usuario, contraseñas, etc.) mediante el envío de comunicaciones electrónicas aparentemente confiables.
- **Propietario de un activo de información:** Parte designada por la entidad (un cargo, proceso o grupo de trabajo) que tiene la responsabilidad de garantizar que la información y los activos asociados con el proceso se clasifican adecuadamente. También se encargan de definir y revisar periódicamente las restricciones y clasificaciones del acceso. El propietario decide sobre la finalidad, contenido y uso del activo de información y es responsable de la seguridad del activo.
- **Riesgo:** Es una combinación de los efectos que pueden seguir a la ocurrencia de un evento no deseado y de la probabilidad de la ocurrencia del evento. La evaluación del riesgo describe cualitativamente el riesgo y permite a los gerentes priorizar los riesgos de acuerdo a su percepción de la gravedad u otros criterios establecidos.
- **Red Activa:** Se refiere a todos los dispositivos que permiten la comunicación como switches, router, AP, etc
- **Registros de auditoría (logs):** Registro histórico de las actividades generadas en un sistema o una aplicación. Se utilizan para rastrear, detectar, auditar y analizar comportamientos no esperados.
- **RPO (Recovery Point Objective – Punto de recuperación objetivo):** Punto de referencia anterior al que debe ser restaurada la información usada por un proceso de negocio después de una interrupción, para lograr su reanudación. Se debe definir su pérdida máxima de información (DRII). RTO (Recovery Time Objective – Tiempo de recuperación objetivo): Periodo de tiempo inmediatamente posterior a la ocurrencia de un evento de interrupción dentro del cual deben reanudarse o recuperarse: la entrega de productos o servicios, las actividades críticas, y los recursos. El RTO debe ser menor al tiempo en el que los impactos financieros y operacionales identificados en el BIA sean inaceptables (DRII).
- **Seguridad de la información:** Es la preservación de la confidencialidad, integridad y disponibilidad de los activos de información a través de la gestión de riesgos.
- **Seguridad informática:** Implementación y mantenimiento de herramientas y controles a nivel de hardware, software y decisiones organizacionales para garantizar la seguridad de la infraestructura tecnológica.
- **Sesión:** Duración de una conexión entre un usuario y un servidor, generalmente involucrando el intercambio de múltiples paquetes de datos entre ambos.
- **PGIYC:** Proceso de Gestión de la Información y Comunicaciones
- **Sistema de información:** Componente de software desarrollado por la Institución o por un fabricante externo que requiere la interacción de uno o más activos de información para efectuar sus tareas.
- **Software malicioso:** Programa que tiene como objetivo infiltrarse o dañar la infraestructura tecnológica. Los objetivos más comunes son los sistemas operativos, redes de datos o los sistemas de información.
- **Tercero:** Persona jurídica o natural que tienen relaciones contractuales o de otro tipo con la Institución y que no son empleados, profesores, estudiantes o egresados. Ejemplo: Proveedores, contratistas y consultores.

- **Vulnerabilidad:** Debilidad frente a una amenaza. Generalmente responde a la ausencia o deficiencia de controles que permiten que una amenaza materialice un riesgo.

1.5. RESPONSABLE

Es responsable de cumplir y hacer cumplir esta política y seguir los estándares establecidos para la utilización de la infraestructura tecnológica de la Fundación Universitaria Católica del Sur es el jefe de la Oficina Asesora de Sistema de Información y Comunicaciones o quien se designe. Además, todo colaborador administrativo, académico y tercero que tenga acceso a los activos de información de la Institución debe conocer, aceptar de manera expresa y cumplir con las disposiciones de esta política. Además, debe utilizar la información sólo para los fines permitidos por la Ley, los establecidos por la Institución o los declarados por los titulares de los datos personales, según sea el caso, buscando garantizar la reserva y confidencialidad de la misma cuando no sea de carácter público y, por lo tanto, se debe abstenerse de suministrarla a personas no autorizadas.

2. ESTRATEGIAS

La fundación Universitaria Católica del Sur define las siguientes estrategias:

2.1. GESTIÓN DE ACTIVOS DE INFORMACIÓN.

Los activos de información de la Institución deben ser identificados y clasificados de acuerdo con su grado de criticidad. Así mismo, deben tener un propietario designado, quien tiene la responsabilidad de garantizar que se clasifican adecuadamente, revisar las restricciones de acceso y la seguridad del activo.

Todos los miembros de la comunidad de la Institución tienen la responsabilidad de proteger y usar adecuadamente los activos de información.

Los activos de información deben categorizarse según la siguiente clasificación:
- **Confidencial:** Información que puede ser conocida y utilizada por personas autorizadas de la Institución, pero no puede ser divulgada sin autorización del propietario.
- **De uso interno:** Información que puede ser utilizada por empleados de la Institución y entidades con la debida autorización del propietario.
- **Pública:** Información conocida y utilizada por cualquier persona.

El etiquetado, manejo, procesamiento, almacenamiento y comunicación de todos los activos de información se dará de acuerdo con la clasificación asignada.

2.2. DE ACCESO A INTERNET

Internet es una herramienta de trabajo que permite navegar en muchos otros sitios relacionados o no con las actividades propias de la universidad por lo cual el uso adecuado de este recurso será controlado, verificado y monitoreado por el jefe de la Oficina Asesora de Sistema de Información y Comunicaciones, considerando, para todos los casos, los siguientes lineamientos:

No está permitido:

- El acceso a páginas relacionadas con pornografía, drogas, alcohol, webproxys, hacking y/o cualquier otra página que vaya en contra de la ética moral, las leyes vigentes o políticas aquí establecidas.
- El intercambio no autorizado de información de propiedad de la Institución, de sus estudiantes y/o de sus empleados, con terceros a través de internet.
- La descarga, uso, intercambio y/o instalación de juegos, música, películas, protectores y fondos de pantalla, software de libre distribución, información y/o productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica (hacking), entre otros. La descarga, uso, intercambio y/o instalación de información audiovisual (videos e imágenes), asociando los procedimientos y controles necesarios para el monitoreo y aseguramiento del buen uso del recurso.

Cada uno de los usuarios es responsable de dar un uso adecuado a este recurso y en ningún momento puede ser usado para realizar prácticas ilícitas o mal intencionadas que atenten contra terceros, la legislación vigente y los lineamientos de seguridad de la información, entre otros.

Los estudiantes, profesores y administrativos, no pueden asumir en nombre de la Fundación Universitaria Católica del Sur, posiciones personales en encuestas de opinión, foros u otros medios similares que se encuentren en Internet.

El uso de Internet no considerado dentro de las restricciones anteriores, es permitido siempre y cuando se realice de manera ética, razonable, responsable, no abusiva y sin afectar la productividad ni la protección de la información y la infraestructura de la Fundación Universitaria Católica del Sur.

2.3. CORREO ELECTRÓNICO Y HERRAMIENTAS DE LA PLATAFORMA GOOGLE

Los estudiantes, profesores y administrativos que se encuentren activos en la Institución se les asignará una cuenta de correo electrónico en la plataforma Google, la cual les dará acceso a otras herramientas de esta plataforma, las cuales deben ser usadas bajo los mismos principios del uso de correo electrónico.

La Fundación Universitaria Católica del Sur a través del jefe de la Oficina Asesora de Sistema de Información y Comunicaciones administrará las cuentas de correo electrónico institucional asociadas a los dominios disponibles, estas cuentas serán asignadas de acuerdo a la disponibilidad de las mismas, y solo se crearán a nombre de las dependencias cuando se trate de cargos directivos o administrativos, en el caso de los estudiantes y los docentes se crearán usando un nombre y un apellido separados por un punto. Se tendrán en cuenta además los siguientes lineamientos:

- Las cuentas de correo electrónico se entregarán a estudiantes, profesores y administrativos que se encuentren activos en la Fundación Universitaria Católica del Sur.
- Si un estudiante, docente o administrativo se encuentra desvinculado a la universidad por un periodo superior a un semestre se procederá a eliminar la cuenta y transferir los archivos que

esta tenga a una cuenta que el administrador disponga.
- La cuenta de correo electrónico y el uso de otras herramientas de la plataforma debe ser usada para el desempeño de las funciones asignadas dentro de la universidad, así mismo estas no podrán ser utilizadas para uso personal.
- Los mensajes y la información contenida en los buzones de correo son propiedad de la Fundación Universitaria Católica del Sur y cada usuario, como responsable de su buzón, debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones.
- Se prohíbe la descarga de archivos ejecutables, en caso de tener dudas con respecto a la procedencia o el contenido de un correo electrónico esto debe ser informado a al jefe de la Oficina Asesora de Sistema de Información y Comunicaciones.

No es permitido:

- Enviar cadenas de correo, mensajes con contenido de proselitismo religioso, político, racista, sexista, pornográfico, publicitario no corporativo o cualquier otro tipo de mensajes que atenten contra la dignidad y la productividad de las personas o el normal desempeño del servicio de correo electrónico en la Institución, mensajes mal intencionados que puedan afectar los sistemas internos o de terceros, mensajes que vayan en contra de las leyes, la moral y las buenas costumbres y mensajes que inciten a realizar prácticas ilícitas o promuevan actividades ilegales.
- Utilizar la dirección de correo electrónico de la universidad como punto de contacto en comunidades interactivas de contacto social, tales como facebook y/o Twitter, entre otras, o cualquier otro sitio que no tenga que ver con las actividades laborales, exceptuando aquellas que sean autorizadas por el jefe de la Oficina Asesora de Sistema de Información y Comunicaciones.
- El envío de archivos que contengan extensiones ejecutables, bajo ninguna circunstancia.
- Bajo ninguna circunstancia el usuario revelará a terceros la contraseña ya que todo daño o perjuicio que pudiera derivarse de este hecho serán atribuidos al usuario y, por consiguiente, de su absoluta responsabilidad

El envío de información propio de la Institución debe ser realizado exclusivamente desde la cuenta de correo que esta le proporciona. De igual manera, las cuentas de correo suministradas no se deben emplear para uso personal. El envío de correspondencia electrónica desde cuentas no oficiales no representará una posición formal u oficial de la universidad.

Toda información de la Fundación Universitaria Católica del Sur generada con los diferentes programas computacionales (Ej. Office, Project, Access, Wordpad, etc.), que requiera ser enviada fuera de la Entidad, y que por sus características de confidencialidad e integridad deba ser protegida, debe estar en formatos no editables, utilizando las características de seguridad que brindan las herramientas usadas para dicho fin. La información puede ser enviada en el formato original bajo la responsabilidad del usuario y únicamente cuando el receptor requiera hacer modificaciones a dicha información.

Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definido por la Fundación Universitaria Católica del Sur y deben conservar en todos los casos el mensaje legal institucional de confidencialidad.

2.4. SISTEMAS DE GESTIÓN DE APRENDIZAJE (UNICATÓLICA VIRTUAL)

La Fundación Universitaria Católica del Sur, brinda a sus estudiantes, docentes y personal de la institución la plataforma Moodle (Module Object-Oriented Dynamic Learning Environment), la cual se utiliza con fines educativos permitiendo la creación, gestión y distribución de estrategias y metodologías de procesos de enseñanza aprendizaje presenciales, a distancia y virtuales, integrando todo material en formato digital junto a las herramientas de comunicación, colaboración y administración educativa.

Para un adecuado funcionamiento de la plataforma Moodle (Unicatólica Virtual), se debe tener en cuenta lo siguiente:

- Para el acceso a la plataforma Moodle, todos los participantes tendrán su Nombre de Usuario y Contraseña personal e intransferible. En caso de pérdida de esta información, debe dirigirse al administrador de la plataforma o recuperarlos por medio del correo institucional.
- Los usuarios no podrán modificar o cambiar su Nombre de Usuario, ya que este quedará registrado como el oficial y al cambiarlo sin autorización puede generar inconvenientes para el administrador.
- El administrador de la plataforma Moodle utilizará la información personal de cada usuario con fines de creación de cursos, creación de usuarios y matriculación de los mismos dentro de la plataforma.
- El administrador realizará copias de seguridad de la información de la plataforma Moodle al finalizar cada semestre académico vigente con fines de seguridad y disponibilidad de la información.
- El usuario subirá una imagen personal para el perfil de usuario siempre y cuando sea de su rostro y no atente contra las normas vigentes de la institución, de lo contrario esta podrá ser retirada sin previo aviso.
- Bajo ninguna circunstancia el usuario revelará a terceros la contraseña ya que todo daño o perjuicio que pudiera derivarse de este hecho serán atribuidos al usuario y, por consiguiente, de su absoluta responsabilidad.
- El usuario deberá utilizar la plataforma Moodle exclusivamente para actividades académicas.
- El usuario deberá dirigirse con respeto hacia los demás usuarios que se encuentren dentro de la plataforma Moodle.
- El usuario con Rol de docente no podrá cambiar, ni modificar los nombres largos y nombres cortos de las asignaturas que han sido asignados por el administrador de la plataforma Moodle teniendo en cuenta el plan de estudios de cada programa académico. Tampoco podrá modificar o cambiar el banner de presentación de cada curso o asignatura.
- Se prohíbe el envío de información que pueda perjudicar el tráfico de la red como correos masivos (cadenas), virus, publicidad con fines no académicos.
- Se prohíbe subir archivos, anunciar, o transmitir cualquier contenido ilegal, amenazador, abusivo, malicioso, agraviante, difamatorio, vulgar, obsceno, pornográfico, invasivo de la privacidad, odioso, racial o étnicamente inaceptable y/ o cualquier otro que generen responsabilidades civiles o penales.
- Se prohíbe suplantar la identidad de una persona para acceder a la plataforma.
- Se prohíbe la publicación de información o conocimiento que viole los derechos de autor.
- Se prohíbe subir archivos, anunciar, o transmitir cualquier contenido que infringe cualquier ley, acuerdo de confidencialidad, patente, derechos de propiedad literaria u otros derechos de propiedad de cualquier parte. Particularmente debe tener presente la normatividad de derechos

de autor, la cual prohíbe la fotocopia de libros, gráficos, música o software que tenga derechos reservados. Ante la duda el usuario no deberá subir el material y consultará a la Oficina Asesora de Sistemas de Información y Comunicaciones.

2.5. RECURSOS TECNOLÓGICOS

El uso adecuado de los recursos tecnológicos asignados por la Fundación Universitaria Católica del Sur a sus estudiantes, profesores, administrativos, contratistas o terceros se reglamenta bajo los siguientes lineamientos:

- La instalación de cualquier tipo de software o hardware en los equipos de cómputo de la universidad es responsabilidad del jefe de la Oficina Asesora de Sistema de Información y Comunicaciones, y por tanto son los únicos autorizados para realizar esta labor. Así mismo, los medios de instalación de software deben ser los proporcionados por la Institución a través de esta dependencia.
- Los estudiantes, profesores, administrativos, contratistas o terceros no deben realizar cambios en las estaciones de trabajo relacionados con la configuración del equipo, tales como conexiones de red, usuarios locales de la máquina, entre otros. Estos cambios pueden ser realizados únicamente por la dependencia encargada de estas tareas.
- Únicamente los estudiantes, docentes, administrativos y terceros autorizados por la universidad, pueden conectarse a la red inalámbrica de la universidad.
- Sólo personal autorizado puede realizar actividades de administración remota de dispositivos, equipos o servidores de la infraestructura de procesamiento de información de la universidad; las conexiones establecidas para este fin, deben utilizar los esquemas y herramientas de seguridad y administración definidos por el jefe de la Oficina Asesora de Sistema de Información y Comunicaciones.

2.6. ACTUALIZACIÓN DE INFRAESTRUCTURA TECNOLÓGICA

Actualizar la infraestructura tecnológica es una tarea fundamental para permitir la productividad, confiabilidad y seguridad en los servicios que presta, por tal razón es necesario mantener los siguientes lineamientos:

- Los equipos de cómputo se revisarán cada año a partir de su fecha de adquisición para comprobar su rendimiento y su operatividad dentro de la universidad, siempre se buscará que el rendimiento de estos no afecte el normal desempeño de las funciones que tienen los estudiantes, profesores o administrativos.
- Todo equipo que presente baja en el rendimiento se pondrá en observación para ver si puede ser actualizado para mantener su rendimiento normal o si tiene que ser cambiado para no afectar el normal desempeño de los estudiantes, profesores o administrativos.
- Los equipos de comunicación (Red Activa) se revisarán cada dos años a partir de su fecha de adquisición para ver su rendimiento, si estos presentaran problemas para prestar un servicio normal se procederá a enviarlos a mantenimiento o a su cambio si no presentan un rendimiento normal.
- Todos los requerimientos que se hagan a la mesa de ayuda que contengan un componente de infraestructura tecnológica tendrán un seguimiento para ver el rendimiento no afecte las funciones que cumplen los estudiantes, profesores o administrativos de la universidad.
- Cada año se evaluará la velocidad de conexión a internet contratada para así proyectar el aumento que se debe tener con base en los nuevos estudiantes que ingresan y los requerimientos internos que se tiene.

2.7. CERO PAPEL

Para que los documentos puedan tener valor probatorio, se necesitan herramientas para conservarlos y hacer que estén disponibles para su utilización. Los sistemas de archivo garantizan el mantenimiento y la conservación de la autenticidad, fiabilidad y accesibilidad de los documentos a lo largo del tiempo, gracias al uso de nuevas tecnologías es posible tener documentos en formato electrónico que cumplan con estas características.

El concepto de oficinas Cero Papel u oficina sin papel se relaciona con la reducción ordenada del uso del papel mediante la sustitución de los documentos en físico por soportes y medios electrónicos, así como la optimización en el uso que se le da al papel.

La Unicatólica del Sur comprometida con su dimensión de protección de la "casa común" establece los siguientes lineamientos:

Fotocopiar e imprimir a doble cara: Una forma eficaz de reducir el consumo de papel en la oficina es utilizar ambas caras de la hoja, en lugar de solo una. Cuando se utilizan las dos caras se ahorra papel, envíos, espacio de almacenamiento, se reduce el peso, son más cómodos para engrapar, encarpetar y transportar.

Reducir el tamaño de los documentos al imprimir o fotocopiar: Es recomendable utilizar las funciones que permiten reducir los documentos a diferentes tamaños, de tal forma que en una cara de la hoja quepan dos o más páginas por hoja, lo que para revisión de borradores resulta muy apropiado. Un amplio porcentaje de las fotocopiadoras modernas tienen la función de reducir el tamaño, lo cual deberá verificarse con los proveedores de estos equipos y servicios.

Configuración correcta de las páginas: Cuando las impresiones salen mal, frecuentemente se debe a que no verificamos la configuración de los documentos antes de dar la orden de impresión. Para evitar estos desperdicios de papel es importante utilizar las opciones de revisión y vista previa para asegurarse que el documento se encuentre bien configurado.

Revisar y ajustar los formatos: Otra estrategia es la de mejorar el uso de los espacios en los formatos usados por las dependencias con el fin de lograr usar menores cantidades de papel, Igualmente es necesaria la revisión de los procedimientos que se llevan a cabo para identificar la posibilidad de integrar varios documentos o formatos en uno solo, reducir el número de copias elaboradas, entre otras.

Lectura y corrección en pantalla: Durante la elaboración de un documento es común que se corrija entre dos y tres veces antes de su versión definitiva. Al hacer la revisión y corrección en papel se está gastando el doble del papel, de modo que un método sencillo para evitar el desperdicio es utilizar el computador para hacer la revisión en pantalla, que adicionalmente nos ofrece la posibilidad de utilizar correctores ortográficos y gramaticales antes de dar la orden de impresión. De esta manera solo se imprime la versión final del documento para su firma o radicación.

Guardar archivos no impresos en el computador: En el disco duro del computador, discos compactos, DVD u otro medio tecnológico que permita conservar temporalmente dicha

información. Es importante que las entidades cuenten con políticas claras sobre la forma de nombrar, clasificar y almacenar documentos digitales, con el fin que puedan ser preservados y garanticen su recuperación y acceso para consulta.

Conocer el uso correcto de impresora y fotocopiadoras: Es importante que todos los empleados conozcan el correcto funcionamiento de impresoras, fotocopiadoras y multifuncionales para evitar el desperdicio de papel que se deriva de errores en su utilización. De ser necesario, deberán realizarse sesiones de entrenamiento sobre el manejo de estos equipos.

Reutilizar el papel usando por una cara: Se utilizarán las hojas de papel que estén usadas por una sola cara siempre y cuando no contenga información sensible o protegida por la ley de protección de datos personales.

Reciclar: El reciclaje del papel disminuye los requerimientos de árboles para la fabricación de papel, así como la emisión de elementos contaminantes. Por tal motivo los empleados deberán mantener políticas y acciones que faciliten el reciclaje del papel.

Uso de la intranet: Se debe aprovechar al máximo el uso de esta herramienta tecnológica que evita la impresión innecesaria de documentos que pueden ser consultados directamente en línea.

Uso del correo electrónico: El correo electrónico debe constituir la herramienta preferida para compartir información evitando el uso de papel, en caso de necesitar la impresión se debe revisar el documento y eliminar aquello que no aporte información importante como los textos de "este mensaje puede contener información confidencial…", entre otros.

Herramientas de colaboración: Herramientas de colaboración tales como espacios virtuales de trabajo, programas de mensajería instantánea, aplicaciones de teleconferencia, calendarios compartidos, aplicaciones para uso y edición de documentos compartidos, entre otros, pueden ofrecer oportunidades importantes para intercambiar información de forma rápida y efectiva, evitando la utilización del papel. La Institución deberá promover su uso, cuidando de implementar las medidas de seguridad necesarias para garantizar que no se ponga en riesgo la información que manejan en sus bases de datos.

2.8. MENSAJERÍA INSTANTÁNEA

Los canales de Mensajería Instantánea (WhatsApp, Telegram, etc) NO son un medio de comunicación oficial de la institución (como lo es el correo electrónico), por lo que debe quedar claro que cualquier acuerdo y/o conversación -en el grupo- debe formalizarse por los medios OFICIALES de la Institución.

Para el uso de estos canales se debe tener en cuenta los siguientes lineamientos:

- Los grupos deben mantener siempre su objetivo y evitar usarlos para promover conversaciones ajenas al mismo, por lo cual se prohíbe el envío de chistes, memes y/o información NO relacionada con el grupo.
- El administrador del grupo debe supervisar que las reglas del mismo se estén cumpliendo, así como dar a conocer a todos los integrantes las reglas del mismo.
- WhatsApp debe ser considerada una aplicación ajena a la Institución, debido a que la misma

no tiene control sobre la aplicación, por lo cual el envío de documentos adjuntos o información sensible debe hacerse por canales oficiales.
- El envío como la recepción de mensajes deberán hacerse en horario laboral, a excepción de casos de emergencia.

3. ORGANIZACIÓN INSTITUCIONAL PARA LA EJECUCIÓN DE LA POLÍTICA

Para la ejecución de esta política se establecen los siguientes puntos:

Implementación de la política. Es responsabilidad de todos los miembros de la Institución, en el marco de sus competencias, velar por el cumplimiento de los principios, objetivos y estrategias definidos en esta política y la aplicación de los procedimientos definidos para tal fin.

Seguimiento, evaluación y recomendaciones de actualización. Las recomendaciones de actualización de la Política de seguridad de la información es responsabilidad de Consejo Directivo y su seguimiento y evaluación deberá estar en el marco del Sistema Interno de Aseguramiento de la Calidad mediante indicadores que permitan la orientación y toma de decisiones informada.

Coordinación para la ejecución de la política. El jefe de la Oficina Asesora de Sistema de Información y Comunicaciones es la dependencia responsable de coordinar la promoción, implementación, seguimiento y autoevaluación de la política de seguridad de la información con el concurso de todas las áreas misionales y de apoyo.

Promoviendo

EL DESARROLLO HUMANO INTEGRAL SOSTENIBLE

UniCatólica del Sur
FUNDACIÓN UNIVERSITARIA CATÓLICA DEL SUR

Calle 18 No. 56-02 Torobajo
PBX (2) 731 3420 Cel. 314 778 3658
Pasto, Nariño - Colombia

www.unicatolicadelsur.edu.co