ACUERDO No. CD - 469

31 DE JULIO DE 2024

"POR MEDIO DEL CUAL SE APRUEBAN LAS POLITICAS DE SEGURIDAD DE LA INFORMACIÓN DE LA CORPORACION UNIVERSIDAD DE LA COSTA".

EL CONSEJO DIRECTIVO DE LA CORPORACION UNIVERSIDAD DE LA COSTA CUC, EN EJERCICIO DE LAS FACULTADES ESTATUTARIAS OTORGADAS POR LA RESOLUCION 3235 DEL 28 DE MARZO DEL 2012 EXPEDIDA POR EL MINISTERIO DE EDUCACION NACIONAL Y

CONSIDERANDO:

1. Que la Ley 30 de 1992 ***"Por la cual se organiza el servicio público de la Educación Superior"***, establece en su artículo **Artículo 28** que. *"La autonomía universitaria consagrada en la Constitución Política de Colombia y de conformidad con la presente Ley, reconoce a las universidades el derecho a darse y modificar sus estatutos, designar sus autoridades académicas y administrativas, crear, organizar y desarrollar sus programas académicos, definir y organizar sus labores formativas, académicas, docentes, científicas y culturales, otorgar los títulos correspondientes, seleccionar a sus profesores, admitir a sus alumnos y adoptar sus correspondientes regímenes y establecer, arbitrar y aplicar sus recursos para el cumplimiento de su misión social y de su función institucional."*

2. Que los Estatutos de la Corporación Universidad de la Costa, CUC, aprobados mediante Resolución No. 3235 del 28 de marzo de 2012, expedidos por el Ministerio de Educación Nacional, establecen en su artículo 28 "Funciones del Consejo Directivo", literal

B: *"Aprobar en primera instancia las políticas generales y los planes de desarrollo de la Corporación Universidad de la Costa, CUC, en concordancia con las políticas de Educación Superior que trace el gobierno, las necesidades regionales y las expectativas del desarrollo social y económico del país".*

3. Que las directivas de la Universidad de la Costa CUC declaran su especial interés en los principios de Seguridad y Privacidad hacia la protección de la información física y digital, buscando alcanzar altos niveles de calidad y excelencia en su desempeño, para reducir el impacto de los riesgos identificados sobre sus activos, garantizando la implementación de los principios de integridad, confidencialidad y disponibilidad de la información, acorde a las necesidades de los diferentes procesos, servicios, sistemas de información y comunidades.

ACUERDA:

Artículo 1. Aprobar la Política de Seguridad de la Información, de conformidad con el siguiente contenido:

TABLA DE CONTENIDO

1. CONSIDERANDO QUE:

1. La Universidad de la Costa es una institución de educación superior comprometida con el adecuado manejo y la seguridad de la información. Una de nuestras premisas es asegurar la protección de los datos de todas las comunidades, respaldándonos en la Ley estatutaria 1581 de 2012 y su Decreto Reglamentario 1377 de 2013. Estas normativas reconocen y protegen los derechos de todas las personas en relación con la salvaguarda de sus datos.

2. Dentro de las normativas institucionales de la Universidad de la Costa CUC, se establecen las políticas que rigen el tratamiento de datos personales, enmarcado en el estricto cumplimiento de las leyes, la normatividad interna y en concordancia con la misión y visión de la Universidad. Estas normas regulan las responsabilidades de quienes manejan los datos personales de aquellos que acceden, de forma permanente o temporal, a los servicios proporcionados por la institución. Además, se cuenta con un manual interno de políticas y procedimientos diseñado para asegurar el cumplimiento adecuado de la Ley en cuestión. Este manual detalla las pautas y pasos necesarios para garantizar el respeto y la protección de los datos personales de acuerdo con las disposiciones legales aplicables.

A través del presente manual, se expondrán las distintas políticas de Seguridad de la Información, junto con los procedimientos para la recolección, almacenamiento, uso, circulación, supresión y consulta de datos personales, conforme a lo establecido en la Ley correspondiente.

2. OBJETIVOS

La Universidad de la Costa CUC orienta sus principios de Seguridad y Privacidad hacia la protección de la información física y digital, buscando alcanzar altos niveles de calidad y excelencia en su desempeño, para reducir el impacto de los riesgos identificados sobre sus activos, garantizando la implementación de los principios de integridad, confidencialidad y disponibilidad de la información, acorde a las necesidades de los diferentes procesos, servicios, sistemas de información y comunidades.

La gestión de la seguridad y privacidad de la información para la Universidad de la Costa CUC estará determinada por los siguientes objetivos:

1. Cumplir con la seguridad de la información.

2. Mantener niveles de seguridad que brinden la confianza a todas las comunidades (académica, administrativos, estudiantes, graduados y externos)

3. Realizar una gestión integral de riesgos asociados a la información y a sus activos de información.

4. Realizar los procesos de migración de información que garanticen la disposición ante la obsolescencia tecnológica.

5. Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.

6. Fortalecer la cultura de seguridad de la información en todas las comunidades de la universidad.

7. Procurar la continuidad de los procesos y servicios frente a incidentes.

3. ALCANCE

Esta política se aplicará a todas las comunidades y cualquier otra persona que tenga acceso a los sistemas de información de la institución. También se aplica esta política a equipos y sistemas informáticos (servidores, computadores personales, estaciones de trabajo, elementos de infraestructura tecnológica, base de datos, sistemas de información que apoyan los procesos académicos o administrativos) que se encuentran bajo la operación de la institución.

4. DOCUMENTOS DE REFERENCIA

1. Norma ISO/IEC 27001, capítulos A.8.3.2, A.11.2.7, A.12.1.1, A.12.1.2, A.12.3.1, A.12.4.1, A.12.4.3, A.13.1.1, A.13.1.2, A.13.2.1, A.13.2.2, A.14.2.4
2. Inventario de activos de información institucional.
3. Políticas para el Tratamiento de Datos Personales en la Universidad de la Costa CUC
4. Proceso de gestión de tecnología informática.

5. TERMINOS Y DEFINICIONES

Para una mejor interpretación del presente manual, de la Ley 1581 de 2012 y los decretos reglamentarios, se recomienda tener en cuenta las siguientes definiciones:

1. **ACTIVOS DE INFORMACIÓN:** Se refiere a cualquier recurso valioso de datos o información dentro de una organización que debe ser protegido adecuadamente para garantizar su disponibilidad, integridad y confidencialidad contra accesos no autorizados o riesgos potenciales.
2. **ADWARE:** Es un software que muestra anuncios automáticamente en la computadora del usuario, generalmente en un navegador web. Puede ser intrusivo y afectar el rendimiento del dispositivo.
3. **ANONIMIZACIÓN**: Proceso mediante el cual los datos personales se modifican para que ya no se puedan asociar a una persona específica. Este proceso es crucial para proteger la privacidad en el manejo de datos.
4. **ÁREA:** Es un departamento o división dentro de una organización, como una universidad, que se encarga de funciones específicas. Cada área tiene responsabilidades y tareas particulares que contribuyen al funcionamiento general de la institución
5. **AUTORIZACIÓN:** Consentimiento otorgado de manera voluntaria por una persona para permitir que una entidad u organización recopile, utilice o divulgue sus datos personales. Dicha entidad está obligada a utilizar la información según los términos establecidos y a garantizar su seguridad y confidencialidad. Cualquier uso no autorizado adicional de los datos puede constituir una violación de la privacidad y conllevar sanciones legales.
6. **AVISO DE PRIVACIDAD:** Es un documento que informa cómo una organización recopila, utiliza y protege sus datos personales. Contiene detalles sobre los tipos de datos recopilados, los propósitos de su uso, las medidas de seguridad implementadas y cómo las personas pueden ejercer sus derechos de privacidad. Este es fundamental para cumplir con las leyes de protección de datos y establecer confianza entre la organización y los usuarios.
7. **BASE DE DATOS:** Es un conjunto de datos organizados y estructurados, cuyo objetivo es permitir un almacenamiento eficiente y una recuperación precisa y rápida de información. Estos datos pueden ser de diversos tipos, como texto, números, imágenes, vídeos, y están diseñados para ser fácilmente accesibles, gestionados y actualizados.
8. **COLABORADOR:** Miembro de la comunidad universitaria.
9. **CONTENIDO MALICIOSO:** Se refiere a cualquier contenido que está diseñado para causar daño a sistemas informáticos, redes o usuarios. Esto incluye virus, malware, troyanos, etc.
10. **DATO PERSONAL:** Cualquier información que esté vinculada o pueda asociarse con una o varias personas naturales específicas se considera un dato personal. Esto incluye desde nombres y direcciones hasta información médica o huellas digitales. Estos datos están

protegidos por leyes de privacidad y protección de datos, para garantizar la privacidad y seguridad de los individuos.

11. **DATO PÚBLICO:** Son aquellos disponibles para ser consultados, utilizados y compartidos por cualquier persona y proporcionados por entidades gubernamentales u organizaciones públicas. Incluyen información sobre datos relativos al estado civil, profesión u oficio, y la calidad de comerciante o servidor público de las personas. Su divulgación fomenta la transparencia y la participación ciudadana, así como el desarrollo de servicios y aplicaciones en beneficio de la sociedad.
12. **DATOS SENSIBLES:** Son información privada que, si se divulga o utiliza incorrectamente, puede causar daños o discriminación. Incluyen aspectos íntimos como salud, orientación sexual, creencias religiosas, origen étnico o racial, y afiliación sindical. También abarcan datos que afectan la intimidad del titular, como orientación política, pertenencia a sindicatos u organizaciones sociales, y datos relacionados con la salud, vida sexual y biométricos.
13. **DEPENDENCIAS:** Es un área o departamento que se encarga de funciones específicas dentro de una organización, como una universidad. Cada dependencia tiene responsabilidades y tareas particulares que contribuyen al funcionamiento general de la institución.
14. **DISCRIMINACIÓN RED:** En el contexto de redes, puede referirse a la práctica de tratar de manera diferente a ciertos tipos de tráfico de red, lo que podría afectar la igualdad de acceso a recursos o información.
15. **HACKING:** Es la actividad de buscar y explotar debilidades en un sistema informático o una red. Los hackers pueden tener intenciones maliciosas (black hat) o pueden estar buscando mejorar la seguridad (white hat).
16. **INFORMACIÓN:** Datos relacionados que tienen significado para la institución. La información es un activo que, como otros activos importantes del negocio, es esencial para las actividades de la entidad y, en consecuencia, necesita una protección adecuada.
17. **IP (INTERNET PROTOCOL):** Es un conjunto de reglas que rige el formato de los datos enviados a través de Internet o una red local. Una dirección IP es un identificador único para un dispositivo en una red.
18. **LAN (LOCAL AREA NETWORK):** Es una red de computadoras que abarca un área geográfica pequeña, como una oficina, un edificio o un campus. Permite la interconexión de dispositivos dentro de ese espacio limitado para compartir recursos e información
19. **MICROSOFT:** Es una empresa multinacional de tecnología, es conocida por desarrollar, fabricar, licenciar y soportar una amplia gama de productos y servicios relacionados con la informática, incluyendo sistemas operativos, software de productividad, hardware, y servicios

en la nube. Además, es la entidad que vende el servicio de infraestructura y las licencias de usuario a la institución.

20. **MICROSOFT AUTHENTICATOR**: Es una aplicación móvil de Microsoft que proporciona autenticación multifactor (MFA) para proteger cuentas y datos. La aplicación genera códigos de verificación o envía notificaciones para aprobar inicios de sesión, mejorando la seguridad al requerir una segunda forma de verificación además de la contraseña.
21. **MICROSOFT ONE DRIVE:** Es el servicio de almacenamiento en la nube que permite a los usuarios guardar, sincronizar y compartir archivos desde cualquier dispositivo con conexión a internet, integrándose con otras herramientas de Microsoft para mejorar la productividad y colaboración.
22. **MICROSOFT TEAMS:** Es una plataforma de colaboración desarrollada por Microsoft que combina chat, videoconferencias, almacenamiento de archivos e integración de aplicaciones. Es parte del conjunto de productos de Microsoft 365 y está diseñada para facilitar la comunicación y el trabajo en equipo dentro de las organizaciones, permitiendo a los usuarios colaborar en tiempo real desde cualquier lugar. Además, es el canal principal de comunicación de la Universidad de la Costa.
23. **REDES PEER-TO-PEER (P2P):** Son redes en las que todos los participantes tienen los mismos privilegios y pueden actuar tanto como clientes como servidores. Permiten el intercambio directo de archivos entre dispositivos sin necesidad de un servidor central.
24. **RESPONSABLE DEL TRATAMIENTO:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos.
25. **SISTEMAS DE INFORMACIÓN DE MISIÓN CRÍTICA:** Son fundamentales para las operaciones esenciales de una organización al gestionar datos sensibles y estratégicos, requieren alta seguridad, disponibilidad y rendimiento para asegurar la continuidad operativa y protegerse contra interrupciones.
26. **SOFTWARES:** Es el conjunto de programas, procedimientos y rutinas asociadas con el funcionamiento de un sistema informático. El software puede ser de sistema, de aplicación o de desarrollo.
27. **SPYWARE:** Es un tipo de software malicioso que se instala en un dispositivo sin el conocimiento del usuario, con el objetivo de recopilar información sobre él y su actividad en línea.
28. **SUPLANTACIÓN DE IDENTIDAD:** Es el acto de hacerse pasar por otra persona, generalmente para obtener información confidencial o acceder a recursos restringidos. En informática, esto suele implicar el uso de técnicas como phishing.

29. **TITULAR:** Persona natural cuyos datos personales sean objeto de Tratamiento.
30. **TRANSFERENCIA DE DATOS:** Se produce una transferencia de datos cuando el responsable y/o encargado del tratamiento de datos personales, con sede en Colombia, transfiere la información o los datos personales a un destinatario, quien a su vez asume la responsabilidad del tratamiento y puede encontrarse dentro o fuera del país.
31. **TRANSMISIÓN:** El tratamiento de datos personales que implica comunicarse dentro o fuera del territorio de la República de Colombia, cuando el encargado lo trate en nombre del responsable.
32. **UPS (Sistema de Alimentación Ininterrumpida):** Dispositivo que proporciona una fuente de suministro eléctrico respaldada por una batería, diseñado para mantener el suministro de energía a un dispositivo incluso en caso de interrupción eléctrica.
33. **USUARIO INSTITUCIONAL:** Se refiere a un usuario que tiene una cuenta y acceso a los recursos de una institución, como una universidad, basada en su rol dentro de la misma. Estos usuarios suelen tener direcciones de correo electrónico y credenciales específicas proporcionadas por la institución.
34. **USUARIOS:** Son individuos que utilizan servicios, sistemas o aplicaciones informáticas. Pueden ser tanto internos (empleados, estudiantes) como externos (clientes, visitantes).
35. **VIDEOCÁMARA:** Dispositivo utilizado para la captura y grabación de imágenes en formato de vídeo.

6. GENERALIDADES

La Universidad de la Costa CUC brinda el acceso a todas las comunidades a fuentes de información nacional e internacional y provee un ambiente que fomenta la difusión del conocimiento, el proceso de creación y los esfuerzos de colaboración, en el marco del servicio educativo.

Los usuarios deben actuar honesta y responsablemente. Cada usuario es responsable por la integridad de los recursos tecnológicos y tiene el deber de respetar los derechos de otros usuarios, la integridad de las instalaciones físicas y sus métodos de control, además de respetar toda licencia y acuerdos contractuales que estén relacionados con los sistemas de información de la institución.

Todas las comunidades deberán actuar según estos lineamientos y las leyes nacionales pertinentes. El incumplimiento de esta política puede resultar en la negación de acceso al sistema de la institución o a otras acciones disciplinarias o legales.

La Universidad de la Costa CUC es un canal de medios de acceso a la vasta y creciente cantidad de información disponibles a través de medios electrónicos de información. La institución no es un ente regulador del contenido de dicha información y no asume responsabilidad alguna por el contenido de esta. Aceptar cualquier cuenta o utilizar cualquier sistema de información de la institución puede restringir o prohibir el uso de sus sistemas de información en cualquier caso que demuestre alguna violación de estas políticas o de alguna ley.

7. LINIEAMIENTOS

Para alcanzar los objetivos establecidos, la UNIVERSIDAD DE LA COSTA CUC adopta los siguientes lineamientos para gestionar la seguridad de la información:

1. Todas las comunidades, tanto internas como externas, tendrán asignadas responsabilidades relacionadas con la seguridad de la información.

2. Para proteger la información generada, procesada o almacenada por la Universidad, se implementarán controles que mitiguen los riesgos derivados de los accesos otorgados a los grupos de interés externos.

3. Se deben aplicar controles que prevengan el uso indebido de la información creada, procesada, transmitida o almacenada por la Universidad, conforme a su clasificación y custodia.

4. Es esencial proteger las instalaciones de procesamiento y la infraestructura tecnológica que soporta los procesos críticos.

5. Se debe controlar la operación de los procesos, garantizando la seguridad de los recursos tecnológicos y de las redes de datos.

6. Es imprescindible implementar controles de acceso a la información, sistemas, recursos de red y correos electrónicos, considerando a los diferentes grupos de interés.

7. La seguridad debe ser una parte integral del ciclo de vida de los sistemas de información.

8. Los incidentes de seguridad deben ser gestionados adecuadamente.

9. Es necesario asegurar la continuidad operativa, considerando el impacto potencial de los eventos de seguridad.

10. Se debe garantizar el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

8. POLÍTICAS ESPECÍFICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

La Universidad de la Costa CUC, en conformidad con su política de Seguridad y Privacidad de la Información, asegura mediante su estructura organizativa la gestión de riesgos para los activos de información institucional. Además, promueve una cultura de seguridad y privacidad entre las comunidades y cumple con políticas específicas de seguridad para gestionar de manera efectiva la información de sus activos.

8.1 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA COLABORADORES

8.1.1 Lineamientos:

1. Cada integrante de la comunidad universitaria, indistintamente del tipo de vinculación, deberá cumplir con los procedimientos, políticas y controles de seguridad y normas vigentes relacionadas con la seguridad y privacidad de la información que sean aplicables a la Universidad, incluyendo las definidas por el Estado o las autoridades competentes.

2. Las personas integrantes de la comunidad universitaria que por su cargo o rol hagan uso de información sensible, asistirán a las capacitaciones y jornadas de educación y formación que programe la Universidad en materia de seguridad de información física y digital, con el fin de adquirir las competencias necesarias para la gestión adecuada de la información y el uso correcto de los recursos y servicios informáticos institucionales.

3. Los colaboradores de la Institución, profesores, administrativos, contratistas y demás personas involucradas deben abstenerse de divulgar información confidencial, en forma escrita, verbal o por cualquier otro medio, así como también deberán abstenerse de incurrir en situaciones que pongan en riesgo la seguridad de la información.

4. El Departamento de Tecnología se encargará de emitir directrices a los funcionarios sobre amenazas de seguridad informática detectadas en la red de datos institucional, que puedan poner en riesgo la información almacenada en las estaciones de trabajo, servidores o activos de información de misión crítica.

8.1.2 Desvinculación, licencias, vacaciones o cambio de funciones

1. Cuando un colaborador o contratista finalice su proceso de vinculación laboral o contractual, o cambie de rol, deberá seguir los lineamientos descritos en el procedimiento interno de entrega de cargo, según sea el caso, de:

a. la información generada en el desarrollo de sus actividades durante el periodo de vinculación.
b. Los activos de información bajo su responsabilidad.
c. Los datos de las credenciales de acceso suministradas para el acceso a los servicios de red.

2. Cuando el colaborador se desvincula de la Universidad, el Departamento de Gestión Humana solicitará al Departamento de Tecnología de manera inmediata, la inactivación o revocación de los permisos de acceso sobre los servicios informáticos institucionales a los cuales tenía acceso para el desarrollo de sus funciones.

8.1.3 Política de uso de dispositivos

Se consideran "usuarios de dispositivos móviles" a quienes por las características de sus funciones asignadas utilizan habitualmente un portátil, smartphone, teléfono móvil, tableta, etc. dentro y fuera de la institución.

1. Realizar el registro de control sobre la asignación, salida, baja y traslado de los dispositivos móviles teniendo en cuenta los parámetros y procedimientos estipulados en el reglamento interno de trabajo de la Universidad de la Costa.

2. Se permite hacer monitoreo de los dispositivos y someterlos a controles en cuanto al tipo y versionado de aplicaciones instaladas. De manera similar, pueden ser limitados a conexión hacia ciertos servicios informáticos que sean considerados no autorizados o maliciosos.

3. Los usuarios de dispositivos móviles institucionales harán uso adecuado de los mismos, teniendo en cuenta:

4. La información que reposa en los dispositivos es responsabilidad del colaborador que tiene a su cargo el dispositivo, por ende, debe hacer copias de respaldo en la plataforma provista por

institución (Microsoft One Drive), la cual cuenta con un espacio limitado, si se requiere más espacio debe contactar al Departamento de Tecnología.

5. Quienes son usuarios no están autorizados a cambiar la configuración, ni a desinstalar software de los equipos móviles institucionales, únicamente se deben aceptar y aplicar las actualizaciones.

6. Quien tenga a su cargo un equipo no podrá realizar la instalación de programas desde fuentes desconocidas y sin licencia, por ende, se requiere instalar aplicaciones únicamente desde repositorios seguros y previa consulta al área de tecnología.

7. Cuando se conectan los dispositivos a redes públicas de datos que no ofrezcan las garantías de seguridad física y lógica necesarias, se incurre en el riesgo de ser víctima de hurto de información; por ende, se debe evitar realizar transacciones o conexiones no seguras con los servicios institucionales.

8. Quienes tengan configurado el correo electrónico institucional en sus dispositivos móviles (Smartphone, tabletas, pc portátil, etc.) deben reportar tan pronto como sea posible, la pérdida o robo de estos al Departamento de Tecnología, a través de los canales establecidos.

9. No deben almacenar videos, fotografías o información personal en los dispositivos móviles institucionales asignados

10. Todos los usuarios de equipos móviles (computadores portátiles, notebooks, PDA, celulares, Tablet, etc.), incluyendo los de personal externo a la institución, que desean hacer uso de la red inalámbrica institucional deben contar con un sistema de autenticación basando en las normas de uso de la red LAN institucional.

11. El Departamento de Tecnología velará por:

a. Implementar los controles tecnológicos que impidan la conexión a redes y servicios de la Universidad de equipos con sistemas operacionales con modificaciones consideradas inseguras o que ejecuten acciones para vulnerar la seguridad de las comunicaciones.
b. Proveer los servicios que faciliten la actualización y aseguramiento de los sistemas operacionales y aplicaciones en los dispositivos institucionales.
c. Monitorear el uso de los servicios y aplicaciones web institucionales accedidos desde dispositivos conectados a la red LAN de datos.
d. Implementar controles de seguridad en dispositivos para monitorear, alertar y prevenir fugas de información.

8.1.4 Política para uso de conexiones remotas

1. Las conexiones por acceso remoto a los servicios informáticos ofrecidos por la Universidad deben estar sujetas a controles y restricciones definidos por la División de Servicios de Información.

2. Las conexiones remotas requieren ser monitoreadas y se emitirán alertas sobre potenciales amenazas internas y externas de acceso no autorizado a la información o recursos.

3. Los usuarios que requieran realizar acceso remoto a los sistemas de información institucional a cargo de la Departamento de Tecnología deberán efectuarlo bajo condiciones de seguridad establecidas.

4. Los usuarios que requieran hacer conexión remota a los sistemas de información de misión crítica deben contar con el visto bueno del Departamento de Tecnología.

5. El soporte, mantenimiento y actualización del hardware y software empleado para realizar las conexiones remotas a los servicios institucionales estará a cargo del Departamento de Tecnología

6. Quienes tengan roles sensibles y que requieran acceder remotamente a información o sistemas de información institucionales no deberán realizar conexiones desde:

a. WIFI de uso gratuito o libre,
b. Equipos de cómputo de uso libre
c. Dispositivos que no cuentan con las condiciones mínimas de seguridad como un antivirus o firewall.

8.2 POLÍTICAS DE GESTIÓN DE ACTIVOS DE INFORMACIÓN DE SEGURIDAD DIGITAL

El Departamento de Tecnología de la Universidad de la Costa llevará a cabo la gestión necesaria para realizar el inventario de sus activos de información en seguridad digital, tanto físicos como lógicos, asegurando su disponibilidad, integridad y confidencialidad.

8.2.1 Generalidades

1. Los recursos tecnológicos son gestionados y clasificados según el uso final para el cual fue adquirido

2. Todos los recursos tecnológicos físicos deben ser inventariados y asignados a un funcionario, coordinación o área responsable, quien velará por su adecuado uso y cuidado.
3. Los recursos tecnológicos digitales sensibles, como bases de datos, software, aplicativos y plataformas críticas para la gestión de la información, deben ser incluidos en el inventario de activos de información digital.
4. Los miembros de la comunidad universitaria son responsables de utilizar adecuadamente los recursos tecnológicos y la información que manejan, cumpliendo con las políticas de seguridad de la información y evitando prácticas ilícitas que puedan afectar a otros funcionarios, colaboradores o terceros, así como infringir la legislación vigente.
5. Los colaboradores deben velar por el correcto funcionamiento de los recursos asignados y, en caso de fallos, deben solicitar soporte al departamento de tecnología, siguiendo los procedimientos establecidos y utilizando correctamente la aplicación AYUDATIC o los canales de comunicación institucional.
6. Todo miembro de la comunidad universitaria que disponga de un equipo tecnológico propiedad de la universidad debe devolverlo al finalizar su vínculo laboral o contractual, o en caso de cambio de cargo si es necesario. Esto incluye documentos institucionales, equipos de cómputo (hardware y software), dispositivos móviles, tarjetas de acceso, manuales, tarjetas de identificación y cualquier información almacenada en dispositivos móviles o removibles.
7. Los activos de información digital institucionales bajo custodia del departamento de tecnología deben gestionarse según los lineamientos establecidos por dicha dependencia.
8. El departamento de tecnología puede realizar monitoreo sobre los activos de información digital institucional sin identificar a usuarios específicos, cuando existan indicios de su vinculación con incidentes de seguridad.
9. En las áreas donde se encuentren equipos de procesamiento de información, está prohibido fumar, consumir bebidas o alimentos para garantizar la integridad y seguridad de los activos tecnológicos.

8.2.2 Política uso de los sistemas de información

1. El sistema de seguridad definido por el departamento de tecnología para los diferentes sistemas de información que apoyan la gestión de la Universidad de la Costa CUC está basado en la estructura de perfil – usuarios.
2. Los perfiles se establecen según las funciones de los colaboradores de cada una de las dependencias.
3. El desarrollo, mantenimiento, cambio y actualización de los sistemas de información institucionales son autorizados por el departamento de tecnología, tras la realización de las pruebas

pertinentes. Estas tareas las ejecutarán los líderes funcionales, dependiendo de su viabilidad, y se harán según el procedimiento establecido para elaborar, mantener software y procesamiento de datos.

4. Los usuarios no pueden realizar copias de los sistemas de información institucionales que se encuentren instalados en los equipos para su distribución.
5. Los usuarios no deberán modificar, revisar, transformar o adaptar, descompilar o realizar ingeniería inversa a cualquier software o sistema de información de propiedad de la Universidad.
6. Los usuarios no pueden realizar copias de la información que arrojan los sistemas de información institucionales para distribuirlas a otros funcionarios que no la requieren para el desarrollo de sus funciones, o a entes externos, sin previa autorización del responsable del activo de información. La distribución de esta información constituye una violación a las políticas de seguridad y privacidad de la información, especialmente de datos personales.
7. Los usuarios de los sistemas de información deberán informar al departamento de tecnología sobre cualquier sospecha de violación de las políticas de seguridad y privacidad, uso indebido y debilidades de seguridad sobre los sistemas de información institucionales.
8. El líder funcional de cada aplicación institucional bajo la custodia del departamento de tecnología es responsable de administrar el aplicativo o delegar dicha función, pero no la responsabilidad, en quien lo considere pertinente.

8.2.3 Política uso de software y licencias

1. Los usuarios deben usar solo software legal adquirido por el departamento de tecnología o bajo licenciamiento institucional, aceptando los términos y condiciones.
2. El departamento de tecnología gestiona la adquisición y renovación de licencias de software para uso general en la Universidad, controlando las instalaciones conforme a las adquisiciones.
3. Solo el Departamento de Tecnología pueden instalar, desinstalar, renovar o actualizar software adquirido legalmente.
4. Descargar, instalar o usar software no autorizado viola las políticas de seguridad y privacidad de la Universidad.
5. En caso de reclamación por software ilegal, la responsabilidad recaerá sobre el usuario responsable del dispositivo donde está instalado dicho software.
6. Todo miembro de la comunidad que se entere de cualquier uso indebido o no autorizado de software o la documentación vinculada a estos, deberá comunicarlo al Departamento de Tecnología

7. El software debe cumplir términos de licenciamiento del fabricante, incluyendo versiones de prueba.
8. Ante cualquier duda referente a los términos de licenciamiento o legalidad de un software, los funcionarios pueden consultar al Departamento de Tecnología.
9. El Departamento de Tecnología deberá desinstalar o desactivar las licencias que hayan caducado, ya sea porque finalizó el periodo de licenciamiento asignado y no fue solicitada su prorroga de uso o por cualquier otra situación que impida su instalación o uso.

8.2.4 Política protección y uso de las estaciones cliente de trabajo (software malicioso)

1. El funcionario aceptará los equipos de cómputo asignados y será el responsable de los equipos y accesorios entregados, de su cuidado y su buen uso. La aceptación se hará por medio del sistema de información que administra los activos de cómputo.
2. El departamento de tecnología habilita las estaciones de trabajo fijas y/o portátiles de los funcionarios dejándolas con el hardware y software básico configurado y requerido para operar según las licencias institucionales.
3. Estaciones de trabajo deben mantener configuraciones de seguridad instaladas por el Departamento de Tecnología, como sistema operativo, office, antivirus, y firewalls.
4. Los usuarios son responsables de asegurar que dispositivos de almacenamiento externo no contengan virus.
5. Usuarios no deben alterar configuraciones físicas o lógicas de las estaciones de trabajo; los cambios deben ser realizados por el Departamento de Tecnología.
6. La gestión de información almacenada en estaciones de trabajo debe seguir los lineamientos definidos en las Políticas de uso de Dispositivos.
7. Procedimientos de formateo o reinstalación de aplicaciones deben ser solicitados a través de la Mesa de soporte de Tecnología AYUDATIC.
8. Es responsabilidad del usuario o colaborador evitar siempre la fuga o pérdida de información de la institución almacenada en los equipos de cómputo personal asignados.
9. La información laboral, institucional o personal no debe ser almacenada en los computadores de áreas comunes como aulas, bibliotecas, salas de computadores y laboratorios.
10. Al reasignar, donar o sacar estaciones de trabajo de la universidad, se debe garantizar que no contengan información personal o institucional sensible, o eliminar esta información de manera que no pueda ser recuperada.
11. Para acceder a los equipos de la universidad se deberán habilitar las credenciales institucionales.

8.2.5 Política para administración de servidores y bases de datos.

1. La Universidad de la Costa dispone de una infraestructura de servidores para almacenar información crítica mediante bases de datos, sistemas de información y desarrollo de software, que apoyan los procesos internos y la misión institucional.
2. El departamento de tecnología, con sus líderes funcionales, administra el funcionamiento de los servidores y bases de datos e infraestructura considerados de misión crítica.
3. Los funcionarios responsables de administrar servidores, bases de datos o servicios instalados en ellos, son los primeros responsables en mantener, velar y mejorar su funcionamiento incluyendo la respectiva seguridad contra accesos malintencionado estableciendo lineamientos de configuración en los servicios o servidores.
4. Los administradores de base de datos del departamento de tecnología tendrán acceso único como "DBA" para cada base de datos institucional. Deben cumplir con las políticas de cambio de clave y asegurar las contraseñas en un lugar seguro.
5. Solo personal autorizado por el departamento de tecnología podrá instalar software o hardware en los servidores e infraestructura de telecomunicaciones sobre los cuales funcionan estos servidores.
6. Los administradores deben supervisar el funcionamiento de los servicios y detectar anomalías en servidores y bases de datos.
7. Los servidores y servicios de la institución deben seguir un plan de actualización regular (por ejemplo, mensual, trimestral, semestral u otro) para mantener actualizados los componentes de seguridad, como motores de detección, bases de datos, software de gestión en el lado cliente y servidor, entre otros.
8. Para los servidores que cuenten con sistemas operativos próximos a salir del periodo de soporte por parte del fabricante se les debe analizar la viabilidad de actualizarse a versiones más recientes.
9. Los administradores de servicios que soliciten aperturas de puertos a la administración de la red LAN institucional, están en la obligación de sustentar sus requerimientos para que a través de un análisis se establezca el nivel de Riesgo y de Impacto.
10. Los administradores de servidores bajo control directo del departamento de tecnología deben tener identificado los servicios publicados y puertos TCP/UDP en los servidores hacia la LAN y la WAN.
11. La información de los servidores principales es respaldada en medios digitales alternos administrados por el Departamento de Tecnología.

12. La información de los servidores principales es respaldada en medios digitales alternos administrados por el Departamento de tecnología y podrá ser recuperada en caso de un desastre o incidentes de seguridad.
13. Las acciones del DBA y/o administrador de servidores TT, o usuarios con permisos privilegiados deben ser revisadas y auditadas de forma ocasional.
14. Solo personal autorizado podrá realizar actividades de administración remota sobre los servidores, bases de datos o infraestructura de procesamiento de información sobre la cual funcionan estos activos, utilizando los medios definidos por el departamento de tecnología.
15. Los servidores deben estar conectados a una red de energía regulada.
16. Los servidores o subdominio bajo el dominio institucional cuc.edu.co deben contar con los lineamientos mencionados en esta política y el Departamento de Tecnología deberá responder por cualquier incidente de seguridad que se presente en sus servidores.

8.3 POLÍTICAS DE GESTIÓN DE MEDIOS DE ALMACENAMIENTO.

Los lineamientos de estas políticas tienen como objetivo principal proteger la información de la Universidad de la Costa CUC asegurando la confidencialidad, integridad y disponibilidad de los datos almacenados en unidades de almacenamiento.

8.3.1 Política para gestión y disposición de medios removibles

1. Antes de establecer los lineamientos de esta política, se aclara que la información puede almacenarse o transportarse en formatos digitales como USB, discos magnéticos, discos duros, tarjetas de memoria, cámaras fotográficas, cámaras de video, celulares, entre otros.
2. No hay restricción inicial para el uso de dispositivos removibles, pero los usuarios deben manejarlos de manera responsable para proteger la información universitaria y personal.
3. La información institucional en medios removibles debe recibir protección especial y ser almacenada de manera segura, siendo responsabilidad del colaborador informar al Departamento de Tecnología para garantizar su protección y uso adecuado.
4. Las dependencias deben cumplir con la Política Institucional de Tratamiento de Datos Personales al almacenar información personal en dispositivos removibles.
5. Los medios removibles conectados a la red institucional están sujetos a monitoreo por parte del Departamento de Tecnología.

6. Se debe realizar seguimiento a los medios removibles críticos para garantizar la transferencia oportuna de información antes de que se vuelvan inaccesibles.
7. Los funcionarios responsables de dispositivos de copias de seguridad deben supervisar todas las operaciones y asegurar la cadena de custodia durante los traslados fuera de la Universidad para prevenir fugas de información.

8.3.2 Política sobre almacenamiento

1. El uso de carpetas compartidas desde Microsoft OneDrive; será permitido siguiendo los lineamientos de almacenamientos dados por el Departamento de Tecnología.
2. Las grabaciones de reuniones y clases por medio Microsoft Teams serán sujetas a una política de retención de tiempo de un año.
3. La Universidad utiliza almacenamiento centralizado en la nube con productos comerciales, siguiendo licencias específicas y restricciones de información clasificada administrado por el Departamento de Tecnología.
4. Los administradores de servidores regulan los accesos según el rol del funcionario para garantizar la seguridad de los datos según el Procedimiento interno de Habilitación de Servicios Tecnológicos.
5. Las copias de respaldo de servicios críticos se almacenan internamente y de forma segura, bajo custodia del Departamento de Tecnología.
6. Solo personal autorizado puede acceder a la información capturada por los sistemas de videovigilancia y dicho ingreso se mantendrá protegido por llave y/o contraseña de acceso, que debe cambiar periódicamente.
7. El Departamento de Tecnología determinará el tiempo máximo de retención de las grabaciones, que podrán prolongarse durante investigaciones judiciales por incidentes graves como robos.

8.4 POLÍTICA USO DE SISTEMAS DE VIDEOVIGILANCIAS

Con el fin de implementar estrategias tecnológicas que apoyen la seguridad en la institución, la Universidad podrá hacer uso de sistemas de videovigilancia en distintos puntos geográficos del campus universitario, los cuales serán gestionados y avalados por el Departamento de Tecnología cuyo objetivo será siempre velar por la seguridad.

1. Las imágenes y videos grabados por medio de los sistemas de videovigilancia serán usados única y exclusivamente para el fin por el cual fueron capturadas y su custodia y tratamiento cumplirán con los requisitos establecidos en la política de tratamiento de datos institucionales.
2. Las cámaras de seguridad como todos los dispositivos tecnológicos deben ser monitoreados y salvaguardados de acciones que conlleven a su deterioro o alteren su buen funcionamiento. Para este caso, el Departamento de Tecnología se encargará de su administración y bien funcionamiento.
3. Cabe resaltar que la base de datos de grabaciones realizadas en las videocámaras de seguridad, tendrán una vigencia de almacenamiento de 15 días establecida por el departamento de tecnología de acuerdo con su infraestructura
4. El personal perteneciente al departamento de tecnología mantendrá bajo su cuidado y custodia las filmaciones que se realicen a través de las videocámaras de vigilancia instaladas en la Universidad de la Costa. En todo caso les asiste el deber contractual de manejar de forma confidencial y bajo reserva, los datos personales de quienes sean monitoreados.
5. Los datos personales relacionados con las imágenes de los titulares, y en general las grabaciones realizadas por las videocámaras instaladas, sólo se darán a conocer en virtud de una orden administrativa y judicial, con el fin de proteger a los demás titulares que son objeto de la video vigilancia.
6. La Dirección de Gestión Humana tendrá acceso a las videograbaciones que se encuentren almacenadas al momento de la solicitud al Departamento de Tecnología, cuando la filmación contenida en ellas sea necesaria para realizar control a las labores de los empleados de la organización, o en caso de ser requeridas para procesos disciplinarios internos.
7. Se encuentra prohibido el acceso al monitor de visualización de las videocámaras, y por ende a las grabaciones en ella contenidas a visitantes, docentes, estudiantes y funcionarios administrativos diferentes a los encargados o expresamente autorizados en esta Política, a menos que medie una orden judicial y administrativa en tal sentido.

8.5 POLÍTICA DE USO DE CORREO ELECTRÓNICO

8.5.1 Generalidades

1. La Universidad de la Costa CUC, considera el correo electrónico como un recurso de información disponible para los usuarios, diseñado como una herramienta colaborativa para respaldar las actividades misionales.

2. La Universidad, por medio de la presente política, regula el uso del correo electrónico y exige a las personas usuarias su uso correcto, de conformidad con las políticas vigentes.
3. El dominio @cuc.edu.co es el dominio de correo electrónico institucional oficial de los miembros de la comunidad universitaria de la Universidad de la Costa CUC.
4. La Universidad posee la propiedad de la información almacenada en los buzones de correo de las cuentas funcionales institucionales, por lo tanto, no se permite reenviarla a otros correos sin autorización expresa de las autoridades universitarias.
5. El servicio de correo electrónico no debe ser utilizado como repositorio para almacenamiento o respaldo de información o archivos, para ello tener presente que:

    a. La información en las cuentas personales institucionales debe ser gestionada adecuadamente por cada usuario, siguiendo los lineamientos de capacidad de almacenamiento institucional y realizando copias de respaldo de la información relevante.

6. La información contenida en las cuentas institucionales es de propiedad de la Universidad y debe conservarse.
7. Las credenciales de acceso al correo electrónico institucional son personales; por lo tanto, ninguna persona usuaria debe utilizar una cuenta de correo que no le haya sido asignada por la Universidad.
8. Quien emita un correo electrónico debe identificarse (nombre, apellido, dependencia y cargo) mediante la firma, cuyo formato ha establecido previamente la Universidad.
9. Los responsables de las diferentes dependencias deben administrar las cuentas de correo funcional de su área, asignándolas o reasignándolas a los empleados correspondientes. Asimismo, deben transferirlas a la persona de mayor jerarquía inmediata al concluir su gestión en el cargo.
10. El servicio de correo electrónico de la Universidad se presta a través de contrato con un proveedor reconocido en el mercado para este tipo de servicio.

8.5.2 Límites en el número de mensajes enviados por correo

1. Se deben cumplir estrictamente los límites establecidos para el número de mensajes que los usuarios pueden enviar en un periodo definido por la universidad, según los términos del servicio de correo contratado con el proveedor o plataforma correspondiente, para consultar el límite debe contactar al Departamento de Tecnología.

2. Los usuarios que requieran enviar correos electrónicos a gran escala (boletines informativos, convocatorias masivas, difusión de programas o eventos, entre otros) deben utilizar el software proporcionado por la institución (Microsoft), previa asesoría y aprobación del Departamento de Tecnología.
3. Los envíos masivos de correos electrónicos deberán regirse a la Política del Departamento de Comunicaciones.

8.5.3 Cuentas de correo funcional institucional

1. La Universidad asignará cuentas de correo funcional institucional en el dominio @cuc.edu.co a las dependencias que lo soliciten, las cuales serán administradas por el colaborador designado por el jefe o director de cada área.
2. Los nombres de las cuentas de correo funcional institucional y su contenido deben conservarse para mantener su recordación y la trazabilidad de la información, la cual es propiedad de la Universidad.
3. Toda dependencia académico-administrativa, grupo de investigación, curso de extensión u otro evento institucional debe usar la cuenta de correo funcional institucional asignada, si se requiere correo electrónico como medio de difusión. La Universidad no autoriza el uso de cuentas de correo fuera del dominio institucional para estos propósitos.
4. Las cuentas de correo electrónico funcional institucional no se consideran correspondencia privada, por lo que los correos electrónicos recibidos pueden ser revisados por la Universidad según sea necesario.

8.5.4 Cuentas de correo institucional

1. La Universidad asigna cuentas de correo @cuc.edu.co a la comunidad académica administrativa y estudiantil.
2. Las personas que cambien su vínculo contractual con la universidad mantendrán la misma cuenta de correo @cuc.edu.co previamente asignada para sus actividades institucionales, en caso de ser estudiantes o graduados.
3. Las cuentas de correo institucional son de correspondencia privada y deben ser utilizadas exclusivamente para fines institucionales.
4. Las cuentas de correo institucional de los usuarios que se desvinculen de la institución serán desactivadas. Se utilizará un correo personal externo para cualquier comunicación relacionada

con su desvinculación, solo serán activadas con autorización de Gestión Humana con búsqueda de información referente a su labor.

5. La Universidad de la Costa asigna cuentas de correo @cuc.edu.co por áreas siempre y cuando sea solicitado por el líder de esta para el desarrollo de sus labores, esta cuenta es asignada y es responsabilidad del usuario a quien el líder designe.
6. Cada cuenta de correo institucional debe tener la firma y el aviso de confidencialidad de acuerdo con la información estipulada por el Departamento de Comunicaciones.

8.5.5 Responsabilidades de los usuarios

1. Cumplir con las políticas establecidas para el uso del correo institucional.
2. Utilizar el correo asignado exclusivamente para fines institucionales, evitando afectaciones al clima organizacional o reputaciones externas.
3. Emplear la cuenta funcional asignada solo para actividades relacionadas con sus responsabilidades institucionales, entregándola de acuerdo con el proceso de entrega de cargo de Gestión Humana.
4. Gestionar y transferir las cuentas de correo de la dependencia responsablemente al cambiar de rol o cargo.
5. Responsabilizarse por todas las acciones realizadas con las cuentas asignadas.
6. Informar a el Departamento de Tecnología sobre cualquier actividad sospechosa que pueda comprometer la seguridad de la cuenta a través de la mesa de Ayuda AYUDATIC o por los canales de comunicación estipulados.
7. Es obligación que todas las cuentas de correo institucionales tengan activo el doble factor de autenticación (Microsoft Authenticator)
8. Tener precaución al abrir correos sospechosos o de dominios desconocidos.
9. Mantener y proteger la confidencialidad de la contraseña del correo institucional la cual es personal e intransferible.

8.5.6 Uso indebido del correo electrónico

1. No compartir la cuenta de correo institucional con terceros.
2. No enviar mensajes no relacionados con las labores institucionales.
3. No redirigir la cuenta institucional a otras cuentas, internas o externas.

4. No vincular la cuenta institucional con perfiles personales en redes sociales.
5. No enviar contenido ilegal como apología del terrorismo, pornografía, amenazas o virus.
6. No comprometer la reputación de la institución o de sus miembros mediante el correo institucional.
7. No falsificar encabezados de correos electrónicos ni usar dominios inválidos para enviar correo.
8. No suplantar la identidad de otra persona en el correo institucional.

8.5.7 Responsabilidades de la universidad

1. La Universidad ofrece servicio de correo electrónico a través de proveedores externos, pero no puede garantizar su disponibilidad por posibles fallas de software, problemas de conexión a Internet u otras imprevisibles. Por ello, no asume responsabilidad por pérdidas de datos derivadas de estas eventualidades.
2. La Universidad no se responsabiliza del uso que las personas usuarias hagan de sus cuentas de correo institucional (personal o funcional).
3. Cada usuario es responsable de realizar y mantener copias de respaldo de la información contenida en sus buzones y carpetas de correo institucional (personal o funcional), ya que esta responsabilidad no recae en Departamento de Tecnología.
4. En caso de eliminación accidental de correos o carpetas por parte de los usuarios, el Departamento de Tecnología no garantiza la reposición de dichos elementos.

8.5.8 Manejo de casos excepcionales

1. Las cuentas de correo institucional pueden ser intervenidas por la Universidad según sea necesario.
2. La Universidad puede acceder a las cuentas de correo institucional asignadas a los funcionarios, si es requerido.
3. La Universidad conservará las cuentas de correo institucional de los funcionarios desvinculados por un máximo de cinco años La autorización para habilitar el acceso a la información en los correos de excolaboradores de la CUC debe ser otorgada por Gestión Humana.
4. En casos de incapacidad temporal o permanente de colaboradores, la Universidad podrá acceder a sus cuentas de correo institucional.

5. Las cuentas de correo de colaboradores fallecidos serán inhabilitadas y el contenido almacenado se conservará por hasta cinco años antes de ser eliminado por la Universidad.
6. La Universidad informará a los usuarios si se ve obligada a suspender el servicio de correo electrónico prestado por un tercero, sin asumir responsabilidad por la información almacenada en las cuentas afectadas.

8.6 POLÍTICA DE ADMINISTRACIÓN Y GESTIÓN DE LA SEGURIDAD DE LA RED INSTITUCIONAL

La Universidad de la Costa cuenta con una infraestructura de red de datos LAN que comprende todo el cableado, switches, fibra, routers, antenas y sistemas inalámbricos que permiten realizar la conexión entre estos dispositivos, los equipos servidores y los usuarios, cuya administración debe regirse por las siguientes políticas, en cualquiera de las sedes que hacen parte de la universidad.

8.6.1 Controles de Red

Para gestionar y controlar la red institucional, el Departamento de Tecnología deberá:

1. Establecer controles especiales para proteger los sistemas de información y la disponibilidad de los servicios y dispositivos de red
2. Establecer mecanismos para el monitoreo de acciones y registro de la autenticación de inicio de sesión, sobre servicios de red o tecnológicos que se consideren relevantes para la seguridad de la información. Por ejemplo: WIFI, sistemas de información.
3. Establecer y dar a conocer los mecanismos de control acceso de los usuarios cuando estos requieran acceder a servicios institucionales desde redes públicas o inalámbricas con el fin de salvaguardar la protección de los datos, tal como VPN entre otros.
4. Implementar los mecanismos informáticos para proteger de forma segura el tráfico de los paquetes de información que se transmiten sobre la red de datos contra ataque informático, introducción o propagación de software malicioso, interceptación, copiado, modificación, enrutado y destrucción
5. Aplicar restricción a las conexiones de red para que los accesos se realicen según los privilegios asignados.
6. establecer los estándares técnicos de configuración de los dispositivos de seguridad y de red, acogiendo buenas prácticas de configuración segura.

7. Implementar firewall o dispositivos de seguridad perimetral para la conexión a internet
8. Considerar y tratar como información confidencial, la información institucional relacionada con las topologías, configuraciones, direccionamiento, enrutamiento, diseños de sistemas de comunicación y de cómputo

8.6.2 Seguridad de los servicios de red

La Universidad de la Costa, a través del Departamento de Tecnología, definirá la tecnología y el conjunto de controles lógicos y físicos a aplicar para garantizar la seguridad sobre los diferentes recursos y servicios informáticos (autenticación, encriptación y controles de conexión de red), con el fin de asegurar el buen uso de estos y mantener los niveles de seguridad establecidos de acuerdo con la disponibilidad de recursos presupuestales. Para ello:

1. El Departamento de Tecnología independientemente de si los servicios de red son internos o externos, asegurara la calidad del servicio mediante acuerdos de Niveles de Servicio o SLA.
2. El Departamento de Tecnología realizará monitoreo sobre el tráfico de la red, auditando la disponibilidad de la red y evaluando los riesgos a los que pueda estar expuesto dicho servicio y los que se ofrecen por medio de él.
3. El Departamento de Tecnología establecerá las responsabilidades y procedimientos para la gestión de las comunicaciones que se realizan sobre la infraestructura de la red de datos, a los cuales se acogerán los usuarios de los servicios de red de todas las dependencias.
4. El Departamento de Tecnología definirá las situaciones y los procedimientos a aplicar para restringir el acceso a los servicios o aplicaciones de red, cuando sea necesario.
5. Las dependencias que requieran desplegar servicios sobre la red deberán identificar, habilitar y justificar ante el Departamento de Tecnología la necesidad de los servicios, protocolos y puertos que requieran, y acatarán los lineamientos de seguridad establecidos por la universidad.

8.6.3 Separación en redes

1. El Departamento de Tecnología establecerá un esquema de segmentación de las redes con el fin de controlar el acceso a los diferentes segmentos de red de acuerdo con los dominios, grupos de servicios, roles y ubicación del personal. El tráfico entre estos segmentos de red estará controlado mediante dispositivos de red que permitan una autorización a un nivel de detalle específico (Dirección IP, puerto, entre otros).

2. El Departamento de Tecnología separará las redes inalámbricas de las redes internas para garantizar los principios de la seguridad de la información.

8.6.4 Uso aceptable del servicio

1. La red LAN institucional permite a la comunidad universitaria el acceso rápido y eficiente a todos sus servicios, tales como correo electrónico, navegación web y uso de aplicaciones informáticas de misión crítica mediante conectividad alámbrica o inalámbrica.
2. Toda modificación, ampliación o remodelación de cualquier segmento de cableado estructurado en la red LAN institucional que requieran realizar, debe contar con la supervisión y aprobación del Departamento de Tecnología.
3. El usuario que se conecte a la red de datos institucional ya sea a la inalámbrica o a la LAN, es el directo responsable de proteger y velar por la seguridad de la información que exponga a través de esta.
4. La conexión de cualquier nuevo dispositivo a la red LAN institucional, incluyendo equipos servidores, computadores, cámaras, teléfonos IP, equipos inalámbricos, entre otros, deberá contar con la supervisión y aprobación del Departamento de Tecnología.
5. Todo usuario de la red LAN institucional debe informar al Departamento de Tecnología, por los canales establecidos de comunicación en la mayor brevedad posible, cualquier anomalía que detecte en el funcionamiento de la red, con el fin de que el Departamento de Tecnología pueda proceder con las acciones correctivas.
6. Para mantener la integridad operacional de la red LAN institucional, el Departamento de Tecnología bloqueará o deshabilitará cualquier equipo o dirección IP que haya sido conectado o asignada sin su aprobación.
7. La conexión remota a la red LAN se permitirá y deberá ser realizada a través de una conexión VPN segura suministrada, autorizada, registrada y auditada por el Departamento de Tecnología.
8. 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 el desarrollo de las funciones institucionales autorizadas.

8.6.5 Uso indebido de la Red

El Departamento de Tecnología procederá a desconectar o desactivar de la red LAN institucional la fuente (equipo o cuenta de usuario) donde se origine cualquiera de las siguientes situaciones de uso indebido, e informará a los entes de control interno de la Universidad. Se considera uso indebido del servicio de la red LAN de la universidad:

1. Utilizar la infraestructura de tecnología de información y redes de la Universidad para conseguir o transmitir material con ánimo de lucro, excepto cuando se trate de fines institucionales. Igualmente, no se permite su utilización para realizar actividades que impliquen acoso, difamación, calumnia o cualquier forma de actividad hostil o delictiva en contra de miembros de la comunidad universitaria o de cualquier persona o institución.
2. Ejecutar cualquier herramienta o mecanismo de monitoreo de la red sin la debida autorización del Departamento de Tecnología.
3. Intentar burlar los mecanismos de seguridad, autenticación, autorización o de auditoría de cualquier servicio de red, aplicación, servidor o cuenta de usuario.
4. Desconectar o manipular los elementos de red tales como switches, enrutadores, antenas, y demás elementos pertenecientes a la infraestructura de red LAN institucional sin la debida autorización por parte del Departamento de Tecnología.
5. Modificar la configuración de red establecida para los equipos de cómputo y de red, en cualquier dependencia de la universidad sin la debida autorización por parte del Departamento de Tecnología.
6. Ingresar a los centros de cableado de la red LAN institucional sin la autorización del Departamento de Tecnología.
7. El Departamento de Tecnología se reserva el derecho de filtrar los contenidos que se reciban desde Internet y/o se envíen desde la red de datos institucional.
8. Transmitir información ilegal, abusiva, que ocasione responsabilidad civil o de cualquier otra índole, revele material protegido por secreto comercial o que afecte la reputación institucional, de acuerdo con la legislación vigente y el reglamento de propiedad intelectual de la Universidad.
9. Se prohíbe el monitoreo no autorizado de datos o tráfico de la red inalámbrica y cableada de la Universidad.
10. Se prohíbe el uso de la red institucional con el fin de probar, explorar o verificar vulnerabilidades, o transgredir las medidas de seguridad informática y autenticación, o demás actos abusivos que estén estipulados por la ley.
11. Se prohíben las transferencias de grandes volúmenes de datos, especialmente si se producen de forma continua.

8.7 POLÍTICA DE USO DE INTERNET

La Universidad de la Costa, consciente de la importancia del uso de Internet como una herramienta para el desarrollo de sus actividades misionales y de apoyo, proporciona los recursos necesarios para asegurar la disponibilidad del servicio de internet a los usuarios que lo requieran para el desarrollo de sus actividades diarias en la universidad. Para ello, establece lo siguiente**:**

8.7.1 Uso aceptable del servicio

1. El servicio de Internet institucional solo se ofrece por medio de la infraestructura de hardware y software de la red local institucional gestionada por el Departamento de Tecnología.
2. El servicio de Internet institucional se debe emplear como una herramienta para investigación, desarrollo, consulta y comunicación de actividades relacionadas con los procesos misionales y de apoyo de la Universidad de la Costa.
2. El servicio de Internet de la universidad puede ser utilizado con fines didácticos, permitiéndole a los usuarios tomar cursos de capacitación en línea en temas que enriquezcan su labor dentro de la institución.
3. Este recurso podrá ser utilizado para uso personal, siempre y cuando se realice de manera ética, razonable, responsable, no abusiva y sin afectar la productividad ni la protección de la información de la universidad.
4. Al utilizar el servicio de Internet de la universidad, se espera que el usuario (estudiante, docente, administrativo o contratista) use los servicios con respeto, cortesía y responsabilidad, procurando no vulnerar los derechos de los demás usuarios de este servicio y realizando una gestión adecuada para la protección de la información que puede circular por medio de este.
5. El acceso a determinadas páginas de Internet puede ser bloqueado para usuarios individuales, grupos de usuarios o para todos los empleados, servidores o colaboradores de la institución, dependiendo del monitoreo y análisis de navegabilidad aplicado a las mismas por parte del Departamento de Tecnología.
6. El personal externo al cual la universidad le permita el acceso a internet se acoge a los lineamientos de conectividad de la red y acepta las responsabilidades en las que incurre por ser usuario de esta y del servicio de internet.
7. Considerar como no confiable la información recibida a través de sitios web no verificados, ya que dicha información puede ser utilizada con fines comerciales o delictivos.

8. Todas las comunicaciones enviadas o recibidas mediante este servicio pueden ser revisadas y/o monitoreadas por el administrador del servicio o cualquier instancia de vigilancia y control de la universidad.

8.7.2 Uso Indebido de Internet

Se considera uso indebido del servicio de internet de la Universidad:

1. Ingresar a páginas web cuyo contenido o autoría sea objetable o ilegal
2. Acceder a contenidos de sitios web pornográficos, de grupos alzados en armas, de grupos terroristas o de sitios dedicados a difundir temas relacionados con violencia de cualquier tipo, al igual que promover o difundir a nombre de la universidad dichos contenidos.
3. Utilizar el canal de conexión a Internet para descargar e instalar contenido digital (música, videos, archivos ejecutables, entre otros) que infrinja derechos de autor o cualquier tipo de software no licenciado por la Universidad.
4. Hacer uso del servicio de Internet de la Universidad para participar de cualquier actividad ilegal o que atente contra el ordenamiento jurídico vigente.
5. Acceder a páginas relacionadas con anonimizadores, actividades relacionadas con crímenes computacionales, hacking, discriminación, contenido malicioso, suplantación de identidad, spyware, adware, redes peer to peer (p2p), o páginas catalogadas como de alto riesgo dictaminado desde la herramienta de administración y monitoreo de navegabilidad.
6. Enviar y/o descargar información masiva de gran tamaño que pueda congestionar la red y que no corresponde para el desarrollo de las actividades institucionales.
7. Cualquier otro propósito diferente al considerado en el apartado de Usos aceptables del servicio de la presente política
8. En caso de que el Departamento de Tecnología detecte la realización de alguno de estos procedimientos no permitidos, procederá a informar a los entes de control interno de la Universidad.

8.8 POLÍTICA SOBRE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

8.8.1 Desarrollo Seguro

El Departamento de Tecnología implementa políticas para el desarrollo de software y sistemas seguros en los proyectos a su cargo, incluyendo:

1. Definir la seguridad del entorno de desarrollo.
2. Enfocar la seguridad en el ciclo de vida del desarrollo de software mediante:
   a. Integración de la seguridad en la metodología de desarrollo de software.
   b. Establecimiento de directrices de codificación segura para cada lenguaje de programación utilizado.
3. Gestionar las distintas versiones de software.
4. Establecer el conocimiento necesario sobre la seguridad de las aplicaciones.

5. Gestionar las vulnerabilidades en el desarrollo: prevenir, identificar y resolver vulnerabilidades.

6. Garantizar que todo el software desarrollado internamente cuente con el nivel de soporte necesario.

7. Definir la separación de los entornos de desarrollo, pruebas y producción.

8. Obtener la aprobación de los propietarios de los sistemas de información para el desarrollo de nuevos sistemas o la implementación de cambios o nuevas funcionalidades en los sistemas existentes.

9. Almacenar copias de seguridad del código fuente de manera segura, previendo riesgos asociados a la pérdida de disponibilidad, confidencialidad o integridad.

11. Verificar que los sistemas de información adquiridos o desarrollados por terceros cuenten con un acuerdo de licenciamiento que especifique las condiciones de uso del software y los derechos de propiedad intelectual.

8.8.2 Control de Cambios de los Sistemas de Información

Cualquier cambio solicitado sobre los sistemas de información a cargo del Departamento de Tecnología seguirá los lineamientos establecidos en el Procedimiento para el Mantenimiento y Actualización de Sistemas de Información. Durante el procedimiento de cambios, los desarrolladores realizarán las siguientes acciones:

1. Asegurar que los cambios se presenten a los administradores del proceso.
2. Revisar los controles y procedimientos de integridad para asegurar que no se vean comprometidos por los cambios.
3. Identificar y notificar los softwares, información, entidades de bases de datos y hardware que requieran corrección.
4. Identificar y verificar vulnerabilidades en los softwares para minimizar la posibilidad de debilidades de seguridad conocidas.
5. Obtener aprobación formal de los administradores del proceso para propuestas detalladas antes de que el trabajo comience.
6. Asegurar que los administradores del proceso acepten los cambios antes de la implementación.
7. Mantener la documentación que soporte la trazabilidad de los cambios implementados, de acuerdo con las tablas de retención documental.
8. Mantener un control de versiones para todas las actualizaciones de software.
9. Mantener un registro de auditoría de todas las solicitudes de cambio.

8.8.3 Restricciones a los Cambios en los Paquetes de Software

El Departamento de Tecnología limitará los cambios en los paquetes de software a su cargo, como medida de buena práctica para reducir la posibilidad de generar incidentes. Evitará aplicar cambios innecesarios y llevará a cabo aquellos considerados necesarios, revisando los siguientes criterios antes de la planificación o implementación de los cambios:

1. Definir el riesgo de comprometer los procesos de integridad del software comparándolos con los beneficios de la actualización a realizar.
2. Obtener la aprobación del propietario del software.
3. Evaluar el impacto en los usuarios finales al realizar cambios de versiones de las librerías en los softwares.
4. Establecer la compatibilidad con otro software en uso.

8.8.4 Pruebas de Seguridad y Aceptación del Sistema

Durante los desarrollos a cargo del Departamento de Tecnología, se llevarán a cabo:

1. Pruebas de funcionalidad en los sistemas antes de pasar a producción.
2. Verificación de que los procesos de detección de incidentes sean probados periódicamente.
3. Revisión de las pruebas y criterios de aceptación establecidos previamente para los sistemas de información nuevos, actualizaciones y nuevas versiones.

Artículo 2. El presente acuerdo rige a partir de la fecha de su aprobación.

Dado en Barranquilla, a los treinta y un (31) días del mes de julio de dos mil veinticuatro (2024).

COMUNÍQUESE PUBLIQUESE Y CUMPLASE

Como constancia de lo anterior firman su Presidente y Secretario,

MARIO MAURY ARDILA
Presidente

FEDERICO BORNACELLI VARGAS
Secretario General