



# **POLITICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION**

Universidad de Caldas  
Verión 2.0  
2025



RECTORÍA



**Tejiendo  
Universidad**

*Autoevaluación Institucional 2018 - 2026*



RECTORÍA

## CONTROL DE VERSIONES

VERSIÓN	FECHA	DESCRIPCIÓN
1.0	16/01/2023	Documento inicial donde se definen la política general de seguridad y privacidad de la información
2.0	27/05/2025	Se realizó la modificación a la totalidad del documento a la luz de la normatividad en materia de seguridad de TI



**Tejiendo  
Universidad**

Autoevaluación Institucional 2018 - 2026



TABLA DE CONTENIDO

**OBJETIVO ..... 11**

**ALCANCE ..... 12**

**DEFINICIONES..... 13**

**PRINCIPIOS..... 16**

**POLÍTICAS..... 18**

    Objetivo de las políticas.....18

    Alcance de las políticas .....18

    1. Políticas de Uso de Recursos Informáticos .....20

        1.1. Instrucciones para el uso de recursos informáticos.....20

        1.2 Uso personal de los recursos informáticos. ....20

        1.3 Acuerdo de confidencialidad firmado para entrega de nombre de usuario. ....20

        1.4 Prohibición de instalación y desinstalación de software y hardware en los computadores de la organización. ....20

        1.5 Uso del aplicativo entregado. ....20

        1.6 El usuario es responsable por toda actividad que involucre su identificación personal o recursos informáticos asignados. ....20

        1.7 Declaración de reserva de derechos de LA UNIVERSIDAD .....21

        1.8 Recursos compartidos. ....21

        1.9 Todo monitoreo debe ser registrado e informado al jefe inmediato del usuario. ....21

        1.10 Acceso no autorizado a los sistemas de información de la Entidad. ....21

        1.11 Posibilidad de acceso no implica permiso de uso. ....21

        1.12 Prohibición a la explotación de vulnerabilidades de seguridad de los recursos informáticos. 22

        1.13 Dejar sistemas sensibles desatendidos.....22

        1.14 Notificación de sospecha de pérdida, divulgación o uso indebido de información sensible. .22



1.15	Etiquetado y presentación de información de tipo confidencial a los usuarios de computadores.....	22
1.16	El traslado de equipos debe estar autorizado.....	22
1.17	Control de recursos informáticos entregados a los usuarios.....	22
1.18	Precauciones para el uso de los recursos informáticos.....	22
1.19	Solicitud de préstamo de recursos informáticos.....	22
1.20	Configuración de sistema operativo de las estaciones de trabajo.....	23
1.21	Uso restringido de modems en las estaciones de trabajo.....	23
1.22	Uso de acceso telefónico a redes y conexión a la red LAN concurrentemente.....	23
1.23	Niveles de seguridad de los elementos usados en los canales.....	23
1.24	Reporte de incidencias.....	23
2.	Políticas de Uso de las Contraseñas.....	24
2.1.	Confidencialidad de las contraseñas.....	24
2.2.	Uso de diferentes contraseñas para diferentes recursos informáticos.....	24
2.3.	Identificación única para cada usuario.....	24
2.4.	Cambios periódicos de contraseñas.....	25
2.5.	Longitud mínima de contraseñas.....	25
2.6.	Contraseñas deben ser difíciles de adivinar.....	25
2.7.	Prohibición de contraseñas cíclicas.....	25
2.8.	Las contraseñas creadas por usuarios no deben ser reutilizadas.....	25
2.9.	Almacenamiento de contraseñas.....	25
2.10.	Almacenamiento seguro de contraseñas.....	25
2.11.	Sospechas de compromiso deben forzar cambios de contraseña.....	25
2.12.	Revelación de contraseñas prohibida.....	25
2.13.	Auditoría periódica a las contraseñas de los usuarios.....	26
2.14.	Todas las estaciones deben tener un sistema de control de acceso.....	26
2.15.	Uso obligatorio de contraseña en el protector de pantalla.....	26
2.16.	Uso de papel tapiz y protector de pantalla.....	26





2.17. Reporte de cambio en las responsabilidades de los usuarios al Administrador de Seguridad.....	26
3. Políticas de Uso de la Información .....	26
3.1. Divulgación de la información manejada por los usuarios de la entidad .....	26
3.2. Transferencia de datos solo a organizaciones con suficientes controles. ....	26
3.3. Registro de las compañías que reciben información privada. ....	27
3.4. Transferencia de la custodia de información de un funcionario que deja LA UNIVERSIDAD..	27
3.5. Transporte de datos sensibles en medios legibles.....	27
3.6. Datos sensibles enviados a través de redes externas deben estar encriptados. ....	27
4. Políticas del Uso de Internet y Correo Electrónico .....	27
4.1. Prohibición de uso de Internet para propósitos personales.....	27
4.2. Formalidad del correo electrónico. ....	27
4.3. Preferencia por el uso del correo electrónico. ....	28
4.4. Uso de correo electrónico.....	28
4.5. Revisión del correo electrónico.....	28
4.6. Mensajes prohibidos. ....	28
4.7. Restricción para el envío masivo de mensajes de correo electrónico a nivel interno. ....	28
4.8. Restricción para el envío masivo de mensajes de correo electrónico a nivel externo. ....	28
4.9. Acciones para frenar el SPAM.....	28
4.10. Direcciones de correo institucionales. ....	28
4.11. Todo buzón de correo debe tener un responsable. ....	29
4.12. Enviando software e información sensible a través de Internet.....	29
4.13. Intercambio de información a través de Internet. ....	29
5. Políticas de la Intranet y Sitios Web de LA UNIVERSIDAD .....	29
5.1. Reglas de uso de la Intranet.....	29
5.2. Prohibición de publicitar la imagen de LA UNIVERSIDAD en sitios diferentes a los institucionales.....	29
5.3. Prohibición establecer conexiones a los sitios web de la entidad .....	29
5.4. Prohibición de anuncios en sitios web particulares.....	29



6.	Políticas Generales de la Oficina Asesora de Planeación y Sistemas .....	30
6.1.	Cuando realizar valoración de riesgos. ....	30
6.2.	Restricción por acceso telefónico e Internet sobre recursos tecnológicos de uso interno a clientes externos. ....	30
6.3.	Los computadores multiusuario y sistemas de comunicación deben tener controles de acceso físico apropiados. ....	30
6.4.	Entrenamiento compartido para labores técnicas críticas. ....	31
6.5.	Preparación y mantenimiento de planes para la recuperación de desastres y para respuesta a emergencias. ....	31
6.6.	Personal competente en el Centro de Cómputo para dar pronta solución a problemas. ....	31
6.7.	Chequeo de virus en archivos recibidos en correo electrónico. ....	32
7.	Políticas para Desarrolladores de Software.....	32
7.1.	Ambientes separados de producción y desarrollo.....	32
7.2.	Cumplimiento del procedimiento para cambios y/o actualizaciones. ....	32
7.3.	Documentación de cambios y/o actualizaciones.....	32
7.4.	Catalogación de programas. ....	32
7.5.	Medidas de seguridad deben ser implantadas y probadas antes de entrar en operación. ....	32
7.6.	Incorporación de contraseñas en el software. ....	32
7.7.	Acceso del usuario a los comandos del sistema operativo.....	32
7.8.	Se requieren registros de auditoría en sistemas que manejan información sensible. ....	32
7.9.	Registros para los usuarios privilegiados en los sistemas en producción que lo permitan. ...	33
7.10.	Los registros del sistema deben incluir eventos relevantes para la seguridad. ....	33
7.11.	Resistencia de los registros contra desactivación, modificación y eliminación.....	33
7.12.	Procesos controlados para la modificación de información del negocio en producción. ...	33
7.13.	Validación de entradas en los desarrollos.....	33
7.14.	Diseño de seguridad para aplicaciones. ....	33
7.15.	Personas autorizadas para leer los registros de auditoría.....	33
7.16.	histórico de contraseñas. ....	34
8.	Políticas para Administradores de Sistemas .....	34



8.1.	Soporte para usuarios con privilegios especiales. ....	34
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. ....	34
8.3.	Cuando y como pueden asignar contraseñas los administradores .....	34
8.4.	Límite de intentos consecutivos de ingreso al sistema. ....	34
8.5.	Cambio de contraseñas por defecto. ....	35
8.6.	Cambio de contraseñas después de compromiso detectado en un sistema multiusuario. ....	35
8.7.	Brindar acceso a personal externo. ....	35
8.8.	Acceso a terceros a los sistemas de la organización requiere de un contrato firmado. ....	35
8.9.	Restricción de administración remota a través de Internet. ....	35
8.10.	Dos usuarios requeridos para todos los administradores. ....	35
8.11.	Privilegios por defecto de usuarios y necesidad de aprobación explícita por escrito. ....	36
8.12.	Negación por defecto de privilegios de control de acceso a sistemas cuyo funcionamiento no es apropiado. ....	36
8.13.	Remoción de software para la detección de vulnerabilidades cuando no esté en uso. ....	36
8.14.	Manejo administrativo de seguridad para todos los componentes de la red. ....	36
8.15.	Captura de información en casos de sospecha de crimen informático o abuso. ....	36
8.16.	Sincronización de relojes para un registro exacto de eventos en la red. ....	36
8.17.	Revisión regular de los registros del sistema. ....	36
8.18.	Confidencialidad en la información relacionada con investigaciones internas. ....	37
8.19.	Información con múltiples niveles de clasificación en un mismo sistema. ....	37
8.20.	Segmentación de recursos informáticos por prioridad de recuperación. ....	37
8.21.	Software de identificación de vulnerabilidades. ....	37
8.22.	Uso de controles de acceso para sistemas informáticos. ....	37
8.23.	Mantenimiento preventivo en computadores y sistemas de comunicación. ....	37
9.	Políticas de Backup .....	37
9.1.	Período de almacenamiento de registros de auditoría. ....	37
9.2.	Tipo de datos a los que se les debe hacer backup y la frecuencia. ....	38
9.3.	Número de copias sobre información sensible. ....	38





10.	Políticas de Uso de Firewall .....	38
10.1.	Detección de intrusos. ....	38
10.2.	Protección de las conexiones externas. ....	38
10.3.	Protección de las conexiones desde y hacia Internet.....	38
10.4.	Filtrado de contenido activo en el Proxy.....	38
10.5.	Segmentación de la red.....	39
10.6.	Inventario de conexiones.....	39
10.7.	El sistema interno de direccionamiento de red. ....	39
10.8.	Revisión periódica y reautorización de privilegios de usuarios. ....	39
11.	Políticas para Usuarios Externos .....	39
11.1.	Términos y condiciones para clientes de Internet. ....	39
11.2.	Acuerdos con terceros que manejan información o cualquier recurso informático de la universidad .....	39
11.3.	Definición de las responsabilidades de seguridad informática de terceros.....	40
12.	Políticas de Acceso Físico.....	40
12.1.	Requerimiento de la apertura del Centro de Cómputo. ....	40
12.2.	Paso a través de puertas controladas. ....	41
12.3.	Protocolo de acceso al Centro de Cómputo.....	41
12.4.	Control de acceso físico para áreas que contienen información sensible.....	41
12.5.	Controles de acceso en áreas que contienen información sensible. ....	42
12.6.	Orden de salida para equipos de TI .....	42
12.7.	Manejo de los privilegios de acceso ante la terminación del vínculo laboral. ....	42
13.	Política de gestión de activos.....	42
13.1.	Inventario de Activos.....	42
13.2.	Protección .....	43
13.3.	Archivos de Gestión .....	43
13.4.	Devolución de los Activos .....	43
13.5.	Gestión de medios removibles .....	43





13.6.	Disposición de los activos.....	44
13.7.	Dispositivos móviles .....	44
14.	Política de seguridad de las operaciones. ....	44
CAPACITACIÓN Y SENSIBILIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN .....		44
ACTUALIZACIÓN DE LA POLÍTICA DE SEGURIDAD INFORMÁTICA .....		45
LISTADO DE ANEXOS .....		45





## 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.



## 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 del a 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.

## 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
- Política uso de las cookies
- Gestión de Incidentes de Seguridad:  
Política de Respuesta a Incidentes: Establecer un protocolo claro para la notificación, investigación y respuesta a incidentes de seguridad (violaciones de datos, ataques de malware, etc.).
- Definir roles y responsabilidades para el equipo de respuesta a incidentes.
- Implementar un sistema de registro y seguimiento de incidentes.

- Política de Continuidad del Negocio y Recuperación ante Desastres: Desarrollar planes para garantizar la continuidad de las operaciones críticas en caso de un incidente mayor.
- Realizar pruebas periódicas de los planos de recuperación ante desastres.
- Seguridad en la Nube y Dispositivos Móviles:
- Política de Seguridad en la Nube: Establecer directrices para el uso seguro de servicios en la nube (almacenamiento, software, etc.).
- Definir los controles de seguridad necesarios para proteger los datos almacenados en la nube.
- Política de Seguridad de Dispositivos Móviles: Establecer normas para el uso de dispositivos móviles (teléfonos, tabletas, laptops) para acceder a información de la universidad.
- Implementar medidas de seguridad para proteger los datos en dispositivos móviles (cifrado, contraseñas, etc.).
- Política de BYOD (Trae tu propio dispositivo).
- Concientización y Capacitación:
- Programa de Concientización sobre Seguridad:
- Realizar capacitaciones periódicas para usuarios sobre buenas prácticas de seguridad.
- Promover una cultura de seguridad en toda la universidad.
- Simulacros de Phishing, y ataques de ingeniería social.
- Política de Capacitación para Roles Específicos: Proporcionar capacitación especializada para administradores de sistemas, desarrolladores de software y otros roles con responsabilidades de seguridad.
- Cumplimiento Normativo:
- Política de Cumplimiento de la Protección de Datos:
- Asegurar el cumplimiento de las leyes y regulaciones aplicables en materia de protección de datos personales.
- Realizar auditorías periódicas para verificar el cumplimiento.
- Política de Gestión de Riesgos: Realizar evaluaciones de riesgos periódicas para identificar y mitigar posibles amenazas a la seguridad de la información.
- Establecer un marco de gestión de riesgos para priorizar y abordar los riesgos identificados.
- Seguridad del Software y el Hardware:
- Política de Gestión de Vulnerabilidades: Establecer un proceso para identificar y corregir vulnerabilidades en software y hardware.
- Realizar escaneos de vulnerabilidades periódicos.
- Política de Seguridad del Ciclo de Vida del Desarrollo de Software (SDLC):
- Integrar la seguridad en todas las fases del desarrollo de software.
- Realizar pruebas de seguridad durante el desarrollo y antes de la implementación.
- Puntos adicionales:
- Política de Registro y Monitoreo: Implementar sistemas para registrar y monitorear la actividad en los sistemas de información, para detectar posibles incidentes de seguridad.
- Política de Destrucción Segura de Datos: Establecer procedimientos para la destrucción segura de datos confidenciales cuando ya no sean necesarios.

- Política de Teletrabajo: Con el aumento del trabajo remoto, es crucial establecer políticas claras sobre cómo mantener la seguridad de la información cuando se trabaja fuera de las instalaciones de la universidad.

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](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 asignado 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 cualquier dispositivo que permita una conexión directa a redes externas como Internet en las estaciones de trabajo, incluyendo, pero no limitado a, obtener módems, puntos de acceso móviles (hotspots) y cualquier otra forma de compartir la conexión a Internet de un dispositivo móvil, 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.

Se prohíbe la conexión directa de estaciones de trabajo a redes externas, incluyendo Internet, mediante cualquier tipo de dispositivo de conexión, tales como módems, puntos de acceso móvil (hotspots) o cualquier otro método que permita el acceso no autorizado que interfiera con el buen funcionamiento de la infraestructura tecnológica de la universidad o su seguridad.

El acceso remoto seguro a la red corporativa desde estaciones de trabajo externas se realizará exclusivamente a través de una conexión VPN (Red Privada Virtual) autorizada por la Oficina Asesora de Planeación y Sistemas.

#### 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 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.

Para la seguridad de la información, las contraseñas deben tener al menos ocho caracteres, combinando letras mayúsculas, minúsculas, números y símbolos. El sistema validará su complejidad al crearlas, rechazando las débiles. Evite palabras comunes y cambie las contraseñas periódicamente.

#### 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.

Para proteger la información de la Universidad de Caldas, es obligatorio que todos los computadores y dispositivos tecnológicos usados para el trabajo, tanto dentro como fuera de las sedes, tengan un sistema de control de acceso. Esto significa que solo personas autorizadas podrán usar estos equipos. La Oficina Asesora de Planeación y Sistemas decidirá qué sistemas de control de acceso son válidos y seguros. Esta medida se aplica siempre, sin importar dónde se encuentre el equipo, para asegurar que la información esté protegida en todo momento.

#### 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 entidad

La Universidad solo compartirá la información de un usuario almacenada en sus sistemas cuando este lo autorice por escrito, cuando una ley así lo exija, o en situaciones específicas detalladas en este documento o en las políticas de protección de datos personales de la Universidad.

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

La Universidad solo compartirá información privada con terceros que garantizan por escrito su protección adecuada, excepto cuando la ley lo exija. En convenios interinstitucionales, como prácticas académicas,

se aplicarán estos mismos criterios. Para proteger datos sensibles, los PDF con información confidencial o internamente irán cifrados con una clave enviada por separado. Dada la especial protección de datos de niños, niñas y adolescentes en Colombia, la Universidad extremará estas medidas cuando la información corresponda a este grupo, obteniendo siempre el consentimiento informado de sus representantes legales para cualquier transmisión o uso de sus datos.

### 3.3. Registro de las compañías que reciben información privada.

Ningún personal de la universidad está autorizado para entregar información a terceros, salvo en los casos que la ley así lo establezca.

### 3.4. 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.

### 3.5. 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.

### 3.6. 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.

El correo electrónico interno de la Universidad es una herramienta de comunicación laboral. Por lo tanto, su uso debe ser para fines relacionados con las actividades de la institución. La supervisión del correo electrónico se realizará de manera excepcional y justificada, cuando existan indicios razonables de incumplimiento de las políticas de la Universidad o de la ley. La supervisión se limitará a revisar el contenido de los correos electrónicos estrictamente relacionados con la investigación en curso, y se realizará con la autorización previa de la Secretaría General de la universidad.

#### 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.

El correo electrónico de la Universidad es una herramienta de comunicación laboral. Se prohíbe su uso para la difusión de contenidos que inciten a la discriminación, al odio, a la violencia, o que vulneren los derechos fundamentales de las personas, así como la transmisión de mensajes pornográficos o que constituyan acoso. Se restringe el uso del correo electrónico para fines religiosos o políticos que impliquen proselitismo o la imposición de creencias a otros. Se permite el uso moderado del correo electrónico para comunicaciones personales o lúdicas, siempre que estén relacionados con fines laborales, ni vulnere derechos de otros. La Universidad promueve un ambiente de respeto y tolerancia, donde se respetan los derechos fundamentales de las personas, la libertad de expresión y la libertad de conciencia.

#### 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 usuarios, 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 asignadas a los usuarios internos de la universidad deben corresponder al dominio de la universidad sobre las diferentes plataformas contratadas (Google, Microsoft). 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 entidad

Para proteger la seguridad de la información y la integridad de la imagen de la universidad, se prohíbe establecer enlaces o cualquier otro tipo de conexión a los sitios web institucionales desde sitios web o páginas particulares de funcionarios, salvo autorización previa de las directivas. Esta restricción incluye, pero no se limita a, la creación de marcos electrónicos que muestren contenido de los sitios web de la Universidad en sitios externos, el uso de nombres comerciales o marcas de la universidad en sitios no institucionales, y la inclusión de metaetiquetas con nombres o marcas de la universidad en sitios externos.

La autorización para establecer enlaces a los sitios web de la Universidad se concederá únicamente en casos justificados, cuando se demuestre que la conexión no representa un riesgo para la seguridad de la información ni para la imagen de la institución. Las solicitudes de autorización deberán dirigirse a la Oficina Asesora de Planeación y Sistemas.

#### 5.4. Prohibición de anuncios en sitios web particulares.

Para proteger la imagen institucional y evitar confusiones, se prohíbe a los funcionarios de la universidad utilizar sus sitios web personales para promocionar productos o servicios personales usando la imagen o

nombre de la Universidad, difundir opiniones que puedan ser interpretadas como funcionarios de la Universidad, a menos que cuenten con autorización expresa, utilizar el logo, la marca o cualquier otro elemento distintivo de la universidad sin autorización previa, o crear sitios web que simulen ser oficiales de la Universidad o que induzcan un error sobre su afiliación con la institución. Esta prohibición se extiende a la inclusión de dibujos o diseños que puedan llevar a los visitantes a creer que existe un vínculo oficial entre el sitio web personal y la universidad.

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

### 6.1. Cuando realizar valoración de riesgos.

Para garantizar la protección de los activos de información de la Universidad, se realizará un análisis de riesgos exhaustivo de los recursos informáticos críticos, incluyendo servidores, bases de datos, aplicaciones y redes, al menos una vez al año. Este análisis será realizado por el equipo de seguridad de la información, utilizando una metodología de evaluación de riesgos reconocida. Además, se realizará un análisis de riesgos siempre que se produzcan cambios significativos en los recursos informáticos, tales como la implementación de nuevos sistemas, la modificación de configuraciones de seguridad, o la incorporación de nuevas tecnologías. También se llevará a cabo un análisis de riesgos ante la identificación de nuevas amenazas en el entorno, tales como ataques cibernéticos, vulnerabilidades de software o desastres naturales. Los resultados de cada análisis de riesgos serán documentados en un informe detallado, que incluirá la identificación de riesgos, la evaluación de su impacto y probabilidad, y la definición de medidas de mitigación. Este informe será utilizado para la toma de decisiones y la mejora continua de la seguridad de la información.

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

Para proteger la información confidencial y la seguridad de los sistemas de la Universidad, el acceso telefónico o a Internet para terceros solo se concederá en casos excepcionales y debidamente justificados. En caso de aprobación, se otorgarán privilegios de acceso mínimos y específicos, limitados a los recursos y funciones estrictamente necesarios para la actividad justificada. El acceso será temporal, con una vigencia claramente definida y limitada al período de tiempo requerido. Se utilizarán mecanismos de control de acceso seguros y aprobados por la Oficina Asesora de Planeación y Sistemas, tales como las VPN, y se realizará una auditoría periódica para verificar el cumplimiento de estas políticas. Al finalizar el período de acceso autorizado, se procederá a la revocación inmediata de los privilegios otorgados.

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

Para salvar la información sensible y los activos tecnológicos de la Universidad, todos los computadores multiusuario, equipos de comunicaciones y demás dispositivos que almacenen o procesen datos confidenciales, así como el software licenciado propiedad de la institución, deberán ser ubicados en centros de cómputo seguros. Estos centros contarán con puertas cerradas y controles de acceso físico

rigurosos, tales como sistemas de tarjetas de proximidad, registros de accesos detallados y/o videovigilancia constante. Además, se implementarán medidas de seguridad lógica, incluyendo firewalls, sistemas de detección de intrusiones y cifrado de datos, para proteger los activos de amenazas cibernéticas. El acceso a los centros de cómputo estará restringido al personal autorizado, siguiendo un procedimiento de autorización formal que garantiza la trazabilidad y el control de acceso. Se realizarán auditorías periódicas para verificar el cumplimiento de estas políticas y se establecerán planes de contingencia para responder a posibles incidentes de seguridad.

#### 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.

Para asegurar la continuidad de las operaciones y la protección de la información, cada sistema y recurso informático crítico de la Universidad contará con un plan de contingencia detallado para la restauración de la operación. Este plan incluye la identificación de los sistemas críticos, los tiempos de recuperación objetivo, los procedimientos de respaldo y restauración, y los roles y responsabilidades del personal involucrado. Se elaborará, actualizará y probará periódicamente un plan integral de recuperación de desastres, simulando diversos escenarios de interrupción, para garantizar la disponibilidad de los sistemas y computadores críticos en caso de desastre. Además, se establecerán planes de respuesta a emergencias informáticas, que definirán los procedimientos para la detección, notificación y resolución de incidentes de seguridad. Estos podrán incluir la creación de un equipo de respuesta a emergencias informáticas, con personal capacitado y roles definidos. Todos estos planes se integrarán en el Plan de Contingencia y Continuidad de la Universidad, que será revisado y actualizado periódicamente para reflejar los cambios en la infraestructura tecnológica y las amenazas emergentes.

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

Para garantizar la disponibilidad y el rendimiento óptimo de los sistemas de información, el Centro de Cómputo contará con un equipo de personal técnico competente o empresa tercerizada, con habilidades y certificaciones actualizadas en las tecnologías utilizadas. Este equipo será responsable de la monitorización proactiva de los sistemas, la detección temprana de posibles problemas, la resolución eficiente de incidentes y la implementación de medidas preventivas para minimizar los riesgos. En caso de ser necesario, se podrá delegar la solución de problemas específicos a terceros especializados, seleccionados mediante un proceso riguroso que garantice el cumplimiento de los estándares de seguridad y confidencialidad de la Universidad. Se establecerán acuerdos de nivel de servicio (SLA) claros, que definirán los tiempos de respuesta y resolución de incidentes, así como las responsabilidades de cada parte. Quien deberá informar las actuaciones adelantadas durante el incidente.

#### 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 alterno de control.

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

Los sistemas de computación que manejan información clasificada como sensible registrarán de forma exhaustiva todos los eventos de seguridad relevantes. Estos registros incluirán, como mínimo, la fecha y hora del evento, el usuario o sistema involucrado, el tipo de evento, el origen del evento y una descripción detallada del mismo. Se registrarán, entre otros, los siguientes eventos: intentos fallidos de autenticación, intentos de acceso no autorizado, modificaciones a la configuración del sistema, modificaciones a las aplicaciones, y cualquier actividad que pueda comprometer la confidencialidad, integridad o disponibilidad de la información.

#### 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 cada aplicación se elaborará en estricta conformidad con las políticas de seguridad de la información vigentes de la Universidad, incluyendo, pero no limitándose a, la Política de Control de Acceso y la Política de Protección de Datos. Este esquema detallará los mecanismos de autenticación, autorización, gestión de sesiones, protección de datos y registro de eventos, y deberá alinearse con las mejores prácticas de seguridad de la industria. La aprobación del esquema requerirá la revisión y autorización de la Oficina Asesora de Planeación y Sistemas.

#### 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 la administración de sus plataformas tecnológicas a terceros, con quienes se establecerán acuerdos contractuales que incluyan la divulgación y el cumplimiento obligatorio de las políticas de seguridad de la información vigentes. Se detallarán específicamente las políticas de acceso, gestión de datos y protección de la infraestructura tecnológica. La Universidad supervisará activamente el cumplimiento de estas políticas por parte de los terceros. En caso de que personal interno asuma estas funciones, se aplicarán las mismas políticas.

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

Todos los sistemas y computadores multiusuario de la Universidad soportarán cuentas de administrador con privilegios elevados, necesarias para las labores administrativas. Estos privilegios se asignarán exclusivamente a personal autorizado, mediante un proceso formal y documentado. Se implementará un sistema de control de acceso basado en roles (RBAC) para gestionar los privilegios de administrador, y se realizarán auditorías periódicas del uso de estos privilegios

#### 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 limitará a tres (3) los intentos consecutivos de inicio de sesión con contraseña incorrecta. Tras el tercer intento fallido, se aplicará un bloqueo temporal de la cuenta por un período de 15 minutos. En caso de conexiones remotas, la sesión será desconectada inmediatamente. Se registrarán todos los intentos fallidos en un registro de auditoría. El desbloqueo de cuentas suspendidas requerirá la intervención del administrador, quien verificará la identidad del usuario antes de reactivar la cuenta.

#### 8.5. Cambio de contraseñas por defecto.

Todas las contraseñas por defecto de equipos y sistemas nuevos se cambiarán durante el proceso de configuración inicial, antes de su puesta en producción, siguiendo los lineamientos de la política 2.6, "Contraseñas deben ser difíciles de adivinar". Se registrarán todos los cambios de contraseñas por defecto en un registro de auditoría. El sistema prevendrá la reutilización de contraseñas por defecto. El personal responsable de la instalación y configuración de los equipos y sistemas será el encargado de realizar el cambio de contraseñas.

#### 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 garantizarán que personas ajenas a la Universidad, incluyendo individuos no empleados, contratistas o consultores, no dispongan de privilegios de acceso a los recursos tecnológicos internos de la Institución. Cualquier excepción a esta norma requerirá una autorización escrita y formalizada por la Oficina Asesora de Planeación y Sistemas, la cual especificará los privilegios otorgados, el período de validez y las condiciones de uso. Se implementarán registros de auditoría para monitorizar y controlar el acceso de terceros a los recursos tecnológicos.

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

Previo al otorgamiento de acceso a terceros a los recursos tecnológicos de la Universidad, se formalizará un contrato que defina claramente los términos y condiciones del acceso, incluyendo los recursos específicos a los que se permitirá el acceso, el alcance de los privilegios otorgados, el período de validez del acceso, y las responsabilidades del tercero en materia de seguridad de la información. El contrato incluirá cláusulas sobre los derechos de la Universidad, las obligaciones de confidencialidad del tercero, y las consecuencias del incumplimiento. Se designará un responsable para supervisar el cumplimiento del contrato, y se realizarán auditorías periódicas del acceso 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.

Los administradores de sistemas multiusuario dispondrán de dos cuentas de usuario separadas: una con privilegios de administrador y otra con privilegios de usuario estándar. La cuenta de administrador se utilizará exclusivamente para tareas administrativas, mientras que la cuenta de usuario estándar se utilizará para las actividades diarias. Esta separación de privilegios minimiza el riesgo de errores y ataques,

y facilita la auditoría de las actividades administrativas. El uso de la cuenta de administrador se registrará en un registro de auditoría.

**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. Captura de información en casos de sospecha de crimen informático o abuso.**

Ante la sospecha de un incidente de seguridad informática, se procederá a la recolección inmediata de evidencia para su uso en investigaciones, procesos judiciales o acciones disciplinarias. La información para recolectar incluirá, como mínimo, la configuración actual del sistema, copias de seguridad, registros de eventos, archivos potencialmente comprometidos y cualquier otra información relevante para la investigación. La recolección de evidencia se realizará siguiendo un procedimiento documentado que garantice la integridad y autenticidad de la información, y se mantendrá una cadena de custodia detallada. La evidencia se almacenará de forma segura en un dispositivo externo y protegido.

**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.

Implementar un programa continuo de gestión de vulnerabilidades que incluye escaneos automatizados semanales con herramientas especializadas, pruebas de penetración (mínimo 1 por año) realizadas por expertos externos y la aplicación inmediata de parches de seguridad para todas las vulnerabilidades críticas detectadas. Este programa debe complementarse con revisiones periódicas de la configuración de seguridad y la capacitación del personal en buenas prácticas de seguridad informática.

#### 8.22. Uso de 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.

Los registros de aplicación que contienen eventos relevantes de seguridad deben ser almacenados por un período mínimo de doce (12) meses en un sistema centralizado de gestión de registros de seguridad (SIEM). Durante este período, los registros deben ser protegidos mediante cifrado y controles de acceso basados en roles (RBAC) para garantizar su integridad y confidencialidad. Se debe implementar un proceso de revisión y análisis periódico de los registros para detectar y responder a incidentes de seguridad de manera proactiva. Además, se debe establecer un procedimiento para la exportación y el análisis forense de los registros en caso de incidentes de seguridad.



### 9.2. Tipo de datos a los que se les debe hacer backup y la 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. Número de copias sobre información sensible.

Se generarán al menos dos copias de seguridad de cada conjunto de datos críticos. Una copia se almacenará en un medio físico diferente al original y en una ubicación geográfica distinta, para proteger contra desastres locales. La segunda copia se resguardará en un entorno de nube seguro, con cifrado y controles de acceso estrictos. El procedimiento de respaldo, que forma parte integral de esta política, detallará los tipos de respaldo, las frecuencias, los medios de almacenamiento permitidos, los responsables y los pasos para la restauración segura de los datos.

## 10. Políticas de Uso de Firewall

### 10.1. Detección de intrusos.

Todos los segmentos de red, incluyendo redes cableadas e inalámbricas, zonas desmilitarizadas (DMZ) y conexiones de red privada virtual (VPN), que sean accesibles desde Internet, deberán contar con sistemas de detección de intrusos (IDS) y sistemas de prevención de intrusos (IPS) configurados para detectar y bloquear tanto ataques conocidos como comportamientos anómalos.

### 10.2. Protección de las conexiones externas.

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. Protección de las conexiones desde y hacia Internet.

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 dependencia de seguridad informática de la universidad, o quien haga sus veces, deberá garantizar que las políticas del servidor proxy incluyan el filtrado de contenido activo y potencialmente malicioso, como scripts, ejecutables, y otros objetos que puedan representar riesgos de seguridad. Esto incluye, pero no se limita a, la inspección y bloqueo de applets de Java, contenido Flash (anteriormente Macromedia), controles ActiveX y cualquier otro tipo de contenido que pueda ser utilizado para explotar vulnerabilidades en los sistemas de información de la universidad.

#### 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.

La información confidencial relacionada con la infraestructura de red interna, incluyendo direcciones IP, topología de red, configuraciones de servidores y otros detalles técnicos, deberá ser protegida mediante controles de acceso estrictos. Solo los usuarios y sistemas autorizados que pertenezcan a la red interna de la universidad, y que requieran esta información para sus funciones, podrán acceder a ella. Se implementará de seguridad para prevenir el acceso no autorizado desde redes externas, incluyendo Internet, y desde usuarios internos que no tengan los privilegios necesarios.

#### 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 exigirá la aceptación explícita de los términos y condiciones por parte de todos los clientes antes de procesar cualquier orden de compra de productos o servicios en línea. Esta aceptación se realizará mediante un mecanismo de confirmación electrónica, como una casilla de verificación o un botón de "Acepto", que registre la fecha y hora de la aceptación. Los términos y condiciones, que detallan los derechos y responsabilidades de ambas partes, estarán claramente visibles y accesibles en la página web de la universidad, y se proporcionará un enlace directo a ellos durante el proceso de compra.

#### 11.2. Acuerdos con terceros que manejan información o cualquier recurso informático de la universidad

Todos los acuerdos celebrados con terceros que involucran el manejo de información confidencial o recursos informáticos propiedad de la universidad, deberán incluir una cláusula contractual detallada que establezca las obligaciones de confidencialidad, las restricciones de uso de la información, los derechos de propiedad intelectual y los mecanismos de protección de datos. Esta cláusula otorgará a la universidad

el derecho de realizar auditorías periódicas para verificar el cumplimiento de los controles de seguridad implementados por el tercero, incluyendo la revisión de políticas, procedimientos y registros de acceso. Se especificarán los requisitos mínimos de seguridad que el tercero deberá cumplir, así como los procedimientos de notificación en caso de incidentes de seguridad.

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

Todos los terceros que tengan acceso a información o recursos informáticos de la universidad, incluyendo socios de negocios, proveedores y clientes, deberán conocer y cumplir con las políticas de seguridad informática de la universidad. Esta responsabilidad se establecerá claramente en los contratos y acuerdos, y será verificada y monitoreada por el departamento de seguridad informática de la universidad. Los contratos con terceros incluirán, como mínimo, los siguientes elementos:

- Definición clara de los niveles de servicio y operación esperada.
- Acuerdos de confidencialidad que protegen la información manejada y las actividades realizadas.
- Definición de la propiedad de la información y las restricciones de uso.
- Restricciones sobre el uso de software y hardware, incluidas licencias y actualizaciones.
- Requisitos de seguridad informática y física, incluidos controles de acceso y protección de datos.
- Procedimientos de notificación y respuesta ante incidentes de seguridad, como la alteración o manipulación de dispositivos o información.
- Procedimientos para la entrega y destrucción segura de la información al finalizar el servicio.
- Requerimiento de un plan de continuidad y contingencia por parte del tercero.

## 12. Políticas de Acceso Físico

La Universidad implementará las presentes políticas de seguridad informática en todos sus entornos de infraestructura, independientemente de su ubicación física o arquitectura. Se establecerán controles de seguridad coherentes y adaptados a las características de cada entorno, incluyendo centros de datos, instalaciones de comunicaciones y entornos en la nube. Se garantizará la protección de la información y los recursos informáticos, independientemente de su seguridad, mediante la implementación de medidas de perimetral, segmentación de red, cifrado de datos y controles de acceso estrictos.

### 12.1. Requerimiento de la apertura del Centro de Cómputo.

En situaciones excepcionales donde la puerta del centro de cómputo deba permanecer abierta, como durante el traslado de equipos, se implementará una vigilancia física continua por personal de seguridad designado en compañía de personal del área de Sistemas. Este personal estará capacitado para controlar el acceso, registrar las entradas y salidas, y responder a cualquier actividad sospechosa. Se aplicarán estrictamente las políticas de control de acceso, registro de visitantes y monitoreo de video durante estos períodos. Se documentarán los motivos y la duración de la apertura de la puerta, así como los nombres del personal de vigilancia.

### 12.2. Paso a través de puertas controladas.

Todo el personal de la universidad, especialmente aquellos designados para la seguridad física, deberá impedir el acceso a las zonas restringidas a personas no identificadas o que no cuenten con la autorización correspondiente. Se implementará un sistema de identificación y control de acceso que permitirá verificar la identidad y los permisos de cada persona antes de permitir el ingreso a estas zonas. Se definirá claramente qué áreas se consideran restringidas y se señalarán adecuadamente. Se mantendrá un registro de todas las entradas y salidas de las zonas restringidas

### 12.3. Protocolo de acceso al Centro de Cómputo.

Todo usuario, incluyendo personal interno, personal externo y visitantes, deberá cumplir estrictamente con el procedimiento de acceso y permanencia establecido para las áreas del centro de cómputo. Este procedimiento incluye los siguientes pasos:

**Identificación y registro:** Todo usuario deberá identificarse y registrar su ingreso y salida en el sistema de control de acceso.

**Autorización:** Solo se permitirá el acceso a usuarios autorizados, según sus roles y responsabilidades.

**Acompañamiento:** Los visitantes deberán estar acompañados por personal autorizado durante su permanencia en el centro de cómputo.

**Restricciones:** Se prohibirá el ingreso de dispositivos no autorizados, alimentos, bebidas y otros elementos que puedan comprometer la seguridad o el funcionamiento del centro de cómputo.

**Conducta:** Se exigirá un comportamiento adecuado y respetuoso durante la permanencia en el centro de cómputo, evitando actividades que puedan interferir con las operaciones o la seguridad.

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

El acceso físico a todas las oficinas, salas de servidores, salas de equipos de comunicaciones y puestos de trabajo que contengan información confidencial o crítica deberá ser restringido y controlado. Se implementarán medidas de seguridad física que incluirán:

- Sistemas de control de acceso electrónico con registro de entradas y salidas.
- Cámaras de vigilancia con grabación continua y monitoreo en tiempo real.
- Puertas y ventanas reforzadas con cerraduras de alta seguridad.
- Alarmas de intrusión y detección de movimiento.
- Restricción de acceso solo a personal autorizado, con identificación y verificación de permisos.
- Registro de visitantes y acompañamiento por personal autorizado.
- Se definirá claramente qué información se considera sensible y qué áreas requieren restricción de acceso, y se señalará adecuadamente.

#### 12.5. Controles de acceso en áreas que contienen información sensible.

Todas las áreas que contienen información clasificada como confidencial o crítica deberán implementar controles de acceso físicos y lógicos efectivos. Estos controles incluirán:

- Sistemas de control de acceso electrónico con identificación y verificación de usuarios autorizados.
- Cámaras de vigilancia con grabación continua y monitoreo en tiempo real.
- Puertas y ventanas reforzadas con cerraduras de alta seguridad y alarmas de intrusión.
- Restricción de acceso solo a personal autorizado, con registro de entradas y salidas.
- Sistemas de autenticación multifactor para el acceso a sistemas informáticos y datos sensibles.
- Cifrado de datos en reposo y en tránsito.
- Auditorías periódicas de los registros de acceso y los controles de seguridad.

#### 12.6. Orden de salida para equipos de TI

Ningún equipo electrónico propiedad de la universidad, incluyendo computadoras portátiles, tabletas, teléfonos móviles y dispositivos de almacenamiento, podrá ser retirado de las instalaciones sin una orden de salida previamente autorizada por la Oficina de Sistemas.

#### 12.7. Manejo de los privilegios de acceso ante la terminación del vínculo laboral.

Al término de la relación laboral, independientemente de la causa, el empleado deberá devolver inmediatamente todos los objetos, incluyendo carnets, tarjetas, llaves y dispositivos biométricos. Asimismo, se revocará de forma inmediata todo privilegio de acceso lógico a los sistemas informáticos y datos de la universidad.

### 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

La Oficina de Inventarios, en colaboración con el departamento de seguridad informática, establecerá y mantendrá un inventario actualizado de todos los activos de información de la universidad. Este inventario incluirá la identificación, clasificación, valoración y asignación de responsabilidades para cada activo. Se definirán criterios claros para la clasificación de los activos según su criticidad y sensibilidad, y se implementarán controles de seguridad adecuados para proteger su confidencialidad, integridad y disponibilidad. Se divulgarán lineamientos específicos para el buen uso de los activos de información, incluyendo políticas de acceso, almacenamiento y eliminación segura.

### 13.2. Protección

Cada dependencia de la universidad, responsable de la información generada en el ejercicio de sus funciones, deberá implementar controles de seguridad físicos y lógicos para proteger dicha información. Estos controles incluirán:

La implementación de medidas para garantizar la confidencialidad, integridad, disponibilidad y trazabilidad de la información.

El mantenimiento y actualización periódica de un inventario detallado de los activos de información relacionados con sus servicios, incluyendo información física y digital, software, hardware y personal.

La definición y aplicación de políticas de acceso, uso, almacenamiento y eliminación segura de la información.

La realización de evaluaciones de riesgos periódicas para identificar vulnerabilidades y amenazas.

La implementación de procedimientos de respuesta ante incidentes de seguridad.

### 13.3. Archivos de Gestión

La Oficina Asesora de Planeación y Sistemas implementará controles de seguridad físicos y lógicos para proteger los archivos de gestión de la universidad, tanto físicos como digitales, de acuerdo con las Tablas de Retención Documental y la normativa vigente. Estos controles incluyen:

Control de acceso físico y lógico a los archivos de gestión, basado en roles y permisos.

Sistemas de almacenamiento seguro para los archivos físicos, con protección contra incendios, inundaciones y otros riesgos.

Cifrado de datos para los archivos digitales y sistemas de control de acceso para protegerlos contra accesos no autorizados.

Implementación de procedimientos de copia de seguridad y recuperación de datos para garantizar la disponibilidad de la información.

### 13.4. Devolución de los Activos

Al término de su relación laboral, contrato o acuerdo con la universidad, todo el personal y los usuarios externos deberán devolver la totalidad de los activos de la organización que se encuentren bajo su responsabilidad. Esto incluye, pero no se limita a, equipos informáticos, dispositivos móviles, documentos físicos y digitales, credenciales de acceso físico y lógico, software y cualquier otro bien propiedad de la universidad. La devolución de los activos deberá realizarse dentro de un plazo máximo de cinco (5) días hábiles a partir de la fecha de terminación de la relación laboral, 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

Toda información de la universidad ya sea en formato digital o físico, debe protegerse durante su traslado para evitar accesos no autorizados, modificaciones o pérdidas. Esto incluye, pero no se limita a, documentos impresos, archivos digitales en computadoras, discos duros, memorias USB y otros dispositivos. El traslado de esta información se realizará siguiendo protocolos de seguridad que consideran la importancia de la información y el impacto que su pérdida o alteración podría tener en las actividades de la universidad. Para equipos como computadoras o servidores, se tienen medidas adicionales como el cifrado de datos y El seguimiento del traslado. Cada departamento o área de la universidad será responsable de aplicar estos protocolos y de capacitar a su personal en el manejo seguro de la información.

## 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 con el 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

La universidad actualizará su política de seguridad informática para adaptarse a los avances tecnológicos, las nuevas amenazas y las leyes. Los cambios en esta política se comunicarán a todos los usuarios y proveedores de servicios a través de correo electrónico, publicaciones en la intranet y reuniones informativas. Los proveedores son responsables de asegurar que su personal conozca y cumpla con la versión más reciente de la política. La universidad realizará actualizaciones periódicas de la política y proporcionará resúmenes de los cambios importantes.

## LISTADO DE ANEXOS

Para complementar la política de seguridad de la información de la universidad, se incluyen los siguientes anexos:



RECTORÍA

**Anexo 1:** Acuerdo de Confidencialidad (Versión 1.0): Documento legal que establece las obligaciones de confidencialidad para empleados, proveedores y terceros que manejan información de la universidad.

**Anexo 2:** Autorización de Traslado de Equipos (Versión 1.0): Formulario para solicitar y autorizar el traslado de equipos informáticos fuera de las instalaciones de la universidad, asegurando la protección de la información durante el transporte.

**Anexo 3:** Formato de Inventario de Equipos y Recursos Informáticos (Versión 1.0): Plantilla para registrar y mantener actualizado el inventario de todos los equipos y recursos informáticos de la universidad, incluyendo información sobre su ubicación, propietario y estado.

**Anexo 4:** Formato de Solicitud y Entrega de Préstamo de Recursos Informáticos (Versión 1.0): Formulario para solicitar y registrar el préstamo de recursos informáticos a empleados o terceros, estableciendo las condiciones de uso y devolución.

**Anexo 5:** Catálogo de Programas (Versión 1.0): Documento que lista todos los programas y aplicaciones utilizadas en la universidad, incluyendo información sobre su licencia, versión y propietario.

