Universidad Pedagógica y Tecnológica de Colombia

LA UNIVERSIDAD QUE QUEREMOS

MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

DTIC UPTC
Dirección de las Tecnologías y Sistemas de Información y de las Comunicaciones

ACREDITACIÓN INSTITUCIONAL DE ALTA CALIDAD
MULTICAMPUS
RESOLUCIÓN 3910 DE 2015 MEN / 6 AÑOS

Fecha de publicación: 10 de Agosto de 2020

www.uptc.edu.co

VIGILADA MINEDUCACIÓN

MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Dirección de las Tecnologías y Sistemas de Información y de las Comunicaciones

MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA LA UNIVERSIDAD PEDAGÓGICA Y TECNOLÓGICA DE COLOMBIA

CONTENIDO Pág.

1. POLITICA PARA EL MANEJO DE LA NFORMACION 5
2. POLITICA DE USO DE RECURSOS TECNOLOGICOS 9
3. POLITICA DE ACCESO REMOTO 15
4. POLITICA DE ESCRITORIO Y PANTALLA LIMPIOS 17
5. POLITICA DE SEGURIDAD FISICA Y DEL ENTORNO 19
6. POLITICA DE CABLEADO ESTRUCTURADO Y FIBRA OPTICA 21
7. POLITICA DE COPIAS DE RESPALDO 23
8. POLITICA DE INTERCAMBIO DE INFORMACIÓN 25
9. POLITICA DE MANEJO DE INCIDENTES Y PETICIONES 27
10. POLITICA DE GESTION DE CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACION 29
11. POLITICA DE CUMPLIMIENTO 32
12. POLITICA DE CONTROL DE ACCESO 34
13. POLITICA DE SEGURIDAD CRIPTOGRAFICA 38
14. POLITICA DE GESTION DE MEDIOS REMOVIBLES 40
15. POLITICA DE DESARROLLO SEGURO 42
16. PROHIBICIONES 44

¿QUÉ VAMOS A ENCONTRAR?

Este documento tiene como objeto dar a conocer las políticas de Seguridad Informática que deben cumplir los usuarios de servicios de tecnologías, para proteger adecuadamente los activos de información de la Universidad Pedagógica y Tecnológica de Colombia.

De igual manera, establecen las reglas básicas con las cuales la UPTC debe manejar sus activos de información, a través de la implantación de normas y procedimientos, de modo que aumente la protección de éstos recursos. Así mismo, identifican responsabilidades y establecen requerimientos mínimos para una protección apropiada y consistente de los activos de información de la Institución.

En este documento se entiende como usuarios a la Comunidad Universitaria (funcionarios públicos, funcionarios oficiales, docentes, aspirantes, estudiantes, egresados, contratistas internos y externos) en General, que hacen uso de servicios de tecnología de la información de la Institución.

1.

POLÍTICA PARA EL MANEJO DE LA INFORMACIÓN

Esta política tiene como finalidad establecer las directrices para proteger la información contra uso no autorizado, divulgación o publicación, modificación, daño o perdida y establecer el cumplimiento de reglamentaciones y leyes aplicables a la Universidad Pedagógica y Tecnológica de Colombia.

1. POLÍTICA PARA EL MANEJO DE LA INFORMACIÓN

Acuerdos de Confidencialidad

- Los funcionarios y contratistas de la Institución, deben firmar acuerdos de confidencialidad al momento de realizar la legalización de sus respectivos contratos, en los cuales se comprometen a no divulgar, usar o explotar la información institucional a la cual tengan acceso.
- Los proveedores que requieran tener acceso a la información confidencial de la Institución, deben firmar el acuerdo. En caso de que el proveedor esté en desacuerdo con la firma de éste, no podrá tener acceso a la información requerida.

Propietario de la Información

La información institucional (artículos, revistas, contenidos de cursos, videos, fotos, información académica, entre otros) administrada, manejada o creada por los empleados de la Universidad, independiente de su forma de vinculación es de la UPTC, al igual que los Sistemas de Información desarrollados por personal interno o externo. La Institución es propietaria de los derechos de esta información.

Derechos de Autor

Está prohibido por las leyes de derechos de autor y por la UPTC, suprimir, alterar o hacer copias no autorizadas de software ya sea adquirido o desarrollado por la Universidad o de información institucional de propiedad intelectual en cualquier formato.

1. POLÍTICA PARA EL MANEJO DE LA INFORMACIÓN

Publicaciones de Seguridad de la Información

- Todos los usuarios de servicios de tecnologías de Información, deben aplicar las directrices dadas a través de publicaciones o comunicadas en capacitaciones o campañas Institucionales respecto a la Seguridad de la Información.
- La cuenta de correo electrónico debe ser usada para el desempeño de las funciones asignadas dentro de la UPTC, así mismo podrá ser utilizada para uso personal, siempre y cuando se realice de manera ética, razonable, responsable y sin afectar la productividad y confidencialidad.
- Los usuarios no deben propagar cadenas de mensajes o comunicaciones de tipo comercial, político, religioso y en general cualquier contenido ofensivo para los funcionarios de la Universidad.

- Es deber de los funcionarios verificar la identidad de todas aquellas personas, que soliciten y a quienes se les entregue información por teléfono, fax, dispositivos móviles, redes sociales, correo electrónico o correo certificado, entre otros.
- Los funcionarios de la Universidad deben cumplir con fidelidad como producto de las tareas que les fueron asignadas y guardar la discreción correspondiente, o la reserva absoluta con respecto a la información de la Institución de la cual tengan conocimiento en el ejercicio de sus funciones.
- Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definido por UPTC y deben conservar en todos los casos el mensaje legal corporativo de confidencialidad.

1. POLÍTICA PARA EL MANEJO DE LA INFORMACIÓN

Equipos de procesamiento de datos tipo servidor

- Los administradores de servidores, bases de datos y demás roles que manejen información clasificada como semiprivada y privada, deben garantizar la confidencialidad de la información y el uso de credenciales de administración (usuario y contraseña), sin excepción.
- La administración de los equipos de procesamiento de datos tipo servidor, que soportan servicios institucionales debe ser realizada por la Dirección de las Tecnologías de Sistemas de Información y de las Comunicaciones.
- Los servidores que no sean administrados por la Dirección de las Tecnologías y Sistemas de información y de las Comunicaciones, el responsable del activo de información, debe presentar por escrito a la Dirección de las Tecnologías y Sistemas de Información y las Comunicaciones los motivos y justificación por los cuales realizará dicha administración.

2.

POLITICA DE USO DE RECURSOS TECNOLOGICOS

Esta política pretende sensibilizar a la comunidad universitaria sobre el buen uso de los recursos tecnológicos y sistemas de información con lo que cuenta la Universidad; respetar la integridad física y lógica de los equipos informáticos y promover las buenas practicas que se deben llevar a cabo de acuerdo a la normatividad nacional vigente.

2. POLÍTICA DE USO DE RECURSOS TECNOLOGICOS

Instalación, Mantenimiento y Actualización de Hardware

El personal adscrito a la Dirección de las Tecnologías y Sistemas de Información y las Comunicaciones, es el único autorizado para instalar aplicaciones y realizar mantenimientos preventivos y correctivos en los equipos de cómputo de la Institución.

Uso de los Equipos de Cómputo

- Los equipos informáticos (Computadores, impresoras, portátiles, servidores, tablets, cámaras de video y fotografía, teléfonos móvil, discos duros, usbs y demás dispositivos móviles) de la Institución serán utilizados únicamente por el personal autorizado para el desarrollo de las actividades asignadas.
- Todo funcionario, contratista y/o docente de la Institución es responsable del equipo que le sea asignado; el cual será incluido a su inventario personal, de acuerdo con el procedimiento Egreso de Bienes de Almacén A-AB-P05.
- Los equipos informáticos (Computadores, impresoras, portátiles, tablets, cámaras de video y fotografía, teléfonos móvil, discos duros, usbs y demás dispositivos móviles) propiedad de la Universidad, no deben ser desatendidos. El usuario deberá tomar las medidas de seguridad pertinentes, que permitan garantizar la integridad y confidencialidad del activo de información.
- En caso de presentarse una falla o problema de hardware o software en una estación de trabajo, equipo portátil o dispositivo móvil, propiedad de la Universidad, el usuario responsable del mismo deberá informarlo a la Dirección de las Tecnologías y Sistemas de Información y las Comunicaciones, a través de la mesa de servicio, para una asistencia especializada y por ningún motivo, deberá intentar resolver el problema.

2. POLÍTICA DE USO DE RECURSOS TECNOLOGICOS

Artículo de Decoración en Equipos de Cómputo

Se debe mantener el equipo de cómputo libre de fotos, calcomanías y cualquier otro elemento que lo pueda deteriorar o comprometer su integridad.

Software en los Equipos de Cómputo

Para todos los equipos de cómputo propiedad de la Institución, se instalará únicamente el software que cuente con licencia autorizada para uso en la Universidad. El software que no cumpla con este lineamiento, se debe desinstalar de manera inmediata para garantizar el cumplimiento de la Ley antipiratería.

Software Antivirus

- Para todos los equipos de cómputo propiedad de la Institución, se instalará únicamente el software antivirus que la Dirección de las Tecnologías y Sistemas de Información y las Comunicaciones establezca.
- Los usuarios que hacen uso de los servicios de Tecnología de Información y Comunicación, deben realizar tareas de escaneo de archivos y directorios, no deben cambiar o eliminar la configuración del software de antivirus en los equipos de cómputo y dispositivos móviles propiedad de la Institución.
- Los usuarios no deben descargar archivos adjuntos que provengan de fuentes desconocidas, para evitar contaminación por virus informáticos y/o instalación de software malicioso en sus estaciones de trabajo, equipos portátiles o dispositivos móviles.

2. POLÍTICA DE USO DE RECURSOS TECNOLOGICOS

Aplicaciones de Ofimática

La suite de ofimática permitida por la Institución para equipos con sistema operativo Windows y Mac, son las versiones de Microsoft Office licenciadas por la Universidad. Se permite el uso de la versión libre de Open Office, en los equipos de cómputo propiedad de la Institución.

Sistemas propietarios Desarrollados en la Institución

La instalación de productos de software desarrollados por la Dirección de las Tecnologías y Sistemas de Información y de las Comunicaciones de la Universidad se realizará en los equipos de cómputo propiedad de la institución designados para tal fin.

Sistemas de Información de Entes de Control

El licenciamiento de los sistemas de información a través de los cuales se reporta información, es responsabilidad del ente de control respectivo.

2. POLÍTICA DE USO DE RECURSOS TECNOLOGICOS

Acceso a Código Fuente de Aplicaciones

- El acceso al código fuente está permitido únicamente a personal autorizado por la Dirección de las Tecnologías y Sistemas de Información y de las Comunicaciones. Si se trata de una aplicación desarrollada por un proveedor externo, se deben revisar las condiciones del contrato.
- Nadie, aunque tenga acceso, deberá realizar cambios al código fuente de las aplicaciones, sin previa autorización de la Dirección de las Tecnologías y Sistemas de Información y de las Comunicaciones.
- Ninguna dependencia esta autorizada para realizar adquisición o desarrollo de software de propósito particular por cuenta propia. Cualquier requerimiento en este sentido deberá gestionarse a través de la Dirección de las Tecnologías y Sistemas de Información y de las Comunicaciones.

Gestión de Cambios

Se deben documentar todos los cambios que se realicen a los recursos tecnológicos de la Universidad de acuerdo con el procedimiento A-RI-P10 Procedimiento para la Gestión de Cambios y Entregas.

Documentos de Pruebas

Se deben documentar todas las pruebas que se realicen a los recursos tecnológicos de la Institución. de acuerdo con el procedimiento A-RI-P10 Procedimiento para la Gestión de Cambios y Entregas

2. POLÍTICA DE USO DE RECURSOS TECNOLOGICOS

Monitoreo de Equipos

- La Institución se reserva el derecho de monitorear los equipos de cómputo, conectados a la red de datos de la universidad, de los cuales se sospeche que están comprometiendo la confidencialidad, integridad y disponibilidad de la información.
- La universidad dispone de un Data Center, como lugar adecuado para el alojamiento de los equipos de procesamiento de datos tipo servidor.
- La Dirección de las Tecnologías y Sistemas de Información y de las Comunicaciones gestiona el mantenimiento periódico para el Data Center junto con los elementos que lo componen, para garantizar la integridad, disponibilidad y confidencialidad de los activos de información que se encuentran allí alojados.
- Los usuarios no pueden portar información de la Universidad clasificada como privada, sin la previa autorización del propietario del activo de información independiente del medio que utilice.
- La instalación de un nuevo componente en la red de datos debe estar autorizada por la Dirección de las Tecnologías y Sistemas de Información y de las Comunicaciones.
- La adopción y uso de tecnologías de la información y la comunicación orientadas a la gestión de servicios institucionales, serán aprobados por la Dirección de las Tecnologías y Sistemas de Información y de las Comunicaciones.

3.

POLITICA DE ACCESO REMOTO

La presente política contempla las comunicaciones electrónicas y conexiones remotas de usuarios autorizados para acceder a los servicios de la red de datos institucional.

3. POLÍTICA DE ACCESO REMOTO

Política de Acceso Remoto

- El Servicio de acceso remoto permite el ingreso desde redes externas o internas a la red de datos institucional a aquellos usuarios expresamente autorizados por La Dirección de las Tecnologías y Sistemas de Información y de las Comunicaciones, el cual debe estar sujeto a autenticación con un nivel adecuado de protección.

4.

POLITICA DE ESCRITORIO Y PANTALLA LIMPIOS

Esta política aplica a la protección a todo tipo de información, que pueda estar contenida en escritorios, estaciones de trabajo, computadores, portátiles, dispositivos móviles, medios ópticos, medios magnéticos, documentos en papel y en general cualquier tipo de información que se utiliza para apoyar la realización de las actividades laborales. El objetivo es reducir los riesgos de acceso no autorizado, pérdida o daño a la información durante y fuera de las horas normales de trabajo.

4. POLÍTICA DE ESCRITORIO Y PANTALLA LIMPIOS

Política de Escritorio y Pantalla Limpios

- Todas las estaciones de trabajo deben usar el papel tapiz Institucional y contar con bloqueo de sesión automática después de 2 minutos de inactividad, el cual, debe mostrar la pantalla de inicio de sesión solicitando el ingreso del usuario y contraseña al ser reanudado.
- La información confidencial o sensible, cuando se imprime se debe retirar inmediatamente de las impresoras.
- Toda vez que el usuario se ausente de su lugar de trabajo, debe bloquear su estación de trabajo para proteger el acceso a las aplicaciones y servicios de la institución de personal no autorizado.
- Los datos sensibles almacenados en los equipos o sistemas de información, deberán encontrarse ubicados en rutas que no sean de fácil acceso.
- Al finalizar la jornada de trabajo, el usuario debe guardar en un lugar seguro los documentos y medios que contengan información confidencial o de uso interno, así mismo debe cerrar la sesión o salir de todas las aplicaciones correctamente y dejar los equipos apagados (no sólo el monitor).

5.

POLITICA DE SEGURIDAD FISICA Y DEL ENTORNO

Esta política establece las pautas a tener en cuenta para la protección de las áreas seguras relacionadas con las tecnologías de información.

5. POLÍTICA DE SEGURIDAD FISICA Y DEL ENTORNO

Política de Seguridad Física y del Entorno

- La Dirección de las Tecnologías y Sistemas de Información y de las Comunicaciones debe elaborar un listado del personal que por el rol de sus funciones está autorizado para ingresar a las áreas seguras.
- Únicamente ingresará al Data Center, área de desarrollo, C126, Centros de Cableados, Planta eléctrica y subestación el personal autorizado con los elementos necesarios para desarrollar sus labores.

- No se permiten las visitas al Data Center, área de desarrollo, C126, Centros de Cableados, Planta eléctrica y subestación a no ser que sea para llevar a cabo labores de mantenimiento o auditorias.
- No se debe proveer información sobre la ubicación de las áreas seguras como mecanismo de seguridad.

- Las puertas de acceso al Data Center, área de desarrollo, C126, Centros de Cableados, Planta eléctrica y subestación deben permanecer siempre cerradas y aseguradas, al igual que todos los gabinetes y puertas de los equipos que se encuentran en estos lugares.

6.

POLITICA DE CABLEADO ESTRUCTURADO Y FIBRA OPTICA

6. POLÍTICA DE INSTALACIÓN DE CABLEADO ESTRUCTURADO Y FIBRA OPTICA

Cableado Estructurado & Fibra Óptica

- Planeación, diseño, construcción, instalación, administración, mantenimiento y certificación del cableado estructurado y fibra óptica de telecomunicaciones de la Institución es responsabilidad del proceso Gestión de Recursos Informáticos, el cual debe cumplir con las normas técnicas o estándares adoptados por el mismo, con el fin de garantizar la integridad, conservar la estética y la seguridad de las redes.

7.

POLITICA DE COPIAS DE RESPALDO

El objeto de esta política es salvaguardar la información de manera responsable, con el fin de evitar posibles afectaciones en la disponibilidad e integridad de la misma.

7. POLÍTICA DE COPIAS DE RESPALDO

Copias de Seguridad

- La Dirección de las Tecnologías y Sistemas de Información y de las Comunicaciones debe respaldar con copias de seguridad la información Institucional que sea crítica, dichas copias deben ser tomadas y probadas de acuerdo al procedimiento A-RI-P03 Copias de Seguridad de la Información.
- La Dirección de las Tecnologías y Sistemas de Información y de las Comunicaciones debe garantizar copia de la información de configuración, contenida en la plataforma tecnológica de la Institución como equipos tipo servidores, equipos activos de red y dispositivos de red inalámbricos, dichas copias deben ser tomadas y probadas de acuerdo al procedimiento A-RI-P03 Copias de Seguridad de la Información.

- La Dirección de las Tecnologías y Sistemas de Información y de las Comunicaciones debe garantizar copia de los productos de software que administra, dichas copias deben ser tomadas y probadas de acuerdo al procedimiento A-RI-P03 Copias de Seguridad de la Información.
- Los medios magnéticos que tienen información crítica deben ser almacenados en otra ubicación diferente a las instalaciones donde se encuentra ubicada. El sitio externo donde se resguardan dichas copias, solo tendrá acceso la Dirección de las Tecnologías y Sistemas de Información y las Comunicaciones.

- Es responsabilidad exclusiva de los usuarios, la creación de copias de seguridad de archivos usados, custodiados o producidos por estos, teniendo en cuenta la Guía para Proteger Información en Equipos Computacionales A-RI-P03-G01.

8.

POLITICA DE INTERCAMBIO DE INFORMACIÓN

8. POLÍTICA DE INTERCAMBIO DE INFORMACION

Política de Intercambio de Información

- Toda información enviada a través del correo Institucional, debe incluir en su pie de página, una advertencia en cuanto a su uso y autorizaciones al respecto, quedando bajo responsabilidad del receptor el cuidado y resguardo de la información.
- Todo intercambio de información a través de acceso remoto, debe cumplir con la Política de Acceso Remoto establecida por la Institución.
- El intercambio de información privada o semiprivada por medio móviles no está permitido.

9.

POLITICA DE MANEJO DE INCIDENTES Y PETICIONES

9. POLÍTICA DE MANEJO DE INCIDENCIAS Y PETICIONES

Política de Incidencia & Peticiones

- Todos los incidentes y peticiones solicitados por los usuarios de la Institución, deben ser canalizados a través de la mesa de servicio.
- Toda la información relativa a los incidentes y peticiones reportados, debe ser manejada con total confidencialidad.
- La Dirección de las Tecnologías y Sistemas de Información y de las Comunicaciones reportará ante la autoridad competente los incidentes de seguridad que estén considerados como un delito informático.

10.

POLITICA DE GESTION DE CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACION

10. POLITICA DE GESTION DE CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACION

Política de Gestión de Continuidad de la Seguridad de la Información

- El líder del SGSI informará el plan de continuidad de la seguridad de la información a los procesos involucrados en el SGSI.
- El Plan de Continuidad de la seguridad de la información debe revisarse anualmente y realizar modificaciones si es necesario, dependiendo de los cambios y nuevos requerimientos en los procesos.
- El Data Center se debe proveer con unidades suplementarias de energía eléctrica (UPS) y se debe garantizar el óptimo funcionamiento de dichas unidades.
- Las copias de seguridad de los sistemas de computación que incluye sistema operativo, base de datos, aplicación, servicios, entre otros; deben ser almacenados en un lugar diferente de donde reside la información original, dentro de las instalaciones de la Universidad.

10. POLITICA DE GESTION DE CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACION

Política de Gestión de Continuidad de la Seguridad de la Información

- Debe realizarse mantenimiento preventivo y periódico a los equipos servidores, de comunicaciones y demás equipos en los cuales haya configurados servicios, de tal forma que el riesgo a fallas físicas se mantenga en una probabilidad de ocurrencia baja.
- Debe realizarse mantenimiento preventivo a intervalos programados a equipos de cómputo de los usuarios finales, propiedad de la Institución, para reducir el riesgo de falla.
- La Institución gestiona y ejecuta los planes de capacitación para garantizar la formación y actualización de los funcionarios de la Dirección de las Tecnologías y Sistemas de Información y de las Comunicaciones conforme a las necesidades de modernización tecnológica que se presenten y mantener la confidencialidad, disponibilidad e integridad de los diferentes activos de información de la institución, así como la continuidad en la prestación de servicios de Tecnología e Información.

11.

POLITICA DE CUMPLIMIENTO

11. POLITICA DE CUMPLIMIENTO

Política de Cumplimiento

- El líder del proceso Gestión Normativa tiene la responsabilidad de identificar la legislación vigente que debe cumplir la Universidad en función de la protección de la información y divulgar estos requerimientos. Además, debe servir de apoyo en la interpretación, asistencia y manejo de dicha legislación.

- Todos los funcionarios de la Universidad deben cumplir con la Normatividad vigente adoptada por la Institución, leyes de derechos de autor, ley de protección de datos personales, acuerdos de licenciamiento de software y acuerdos de confidencialidad.

12.

POLITICA DE CONTROL DE ACCESO

12. POLÍTICA DE CONTROL DE ACCESO

Política de Control de Acceso

- El control de acceso a todos los Sistemas de Información de la entidad y en general cualquier servicios de Tecnologías de Información, debe realizarse por medio de Credenciales de Acceso (Usuario y Contraseña), las cuales son de uso exclusivo e intransferible.
- Para la asignación y/o eliminación de credenciales de acceso de usuarios institucionales administrativos, docentes y contratistas se hará de acuerdo al procedimiento de vinculación de servidores públicos A-GH-P03 y entrega de cargos A-GH-P05, y se tendrá en cuenta los lineamientos por la Dirección de las Tecnologías y Sistemas de Información y las Comunicaciones en el procedimiento de Gestión de Identidad y Acceso A-RI-P20.

- El acceso a plataformas, aplicaciones, servicios y en general cualquier recurso de información de la UPTC, debe ser asignado de acuerdo a la identificación previa de requerimientos de seguridad y de la Institución, que se definan por las diferentes dependencias de la Universidad, así como normas legales o leyes aplicables a la protección de acceso a la información presente en los sistemas de información.
- El acceso lógico a equipo especializado de cómputo (servidores, enrutadores, bases de datos, etc.) conectado a la red es administrado por la Dirección de las Tecnologías y Sistemas de Información y las Comunicaciones.

- La asignación de la contraseña para acceso a sistemas, se debe realizar de forma individual, por lo que el uso de contraseñas compartidas está prohibido. Al revelar o compartir la contraseña el usuario autorizado se expone a responsabilizarse de acciones que otras personas hagan con su contraseña.
- Los usuarios son responsables de todas las actividades llevadas a cabo con su identificación de usuario y contraseña.

12. POLÍTICA DE CONTROL DE ACCESO

Política de Control de Acceso

- Es responsabilidad de los usuarios la privacidad de la contraseñas, por lo tanto, se recomienda no registrarlas en ningún medio impreso o escrito en el área de trabajo del usuario, ni almacenarlas en programas o sistemas, con el fin de evitar que las personas no autorizadas tengan conocimiento de las mismas..
- Los usuarios deben tener en cuenta las siguientes características para la construcción de sus contraseñas:

Que contenga mínimo ocho (8) caracteres, los cuales deben incluir letras mayúsculas, minúsculas, números y símbolos o caracteres especiales y que no contenga información de tipo personal (nombres, numero de documento, fecha de nacimiento, numero de teléfono, entre otros).

- Todo usuario que tenga la sospecha de que su contraseña es conocida por otra persona, tendrá la obligación de cambiarla inmediatamente.
- La Dirección de las Tecnologías y Sistemas de Información y de las Comunicaciones debe implementar en las bases de datos un límite de intentos consecutivos infructuosos para ingresar la contraseña.

12. POLÍTICA DE CONTROL DE ACCESO

Política de Control de Acceso

- Cuando un usuario bloquee su cuenta debido a la superación del número máximo de intentos, debe reportarlo a la Dirección de las Tecnologías y Sistemas de Información y de las Comunicaciones, indicando a que sistema de información, para que se le active la cuenta y restaure su contraseña.
- La activación de la cuenta y obtención de acceso a la contraseña debe hacerse de forma segura; el usuario deberá acreditarse ante la Dirección de las Tecnologías y Sistemas de Información y de las Comunicaciones como Usuario de la Universidad.
- Se debe hacer el cambio de las contraseñas proporcionadas por el fabricante (contraseñas por defecto) antes de poner en producción cualquier activo de información en la Institución

13.

POLITICA DE SEGURIDAD CRIPTOGRAFICA

La Universidad establece la presente Política de seguridad criptográfica, a fin de determinar su correcto uso.

13. POLÍTICA DE USO DE CONTROLES CRIPTOGRAFICOS

Política de Seguridad Criptográfica

- Las copias de seguridad de las Bases de Datos, gestionadas por los sistemas de información deben estar encriptadas.
- La información que se comunique entre el Backend y Frontend en los sistemas de información debe estar encriptada y la duración de las llaves que se utilicen para esa transmisión deben tener un tiempo máximo de 30 segundos.

14.

POLITICA DE GESTION DE MEDIOS REMOVIBLES

Esta política define las reglas para la protección de datos en diferentes medios de almacenamiento removible; considerando su administración y protección.

14. POLÍTICA DE GESTION DE MEDIOS REMOVIBLES

Política de Gestión de Medios Removibles

- El usuario que tenga asignados medios removibles, tendrá la responsabilidad de tomar las medidas adecuadas para su custodia, con el fin de protegerlos de daño o pérdida y de accesos no autorizados si estos contienen información sensible o confidencial.
- Los medios removibles deben ser escaneados cada vez que sea conectado a un equipo de la red de la Universidad, especialmente en lo concerniente a posible código malicioso.
- Debe formatearse el medio removible cuando la información pierda vigencia de acuerdo al Procedimiento A-RI-P23 Eliminación Segura de la Información.

15.

POLITICA DE DESARROLLO SEGURO

15. POLÍTICA DE DESARROLLO DE SEGURO

Desarrollo Seguro

- La Dirección de las Tecnologías y Sistemas de Información y las Comunicaciones debe elaborar, mantener y aplicar un procedimiento para la incorporación de sistemas de información, el cual debe incluir lineamientos, procesos, buenas prácticas, plantillas y guías que sirvan para regular los desarrollos de productos de software internos en un ambiente de aseguramiento de calidad.
- Los productos de software adquiridos a través de terceras partes deben cumplir con el procedimiento de incorporación de sistemas de información establecido por la Universidad.

Acceso a Código Fuente de Aplicaciones

- El acceso al código fuente está permitido únicamente a personal autorizado por la Dirección de las Tecnologías y Sistemas de Información y de las Comunicaciones. Si se trata de una aplicación desarrollada por un proveedor externo, se deben revisar las condiciones del contrato.
- Nadie, aunque tenga acceso, deberá realizar cambios al código fuente de las aplicaciones, sin previa autorización de la Dirección de las Tecnologías y Sistemas de Información y de las Comunicaciones.
- Ninguna dependencia esta autorizada para realizar adquisición o desarrollo de software de propósito particular por cuenta propia. Cualquier requerimiento en este sentido deberá gestionarse a través de la Dirección de las Tecnologías y Sistemas de Información y de las Comunicaciones.

16.

PROHIBICIONES

16. PROHIBICIONES

Prohibiciones

- Queda prohibido el uso de cualquier herramienta o mecanismo de monitoreo de la red de manera no autorizada, así como evadir los mecanismos de seguridad, autenticación, autorización o de auditoría de cualquier servicio de red, aplicación, servidor o cuenta de usuario.
- Está prohibida la utilización de la infraestructura tecnológica de la Universidad para llevar a cabo algún tipo de acoso, difamación, calumnia o cualquier forma de actividad hostil en contra de los integrantes de la comunidad universitaria y, en general, de cualquier persona o institución.
- Queda prohibida la instalación de puntos de acceso inalámbricos no autorizados en la Institución.
- La infraestructura tecnológica de la Universidad es para el desarrollo de los procesos institucionales exclusivamente. Por lo tanto, está prohibido el uso de estos recursos con fines personales o de lucro.
- No se exime a los usuarios de la responsabilidad disciplinaria y legal correspondiente de toda aquella acción que no esté aquí documentada y pueda afectar la Seguridad de la Información de la Institución.