



Rectoría

OFICINA DE PLANEACIÓN Y SISTEMAS



POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Universidad de Caldas
Enero de 2023

Versión 2.0



ucaldas@ucaldas.edu.co



www.ucaldas.edu.co



PBX (57) (6) 878 15 00



Calle 65 # 26 - 10 | Manizales - Colombia



TABLA DE CONTENIDO

OBJETIVO..... 9

ALCANCE 10

DEFINICIONES..... 11

PRINCIPIOS..... 15

POLÍTICAS 17

 Objetivo de las políticas..... 17

 Alcance de las políticas..... 17

1. Políticas de Uso de Recursos Informáticos 18

 1.1. Instrucciones para el uso de recursos informáticos..... 18

 1.2 Uso personal de los recursos informáticos..... 18

 1.3 Acuerdo de confidencialidad firmado para entrega de nombre de usuario..... 18

 1.4 Prohibición de instalación y desinstalación de software y hardware en los computadores de la organización..... 18

 1.5 Uso del aplicativo entregado..... 18

 1.6 El usuario es responsable por toda actividad que involucre su identificación personal o recursos informáticos asignados..... 18

 1.7 Declaración de reserva de derechos de LA UNIVERSIDAD 19

 1.8 Recursos compartidos..... 19

 1.9 Todo monitoreo debe ser registrado e informado al jefe inmediato del usuario..... 19

 1.10 Acceso no autorizado a los sistemas de información de la Entidad..... 19

 1.11 Posibilidad de acceso no implica permiso de uso..... 19

 1.12 Prohibición a la explotación de vulnerabilidades de seguridad de los recursos informáticos..... 20

 1.13 Dejar sistemas sensibles desatendidos..... 20

 1.14 Notificación de sospecha de pérdida, divulgación o uso indebido de información sensible..... 20



| | | |
|-------|--|----|
| 1.15 | Etiquetado y presentación de información de tipo confidencial a los usuarios de computadores. | 20 |
| 1.16 | El traslado de equipos debe estar autorizado. | 20 |
| 1.17 | Control de recursos informáticos entregados a los usuarios. | 20 |
| 1.18 | Precauciones para el uso de los recursos informáticos. | 21 |
| 1.19 | Solicitud de préstamo de recursos informáticos. | 21 |
| 1.20 | Configuración de sistema operativo de las estaciones de trabajo. | 21 |
| 1.21 | Uso restringido de modems en las estaciones de trabajo. | 21 |
| 1.22 | Uso de acceso telefónico a redes y conexión a la red LAN concurrentemente. | 21 |
| 1.23 | Niveles de seguridad de los elementos usados en los canales | 21 |
| 1.24 | Reporte de incidencias | 21 |
| 2. | Políticas de Uso de las Contraseñas..... | 22 |
| 2.1. | Confidencialidad de las contraseñas. | 22 |
| 2.2. | Uso de diferentes contraseñas para diferentes recursos informáticos. | 23 |
| 2.3. | Identificación única para cada usuario. | 23 |
| 2.4. | Cambios periódicos de contraseñas. | 23 |
| 2.5. | Longitud mínima de contraseñas. | 23 |
| 2.6. | Contraseñas deben ser difíciles de adivinar. | 23 |
| 2.7. | Prohibición de contraseñas cíclicas. | 23 |
| 2.8. | Las contraseñas creadas por usuarios no deben ser reutilizadas. | 23 |
| 2.9. | Almacenamiento de contraseñas. | 24 |
| 2.10. | Almacenamiento seguro de contraseñas. | 24 |
| 2.11. | Sospechas de compromiso deben forzar cambios de contraseña. | 24 |
| 2.12. | Revelación de contraseñas prohibida. | 24 |
| 2.13. | Auditoría periódica a las contraseñas de los usuarios. | 24 |
| 2.14. | Todas las estaciones deben tener un sistema de control de acceso. | 24 |
| 2.15. | Uso obligatorio de contraseña en el protector de pantalla. | 24 |
| 2.16. | Uso de papel tapiz y protector de pantalla. | 25 |
| 2.17. | Reporte de cambio en las responsabilidades de los usuarios al Administrador de Seguridad. | 25 |
| 3. | Políticas de Uso de la Información..... | 25 |
| 3.1. | Divulgación de la información manejada por los usuarios de LA UNIVERSIDAD..... | 25 |





- 3.2. Transferencia de datos solo a organizaciones con suficientes controles.25
- 3.3. Registro de las compañías que reciben información privada.25
- 3.4. Eliminación regular de la información que no se necesita.....25
- 3.5. Transferencia de la custodia de información de un funcionario que deja LA UNIVERSIDAD.....26
- 3.6. Transporte de datos sensibles en medios legibles.....26
- 3.7. Datos sensibles enviados a través de redes externas deben estar encriptados.26
- 4. Políticas del Uso de Internet y Correo Electrónico26
- 4.1. Prohibición de uso de Internet para propósitos personales.26
- 4.2. Formalidad del correo electrónico.....26
- 4.3. Preferencia por el uso del correo electrónico.....26
- 4.4. Uso de correo electrónico.....26
- 4.5. Revisión del correo electrónico.....27
- 4.6. Mensajes prohibidos.27
- 4.7. Restricción para el envío masivo de mensajes de correo electrónico a nivel interno. 27
- 4.8. Restricción para el envío masivo de mensajes de correo electrónico a nivel externo. 27
- 4.9. Acciones para frenar el SPAM.27
- 4.10. Direcciones de correo institucionales.27
- 4.11. Todo buzón de correo debe tener un responsable.27
- 4.12. Enviando software e información sensible a través de Internet.....28
- 4.13. Intercambio de información a través de Internet.28
- 5. Políticas de la Intranet y Sitios Web de LA UNIVERSIDAD28
- 5.1. Reglas de uso de la Intranet.....28
- 5.2. Prohibición de publicitar la imagen de LA UNIVERSIDAD en sitios diferentes a los institucionales.....28
- 5.3. Prohibición establecer conexiones a los sitios web de LA UNIVERSIDAD.....28
- 5.4. Prohibición de anuncios en sitios web particulares.....28
- 6. Políticas Generales de la Oficina Asesora de Planeación y Sistemas.....29
- 6.1. Cuándo realizar valoración de riesgos.....29
- 6.2. Restricción por acceso telefónico e Internet sobre recursos tecnológicos de uso interno a clientes externos.....29



6.3. Los computadores multiusuario y sistemas de comunicación deben tener controles de acceso físico apropiados.....29

6.4. Entrenamiento compartido para labores técnicas críticas.....29

6.5. Preparación y mantenimiento de planes para la recuperación de desastres y para respuesta a emergencias.....29

6.6. Personal competente en el Centro de Cómputo para dar pronta solución a problemas.....30

6.7. Chequeo de virus en archivos recibidos en correo electrónico.....30

7. Políticas para Desarrolladores de Software.....30

7.1. Ambientes separados de producción y desarrollo.....30

7.2. Cumplimiento del procedimiento para cambios y/o actualizaciones.....30

7.3. Documentación de cambios y/o actualizaciones.....30

7.4. Catalogación de programas.....30

7.5. Medidas de seguridad deben ser implantadas y probadas antes de entrar en operación.....30

7.6. Incorporación de contraseñas en el software.....31

7.7. Acceso del usuario a los comandos del sistema operativo.....31

7.8. Se requieren registros de auditoría en sistemas que manejan información sensible. 31

7.9. Registros para los usuarios privilegiados en los sistemas en producción que lo permitan.....31

7.10. Los registros del sistema deben incluir eventos relevantes para la seguridad.....31

7.11. Resistencia de los registros contra desactivación, modificación y eliminación.....31

7.12. Procesos controlados para la modificación de información del negocio en producción.....31

7.13. Validación de entradas en los desarrollos.....32

7.14. Diseño de seguridad para aplicaciones.....32

7.15. Personas autorizadas para leer los registros de auditoría.....32

7.16. histórico de contraseñas.....32

8. Políticas para Administradores de Sistemas32

8.1. Soporte para usuarios con privilegios especiales.....32

8.2. Los privilegios de acceso a los sistemas de información otorgados a un usuario terminan cuando el usuario finaliza su vínculo contractual con la universidad.....33



| | | |
|-------|--|----|
| 8.3. | Cuando y como pueden asignar contraseñas los administradores | 33 |
| 8.4. | Límite de intentos consecutivos de ingreso al sistema..... | 33 |
| 8.5. | Cambio de contraseñas por defecto..... | 33 |
| 8.6. | Cambio de contraseñas después de compromiso detectado en un sistema multiusuario..... | 33 |
| 8.7. | Brindar acceso a personal externo..... | 33 |
| 8.8. | Acceso a terceros a los sistemas de la organización requiere de un contrato firmado..... | 34 |
| 8.9. | Restricción de administración remota a través de Internet..... | 34 |
| 8.10. | Dos usuarios requeridos para todos los administradores..... | 34 |
| 8.11. | Privilegios por defecto de usuarios y necesidad de aprobación explícita por escrito. 34 | |
| 8.12. | Negación por defecto de privilegios de control de acceso a sistemas cuyo funcionamiento no es apropiado..... | 34 |
| 8.13. | Remoción de software para la detección de vulnerabilidades cuando no esté en uso. 34 | |
| 8.14. | Manejo administrativo de seguridad para todos los componentes de la red..... | 34 |
| 8.15. | Información a capturar cuando crimen informático o abuso es sospechado..... | 34 |
| 8.16. | Sincronización de relojes para un registro exacto de eventos en la red..... | 35 |
| 8.17. | Revisión regular de los registros del sistema..... | 35 |
| 8.18. | Confidencialidad en la información relacionada con investigaciones internas.... | 35 |
| 8.19. | Información con múltiples niveles de clasificación en un mismo sistema..... | 35 |
| 8.20. | Segmentación de recursos informáticos por prioridad de recuperación..... | 35 |
| 8.21. | Software de identificación de vulnerabilidades..... | 35 |
| 8.22. | En dónde usar controles de acceso para sistemas informáticos..... | 35 |
| 8.23. | Mantenimiento preventivo en computadores y sistemas de comunicación..... | 36 |
| 9. | Políticas de Backup | 36 |
| 9.1. | Período de almacenamiento de registros de auditoría..... | 36 |
| 9.2. | Tipo de datos a los que se les debe hacer backup y con qué frecuencia..... | 36 |
| 9.3. | Dos copias de información sensible..... | 36 |
| 10. | Políticas de Uso de Firewall | 36 |
| 10.1. | Detección de intrusos..... | 36 |
| 10.2. | Toda conexión externa debe estar protegida por el firewall..... | 37 |



| | | |
|--------|--|----|
| 10.3. | Toda conexión desde y hacia Internet debe pasar por el Firewall..... | 37 |
| 10.4. | Filtrado de contenido activo en el Proxy. | 37 |
| 10.5. | Segmentación de la red. | 37 |
| 10.6. | Inventario de conexiones. | 37 |
| 10.7. | El sistema interno de direccionamiento de red no debe ser público..... | 37 |
| 10.8. | Revisión periódica y reautorización de privilegios de usuarios..... | 37 |
| 11. | Políticas para Usuarios Externos | 38 |
| 11.1. | Términos y condiciones para clientes de Internet..... | 38 |
| 11.2. | Acuerdos con terceros que manejan información o cualquier recurso informático de LA UNIVERSIDAD..... | 38 |
| 11.3. | Definición clara de las responsabilidades de seguridad informática de terceros. 38 | |
| 12. | Políticas de Acceso Físico..... | 39 |
| 12.1. | Cuando se requiera que las puertas del Centro de Cómputo estén abiertas, debe estar presente la Oficina Asesora de Planeación y Sistemas. | 39 |
| 12.2. | Permitir paso a través de puertas controladas. | 39 |
| 12.3. | Se requiere cumplir el procedimiento por parte de todos los usuarios al visitar el Centro de Cómputo..... | 39 |
| 12.4. | Control de acceso físico para áreas que contienen información sensible. | 39 |
| 12.5. | Las puertas deben estar cerradas con llave cuándo las oficinas personales no estén siendo utilizadas. | 39 |
| 12.6. | Controles de acceso en áreas que contienen información sensible..... | 39 |
| 12.7. | Reporte de pérdida o robo de identificación. | 39 |
| 12.8. | Obligación de portar el carnet..... | 40 |
| 12.9. | Prohibición a los intentos de acceso físico a zonas restringidas. | 40 |
| 12.10. | Orden de salida para equipos electrónicos..... | 40 |
| 12.11. | Toda persona debe mostrar sus maletines al ingresar o salir de la oficina..... | 40 |
| 12.12. | Mantenimiento de los registros de ingreso. | 40 |
| 12.13. | Cuando se da una terminación laboral, los privilegios de acceso al edificio deben ser revocados. | 40 |
| 13. | Política de gestión de activos | 40 |
| 13.1. | Inventario de Activos | 40 |
| 13.2. | Protección | 41 |





| | | |
|--|---|----|
| 13.3. | Archivos de Gestión | 41 |
| 13.4. | Devolución de los Activos | 41 |
| 13.5. | Gestión de medios removibles | 41 |
| 13.6. | Disposición de los activos..... | 41 |
| 13.7. | Dispositivos móviles | 41 |
| 14. | Política de seguridad de las operaciones..... | 42 |
| CAPACITACIÓN Y SENSIBILIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN..... | | 42 |
| ACTUALIZACIÓN DE LA POLÍTICA DE SEGURIDAD INFORMÁTICA..... | | 43 |
| LISTADO DE ANEXOS..... | | 43 |



OBJETIVO

El objetivo de este capítulo de POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN es el de establecer y definir los principios, procedimientos, lineamientos, responsabilidades, procesos, funciones, etapas, estructura Organizacional, capacitación y concientización frente a los riesgos de seguridad y privacidad de la información para una gestión efectiva en la Universidad de Caldas, en consonancia de lo establecido en la Guía Nro 2 de elaboración de la Política General de Seguridad y Privacidad de la Información.

Este manual deberá ajustarse y actualizarse con la participación de los integrantes del comité de Seguridad y Privacidad de la Información en la medida que las circunstancias y las necesidades lo ameriten, para la obtención de objetivos institucionales previstos en el buen servicio y los intereses de los clientes y usuarios.

Objetivos Específicos:

- Establecer los principios, procedimientos y lineamientos para la gestión de la seguridad y privacidad de la Información.
- Establecer los principios y lineamientos para promover la cultura de la seguridad y la privacidad de la información al interior de la Universidad.
- Documentar las responsabilidades, procesos, procedimientos y etapas frente a la gestión de seguridad y privacidad de la información.
- Definir las funciones, roles y responsabilidades de la unidad de seguridad y privacidad de la Información "USPI".
- Asegurar el cumplimiento de normas, leyes y regulaciones, aplicables a la Universidad de Caldas, en términos de Seguridad y Privacidad de la Información.
- Asegurar la disposición de los recursos técnicos y humanos necesarios para la gestión efectiva de los riesgos de seguridad y privacidad de la información.
- Definir la estrategia de comunicación, difusión, capacitación y sensibilización hacia los funcionarios y demás partes interesadas involucrados con los servicios prestados por la organización.





Rectoría

ALCANCE

Esta política aplica a toda la entidad, sus funcionarios, contratistas, terceros de la Universidad de Caldas y la ciudadanía en general.



ucaldas@ucaldas.edu.co

www.ucaldas.edu.co

PBX (57) (6) 878 15 00

Calle 65 # 26 - 10 | Manizales - Colombia



DEFINICIONES

Acuerdo de Confidencialidad: Es un documento que debe suscribir todo usuario con el objeto de lograr el acceso a recursos informáticos de LA UNIVERSIDAD

Administradores: Usuarios a quienes LA UNIVERSIDAD ha otorgado funciones de administración de los recursos informáticos y que poseen un identificador que les permite tener privilegios administrativos sobre los recursos informáticos, quienes estarán bajo la Oficina Asesora de Planeación y Sistemas.

Backup: Copia de la información en un determinado momento, que puede ser recuperada con posterioridad.

Contraseña: Clave de acceso a un recurso informático.

Desarrolladores: Son los usuarios encargados de diseñar, elaborar y probar el código de las aplicaciones para cumplir con el objetivo de las mismas, así como los auditores que desarrollan programas y pruebas para validar la efectividad de dichas aplicaciones.

Estándar: Regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares son orientaciones obligatorias que buscan hacer cumplir las políticas. Los estándares son diseñados para promover la implementación de las políticas de alto nivel de la entidad antes de crear nuevas políticas.

Firewall: Conjunto de recursos de hardware y software que protegen recursos informáticos de accesos indebidos.

Guía: Una guía es una declaración general utilizada para recomendar o sugerir un enfoque para implementar políticas, estándares, buenas prácticas. Las guías son esencialmente, recomendaciones que deben considerarse al implementar la seguridad. Aunque no son obligatorias, serán seguidas a menos que existan argumentos documentados y aprobados para no hacerlo.

Información confidencial: Información generada por LA UNIVERSIDAD, que debe ser conocida solamente por un grupo autorizado de funcionarios de la misma. El acceso a este tipo de información debe ser restringido y basado en el principio del menor privilegio. Su divulgación a terceros requiere permiso del dueño y de acuerdos de confidencialidad. Así mismo, su divulgación no autorizada puede causar daños importantes a la Entidad. Todo material generado durante la creación de copias de este tipo de información (ejemplo, mala calidad de impresión), debe ser destruido.



Información privada (solo para uso interno): Información generada por LA UNIVERSIDAD, que no debe ser conocida por el público en general. Su divulgación no autorizada no causa grandes daños a la Entidad y es accesible por todos los usuarios por medio de la Intranet.

Información pública: Es la información administrada por LA UNIVERSIDAD, que está a disposición del público en general; un ejemplo son los catálogos de productos y servicios.

LAN: Grupo de computadores y dispositivos asociados que comparten un mismo esquema de comunicación y se encuentran dentro de una pequeña área geográfica (un edificio o una oficina).

Mejor Práctica: Una regla de seguridad específica o una plataforma que es aceptada, a través de la industria al proporcionar el enfoque más efectivo a una implementación de seguridad concreta. Las mejores prácticas son establecidas para asegurar que las características de seguridad de los sistemas utilizados con regularidad estén configurados y administrados de manera uniforme, garantizando un nivel consistente de seguridad a través de la entidad.

Módem (Modulador - Demodulador de señales): Elemento de comunicaciones que permite transferir información a través de líneas telefónicas fijas o celulares.

Monitoreo: Verificación de las actividades de un usuario con respecto a los recursos informáticos de la Entidad.

OTP (One Time Password): Contraseña entregada por el administrador de un recurso informático que permite el primer acceso a dicho recurso y obliga al usuario a cambiarla una vez ha hecho este acceso.

Plan de contingencia: Plan que permite el restablecimiento ágil en el tiempo de los servicios asociados a los Sistemas de Información de LA UNIVERSIDAD en casos de desastres y otros casos que impidan el funcionamiento normal.

Política: Declaración de alto nivel que describe la posición de la entidad sobre un tema específico.

Procedimiento: Los procedimientos, definen específicamente como las políticas, estándares, mejores prácticas y guías que serán implementadas en una situación dada. Los procedimientos son independientes de la tecnología o de los procesos y se refieren a las plataformas, aplicaciones o procesos específicos. Son utilizados para delinear los pasos que deben ser seguidos por una dependencia para implementar la seguridad relacionada con dicho proceso o sistema específico. Generalmente los procedimientos son desarrollados, implementados y supervisados por el dueño del proceso o del sistema, los procedimientos seguirán las políticas de la entidad, los estándares, las mejores prácticas y las guías tan cerca como les sea posible,



y a la vez se ajustarán a los requerimientos procedimentales o técnicos establecidos dentro de la dependencia donde ellos se aplican.

Protector de pantalla: Programa que se activa a voluntad del usuario ó automáticamente después de un tiempo en el que no ha habido actividad.

Proxy: Servidor que actúa como puerta de entrada a la Red Internet.

Recursos informáticos: Son aquellos elementos de tecnología de Información tales como: computadores servidores de aplicaciones y de datos, computadores de escritorio, computadores portátiles, elementos de comunicaciones, elementos de los sistemas de imágenes, elementos de almacenamiento de información, programas y datos.

Router: Equipo que permite la comunicación entre dos o más redes de computadores.

Seguridad informática: Es el proceso mediante el cual LA UNIVERSIDAD aplica sistemáticamente las políticas, procedimientos y las prácticas con el fin de asegurar los recursos informáticos.

Sesión: Conexión establecida por un usuario con un Sistema de Información.

Sistema de control de acceso: Elementos de hardware o software que autorizan o niegan el acceso a los recursos informáticos de acuerdo con políticas definidas.

Sistema de detección de intrusos (IDS): Es un conjunto de hardware y software que ayuda en la detección de accesos o intentos de acceso no autorizados a los recursos informáticos de LA UNIVERSIDAD

Sistema de cifrado: Elementos de hardware o software que permiten cifrar la información, para evitar que usuarios no autorizados tengan acceso a la misma.

Sistema multiusuario: Computador y su software asociado, que permiten atender múltiples usuarios a la vez a través de las redes de comunicación.

Sistema operativo: Software que controla los recursos físicos de un computador.

Sistema sensible: Es aquel que administra información confidencial ó de uso interno que no debe ser conocida por el público en general.

Usuario: Toda persona que pueda tener acceso a un recurso informático de LA UNIVERSIDAD





Usuarios de red y correo: Usuarios con los cuales LA UNIVERSIDAD ha establecido un contrato de al menos 30 días de duración y a quienes se les entrega un identificador de cliente para acceso a sus recursos informáticos.

Usuarios externos: Son aquellos clientes externos que utilizan los recursos informáticos de LA UNIVERSIDAD a través de Internet o de otros medios y tienen acceso únicamente a información clasificada como pública.

Usuarios externos con contrato: Usuarios externos con los cuales LA UNIVERSIDAD establece un contrato y a quienes se da acceso limitado a recursos informáticos de uso interno.



ucaldas@ucaldas.edu.co

www.ucaldas.edu.co

PBX (57) (6) 878 15 00

Calle 65 # 26 - 10 | Manizales - Colombia



PRINCIPIOS

La dirección de la Universidad de Caldas, 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 de Caldas, 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 la universidad 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:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus clientes, socios y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de la Universidad de Caldas.
- Garantizar la continuidad del negocio frente a incidentes.
- la Universidad de Caldas 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 del negocio, y a los requerimientos regulatorios.

Finalmente es de gran ayuda incluir la descripción general de otras políticas relevantes para el cumplimiento de los Objetivos planteados dentro del proyecto del SGSI ya que éstas son el apoyo sobre el cual se desarrolla; éstas deben ser descritas de forma sencilla, puntual y muy efectiva.



A continuación, se establecen 12 principios de seguridad que soportan el SGSI de la Universidad de Caldas:

- Las **responsabilidades** frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de **los empleados, proveedores, socios de negocio o terceros**.
- La Universidad de Caldas **protegerá la información** generada, procesada o resguardada por los procesos de negocio, su infraestructura tecnológica y activos del riesgo que se genera de los accesos **otorgados a terceros** (ej.: proveedores o clientes), o como resultado de un servicio interno en outsourcing.
- La Universidad de Caldas **protegerá la información** creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un **uso incorrecto** de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
- La Universidad de Caldas **protegerá su información** de las amenazas originadas por parte **del personal**.
- La Universidad de Caldas **protegerá las instalaciones** de procesamiento y la infraestructura tecnológica **que soporta sus procesos críticos**.
- La Universidad de Caldas **controlará la operación** de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- La Universidad de Caldas **implementará control de acceso** a la información, sistemas y recursos de red.
- La Universidad de Caldas garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- La Universidad de Caldas garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
- La Universidad de Caldas **garantizará la disponibilidad** de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.
- La Universidad de Caldas garantizará el cumplimiento de las **obligaciones legales, regulatorias y contractuales establecidas**.



POLÍTICAS

Objetivo de las políticas

La Alta Dirección, consciente que los recursos tecnológicos son utilizados hoy en día de manera permanente por los usuarios de LA UNIVERSIDAD definidos en este documento, han considerado oportuno transmitir a los mismos a las normas de comportamiento básicas en la utilización de los equipos de cómputo y demás recursos tecnológicos.

Las políticas de seguridad informática tienen como objetivo:

- Reducir el riesgo de incidentes de seguridad y minimizar su efecto.
- Establecer las reglas básicas con las cuales la organización debe operar sus recursos informáticos.
- Formación de las políticas de seguridad informática encaminada a disminuir y eliminar muchos factores de inseguridad, principalmente el riesgo de ocurrencia.

Alcance de las políticas

Estas normas son de obligatorio cumplimiento por parte de todos los usuarios de recursos informáticos y se han clasificado en:

- Políticas de uso de recursos informáticos.
- Políticas de contraseñas.
- Políticas de uso de información.
- Políticas de uso de internet y correo electrónico.
- Políticas de uso de Intranet y sitios Web.
- Políticas generales de la Oficina Asesora de Planeación y Sistemas.
- Políticas para desarrolladores de software
- Políticas para administradores de sistemas
- Políticas de Backup
- Detección de intrusos
- Políticas para usuarios externos
- Políticas de acceso físico

Respecto a las políticas de protección de datos personales, estas se encuentran publicadas en la URL:

http://www.ucaldas.edu.co/docs/2015/acuerdo_31_10_sep_proteccion_bases_datos.pdf y hacen parte integral del presente documento en lo relacionado con la privacidad de los datos en cumplimiento de la Ley 1581 de 2012 y demás normas concordantes.



1. Políticas de Uso de Recursos Informáticos

1.1. Instrucciones para el uso de recursos informáticos.

El uso del computador personal y demás recursos informáticos por parte de los funcionarios debe someterse a todas las instrucciones técnicas, que imparta la Oficina Asesora de Planeación y Sistemas.

1.2 Uso personal de los recursos informáticos.

Los recursos informáticos de LA UNIVERSIDAD sólo deben ser usados para fines laborales. El producto del uso de dichos recursos tecnológicos será de propiedad de LA UNIVERSIDAD y estará catalogado como lo consagra el presente documento. Cualquier otro uso está sujeto a autorización previa por la Oficina Asesora de Planeación y Sistemas.

1.3 Acuerdo de confidencialidad firmado para entrega de nombre de usuario.

Todo usuario debe firmar un acuerdo de confidencialidad y un acuerdo de la seguridad de los sistemas de información antes de otorgarle su identificación de usuario y contraseña y sus respectivos privilegios para el uso de los recursos tecnológicos de LA UNIVERSIDAD.

1.4 Prohibición de instalación y desinstalación de software y hardware en los computadores de la organización.

La instalación o desinstalación de hardware o software, la reparación o retiro de cualquier parte o elemento en los equipos de computación o demás recursos informáticos solo puede ser realizada por los funcionarios autorizados de la Oficina Asesora de Planeación y Sistemas.

1.5 Uso del aplicativo entregado.

LA UNIVERSIDAD ha suscrito con los fabricantes y proveedores un contrato de “LICENCIA DE USO” para los aplicativos que utiliza. Está terminantemente prohibido copiar cualquiera de los aplicativos que se aloja en los computadores o medios de almacenamiento de LA UNIVERSIDAD.

1.6 El usuario es responsable por toda actividad que involucre su identificación personal o recursos informáticos asignados.

Todo usuario es responsable por todas las actividades relacionadas con su identificación. La identificación no puede ser usada por otro individuo diferente a quien fue otorgada. Los usuarios no deben permitir que otros usuarios realicen labores bajo su identidad. De forma similar, los usuarios no deben realizar actividades bajo la identidad de alguien más. La utilización de los



recursos informáticos por parte de terceras personas con conocimiento o consentimiento del usuario, o por su descuido o negligencia, lo hace responsable de los posibles daños que estas personas ocasionen a los equipos o a la propiedad de LA UNIVERSIDAD.

1.7 Declaración de reserva de derechos de LA UNIVERSIDAD

LA UNIVERSIDAD usa controles de acceso y otras medidas de seguridad para proteger la confidencialidad, integridad y disponibilidad de la información manejada a través de los computadores y sistemas de información. Para mantener estos objetivos, LA UNIVERSIDAD se reserva el derecho y la autoridad de:

- Restringir o revocar los privilegios de cualquier usuario;
- Inspeccionar, copiar, remover cualquier dato, programa u otro recurso que vaya en contra de los objetivos antes planteados;
- Tomar cualquier medida necesaria para manejar y proteger los sistemas de información de LA UNIVERSIDAD. Esta autoridad se puede ejercer con o sin conocimiento de los usuarios, bajo la responsabilidad de la Oficina Asesora de Planeación y Sistemas o de quién le sea delegada esta función.

1.8 Recursos compartidos.

Está **terminantemente prohibido** compartir los discos duros o las carpetas de los computadores de escritorio, aunque estén protegidos por contraseña. Así mismo, solamente en los casos donde la información se clasificada como pública, podrá exponerse en los portales o herramientas de la Universidad. Para los demás casos, se debe revisar la clasificación de los activos de información para la publicación según allí se estipule el acceso, bien sea a través de la red de la Universidad o a través de repositorios en la nube.

1.9 Todo monitoreo debe ser registrado e informado al jefe inmediato del usuario.

Un usuario puede ser monitoreado bajo previa autorización de la autoridad respectiva.

1.10 Acceso no autorizado a los sistemas de información de la Entidad.

Los usuarios tienen la prohibición de obtener acceso a sistemas de información a los que no se tiene privilegios y de alguna forma dañar o alterar la operación de dichos sistemas. Esto implica la prohibición de capturar contraseñas, llaves de cifrado y otros mecanismos de control acceso que le puedan permitir obtener acceso a sistemas no autorizados. Se excluye lo estipulado en la política 4.4.13 “Auditoría periódica a las contraseñas de los usuarios”.

1.11 Posibilidad de acceso no implica permiso de uso.

Los usuarios no deben leer, modificar, copiar o borrar información perteneciente a otro usuario sin la debida autorización de este.



1.12 Prohibición a la explotación de vulnerabilidades de seguridad de los recursos informáticos.

A no ser que exista una aprobación por escrito para ello o sea parte de su función laboral, los usuarios no deben explotar las deficiencias de seguridad de los sistemas de información para dañar los sistemas o la información contenida en ellos, obtener acceso a recursos a los cuales no se le ha dado acceso. En el caso de encontrar vulnerabilidades, estas deben ser reportadas de inmediato a la Oficina Asesora de Planeación y Sistemas.

1.13 Dejar sistemas sensibles desatendidos.

Si el usuario está conectado a un sistema que contiene información sensible, éste no debe dejar el computador desatendido sin cerrar primero la sesión iniciada.

1.14 Notificación de sospecha de pérdida, divulgación o uso indebido de información sensible.

Si se pierde, se divulga información sensible a un tercero no autorizado, o se sospecha de pérdida o de divulgación a un tercero no autorizado, quien se entere debe reportarlo a la mayor brevedad al jefe inmediato a la Oficina Asesora de Planeación y Sistemas mediante una comunicación escrita por el correo electrónico interno de la Entidad o mediante una llamada telefónica.

1.15 Etiquetado y presentación de información de tipo confidencial a los usuarios de computadores.

Información de tipo confidencial que sea presentada a un usuario debe indicar **explícitamente** este nivel de clasificación de la información.

1.16 El traslado de equipos debe estar autorizado.

Ningún equipo de cómputo debe ser reubicado o trasladado sin previa autorización. El traslado de los equipos se debe hacer con las medidas de seguridad necesarias, por el personal autorizado y siguiendo los procedimientos establecidos para tal fin.

1.17 Control de recursos informáticos entregados a los usuarios.

Cuando un usuario inicie o termine su vinculación laboral con la universidad, sea trasladado a otra dependencia o por alguna otra circunstancia deje de utilizar el computador personal o el recurso tecnológico suministrado con carácter permanente, deberá hacerse igualmente un inventario del estado del mismo. El funcionario será responsable de los desperfectos o daños que por su negligencia haya ocasionado a la máquina.



1.18 Precauciones para el uso de los recursos informáticos.

Está prohibida la ingesta de bebidas u otro tipo de alimentos sobre o en las proximidades de cualquiera de los computadores o aparatos electrónicos de la Entidad, así como el manejo de sustancias o elementos que puedan ocasionar daños a los mismos.

1.19 Solicitud de préstamo de recursos informáticos.

Toda solicitud para la utilización de un recurso informático, debe venir respaldada por la autorización del jefe de área respectivo y siguiendo los procedimientos establecidos para ello.

1.20 Configuración de sistema operativo de las estaciones de trabajo.

Solamente el funcionario designado por la Oficina Asesora de Planeación y Sistemas o el responsable del área de Soporte Técnico está autorizado para cambiar la configuración del sistema operativo de las estaciones de trabajo de los usuarios.

1.21 Uso restringido de modems en las estaciones de trabajo.

Queda prohibido el uso de modems en las estaciones de trabajo que permitan obtener una conexión directa a redes externas como Internet a menos que se cuente con aprobación escrita por parte de la Oficina Asesora de Planeación y Sistemas.

1.22 Uso de acceso telefónico a redes y conexión a la red LAN concurrentemente.

No se podrá conectar por módem una estación de trabajo a una red externa, es obligatorio el uso de VPN.

1.23 Niveles de seguridad de los elementos usados en los canales

LA UNIVERSIDAD velará porque los niveles de seguridad de los elementos activos de red usados en los canales de comunicación no se tornen obsoletos frente a las nuevas versiones que los fabricantes determinen.

1.24 Reporte de incidencias

La Oficina Asesora de Planeación y Sistemas dispondrá del mecanismo o mecanismos necesarios para la implementación del proceso de reporte de incidencias. Así mismo, determinará el acuerdo de nivel de servicios y definirá una responsable por cada sistema o proceso involucrado en la definición. La Oficina Asesora de Planeación y Sistemas divulgará esta información a los funcionarios o usuarios internos y externos de las diferentes plataformas y recursos informáticos. De igual manera, asignará responsables para el tratamiento de los incidentes de seguridad de la información, quienes tendrán la responsabilidad de investigar y solucionar los incidentes reportados, tomando las medidas necesarias para evitar su reincidencia y escalando los incidentes de acuerdo con su criticidad. La Alta Dirección o a quien



delegue, ¡son los únicos autorizados para reportar incidentes de seguridad ante las autoridades; así mismo, son los únicos canales de comunicación autorizados para hacer pronunciamientos oficiales ante entidades externas.

Los propietarios de los activos de información deben informar a la Oficina Asesora de Planeación y Sistemas, los incidentes de seguridad que identifiquen o que reconozcan su posibilidad de materialización.

La Oficina Asesora de Planeación y Sistemas debe establecer responsabilidades y procedimientos para asegurar una respuesta rápida, ordenada y efectiva frente a los incidentes de seguridad de la información.

La Oficina Asesora de Planeación y Sistemas debe evaluar todos los incidentes de seguridad de acuerdo a sus circunstancias particulares y escalar a quien corresponda aquellos en los que se considere pertinente.

La Oficina Asesora de Planeación y Sistemas debe designar personal calificado, para investigar adecuadamente los incidentes de seguridad reportados, identificando las causas, realizando una investigación exhaustiva, proporcionando las soluciones y finalmente previniendo que la situación o evento se repita, estableciendo planes de mitigación y controles.

La Oficina Asesora de Planeación y Sistemas debe crear bases de conocimiento para los incidentes de seguridad presentados con sus respectivas soluciones, con el fin de reducir el tiempo de respuesta para los incidentes futuros, partiendo de dichas bases de conocimiento.

La Oficina Asesora de Planeación y Sistemas debe analizar los incidentes de seguridad que le son escalados y activar el procedimiento de contacto con las autoridades, cuando lo estime necesario.

Todos los funcionarios de la Universidad y el personal provisto por terceras partes son responsables de reportar cualquier evento o incidente relacionado con la información y/o los recursos tecnológicos a la mayor brevedad posible a la Oficina Asesora de Planeación y Sistemas.

Todos los funcionarios, en caso de conocer la pérdida o divulgación no autorizada de información clasificada como uso interno, reservada o restringida, deben notificarlo a la Oficina Asesora de Planeación y Sistemas para que se registre y se le dé el trámite necesario.

2. Políticas de Uso de las Contraseñas

2.1. Confidencialidad de las contraseñas.

La contraseña que cada usuario asigna para el acceso a los sistemas de información debe ser personal, confidencial e intransferible, cada usuario debe velar porque sus contraseñas no sean vistas y aprendidas por otras personas ni deben ser escritas en ningún medio impreso o magnético.



2.2. Uso de diferentes contraseñas para diferentes recursos informáticos.

Para impedir el compromiso de múltiples recursos informáticos, cada usuario deberá utilizar diferentes contraseñas para cada recurso al que tiene acceso. Esto involucra así mismo a los equipos de comunicación (firewall, routers, switches, servidores de control de acceso, otros) y a los administradores de los mismos.

2.3. Identificación única para cada usuario.

Cada usuario tendrá una identificación única en cada sistema al que tenga acceso, acompañado de un elemento para su autenticación (contraseña) de carácter personal y confidencial para la utilización de los recursos tecnológicos necesarios para sus labores.

2.4. Cambios periódicos de contraseñas.

Todos los usuarios deben ser automáticamente forzados a cambiar su contraseña por lo menos una vez cada 30 días.

2.5. Longitud mínima de contraseñas.

Todas las contraseñas deben tener una longitud mínima de ocho (8) caracteres. Este tamaño debe ser validado por el sistema en el momento de generar la contraseña para impedir un tamaño menor.

2.6. Contraseñas deben ser difíciles de adivinar.

Las contraseñas no deben ser nombres propios ni palabras del diccionario, debe ser una mezcla de números y letras difícil de adivinar.

2.7. Prohibición de contraseñas cíclicas.

No se debe generar contraseñas compuestas por una combinación fija de caracteres y una combinación variable pero predecible. Un ejemplo de este tipo de contraseñas prohibidas es "Enero-2022" que según la política 2.6 "Contraseñas deben ser difíciles de adivinar" es una contraseña válida, pero al mes siguiente pasa a ser "Febrero-2023" y así sucesivamente.

2.8. Las contraseñas creadas por usuarios no deben ser reutilizadas.

El usuario no debe generar una contraseña idéntica o sustancialmente similar a una que ya haya utilizado anteriormente. Esta política es complementada por la política 4.4.7 "Prohibición de contraseñas cíclicas" y por la 4.9.17 "Archivo histórico de contraseñas".



2.9. Almacenamiento de contraseñas.

Ninguna contraseña debe ser guardada de forma legible en archivos “batch”, scripts, macros, teclas de función de terminal, archivos de texto, en computadores o en otras ubicaciones en donde personas no autorizadas puedan descubrirlas o usarlas. Ningún usuario bajo ninguna circunstancia está autorizado para tener su contraseña en cualquier medio impreso, con excepción de lo contemplado en la política 4.10.3 “Almacenamiento de contraseñas de administrador”.

2.10. Almacenamiento seguro de contraseñas.

En el caso de ser necesario almacenar contraseñas porque por su cantidad la memorización se dificulta, se debe solicitar a la Oficina Asesora de Planeación y Sistemas la instalación de un sistema de cifrado fuerte, aprobado para este fin.

2.11. Sospechas de compromiso deben forzar cambios de contraseña.

Toda contraseña deberá ser cambiada de forma inmediata si se sospecha o se conoce que ha perdido su confidencialidad.

2.12. Revelación de contraseñas prohibida.

Bajo ninguna circunstancia está permitido revelar la contraseña a empleados o a terceras personas. La contraseña personal no debe ser digitada en presencia de terceras personas, así sean funcionarios de la Entidad. Ningún usuario deberá intentar obtener contraseñas de otros usuarios, excluyendo lo contemplado en la política 2.13 “Auditoría periódica a las contraseñas de los usuarios”.

2.13. Auditoría periódica a las contraseñas de los usuarios.

Solamente una Auditoría de Sistemas (interna o externa) o personal autorizado por la Oficina Asesora de Planeación y Sistemas realizarán auditorías a las bases de datos de las contraseñas de los usuarios, para determinar quiénes están incumpliendo las políticas de seguridad.

2.14. Todas las estaciones deben tener un sistema de control de acceso.

Todos los computadores y demás recursos tecnológicos que lo permitan, utilizados para el negocio de la Entidad deben usar, sin importar el lugar en donde estén ubicados, un sistema de control de acceso aprobado por la Oficina Asesora de Planeación y Sistemas.

2.15. Uso obligatorio de contraseña en el protector de pantalla.

Todas las estaciones de trabajo de los usuarios deben tener activado el protector de pantalla protegido por contraseña, el cual debe activarse luego de un período de ausencia no mayor a tres (3) minutos.



2.16. Uso de papel tapiz y protector de pantalla.

Todas las estaciones de trabajo deben utilizar el papel tapiz y el protector de pantalla institucional o el estándar de Windows, no se debe instalar un papel tapiz diferente de estos estándares. Al reingresar a la sesión, se debe solicitar contraseña.

2.17. Reporte de cambio en las responsabilidades de los usuarios al Administrador de Seguridad.

La Oficina de Gestión Humana debe reportar por medio de un correo electrónico, de manera oportuna a la Oficina Asesora de Planeación y Sistemas, todos los cambios significantes en las responsabilidades de un usuario, de su estado laboral, de su ubicación dentro de la organización, con el fin de mantener el principio de seguridad informática.

3. Políticas de Uso de la Información

3.1. Divulgación de la información manejada por los usuarios de LA UNIVERSIDAD

LA UNIVERSIDAD podrá divulgar la información de un usuario almacenada en los sistemas de acuerdo con la autorización suscrita por él mismo, por disposición legal o salvo las excepciones indicadas en este documento o en las políticas de tratamiento de datos personales.

3.2. Transferencia de datos solo a organizaciones con suficientes controles.

LA UNIVERSIDAD puede transmitir información privada solamente a terceros que por escrito se comprometan a mantener dicha información bajo controles adecuados de protección. Se da una excepción en casos en los que la divulgación de información es forzada por la ley.

LA UNIVERSIDAD deberá emitir documentos en formato PDF y, si contiene información confidencial o de uso interno, deberá tener clave, la cual se comunicará en un correo electrónico aparte del correo en el que se remita el documento.

3.3. Registro de las compañías que reciben información privada.

El personal de LA UNIVERSIDAD que liberó **información privada** a terceros debe mantener un registro de toda divulgación y este debe contener qué información fue revelada, a quién fue revelada y la fecha de divulgación.

3.4. Eliminación regular de la información que no se necesita.

La información debe ser almacenada solamente por el período de tiempo necesario establecido en la matriz de activos de información. Luego de este tiempo, la información debe ser destruida utilizando los mecanismos aprobados y con la debida autorización.



3.5. Transferencia de la custodia de información de un funcionario que deja LA UNIVERSIDAD

Cuando un empleado se retira de LA UNIVERSIDAD, su jefe inmediato debe revisar tanto los archivos magnéticos, correo electrónico como documentos impresos para determinar quién se encargará de dicha información o para ejecutar los métodos para la destrucción de la información.

3.6. Transporte de datos sensibles en medios legibles.

Si se transporta información sensible en medios legibles por el computador (cintas magnéticas, CD's, discos ópticos), la información deberá ser encriptada, siempre y cuando el receptor acepte el intercambio de datos cifrados.

3.7. Datos sensibles enviados a través de redes externas deben estar encriptados.

Si se ha de transmitir datos sensibles a través de cualquier canal de comunicación externo, dichos datos deben ser enviados en forma encriptada, siempre y cuando el receptor tenga los recursos necesarios y acepte el intercambio de datos cifrados.

4. Políticas del Uso de Internet y Correo Electrónico

4.1. Prohibición de uso de Internet para propósitos personales.

El uso de Internet está limitado exclusivamente para propósitos laborales. Los usuarios de Internet deben ser advertidos sobre la existencia de recursos tecnológicos que generan registros sobre las actividades realizadas. Esta política se complementa con la política 1.1 "Instrucciones para el uso de recursos informáticos".

4.2. Formalidad del correo electrónico.

Toda comunicación a través del correo electrónico interno se considera una comunicación de tipo laboral y formal, por tanto podrá ser supervisada por el superior inmediato del empleado.

4.3. Preferencia por el uso del correo electrónico.

Debe preferirse el uso del correo electrónico al envío de documentos físicos siempre que las circunstancias lo permitan.

4.4. Uso de correo electrónico.

La cuenta de correo asignada es de carácter individual por lo cual ningún empleado bajo ninguna circunstancia debe usar la cuenta de otro empleado.



4.5. Revisión del correo electrónico.

Todos los usuarios que dispongan de correo electrónico están en la obligación de revisarlo al menos dos veces diarias. Así mismo, es su responsabilidad mantener espacio libre en el buzón.

4.6. Mensajes prohibidos.

Se prohíbe el uso del correo electrónico con fines religiosos, políticos, lúdicos o personales o en beneficio de terceros o que vulnere los derechos fundamentales de las personas. Por tanto, está prohibido el envío, envío o en general cualquier otra conducta tendiente a la transmisión de mensajes humorísticos, pornográficos, en cadena, publicitarios y en general cualquier otro mensaje ajeno a los fines laborales sin importar si son de solo texto, audio, video o una combinación de los tres.

4.7. Restricción para el envío masivo de mensajes de correo electrónico a nivel interno.

Tan Solo personal autorizado y habilitado en la plataforma de correos podrá enviar mensajes de correo electrónico dirigidos a todos los funcionarios, docentes o estudiantes de LA UNIVERSIDAD, siempre en ejercicio de sus funciones.

4.8. Restricción para el envío masivo de mensajes de correo electrónico a nivel externo.

Solo personal autorizado podrá solicitar a la Oficina Asesora de Planeación y Sistemas, el envío masivo de mensajes de correo electrónico dirigidos a clientes o proveedores de LA UNIVERSIDAD

4.9. Acciones para frenar el SPAM.

En el caso de recibir un correo no deseado y no solicitado (también conocido como SPAM), el usuario debe abstenerse de abrirlo y avisar inmediatamente a la Oficina Asesora de Planeación y Sistemas.

4.10. Direcciones de correo institucionales.

Todas las direcciones de correo electrónico externo asignados a los usuarios internos de LA UNIVERSIDAD, deben corresponder al dominio de LA UNIVERSIDAD sobre el servicio contratado. En general se puede utilizar el primer nombre y primer apellido de la persona, separado por un punto o su función dentro de la organización como nombre válido de usuario. No deben asignarse direcciones externas de carácter personal.

4.11. Todo buzón de correo debe tener un responsable.

Todo buzón de correo asignado debe tener una persona responsable de su administración, incluidos los buzones de las aplicaciones.



4.12. Enviando software e información sensible a través de Internet.

Software e información sensible de LA UNIVERSIDAD que requiera ser enviado por Internet debe transmitirse con la mayor seguridad posible acordada entre las partes.

4.13. Intercambio de información a través de Internet.

La información interna puede ser intercambiada a través de Internet pero exclusivamente para propósitos laborales, con la debida aprobación y usando los mecanismos de seguridad apropiados.

5. Políticas de la Intranet y Sitios Web de LA UNIVERSIDAD

5.1. Reglas de uso de la Intranet.

LA UNIVERSIDAD utiliza la intranet como un recurso de publicación de los documentos que rigen la relación entre ésta y los funcionarios, por lo tanto, el funcionario debe consultar la intranet permanentemente, así como todos los documentos que en ella se encuentran publicados.

5.2. Prohibición de publicitar la imagen de LA UNIVERSIDAD en sitios diferentes a los institucionales.

La publicación de logos, marcas o cualquier tipo de información sobre la universidad o sus actividades en Internet solo podrá ser realizada a través de las páginas institucionales de la misma. En consecuencia, se encuentra terminantemente prohibido el manejo de esta información en páginas personales de los funcionarios.

5.3. Prohibición establecer conexiones a los sitios web de LA UNIVERSIDAD

Está prohibido igualmente establecer enlaces o cualquier otro tipo de conexión a cualquiera de los sitios web de LA UNIVERSIDAD por parte de los funcionarios y de sus sitios web o páginas particulares, salvo previa autorización de las directivas de la universidad, dependiendo del caso. Particularmente se encuentra prohibido el establecimiento de links o marcos electrónicos, y la utilización de nombres comerciales o marcas de propiedad de la universidad en sitios diferentes a los institucionales o como meta-etiquetas.

5.4. Prohibición de anuncios en sitios web particulares.

Está terminantemente prohibido anunciarse en los sitios web particulares como funcionarios de LA UNIVERSIDAD o como sus representantes, o incluir dibujos o crear diseños en los mismos que lleven al visitante del sitio web a pensar que existe algún vínculo con LA UNIVERSIDAD.



6. Políticas Generales de la Oficina Asesora de Planeación y Sistemas

6.1. Cuándo realizar valoración de riesgos.

Se debe realizar un análisis de riesgos a los recursos informáticos de LA UNIVERSIDAD por lo menos una vez al año. Se debe hacer un análisis de riesgos cuando se han realizado cambios importantes relacionados con dichos recursos o por amenazas en el entorno.

6.2. Restricción por acceso telefónico e Internet sobre recursos tecnológicos de uso interno a clientes externos.

No se le deben otorgar privilegios de acceso telefónico o Internet a terceros a no ser que la necesidad de dicho acceso sea justificada y aprobada. En tal caso se deben habilitar privilegios específicos para ese usuario, con vigencia solamente del período de tiempo necesario para la actividad justificada y mediante el uso de los mecanismos de control de acceso aprobados por la Oficina Asesora de Planeación y Sistemas, como son el uso de las VPN.

6.3. Los computadores multiusuario y sistemas de comunicación deben tener controles de acceso físico apropiados.

Todos los computadores multiusuario, equipos de comunicaciones, otros equipos que contengan información sensible y el software licenciado de propiedad de la Entidad deben ubicarse en centros de cómputo con puertas cerradas y controles de acceso físico apropiados.

6.4. Entrenamiento compartido para labores técnicas críticas.

Al menos dos personas deben tener la misma capacidad técnica para la adecuada administración de los sistemas de información críticos de LA UNIVERSIDAD.

6.5. Preparación y mantenimiento de planes para la recuperación de desastres y para respuesta a emergencias.

Todo sistema o recurso informático debe tener definido un plan de contingencia para la restauración de la operación. Se debe preparar, actualizar y probar periódicamente un plan para la recuperación de desastres que permita que sistemas y computadores críticos puedan estar operativos en la eventualidad de un desastre. De igual forma se deben crear planes de respuesta a emergencia con el fin de que se pueda dar una pronta notificación de problemas y solución a los mismos en la eventualidad de emergencias informáticas. Estos planes de respuesta a emergencias pueden llevar a la formación de un equipo dedicado a esta labor. Estos planes estarán incluidos en el Plan de Contingencia y Continuidad de LA UNIVERSIDAD



6.6. Personal competente en el Centro de Cómputo para dar pronta solución a problemas.

Con el fin de garantizar la continuidad de los sistemas de información, el Centro de Cómputo debe contar con personal técnico competente que pueda detectar problemas y buscar la solución de una forma eficiente o delegar esta función en un tercero contratado por LA UNIVERSIDAD, cumpliendo con las normas generales que rigen a la universidad.

6.7. Chequeo de virus en archivos recibidos en correo electrónico.

La Oficina Asesora de Planeación y Sistemas debe asegurar que todos los archivos descargados de Internet sean chequeados por un software de detección de virus informático, antes de ser transferidos a los computadores de los usuarios.

7. Políticas para Desarrolladores de Software

7.1. Ambientes separados de producción y desarrollo.

Todo sistema o aplicativo debe contar con ambiente de desarrollo y ambiente de producción. La Oficina Asesora de Planeación y Sistemas es responsable de controlar y verificar el cumplimiento de esta política.

7.2. Cumplimiento del procedimiento para cambios y/o actualizaciones.

Todo cambio y/o actualización en los sistemas de información que se encuentren en producción, debe cumplir con los procedimientos establecidos para tal fin.

7.3. Documentación de cambios y/o actualizaciones.

Todo cambio y/o actualización en los sistemas de información que se encuentren en producción, debe tener la documentación respectiva.

7.4. Catalogación de programas.

Debe cumplirse con el procedimiento establecido para pasar programas del ambiente de desarrollo al ambiente de producción previa prueba por parte del área encargada.

7.5. Medidas de seguridad deben ser implantadas y probadas antes de entrar en operación.

Todos los controles de seguridad para los sistemas de información deben ser implantados y probados sobre ambientes de pruebas o desarrollo y antes que dicho sistema entre en operación.



7.6. Incorporación de contraseñas en el software.

Ninguna contraseña deberá ser incorporada en el código de un software desarrollado o modificado por LA UNIVERSIDAD, para permitir que las contraseñas sean cambiadas con la regularidad establecida en la política 2.4 “Cambios periódicos de contraseñas”.

7.7. Acceso del usuario a los comandos del sistema operativo.

Después de haber iniciado una sesión, el usuario debe mantenerse en menús que muestren solo las opciones habilitadas para dicho usuario y de esta manera impedir la ejecución de comandos del sistema operativo y la divulgación de las capacidades del sistema.

7.8. Se requieren registros de auditoría en sistemas que manejan información sensible.

Todo sistema que maneje información sensible para LA UNIVERSIDAD debe generar registros de auditoría que guarde toda modificación, adición y eliminación de dicha información.

7.9. Registros para los usuarios privilegiados en los sistemas en producción que lo permitan.

Toda actividad realizada en los sistemas por usuarios con privilegios de administración debe ser registrada, si los mismos lo permiten, o de lo contrario debe existir un procedimiento alternativo de control.

7.10. Los registros del sistema deben incluir eventos relevantes para la seguridad.

Los sistemas de computación que manejan información sensible deben registrar todos los eventos de seguridad relevantes. Ejemplos de eventos de seguridad relevantes son: intentos de adivinación de contraseñas, intentos de uso de privilegios no otorgados, modificaciones a la aplicación y modificaciones al sistema.

7.11. Resistencia de los registros contra desactivación, modificación y eliminación.

Los mecanismos para detectar y registrar eventos de seguridad informática significativos deben ser resistentes a ataques, en los sistemas que permitan dicha configuración. Estos ataques incluyen intentos por desactivar, modificar o eliminar el software de registro y/o los registros mismos.

7.12. Procesos controlados para la modificación de información del negocio en producción.

La modificación de información en producción debe darse únicamente mediante procesos con privilegios dentro de la aplicación que maneja dicha información. Esto con el fin de evitar que la información pueda ser modificada por medios diferentes a los canales establecidos. Se excluyen los casos de emergencia, previa autorización de la Oficina Asesora de Planeación y Sistemas.



7.13. Validación de entradas en los desarrollos.

El desarrollador debe tener en cuenta durante la elaboración de la aplicación, la validación de las entradas de código con el objeto de evitar la ejecución de comandos que pongan en riesgo la seguridad de los sistemas.

7.14. Diseño de seguridad para aplicaciones.

El esquema de seguridad de aplicación, debe elaborarse de acuerdo con las definiciones establecidas para LA UNIVERSIDAD.

7.15. Personas autorizadas para leer los registros de auditoría.

Los registros de sistemas y aplicaciones no deben estar disponibles para personal no autorizado. Personal no autorizado es aquel que no pertenece a auditoría interna o externa, personal de seguridad informática, personal de administración de sistemas o administradores de bases de datos.

7.16. histórico de contraseñas.

En todo sistema multiusuario, software del sistema o software desarrollado localmente se debe mantener un archivo histórico encriptado de las contraseñas anteriores. Este archivo deberá ser usado para prevenir que un usuario seleccione una contraseña ya usada y debe contener como mínimo las últimas cinco (5) contraseñas de cada usuario. Esta política rige a partir de la fecha de liberación de este documento.

8. Políticas para Administradores de Sistemas

LA UNIVERSIDAD podrá delegar en terceros la administración de su plataforma, con los cuales divulgará las siguientes políticas. Sin embargo, en caso que algún funcionario de LA UNIVERSIDAD asuma estas funciones, deberá aplicar las políticas descritas en este capítulo.

8.1. Soporte para usuarios con privilegios especiales.

Todos los sistemas y computadores multiusuarios deben soportar un usuario con privilegios superiores a un usuario normal con el fin de poder ejercer las correspondientes labores administrativas y por lo cual estos privilegios deben ser asignados únicamente a los administradores.



8.2. Los privilegios de acceso a los sistemas de información otorgados a un usuario terminan cuando el usuario finaliza su vínculo contractual con la universidad.

Todos los privilegios sobre los recursos informáticos de LA UNIVERSIDAD otorgados a un usuario deben eliminarse en el momento que éste abandone la universidad y la información almacenada queda en manos de su jefe inmediato para aplicar los procedimientos de retención o destrucción de información.

8.3. Cuando y como pueden asignar contraseñas los administradores

Las contraseñas iniciales otorgadas por el administrador deben servir únicamente para el primer ingreso del usuario al sistema. En ese momento el sistema debe obligar al usuario a cambiar su contraseña.

8.4. Límite de intentos consecutivos de ingreso al sistema.

El sistema debe limitar el número de intentos consecutivos de introducir una contraseña válida. Después de tres (3) intentos el usuario debe pasar a alguno de los siguientes estados:

- Ser suspendido hasta nueva reactivación por parte del administrador;
- Ser temporalmente bloqueado (no menos de 5 minutos);
- Ser desconectado si se trata de una conexión remota.

8.5. Cambio de contraseñas por defecto.

Todas las contraseñas por defecto que incluyen equipos y sistemas nuevos deberán ser cambiadas antes de su utilización siguiendo los lineamientos de la política 2.6 “Contraseñas deben ser difíciles de adivinar”.

8.6. Cambio de contraseñas después de compromiso detectado en un sistema multiusuario.

Si un sistema multiusuario utiliza contraseñas como su sistema de control de acceso principal, el administrador del sistema debe asegurarse de que todas las contraseñas del mismo sean cambiadas de forma inmediata si se conoce evidencia de que el sistema ha sido comprometido. En este caso los usuarios deben ser advertidos de cambiar su contraseña en otros sistemas en los que estuvieran utilizando la misma contraseña del sistema en cuestión.

8.7. Brindar acceso a personal externo.

Los Administradores de Sistemas velarán porque individuos que no sean funcionarios, contratistas o consultores de LA UNIVERSIDAD no tengan privilegio alguno sobre los recursos tecnológicos de uso interno de la Entidad a menos que exista una aprobación escrita de la Oficina Asesora de Planeación y Sistemas.



8.8. Acceso a terceros a los sistemas de la organización requiere de un contrato firmado.

Antes de otorgarle acceso a un tercero a los recursos tecnológicos de LA UNIVERSIDAD, se debe firmar un contrato por las partes en las que se define los términos y condiciones del acceso a otorgar, derechos de LA UNIVERSIDAD y restricción de confidencialidad por parte del tercero.

8.9. Restricción de administración remota a través de Internet.

La administración remota desde Internet no es permitida a menos que se utilicen mecanismos para cifrado (VPN) del canal de comunicaciones.

8.10. Dos usuarios requeridos para todos los administradores.

Administradores de sistemas multiusuarios deben tener dos identificaciones de usuario: una con privilegios de administración y otra con privilegios de usuario normal.

8.11. Privilegios por defecto de usuarios y necesidad de aprobación explícita por escrito.

Sin autorización escrita de la Oficina Asesora de Planeación y Sistemas, los administradores no deben otorgarle privilegios de administración a ningún usuario.

8.12. Negación por defecto de privilegios de control de acceso a sistemas cuyo funcionamiento no es apropiado.

Si un sistema de control de acceso no está funcionando adecuadamente, el administrador debe negar todo intento de acceso hasta que su operación normal se haya recuperado.

8.13. Remoción de software para la detección de vulnerabilidades cuando no esté en uso.

Las herramientas de detección de vulnerabilidades usadas por los administradores se deben desinstalar cuando no estén operativas o implementar un mecanismo de control de acceso especial basado en contraseñas o en cifrado del software como tal.

8.14. Manejo administrativo de seguridad para todos los componentes de la red.

Los parámetros de configuración de todos los dispositivos conectados a la red de LA UNIVERSIDAD deben cumplir con las políticas y estándares internos de seguridad. Si se contrata un tercero para su administración, este deberá garantizar el cumplimiento de esta política.

8.15. Información a capturar cuando crimen informático o abuso es sospechado.

Para suministrar evidencia para investigación, persecución y acciones disciplinarias, cierta información debe ser capturada inmediatamente cuando se sospecha un crimen informático o abuso. Esta información se deberá almacenar de forma segura en algún dispositivo fuera de



línea. La información a recolectar incluye configuración actual del sistema, copias de backup y todos los archivos potencialmente involucrados.

8.16. Sincronización de relojes para un registro exacto de eventos en la red.

Los dispositivos multiusuario conectados a la red interna de LA UNIVERSIDAD deben tener sus relojes sincronizados con la hora oficial.

8.17. Revisión regular de los registros del sistema.

La Oficina Asesora de Planeación y Sistemas debe revisar regularmente los registros de cada uno de los diferentes sistemas para tomar acción oportuna sobre los eventos relevantes de seguridad informática.

8.18. Confidencialidad en la información relacionada con investigaciones internas.

Hasta que no se hayan presentado cargos o se haya tomado alguna acción disciplinaria, toda investigación relacionada con abusos de los recursos tecnológicos o actividad criminal debe ser confidencial para mantener la reputación del funcionario.

8.19. Información con múltiples niveles de clasificación en un mismo sistema.

Si un sistema o computador maneja información con diferentes niveles de sensibilidad, los controles usados deben ser los adecuados para proteger la información más sensible.

8.20. Segmentación de recursos informáticos por prioridad de recuperación.

Se debe establecer y usar un marco lógico para la segmentación de recursos informáticos por prioridad de recuperación. Esto hará que los sistemas más críticos sean recuperados primero. Todos los departamentos deberán usar el mismo marco para preparar los planes de contingencia a los sistemas de información.

8.21. Software de identificación de vulnerabilidades.

Para asegurar que el equipo técnico de LA UNIVERSIDAD ha tomado las medidas preventivas adecuadas, a todos los sistemas conectados a Internet se les debe correr un software de identificación de vulnerabilidades por lo menos dos veces al año.

8.22. En dónde usar controles de acceso para sistemas informáticos.

Todo computador que almacene información sensible de LA UNIVERSIDAD debe tener un sistema de control de acceso para garantizar que esta información no sea modificada, borrada o divulgada.



8.23. Mantenimiento preventivo en computadores y sistemas de comunicación.

Se debe realizar mantenimiento preventivo regularmente en todos los computadores y sistemas para que el riesgo de falla se mantenga en un nivel bajo.

9. Políticas de Backup

9.1. Período de almacenamiento de registros de auditoría.

Registros de aplicación que contengan eventos relevantes de seguridad deben ser almacenados por un período no menor a tres (3) meses. Durante este período los registros deben ser asegurados para evitar modificaciones y para que puedan ser vistos solo por personal autorizado. Estos registros son importantes para la corrección de errores, auditoría forense, investigaciones sobre huecos de seguridad y demás esfuerzos relacionados.

9.2. Tipo de datos a los que se les debe hacer backup y con qué frecuencia.

A toda información sensible y software crítico de LA UNIVERSIDAD residente en los recursos informáticos, se le debe hacer backup con la frecuencia necesaria soportada por los planes de contingencia. Se deben hacer pruebas periódicas para garantizar el buen estado de la información almacenada.

9.3. Dos copias de información sensible.

Se deben elaborar dos copias de cada backup con el fin de minimizar el riesgo por daño del medio de almacenamiento. Se establecerá un procedimiento para backup, el cual hace parte integral de estas políticas.

10. Políticas de Uso de Firewall

10.1. Detección de intrusos.

Todo segmento de red accesible desde Internet debe tener un sistema de detección de intrusos (IDS) con el fin de tomar acción oportuna frente a ataques.



10.2. Toda conexión externa debe estar protegida por el firewall.

Toda conexión a los servidores de LA UNIVERSIDAD proveniente del exterior, sea Internet, acceso remoto o redes externas debe pasar primero por el Firewall. Esto con el fin de limitar y controlar las puertas de entrada a la organización.

10.3. Toda conexión desde y hacia Internet debe pasar por el Firewall.

El firewall debe ser el único elemento conectado directamente a Internet por lo cual toda conexión desde la red interna hacia Internet debe pasar por el firewall.

10.4. Filtrado de contenido activo en el Proxy.

La Oficina Asesora de Planeación y Sistemas de LA UNIVERSIDAD debe asegurar que dentro de las definiciones de políticas de Proxy, se filtre todo contenido activo como applets de java, Macromedia, controles de ActiveX debido a que estos tipos de datos pueden comprometer la seguridad de los sistemas de información.

10.5. Segmentación de la red.

Todos los servidores públicos deben ser ubicados en un segmento de red especial, protegidos por el Firewall, con el fin de proteger la red Interna y los servidores críticos. De igual forma los servidores críticos deben ser ubicados en un segmento de red especial con controles de acceso adecuados, siempre y cuando no se afecte la operación normal de la red y de sus servicios.

10.6. Inventario de conexiones.

Se debe mantener un registro de las conexiones VPN hacia o desde redes externas con el fin de tener una imagen clara de todos los puntos de entrada a la organización.

10.7. El sistema interno de direccionamiento de red no debe ser público.

Las direcciones internas de red y configuraciones internas deben estar restringidas de tal forma que sistemas y usuarios que no pertenezcan a la red interna no puedan acceder a esta información.

10.8. Revisión periódica y reautorización de privilegios de usuarios.

Los privilegios otorgados a un usuario deben ser revaluados una vez al año con el fin de analizar si los privilegios actuales siguen siendo necesarios para las labores normales del usuario, o si se necesita otorgarle privilegios adicionales. Esta política debe ser ejecutada por la Auditoría de Sistemas con la participación de cada uno de los jefes de área, quienes harán la revisión y solicitud de cambios de la Oficina Asesora de Planeación y Sistemas.



11. Políticas para Usuarios Externos

11.1. Términos y condiciones para clientes de Internet.

LA UNIVERSIDAD asume que todos los clientes que usan Internet para comprarle a LA UNIVERSIDAD productos o servicios, aceptan los términos y condiciones impuestos por LA UNIVERSIDAD para la realización operaciones o transacciones, antes de que la orden sea procesada. Esto se debe ver reflejado en el documento: Términos y Condiciones, el cual está publicado en la página de LA UNIVERSIDAD.

11.2. Acuerdos con terceros que manejan información o cualquier recurso informático de LA UNIVERSIDAD

Todos los acuerdos relacionados con el manejo de información o de recursos de informática de LA UNIVERSIDAD por parte de terceros, deben incluir una cláusula especial que involucre confidencialidad y derechos reservados. Esta cláusula debe permitirle a LA UNIVERSIDAD ejercer auditoría sobre los controles usados para el manejo de la información y específicamente de cómo será protegida la información de LA UNIVERSIDAD

11.3. Definición clara de las responsabilidades de seguridad informática de terceros.

Socios de negocios, proveedores, clientes y otros asociados a los negocios de LA UNIVERSIDAD deben tener conocimiento de sus responsabilidades relacionadas con la seguridad informática y esta responsabilidad se debe ver reflejada en los contratos y verificada por la Oficina Asesora de Planeación y Sistemas.

Los contratos suscritos con los terceros deben contener al menos, los siguientes aspectos:

- Niveles de servicio y operación.
- Acuerdos de confidencialidad sobre la información manejada y sobre las actividades desarrolladas.
- Propiedad de la información.
- Restricciones sobre el software empleado.
- Normas de seguridad informática y física a ser aplicadas.
- Procedimientos a seguir cuando se encuentre evidencia de alteración o manipulación de dispositivos o información.
- Procedimientos y controles para la entrega de la información manejada y la destrucción de la misma por parte del tercero una vez finalizado el servicio.
- Los terceros contratados por LA UNIVERSIDAD deben contar con Plan de Continuidad y Contingencia.



12. Políticas de Acceso Físico

A pesar de que LA UNIVERSIDAD no cuenta con infraestructura en un único centro de cómputo, se considerarán estas políticas en caso que lo desarrolle o que disponga de su actual espacio de infraestructura de comunicaciones.

12.1. Cuando se requiera que las puertas del Centro de Cómputo estén abiertas, debe estar presente la Oficina Asesora de Planeación y Sistemas.

Cuando la puerta del Centro de Cómputo requiera mantenerse abierta (por ejemplo, traslados de equipos), la entrada debe estar permanentemente vigilada por la Oficina Asesora de Planeación y Sistemas. Las demás políticas deberán ser aplicadas.

12.2. Permitir paso a través de puertas controladas.

Los funcionarios no deben permitir que personal desconocido o no autorizado entre a zonas restringidas que se definan.

12.3. Se requiere cumplir el procedimiento por parte de todos los usuarios al visitar el Centro de Cómputo.

Todo usuario, deberá seguir el procedimiento para el ingreso y permanencia en las áreas del Centro de Cómputo.

12.4. Control de acceso físico para áreas que contienen información sensible.

El acceso a cada oficina, cuarto de computadores, cuarto de equipos de comunicaciones y puestos de trabajo que contengan información sensible, debe estar físicamente restringido.

12.5. Las puertas deben estar cerradas con llave cuándo las oficinas personales no estén siendo utilizadas.

Todos los funcionarios con oficinas personales deben mantener la puerta cerrada con llave cuando no se encuentre en la oficina.

12.6. Controles de acceso en áreas que contienen información sensible.

Toda área que contenga información sensible debe tener controles de acceso efectivos.

12.7. Reporte de pérdida o robo de identificación.

Todo empleado debe reportar con la mayor brevedad, cualquier sospecha de pérdida o robo de carnets de identificación y tarjetas de acceso físico a las instalaciones.



12.8. Obligación de portar el carnet.

Todo empleado debe portar el carnet durante su permanencia en las instalaciones de LA UNIVERSIDAD

12.9. Prohibición a los intentos de acceso físico a zonas restringidas.

Los funcionarios no deben intentar entrar a zonas restringidas a las cuales no han recibido autorización de acceso.

12.10. Orden de salida para equipos electrónicos.

Ningún equipo electrónico podrá salir de las instalaciones de LA UNIVERSIDAD sin una orden de salida otorgada por el personal adecuado o sin haber sido registrado en el momento de su ingreso.

12.11. Toda persona debe mostrar sus maletines al ingresar o salir de la oficina.

Toda persona debe mostrar su maletín o bolso a la persona de recepción al entrar y al retirarse de las instalaciones de LA UNIVERSIDAD.

12.12. Mantenimiento de los registros de ingreso.

Se debe mantener los registros de personas y equipos que han ingresado a las instalaciones de LA UNIVERSIDAD por un tiempo no menor a tres (3) meses.

12.13. Cuando se da una terminación laboral, los privilegios de acceso al edificio deben ser revocados.

Cuando exista una terminación laboral, el usuario deberá devolver los objetos de acceso físico a las instalaciones (carnets, tarjetas de acceso, etc.) y a su vez todos sus privilegios de acceso deberán ser revocados con la mayor brevedad.

13. Política de gestión de activos

La Oficina de Inventarios con el acompañamiento permanente de la Oficina de Sistemas establecerá y divulgará los lineamientos específicos para la identificación, clasificación, valoración y buen uso de los activos de información, con el objetivo de garantizar su protección.

13.1. Inventario de Activos

Los activos de la Universidad de Caldas deben ser identificados, clasificados, valorados y controlados para garantizar su uso adecuado, protección y recuperación ante desastres. Por tal motivo, se aplicará el procedimiento vigente con los lineamientos necesarios para llevar el



Inventarlo de los activos de información de su propiedad, discriminado por procesos y dependencia, tipo, nivel de criticidad, clasificación, ubicación, responsable, custodio, y demás atributos que la Universidad disponga.

13.2. Protección

Con el objetivo de establecer los controles de seguridad físicos y digitales, las dependencias que tienen la custodia de la información generada en el marco de su función se encargarán de proteger la Información, mantener y actualizar el inventario de activos de información relacionados con sus servicios (Información física o digital, software, hardware y recurso humano).

13.3. Archivos de Gestión

La Oficina Asesora de Planeación y Sistemas deberá implementar los controles necesarios para que los archivos de gestión cuenten con los mecanismos de seguridad apropiados, de acuerdo a las Tablas de Retención Documental, con el fin de proteger y conservar la confidencialidad, integridad y disponibilidad de la información física de la Universidad.

13.4. Devolución de los Activos

Todos los funcionarios y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo

13.5. Gestión de medios removibles

Se deben implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la entidad.

13.6. Disposición de los activos

Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando el procedimiento establecido

13.7. Dispositivos móviles

Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.

El traslado de activos de información debe efectuarse aplicando medidas de control acordes con la evaluación de criticidad del activo y el impacto para el proceso al cual está relacionado. En particular, el traslado de activos de información tales como equipos, computadores, u otros dispositivos tecnológicos.



14. Política de seguridad de las operaciones.

La Oficina Asesora de Planeación y Sistemas de la Universidad será la encargada de la operación y administración de los recursos tecnológicos que soportan la operación. Así mismo, velará por la eficiencia de los controles asociados a los recursos tecnológicos protegiendo la confidencialidad, integridad y disponibilidad de la Información, y para que los cambios efectuados sobre los recursos tecnológicos y sistemas de información en ambientes de prueba y producción sean controlados y debidamente autorizados. De Igual manera, proveerá la capacidad de procesamiento requerida en los recursos tecnológicos y sistemas de información, efectuando proyecciones de crecimiento y provisiones en la plataforma tecnológica de acuerdo al crecimiento de la Universidad, e implementará mecanismos de contingencias y recuperación ante desastres con el fin de propender por la disponibilidad de los servicios de TI en el marco de la operación de la Universidad.

La Oficina Asesora de Planeación y Sistemas deberá realizar y mantener copias de seguridad de la Información de la Universidad en medio digital, siempre que ésta sea reportada por el responsable de la misma, con el objetivo de recuperarla en caso de cualquier tipo de falla. Efectuará la copia respectiva de acuerdo con el esquema definido previamente en un procedimiento que enmarque la gestión, copias de seguridad de la Información digital, sistemas de Información, bases de datos y demás recursos tecnológicos de la Entidad; el diseño de este procedimiento se hará en conjunto con los líderes de proceso, con el fin de determinar la Información a respaldar y la periodicidad del respaldo, los tiempos de recuperación y restauración, y los mecanismos para generar el menor Impacto en la prestación del servicio durante el tiempo de la indisponibilidad de la Información.

CAPACITACIÓN Y SENSIBILIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

La Oficina Asesora de Planeación y Sistemas establece el programa y los planes de capacitación y concienciación considerando las necesidades de capacitación de los funcionarios y partes interesadas en los servicios prestados por la Universidad.

Los costos del programa de capacitación y concienciación en seguridad de la información deben ser previamente establecidos, aprobados e incluidos dentro del presupuesto anual de operación de la Oficina de Gestión Humana.

El área de Talento Humano en conjunto con la Oficina Asesora de Planeación y Sistemas y las demás áreas de apoyo ayudaran al desarrollo satisfactorio del programa de capacitación y concienciación hacia el total de funcionarios que laboran en la organización, extendiéndolo también hacia los terceros que conforman las partes interesadas del modelo de seguridad.



El programa de seguridad de la información es anual y los resultados de su evolución, ejecución y aplicabilidad deben ser presentados dentro de los informes periódicos de gestión de seguridad de la información.

La capacitación en el sistema deberá reforzarse por lo menos una vez al año; deberá hacer parte del proceso de inducción de la Universidad y ser objeto de evaluación para eficacia frente a las políticas y objetivos del sistema.

Como estrategia para la concientización la estrategia se apoyará en la generación de actividades dinámicas y colaborativas que involucren a los funcionarios con el proceso de entendimiento y compromiso para la prevención de los riesgos de seguridad. Parte de estas actividades serán dirigidas por expertos temáticos externos a la Universidad.

ACTUALIZACIÓN DE LA POLÍTICA DE SEGURIDAD INFORMÁTICA

Debido a la propia evolución de la tecnología, las amenazas de seguridad y a los nuevos aportes legales en la materia, LA UNIVERSIDAD se reserva el derecho a modificar estas políticas cuando sea necesario. Los cambios realizados en estas políticas serán divulgados a los usuarios y a todas las empresas proveedoras de servicios a las que les aplique, utilizando los medios que se consideren pertinentes. Es responsabilidad de cada empresa proveedora garantizar la lectura y conocimiento de las políticas de seguridad más recientes de LA UNIVERSIDAD por parte de su personal.

LISTADO DE ANEXOS

| | |
|---------|--|
| Anexo 1 | Acuerdo de Confidencialidad |
| Anexo 2 | Autorización de traslado de equipos |
| Anexo 3 | Formato de inventario de equipos o recursos informáticos |
| Anexo 4 | Formato de solicitud y entrega de préstamo de recursos informáticos |
| Anexo 5 | Formato de divulgación de información a terceros |
| Anexo 6 | Formato de conocimiento de las políticas de seguridad |
| Anexo 7 | Catálogo de programas |
| Anexo 8 | Autorización escrita para entregar permisos de administrador a usuarios o terceros |

