POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

UNIVERSIDAD TECNOLÓGICA DEL CHOCÓ
DIEGO LUIS CÓRDOBA

2022

TABLA DE CONTENIDO

INTRODUCCIÓN

La Universidad Tecnológica del Chocó Diego Luis Córdoba - UTCH, reconoce la importancia de la información que gestiona, debido a que es uno de los activos más significativos para su funcionamiento y que ésta puede ser de naturaleza legal, estratégica, financiera, operativa y en muchos casos corresponder a datos personales de servidores públicos, contratistas y partes interesadas.

De igual manera, es consciente de las amenazas que enfrenta la información y de las consecuencias a las que se expone nuestra institución cuando no cuente con las medidas de seguridad y protección adecuadas. En ese sentido, se debe tener una visión general de los riesgos de seguridad digital que pueden afectar la seguridad y privacidad de la información, donde se podrán establecer controles y medidas efectivos, viables y transversales con el propósito de realizar el aseguramiento de la disponibilidad, integridad y confidencialidad tanto de la información de la institución como de los datos de los servidores públicos, contratistas y partes interesadas.

Es indispensable que la Universidad realice una adecuada identificación, clasificación, valoración, gestión y tratamiento de los riegos de seguridad digital que puedan afectar la información de la entidad, con el propósito de implementar medidas y controles efectivos que permitan estar preparados ante situaciones en las que se vea comprometida tanto la seguridad física y lógica de sus instalaciones, personas, recursos y sistemas, como la seguridad de su información.

Teniendo en cuenta lo anterior, el presente Documento tiene como finalidad de establecer los principios orientadores en seguridad que buscan garantizar la disponibilidad, integridad, confidencialidad, privacidad, continuidad, autenticidad y no repudio de la información de la Universidad Tecnológica del Chocó , así como dar lineamientos para la aplicación de mecanismos que eviten la vulneración de la seguridad y privacidad de la información, orientados a la mejora continua y al alto desempeño del Sistema de Gestión de Seguridad de la Información – SGSI, que soporta el Modelo MSPI.

1. OBJETIVO GENERAL

Desarrollar e implementar el Modelo de Privacidad y Seguridad de la Información en la Universidad Tecnológica del Chocó Diego Luis Córdoba, acorde con los lineamientos establecidos por la Universidad, con la finalidad de preservar la confidencialidad, integridad y disponibilidad de la información.

2. ALCANCE

Los parámetros contenidos en el presente documento son aplicables para todos los aspectos administrativos y de control que deben ser cumplidos por el personal administrativo, docentes, estudiantes, visitantes y terceras partes que presten sus servicios o tengan algún tipo de relación con la Universidad Tecnológica del Chocó Diego Luis Cordoba a través de la recolección, procesamiento, almacenamiento, recuperación, intercambio y consulta de información, con personal interno o externo, en el desarrollo de la misión institucional y el cumplimiento de sus objetivos estratégicos.

3. DEFINICIONES

3.1. Activo: Se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas) que tienen un valor para la entidad.

3.2. Activo crítico: Son aquellos recursos, infraestructuras y sistemas que son esenciales e imprescindibles para mantener y desarrollar las capacidades institucionales, o que están destinados a cumplir dicho fin, y, cuya afectación, perturbación o destrucción no permite soluciones alternativas inmediatas, generando grave perjuicio a la Universidad Tecnológica del Chocó.

3.3. Administración de Riesgos: Es una función de la organización que Implica alinear estrategias, procesos, personas, tecnologías y conocimiento para manejar la incertidumbre que toda empresa enfrenta. No se refiere solamente al riesgo de contingencias, sino a los peligros inherente a toda actividad institucional.

3.4. Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la entidad.

3.5. Análisis de Impacto al Negocio (BIA-Business Impact **Analysis**)**:** es una etapa que permite identificar la urgencia de recuperación de cada procedimiento, los recursos y sistemas críticos para estimar el tiempo que la Universidad tecnológica del Chocó puede tolerar en caso de un incidente o desastre, permite identificar con claridad los procesos misionales de cada entidad y analizar el nivel de impacto con relación a la gestión del negocio.

3.6. Autenticidad: La autenticidad se refiere a que la información provenga de una fuente fidedigna, es decir, que el origen sea realmente quien envía la información.

3.7. Alta Dirección: Se refiere a la profesionalización de la gestión de las organizaciones para desempeñar exitosamente funciones directivas valiéndose de un razonamiento lógico y fundamentado para la toma de decisiones de alto impacto en la organización.

3.8. Centro de cableado: Es un sistema colectivo compuesto de cables, canalizaciones, etiquetas, espacios, conectores y otros dispositivos que deben ser instalados para establecer una infraestructura de telecomunicaciones genérica en un edificio, como (Switch, patch, panel, UPS, Router, Cableado de voz y de datos, etc).

3.9. Cifrado: es la conversión de datos de un formato legible a un formato codificado. Los datos cifrados solo se pueden leer o procesar luego de descifrarlos, este es la base principal de la seguridad de datos.

3.10. Control: Son todas aquellas políticas y procedimientos que se han establecido para proteger los datos personales almacenados en la organización y salvaguardarlos contra incidentes de seguridad y violaciones de datos.

3.11. Confiabilidad de la Información: se refiere a que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

3.12. Confidencialidad: se entiende en el ámbito de la seguridad informática, como la protección de datos y de información intercambiada entre un emisor y uno o más destinatarios frente a terceros y que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.

3.13. Código malicioso: El código malicioso es un tipo de código informático o script web dañino diseñado para crear vulnerabilidades en el sistema que permiten la generación de puertas traseras, brechas de seguridad, robo de información y datos, así como otros perjuicios potenciales en archivos y sistemas informáticos.

3.14. Dato personal: Las distintas informaciones, que recopiladas pueden llevar a la identificación de una determinada persona, también constituyen datos de carácter personal. Su finalidad es el “dato personal” como una información relacionada con una persona natural (persona individualmente considerada).

3.15. Dato personal público: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables, Son

considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público.

3.16. Dato personal privado: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular de la información.

3.17. Dato semiprivado: Aquel que no tiene naturaleza íntima, reservada ni pública y cuyo conocimiento o divulgación puede interesar no solo a su titular, sino a cierto sector o grupo de personas o a la sociedad en general.

3.18. Datos sensibles: Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así́ como los datos relativos a la salud, a la vida sexual, y los datos biométricos.

3.19. Datacenter: Se denomina también Centro de Procesamiento de Datos (CPD) a aquella ubicación o espacio donde se concentran los recursos necesarios (TI) para el procesamiento de la información de una organización.

3.20. Disponibilidad: Se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

3.21. Dispositivos móviles: Equipo celular smartphone, equipos portátiles, tablets, o cualquiera cuyo concepto principal sea la movilidad, el cual permite almacenamiento limitado, acceso a internet y cuenta con capacidad de procesamiento.

3.22. Evento: Es el suceso identificado en un sistema, servicio o estado de la red que indica una posible brecha en la política de seguridad de la información o fallo de las salvaguardas, o una situación anterior desconocida que podría ser relevante para la seguridad.

3.23. Evento de seguridad de la información: Presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o falla de salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.

3.24. Incidente de Seguridad: Evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen probabilidad significativa a comprometer las operaciones del negocio y amenazar la seguridad de la información.

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

3.26. Integridad: Se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.

3.27. Impacto: Resultado de un incidente de seguridad de la información.

3.28. Legalidad: Referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeta la entidad.

3.29. No repudio: Es la capacidad de demostrar o probar la participación de las partes (origen y destino, emisor y receptor, remitente y destinatario), mediante su identificación, en una comunicación o en la realización de una determinada acción.

3.30. Partes interesadas: Persona u organización que puede afectar o ser afectada o percibirse a sí misma como afectada por una decisión o actividad.

3.40. Plan de Continuidad de Negocio: Actividades documentadas que guían a la Entidad en la respuesta, recuperación, reanudación y restauración de las operaciones a los niveles predefinidos después de un incidente que afecte la continuidad de las operaciones.

3.41. Privacidad de la información: Es cuando una organización o individuo debe determinar qué datos en un sistema informático se pueden compartir con terceros.

3.42. Propietario de la información (titular): es la persona responsable de la integridad, confidencialidad y disponibilidad de una cierta información.

3.43. Riesgo: Se define como la combinación de la probabilidad de que se produzca un evento y sus consecuencias negativas.

3.44. Sistema de Información: que interactúan entre sí para apoyar un área o proceso de la Universidad Tecnológica del Chocó.

3.45. Terceros: Personas naturales o jurídicas que tienen un contrato tercerizado y prestan un servicio a la entidad y hacen uso de la información y los medios tecnológicos dispuestos por la entidad.

3.46. Vulnerabilidad: es un fallo o debilidad de un sistema de información que pone en riesgo la seguridad de la misma. Se trata de un “agujero” que puede ser producido por un error de configuración, una carencia de procedimientos o un fallo de diseño.

4. MARCO LEGAL

- Constitución Política de Colombia. Artículo 15.

- **Ley 44 de 1993:** Por la cual se modifica y adiciona la Ley 23 de 1982 y se modifica la Ley 29 de 1944 y Decisión Andina 351 de 2015 (Derechos de autor).

- **Ley 527 de 1999:** Por la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen las entidades de certificación y se dictan otras disposiciones.

- **Ley 594 de 2000**: Por medio de la cual se expide la Ley General de Archivos.

- **Ley 850 de 2003:** Por medio de la cual se reglamentan las veedurías ciudadanas.

- **Ley 1266 de 2008**: Por la cual se dictan las disposiciones generales del Habeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

- **Ley 1273 de 2009:** Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

- **Ley 1341 de 2009:** Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones – TIC, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones.

- **Ley 1474 de 2011:** Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.

- **Ley 1581 de 2012:** Por la cual se dictan disposiciones generales para la protección de datos personales.

- **Ley 1712 de 2014:** Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.

- **Ley 1915 de 2018:** Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.

- **Resolución 512 de 2019:** Por la cual se adopta la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de los servicios del Ministerio/Fondo de Tecnologías de la Información y las Comunicaciones y se definen lineamientos frente al uso y manejo de la información.

- **CONPES 3701 de 2011.** Lineamientos de Política para Ciberseguridad y Ciberdefensa.

- **CONPES 3854 de 2016.** Política Nacional de Seguridad digital.

5. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL

La dirección de La Universidad Tecnológica del Chocó Diego Luis Córdoba, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

Para La Universidad Tecnológica del Chocó Diego Luis Córdoba, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados.

De acuerdo con lo anterior, esta política aplica a nuestra institución según como se defina en el alcance, sus funcionarios, terceros, aprendices, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI estarán determinadas por las siguientes premisas:

1. Minimizar el riesgo en las funciones más importantes de la entidad.
2. Cumplir con los principios de seguridad de la información.
3. Cumplir con los principios de la función administrativa.
4. Mantener la confianza de sus clientes, socios y empleados.
5. Apoyar la innovación tecnológica.
6. Proteger los activos tecnológicos.
7. Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
8. Promover, Fortalecer y mantener la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de La Universidad Tecnológica del Chocó.
9. Garantizar la continuidad de los procesos frente a incidentes.

10. La Universidad Tecnológica del Chocó ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades de los diferentes procesos, y a los requerimientos regulatorios.

5.1 POLÍTICAS ESPECÍFICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

5.1.1. POLÍTICA DE ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

ORGANIZACIÓN INTERNA

a) Se deben definir y asignar todas las responsabilidades de la seguridad de la información.
b) Los deberes y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la Universidad Tecnológica del Chocó.
c) Se deben mantener contactos apropiados con las autoridades pertinentes por parte de la oficina de Sistemas y Soporte Técnico y documentar los contactos con autoridades (Policía, bomberos, COLCERT etc.) u otros especializados, con el fin de contactar en caso de que se presente un incidente de seguridad de la información y requiera de asesoría externa.
d) La Universidad Tecnológica del Chocó a través de la oficina de Sistemas y Soporte Técnico y demás personal que se determine, debe mantener contacto con grupos de interés especializados en seguridad y privacidad de la información, con el fin de compartir e intercambiar conocimientos, que permita la mejora continua del Sistema de Gestión de Seguridad de la Información de la misma.
e) La seguridad de la información se debe tratar en la gestión de proyectos, independientemente del tipo de proyecto, lo cual incluye una identificación de los riesgos y la definición de la forma como serán gestionados.

DISPOSITIVOS MOVILES

a) La Universidad Tecnológica del Chocó se reserva el derecho de autorizar o denegar el acceso al servicio de acuerdo con las condiciones de seguridad que se detecten en el dispositivo.

b) La Oficina de Sistemas y Soporte Técnico, debe mantener un inventario actualizado de los dispositivos móviles autorizados
c) Los dispositivos móviles de propiedad de los de Servidores Públicos, contratistas, o terceros no deben estar incluidos en el dominio utch.edu.co o cualquiera que funcione dentro de la institución, para conectarse a los servicios de la red de datos deberán realizar solicitud a la Oficina de Sistemas y Soporte Técnico y cumplir con los lineamientos referentes a seguridad de la información.
d) Todos los dispositivos móviles que almacenen información de La Universidad Tecnológica del Chocó deben tener instalado un software antivirus, y sistema operativo actualizado.
e) En dispositivos móviles entregados por La Universidad Tecnológica del Chocó, los Servidores Públicos no están autorizados a cambiar la configuración, a desinstalar software, formatear o restaurar de fábrica.
f) En caso de pérdida o robo de un dispositivo móvil de propiedad de La Universidad Tecnológica del Chocó, los Servidores Públicos, tendrá que realizar la respectiva denuncia ante la entidad competente, luego debe dar aviso inmediato al personal de la Oficina de Sistemas y Soporte Técnico, quienes deben realizar las acciones necesarias para la protección de la información.

TELETRABAJO – TRABAJO EN CASA

a) La Oficina de Sistemas y Soporte Técnico debe establecer los requerimientos para autorizar conexiones remotas a la infraestructura tecnológica necesaria para la ejecución de las funciones de la comunidad Universitaria, garantizando las herramientas y controles para proteger la confidencialidad, integridad y disponibilidad de las conexiones remotas.
b) Toda información gestionada por La Universidad Tecnológica del Chocó, y que sea accedida remotamente debe ser utilizada solamente para el cumplimiento de las funciones del cargo o de las obligaciones contractuales.

5.1.2. POLITICA DE SEGURIDAD DE LOS RECURSOS HUMANOS

ANTES DE ASUMIR EL EMPLEO

a) Dirección de Talento Humano, debe contar con procedimientos para la vinculación de personal, de acuerdo con la normatividad establecida para tal fin.

b) La oficina de contratación debe definir una lista de verificación que contenga los aspectos necesarios para la revisión de los antecedentes del personal a contratar por prestación de servicios de acuerdo con la normatividad vigente.
c) Dirección de Talento Humano y la oficina de contratación, deben establecer mecanismos o controles necesarios para proteger la confidencialidad y reserva de la información contenida en las historias laborales y expedientes contractuales.
d) Todo funcionario o contratista, debe firmar un documento o cláusulas en las que se establezcan acuerdo de confidencialidad y no divulgación de la información reservada de la Universidad Tecnológica del Chocó, estos deben reposar en la historia laboral o expediente contractual según sea el caso.

DURANTE LA EJECUCIÓN DEL EMPLEO

a) Los Docentes, Estudiantes, Administrativos, contratista o personal provisto por terceros, deben suscribir la autorización para el tratamiento de los datos personales de acuerdo con la Política de tratamiento de datos personales de la Universidad Tecnológica del Chocó y de acuerdo con lo establecido en la Ley 1581 de 2012 y sus decretos reglamentarios.
b) Una vez formalizado el proceso de vinculación, el jefe inmediato, supervisor o el delegado del área para tal fin, debe solicitar a través de la oficina de sistemas, la apertura del inventario y demás servicios que requiera el Servidor Público, contratista o tercero, para la ejecución de sus funciones u obligaciones contractuales.
c) La Oficina de Sistemas y Soporte Técnico y el personal de apoyo que se requiera, debe diseñar y ejecutar de manera permanente, un programa de concientización en seguridad de la información, con el fin de apoyar la protección adecuada de la información.
d) La Oficina de Sistemas y Soporte Técnico en conjunto con la Oficina Asesora de Comunicaciones deben diseñar y ejecutar un plan de Uso y apropiación de comunicaciones en apropiación del Sistema de Gestión de la Seguridad de la Información - SGSI, el cual se debe ejecutar durante la vigencia al interior de la Universidad Tecnológica del Chocó.
e) Es responsabilidad de los Docentes, Estudiantes, Administrativos, contratista o personal provisto por terceros, informar de los incidentes de seguridad de la información a través de los medios dispuestos por la oficina de Sistemas y Soporte Técnico.

f) En lo pertinente al incumplimiento de las políticas de la seguridad de la información, se aplicará lo establecido en los procedimientos destinados para tal fin, enmarcados en la normatividad vigente.

TERMINACIÓN Y CAMBIO DE EMPLEO

a) Es de responsabilidad del Servidor Público realizar la entrega de la información propia la Universidad Tecnológica del Chocó, que se encuentra en gestión del empleado, cuando existe una novedad de retiro, investigación, inhabilidades, o cambio de funciones.
b) El supervisor del contrato o a quien este delegue debe recoger y custodiar la información la Universidad Tecnológica del Chocó bajo la responsabilidad del contratista en caso de terminación anticipada, definitiva, temporal o cesión del contrato.
c) La Oficina de Sistemas y Soporte Técnico debe parametrizar en el directorio activo, la inactivación automática de los contratistas, teniendo en cuenta la fecha de terminación del contrato; la inactivación de los usuarios de los sistemas de información que no se autentican con el directorio activo, se debe hacer de forma manual.
d) Grupo Interno de trabajo de apoyo logística y documental o a quienes se deleguen, deben informar a la Oficina de Sistemas y Soporte Técnico, a través de la Mesa de Servicios o canal dispuesto para tal fin, cualquier novedad de desvinculación administrativa, laboral o contractual del Servidor Público, contratista o tercero; una vez notificada la novedad la Oficina de Sistemas y Soporte Técnico, debe proceder a la inactivación de los y servicios accesos y servicios de red del Servidor Público, contratista o tercero
e) Se creará una copia de respaldo del buzón de correo electrónico una vez se dé por terminada la vinculación con la Universidad Tecnológica del Chocó.
f) Bajo ningún parámetro se podrán restablecer los accesos a correos electrónicos; solo se podrán restablecer buzones para consulta y no se podrán emitir correos ni notificaciones desde estos buzones.
g) Se deben inactivar todos los accesos a los sistemas de información.
h) Se debe solicitar la devolución del carné, tarjeta de proximidad o cualquier distintivo de autenticación, que lo acredita como Docente, Administrativo, contratista o tercero de la Universidad Tecnológica del Chocó.

5.1.3. POLÍTICA DE GESTIÓN DE ACTIVOS

Responsabilidad por los activos

a) Todos los procesos de La Universidad Tecnológica del Chocó deben contar con un inventario de sus activos de información y se debe evidenciar a través de los instrumentos dispuestos.
b) Todos los activos de información mantenidos en el inventario deben tener un propietario.
c) La Oficina de Sistemas y Soporte Técnico, debe establecer una configuración adecuada para los recursos tecnológicos, con el fin de preservar la confidencialidad, integridad y disponibilidad de la información.
d) El personal Docente, Administrativos, contratistas o terceros, no deben usar software no autorizado o de su propiedad en activos de la Universidad Tecnológica del Chocó.
e) El personal Docente, Administrativos, contratistas o terceros, de la Universidad Tecnológica del Chocó, deben hacer entrega de los activos bajo su responsabilidad de acuerdo con el formato de Entrega de Bienes y documentos.

Manejo de medios

a) La Oficina de Sistemas y Soporte Técnico debe definir un procedimiento para el uso de medios removibles.
b) La Oficina de Sistemas y Soporte Técnico debe proveer a los usuarios de la Universidad Tecnológica del Chocó los métodos de cifrado de la información, así como administrar el software o herramienta utilizado para tal fin, y generar la guía de uso para el usuario.
c) Todo medio removible debe ser escaneado mediante las soluciones de seguridad, suministrado por la Oficina de Sistemas y Soporte Técnico cada vez que se conecte a un equipo de la Universidad Tecnológica del Chocó.
d) Es responsabilidad de cada funcionario, contratista o tercero tomar las medidas para la protección de la información contenida en medios removibles, para evitar acceso físico y lógico no autorizado, daños, pérdida de información o extravío del mismo.
e) Se prohíbe el uso de medios removibles que contengan información reservada o clasificada de la Universidad Tecnológica del Chocó.
f) Dirección de Talento Humano de la Universidad Tecnológica del Chocó, en conjunto con la oficina de Sistema de Información debe crear o actualizar si fuere

necesario el procedimiento o documento donde se establezca la disposición final de residuos de aparatos eléctricos y electrónicos (RAEE).

g) Cuando se requiera transferir un medio de almacenamiento de información de la Universidad Tecnológica del Chocó a otras entidades se debe establecer un acuerdo de confidencialidad y seguridad, entre las partes. Dichos acuerdos deben dirigirse al mecanismo de transferencia segura de información de interés entre el La Universidad Tecnológica del Chocó y las partes.
h) La Oficina de Sistemas y Soporte Técnico debe generar y aplicar lineamientos para la disposición segura de los dispositivos que almacenen información de la entidad, ya sea cuando son dados de baja o asignados a un nuevo usuario.
i) La Oficina de Sistemas y Soporte Técnico debe autorizar el uso de periféricos o medios de almacenamiento externo, de acuerdo con las necesidades requeridas para el cumplimiento de las funciones y del perfil del cargo de los servidores públicos o Contratistas.
j) Los funcionarios de la Universidad Tecnológica del Chocó, Contratistas o personal provisto por terceras partes deben acoger las condiciones de uso de periféricos y medios de almacenamiento establecidos por la Oficina de Sistemas y Soporte Técnico.
k) Se deben emplear herramientas de borrado seguro y demás mecanismos de seguridad pertinentes en los medios de propiedad de la Universidad Tecnológica del Chocó que sean reutilizados o dados de baja, con el fin de controlar que la información de la Universidad Tecnológica del Chocó contenida en estos medios no se pueda recuperar.
l) Cuando se requiera transferir un medio de almacenamiento se debe tener en cuenta el registro de contenido de los medios, la protección aplicada, al igual que los tiempos de transferencia a los responsables durante el transporte y el recibido.
m) El transporte para los medios de almacenamiento debe contar con las condiciones apropiadas para salvaguardar la integridad, confidencialidad y disponibilidad de la información de la Universidad Tecnológica del Chocó.

5.1.4. POLITICA CONTROL DE ACCESOS

Requisitos de la entidad para el control de acceso

a) La Oficina de Sistemas y Soporte Técnico debe suministrar y garantizar el cambio de contraseña, a los usuarios las credenciales para el acceso a los

servicios de red y sistemas de información a los que hayan sido autorizados, según su perfil y rol, las credenciales de acceso son de uso personal e intransferible.

b) b. La conexión remota a la red de área local de la Universidad Tecnológica del Chocó debe establecerse a través de una conexión VPN, la cual debe ser aprobada, registrada y monitoreada por la Oficina de Sistemas y Soporte Técnico.
c) c. La Oficina de Sistemas y Soporte Técnico debe establecer una segregación de las redes, separando los entornos de red de usuarios de los entornos de red de servidores y servicios publicados
d) La Oficina de Sistemas y Soporte Técnico debe asegurar que las redes inalámbricas de la Entidad cuenten con métodos de autenticación que evite accesos no autorizados.
e) La Oficina de Sistemas y Soporte Técnico debe realizar el cambio de contraseña de la red inalámbrica de la Entidad mínimo tres (3) veces al año.
f) La Oficina de Sistemas y Soporte Técnico para los eventos que se realicen en la Entidad debe generar usuario y clave de red Wifi, el cual debe expirar una vez finalizado el evento.
g) La Oficina de Sistemas y Soporte Técnico debe revisar que los equipos personales de los funcionarios, contratistas o terceros de la Universidad Tecnológica del Chocó que se conecten a las redes de datos de la Universidad Tecnológica del Chocó cumplan con todos los requisitos o controles para autenticarse y únicamente podrán realizar las tareas para las que fueron autorizados.

Gestión de acceso de usuarios

a) La Oficina de Sistemas y Soporte Técnico debe definir un procedimiento que contemple la creación, actualización, activación e inactivación de cuentas de usuario.
b) El usuario de correo electrónico debe ser igual al usuario de red, y contar con single on (mismo usuario, misma contraseña en los dos (2) servicios).
c) La Oficina de Sistemas y Soporte Técnico sólo otorgará a los usuarios, los accesos solicitados y autorizados por el jefe inmediato, supervisor del contrato o un jefe de mayor jerarquía.
d) Por defecto los usuarios creados no tienen permisos de administrador. En caso de requerirlo deben realizar la solicitud a la página de soporte. Sólo se otorgan

los privilegios para la administración de recursos tecnológicos, servicios de red, sistemas operativos y sistemas de información a aquellos usuarios que cumplan dichas actividades.

e) El usuario y la contraseña asignados para el acceso a los diferentes servicios tecnológicos, es personal e intransferible. Cualquier actividad que se realice con el usuario y clave será responsabilidad del servidor público y contratista al cual le fue asignado.
f) La Oficina de Sistemas y Soporte Técnico debe garantizar que las estaciones de trabajo con perfil de administrador local sean las que estén autorizadas, en caso contrario se debe modificar el permiso en la configuración de la estación de trabajo.
g) Una vez finalizada la gestión de servicios prestados por terceras partes para la Institución, el supervisor de contrato debe garantizar que los accesos queden cerrados al finalizar el proceso o contrato.
h) La Oficina de Sistemas y Soporte Técnico, con el apoyo de mesa de servicios, debe garantizar que los usuarios, realicen el cambio de contraseña de acceso a los servicios de la Universidad Tecnológica del Chocó, cada vez que sea requerido.
i) La Oficina de Sistemas y Soporte Técnico, con el apoyo de mesa de servicios, debe garantizar que los usuarios, realicen el cambio de contraseña de acceso a los servicios de la Universidad Tecnológica del Chocó, cada vez que sea requerido.
j) Todos los accesos de servicios de red deben estar conectados a la cuenta del directorio activo, si esta caduca, todos los accesos también, como son (VPN, cuentas de usuario, Plataforma Academia, Academusoft, servicio de impresión y telefonía, etc.).
k) La Oficina de Tecnología y sistemas de Información debe deshabilitar los servicios o funcionalidades no utilizadas de los sistemas operativos, el firmware, bases de datos y demás recursos tecnológicos.
l) La Oficina de Sistemas y Soporte Técnico debe mantener un listado actualizado con las cuentas que administren todos los recursos tecnológicos.
m) La contraseña para la autenticación se debe suministrar a los usuarios de manera segura, y el sistema debe solicitar el cambio inmediato de la misma al ingresar.
n) La Oficina de Sistemas y Soporte Técnico debe establecer controles para que los usuarios finales de los servicios tecnológicos no tengan instalado en sus

equipos de cómputo software o herramientas que permitan la obtención de privilegios no autorizados.

Responsabilidades de los usuarios

a) La Oficina de Sistemas y Soporte Técnico debe garantizar que para el ingreso a los servicios tecnológicos de la entidad las contraseñas no sean visibles en texto claro.
b) Las contraseñas deben poseer algún grado de complejidad y no deberán ser palabras comunes que se puedan encontrar en diccionarios, ni tener información personal, por tanto:

- Debe cambiarse obligatoriamente cada 45 días de lo contrario la contraseña caducará y obligará su cambio.
- Después de tres (3) intentos fallidos de ingreso de la contraseña el usuario se bloquea de manera inmediata y deberá esperar un tiempo determinado de dos (2) minutos para volver a intentar, o solicitar el desbloqueo a través de la Mesa de Servicios.
- Debe cambiarse la contraseña si se ha detectado anomalía en la cuenta de usuario.
- No ser visible en la pantalla, al momento de ser ingresada.
- No se debe registrar en papel, correo electrónico, archivos digitales a menos que se puedan almacenar de forma segura y el método de almacenamiento debe estar aprobado por la Oficina de Sistemas y Soporte Técnico.

c) Los administradores de los servicios tecnológicos deben cumplir con los lineamientos de contraseñas seguras indicadas.
d) Los administradores de los servicios tecnológicos o Sistema de Información deben de entregar de manera adecuada las credenciales de acceso.

Control de accesos a sistemas y aplicaciones

a) La Oficina de Sistemas y Soporte Técnico, deben velar por que los servicios tecnológicos sean debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico, teniendo en cuenta la matriz de roles y perfiles para cada sistema de información.

b) La Oficina de Sistemas y Soporte Técnico, se debe acoger a las buenas prácticas de desarrollo seguro en los productos entregados, controlando el acceso lógico cuando estos estén en producción.
c) La Oficina de Sistemas y Soporte Técnico, deben revisar los perfiles definidos, de acuerdo con la matriz de roles y perfiles, en los casos cuando exista novedades de gestión de cuenta (creación, traslado, inactivación, incapacidades y licencias).
d) La Oficina de Sistemas y Soporte Técnico debe establecer ambientes separados a nivel físico y lógico para el desarrollo-pruebas y producción; contando con su plataforma, servidores, aplicativos, dispositivos y versiones independientes de los otros ambientes, para evitar así que las actividades de desarrollo y pruebas puedan poner en riesgo la integridad, confidencialidad y disponibilidad de la información de los servicios en producción.
e) La Oficina de Sistemas y Soporte Técnico debe asegurar mediante los controles necesarios, que los usuarios utilicen diferentes cuentas de usuario para los ambientes pruebas y producción y así mismo que los menús muestren los mensajes de identificación apropiados para reducir el riesgo de error.
f) Los desarrolladores deben asegurar que no se desplieguen en pantalla las contraseñas ingresadas.
g) Los desarrolladores deben, a nivel de los aplicativos, restringir el acceso a archivos u otros recursos, a direcciones URL protegidas, a funciones protegidas, a servicios, a información de las aplicaciones, a atributos y políticas utilizadas para los controles de acceso y a la información relevante de la configuración, solamente a usuarios autorizados.

5.1.5. POLÍTICA SEGURIDAD PARA EL USO DE RECURSOS CRIPTOGRÁFICOS.

Controles criptográficos

a) La Oficina de Sistemas y Soporte Técnico debe gestionar los controles criptográficos para protección de claves de acceso a sistemas, datos y servicios.
b) La Oficina de Sistemas y Soporte Técnico debe verificar que todo sistema de información que requiera realizar transmisión de información clasificada o reservada cuente con mecanismos de cifrado de datos.
c) La Oficina de Sistemas y Soporte Técnico, en cabeza de los proveedores de desarrollado de software deben asegurar que los controles criptográficos de los

sistemas construidos cumplen con los estándares establecidos por la Universidad Tecnológica del Chocó.

d) La Oficina de Sistemas y Soporte Técnico debe disponer de herramientas que permitan el cifrado de medios de almacenamiento de información.

5.1.6. POLÍTICA FIRMA DIGITAL

a) La Oficina de Sistemas y Soporte Técnico establece los lineamientos necesarios para el control y el uso de las firmas digitales para la Universidad Tecnológica del Chocó.
b) Toda solicitud de asignación de firma digital se realiza a través de la mesa de servicios de la Universidad Tecnológica del Chocó, para el caso de usuarios nuevos, esta debe ser solicitada a través del formato de gestión de cuentas y servicios informáticos respectivo.
c) Los funcionarios y contratistas deben firmar el documento de “Acuerdo sobre uso del mecanismo de firma digital”
d) Los funcionarios y contratistas, que realicen actividades para la Universidad Tecnológica del Chocó, y tengan a su cargo una firma digital, deben hacer buen uso de esta de acuerdo con lo establecido en el Instructivo de Firma Digital.
e) Los funcionarios y contratistas que se les haya asignado firma digital deben hacer uso de esta para el desarrollo de sus actividades, así mismo gestionar la renovación del certificado de la firma, cuando este próxima a vencer.
f) Todos los documentos firmados digitalmente son auténticos se tomarán como originales y finales. Adicional cumplen con los criterios de seguridad de la información de integridad, confidencialidad, y disponibilidad.
g) En caso de presentarse o identificar algún incidente de seguridad de la información relacionado con el uso de la firma digital, el usuario debe reportarlo tan pronto como sea posible, a la oficina de sistemas a través de la página de soporte.
h) Es responsabilidad del usuario hacer buen uso de los servicios tecnológicos donde se pretenda usar la firma digital.
i) En caso de que tenga dudas debe informar a la oficina de sistemas a través de la página de soporte, para realizar la respectiva revisión.
j) Los funcionarios y contratistas que realicen actividades para la Universidad Tecnológica del Chocó, y se les haya asignado un certificado de firma digital,

son responsables de la seguridad de los dispositivos que utilicen para firmar los documentos.

k) El certificado asignado es personal e intransferible, por lo cual es responsabilidad del usuario los documentos que firme.
l) Los documentos que son firmados con la solución de firma digital de la Universidad Tecnológica del Chocó, deben ser validados digitalmente y su custodia debe estar en un repositorio institucional destinado para tal fin, de acuerdo a la ley 527 de 1999 “Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones” y el decreto 2364 de 2012 “Por medio del cual se reglamenta el artículo 7° de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones”.
m) El usuario debe comprobar la información que va a firmar, es decir, antes de realizar la firma el usuario debe comprobar que está de acuerdo con el contenido que va a firmar en las condiciones o contexto en el que se realiza la firma.

5.1.7. POLÍTICA SEGURIDAD FÍSICA Y DEL ENTORNO

Áreas seguras

Equipos

a) El Grupo Interno de trabajo de apoyo logística y documental con el apoyo de la Oficina de Sistemas y Soporte Técnico velarán que los equipos de cómputo, escáneres e impresoras estén situados y protegidos en áreas para reducir el riesgo contra amenazas ambientales y de acceso no autorizado.
b) El Grupo Interno de trabajo de apoyo logística y documental y la Oficina de Tecnología y Sistemas de Información, debe propender que los equipos de cómputo portátiles suministrados por la Universidad Tecnológica del Chocó se protejan mediante mecanismos que no permitan su pérdida.
c) La Oficina de Sistemas y Soporte Técnico establece los lineamientos para el uso de la red de energía regulada en los puestos de trabajo en los cuales solo se deben conectar equipos como computadores de escritorio, portátiles y pantallas; los otros elementos deben conectarse a la red eléctrica no regulada.

d) La Oficina de Sistemas y Soporte Técnico debe proteger el cableado que transporta voz, datos y suministro de energía eléctrica contra la interceptación, interferencia o daños de cualquier tipo dentro de las diferentes sedes de la Universidad Tecnológica del Chocó.
e) La Oficina de Sistemas y Soporte Técnico debe definir mecanismos para que los cables de energía eléctrica deben estar separados de los cables de comunicaciones para evitar interferencia y ruido.
f) La Oficina de Sistemas y Soporte Técnico debe definir mecanismos de soporte y mantenimiento a los equipos de cómputo, servidores y equipos activos de red y debe llevar registro de estos.
g) Cuando un equipo o medio extraíble sea reasignado o retirado de servicio, la Oficina de Tecnologías y Sistemas de Información debe garantizar la eliminación de toda información mediante mecanismos de borrado seguro teniendo en cuenta que previo a esta actividad debe realizarse una copia de seguridad de esta.
h) Los funcionarios, contratista o terceros que tengan asignado un equipo portátil propiedad de la Universidad Tecnológica del Chocó deben asegurarlo mediante una guaya de seguridad. El código de seguridad deberá ser entregado a la mesa de servicios una vez termine su vínculo contractual con la entidad.
i) Es responsabilidad de los usuarios registrar el ingreso o salida de los equipos portátiles ya sean propios o de la entidad.
j) El personal de seguridad y vigilancia de la Universidad Tecnológica del Chocó tendrá la potestad de recoger y entregar al Grupo Interno de trabajo de apoyo logística y documental los equipos que se encuentren sin su respectiva guaya de seguridad, en el caso de que el responsable del equipo se encuentre ausente.
k) La Oficina de Sistemas y Soporte Técnico debe configurar como política general que todos los equipos de cómputo que se encuentren en los dominios de la Universidad Tecnológica del Chocó bloqueen automáticamente su sesión después de tres (3) minutos de inactividad
l) Los funcionarios, contratista o terceros de la Universidad Tecnológica del Chocó, durante su ausencia no deben conservar sobre el escritorio información propia de la institución como: documentos físicos o medios de almacenamiento, por lo tanto, se requiere guardar en un lugar seguro para

impedir su pérdida, daño, copia o acceso por parte terceros o personal que no tenga autorización para su uso o conocimiento.

m) Los funcionarios, contratista o terceros de la Universidad Tecnológica del Chocó, deben bloquear la pantalla del computador a su cargo cuando se ausenten de su puesto de trabajo, para impedir el acceso de terceros no autorizados a la información almacenada en el equipo de cómputo.
n) Los Servidores Públicos, contratista o terceros que impriman documentos con clasificación (Clasificada – Reservada), estos deben ser retirados de la impresora inmediatamente y no se deben dejar en el escritorio sin custodia.
o) No se debe reutilizar documentos impresos con clasificación (Clasificada – Reservada), estos deben ser destruidos y no deben estar como papel reciclable.

5.1.8. POLÍTICA SEGURIDAD DE LAS OPERACIONES

Procedimientos operacionales y responsabilidades

a) La Oficina de Sistemas y Soporte Técnico con el apoyo de la Oficina Asesora de Planeación Institucional, debe documentar y mantener actualizados todos sus procedimientos operativos para garantizar la disponibilidad, integridad y confidencialidad de la información.
b) La Oficina de Sistemas y Soporte Técnico debe establecer un procedimiento que permita asegurar la gestión de cambios a nivel de infraestructura, aplicativos y servicios tecnológicos para que estos sean desarrollados bajo estándares de eficiencia, seguridad, calidad y permitan determinar las actividades y responsables en la gestión de cambios.
c) La Oficina de Sistemas y Soporte Técnico debe establecer mesas de trabajo de gestión de cambios, quien se encargará de evaluar, aprobar o negar la implementación de los cambios y este a su vez será presidido por el Gestor de Cambios.
d) La Oficina de Sistemas y Soporte Técnico debe documentar la gestión de capacidad de la plataforma tecnológica, definir su responsable y mantenerla actualizada
e) La Oficina de Sistemas y Soporte Técnico debe velar por la capacidad de procesamiento requerida en los recursos tecnológicos de la información de la entidad, efectuando proyecciones de crecimiento y provisiones en la plataforma tecnológica con una periodicidad definida.

f) La Oficina de Sistemas y Soporte Técnico debe realizar las tareas de optimización de servicios tecnológicos y sistemas de información, al igual que la verificación de capacidad de los servicios de red de la entidad.
g) La Oficina de Sistemas y Soporte Técnico debe proveer los recursos necesarios para la implantación de controles que permitan la separación de ambientes de pruebas y producción, teniendo en cuenta consideraciones como: controles para el intercambio de información entre los ambientes de pruebas y producción, la inexistencia de compiladores editores o fuentes en los ambientes de producción y un acceso diferente para cada uno de los ambientes.
h) La Oficina de Sistemas y Soporte Técnico debe definir y documentar las reglas para la transferencia de software del ambiente de pruebas a producción.
i) La Oficina de Sistemas y Soporte Técnico debe garantizar que todo cambio que se deba realizar en los sistemas información en producción deba ser probados en un ambiente de pruebas antes de aplicarlos a los sistemas en producción, de acuerdo con la metodología de desarrollo de la Entidad, salvo que sean cambios de emergencia.
j) La Oficina de Sistemas y Soporte Técnico debe garantizar que los compiladores, editores y otras herramientas de desarrollo y utilitarios del sistema, no sean accedidos desde sistemas de producción cuando se no se requieren.

Protección contra códigos maliciosos

a) La Oficina de Sistemas y Soporte Técnico debe definir y documentar los controles para la detección, prevención y recuperación contra códigos maliciosos. Además, proporcionará los mecanismos para generar cultura de seguridad entre los Servidores Públicos, contratistas y terceros frente a los ataques de software malicioso.
b) La Oficina de Sistemas y Soporte Técnico de Información debe contar con herramientas tales como antivirus, antimalware, antispam y antispyware que reduzcan el riesgo de contagio de software malicioso
c) La Oficina de Sistemas y Soporte Técnico debe asegurar que el software de antivirus, antimalware, antispyware y antispam cuente con las licencias de uso requeridas, certificando su autenticidad y la posibilidad de actualización periódica de las ultimas bases de datos de firmas del proveedor de servicios.
d) La Oficina de Sistemas y Soporte Técnico debe velar por que la información almacenada en la plataforma tecnológica sea escaneada por el software de

antivirus, incluyendo la información que se encuentra contenida y es transmitida por el servicio de correo electrónico.

e) La Oficina de Sistemas y Soporte Técnico, debe asegurar que no se pueda realizar cambios en la configuración del software de antivirus, antispyware, antispam y antimalware.
f) La Oficina de Sistemas y Soporte Técnico debe velar que el software de antivirus, antispyware, antispam y antimalware posea las últimas actualizaciones y parches de seguridad, para mitigar las vulnerabilidades de la plataforma tecnológica.
g) Los funcionarios, contratista o terceros de la Universidad Tecnológica del Chocó, deben abstenerse de abrir o ejecutar archivos y/o documentos de fuentes desconocidas, especialmente los que se encuentran en medios de almacenamiento externo o que provienen de correos electrónicos desconocidos.
h) Los funcionarios, contratista o terceros de la Universidad Tecnológica del Chocó no deben descargar archivos de internet de fuentes desconocidas, en caso de requerirlo, debe generar la solicitud a la Oficina de Sistemas y Soporte Técnico a través de la mesa de servicios.
i) Los funcionarios, contratista o terceros de la Universidad Tecnológica del Chocó que sospechen o detecten alguna infección por software malicioso deben notificar de inmediato a la Oficina de Sistemas y Soporte Técnico de Información a través de la mesa de servicios, con el fin de ejercer los controles correspondientes.

Copias de respaldo

a) La Oficina Sistemas de Información debe definir y documentar un plan o procedimiento de copias de respaldo y restauración de la información de la Universidad Tecnológica del Chocó, donde se establezca el esquema, de qué, cómo, quién, con qué periodicidad, tipo de respaldo y nivel de criticidad.
b) La Oficina de Sistemas y Soporte Técnico, velará por que los medios magnéticos que contienen la información sean almacenados en una ubicación diferente a las instalaciones donde se encuentra dispuesta. El sitio externo donde se resguarden las copias de respaldo debe contar con la seguridad física y medioambientales apropiados.
c) La Oficina de Sistemas y Soporte Técnico debe disponer de los recursos necesarios para permitir la identificación de los medios de almacenamiento, la información contenida en ellos y la ubicación física de los mismos para permitir

un rápido y eficiente acceso a los medios que contienen la información resguardada.

d) La Oficina de Sistemas y Soporte Técnico debe llevar a cabo los procedimientos para realizar pruebas de recuperación a las copias de respaldo, para así comprobar su integridad y posibilidad de uso en caso de ser necesario.
e) Gestión Documental debe definir las condiciones de transporte, transmisión o custodia de las copias de respaldo de la información que son almacenadas externamente.
f) La Oficina de Sistemas y Soporte Técnico debe proporcionar los lineamientos para la definición de las estrategias de generación, retención y rotación de las copias de respaldo de los activos de información de la entidad.
g) La Oficina de Sistemas y Soporte Técnico debe velar por que el software de respaldo esté instalado en las estaciones de trabajo y servidores para los cuales sea necesario la realización de Backup. Se debe contar con las licencias necesarias para garantizar continuidad en el proceso.
h) La Oficina de Sistemas y Soporte Técnico debe garantizar el almacenamiento del respaldo de la información de los usuarios, por lo menos un año antes de su envío a Gestión Documental.
i) Es responsabilidad de los procesos dueños de las aplicaciones, definir la frecuencia de la generación de copias de respaldo adicionales a las definidas por la Oficina de Sistemas y Soporte Técnico
j) Es responsabilidad de los funcionarios, contratistas y terceros de la Universidad Tecnológica del Chocó, guardar la información crítica de sus funciones en unidades de almacenamiento destinadas para tal fin, garantizando su respaldo.
k) Es responsabilidad de los funcionarios, contratistas y terceros de la Universidad Tecnológica del Chocó, guardar la información para el desarrollo de sus funciones, en la carpeta “Institucionales” en sus estaciones de trabajo. La información que no se aloje en esta carpeta no se respaldará y cualquier pérdida de esta será responsabilidad del usuario.
l) Los Servidores Públicos, contratistas y terceros de la Universidad Tecnológica del Chocó son responsables de hacer buen uso de los servicios tecnológicos de la Universidad y en ningún momento pueden ser usados para beneficio propio o para realizar prácticas ilícitas o mal intencionadas que atenten contra otros Servidores Públicos, contratistas y terceros,
m) Por ningún motivo se permite alojar en servidores información catalogada como personal, música, videos, etc.

n) Oficina de Sistemas y Soporte Técnico garantizará el respaldo de los archivos con extensión .pdf .doc, .docm, .docx, .dot, .dotm .xls, .xlsm, .xlsx, .xlt, .xltm, .xltx, .bmp, .gif, .jpg, .odp, .png, .pot, .potm, .potx, .pps, .ppt, .pptm, .jpeg.

Registro de eventos y seguimiento

a) La Oficina de Sistemas y Soporte Técnico debe generar registros de auditoría que contengan excepciones o eventos relacionados a la seguridad en los sistemas de información que se consideren.
b) La Oficina de Sistemas y Soporte Técnico debe salvaguardar los registros de auditoría que se generen de cada sistema.
c) La Oficina de Sistemas y Soporte Técnico debe monitorear excepciones o los eventos de la seguridad de información.
d) La Oficina de Sistemas y Soporte Técnico debe monitorear la infraestructura tecnológica para verificar que los usuarios sólo la usen para actividades propias de su labor y la Misión de la Universidad Tecnológica del Choco.
e) La Oficina de Sistemas y Soporte Técnico, debe garantizar que todos los sistemas de procesamiento de información, los equipos y demás servicios tecnológicos que lo ameriten se sincronicen con una única fuente de referencia de tiempo, con el fin de garantizar la exactitud de los registros de auditoría.

Control de software operacional

a) La Oficina de Sistemas y Soporte Técnico designará responsables y establecerá instructivos y guías para controlar la instalación de software operativo, se cerciorará de contar con el soporte de los proveedores de dicho software y asegurará la funcionalidad de los sistemas de información que operan sobre la plataforma tecnológica cuando el software operativo es actualizado.
b) La Oficina de Sistemas y Soporte Técnico debe establecer responsabilidades y procedimientos para controlar la instalación del software operativo que interactúa con el procedimiento de cambios existente en la Universidad Tecnológica del Choco.
c) La Oficina de Sistemas y Soporte Técnico debe conceder accesos temporales y controlados a los fabricantes y terceros autorizados para realizar actualizaciones sobre el software operativo, así como monitorear dichas actualizaciones.
d) La Oficina de Sistemas y Soporte Técnico debe establecer las restricciones y limitaciones para la instalación del software operativo en los equipos de cómputo de la Universidad Tecnológica del Chocó.

e) La Oficina de Sistemas y Soporte Técnico debe generar un plan de actualizaciones para el software, aplicaciones y librerías de programas que deberán llevar a cabo los administradores, bajo la autorización de la dirección de la Oficina.
f) La Oficina de Sistemas y Soporte Técnico debe manejar un sistema de control de configuración para mantener el control de todo el software implementado, al igual que se debe mantener la documentación del sistema.

Gestión de vulnerabilidades técnicas

a) La Oficina de Sistemas y Soporte Técnico debe realizar mínimo una vez al año una revisión de vulnerabilidades técnicas a los sistemas de información críticos y misionales por medio de ethical hacking y/o pruebas de penetración.
b) La Oficina de Sistemas y Soporte Técnico debe documentar, informar, gestionar y corregir las vulnerabilidades encontradas, adoptando acciones correctivas para mitigar los hallazgos, minimizar el nivel de riesgo y reducir el impacto.
c) La Oficina de Sistemas y Soporte Técnico debe restringir a los usuarios finales la instalación de software en los equipos de la Universidad Tecnológica del Chocó.
d) La Oficina de Sistemas y Soporte Técnico debe establecer y monitorear que la infraestructura tecnológica sea usada exclusivamente para el desempeño laboral, o para el desarrollo de las funciones, actividades y obligaciones acordadas o contratadas.
e) La Oficina de Sistemas y Soporte Técnico debe controlar la instalación y uso de máquinas virtuales y sólo podrá realizarse siempre y cuando sea una necesidad para el uso de las funciones o labor contratada.
f) La Oficina de Sistemas y Soporte Técnico debe realizar de manera periódica una inspección del software instalado en los equipos de la Universidad Tecnológica del Chocó y debe desinstalar el software no autorizado.
g) La Oficina de Sistemas y Soporte Técnico a través de la Mesa de Servicios es la responsable de instalar, configurar y dar soporte a los equipos de la Universidad Tecnológica del Chocó.
h) Sólo está permitido el uso de software licenciado por el Universidad Tecnológica del Chocó y/o aquel que sin requerir licencia de uso comercial sea expresamente autorizado La Oficina de Tecnologías y Sistemas de Información.

Consideraciones sobre auditorias de sistemas de información

a) La Oficina de Sistemas y Soporte Técnico debe planificar periódicamente actividades que involucren auditorias de los sistemas críticos en producción.
b) La Oficina de Sistemas y Soporte Técnico debe documentar los resultados de las auditorias de los sistemas de Información de la Universidad Tecnológica del Chocó.

5.1.9. POLÍTICA SEGURIDAD DE LAS COMUNICACIONES

Gestión de seguridad de las redes

a) Sistemas de Información debe disponer de controles para realizar transferencias completas, sin alteraciones y visualizaciones no autorizadas de la información entre las aplicaciones de la Universidad Tecnológica del Chocó.
b) La Oficina de Sistemas y Soporte Técnico debe proporcionar recursos necesarios para la implementación, administración y mantenimiento requeridos para la prestación del servicio de internet.
c) La Oficina de Oficina de Sistemas y Soporte Técnico debe monitorear continuamente el canal o canales que prestan el servicio de internet, con el fin de prevenir y atender cualquier incidente que se presente tan pronto como sea posible.
d) La Oficina de Sistemas y Soporte Técnico debe generar registros de navegación y los accesos de los usuarios a Internet, así como establecer e implementar procedimientos de monitoreo sobre la utilización del servicio de internet.
e) La Oficina de Sistemas y Soporte Técnico debe implementar controles que eviten el ingreso a páginas con código malicioso incorporado o sitios catalogados como peligrosos
f) La Oficina de Sistemas y Soporte Técnico debe proporcionar una plataforma Tecnológica que soporte los sistemas de información, esta debe estar separada en segmentos de red físicos y lógicos e independientes de los segmentos de red de usuarios, de conexiones con redes con terceros y del servicio de acceso a internet. La división de estos segmentos debe ser realizada por medio de dispositivos perimetrales e internos de enrutamiento y de seguridad.
g) La Oficina de Sistemas y Soporte Técnico debe realizar segmentación de Redes para Servidores Públicos, Contratistas y visitantes de la Universidad Tecnológica del Chocó.

h) La Oficina de Sistemas y Soporte Técnico debe establecer el perímetro de seguridad necesario para proteger dichos segmentos, de acuerdo con el nivel de criticidad del flujo de la información transmitida.
i) La Oficina de Sistemas y Soporte Técnico debe mantener las redes de datos segmentadas por dominios, grupos de servicios, grupos de usuarios, ubicación geográfica o cualquier otra tipificación que se considere conveniente para la Institución.
j) La Oficina de Oficina de Sistemas y Soporte Técnico debe instalar protección entre las redes internas y cualquier red externa, que este fuera de la capacidad de control y administración de la Entidad.
k) La Oficina de Sistemas y Soporte Técnico debe permitir el acceso a redes inalámbricas mediante un portal de acceso en donde permita al usuario ingresar un usuario y contraseña.
l) La Oficina de Sistemas y Soporte Técnico debe realizar de manera periódica el cambio de las claves de acceso a la red WIFI de la Universidad Tecnológica del Chocó.

Transferencia de información

a. La Oficina de Sistemas y Soporte Técnico, debe establecer el procedimiento de intercambio de información con los diferentes terceros que, hacen parte de la operación de la Universidad Tecnológica del Chocó, donde se contemple la recepción o envío de la información, utilización de medios de transmisión confiables y la adopción de controles, con el fin de proteger la confidencialidad e integridad de esta.
b. La Oficina de Sistemas y Soporte Técnico, debe ofrecer servicios o herramientas de intercambio de información seguros, así como adoptar controles como el cifrado de información, que permitan el cumplimiento del procedimiento para el intercambio de información (digital o medio magnético), con el fin de proteger dicha información contra divulgación o modificaciones no autorizadas.
c. Grupo Interno de trabajo de apoyo logística y documental debe dictar directrices sobre retención, disposición y transferencia de la información física de la Universidad Tecnológica del Chocó, de acuerdo con la normatividad vigente
d. La Oficina de Tecnologías y Sistemas de Información debe establecer controles para proteger la información que se transmite como documentos adjuntos a través del correo electrónico de la Universidad Tecnológica del Chocó.

e. Los mensajes y la información contenida en los buzones de correo son propiedad de la Universidad Tecnológica del Chocó y cada responsable, el cual debe mantener únicamente los mensajes relacionados con el desarrollo de sus actividades.
f. El único servicio de correo electrónico controlado por la Universidad Tecnológica del Chocó es el asignado directamente por la Oficina de Tecnologías y Sistemas de Información, el cual cumple con todos los requerimientos técnicos y de seguridad para evitar ataques informáticos, virus, spyware y otro tipo de software o código malicioso.
g. Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definidos por la Universidad Tecnológica del Chocó y deben conservar en todos los casos el mensaje legal corporativo de confidencialidad.
h. Los usuarios de correo electrónico tienen prohibido el envío de cadenas de mensajes de cualquier tipo, ya sea comercial, político, religioso, material audiovisual, contenido discriminatorio, pornografía y demás condiciones que degraden la condición humana y resulten ofensivas para los servidores públicos de la entidad y el personal provisto por terceras partes.
i. Está prohibido el envío de o intercambio de mensajes con contenido que atente contra la integridad de las personas o instituciones, tales como: ofensivo, obsceno, pornográfico, chistes, información terrorista, cadenas de cualquier tipo, racista, o cualquier contenido que atente con la integridad de las personas.
j. Es responsabilidad del usuario etiquetar el mensaje de correo electrónico de acuerdo con los niveles de clasificación teniendo en cuenta el tipo de información que se pretende compartir.
k. Es responsabilidad del usuario reportar un correo electrónico cuando crea que es de dudosa procedencia a la Oficina de Sistemas y Soporte Técnico, con el fin de que el administrador tome las medidas necesarias para evitar su propagación dentro de la entidad.
l. Es responsabilidad de cada usuario asegurar los destinarios a los cuales va dirigida una comunicación, si estas son listas de distribución, también debe revisarlas con el fin de evitar compartir información a personas no autorizadas.
m. El servicio de correo electrónico debe ser usado de manera ética, razonable, eficiente, responsable, no abusiva y sin generar riesgos para la operación de equipos, sistemas de información e imagen de la Entidad.

n. No es permitido el envío o recepción de archivos que contengan extensiones ejecutables, en ninguna circunstancia.
o. Es obligación del usuario realizar la activación de las repuestas automáticas en el servicio de correo de la Entidad, cuando su ausencia sea mayor a tres (3) días, igualmente, está deberá indicar quién es la persona asignada para cubrir su ausencia. Nota: La persona encargada de cubrir la ausencia debe estar autorizada por parte del jefe inmediato o supervisor del contrato.
p. La Oficina de Sistemas y Soporte Técnico define las pautas generales para asegurar un adecuado uso de la Suite de Office 365 (correo electrónico, grupos, drive, calendario, sitios y formularios) por parte de los usuarios.
q. Está prohibida la divulgación no autorizada de información de propiedad de la Universidad Tecnológica del Chocó a través de la plataforma Suite office 365.
r. Está prohibido la creación, almacenamiento o intercambio de mensajes que atenten contra las leyes de derechos de autor.
s. Se deben establecer acuerdos de confidencialidad o de no divulgación de Información.
t. Para el personal externo que ejecute tareas propias de la Universidad Tecnológica del Chocó y haya sido contratado en el marco de un contrato o convenio con la Universidad Tecnológica del Chocó, debe firmar un acuerdo de confidencialidad y no divulgación de la información firmado entre la Universidad Tecnológica del Chocó (Supervisor del Contrato) y el Representante Legal, y este debe reposar en la carpeta de ejecución del contrato.

Adquisición, desarrollo y mantenimiento de sistemas

a) Las áreas técnicas propietarias de sistemas de información en conjunto con la oficina de Sistemas y Soporte Técnico incluirán requisitos de desarrollo seguro en la definición de requerimientos y, posteriormente se asegurarán de que estos se encuentren generados a cabalidad durante las pruebas realizadas sobre los desarrollos del software construido.
b) Todos los sistemas de información o desarrollos de software deben tener un área técnica formalmente asignada que sea la responsable de la administración y su custodia dentro de la Universidad Tecnológica del Chocó.
c) La Oficina de Tecnologías y Sistemas de Información debe establecer metodologías para el desarrollo de software seguro, que incluyan la definición de requerimientos de seguridad y las buenas prácticas, con el fin de proporcionar a los desarrolladores una visión clara de lo que se espera.

d) Las áreas técnicas responsables de la administración de los sistemas de información en acompañamiento con la Oficina de Sistemas y Soporte Técnico deben establecer las especificaciones de adquisición o desarrollo de sistemas de información considerando siempre los requerimientos de Seguridad de la Información.
e) El área técnica responsable de la administración de los sistemas de información puede definir qué perfiles deben contener los sistemas de información a desarrollar, igualmente, deben aprobar la asignación de estos perfiles cuando sea necesario.
f) La Oficina de Sistemas y Soporte Técnico debe liderar la definición de requerimientos de seguridad de los sistemas de información, teniendo en cuenta aspectos como la estandarización de herramientas de desarrollo, controles de autenticación, la arquitectura de aplicaciones, entre otros. Igualmente, el área técnica debe definir los controles de acceso
g) La Oficina de Sistemas y Soporte Técnico debe asegurar que cada vez que se pretenda implementar un sistema de información ya sea propio o de terceros, este sea sometido a un análisis de vulnerabilidades supervisadas las cuales deberán ser remediadas antes del despliegue en producción por las áreas encargadas.
h) La Oficina de Tecnologías y Sistemas de Información debe establecer mecanismos que permitan deshabilitar las funcionalidades de autocompletar en formularios de solicitud que requieran información sensible.
i) La Oficina de Sistemas y Soporte Técnico debe asegurar que no se permitan conexiones recurrentes con el mismo usuario a los sistemas de información construidos, garantizando la seguridad de las conexiones a los sistemas de información mediante mecanismos que aseguren una única autenticación.
j) La Oficina de Tecnologías y Sistemas de Información debe exigir la documentación relacionada con el código fuente para los desarrollos propios y para los casos en que la Entidad adquiera el sistema de información a un proveedor externo
k) La Oficina de Tecnologías y Sistemas de Información debe exigir toda la documentación de los repositorios y bases de datos de los sistemas de información a los proveedores externos.

Seguridad en los procesos de desarrollo y de soporte

a) La Oficina de Sistemas y Soporte Técnico debe velar por el desarrollo interno o externo de los sistemas de información cumpla con las buenas prácticas para el desarrollo seguro de aplicativos, así como con metodologías para la realización de pruebas de aceptación y seguridad al software desarrollado.
b) La Oficina de Sistemas y Soporte Técnico debe establecer y mantener ambientes separados de Desarrollo/Pruebas y Producción, dentro de la infraestructura de la Universidad Tecnológica del Chocó.

- El ambiente de desarrollo/pruebas se debe utilizar para propósitos de implementación, modificación, ajuste y/o revisión de código fuente; además se debe utilizar para realizar el conjunto de validaciones funcionales y técnicas del software, aplicación o sistema de información, teniendo como base los criterios de aceptación y los requerimientos de desarrollo.

- El ambiente de producción debe utilizarse para la prestación de un servicio que involucra el manejo de datos reales y que tiene un impacto directo sobre las actividades realizadas como parte de un proceso de la Universidad Tecnológica del Chocó.

c) La Oficina de Sistemas y Soporte Técnico debe restringir el acceso a compiladores, editores y otros utilitarios del sistema operativo en el ambiente de producción, cuando no sean indispensables para el funcionamiento del mismo
d) Los administradores de los sistemas de información (Líder Funcional) con el apoyo de la Oficina de Sistemas y Soporte Técnico son responsables de asegurar que la calidad de los entregables cumpla con los requerimientos de seguridad y establecidos, antes del paso a producción de los sistemas utilizando metodologías para este fin, documentando las pruebas realizadas y aprobando los pasos a producción
e) Las áreas técnicas propietarias de los sistemas de información deben probar las migraciones entre los ambientes de desarrollo, pruebas y producción que han sido aprobadas.
f) La Oficina de Sistemas y Soporte Técnico debe asegurar que la plataforma tecnológica, las herramientas de desarrollo y los componentes de cada sistema de información estén actualizados con los últimos parches generados para las versiones en uso y que estén ejecutando la última versión aprobada del sistema

g) La Oficina de Sistemas y Soporte Técnico debe incluir dentro del procedimiento y los controles de gestión de cambios el manejo de los cambios en el software, aplicativos y sistemas de información de la Universidad Tecnológica del Chocó.
h) Los desarrolladores internos y externos de los sistemas de información deben considerar las buenas prácticas y lineamientos de desarrollo seguro durante el ciclo de vida de estos, pasando desde el diseño hasta la puesta en marcha.
i) Los desarrolladores internos y externos deben proporcionar un nivel adecuado de soporte para solucionar los problemas en los sistemas de información de la Entidad; de acuerdo a los niveles de servicio acordados entre las partes.
j) Los desarrolladores internos y externos deben construir los sistemas de información de tal manera que efectúen las validaciones de datos de entrada y la generación de datos de salida de manera confiable, utilizando rutinas de validación centralizada y estandarizadas.
k) Los desarrolladores internos y externos deben asegurar que los sistemas de información construidos validen la información suministrada por los usuarios antes de procesarla, teniendo en cuenta aspectos como: tipos de datos, rangos válidos, longitud, listas de caracteres aceptados, caracteres considerados peligrosos y caracteres de alteración de rutas, entre otros.
l) Los desarrolladores internos y externos deben suministrar opciones de desconexión o cierre de sesión de los sistemas de información (Logout) que permitan terminar completamente con la sesión o conexión asociada.
m) Los desarrolladores internos y externos deben asegurar el manejo de operaciones sensibles o críticas de los aplicativos desarrollados permitiendo el uso de dispositivos adicionales como tokens o el ingreso de parámetros adicionales de verificación.
n) Los desarrolladores internos y externos deben asegurar que los aplicativos proporcionen la mínima información de la sesión establecida, almacenada en cookies y complementos, entre otros.
o) Los desarrolladores internos y externos deben garantizar que no se divulgue información sensible en respuestas de error, incluyendo detalles del sistema, identificadores de sesión o información de las cuentas de usuarios; así mismo, deben implementar mensajes de error genéricos.
p) Los desarrolladores internos y externos deben remover todas las funcionalidades y archivos que no sean necesarios para los aplicativos, previo a la puesta en producción.

q) Los desarrolladores internos y externos deben prevenir la revelación estricta de directorios de los sistemas de información construidos.
r) Los desarrolladores internos y externos deben remover información innecesaria en los encabezados de respuesta que se refieran a los sistemas operativos y versiones del software utilizado.
s) Los desarrolladores internos y externos deben evitar incluir las cadenas de conexión a las bases de datos en el código de los aplicativos. Dichas independientes, los cuales se recomienda que estén cifrados.
t) Los desarrolladores internos y externos deben certificar el cierre de la conexión con las bases de datos desde los aplicativos tan pronto como estas sean requeridas.
u) Los desarrolladores deben implementar controles necesarios para la transferencia de archivos, como exigir autenticación, vigilar los tipos de archivos a transmitir, almacenar los archivos transferidos en el repositorio destinado para este fin o en bases de datos, eliminar privilegios de ejecución a los archivos transferidos y asegurar que dichos archivos solo tengan privilegios de lectura.
v) Ni los desarrolladores ni terceros deben realizar pruebas, instalaciones o desarrollos de software, directamente sobre el entorno de producción. Esto puede conducir a fraude o inserción de código malicioso.
w) Los desarrolladores deben proteger el código fuente de los aplicativos construidos, de tal forma que no pueda ser descargado ni modificado por usuarios no autorizados.
x) Los desarrolladores deben asegurar que no se permite que los aplicativos desarrollados ejecuten comandos directamente en el sistema operativo.
y) La Oficina de Sistemas y Soporte Técnico en conjunto con los desarrolladores, debe crear e implementar una guía de desarrollo seguro usando metodologías de desarrollo seguro.
z) Todo desarrollo realizado por el equipo de la Oficina de Sistemas y Soporte Técnico o terceros debe estar alineado con los lineamientos de desarrollo seguro para Sistemas Información

Proteger los datos usados para pruebas

a) La Oficina de Sistemas y Soporte Técnico protegerá los dato e prueba que se entregarán a los desarrolladores, asegurando que no revelan información confidencial de los ambientes de producción.

b) La Oficina de Sistemas y Soporte Técnico debe certificar que la información a ser entregada a los desarrolladores para sus pruebas será enmascarada y no revelará información confidencial de los ambientes de producción.
c) La Oficina de Sistemas y Soporte Técnico debe eliminar la información de los ambientes de pruebas una vez estas hayan concluido.
d) Cada vez que se realicen copias de información de producción se debe contar con un registro que permita realizar auditoria.

5.1.10. POLÍTICA SEGURIDAD DE RELACIÓN CON PROVEEDORES

a) La Oficina de Contratación debe establecer lineamientos para el cumplimiento de las obligaciones contractuales de la dimensión de Seguridad y Privacidad de la Información con terceros o proveedores.
b) La Oficina de Contratación debe establecer en el momento de suscribirse contratos de cualquier tipo los riesgos asociados a la seguridad y privacidad de la información, los compromisos establecidos de confidencialidad de la información y el cumplimiento de las políticas de seguridad de la información de la Universidad Tecnológica del Chocó.
c) La Oficina de Contratación debe establecer en los contratos con terceros y proveedores los requisitos legales y regulatorios relacionados con la protección de datos personales, los derechos de propiedad intelectual y derechos de autor.
d) La Oficina de Sistemas y Soporte Técnico debe documentar, establecer controles y permisos cuando un tercero o proveedor requiera tener accesos a la información por medio de la infraestructura tecnológica de la Universidad Tecnológica del Chocó.
e) La Oficina de Sistemas y Soporte Técnico debe verificar mensualmente el cumplimiento de Acuerdos de Nivel de Servicio establecidos con sus proveedores de tecnología.
f) La Oficina de Sistemas y Soporte Técnico debe establecer un procedimiento que permita asegurar la gestión de cambios a nivel de infraestructura, aplicativos y servicios tecnológicos que son soportados por terceros y/o proveedores, para garantizar estándares de eficiencia, seguridad, calidad y que permitan determinar los responsables y tareas a seguir para garantizar el éxito en la gestión de cambios.
g) Cada dependencia de la Universidad Tecnológica del Chocó que establezca relación con proveedores y su cadena de suministro, debe solicitar

acompañamiento periódico a la dimensión de Seguridad y Privacidad de la Información con el fin de dar a conocer las políticas que tiene el Universidad.

h) La Oficina de Contratación debe incluir en las guías de contratación y supervisión obligaciones generales sobre seguridad y privacidad de la información y los formatos para su cumplimiento y verificación por parte del supervisor de contrato.

5.1.11. POLÍTICA GESTIÓN DE INCIDENTES DE SEGURIDAD

a) La Oficina de Sistemas y Soporte Técnico en conjunto con el Oficial o persona encargada de la Seguridad de la Información debe definir un procedimiento para la gestión de incidentes de seguridad de la información.
b) La Oficina de Sistemas y Soporte Técnico debe definir los canales para que los Servidores Públicos, contratistas y terceros de la Universidad Tecnológica del Chocó puedan reportar los incidentes de Seguridad de la Información.
c) La Oficina de Sistemas y Soporte Técnico es la encargada de la evaluación de eventos de seguridad de la información y la decisión tomada sobre los mismos.
d) La Oficina de Sistemas de la Información es la encargada para la recolección de evidencias de los incidentes de seguridad de la información.
e) La Oficina de Sistemas y Soporte Técnico debe contar con los mecanismos para el cumplimiento de los tiempos en la respuesta de incidentes establecido en los lineamientos para la Gestión de Incidentes.
f) La Oficina de Sistemas y Soporte Técnico debe proporcionar los medios para el aprendizaje a la Universidad Tecnológica del Chocó de los incidentes de Seguridad de la Información.
g) La Oficina de Sistemas y Soporte Técnico deberá dar a conocer a los Servidores Públicos, contratistas y terceros de la Universidad Tecnológica del Chocó los lineamientos establecidos para la Gestión de Incidentes de Seguridad de la Información.
h) La Oficina de Sistemas y Soporte Técnico debe velar por que la recolección de evidencia tenga en cuenta la cadena de custodia, la seguridad del personal, los roles y responsabilidades del personal involucrado, la competencia del personal, y la documentación.

5.1.12. POLÍTICA GESTIÓN CONTINUIDAD DEL NEGOCIO

Continuidad de seguridad de la información

a) Establecer un análisis de impacto al negocio (BIA por sus siglas en ingles), por medio del cual se identifiquen los servicios críticos de la Universidad Tecnológica del Chocó.
b) Diseñar las estrategias y tiempos de recuperación de la operación de los servicios críticos de la Universidad Tecnológica del Chocó.
c) La Oficina de Sistemas y Soporte Técnico debe disponer de planes de contingencia de los servicios Tecnológicos de Información y un plan de recuperación ante desastres, enfocados a lograr el retorno a la operación normal.

5.1.13. POLÍTICA DE PROTECCIÓN Y TRATAMIENTO DE DATOS PERSONALES

1) Regular la recolección, almacenamiento, uso, circulación y supresión de datos personales, brindando las herramientas que garanticen la autenticidad, confidencialidad, integridad y disponibilidad de la información y datos personales almacenados en las bases de datos de la infraestructura propia y/o de un tercero.
2) Velar por el cumplimiento de la ley 1581 de 2012, su decreto reglamentario 1377 de 2013, el Acuerdo 0035 de 2018 emanado por el Consejo Superior y demás normas que la adicionen, modifiquen o deroguen cuya materia se refiera a la protección y tratamiento de datos personales.
3) Infundir y aplicar los principios establecidos en la ley de protección y tratamiento de datos personales.
4) Solicitar autorización para el tratamiento de datos personales a través de una autorización previa, expresa e informada a los titulares de los datos personales, o a sus representantes. Esta autorización puede ser por escrito diligenciando un formato elaborado previamente por la Universidad o también se podrá dar de forma Biométrica (llamada telefónica, video, etc.), asegurando que el detalle de la descripción del tratamiento de los datos personales se informará mediante el mismo documento específico o adjunto, al titular de los datos, incluyendo como mínimo:
5) La descripción del tratamiento al que serán sometidos sus datos sensibles y la finalidad del mismo.
6) Los derechos que le asisten como titular.

7) Los canales en los cuales podrá formular consultas y/o reclamos
8) Garantizar el derecho de acceso y consulta de los datos, previa acreditación de la identidad del titular, legitimidad o personalidad de su representante, poniendo a disposición de este, sin costo o erogación alguna, de manera pormenorizada y detallada, los respectivos datos personales.
9) Llevar a cabo un adecuado tratamiento y protección de los datos personales mediante el fortalecimiento de la Seguridad y Privacidad de la Información, el desarrollo y la actualización de la política de privacidad y la normatividad relacionadas, como la clasificación de la información y gestión de activos, de conformidad a lo dispuesto en la Ley 1581 de 2012, del Acuerdo 0035 de 2018 emanado por el Consejo Superior y demás desarrollos normativos que le apliquen.
10) Comunicar la responsabilidad de los servidores públicos, contratistas y terceros de la Universidad en reportar cualquier incidente de fuga de información, daño informático, violación de datos personales, comercialización de datos, uso de datos personales de niños, niñas o adolescentes, suplantación de identidad o conductas que puedan vulnerar la intimidad de una persona.
11) Divulgar, sensibilizar y capacitar a todos los servidores públicos, contratistas y terceros de la Universidad en los derechos que se derivan de la protección y tratamiento de datos personales a través de las directrices del Secretario General en apoyo con el área de Tecnologías y Sistemas de Información, disponga para tal fin.
12) Las excepciones para la autorización del Titular lo complementan y debe entenderse como una lista no exhaustiva, de acuerdo con las normas y demás normas que los modifiquen, adicionen o sustituyan:

- Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial.
- Datos de naturaleza pública.
- Casos de urgencia médica o sanitaria.
- Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos.
- Datos relacionados con el Registro Civil de las Personas

Alcance

La política de tratamiento de datos personales aplica para toda la información personal registrada en las bases de datos manuales, automatizadas o semiautomatizadas de la Universidad Tecnológica del Chocó, quien actúa en calidad de responsable del tratamiento de los datos personales.

Así mismo tiene el propósito de dar a conocer el compromiso de la Universidad Tecnológica del Chocó con el cumplimiento de las leyes, decretos y demás normas que tienen como objetivo la protección de los datos personales.

Principios Rectores

Con el fin de garantizar la protección y tratamiento de datos personales la Universidad Tecnológica del Chocó, aplica los principios señalados en la Ley 1581 de 2012, "*Por el cual se dictan disposiciones generales para la protección de datos personales*" y del Acuerdo 0035 de 2018, emanado por el Consejo Superior de la UTCH.

5.1.14. POLÍTICA DE USO DE CORREO ELECTRÓNICO

Objetivo

Definir las directrices generales del buen uso del correo electrónico en el UTCH.

Usos aceptables del servicio

1) Se debe utilizar exclusivamente para las actividades propias del desempeño de las funciones o actividades laborales a desempeñar en la UTCH y no se debe utilizar para otros fines.
2) Se debe utilizar de manera ética, razonable, eficiente, responsable, no abusiva y sin generar riesgos para la operación de equipos o sistemas de información e imagen de la UTCH.
3) Todos los funcionarios, colaboradores y terceros que son autorizados para acceder a la red de datos y los componentes de Tecnologías de Información son responsables de todas las actividades que se ejecuten con sus credenciales de acceso a los buzones de correo.
4) Todos los funcionarios, colaboradores y terceros deben dar cumplimiento a la reglamentación y leyes, en especial la Ley 1273 de 2009 de Delitos Informáticos, así mismo evitar prácticas o usos que puedan comprometer la seguridad de la información la UTCH.

5) El servicio de correo electrónico institucional debe ser empleado para servir a una finalidad operativa y administrativa en relación con la UTCH. Todas las comunicaciones establecidas mediante este servicio, sus buzones y copias de seguridad se consideran de propiedad de la UTCH y pueden ser revisadas por el administrador del servicio o cualquier instancia de vigilancia y control, en caso de una investigación o incidentes de seguridad de la información.
6) Cuando un Proceso tenga información de interés institucional para divulgar, lo debe hacer a través del área de Comunicaciones de la UTCH o el medio formal autorizado para realizar esta actividad.
7) Todos los mensajes enviados deben respetar el estándar de formato e imagen institucional definido por la UTCH y deberán conservar en todos los casos el mensaje legal institucional.
8) El único servicio de correo electrónico controlado en la entidad es el asignado directamente por el área responsable de las Tecnologías de la Información y las Comunicaciones, el cual cumple con todos los requerimientos técnicos y de seguridad necesarios para evitar ataques informáticos, virus, spyware y otro tipo de software o código malicioso.
9) Los demás servicios de correo electrónico son utilizados bajo responsabilidad directa y riesgo de los usuarios.
10) Es responsabilidad del usuario etiquetar el mensaje de correo electrónico de acuerdo a los niveles de clasificación para los cuales se requiere etiquetado (Reservado o Confidencial), de acuerdo a la Clasificación y Etiquetado de la Información establecida en la UTCH.
11) El tamaño del buzón de correo electrónico se asigna de manera estandarizada, la capacidad específica es definida y administrada por el área de Tecnologías de la Información y las Comunicaciones.
12) Todos los funcionarios, colaboradores y terceros son responsables de informar si tienen accesos a contenidos o servicios que no estén autorizados y no correspondan a sus funciones o actividades designadas dentro de la UTCH, para que de esta forma el área de Tecnologías de la Información y las Comunicaciones realicen el ajuste de permisos requerido.
13) El usuario debe reportar cuando reciba correos de tipo SPAM, es decir correo no deseado o no solicitado, correos de dudosa procedencia o con virus al área de Tecnologías de la Información y las Comunicaciones, con el fin de tomar las acciones necesarias que impidan el ingreso de ese tipo de correos. De la misma forma el usuario debe reportar cuando no reciba correos y este seguro

que este no es de tipo SPAM, así el área de Tecnologías de la Información y las Comunicaciones hacen el análisis para evaluar el origen y así tomar las medidas pertinentes.

14) Cuando un usuario se retire de la UTCH, y se le haya autorizado el uso de una cuenta con acceso a la red y al servicio de correo de la institución, debe abstenerse de continuar empleándolas y debe verificar que su cuenta y acceso a los servicios sean cancelados.
15) Los mensajes y la información contenida en los buzones de correo son de propiedad de la UTCH.
16) Cada usuario se debe asegurar que, en el reenvío de correos electrónicos, la dirección de destino es correcta, de manera que esté siendo enviado a los destinatarios que son. Si tiene listas de distribución también se deben depurar. El envío de información a personas no autorizadas es responsabilidad de quien envía el mensaje de correo electrónico.
17) Las cuentas institucionales (Ejemplo: Comunicaciones, Atención al Ciudadano, Apoyo sistemas, Control Interno, etc.) deben tener una persona responsable que haga depuración del buzón periódicamente.
18) Todo usuario es responsable de reportar los mensajes cuyo origen sean desconocidos, y asume la responsabilidad de las consecuencias que puede ocasionar la ejecución de cualquier archivo adjunto. En los casos en que el Funcionario, Colaborador o Tercero desconfíe del remitente de un correo electrónico debe remitir la consulta al correo gestioninformatica@utch.edu.co o a la Mesa de Servicios Tecnológicos (sistema de tickets para la solución de problemas).
19) Si una cuenta de correo es interceptada por personas mal intencionado o delincuentes informáticos (crackers) o se reciba cantidad excesiva de correos no deseado (SPAM), el área de Tecnologías de la Información y Comunicaciones actuará según sea el caso.
20) El área de Tecnologías de la Información y las Comunicaciones se reserva el derecho de filtrar los tipos de archivo que vengan anexos al correo electrónico para evitar amenazas de virus y otros programas destructivos. Todos los mensajes electrónicos serán revisados para evitar que tengan virus u otro programa destructivo.
21) Ningún Funcionario, Colaborador o Tercero debe suscribirse en boletines en líneas, publicidad o que no tenga que ver con sus actividades laborales, con el correo institucional.

22) El Funcionario, Colaborar o Tercero no debe responder mensajes donde les solicitan información personal o financiera que indican que son sorteos, ofertas laborales, ofertas comerciales o peticiones de ayuda humanitaria. Por el contrario, debe notificar al área de Tecnologías de la Información y las Comunicaciones, con el fin de ejecutar las actividades pertinentes como bloquear por remitente y evitar que esos mensajes lleguen a más buzones de correo de la UTCH.
23) Todo mensaje electrónico dirigido a otros dominios debe contener una sentencia o cláusula de confidencialidad.

Usos no aceptables del servicio

1) Envío, reenvío o intercambio de mensajes no deseados o considerados como SPAM, cadena de mensajes o publicidad.
2) Envío o intercambio de mensajes con contenido que atente contra la integridad de las personas o instituciones, tales como: ofensivo, obsceno, pornográfico, chistes, información terrorista, cadenas de cualquier tipo, racista, o cualquier contenido que represente riesgo de virus.
3) Envío o intercambio de mensajes que promuevan la discriminación sobre la raza, nacionalidad, género, edad, estado marital, orientación sexual, religión o discapacidad, o que inciten a realizar prácticas ilícitas o promuevan actividades ilegales incluidas el lavado de activos.
4) Envió de mensajes que contengan amenazas o mensajes violentos.
5) Divulgación no autorizada de información propiedad de la UTCH.
6) Enviar, crear, modificar o eliminar mensajes de otro usuario sin su autorización.
7) Abrir o hacer uso y revisión no autorizada de la cuenta de correo electrónico de otro usuario sin su autorización.
8) Adulterar o intentar adulterar mensajes de correo electrónico.
9) Cualquier otro propósito inmoral, ilegal o diferente a los considerados en el apartado “Usos aceptable del servicio” de la presente política.

5.1.15. POLÍTICA DE USO DE INTERNET

Objetivo

Definir los lineamientos generales para el buen uso del internet y asegurar una adecuada protección de la información.

Usos aceptables del servicio

1) Este servicio debe utilizarse exclusivamente para el desempeño de las funciones y actividades desarrolladas durante la contratación en la UTCH y no debe utilizarse para ningún otro fin.
2) Los usuarios autorizados para hacer uso del servicio de Internet son responsables de evitar prácticas o usos que puedan comprometer los recursos tecnológicos de la Entidad o que afecte la seguridad de la información de la UTCH.
3) Todas las comunicaciones establecidas mediante este servicio pueden ser revisadas y/o monitoreadas por el administrador del servicio o cualquier instancia de vigilancia y control.
4) El navegador autorizado para el uso de Internet en la red de la UTCH es el instalado por el área de Tecnologías de la Información y las Comunicaciones, el cual cumple con todos los requerimientos técnicos y de seguridad necesarios para prevenir ataques de virus, spyware y otro tipo de software o código malicioso.
5) No se permite la conexión de módems externos o internos en la red de la UTCH.
6) Todo usuario es responsable de informar el acceso a contenidos o servicios no autorizados o que no correspondan al desempeño de sus funciones o actividades dentro de la UTCH.
7) Para realizar intercambio de información de propiedad de la UTCH con otras entidades, se debe seguir un proceso formal de requisición de la información, el cual debe contar con la previa autorización del dueño de la información.
8) La UTCH se reserva el derecho de realizar monitoreo permanente de tiempos de navegación y páginas visitadas por parte de los usuarios. Así mismo, revisar, registrar y evaluar las actividades realizadas durante la navegación.
9) Todos los usuarios que se encuentren autorizados son responsables de dar un uso adecuado de este recurso y por ninguna razón pueden hacer uso para realizar prácticas ilícitas o mal intencionadas que atenten contra terceros, la legislación vigente, las políticas de seguridad de la información, la seguridad de la información, entre otros.
10) Los funcionarios y colaboradores y tercero de la UTCH, no deben asumir en nombre de esta, posiciones personales en encuestas de opinión, foros u otros medios similares.

11) Este recurso puede 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 UTCH.

Usos no aceptables del servicio

1) Envío o descarga de información masiva de un tamaño grande o pesado que pueda congestionar la red a menos que el desempeño de las funciones lo amerite.
2) Envío, descarga o visualización de información con contenidos restringidos y que atenten contra la integridad moral de las personas o instituciones.
3) Cualquier otro propósito diferente al considerado en el apartado de Usos aceptables del servicio de la presente política.
4) Todos los usuarios invitados que tengan acceso al servicio de Internet deben cumplir estrictamente con las políticas de seguridad de la información, de lo contrario asumirán las acciones pertinentes.
5) No se permite la descarga, uso, intercambio o instalación de juegos, música, videos, películas, imágenes, protectores y fondos de pantalla, software de libre distribución, información o productos que atenten contra la propiedad intelectual, archivos ejecutables que comprometan la seguridad de la información, herramientas de hacking, entre otros.

5.1.16. POLÍTICA DE USO DE REDES SOCIALES

Objetivo

Definir los lineamientos generales para el uso del servicio de Redes sociales por parte de los usuarios autorizados en la UTCH.

Usos aceptables del servicio

1) Todos los usuarios autorizados para hacer uso de los servicios de Redes Sociales son responsables de evitar prácticas o usos que puedan comprometer la seguridad de la información de la UTCH.
2) El servicio autorizado debe ser utilizado exclusivamente para el desarrollo de las actividades relacionadas con la UTCH. Todas las comunicaciones establecidas mediante este servicio pueden ser monitoreadas por el administrador del servicio o cualquier instancia de vigilancia y control que lo requiera.

3) Es permitido el uso de redes sociales utilizando video conferencia y streaming (descarga de audio y video), siempre y cuando no interfiera o altere la operación normal de los sistemas de información de la UTCH.
4) La UTCH facilita el acceso a estas herramientas, teniendo en cuenta que constituyen un complemento de varias actividades que se realizan por estos medios y para el desempeño de las funciones y actividades a desempeñar por parte de funcionarios, colaboradores y terceros, sin embargo es necesario hacer buen uso de estas herramientas de forma correcta y moderada.
5) No se deben descargar programas ejecutables o archivos que puedan contener software o código malicioso.
6) No se permiten descargas, distribución de material obsceno y no autorizado, degradante, terrorista, abusivo a través del servicio de Redes Sociales.
7) No se debe practicar e intentar acceder de forma no autorizada a los sistemas de seguridad del servicio de Internet de la UTCH, o aprovechar el acceso a Redes Sociales para fines ilegales.
8) Es claro que no se puede difundir cualquier tipo de virus o software de propósito destructivo o malintencionado.
9) Todos los funcionarios, colaboradores y terceros de la UTCH, deben seguir los procedimientos y planes de comunicaciones interna y externa.
10) El área de Tecnologías de la Información y las Comunicaciones, será el encargado de determinar las directrices y lineamientos para el uso de las diferentes herramientas o plataformas de redes sociales en la UTCH, previo acuerdo con el Proceso de Gestión de Comunicaciones.

5.1.17. POLÍTICA DE USO DE RECURSOS TECNOLÓGICOS

Objetivo

Definir los lineamientos generales para el uso aceptable de los recursos tecnológicos de la UTCH.

Usos aceptables del servicio

La UTCH asigna los recursos tecnológicos necesarios como herramientas de trabajo para el desempeño de las funciones y actividades laborales de los funcionarios, colaboradores y terceros de ser necesario.

El uso adecuado de estos recursos se establece bajo los siguientes criterios:

1) La instalación de software se encuentra bajo la responsabilidad del área de Tecnologías de la Información y las Comunicaciones y por tanto son los únicos autorizados para realizar esta actividad.
2) Ningún usuario debe realizar cambios relacionados con la configuración de los equipos, como conexiones de red, usuarios locales de la máquina, papel tapiz y protector de pantalla corporativo. Estos cambios únicamente deben ser realizados por el área de Tecnologías de la Información y las Comunicaciones.
3) El área de Tecnologías de la Información y las Comunicaciones es el responsable de definir la lista actualizada de software y aplicaciones autorizadas que se encuentran permitidas en la UTCH, para ser instaladas en las estaciones de trabajo de los usuarios; así mismo, realizará el control y verificación del cumplimiento del licenciamiento del respectivo software y aplicaciones asociadas.
4) Sólo el personal autorizado por el área de Tecnologías de la Información y las Comunicaciones podrá realizar actividades de administración remota de dispositivos, equipos o servidores de la infraestructura de procesamiento de información de la UTCH; las conexiones establecidas para este fin utilizan los esquemas de seguridad establecidos por la entidad.
5) Los funcionarios, colaboradores y terceros de la UTCH, son responsables de hacer buen uso de los recursos tecnológicos de la UTCH y en ningún momento pueden ser usados para beneficio propio o para realizar prácticas ilícitas o mal intencionadas que atenten contra otros funcionarios, colaboradores y terceros, legislación vigente y políticas y lineamientos de seguridad de la información establecidas por la UTCH.
6) La información clasificada como personal almacenada en los equipos de cómputo, medios de almacenamiento o cuentas de correo institucionales, debe ser guardada en su totalidad en una carpeta especificada para tal fin, la cual debe ser nombrada como “PERSONAL”.
7) Todo activo de propiedad de la UTCH, asignado a sus funcionarios, colaboradores y terceros de la UTCH, debe ser entregado al finalizar el vínculo laboral o contractual o por cambio de cargo si es necesario. Esto incluye los documentos corporativos, equipos de cómputo (Hardware y Software), y la información que tenga almacenada en dispositivos removibles.

5.1.18. POLÍTICA DE CLASIFICACIÓN DE LA INFORMACIÓN

Objetivo
Asegurar que la información de la UTCH es clasificada, con el fin de que sea tratada y protegida adecuadamente.

Esquema de Clasificación de la Información
Toda la información del UTCH debe ser identificada y clasificada de acuerdo a los niveles de clasificación definidos por la entidad.

El área de Tecnologías de la Información y las Comunicaciones, Gestión Documental, Gestión Normativa y Gestión Administrativa y Financiera son los responsables de definir las directrices de clasificación de la información y las medidas de tratamiento y manejo de la información.

De acuerdo con la clasificación establecida por la UTCH el manejo y almacenamiento de la información, se debe tener en cuenta lo siguiente:

- Acceso a la información sólo de personal autorizado.
- Llevar un registro formal de acceso a la información.
- Conservar y mantener los medios de almacenamiento de información en un ambiente seguro.

Etiquetado y manejo de Información

1) Todos los funcionarios, colaboradores y terceros cuando sea el caso, deben mantener organizado el archivo de gestión, siguiendo los lineamientos establecidos por Gestión Documental.
2) Rector y Vicerrectores deben establecer mecanismos de control de documentos, con el fin de garantizar y mantener la disponibilidad, integridad y confidencialidad de la información.
3) Todos los funcionarios, colaboradores y terceros cuando sea el caso de la UTCH son responsables de la organización, conservación, uso y manejo de los documentos.
4) Los archivos de Gestión de las oficinas de la UTCH deben custodiar sus documentos de acuerdo a lo especificado en las tablas de Retención Documental.
5) La plataforma tecnología usada para salvaguardar, conservar y facilitar la información de los documentos en medios magnéticos, electrónicos o digitales,

debe garantizar los principios fundamentales de la seguridad como son la integridad, confidencialidad y disponibilidad de la información y por gestión documental usabilidad y acceso.

6) Se debe definir procedimientos de etiquetado de la información, de acuerdo con el esquema de clasificación definido por la UTCH.
7) El etiquetado de información debe incluir la información física y electrónica. Las etiquetas de la información se deben identificar y reconocer fácilmente.
8) Se debe garantizar la conservación, uso y recuperación de la información contenida en medios digitales, físicos y otros.

Usos no aceptables

1) Hacer caso omiso, retardar o no entregar de manera oportuna las respuestas a las peticiones, quejas, reclamos y solicitudes de igual forma retenerlas o enviarlas a un destinatario que no corresponde o que no esté autorizado, que lleguen por los diferentes medios, presencial, verbal, escrito, telefónico, correo y web.
2) Dañar o dar como perdido los documentos o archivos que se encuentren bajo su administración por la naturaleza de su cargo.
3) Divulgación no autorizada de los documentos, información o archivos.
4) Realizar actividades tales como borrar, modificar, alterar o eliminar información de la UTCH de manera malintencionada.

5.1.19. POLÍTICA DE GESTIÓN DE MEDIOS DE ALMACENAMIENTO

Objetivo

Proteger la información de la UTCH velando por la protección de la confidencialidad, integridad y disponibilidad de la información que se encuentra en unidades de almacenamiento.

Gestión y Disposición de medios removibles

1) Todos los dispositivos y unidades de almacenamiento removibles, tales como cintas, CD’s, DVD’s, dispositivos personales “USB”, discos duros externos, cámaras fotográficas, cámaras de video, celulares, entre otros, deben ser controlados desde su acceso a la red de la UTCH, uso hasta finalización de su contrato o cese de actividades.

2) Toda la información clasificada como CONFIDENCIAL o RESERVADA que sea almacenada en medios removibles y que se requiera de protección especial, debe cumplir con las directrices de seguridad emitidas por el área de Tecnologías de la Información y las Comunicaciones.
3) El área de Tecnologías de la Información y las Comunicaciones puede restringir que medios de almacenamiento removibles se conecten a los equipos de cómputo que sean propiedad de la UTCH o que estén bajo su custodia, y puede llevar a cabo cualquier acción de registro o restricción, con el fin de evitar fuga de información a través de medios removibles.
4) Los medios de almacenamiento removibles que se conecten a la red de datos de la UTCH o que se encuentren bajo su custodia, están sujetos a monitoreo por parte del área de Tecnologías de la Información y las Comunicaciones.
5) Todos los retiros de medios de almacenamiento de las instalaciones de la UTCH, como discos duros externos, se deben realizar con la autorización del propietario del proceso misional, estratégico, mejora continua o de apoyo, definidos de acuerdo con el mapa de procesos de la UTCH, a través del formato orden de salida de elementos.
6) Todos los medios de almacenamiento removibles propiedad de la UTCH, deben estar almacenados en un ambiente seguro.
7) Se debe hacer seguimiento a los medios de almacenamiento removibles como Discos Duros con el fin de garantizar que la información sea transferida a otro medio antes de que esta quede inaccesible por deterioro o el desgaste que sufren a causa de su vida útil.

Borrado seguro

1) Todos los medios de almacenamiento que sean de propiedad de terceros y que sean autorizados por la UTCH para su uso dentro de la red de la institución, deben contar con su respectivo soporte.
2) Todos los medios de almacenamiento que contengan información de la UTCH y que salgan de la misma que no se les vaya a dar más uso, deben seguir el procedimiento de borrado seguro definido por la UTCH, el cual garantiza que la información no es recuperable (Aplica para medios de almacenamiento de equipos, discos duros externos, etc.).
3) Los medios de almacenamiento que contengan información de la UTCH que vayan a ser dados de baja o reutilizados, deben seguir el procedimiento de borrado seguro definido por la UTCH, el cual garantiza que la información no se

es recuperable (Aplica para medios de almacenamiento externos o de equipos que son reasignados, formateados, reinstalados o que por degaste o falla son retirados o dados de baja).

4) Eliminar de forma segura (destrucción o borrado) los medios de almacenamiento que no se utilicen y que contengan información de la UTCH.

5.1.20. POLÍTICA DE ESCRITORIO Y PANTALLA LIMPIA

Objetivo

Definir los lineamientos generales para mantener el escritorio y la pantalla despejada, con el fin de reducir el riesgo de acceso no autorizado, pérdida y daño de la información de la UTCH.

Criterios establecidos

1) Todo el personal debe conservar su escritorio libre de información propia de la entidad, que pueda ser copiada, utilizada o estar al alcance de terceros o por personal que no tenga autorización para su uso o conocimiento.
2) Todo el personal debe bloquear la pantalla de su equipo de cómputo cuando no estén haciendo uso de ellos o que por cualquier motivo deban dejar su puesto de trabajo.
3) Todos los usuarios al finalizar sus actividades diarias deben salir de todas las aplicaciones y apagar las estaciones de trabajo.
4) Al imprimir documentos de carácter CONFIDENCIAL, estos deben ser retirados de la impresora inmediatamente. Así mismo, no se deben reutilizar papel que contenga información CONFIDENCIAL.
5) En horario no hábil o cuando los lugares de trabajo se encuentren desatendidos, los usuarios deben dejar la información CONFIDENCIAL protegida bajo llave.

5.1.21. POLITICAS DEL TELETRABAJO UNIVERSIDAD TECNOLÓGICA DEL CHOCÓ

Objetivo

Lograr que los datos que sean utilizados a través del Teletrabajo reciban la protección acorde con requerimientos de la Universidad Tecnológica del Chocó Diego Luís Córdoba.

Alcance

El alcance de esta política es para todos los colaboradores, contratistas y proveedores que requieran acceso a los sistemas de información o aplicaciones de la Universidad Tecnológica del Chocó Diego Luís Córdoba de manera remota.

Criterios establecidos

1) Informar al personal de la Universidad Tecnológica del Chocó, sobre la normativa de protección del puesto de trabajo fuera de la oficina llevando a cabo auditorías periódicas para asegurar su cumplimiento.
2) Llevar un control de las personas que, por su perfil dentro de la Universidad Tecnológica del Chocó o las características de su trabajo, tienen la opción de teletrabajar.
3) Redactar un documento donde se contemplen todas las cuestiones relativas al teletrabajo (duración del mismo, dispositivos facilitados, etc.), que será firmado por cada teletrabajador de la Universidad Tecnológica del Chocó.
4) Determinar un Periodo de implantación y pruebas valorando diferentes escenarios y configuraciones antes de habilitar el teletrabajo, contemplando todos los riesgos de seguridad.
5) Realizar pruebas de carga en escenarios simulados, si existe un volumen considerable de empleados que van a teletrabajar al mismo tiempo, valorar la carga que esto ocasiona en los sistemas internos de la Universidad Tecnológica del Chocó.
6) Establecer las aplicaciones y recursos a los que tiene acceso cada usuario, dando acceso a cada empleado solo a las aplicaciones y recursos necesarios para llevar a cabo su trabajo, dependiendo de su perfil dentro de la institución, detallar las aplicaciones permitidas, así como sus condiciones de uso, y valorar la inclusión del nuevo software solicitado por los empleados de la Universidad Tecnológica del Chocó.
7) Establecer el acceso seguro a través de la gestión de credenciales de ingreso de los empleados forzando el uso de contraseñas robustas y su cambio periódico, además de incluir el doble factor de autenticación siempre que sea posible.
8) Los usuarios y contraseñas que se lleguen a suministrar para el uso de los equipos y programas que se entreguen a los teletrabajadores son intransferibles y de uso exclusivo de los teletrabajadores.

9) Los teletrabajadores deberán mantener la confidencialidad y reserva de las contraseñas suministradas para el acceso a los equipos y programas.
10) Configurar los dispositivos utilizados por el empleado para teletrabajar (sistema operativo, antivirus, control de actualizaciones, etc.), tanto si son corporativos como si son aportados por el trabajador (Bring Your Own Device - BYOD).
11) Los equipos informáticos que sean aportados por el teletrabajador (Bring Your Own Device - BYOD) deberán almacenar la información en la nube institucional (nube privada), contar con antivirus y licencias de acuerdo con las directrices de la Oficina de Sistemas y Soporte Técnico.
12) Es responsabilidad del Teletrabajador o trabajo remoto, actualizar el antivirus rutinariamente.
13) Informar oportunamente al empleador las novedades que se presenten en relación con las licencias o programas que le hayan sido instalados en los equipos suministrados para desarrollar la labor contratada.
14) Los Teletrabajadores deberán hacer uso del correo electrónico (corporativo/institucional) como medio de comunicación principal dejando la trazabilidad de sus actividades.
15) El responsable de la Seguridad de la Información de la Universidad Tecnológica del Chocó deberá habilitar bloqueo de sesiones por inactividad.
16) Las redes sociales permitidas para envío de información institucional, será las licenciadas de uso institucional, incluyendo la intranet.
17) Guardar de manera segura y de conformidad con las políticas informáticas de la Universidad, la información que utilice para el desarrollo de sus labores.
18) Conservar, mantener y restituir en buen estado, salvo deterioro natural y razonable, en el momento en que el empleador lo solicite, los instrumentos, equipos informáticos y los útiles que se le haya facilitado para la prestación de sus servicios.
19) Cifrar los soportes de información, Implantando tecnologías de cifrado que protegen la información de posibles accesos malintencionados.
20) Definir los procedimientos de almacenamiento en los equipos de trabajo y en la red corporativas y detallar a los empleados de la Universidad Tecnológica del Chocó dónde deben guardar la información con la que trabajan en remoto.
21) Mantener actualizados y con información verídica los sistemas de almacenamiento de información y/o bases de datos utilizados por el empleador

con el fin de tener control de los datos que maneja la Universidad Tecnológica del Chocó.

22) Planificar las copias de seguridad de todos los soportes y comprobar regularmente que se realizan periódicamente y que pueden restaurarse.
23) Implementar una red VPN extremo a extremo que permite que la información que se intercambia entre los equipos de la Universidad Tecnológica del Chocó viaje cifrada a través de Internet, que garanticen el uso de conexiones seguras a través de esta red.
24) Valorar la implementación de la virtualización como método para proporcionar a cada empleado de la Universidad Tecnológica del Chocó, su propio espacio de trabajo, eliminando los riesgos asociados al uso de un dispositivo físico.
25) Priorizar el uso de dispositivos corporativos, eligiendo los corporativos para teletrabajar, ya que cuentan con las políticas de seguridad que la Universidad Tecnológica del Chocó considera necesarias y tienen instalado el software preciso para realizar el trabajo de forma segura.
26) Concientizar a los empleados de la Universidad Tecnológica del Chocó antes de empezar a teletrabajar, capacitándolos en ciberseguridad antes de que comiencen a teletrabajar para que conozcan las políticas y las medidas que se llevaran a cabo en la institución.
27) Abstenerse de darle un uso inadecuado a cualquier tipo de información a la que tenga acceso y que pueda ser considerada como propiedad intelectual.
28) Cumplir con las normas de propiedad intelectual, respecto a la información a la que tenga acceso en virtud de su calidad de teletrabajador.
29) Se deben considerar los requerimientos de seguridad definidos por la Oficina de Sistemas y Soporte Técnico y/o el Coordinador de Seguridad de la Información establecido por la Universidad Tecnológica del Chocó para los activos de información involucrados, es decir aplicar todas las restricciones y protecciones para la confidencialidad, integridad y disponibilidad definidas.
30) Acatar las órdenes del empleador frente a la revocación total o parcial de las condiciones de acceso a los recursos informáticos que tenga con ocasión de sus funciones laborales.
31) Los teletrabajadores y en general todos los trabajadores de la Universidad Tecnológica del Chocó deberán garantizar de forma íntegra la confidencialidad y reserva de la información a la que tengan conocimiento en ejecución de sus funciones, la cual en todo caso sólo podrá ser utilizada como desarrollo de su contrato de trabajo.

32) Reportar cualquier evento anormal aplicando la Política de Gestión de Incidentes.
33) Hacer uso responsable de los dispositivos con los que se realizan las actividades en teletrabajo.
34) Las redes sociales podrán ser usadas para comunicación (Comunicación bidireccional interactiva, Comunicación interactiva con múltiples interlocutores, Comunicación móvil) que no comprometa información institucional, pero que ayuda a la fluides comunicacional.
35) El equipo de la Oficina de Sistemas y Soporte Técnico debe velar por el cumplimiento de la presente política, garantizando los niveles de seguridad adecuados para el teletrabajo o trabajo remoto.
36) El Jefe de la Oficina de Sistemas y Soporte Técnico deberá designar el personal idóneo para que configure la conexión remota para las actividades de teletrabajo.
37) No es permitido que la sesión establecida con la Universidad Tecnológica del Chocó sea utilizada por una persona diferente al colaborador autorizado.
38) No está permitido conectarse desde un sitio de acceso público como un Café Internet, Aeropuerto y Restaurante, entre otros.
39) No consentir ni permitir sin autorización previa y escrita del empleador y/o sus representantes, que terceras personas tengan acceso a los equipos de propiedad de la Universidad Tecnológica del Chocó, ni a la información que reposa dentro de los mismos.
40) Se prohíbe divulgar a terceros sin autorización previa y escrita del empleador y/o sus representantes, información del hardware, software, configuraciones, bases de datos, usuarios, contraseñas y demás información involucrada con la prestación del servicio.
41) Se prohíbe permitir a terceros, salvo autorización previa y escrita del empleador y/o sus representantes, el acceso a los equipos que le hayan sido suministrados con ocasión a su trabajo.
42) No está permitido la comunicación a través de correos personales con información institucional.
43) No está permitido el envío de información sensible, crítica, privada y confidencial por medios no institucionales.
44) Se prohíbe modificar, adicionar o suprimir el software o hardware que le haya sido suministrado por la Universidad, sin autorización previa y escrita del empleador y/o sus representantes.

45) Se prohíbe borrar de las bases de datos cualquier tipo de archivo, sin previa autorización escrita del empleador.
46) Se prohíbe modificar, adicionar o suprimir el software o hardware que le haya suministrado la Universidad Tecnológica del Chocó, sin el cumplimiento de los procedimientos y estándares que le señale el empleador, en aquellos casos en que el teletrabajador haya sido autorizado para ello.
47) Bajo ningunas circunstancias el Teletrabajador podrá acceder o comunicar a través de protocolos no seguros (ejemplo: no usar http, debe ser https que permita garantizar la seguridad de la información que viaja por la red).
48) No obstaculizar el control, monitoreo y/o auditoría de la información que repose en cualquier tipo de herramientas que el empleador le haya suministrado para desarrollar sus funciones, ya sea en medio físico o electrónico, control que no requiere autorización previa del teletrabajador, pero que en todo caso deberá ser autorizada previamente y por escrito por el empleador, y realizado por el funcionario que para tal efecto señale la Universidad.
49) Se prohíbe expresamente a todos los trabajadores: revelar, suministrar, vender, arrendar, publicar, copiar, reproducir, remover, disponer, transferir y en general utilizar, directa o indirectamente, en favor propio o de otras personas, en forma total o parcial, cualquiera que sea su finalidad, la información confidencial o propiedad intelectual de la Institución a la cual hayan tenido acceso, o de la cual hayan tenido conocimiento en desarrollo de su cargo o con ocasión de este.
50) La revisión periódica de esta política de seguridad estará a cargo de la Oficina de Sistemas y Soporte Técnico la cual constituye un proceso de mejora continuo que permite mantenerla vigente ante los constantes cambios del entorno tecnológico y nuevas amenazas.
51) El incumplimiento de esta política de seguridad y privacidad de la información traerá consigo las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al Gobierno Nacional y Territorial en cuanto a seguridad y privacidad de la información se refiere.

5.1.22. POLITICA DE CUMPLIMIENTO

Cumplimiento de requisitos legales y contractuales

La Universidad Tecnológica del Choco, gestiona la seguridad y privacidad de la información dando cumplimiento adecuado a la legislación vigente. Analizando los requisitos legales aplicables a la información de derechos de autor y propiedad intelectual, protección de datos personales, ley de transparencia y del derecho de acceso a la información pública nacional. Igualmente, velara por la protección de los registros ante cualquier perdida, destrucción, falsificación acceso o liberación no autorizada de acuerdo con los requisitos legislativos, de reglamentación y contractuales de la Universidad.

Revisiones de seguridad de la información

a) La Oficina de Control Interno, debe realizar de manera periódica auditorías internas para comprobar el correcto funcionamiento del Sistema de Gestión de Seguridad de la Información en cuanto a los objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información.
b) Los líderes de los procesos deben asegurar que todos los procedimientos de seguridad dentro de su área de responsabilidad se realicen correctamente, con el fin de cumplir las políticas y normas de seguridad; en caso de incumplimiento se evaluarán y propondrán acciones correctivas
c) La Oficina de Sistemas y Soporte Técnico debe realizar revisiones mínimo una vez al año del cumplimiento de las políticas de Seguridad y Privacidad de la Información
d) Es un deber de los funcionarios contratistas y terceros de la Universidad Tecnológica del Chocó, conocer esta Política y realizar todos los actos conducentes para su cumplimiento, implementación y mantenimiento.

Cumplimiento

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento con la presente política. El incumplimiento a la política de Seguridad y Privacidad de la Información traerá consigo, las consecuencias legales que apliquen a la normativa de la Universidad Tecnológica del Chocó, incluyendo lo establecido en las normas que competen al gobierno nacional y territorial en cuanto a seguridad y privacidad de la información se refiere.

BIBLIOGRAFÍA

Norma Técnica Colombiana **NTC-ISO-IEC-27001** (2013). Tecnología de información. Técnicas de Seguridad. Sistema de Gestión de la seguridad de la información. Requisitos.

Ministerio de Tecnologías de la Información y las Comunicaciones. Seguridad y Privacidad de Información (2016). Elaboración de la política general de seguridad y privacidad de la información.

Sistema De Gestión Institucional Del Ministerio De Ciencia, Tecnología E Innovación (2020). Manual De Políticas De Seguridad Y Privacidad De La Información

CONTROL DE CAMBIOS

Versión	Fecha	Numerales	Descripción de la Modificación
0.0	25-02-2022	Todos	Creación del Documento

Elaboró	Revisó	Fecha
Jilmar Chaverra Barco – Oficina Sistemas y Soporte Técnico	Yunner Moreno Córdoba	Marzo de 2022